Dagli autori della rivista di informatica e tecnologia **più venduta in Italia**

EDIZIONI MASTER

Anno VII - n.ro 1 (16) • **FEBBRAIO-MARZO** 2015 • Periodicità bimestrale

Il DVD usato dagli **INVESTIGATORI INFORMATICI**

SPECIALI

Win Magazine

IL MANUALE DEL PERFETTO CYBER 007

CON LICENZA DI SPIARE

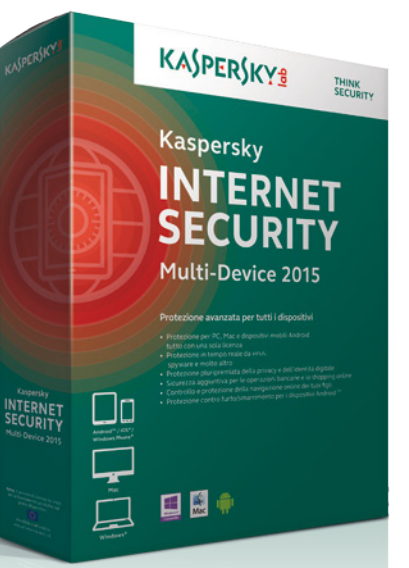
Scopri le tecniche e i software che gli agenti segreti informatici utilizzano per **entrare in qualsiasi computer**

■ **Scova documenti privati**, profili Facebook, foto... ■ **Analizza PC, tablet e cellulari** alla ricerca di informazioni nascoste ■ **Smaschera i bugiardi** col software "Macchina della verità" ■ **Rimuovi a fondo foto compromettenti** e **dati sensibili** ■ **Blocca eventuali hacker** nella tua rete ■ **Intercetta telefonate, e-mail e sms** ■ **Naviga su Internet in perfetto** anonimato e senza lasciare tracce

I tuoi dispositivi parlano di te. Proteggili.

Kaspersky Internet Security — Multi-Device 2015

- Protezione per PC, Mac e dispositivi mobili Android, tutto con una sola licenza
- Protezione in tempo reale da virus, spyware e molto altro
- Sicurezza aggiuntiva per le operazioni bancarie e lo shopping online
- Protezione contro furto/smarrimento per i dispositivi Android



PENSACI. NOI LO FACCIAMO.

KASPERSKY LAB TEAM

www.kaspersky.it

KASPERSKY lab

IL MANUALE DEL PERFETTO CYBER 007

CON LICENZA DI SPIARE

Scopri le tecniche e i software che gli agenti segreti informatici utilizzano per **entrare in qualsiasi computer**

■ **Scova documenti privati**, profili Facebook, foto... ■ **Analizza PC, tablet e cellulari** alla ricerca di informazioni nascoste ■ **Smaschera i bugiardi** col software "Macchina della verità" ■ **Rimuovi a fondo foto compromettenti** e **dati sensibili** ■ **Blocca eventuali hacker** nella tua rete ■ **Intercetta telefonate, e-mail e sms** ■ **Naviga su Internet in perfetto** anonimato e senza lasciare tracce

Sommario

Win Magazine Speciali
Anno VII - n.ro 1 (16) - Febbraio/Marzo 2015
Periodicità bimestrale
Reg. Trib. di Cs: 741 del 6 Ottobre 2009
Cod. ISSN: 2037-1608
e-mail: winmag@edmaster.it
www.winmagazine.it

DIRETTORE EDITORIALE: Massimo Mattone
DIRETTORE RESPONSABILE: Massimo Mattone

RESPONSABILE EDITORIALE: Gianmarco Bruni

EDITOR: Carmelo Ramundo
REDAZIONE: Paolo Tarsitano, Giancarlo Giovinazzo, Raffaele del Monaco

SEGRETERIA DI REDAZIONE: Rossana Scarcelli

REALIZZAZIONE GRAFICA: CROMATIKA s.r.l.
RESPONSABILE GRAFICO DI PROGETTO: Salvatore Vuono
AREA TECNICA: Giancarlo Sicilia (Responsabile), Dario Mazzei
ILLUSTRAZIONI: Tony Intieri
IMPAGINAZIONE: E. Monaco, L. Ferraro, F. Maddalone, T. Diacono

PUBBLICITÀ: MASTER ADVERTISING s.r.l.
Viale Andrea Doria, 17 - 20124 Milano - Tel. 02 83121211
Fax 02 83121207
advertising@edmaster.it

EDITORE: Edizioni Master S.p.A.
Via B. Diaz, 13 – 87036 RENDE (CS)
PRESIDENTE E AMMINISTRATORE DELEGATO: Massimo Sesti

ARRETRATI
ITALIA
Costo arretrati (a copia): il prezzo di copertina + € 6,10 (spedizione con corriere).
Prima di inviare i pagamenti, verificare la disponibilità delle copie arretrate inviando una e-mail ad arretrati@edmaster.it e la copia del pagamento potrà essere inviata via email o via fax al n. 199.50.00.05. La richiesta contenente i Vs. dati anagrafici e il nome della rivista, dovrà essere inviata via fax al num. 199.50.00.05* oppure via posta a EDIZIONI MASTER S.p.A. Viale Andrea Doria, 17 - 20124 Milano, dopo avere effettuato il pagamento, secondo le modalità di seguito elencate:

- assegno bancario non trasferibile (da inviare in busta chiusa con la richiesta);
- carta di credito, circuito Visa, Cartasì, o Eurocard/Mastercard (inviando la Vs. autorizzazione, il numero di carta, la data di scadenza, l'intestatario della carta e il codice CVV2, cioè le ultime 3 cifre del codice numerico riportato sul retro della carta).
- Bonifico bancario intestato a EDIZIONI MASTER S.p.A. c/o BANCA DI CREDITO COOPERATIVO DI CARUGATE E INZAGO S.C. - IBAN IT47R0845333200000000066000 (inviare copia della distinta insieme alla richiesta).

SOSTITUZIONE: Qualora nei prodotti fossero rinvenuti difetti o imperfezioni che ne limitassero la fruizione da parte dell'utente, è prevista la sostituzione gratuita, previo invio del materiale difettato. La sostituzione sarà effettuata se il problema sarà riscontrato e segnalato entro e non oltre 10 giorni dalla data effettiva di acquisto in edicola e nei punti vendita autorizzati, facendo fede il timbro postale di restituzione del materiale.
Inviare il supporto difettoso in busta chiusa a:
Edizioni Master - Servizio clienti Viale Andrea Doria, 17 - 20124 Milano

SERVIZIO CLIENTI
servizioclienti@edmaster.it
199.50.00.05* sempre in funzione
199.50.50.51* dal lunedì al venerdì 10.00 -13.00
*Costo massimo della telefonata 0,118 € + iva a minuto di conversazione, da rete fissa, indipendentemente dalla distanza. Da rete mobile costo dipendente dall'operatore utilizzato.

ASSISTENZA TECNICA (e-mail): winmag@edmaster.it
STAMPA: GRAFICA VENETA S.p.A. - Via Malcanton, 2
35010 Trebaseleghe (PD)
DUPLICAZIONE SUPPORTI: Ecodisk S.r.L. - Via dell'Aprica, 16 - 20158 Milano

DISTRIBUTORE ESCLUSIVO PER L'ITALIA:
m-dis distribuzione media S.p.A. - via Cazzaniga, 19 - 20132 Milano
tel: 02/25.82.1

Finito di stampare nel mese di Gennaio 2015

Sommario

I prezzi di tutti i prodotti riportati all'interno della rivista potrebbero subire variazioni e sono da intendersi IVA inclusa

INCLUDE
DVD da 4,3 GB

OSForensics 0.99i
Esaminiamo a fondo gli aspetti più nascosti del sistema
Tipo: Freeware
File: OSForensics.zip

abylon BASIC 11
Metti in cassaforte file e dati sensibili
Tipo: Commerciale completo
File: Basic11.zip

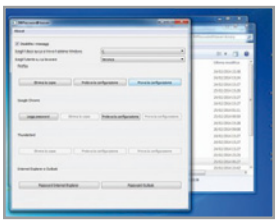
G Data Internet Security Suite 2015
La suite di sicurezza che blinda il PC
Tipo: Completo
File: ITA_R_TRL_AutoTrial_2015.zip

Active@ File Recovery 12
Recuperare file cancellati dal disco per sbaglio
Tipo: Trial
File: filerecovery-demo.zip

Eulerian video Magnification
Macchina della verità? Di più!
Tipo: Freeware
File: EulerianVideoMagnification.zip

Driver Genius 12
Backup, aggiornamento e ripristino dei driver
Tipo: Commerciale completo
File: Driver_Genius_12_PRO_ITA.zip

WMPasswordHoover
La chiavetta di WinMagazine che aspira le password
Tipo: Freeware
File: WMPasswordHoover.zip



Disk Wipe
Radi a zero il contenuto delle memorie digitali
Tipo: Freeware
File: diskwipe.zip

Wondershare Dr.Fone
Recupera i file importanti dallo smartphone
Tipo: Trial
File: drfone.zip

Google Chrome 39.0.2171.65
Il browser multifunzione che mette il turbo
Tipo: Freeware
File: ChromeSetup.zip

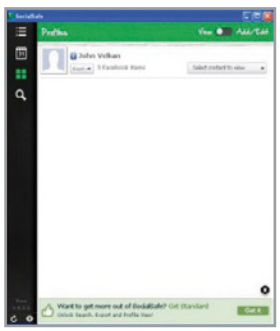
Windows Media Encoder
Codifica e gestione di contenuti multimediali
Tipo: Freeware
File: WMEncoder.zip

Ivideon Server 3.4.6
Crea un sistema di videosorveglianza con il PC
Tipo: Freeware
File: IvideonServer_3.4.6_win32_setup.zip

OpenVPN
Connettiti in rete con la massima invisibilità
Tipo: Freeware
File: openvpn.zip

FBChecker
Scoprire i falsi profili di Facebook
Tipo: Freeware
File: fbchecker.zip

SocialSafe
Backup totale del profilo
Tipo: Freeware
File: SocialSafe.zip

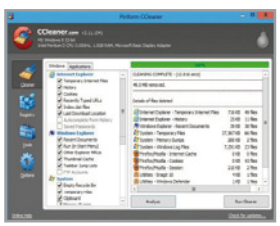


OpenWRT per Raspberry Pi
Il lampone viaggia in rete
Tipo: Freeware
File: openwrt_rasp.zip

Win32DiskImager 0.9.5
Il tool per avviare i sistemi operativi da Pendrive USB
Tipo: Freeware
File: Win32DiskImager-0.9.5-install.zip

Convert-All Media Converter
Converti l'impossibile
Tipo: Freeware
File: convertall.zip

CCleaner 4.18
Ripulisci a fondo il PC da file inutili e obsoleti
Tipo: Freeware
File: ccsetup418.zip



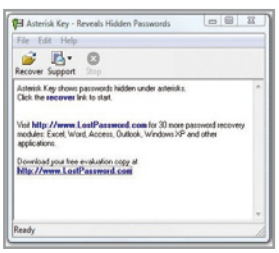
Recuva 1.51.1063
Recupera in un lampo i file cancellati
Tipo: Freeware
File: rcsetup151.zip

TOR Browser 4.01
Naviga e scarica da Internet senza lasciare tracce
Tipo: Freeware
File: torbrowser-install-4.0.1_it.zip

Ophcrack 3.6.0
Recupero immediato della password Windows
Tipo: Freeware
File: ophcrack-win32-installer-3.6.0.zip

UNetbootin 563
Installa Linux sulla tua chiavetta USB
Tipo: Freeware
File: unetbootin-windows-585.zip

Asterisk Key 10.0
Recupera le password nascoste sotto gli asterischi
Tipo: Freeware
File: ariskkey.zip



TrueCrypt 7.1a
Rendi invisibile il sistema operativo installato sul PC
Tipo: Freeware
File: TrueCrypt Setup 7.1a.zip

Dropbox 2.6.2
Gestisci e condividi i file sul Web con chi vuoi tu
Tipo: Freeware
File: Dropbox 2.6.2.zip

Appnimi Word Password Recovery 1.1
Recupera i documenti Word protetti da password
Tipo: Freeware
File: Appnimi-Word-Password-Recovery-Setup-20130918-1.1.zip

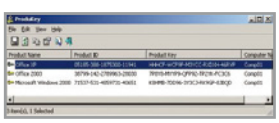
Appnimi PDF Password Recovery 2.0
Recupera file e documenti PDF protetti da password
Tipo: Freeware
File: Appnimi-PDF-Password-Recovery-Setup-20130922-2.0.zip

Appnimi RAR Password Unlocker 2.3
Scova le password usate all'interno dei file Rar
Tipo: Freeware
File: Appnimi-RAR-Password-Unlocker-Setup-20130911-2.3.zip

CryptoSMS
Invia e ricevi SMS criptati
Tipo: Freeware
File: CryptoSMS.zip

NTPassword
Avviare direttamente il PC da CD-ROM
Tipo: Freeware
File: cd140201.zip

ProduKey 1.67
Recupera il codice seriale del tuo sistema operativo!
Tipo: Freeware
File: produkey.zip



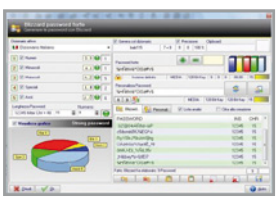
WebBrowserPassView 1.50
In chiaro le password usate nei browser Web
Tipo: Freeware
File: webbrowserpassview.zip

Appnimi RAR Password Unlocker 2.02
Scova con un clic le password dei file Rar
Tipo: Freeware
File: RARPasswordUnlocker.zip

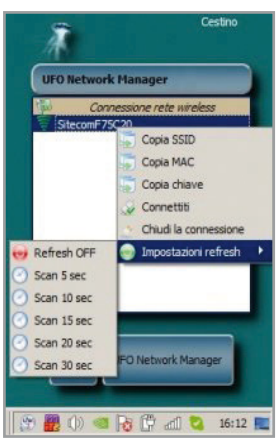
Appnimi PDF Unlocker 2.0
Recupera le password dei documenti PDF
Tipo: Freeware
File: pdfpasswordrecovery.zip

Appnimi Word Password Recovery 2.5
Aprire e recuperare documenti Word protetti
Tipo: Freeware
File: WordPasswordRecovery.zip

Sicurpas Freeware 4.0 Professional
Il tool di sicurezza file e dati Made in Italy
Tipo: Freeware
File: SicurpasFreeware.rar



Ufo Wardriving 4 Invasion
Recupera le chiavi di Rete di tantissimi router Wifi
Tipo: Freeware
File: setup_ufo4.zip



RunAsDate v1.21
Prolunga la data di scadenza dei programmi trial
Tipo: Freeware
File: runasdate.ZIP

OllyDbg 1.10
Il debugger che crea patch per programmi
Tipo: Freeware
File: odbg110.zip

WPA Tester 4
Scova i bug nel tuo router Wifi
Tipo: Freeware
File: www.edmaster.it/url/3528/

Secure Eraser Free 4.201
Cancellazione definitiva di file e cartelle
Tipo: Freeware
File: sEraser.zip

Recuva 1.51.1063
Ripristina in un lampo i file cancellati per errore
Tipo: Freeware
File: rcsetup151.zip

iSpy 6.2.2
Crea e gestisci un sistema di videosorveglianza
Tipo: Freeware
File: iSpy_6_2_2_0.zip

Hide My Windows 2
Nascondere app, finestre e giochi a occhi indiscreti
Tipo: Freeware
File: hidemywins_installer.zip

Clicky Gone Portable 1.4.4.1
Così nascondi finestre Windows e applicazioni
Tipo: Freeware
File: ClickyGone_1.4.4.1.Setup.zip

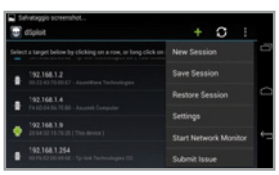
Exif Pilot 4.7.2
Leggere e modificare le informazioni delle foto!
Tipo: Freeware
File: hidemywins_installer.zip

REFOG Free Keylogger
Controllare tutto quello che succede sul computer
Tipo: Freeware
File: free-keylogger.zip

SilentEye
La steganografia per nasconder file e dati
Tipo: Freeware
File: silenteye-0.4.1-win32.zip

G Data Internet Security Suite 2015
La suite di sicurezza che blinda il PC
Tipo: Trial
File: www.edmaster.it/url/3395

dSploit 1.0.31b
L'app android per scardinare qualsiasi rete
Tipo: Freeware
File: dSploit-1.0.31b.zip



WPA Tester Android
Scova i bug nel tuo router Wifi
Tipo: Freeware
File: wpatester.zip

AircrackGUI
Il passepartout per le connessioni WiFi!
Tipo: Freeware
File: aircrack.zip

Music Rescue 4
Recupera la musica da iTunes
Tipo: Freeware
File: musicrescue.zip

RAR PAssword Finder
Le password degli archivi in chiaro
Tipo: Freeware
File: rarpassword.zip

John the Ripper 1.7.9
"Il piede di porco" diventa digitale
Tipo: Freeware
File: john179w2.zip

FaceNiff 2.4
I dati sensibili di Facebook in un tocco
Tipo: Freeware
File: ProgDVB.zip

Foxit Reader 6.0.6
Visualizza al meglio i tuoi PDF
Tipo: Freeware
File: FaceNiff-2.4.zip

Wireshark 1.10.7
Analizza e filtra il contenuto di tutti i pacchetti di rete
Tipo: Freeware
File: Wireshark-win.zip

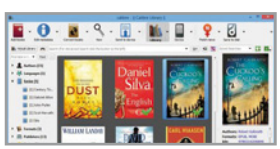
Firesheep
Sniffa tutto dal browser
Tipo: Freeware
File: firesheep.zip

ISO2God
Le ISO su XBOX
Tipo: Freeware
File: iso2god.zip

WBFS Manager 3.0
Tutti i giochi che vuoi, su Wii
Tipo: Freeware
File: wbfs.zip

Calibre 1.34 **+ Plugin**
Legge, converte e gestisce gli e-book
Tipo: Freeware
File: calibre-1.34.0.zip

Cain & Abel 4.2



Un pronto recupero per le password perdute
Tipo: Freeware
File: ca_setup.zip

Il computer poliziotto

Installa subito il software usato dalla Polizia Scientifica e diventa un abile investigatore informatico

Cosa ci occorre

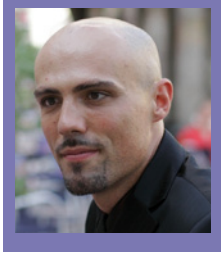
30 MIN. DIFFICILE

TOOL DI ANALISI FORENSE
OS FORENSICS
Lo trovi su: ☑DVD
SOFTWARE COMPLETO
Sito Internet:
www.osforensics.com

NOTE SULL'AUTORE

Vista la complessità e la delicatezza dell'argomento trattato nell'articolo, abbiamo deciso di chiedere un prezioso contributo a uno dei massimi esperti del settore.

Riccardo Meggiato, divulgatore tecnologico che ha realizzato centinaia di guide, tutorial e articoli per numerose riviste e pubblicazioni tecniche, è l'autore del libro "L'investigatore informatico" edito da Apogeo (www.winmagazine.it/link/1088).



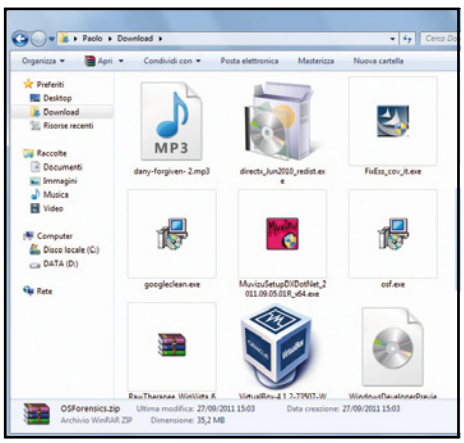
Le parole "Computer Forensics" spaventano un sacco di persone, più che altro perché il loro significato non è così immediato. Diciamo che hanno a che fare con le investigazioni informatiche, quelle che si svolgono su ormai buona parte delle scene del crimine. Di qualsiasi crimine. Partendo da brutte storie di spionaggio, per arrivare ad ancor più spiacevoli omicidi, spesso la risoluzione del caso passa per l'analisi di computer, smartphone, tablet e altri apparecchi digitali che fanno parte del nostro vivere quotidiano, alla pari delle più classiche "armi del delitto". Nella memoria di un computer, per esempio, si può celare la cronologia di una chat nella quale la vittima di un omicidio si è confidata con il suo assassino. Per non parlare della posta elettronica con la quale ha stabilito, magari, luogo e ora del primo, e fatale, appuntamento. Come accennato, la computer forensics riveste un ruolo di grande importanza anche nei casi di spionaggio industriale. Un dipendente invia tramite posta elettronica un allegato con un progetto da milioni di euro, per poi cancellarlo, sicuro di non essere beccato. Così sta all'investigatore setacciare il sistema nel tentativo di riportare in vita l'e-mail e dimostrare la colpevolezza del sospettato.

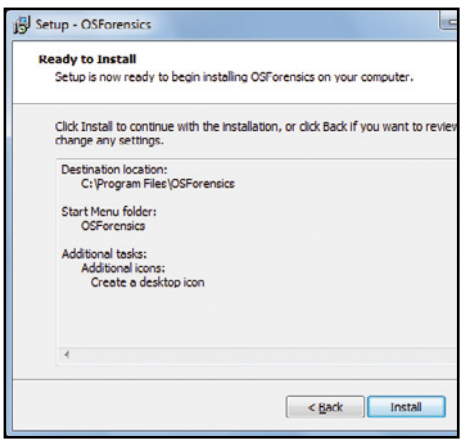
Questione di conoscenze…

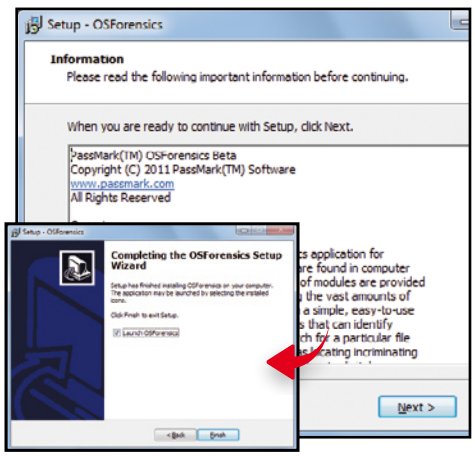
Al solito, tra il dire e il fare c'è di mezzo un mare di tecnica e conoscenze che richiedono una grande preparazione prima di potersi definire esperti di computer forensics. Questa disciplina, infatti, necessita di competenze che riguardano un po' tutti gli aspetti di un sistema informatico. Si parte dalle reti, anche quelle più complesse (necessarie per le strutture industriali), per arrivare al funzionamento a basso

A Prepariamo il segugio

L'installazione di OSForensics non richiede particolari accortezze: bastano solo pochi clic del mouse e al termine saremo pronti per iniziare le indagini forensi sul nostro computer!







1 Tutto a portata di mano

Scompattiamo l'archivio compresso *OSForensics.zip* che troviamo sul DVD-Rom e facciamo doppio clic sul file eseguibile *osf.exe* contenuto al suo interno per avviare la procedura guidata di installazione di OSForensics.

2 L'installazione è cosa fatta

Clicchiamo *Next* nella prima schermata del wizard, spuntiamo *I accept the agreement* per accettare i termini d'uso del software e procediamo con *Next*. Premiamo *Next* nelle schermate successive per accettare le impostazioni predefinite e poi clicchiamo *Install*.

3 Gli ultimi ritocchi

Dopo qualche secondo, apparirà la schermata *Information*: clicchiamo *Next* per proseguire. Lasciamo il segno di spunta su *Launch OSForensics* nella finestra successiva e premiamo su *Finish* per completare la procedura d'installazione e avviare il programma.

livello di ogni periferica, passando per struttura e gestione interna della memoria, protocolli di trasmissione dati e tanto, tantissimo altro ancora. Ovviamente non si può prescindere anche da noiose ma fondamentali competenze legali. Eh sì, perché le indagini, per avere valenza in sede processuale, vanno certificate secondo rigidi parametri, per evitare inquinamenti pronti a mandare in fumo investigazioni lunghe mesi e mesi. È pur vero, tuttavia, che chi vuole divertirsi con la computer forensics può farlo in privato, ignorando un sacco di queste antipatiche nozioni, e ricavandone pure degli strumenti utili per risolvere piccoli misteri quotidiani. Per esempio, per recuperare file cancellati erroneamente, ripristinare e-mail eliminate o spostate in zone nascoste del disco rigido, analizzare attività sospette da parte di colleghi invidiosi nel nostro computer, e via dicendo. Il tutto, se eseguito nel nostro computer, è legale e divertente, ma va da sé che, se applicato su un sistema altrui, si tramuta in vero e proprio spionaggio di alto livello. Un'attività di sicuro emozionante, ma anche illegale: si tratta di scegliere se andare dalla parte dei buoni o dei cattivi.

... ma anche di strumenti

Posto, dunque, che tutti hanno la possibilità di accedere al mondo delle investigazioni informatiche, andiamo a parlare di mezzi, ossia quegli strumenti che consentono di svolgerle. I professionisti, ovviamente, dispongono di un arsenale di programmi e apparecchi costosi, pronti ad accompagnarli dai primi rilievi fino alle analisi finali. La classica indagine, semplificando, inizia infatti con uno studio della scena del crimine e questo viene fatto non solo dall'investigatore informatico ma anche dai colleghi della polizia scientifica. Insomma, si deve stabilire che toccando l'oggetto hi-tech di turno non ci sia il rischio di compromettere altre prove, e dunque si usano lampade U.V. e tutte quegli apparecchi resi famosi da serie come C.S.I.. A questo punto si passa alla vera computer forensics, di solito con un processo chiamato "clonazione". Analizzare direttamente la memoria del computer incriminato, infatti, è pericoloso: qualsiasi utilizzo porta alla modifica di qualche dato. Così si procede con la copia del disco, per creare un clone da analizzare poi con calma, nel proprio laboratorio. Esistono diversi kit utili allo scopo. Alcuni sono sotto forma di valigette con cavetteria assortita e una piccola scheda madre con tutto il necessario per effettuare il trasferimento, in modo veloce e preciso. Altri consistono, più semplicemente, in un notebook con parecchia memoria libera. Il concetto di base, comunque, non è diverso dal fare una copia "byte per byte", la più affidabile, del disco rigido. Per questo motivo, l'importante è scollegare il disco originario, collegarlo alla propria strumentazione, qualunque essa sia, ed effettuare la copia in modalità lettura. Si deve infatti disabilitare qualunque tipo di scrittura verso la memoria prelevata dalla scena del crimine, per evitare di sovrascrivere e cancellare per sempre dati che potrebbero tornare utili alle indagini.

Investigazioni per tutti

Una volta che il disco è nelle mani dell'investigatore, si procede con la sua analisi. Questa viene effettuata con una molteplicità di metodi diversi. C'è chi apprezza il "fai da te", quindi si adopera con software in grado di analizzare ogni singoli indirizzo di memoria, e chi invece vuole semplificarsi la vita, sfruttando programmi automatici e dannatamente costosi

BUONI CONSIGLI

UTILI ALLEGATI

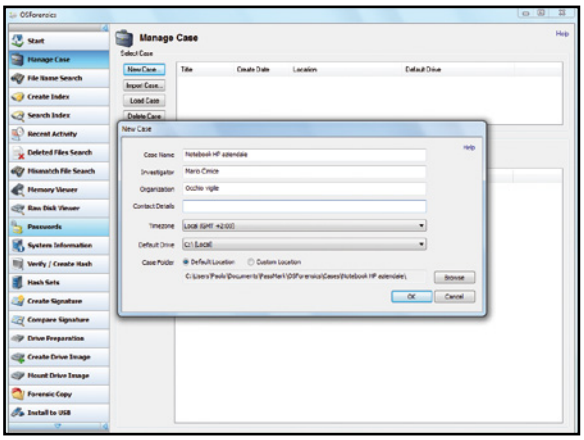
Così come avviene nella realtà, anche al nostro faldone digitale delle indagini possiamo allegare immagini o documenti che, in futuro, ci potrebbero aiutare a ricostruire il "caso". Dall'interfaccia principale di OSForensics clicchiamo su *Manage case*, selezioniamo l'indagine che ci interessa (archiviata nel Macropasso B) e premiamo il pulsante *Add Attachment*. Nella schermata che appare selezioniamo il file da allegare, clicchiamo *Apri* e poi *Add*. Per visualizzarlo, successivamente, basterà evidenziarlo nella sezione *Case Items* e cliccare su *Open*.

CHAT SOTTO CONTROLLO

Una delle attività più comuni al computer è sicuramente la chat, usata da tutti per comunicare velocemente con i propri amici. Nella cronologia dei programmi di chat, quindi, è possibile trovare ogni tipo di informazione, anche quelle più compromettenti. Persino il sicuro Skype non scappa a questa regola. Se l'utente non si ricorda di cancellare periodicamente la cronologia (da *Strumenti/Opzioni/Privacy*, cliccando *Cancella la cronologia*), basta un tool gratuito come SkypeLogView (www.winmagazine.it/link/1087), che non deve essere neanche installato, per leggere tutti i vecchi messaggi scambiati via chat.

B Si parte con le indagini

Un investigatore che si rispetti sa sempre come analizzare un sistema nel minimo dettaglio. Ecco come scoprire i segreti che il proprietario di un PC vuol nascondere a occhi indiscreti!

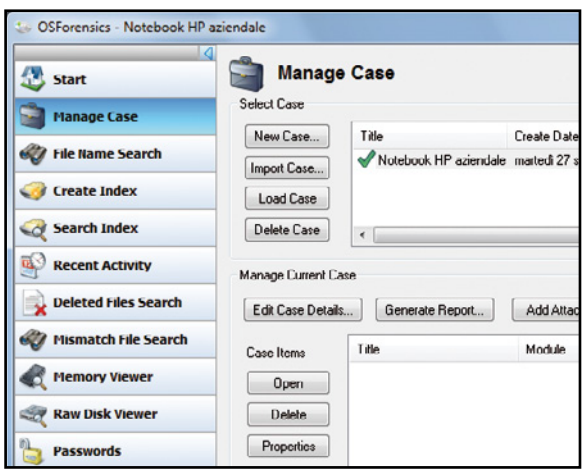


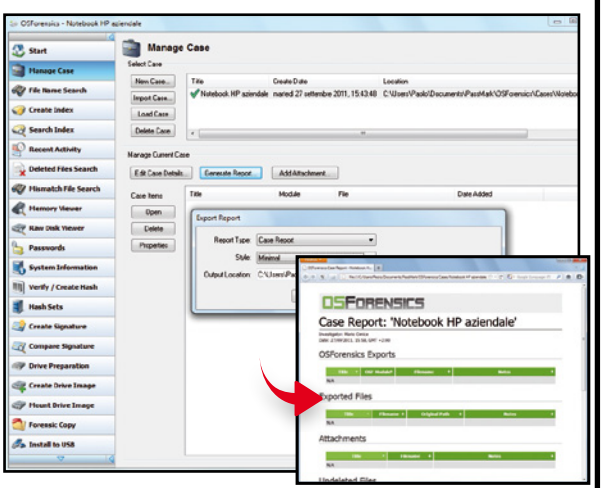
1 Iniziamo l'analisi

La prima operazione da compiere è quella di aprire un incartamento per le indagini, usando il gergo dei vecchi investigatori. Noi parliamo di informatica e così apriremo una cartella, nella quale andremo ad archiviare tutti i risultati delle nostre analisi. In *Start* clicchiamo *Create Case*.

2 I dettagli del caso

Come tutte le cartelline documentali che si rispettino, anche per quella digitale servono alcune informazioni per archiviarla correttamente. In *Case name* diamo un nome al caso, indichiamo anche quello dell'investigatore, lasciamo invariate *Timezone*, *Default Drive* e *Case folder* e diamo *OK*.





3 Il faldone delle indagini

Per accedere (anche in seguito) alla cartella contenente tutti i resoconti delle nostre indagini, dall'interfaccia principale di OSForensics accediamo alla sezione *Manage Case*. Per aggiungere ulteriori dettagli sul caso, selezioniamo la cartella e clicchiamo sul pulsante *Edit Case Details*.

4 Il punto della situazione

Per stampare un resoconto delle indagini, selezioniamo il caso che ci interessa e clicchiamo *Generate Report*. In *Export Report* lasciamo invariati i menu *Case Report* e *Style*, e clicchiamo *OK*. Nel percorso indicato in *Output Location* troveremo il report del caso in formato HTML.

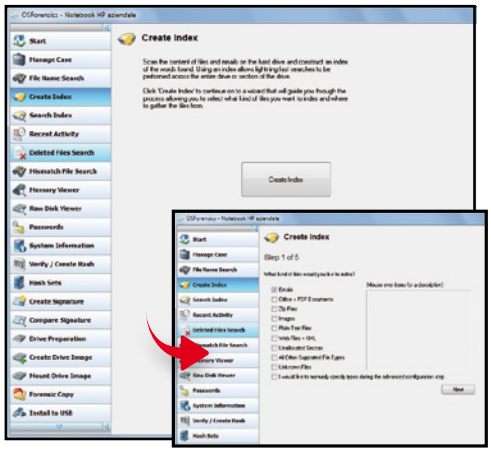
(come EnCase, che è lo standard del settore, www.guidancesoftware.com). E poi c'è chi è furbo e usa OSForensics.

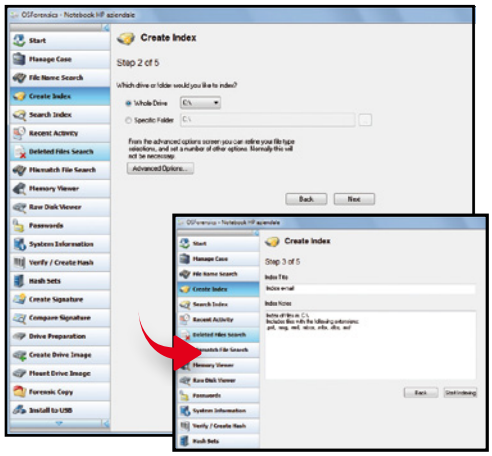
Lo strumento adatto a tutti

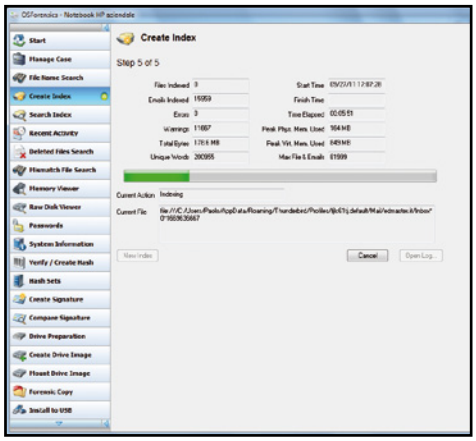
Si tratta di uno dei software più nuovi nel campo della computer forensics, tanto che il suo slogan è "Digital investigation for a new era" (investigazione digitale per una nuova era). Un programma potente e veloce, abbastanza semplice da utilizzare, che include tutti gli strumenti essenziali e professionali per svolgere un'indagine forense accurata oppure un controllo veloce e divertente nel nostro sistema. Tanta bontà si paga cara, circa 400 dollari, ma al momento è disponibile una versione "beta" completa e gratuita, pronta a trasformarci in esperti di computer forensics. In queste pagine, i trucchi per utilizzarla al meglio.

C Prepariamo l'hard disk

Per ottimizzare le ricerche di file nascosti nei meandri dell'hard disk, è opportuno effettuare un'indicizzazione di tutto il contenuto. In questo modo, troveremo le tracce del "crimine" molto più velocemente!







1 Un indice per l'hard disk

Dall'interfaccia principale di OSForensics selezioniamo *Create Index* e clicchiamo *Create Index*. Nella schermata che appare, scegliamo i contenuti da indicizzare (ad esempio, *Emails*, ma possiamo anche selezionare tutte le voci proposte come foto, PDF, ZIP...) e premiamo *Next*.

2 Scansioni approfondite

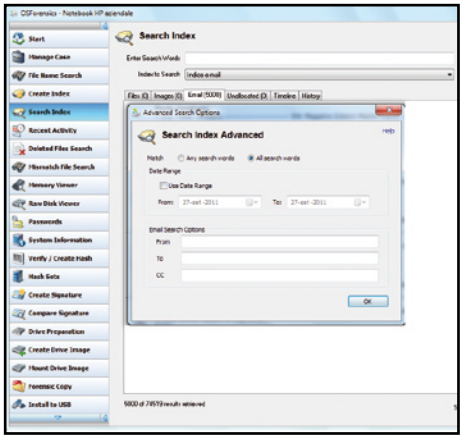
Nella schermata successiva lasciamo attiva la voce *Whole Drive* per indicizzare tutto il contenuto dell'hard disk. Clicchiamo su *Advanced Options* se vogliamo personalizzare la procedura di indicizzazione del disco. Procediamo con *Next* e in *Index Title* diamo un nome all'indice.

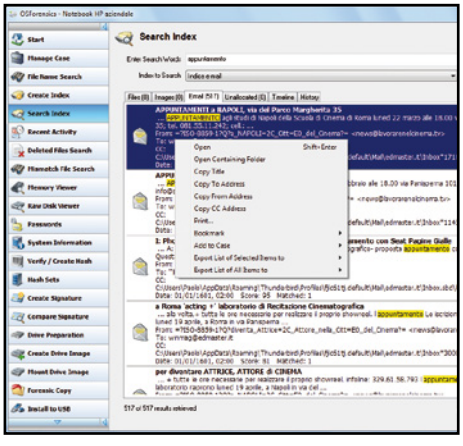
3 Ora è tutto a portata di clic

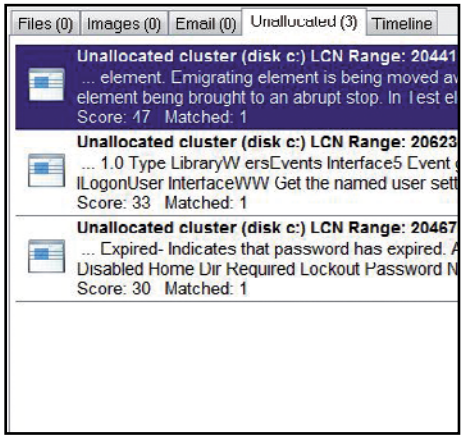
Clicchiamo *Start Indexing* per avviare l'indicizzazione del disco: la procedura durerà diversi minuti, a seconda delle dimensioni dell'hard disk. Una barra di avanzamento ci aggiornerà su quanto tempo manca e quante e-mail sono state indicizzate, gli errori e il tempo trascorso.

D Al via con i recuperi estremi

Ora che il disco è stato indicizzato, possiamo andare alla ricerca di tutte le e-mail archiviate. E non solo quelle elencate nel client di posta elettronica, ma anche quelle già cancellate! Ecco come procedere.







1 Parole compromettenti

Spostiamoci in *Search Index*: in *Enter Search Words* scriviamo una parola chiave che potrebbe essere contenuta nelle e-mail incriminate e in *Index to search* indichiamo dove cercarla. Clicchiamo sul pulsante *Search* per avviare l'operazione.

2 Ecco tutte le tracce

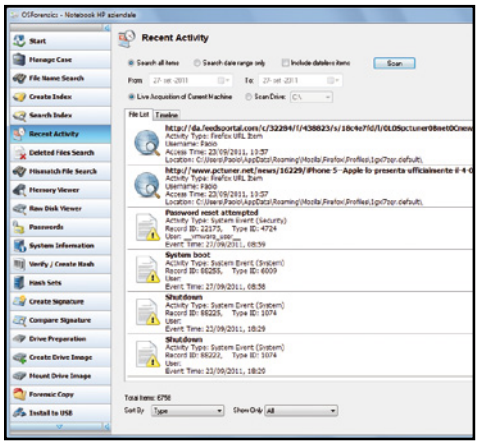
Terminata la ricerca, i risultati verranno elencati nella schermata *Search Index*, ordinati per tipologia. Nel nostro caso, spostiamoci nel tab *Email*. Avremo un'anteprima di quelle contenenti la parola chiave. Per leggerle, selezioniamole col tasto destro del mouse e clicchiamo *Open*.

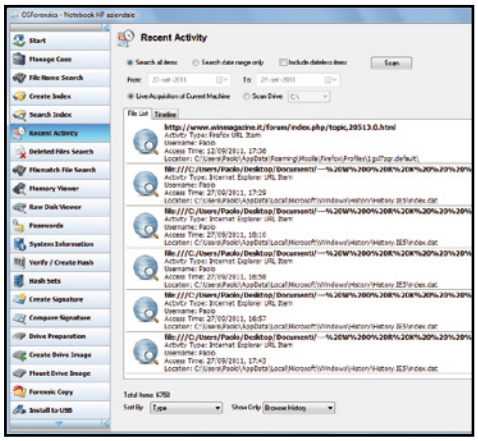
3 Ti ho scoperto!

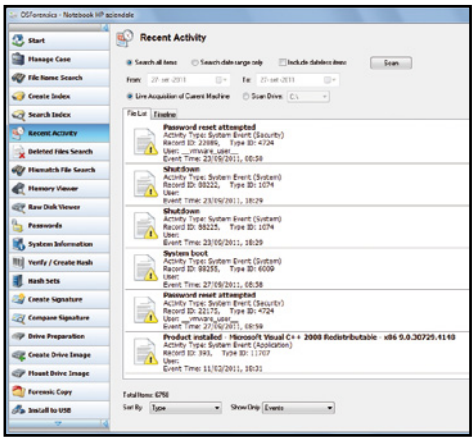
Se non troviamo indizi, spostiamoci nel tab *Unallocated*. Qui vengono elencati quegli elementi che in una ricerca normale non comparirebbero, perché cancellati o non più leggibili. Anche in questo caso, selezioniamoli col tasto destro del mouse e clicchiamo *Open* per leggerli.

E Analisi dettagliata dei log

Una ricerca di informatica forense permette di scoprire lo stile d'uso del PC: quanti accessi sono stati effettuati, il browser usato e i siti più visitati, se sono stati usati supporti esterni… Ecco in che modo.







1 Analisi di un comportamento

Spostiamoci nella sezione *Recent Activity*, impostiamo dei parametri di ricerca, sia temporali sia per i dischi su cui cercare, e clicchiamo *Scan*. Lasciando *All* nel menu *Show only* verranno elencate tutte le attività recenti: accessi a siti Web, chiavette inserite e ogni azione effettuata.

2 Navigazione sotto controllo

Se nel menu a tendina *Show only* selezioniamo la voce *Browser History*, ecco le azioni compiute sul Web. Nello stesso modo possiamo vedere i download effettuati e i log delle chat, le connessioni ad una chiavetta Usb. È davvero un potente mezzo di ricerca, questo programma!

3 I log di tutto!

Possiamo anche avere una panoramica generale di quelle che sono state le operazioni compiute nel periodo preso in esame, con i log delle operazioni. Nel menu *Show Only* selezioniamo *Events*. Gli eventi sono, appunto, le azioni in generale e il risultato è a dir poco sorprendente.

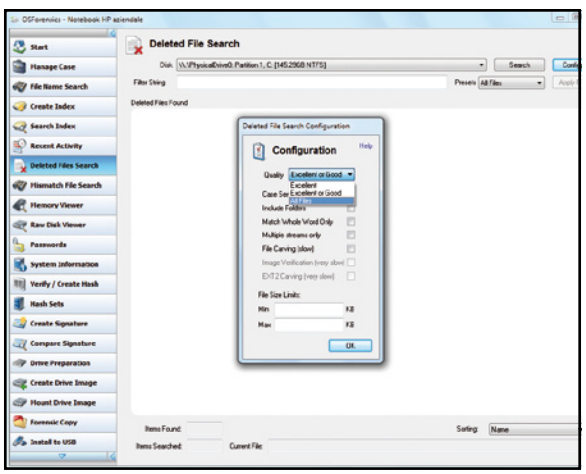
BUONI CONSIGLI

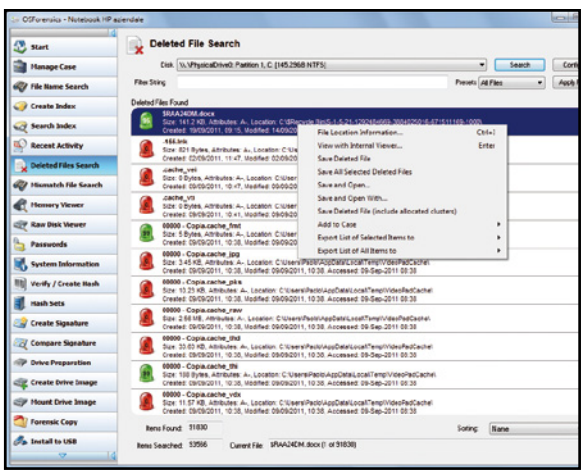
ECCO ANCHE LE PASSWORD

Con OSForensics è possibile recuperare anche tutte le password celate nel sistema. Abbiamo il menu *Passwords* che fa proprio al caso nostro. Ci sono diverse schede in questo menu. La prima ci permette di fare una ricerca generica. Clicchiamo su *Retrieve Password*. Aspettiamo un attimo che il programma effettui la ricerca per avere i risultati nella parte centrale della scheda. Da non credere! In pochi secondi ecco a nostra disposizione i siti visitati, lo username e la password utilizzati per accedervi, addirittura il browser utilizzato per l'accesso, l'eventuale posizionamento in blacklist, l'utente che ha effettuato l'accesso e anche il percorso!

F File cancellati? Rieccoli!

È difficile che qualcuno lasci sul PC documenti "piccanti": in genere, dopo averli letti e visualizzati, li cancella. Se non fosse che con OSForensics bastano pochi clic per recuperarli.





1 Un segugio nel PC

Dal menu principale di OSForensics, spostiamoci in *Deleted Files Search*. Come prima cosa, clicchiamo sul pulsante *Config* e, nella finestra che appare, impostiamo il menu *Quality* su *Excellent or Good*, per ottenere i risultati migliori nella ricerca di file cancellati.

2 A me non sfugge nulla!

Clicchiamo *Search*. Dopo pochi secondi, ecco l'elenco di tutti i file cancellati. Per ognuno, è indicato un numero che rappresenta l'integrità e la possibilità di recuperarlo. Selezioniamo quello che ci interessa col tasto destro del mouse e clicchiamo *Save Deleted File* per recuperarlo.

File cancellati? Recuperiamoli!

✓ Come posso "risuscitare" i file che ho eliminato per errore dal disco rigido del mio computer?

✓ Esiste un modo per ripristinare i dati da un hard disk guasto?

SERVE A CHI...
... ha cancellato per sbaglio o perso dei file memorizzati sull'hard disk e vuole recuperarli

Come molti di noi hanno potuto constatare personalmente i dati memorizzati sul disco rigido del computer non sono al sicuro da cancellazioni involontarie. Windows, come meccanismo di sicurezza, prevede l'eliminazione dei file in 2 fasi, ovvero depositandoli all'atto dell'eliminazione nel Cestino e poi svuotando lo stesso. In questo modo un file finito nel Cestino rimane comunque recuperabile a meno che non si decida di eliminarlo volontariamente. Bisogna dire però che basta utilizzare la combinazione di tasti ***Shift+Canc*** per bypassare in un attimo questo sistema e che, quando si cancellano file di grandi dimensioni, talvolta Windows ne propone l'eliminazione diretta senza passare dal Cestino. Il problema è che basta una semplice distrazione, un crash di sistema o un clic di troppo per cancellare dal disco rigido file importanti se non addirittura un'intera cartella piena di documenti, immagini o altri dati cui teniamo in modo particolare.

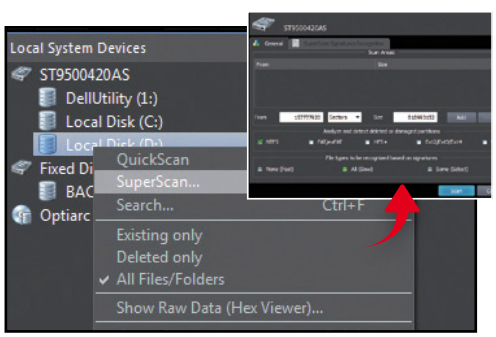
Un recupero possibile

L'ideale per prevenire situazioni del genere è quella di effettuare periodicamente dei backup dei file più importanti, ma se ci siamo dimenticati di farlo l'unica soluzione è quella di verificare comunque se è possibile effettuare un ripristino. Infatti, quando un file viene cancellato, in realtà non è eliminato fisicamente ma i dati che esso contiene rimangono ancora memorizzati nei settori del disco rigido ad esso precedentemente assegnati finché non vengono sovrascritti da qualche altro file. L'hard disk è infatti gestito dal cosiddetto "file system", un meccanismo che provvede a mappare i settori e a tenere quindi traccia di quelli occupati da ciascun file. Se i settori che prima erano occupati da un file cancellato non sono stati sovrascritti da un altro file, è ancora possibile recuperare i dati. Per effettuare il ripristino bisogna in questo caso affidarsi ad appositi tool come Active@ File Recovery, in grado di recuperare file anche dopo una formattazione del disco o la cancellazione di una partizione.

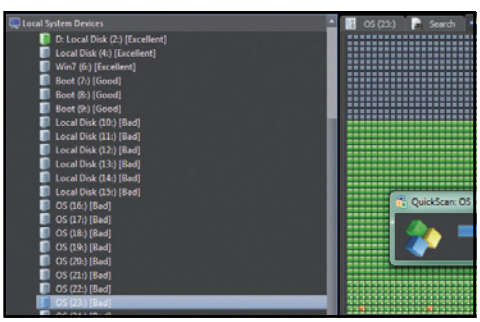
ACTIVE@ FILE RECOVERY
Il software completo lo trovi sul ✓DVD

RECUPERARE L'IMPOSSIBILE
Nei casi più disperati, pensiamo ad esempio ad un guasto alla meccanica o all'elettronica del disco rigido, per recuperare i dati è necessario rivolgersi a ditte specializzate che offrono servizi ad hoc, come ad esempio Kroll Ontrack (www.ontrackdatarecovery.it). Queste aziende procedono al recupero delle informazioni memorizzate su hard disk intervenendo direttamente sul dispositivo di memorizzazione guasto, ripristinandone temporaneamente il funzionamento, procedendo all'estrazione dei dati e alla loro conversione in file e cartelle. Ovviamente si tratta di servizi a pagamento cui conviene ricorrere se i dati da recuperare sono estremamente importanti.

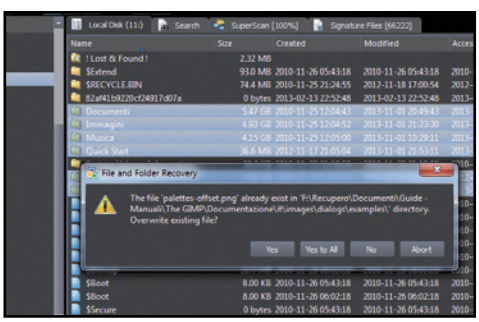
Ecco come effettuare una scansione del disco e recuperare i file eliminati



1 Dalla schermata principale selezioniamo l'unità all'interno della quale tentare il recupero e, con il tasto destro del mouse, scegliamo l'opzione ***SuperScan***. Impostiamo i criteri con cui effettuare la scansione, clicchiamo su ***Scan*** e attendiamo la fine del processo.



2 A sinistra verrà mostrato il risultato della scansione con i volumi e le partizioni cancellate o danneggiate recuperate. Selezioniamo ciascuna delle partizioni individuate e, con il tasto destro, avviamo una ***Quick Scan*** per la ricerca dei file in esse contenuti.



3 Al centro vedremo la struttura della partizione ricostruita. Possiamo controllare l'integrità dei file visualizzandone un'anteprima. Se siamo soddisfatti del recupero, dopo aver acquistato la versione completa del software, selezioniamo ***Recover*** dal menu contestuale.

La macchina della verità

La guida pratica e i software per trasformare il PC in uno 007 digitale "smaschera bugiardi"

Cosa ci occorre

30 MIN. DIFFICILE

TOOL DI ANALISI VIDEO
EULERIAN VIDEO MAGNIFICATION
Quanto costa: Gratuito
Sito Internet: www.winmagazine.it/link/2155

SOFTWARE DI VIDEO EDITING
ADOBE PREMIERE PRO
Lo trovi su: ☑DVD
Quanto costa:
Sito Internet: www.adobe.it

TOOL CONVERSIONE VIDEO
ALL MEDIA CONVERTER
Lo trovi su: ☑DVD
Quanto costa: Gratuito
Sito Internet: www.danusoft.com

Sei proprio sicuro che le cose stiano davvero come ti fanno credere? Puoi veramente fidarti delle persone che hai intorno? E se fosse tutto un enorme complotto? Qui bisogna correre ai ripari e studiare il nostro "nemico" usando tutte le tecnologie che abbiamo a disposizione, come ad esempio la "video macchina della verità"! Non si tratta di una genialata di nostro amico burlone. Il progetto è stato sviluppato nientemeno che dai ricercatori del Computer Science and Artificial Intelligence Laboratory (CSAIL) del Massachusetts Institute of Technology (MIT). Eulerian Video Magnification, questo il nome del progetto, è interamente basato sul software di calcolo numerico Matlab (www.winmagazine.it/link/2156) e sfrutta una nuova tecnologia di analisi video che permette di cogliere anche la più piccola variazione nella colorazione della pelle e il minimo movimento dei muscoli facciali.

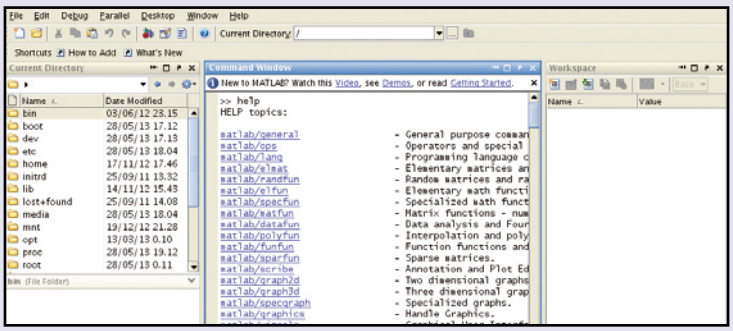
Attendo a quel che dici

I mentitori di professione ora hanno le ore contate! Eulerian, infatti, è in grado di cogliere ogni loro più piccola incertezza nell'espressione del volto! Ma non finisce qui! I ricercatori del MIT hanno deciso di condividere con gli utenti del Web questo progetto, consentendo a chiunque di caricare un video di trenta secondi che verrà poi scansionato dall'Eulerian Video Magnification alla ricerca della più piccola incertezza nell'espressione dell'interlocutore. Ma funzionerà veramente? Abbiamo deciso di mettere Eulerian alla prova caricando sul sito del MIT un primo piano di trenta secondi con un'attrice che guarda fissa in camera. Dopo aver scansionato il volto con Eulerian abbiamo scaricato il video risultato usando un plug-in per browser in grado di effettuare il download di qualunque formato dal Web.

EULERIAN VIDEO MAGNIFICATION: ECCO COME FUNZIONA

Sviluppato dalla MathWorks, MatLab è un programma che fornisce un ambiente per il calcolo scientifico e la visualizzazione grafica dei dati, tanto da essere diventato il programma di punta in ambito didattico e applicativo (www.mathworks.it/products/matlab). Al centro della schermata principale è presente la finestra ***Command Window*** nella quale, impartendo il comando ***help***, si ha accesso a tutta la documentazione dei pacchetti software dedicati a specifiche applicazioni. In questo ambiente, oltre alle svariate operazioni di "uso immediato" come funzioni matematiche, matrici numeriche ecc, nei diversi ambiti (dall'Ingegneria all'Economia) è possibile operare anche con un linguaggio di programmazione semplice da usare. Sfruttando questo linguaggio si possono creare i cosiddetti M-files che si dividono in script, funzioni e classi: dal menu ***File***, cliccando ***New*** è possibile scegliere uno di questi tre tipi affinché l'editor/debugger interno adotti il template predefinito che ne facilita la scrittura. Per eseguire un M-file è sufficiente entrare nella directory di salvataggio utilizzando il pannello (o la riga) ***Current Directory*** e digitare nella ***Command Window*** solo il nome del file, senza estensione.

È anche possibile operare con progetti complessi composti da decine o centinaia di M-file: in questi casi, sarà generalmente presente un file con nome ***make.m*** che permette di "compilare" l'intero progetto, rendendolo eseguibile. È questo il caso del progetto Eulerian Video Magnification realizzato dal MIT (trovi il codice sorgente nel DVD-Rom): scompattando l'archivio ***EVM_Matlab-1.1.zip*** accediamo tra gli altri anche al file ***make.m***. Una volta eseguito, verranno caricati anche tutti gli altri file. Questi ultimi sono un insieme di comandi che, applicati al file video caricato in MatLab, applicheranno gli effetti grafici che permettono di analizzarne i singoli fotogrammi. In questo modo, come spiegheremo nell'articolo, sarà possibile individuare variazioni anche minime del colorito di una persona o movimenti muscolari impercettibili. Ecco quindi che, grazie alla potenza di MatLab, semplici righe di codice possono trasformarsi in una efficiente macchina della verità. MatLab può essere acquistato sul sito della MathWorks, anche come Student Version (www.mathworks.it/store/productIndexLink.do).



L'interfaccia di MatLab è apparentemente semplice, ma per usarla meglio occorrono conoscenze avanzate di programmazione e calcolo numerico.

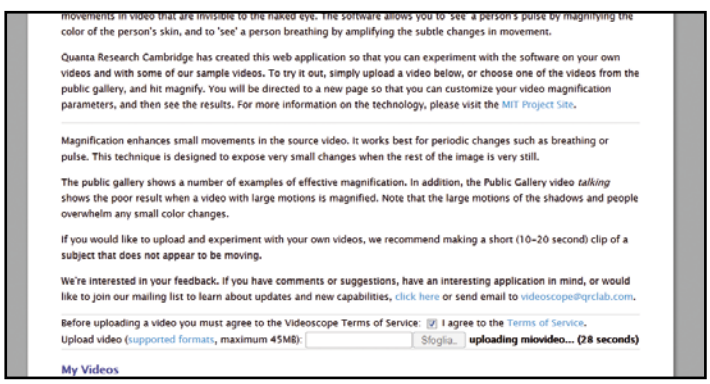
Infine abbiamo realizzato un video confronto tra la clip originale e quella trattata con Eulerian, utilizzando Premiere CS6.

Non si tratta di soli video

Affinché una macchina della verità sia davvero efficiente, però, non può limitarsi soltanto all'analisi dei video. Abbiamo quindi realizzato un kit di strumenti con cui potremo analizzare anche la voce nelle nostre videochat ed elaborare le immagini digitali per scoprire se sono state in qualche modo ritoccate o "corrette" per far sembrare vere situazioni altrimenti irrealizzabili! E per finire, ecco anche la versione portable del nostro kit, funzionante anche sullo smartphone. Insomma, se è vero che le bugie hanno le gambe corte, grazie alla nostra potente macchina della verità virtuale ora anche i furbetti verranno presto smascherati!

A Facciamo partire le indagini

La prima cosa da fare è filmare il soggetto di cui vogliamo studiare l'attendibilità. Al termine, carichiamo il video sul sito del MIT e prepariamoci a scansionarne ogni singolo fotogramma!



movements in video that are invisible to the naked eye. The software allows you to 'see' a person's pulse by magnifying the color of the person's skin, and to 'see' a person breathing by amplifying the subtle changes in movement.

Quanta Research Cambridge has created this web application so that you can experiment with the software on your own videos and with some of our sample videos. To try it out, simply upload a video below, or choose one of the videos from the public gallery, and hit magnify. You will be directed to a new page so that you can customize your video magnification parameters, and then see the results. For more information on the technology, please visit the MIT Project Site.

Magnification enhances small movements in the source video. It works best for periodic changes such as breathing or pulse. This technique is designed to expose very small changes when the rest of the image is very still.

The public gallery shows a number of examples of effective magnification. In addition, the Public Gallery video *talking* shows the poor result when a video with large motions is magnified. Note that the large motions of the shadows and people overwhelm any small color changes.

If you would like to upload and experiment with your own videos, we recommend making a short (10–20 second) clip of a subject that does not appear to be moving.

We're interested in your feedback. If you have comments or suggestions, have an interesting application in mind, or would like to join our mailing list to learn about updates and new capabilities, click here or send email to videoscope@qrclab.com.

Before uploading a video you must agree to the Videoscope Terms of Service: I agree to the Terms of Service.
Upload video (supported formats, maximum 45MB): Sfoglia... uploading miovideo... (28 seconds)

My Videos

1 Sempre in primo piano

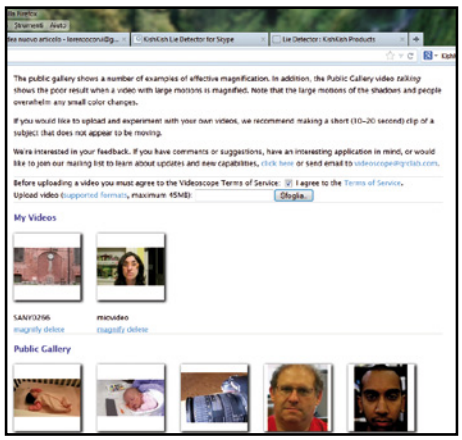
Per capire se il nostro interlocutore ci sta nascondendo qualcosa, facciamolo sedere davanti alla videocamera, quindi riprendiamolo per 30 secondi chiedendogli di rimanere il più possibile immobile davanti all'obiettivo. In questo modo Eulerian sarà in grado di cogliere ogni più piccola incertezza del soggetto.

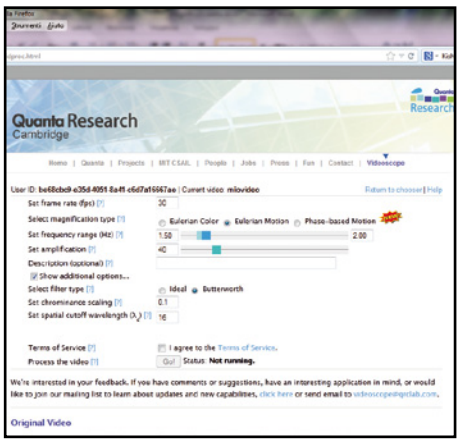
2 Carichiamo il video

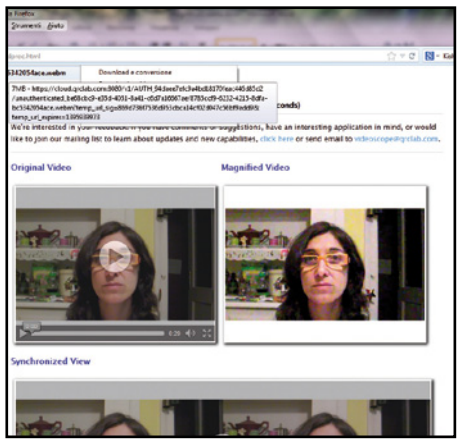
Colleghiamoci a www.winmagazine.it/link/2157 e spostiamoci a fondo pagina. Spuntiamo *I agree to the Terms of Service*, clicchiamo *Sfoglia* e selezioniamo il video realizzato (nel formato AVI, H264, MOV, MP4, ecc) e che caricheremo sui server del MIT. Premiamo *Apri* e attendiamo il termine dell'operazione.

B Scansioniamo le riprese

È arrivato il momento di dare il video in pasto a Eulerian Video Magnification e scansionare ogni singolo fotogramma della clip alla ricerca della verità. Infine esporteremo la clip usando un plug-in per browser.







1 Magnifichiamo il video!

Una volta terminato il caricamento del video, lo vedremo comparire nella sezione principale di Eulerian Video Magnification sotto l'area di *Upload*, con l'indicazione *My videos*. A questo punto non ci resta che premere il pulsante *Magnify* per spostarci nella pagina di scansione video.

2 La configurazione giusta

Nella nuova finestra impostiamo *Set frequency range (Hz)* con un valore di *1,5*. Tale valore corrisponde alla frequenza del battito cardiaco umano. Impostiamo *Set Amplification* a *40* per cogliere ogni più piccola variazione nel soggetto. Infine spuntiamo la voce *Show additional Options*.

3 Pronti a esportare

In *Additional Options* impostiamo *Set chrominance scaling 1*, spuntiamo *I agree to the Terms of Service* e premiamo *Go!*. Terminata la scansione clicchiamo *OK* e mettiamo in *Play* il Magnified Video risultato. Scarichiamo la clip usando uno dei plug-in per browser descritti nel sottostante.

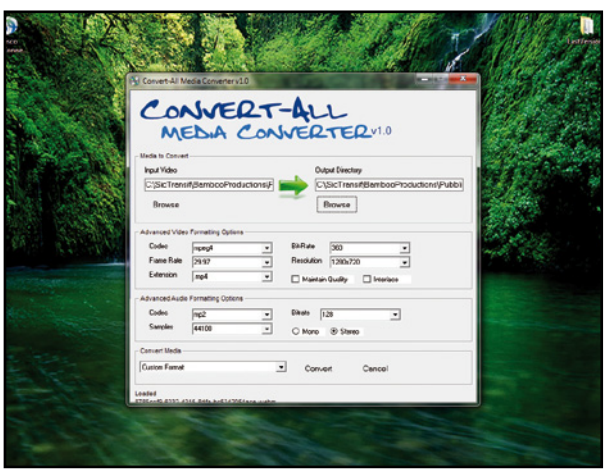
BUONI CONSIGLI

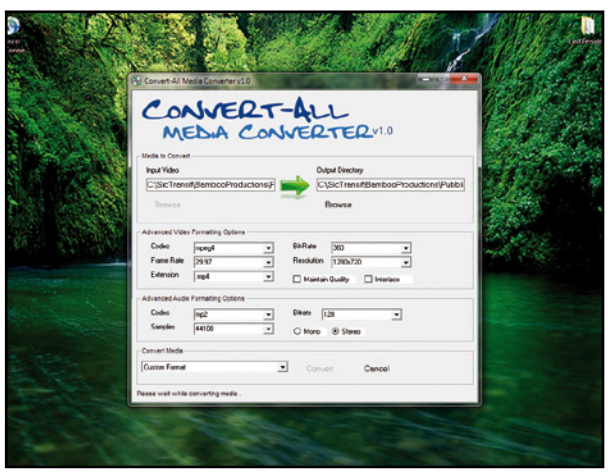
SCARICHIAMO IL VIDEO

Per scaricare su PC il video realizzato con Eulerian useremo un plug-in per browser. Su Firefox c'è *Video Dowload Helper*. Cerchiamolo da *Strumenti/Componenti aggiuntivi*: una volta installato, avviamo la clip e premiamo il triangolo a lato dell'icona di Download Helper appena comincia a muoversi. Per Chrome c'è *FDV Video Downloader* ricercabile da *Strumenti/Estensioni/Prova altre estensioni*. Basta premere la freccia blu per scaricare il video. Per i fedelissimi di Internet Explorer c'è *IEDownloadhelper* (http://iedownloadhelper.com), che funziona allo stesso modo degli altri.

C Convertiamo il video

Il sito del MIT usa il formato video Webm, molto diffuso in Rete ma incompatibile con Premiere. Per ovviare al problema convertiamo il video in formato MP4 utilizzando All Media Converter!





1 Installiamo All Media Converter

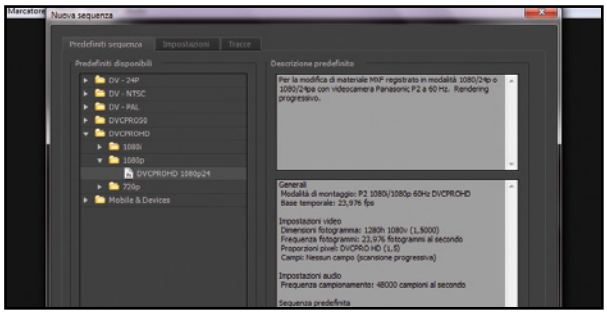
Dal DVD allegato a questo speciale scarichiamo e installiamo il file *ConvertAllSetup.exe*. Al termine avviamo il programma, impostiamo con i pulsanti *Browse* l'*Input Video* scegliendo *Webm* dal menu a tendina e la *Output Directory* (la cartella in cui salvare il file convertito).

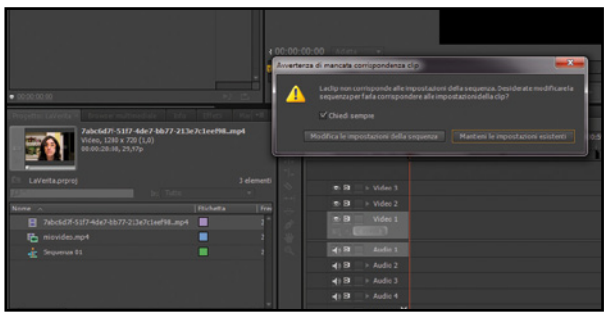
2 Pronti a convertire!

Impostiamo *Mpeg4* come *Codec* ed *.mp4* come *Extension*. Nel campo *Resolution* selezioniamo *1280x1024* e modifichiamo a mano il valore impostando *1280x720* (nel caso in cui il video di partenza sia in HD) oppure *1920x1080* se abbiamo un filmato Full HD. Infine clicchiamo sul pulsante *Convert*.

D Interrogatorio doppio!

Scaricata la clip scansionata da Eulerian, importiamola in Premiere CS6 insieme alla clip originale. Creiamo un video confronto dividendo lo schermo e osserviamo il "prima e dopo"!



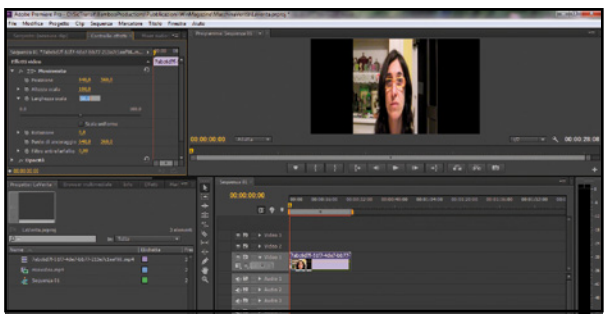


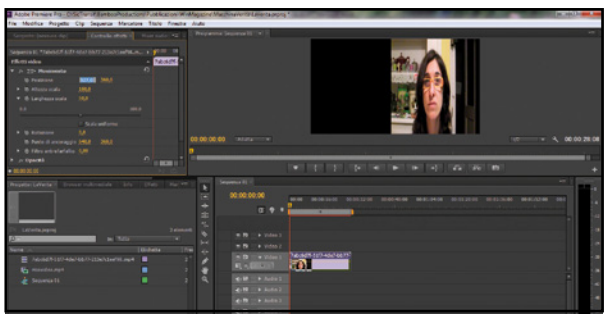
1 Un nuovo progetto

Avviamo Adobe Premiere CS6 e dalla schermata di *Benvenuto* scegliamo la cartella in cui archiviare il nostro progetto, diamogli un nome e confermiamo le modifiche premendo il pulsante *OK*. Nella nuova finestra ignoriamo la scelta del formato di importazione e premiamo nuovamente *OK*.

2 Importiamo le clip

Clicchiamo due volte nell'area *Progetto*, importiamo la clip originale e quella scansionata da Eulerian Video Magnification e convertita nei passi precedenti. Trasciniamo in timeline quest'ultima clip disponendola sulla traccia *Video 1* e scegliamo *Modifica le impostazioni della Sequenza*.



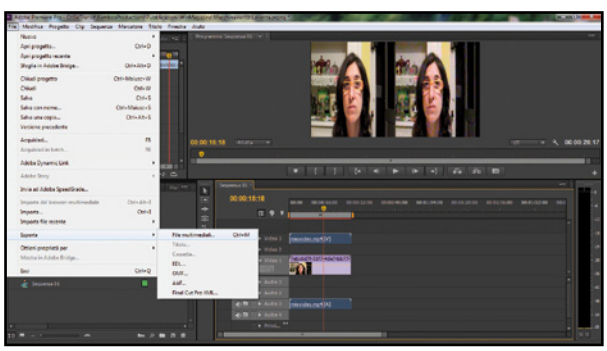


3 Facciamo un po' di spazio

Clicchiamo sulla traccia appena importata nella timeline, quindi posizioniamoci sull'etichetta *Controllo Effetti* ed espandiamo la voce *Movimento/Scala*. Togliamo anche il segno di spunta dalla casella di controllo *Scala uniforme*, quindi impostiamo un valore *Larghezza scala* al *50%*.

4 Tutto a sinistra

Rimanendo all'interno della sezione *Controllo Effetti*, clicchiamo sulla voce *Movimento/Posizione* per espandere il menu contestuale e modifichiamo i valori sull'asse *X* (sono i valori riportati a sinistra) in modo da posizionare la clip nella parte destra all'interno della finestra *Monitor*.



5 Come un'intervista doppia

A questo punto, possiamo importare anche la clip originale in timeline: ridimensioniamola e riposizioniamo il filmato come già visto nei due passi precedenti. Infine dalla barra dei menu *do Premiere* in alto clicchiamo *File/Esporta/File multimediali* ed esportiamo il nostro video doppio.

RISULTATO FINALE L'analisi del video magnificato evidenzia anche le più piccole variazioni fisiche del nostro intervistato, come ad esempio un impercettibile battito delle ciglia. Per esaminare con attenzione il lavoro eseguito da Eulerian Video Magnification possiamo scaricare dal DVD il video d'esempio usato nel tutorial. Nome file: doppio.mp4

BUONI CONSIGLI

IMPOSTAZIONI DI ESPORTAZIONE

Dalla finestra *Impostazioni di esportazione* di Premiere CS6 possiamo impostare in assoluta libertà i formati di esportazione audio e video. Poniamo tuttavia la massima attenzione al formato video! Scegliere quello sbagliato può infatti compromettere il risultato finale. Ad esempio, se il nostro filmato è in HD (quindi 1280x720) e decidiamo di esportare in AVI, avremo un filmato a 720x480 pixel, quindi decisamente troppo "tagliato". Per non perderci tra i formati di esportazione, teniamo sempre d'occhio la voce *Riepilogo*.

ESPORTIAMO SU DVD

Con Premiere CS6 è possibile esportare le nostre clip e creare un DVD sfruttando il programma integrato Adobe Encore DVD. Un volta completato il montaggio della sequenza video è sufficiente selezionare, dalla barra dei menu, *File/Adobe dynamic link/Invia a encore*. Il progetto verrà esportato su Adobe Encore e sarà possibile creare un DVD o un Blu-ray con tanto di menu personalizzato.

VISTA MINIATURE

Nell'area Progetto esiste una interessante funzione, denominata Vista miniature che consente non solo di muoversi più agevolmente tra le clip importate, ma anche di vederne un'anteprima semplicemente scorrendo il mouse sopra la miniatura.

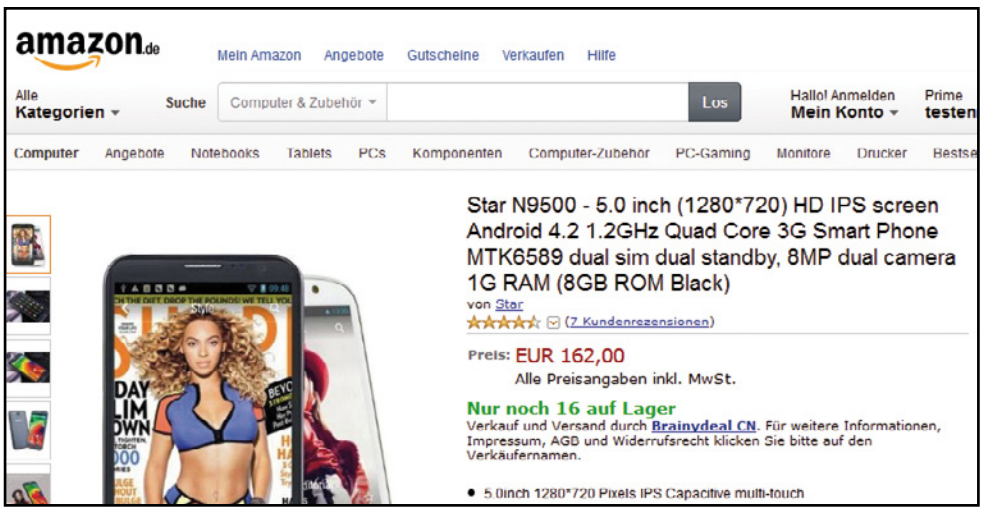
I cellulari con la spia!

Abbiamo scoperto che sul mercato europeo viene venduto un clone economico del Samsung Galaxy S4 davvero pericoloso. Ecco perché!

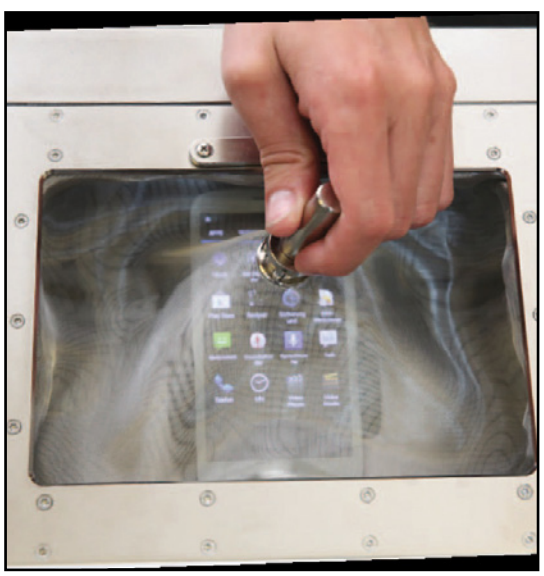
Gli aficionados di Amazon probabilmente lo avranno già visto (e magari volevano acquistarlo). Stiamo parlando dello "Star N9500", uno smartphone molto apprezzato dagli utenti e venduto in Europa su diversi siti di e-commerce. Tuttavia, anche se l'N9500 costa circa 160 euro, chi aveva dei dubbi su di esso aveva ragione, come dimostrato da recenti test di sicurezza.

Preoccupazioni legittime

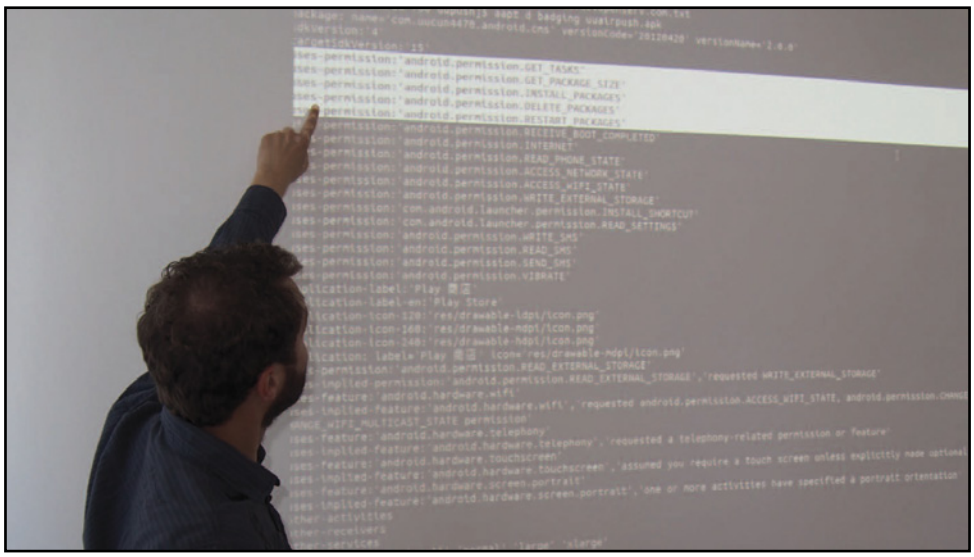
Tecnicamente non ci si può lamentare dello smartphone, che è una replica 1:1 del Galaxy S4, fatta talmente bene da renderlo esteriormente indistinguibile dal telefono Samsung (che costa circa 300 euro). Per quanto riguarda i componenti utilizzati, il



Invece di spendere oltre 300 euro per un Galaxy S4, è meglio spenderne 160 per un clone cinese? Peccato che questo abbia anche pericolose funzioni di spionaggio!



Gli esperti di sicurezza Mathias Otten e Olaf Pursche hanno inserito lo smartphone in uno speciale dispositivo per isolarlo e analizzarlo. Così facendo è possibile esaminare qualunque comunicazione Wireless senza che il produttore possa avere accesso al sistema.



L'analisi del firmware operata dal team di Geschkat ha svelato che il produttore ha inserito nel sistema Android dell'N9500 un app store nascosto che tra le altre cose gli permette di avere accesso completo al device tramite server cinesi.

display da 5 pollici offre una qualità decente, mentre il processore quad core da 1,2 GHz e gli 8 gigabyte di memoria sono più che sufficienti per far girare Android 4.2. Inoltre, su alcuni mercati, è possibile trovare in dotazione oltre alle cuffie anche una seconda batteria. Peccato che questo smartphone abbia una doppia identità: da un lato clone perfetto ed economico, dall'altro indomito spione. Questo, almeno, è quello che ha rilevato la squadra di tecnici capitanata da Christian Geschkat nei laboratori di G Data. L'esperto di sicurezza ha dichiarato che "***Molti dei nostri clienti ci hanno segnalato come la nostra suite di sicurezza rilevasse come pericolosa un'app con l'icona del Google Play. Poiché l'alert riguardava un'applicazione presente nel firmware, abbiamo recuperato uno smartphone per analizzarlo.***"

Possibilità illimitate di manipolazione

L'analisi del codice del firmware in laboratorio ha fatto emergere che il sistema operativo dello Star N9500 è stato manipolato dal produttore. Oltre al Google Play c'è una seconda alternativa per installare le app, che però non compare nel menu dello smartphone. Questo secondo app store segreto nascosto all'utente serve solo al produttore dello smartphone per scopi discutibili. Permette di nascondere le porte che il sistema lascia aperte per consentire un eventuale accesso remoto, proprio come se fosse un vero e proprio trojan.

- **Applicazioni dannose:** questo app store segreto può consentire al produttore cinese di iniettare programmi dannosi nel sistema e utilizzare il dispositivo come parte di una botnet. Queste app, una volta installate, non appariranno all'interno del menu del telefono. Ma non è tutto: le istruzioni relative all'installazione vengono immediatamente cancellate dai registri dello smartphone e, come svelato dal team di Geschkat, gli aggiornamenti di sicurezza distribuiti da Google possono essere bloccati.
- **Intercettazione delle telefonate:** il produttore può vedere quando e con chi si è parlato. E caricando delle apposite app è possibile anche intercettare le conversazioni.
- **Spionaggio tramite fotocamera e microfono:** la fotocamera e il microfono possono essere attivate a distanza così l'utente sarà spiato facilmente. Inoltre, il produttore può accedere anche ai dati di geo-localizzazione dello smartphone.
- **Intercettazione di SMS ed e-mail:** anche gli SMS possono essere spiati dal produttore cinese di questo smartphone che, ad esempio, potrebbe leggere codici di sicurezza per l'accesso a siti o addirittura al nostro on-line banking. Si può cadere vittima dell'invio di SMS a pagamento con servizi premium e le impostazioni del dispositivo permettono addirittura al produttore di avere accesso alle e-mail e ad altri dati ancora.

L'app di sicurezza di G Data ha individuato il "play store" segreto che non compare in nessun menu del dispositivo. Solo chi ha familiarità con la programmazione Android riesce ad individuarlo.

Alla larga dallo spione cinese!

Il team di Geschkats ha individuato la destinazione dei dati trasmessi dallo smartphone: "Tutti i dati vengono trasmessi ad un server anonimo. Le loro tracce si perdono in Cina", ma è chiaro che per il produttore l'N9500 è un doppio investimento. Gli utenti non solo lo pagano con denaro contante, ma anche con i propri dati. Gli esperti di sicurezza di G Data hanno informato Amazon, che lo ha rimosso dal proprio sito, ma il telefono spia è ancora disponibile su altri canali. Il nostro consiglio è di non acquistarlo per nessun motivo!

Ha dell'incredibile, ma funziona davvero

Il tasto segreto dell'hacker

Esiste una pericolosa "scorciatoia da tastiera" che permette di accedere a qualunque PC eludendo antivirus e scardinando password...

Tra gli ultimi Anni 90 e i primi anni duemila, i worm erano la minaccia più diffusa. Pensiamo all'ormai famoso ILOVEYOU, che proprio a cavallo tra i due millenni paralizzò il sistema di comunicazione delle e-mail e sembrava inarrestabile. Il parlamento inglese decise addirittura di spegnere i propri computer finché il worm non fosse stato fermato, e similmente si comportarono anche il Pentagono e alcune grandi aziende di tutto il mondo. La finalità principale dei worm era, fondamentalmente, il vandalismo. Questi programmi non arricchivano in modo particolare il loro autore, si limitavano a danneggiare tutto ciò che incontravano, diffondendosi in modo molto rapido. Forse anche perché in quegli anni l'informatica stessa non era utilizzata in modo particolarmente vario e anche potendo rubare informazioni dai computer delle vittime, si sarebbe potuto guadagnare poco. Non c'erano flussi di denaro in rete, il commercio e le banche on-line erano quasi inesistenti.

Scorciatoie... da tastiera!

Oggi la situazione è cambiata: i computer sono dovunque e si occupano anche di aspetti molto importanti della nostra vita, oltre che del nostro denaro. Non è un caso che con l'aumento dell'alfabetizzazione informatica i worm siano lentamente scomparsi per lasciare posto ad attacchi informatici di vario genere, atti non semplicemente a dare fastidio ma specificatamente a rubare dati sensibili. Se un tempo il pericolo arrivava dalle e-mail infette, oggi può nascondersi anche dietro pericolose scorciatoie da tastiera che i pirati usano per acquisire diritti di amministratore su qualsiasi PC e compiere le loro malefatte eludendo l'antivirus e scardinando le password più robuste. Proprio

Come tutte le periferiche USB, anche la tastiera è esposta ad attacchi di tipo BadUSB.
Tutorial a pag. 22

Attenti, perché un pirata può accendere di nascosto la Webcam!
PDF sul WinDVD

Uno smartphone opportunamente modificato può clonare il nostro hard disk?
Tutorial a pag. 24

così: anche una semplice tastiera USB può rappresentare un serio pericolo per la nostra sicurezza on-line. Paradossi dell'informatica: se finora la combinazione di tasti Win+L serviva per bloccare la sessione in uso di Windows, ora dobbiamo preoccuparci che qualcuno possa usare segrete scorciatoie da tastiera per superare ogni nostra difesa!

Attenti alle porte USB

Le tecniche di attacco dunque sono cambiate, anche se solo apparentemente. Da sempre i pirati si sono dedicati a sfruttare qualche bug presente nei sistemi operativi o nei programmi di uso comune e continuano a farlo ancora oggi. Semmai sono cambiate le fonti che i pirati utilizzano per sfruttare questi bug. Se prima concentravano le loro attenzioni sui sistemi operativi e sui software di uso comune, adesso cercano di sfruttare anche le varie periferiche hardware collegate al PC: se ci pensiamo bene, però, tutte le periferiche, anche la "solita" tastiera USB oppure una normale pendrive, hanno un firmware che ne gestisce le funzionalità e un firmware non è altro che un software capace di eseguire determinate operazioni. E in quanto tale, può essere malevolmente modificato!

Il pericolo che non ti aspetti

Con la graduale scomparsa di worm e trojan, i pirati hanno quindi iniziato ad usare sempre meno le tecniche di ingegneria sociale che stavano alla base di questi attacchi, spostando tutti i loro sforzi principalmente verso quei bug che non richiedono l'intervento diretto da parte dell'utente. Un attacco Heartbleed,

ad esempio, può essere eseguito a totale insaputa dell'utente. Lo stesso vale per il nuovo bug che sta spaventando la Rete, anche se senza un reale motivo: BadUSB. Questo tipo di attacco è salito agli onori della cronaca perché capace di diffondersi attraverso normalissime chiavette USB. Per capire la natura del bug BadUSB dobbiamo comprendere il funzionamento dei dispositivi USB. Ogni dispositivo contiene un piccolo computer, con un microprocessore e una memoria ROM sulla quale viene scritto un bootloader (non serve RAM perché i registri di memoria interni al processore sono sufficienti per i pochi calcoli da eseguire). Attenzione, abbiamo parlato di "dispositivo". Questa struttura e il bug si trovano solo nei dispositivi veri e propri: a differenza di quanto strillato erroneamente sul Web, quindi, i semplici cavi USB non soffrono di questo bug proprio perché non dispongono di un microprocessore. Perché questa apparente complicazione? Perché così appena il dispositivo viene collegato ad un computer e dunque alimentato, il processore comincia a leggere le istruzioni del bootloader che a sua volta si occupa di fornire al sistema operativo del computer il firmware. Grazie a quest'ultimo, il sistema operativo può riconoscere ogni singolo dispositivo tra i milioni di modelli presenti nel mondo. Se, per noi, una stampante è ben diversa da un mouse, per il computer si tratta della stessa cosa finché non gli viene inviato un firmware che indica la stampante collegata ad un delle porte USB e il mouse ad un'altra. Se ci è mai capitato di usare una chiavetta internet 3G, avremo notato che questi piccoli dispositivi possono funzionare in due modi: come sistemi di archiviazione di massa (compaiono in Windows come CD virtuali) oppure come modem Internet. Chi è che dice al computer quali sono queste due modalità? Il bootloader della pennetta, ovviamente, che invia il firmware corretto al sistema operativo del PC. Ovviamente bootloader e firmware possono essere aggiornati, questo lo sappiamo.

Il punto debole

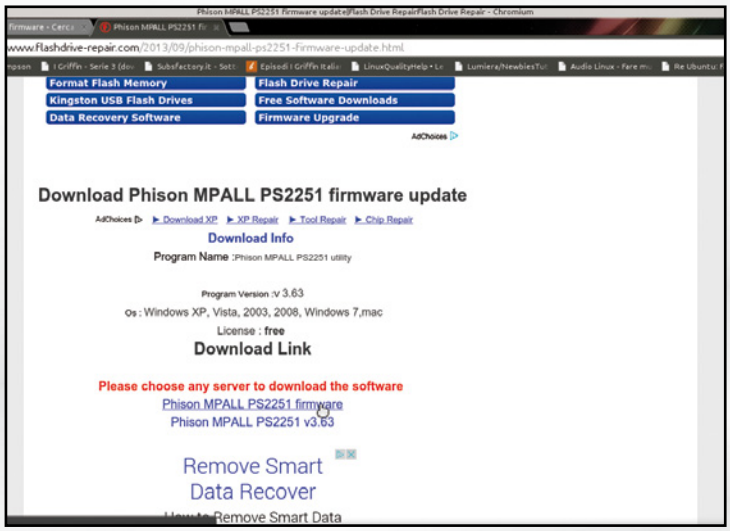
Il problema, come si può intuire, è che in questo modo un malintenzionato potrebbe scrivere un firmware modificato appositamente per compiere azioni pericolose (rubare file, distruggere dischi, leggere i tasti digitati, eccetera...) e caricarlo su un dispositivo come se fosse un aggiornamento del firmware. A questo punto gli utenti che utilizzano quel dispositivo "compromesso" verranno a loro insaputa attaccati da un codice "nascosto", che nemmeno gli antivirus possono individuare (perché il firmware di un dispositivo è a loro irraggiungibile). Che tale problema esista non è quindi una scoperta nuova, è evidente fin dagli albori dell'USB, ma finora nessuno aveva dato particolare importanza a q uesto difetto. Proprio perché, in realtà, non è poi un gran problema.

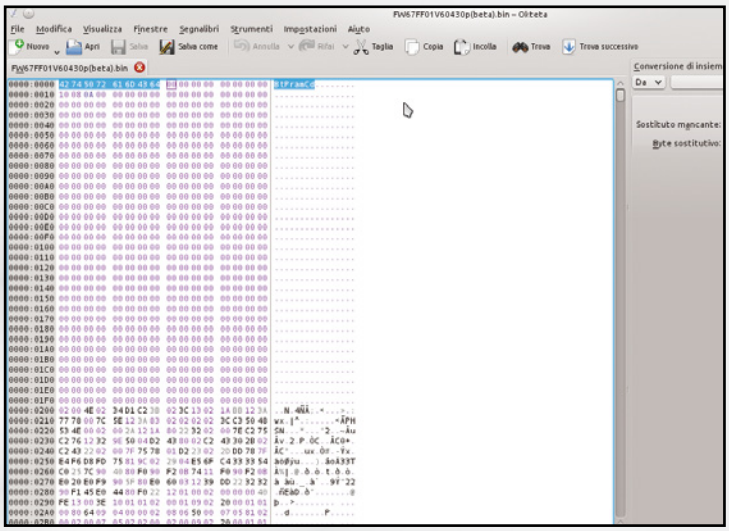
Poco pratico per un pirata

Per nostra fortuna, questo bug non può essere utilizzato facilmente dai pirati. Il motivo fondamentale è che ogni dispositivo dispone di un chipset (processore) differente e quindi il bootloader ed il firmware devono essere scritti appositamente. Per esempio, se il pirata vuole prendere di mira le pendrive, dovrà costruire un firmware cracckato per il chip Phison ps2231 (www.usbdev.ru/cics/icphison), poi uno per il Phison 2251, poi uno per il Toshiba TC58NC2303G5T, eccetera. Insomma: dovrà realizzare un firmware per ciascuno delle centinaia di chip differenti. Anche supponendo che riesca a realizzare un firmware cracckato in una settimana, sarebbero comunque necessari degli anni prima di poter condurre un attacco contro la maggioranza delle pendrive in circolazione. Inoltre, per scrivere un firmware malevolo il pirata ha due problemi: il primo è dato dal fatto che il suo firmware deve essere simile a quello originale, quindi deve prima di tutto procurarsi il firmware ufficiale, poi deve de-

Cronistoria di un attacco di

Sfruttando una chiavetta USB, un pirata può entrare di nascosto in un qualsiasi computer e prenderne





1 Trovare il firmware

La prima cosa che un pirata deve fare è scegliere una chiavetta su cui lavorare e capire quale sia il suo chipset. Trovato il modello esatto, può cercare il firmware corretto su Internet e scaricarlo per comprenderne il funzionamento.

2 Capire di cosa si tratta

Il firmware viene solitamente fornito come un file BIN all'interno di un archivio compresso. Il problema è che quel file BIN rappresenta l'immagine del firmware, quindi non è un semplice programma ma una intera partizione EEPROM.

assemblarlo e cercare di modificarlo in linguaggio assembler senza pregiudicare il funzionamento del dispositivo ma soltanto inserendo alcune istruzioni malevole. Il secondo problema è che lo spazio per il firmware è poco, quindi il pirata non può scrivere molto codice e può eseguire soltanto comandi semplici. È anche difficile che possa diffondersi un "contagio", cioè che per esempio una pendrive infettata possa inviare il suo codice malevolo ad altre pendrive collegate allo stesso PC: sia perché per flashare il firmware sono necessari privilegi di amministrazione, sia perché comunque le varie pendrive dovrebbero essere realizzate con lo stesso chipset (cosa che invece spesso non si verifica). Certo, si potrebbe realizzare abbastanza facilmente una pendrive capace

COSÌ IL PIRATA MODIFICA IL FIRMWARE DELLA PENDRIVE

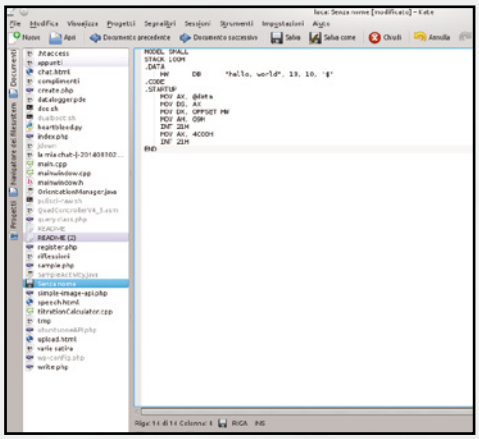
Le operazioni da compiere per modificare il firmware di una periferica hardware e, in particolare, di una pendrive USB, sono lunghe e complicate e richiedono ottime conoscenze dei linguaggi macchina come l'Assembly con cui, di solito, vengono programmati i chipset di riferimento e la struttura del firmware. Ad esempio, analizzando il codice binario, il pirata prova ad individuare la parola BtPramCd sapendo che quello è il punto di inizio del primo settore della partizione creata sulla chiavetta USB. Allo stesso modo, il pirata sa che ad un certo punto, dopo qualche migliaio di righe di codice, dovrebbero essere presenti le seguenti istruzioni di memoria:

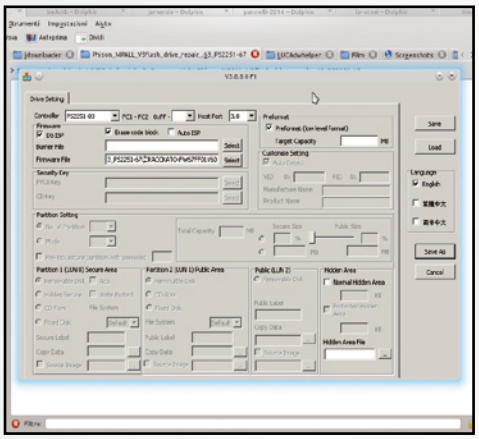
32 03 55 00 53 00 42 00
20 00 44 00 49 00 53 00
4B 00 20 00 33 00 30 00

Che, tradotte dall'esadecimale, corrispondono al testo 2.U.S.B. .D.I.S.K. .3.0. Come è facile intuire, questa stringa rappresenta il tipo di dispositivo che verrà riconosciuto dal sistema operativo. Se il pirata modifica questa stringa scrivendo, per esempio, quella di una tastiera USB, appena la pendrive viene collegata al computer, il sistema sarà convinto di vedere una tastiera USB. Ma chiaramente le modifiche apportare al firmware saranno molto più dannose di un semplice cambio di tipologia della periferica hardware!

tipo BadUSB

il controllo totale. Per farlo, deve modificare il firmware della pendrive eseguendo un'operazione lunga e complicata…





3 Si lavora col codice binario

Il pirata, quindi, apre il file con un editor esadecimale e cerca il punto giusto per inserire il suo codice malevolo, che dovrà essere in codice binario compilato. Per realizzare tale codice, scrive un programma in Assembly (o eventualmente in C) e poi lo compila.

4 BadUSB in azione

Come è ovvio, ormai, l'unico passo che rimane, al pirata, è consegnare la pendrive all'utente che ha scelto come vittima. Quando questo collegherà la chiavetta al proprio PC, il codice malevolo verrà eseguito. Poi, il pirata dovrà anche rientrare in possesso della pendrive, se necessario.

5 BadUSB in azione

Come è ovvio, ormai, l'unico passo che rimane, al pirata, è consegnare la pendrive all'utente che ha scelto come vittima. Quando questo collegherà la chiavetta al proprio PC, il codice malevolo verrà eseguito. Poi, il pirata dovrà anche rientrare in possesso della pendrive, se necessario.

LA PRIMA PATCH PER IL BUG BADUSB

I ricercatori che per primi avevano fatto esplodere il caso BadUSB hanno anche pubblicato una patch che dovrebbe risolvere il bug. Non si tratta di una soluzione definitiva, perché si basa sul protocollo USB 3.0, mentre esistono ancora milioni di dispositivi USB 2.0. Inoltre, la patch pubblicata è valida soltanto per le pendrive e solo per alcuni specifici modelli (anche se teoricamente estendibile a qualsiasi altro modello). La loro soluzione si basata su una caratteristica che consente, nei nuovi dispositivi, il blocco del "boot mode", impedendo quindi un reset completo del firmware del dispositivo. È comunque evidente che un pirata intenzionato ad eseguire un attacco mirato potrebbe aggirare anche questa patch aprendo la pendrive e collegando direttamente il chipset ad un programmatore (come si faceva per crackkare le chiavette del caffè). I ricercatori, per ovviare a questo problema, hanno suggerito di sigillare le pendrive con resina epossidica: in questo modo, se qualcuno cercasse di aprirne una, romperebbe inevitabilmente il chipset e non potrebbe quindi eseguire alcun attacco. Ma è chiaro che gli utenti non possono fare nessuna di queste operazioni: sta ai produttori il compito di prendere delle misure di sicurezza.

di leggere i tasti digitati (e quindi indovinare le password dell'utente). Ma questo tipo di attacco prevede che il pirata infetti una pendrive, la fornisca alla sua vittima e poi, in qualche modo, ne rientri in possesso. Non può quindi trattarsi di un attacco globale, ma piuttosto di un tentativo molto mirato di carpire informazioni da una specifica persona.

Il PC è sotto sequestro

Nel filone degli attacchi che non richiedono l'intervento diretto dell'utente rientra anche il bug nominato Shellshock. Questa minaccia ha dimostrato a tutti, in maniera incontrovertibile, che anche i sistemi Linux e Mac sono vulnerabili ad attacchi esterni. La caratteristica comune di questi bug è il loro successo mediatico: nomi come HeartBleed (Cuore Sanguinante), BadUSB (Cattiva USB) e ShellShock (Psicosi traumatica, anche se il termine Shell andrebbe più correttamente riferito in realtà alla console dei comandi presente su sistemi operativi Linux e Mac) sono invenzioni mediatiche che spesso confondono le idee degli utenti ben oltre le intenzioni dei pirati.

Così ci attaccano dal cellulare

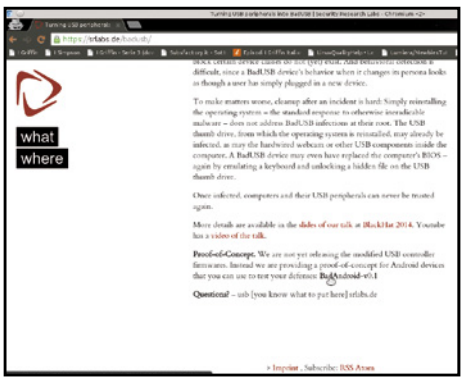
Il pericolo, infatti, è reale ma l'allarmismo generatosi sul Web è decisamente fuorviante. Tutti, infatti, parlano dell'attacco BadUSB in riferimento a pendrive e periferiche USB in generale. Nelle pagine precedenti abbiamo visto come in effetti un malintenzionato potrebbe portare a termine un attacco del genere semplicemente modificando il firmware di una chiavetta. Praticamente, però, l'attacco può essere utilizzato realmente solo in casi davvero rari e nella maggioranza delle situazioni il sistema "vittima" non risentirebbe di alcun danno. In pratica, possiamo paragonare BadUSB al raffreddore: centinaia di milioni di persone ogni giorno si ritrovano con un raffreddore. Eppure, quasi nessuno si ritrova in fin di vita per questo motivo, anzi: nella maggioranza dei casi nemmeno ci si accorge di essere malati! Analizzando più attentamente le caratteristiche di un attacco BadUSB abbiamo invece scoperto, con nostra grande sorpresa, che il vero pericolo arriva da smartphone e tablet!

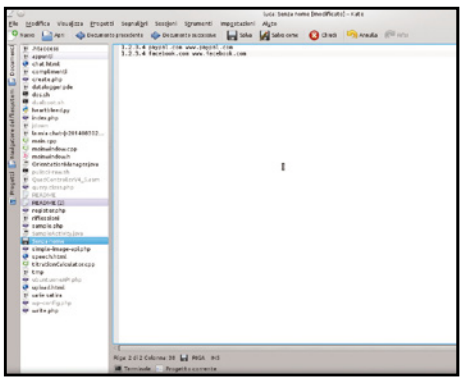
La minaccia nascosta

Anche i dispositivi mobili, infatti, possono essere collegati ad un computer tramite USB, e anche loro utilizzano il meccanismo di identificazione tramite firmware. La differenza, con altri dispositivi, è che questi sono molto più facili da riprogrammare, quindi un pirata potrebbe davvero utilizzarne qualcuno per rubare informazioni. Gli smartphone, quindi, sembrano

Con un firmware modificato

Chiunque abbia un minimo di competenze di programmazione può trasformare il proprio smartphone





1 Il codice dell'exploit

La prima cosa che il pirata deve fare è procurarsi il codice dell'exploit, realizzato dai gestori del sito srlabs.de. Il codice può essere scaricato dall'indirizzo www.winmagazine.it/link/2853 e si tratta di un semplice file ZIP con due script che verranno eseguiti su Android.

2 Root del dispositivo

Per poter realizzare questo attacco è necessario che lo smartphone del pirata sia rootato, cioè disponga dei privilegi di amministrazione. Per ogni modello esiste una metodica differente, ma sui più diffusi si può utilizzare l'app Towelroot.

3 Un file hosts "cattivo"

Adesso il pirata deve estrarre sul proprio PC il contenuto del file ZIP scaricato da SRLabs e poi creare nella stessa cartella del file *bad.sh* un file di testo chiamato *hosts*, senza alcuna estensione. Per farlo può usare il *Blocco Note* di Windows.

perfetti per BadUSB, sia perché i modelli più diffusi sono pochi, e quindi non c'è molto lavoro da fare per modificare i firmware, sia perché hanno risorse di calcolo (sono veri e propri computer) molto maggiori e una connettività diretta ad Internet. Sul Web, ad esempio, si può trovare uno script di pronto all'uso che consente di trasformare uno smartphone Android in una sorta di router virtuale, obbligando il sistema operativo del PC a cui viene collegato a dirottare verso di esso tutto il traffico Internet (www.winmagazine.it/link/2853). Questo smartphone potrebbe dunque essere utilizzato per spiare tutta la navigazione della vittima. Naturalmente, è comunque un tipo di attacco relativamente difficile da attuare, perché il pirata dovrebbe riprogrammare il proprio smartphone e poi trovare una scusa per collegarlo al PC di una vittima (per esempio con la scusa di ricaricarsi la batteria). Avendo però questi dispositivi molte più risorse a disposizione, è effettivamente possibile che in questo caso uno smartphone infetto possa diffondere il contagio ad altri telefoni, anche di modello differente.

Le giuste contromosse

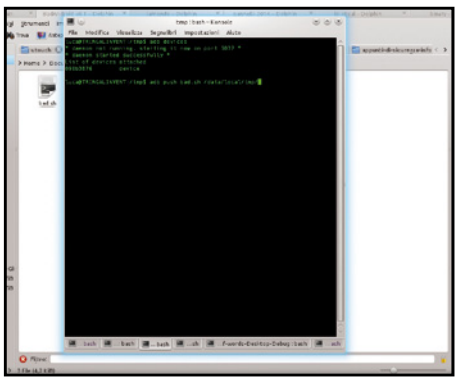
L'unico modo per proteggersi dal bug BadUSB è adottare dei comportamenti di buon senso: se vogliamo aggiornare i firmware di un dispositivo dobbiamo sempre scaricarli dal sito ufficiale del produttore e mai da altre parti. Inoltre, è buona norma non permettere a degli sconosciuti di collegare loro dispositivi ad un nostro computer oppure, se proprio non possiamo dire di no, cerchiamo almeno di non collegare contemporaneamente anche altri dispositivi di nostra proprietà (per evitare il contagio) e soprattutto non manteniamo connesso il nostro smartphone mentre colleghiamo allo stesso computer il telefono di un'altra persona. Come diceva un vecchio adagio: fidarsi è bene, non fidarsi è meglio!

Bancomat sotto attacco

È notizia recente, inoltre, che un team di pirati informatici chiamato Tyupkin abbia trovato il modo di crackkare gli sportelli bancomat e guadagnare migliaia di euro. Del resto, uno sportello

lo smartphone diventa cattivo

in un dispositivo per attaccare qualsiasi PC e intercettare il traffico Internet delle sue vittime, password comprese.



4 I file sullo smartphone

Nel file *hosts* andrà a scrivere l'indirizzo del server Web malevolo del pirata, assieme ai siti da prendere di mira, nella forma *1.2.3.4 paypal.com*. Così, tutte le richieste a PayPal verranno indirizzate al server 1.2.3.4. Il passo successivo è trasferire tutti i file sullo smartphone.

5 L'aiuto del terminale

Per spostare un file sullo smartphone si può usare il *Prompt dei comandi* di Windows, con un comando del tipo *adb push bad.sh /data/local/tmp/*. Spostati tutti i file (*bad.sh*, *cleanup.sh* e *hosts*), il pirata esegue il codice sul proprio smartphone aprendo un terminale.

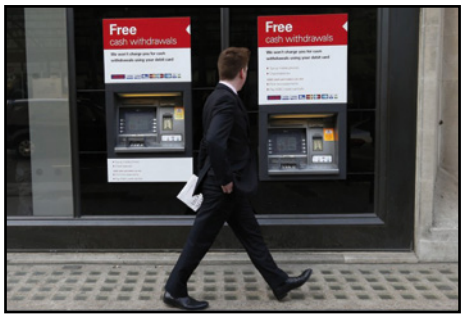
6 Dirottamento in corso

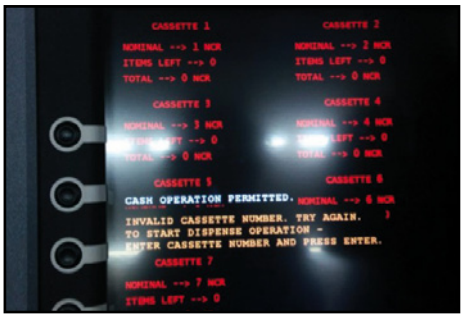
Per esempio, utilizzando l'app *Terminal Emulator*, il pirata può dare il comando *sh /data/local/tmp/bad.sh*. A questo punto deve solo trovare un pretesto per collegare lo smartphone al PC di una vittima e tutte le volte che questa andrà su PayPal, verrà indirizzata al server del pirata.

bancomat non è altro che un computer che gestisce del denaro. E buona parte di questi computer è tutt'oggi basata su Windows XP, un sistema operativo che non è più supportato da Microsoft ed è quindi alla mercé dei pirati. Questo ci da una idea della scarsa attenzione alla sicurezza informatica delle banche di tutto il mondo. Il gruppo Tyupkin comincia il proprio attacco avvicinandosi ad uno sportello bancomat (ovviamente con la complicità di un dipendente interno alla banca o utilizzando qualche furbo escamotage) e inserendo nel suo lettore CD un disco bootable contenente un sistema operativo appositamente realizzato. I lettori CD dei bancomat, infatti, sono solitamente protetti da un semplice pezzo di plastica con lucchetto: una volta forzato il lucchetto in questione, si può inserire nel computer che gestisce il bancomat qualsiasi programma.
Il criminale che ha, in questo modo, avviato il malware, telefona ad un complice che, da remoto, gli comunica un numero di sessione indispensabile per accedere al circuito bancomat internazionale (il numero viene calcolato sul momento proprio da questo complice, sfruttando un altro computer ed un apposito algoritmo). A quel punto il bancomat, senza richiedere alcuna tessera, emette 40 banconote. Considerando che il taglio più piccolo di banconote presenti in questo sportelli è solitamente di 20 euro (o dollari), stiamo parlando di un valore minimo totale di 800 euro (o dollari), rubati da un solo sportello nel giro di una trentina di minuti. I pirati di Tyupkin lavoravano soprattutto di notte, per non farsi scoprire dai passanti mentre manomettevano il lucchetto, e tutt'oggi non sono ancora stati identificati. Si calcola che abbiano già rubato una somma che supera il milione di dollari.

Il bancomat regala soldi

In quattro passi i pirati informatici possono rubare denaro da qualsiasi bancomat, senza scassinare nulla! Ecco in che modo compiono la loro malefatta.





1 Trovare il CD-Rom

Per prima cosa, il pirata "numero 1" (chiamiamolo così per comodità) si avvicina al bancomat su cui intende operare. Poi prende un cacciavite e un grimaldello e tenta di forzare il pannello di plastica dello sportello bancomat. Il suo obiettivo è quello di avere accesso al lettore CD-ROM.

2 Avvio automatico

Appena trova l'unità CD-ROM, il pirata "numero 1" può inserirvi il disco che contiene il malware. Questo disco può contenere un intero sistema operativo bootable, oppure un semplice programma malevole che viene lanciato in automatico con il vecchio AUTORUN.INF.

3 Il codice segreto

Comunque sia, ora il sistema del bancomat è compromesso. Il "pirata 1" ha bisogno di un codice di 8 cifre, che deve farsi comunicare da un complice. Quindi telefona al "pirata 2", il quale calcola all'istante il codice corretto con un algoritmo sul proprio PC e lo detta al "pirata 1".

4 Ecco il denaro

Grazie al codice, ora il "pirata 1" può entrare nel circuito bancomat e inviare ordini alla parte robotica dello sportello. In particolare, il programma con cui ha infettato questo bancomat è predisposto per fare uscire dallo sportello esattamente 40 banconote, di vario taglio.

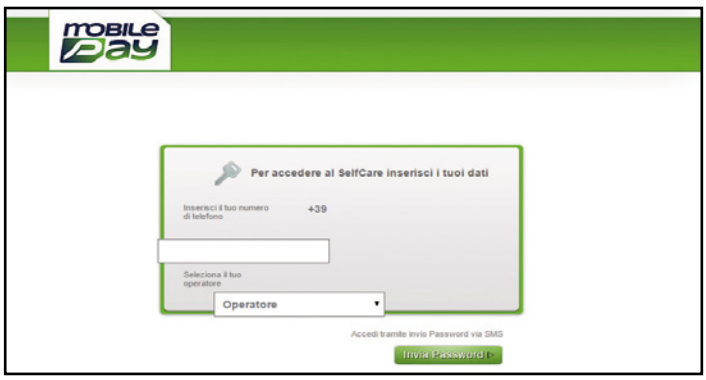
Il virus che viene dalle casse

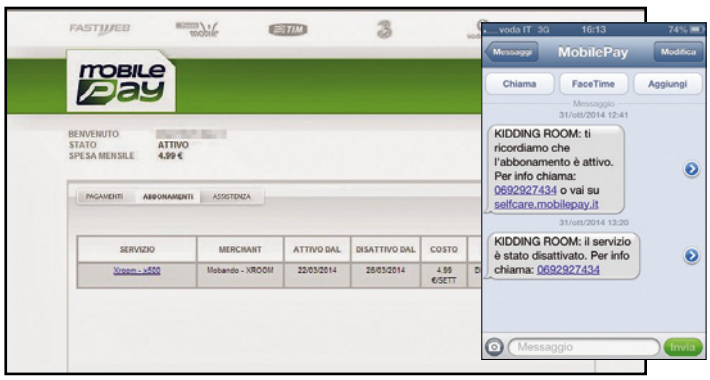
Se la vostra reazione a questo dilagare di notizie a proposito di attacchi informatici è quella di scollegare il vostro pc da internet, sappiate che esistono altri mezzi tramite i quali un malware può diffondersi. Il ricercatore Dragos Ruju ha infatti scoperto che è effettivamente possibile trasmettere informazioni da un computer all'altro tramite gli alto parlanti ed il microfono. Fondamentalmente, due computer abbastanza vicini possono dialogare "a voce" come due essere umani. La differenza fondamentale sta nel fatto che i computer possono dialogare anche con gli ultrasuoni, cioè suoni ad una frequenza tanto alta che noi non potremmo sentirla. Ciò significa che un computer infettato con un particolare virus, se lasciato con gli altoparlanti accesi, potrebbe inviare nell'aria delle onde sonore ad ultrasuoni impercettibili per gli esseri umani, ma perfettamente captabili dai microfoni di altri computer. E, considerando che spesso i microfoni vengono lasciati accesi, magari con funzioni per l'esecuzione di comandi vocali, sarebbe possibile realizzare un vero e proprio virus capace di diffondersi in questo modo. Finora sono stati sviluppati soltanto dei "proof of concept", cioè dei malware che sfruttando questo metodo, ma non creano gravi danni. In futuro però, soprattutto con l'aumento dei sistemi di riconoscimento vocale (anche in dispositivi mobili) potremmo veder comparire dei virus anche molto pericolosi.

L'app che aspira credito

Con la diffusione di smartphone e tablet sempre più evoluti e potenti è aumentato anche il traffico Internet sulle reti mobile: per controllare la posta elettronica, aggiornare il Diario di Facebook e leggere le ultime notizie si cronaca non serve più avviare il computer: bastano pochi tap sul display touchscreen. La diretta conseguenza è che sono aumentati anche i pericoli che mettono a repentaglio la sicurezza dei nostri dispositivi. Non mancano i virus che attaccano i sistemi operativi mobile, ma la vera minaccia sono le app e i servizi malevoli il cui unico scopo è quello di prosciugare il credito telefonico della nostra SIM. Il fatto è che queste applicazioni il più delle volte si nascondono all'interno di altre assolutamente "pulite" e diventa quindi molto difficile riconoscerle: basta cliccare su un link pubblicato in qualche post su Facebook o su un banner pubblicitario (a volte così ben integrati nell'interfaccia delle app da essere quasi invisibile) per attivare costosi abbonamenti ai servizi più diversi: dalle suonerie alle foto e ai video sexy! Accorgendocene subito possiamo cancellare la sottoscrizione, ma non sempre le procedure sono così semplici e intuitive. Il più delle volte è sufficiente informare il proprio operatore telefonico e chiedere di disabilitare il servizio a pagamento. Altre volte, invece, è l'app stessa che ci suggerisce un numero a cui mandare un messaggio di disdetta: peccato, però, che di solito quel numero non esiste. In questi casi, è sufficiente una veloce ricerca su Google per trovare il numero giusto al quale rivolgersi. Ultimamente, poi, è sempre più facile imbattersi in link malevoli nascosti soprattutto sui social network che, una volta selezionati (anche per sbaglio), attivano immediatamente servizi via SMS a pagamento (fino a 5 euro a settimana) tipo X-Room o Kidding Room. In genere, questi servizi utilizzano l'app Mobile Pay per recuperare il credito e possiamo disattivarli seguendo la procedura indicata di seguito.

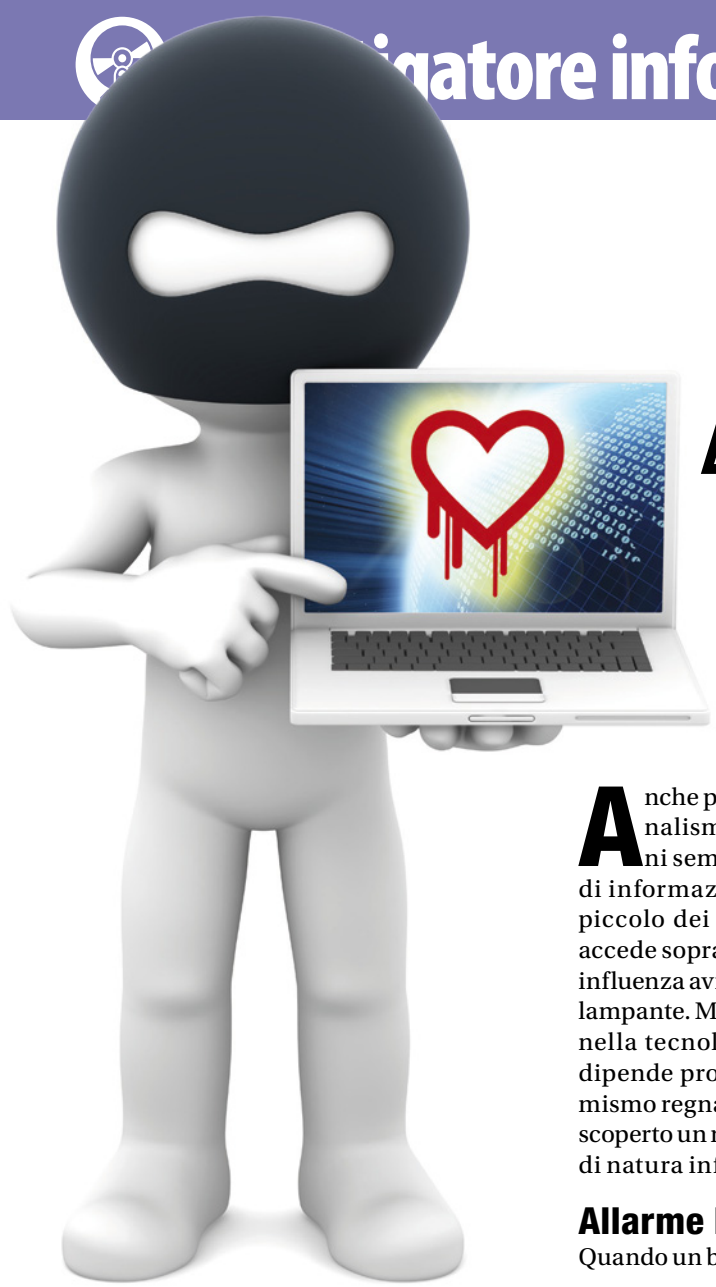
Così disattivi i servizi a pagamento abilitati sulla tua SIM telefonica





1 Innanzitutto, colleghiamoci al sito http://selfcare.mobilepay.it/m/selfcare, indichiamo il nostro numero di telefono, l'operatore e clicchiamo Invia password: riceveremo un SMS contenente un codice che dovremo copiare nella nuova pagina del sito di MobilePay.

2 Verremo così reindirizzati ad una nuova pagina di MobilePay con il riepilogo dei servizi attivi sul nostro numero di telefono: scegliamo quello che ci interessa e clicchiamo sul pulsante Disattiva. Un nuovo SMS ci informerà che il servizio è stato disattivato.



HACKER ATTACCO & DIFESA

Con la nostra guida impari ad usarei tool proibiti per entrare in ogni PC e apprendi le mosse per blindare Windows

Anche per colpa del clima di sensazionalismo che in questi ultimi decenni sembra aver posseduto gli organi di informazione, al manifestarsi del più piccolo dei problemi è già allarme. Ciò accede soprattutto per le epidemie "reali": influenza aviaria o simili ne sono l'esempio lampante. Ma poiché siamo ormai immersi nella tecnologia (e spesso la nostra vita dipende proprio da essa), lo stesso allarmismo regna sovrano ogniqualvolta viene scoperto un nuovo virus o una vulnerabilità di natura informatica.

Allarme Heartbleed

Quando un bug mette fuori uso per qualche ora un server importante (ad esempio, quelli di Facebook) i media annunciano l'evento come un presagio dell'inizio dell'apocalisse. Il problema è che, proprio perché siamo ormai abituati a veder drammatizzare qualsiasi inezia, tendiamo a dare per scontato che "si esageri" e quindi a non prendere seriamente in considerazione neppure vulnerabilità davvero pericolose. È il caso di Heartbleed, un bug particolarmente grave legato al protocollo di comunicazione sicura OpenSSL (www.openssl.org). Nonostante si tratti, senza ombra di dubbio, della vulnerabilità più pericolosa degli ultimi anni, gli utenti hanno fatto fatica a comprendere l'entità e la gravità del problema.

Così avviene un attacco ad un sito Web sfruttando il bug Heartbleed

```
s = socket.socket(socket.AF_INET,⤵
                  socket.SOCK_STREAM)
s.connect(("localhost", "443"))
s.send(create_hello(version[i]
```

È TUTTO FIN TROPPO FACILE?
Per sfruttare il bug Heartbleed è sufficiente usare uno script in Python. Ovviamente non esiste una versione pronta all'uso del codice, ma qualsiasi pirata potrebbe "iniettarlo" all'interno di un server e usarlo per prelevare 64 KB casuali dalla memoria RAM non allocata.

```
while True:
    typ, ver, pay = ⤵
                    recvmsg(s)
    if typ == None:
        return
    if typ == 22 and ⤵
       ord(pay[0]) == 0x0E:
        break
```

UNA SOLA PORTA DA APRIRE
Per prima cosa, il pirata si connette al server sulla porta 443, che è quella di un server HTTPS. Dopodiché attende una risposta dal server stesso per capire se è off-line o meno. Inutile dire che in caso il server fosse irraggiungibile il pirata non otterrebbe alcun risultato.

> *A causa del bug Heartbleed, un malintenzionato può "estrarre" enormi quantità di dati dalla memoria di server vulnerabili compromettendo qualsiasi cosa, dalle chiavi private SSL alle password utente e tutto il resto*
>
> ***Bruce Schneier**, esperto di sicurezza e crittografo statunitense*

SVELATI TUTTI I DETTAGLI DELL'ATTACCO AL CUORE DEL WEB

Il bug Heartbleed, letteralmente "cuore sanguinante", non è legato al protocollo SSL, e nemmeno all'implementazione di OpenSSL di per sé, ma all'estensione Heartbeat (letteralmente "battito del cuore"). Questa è stata scritta nel dicembre 2011 da Robin Seggelmann, un dottorando dell'università di Duisburg-Essen, e approvata da Stephen Henson (uno dei gestori del progetto OpenSSL) senza che quest'ultimo si accorgesse del bug.
Heartbeat si occupa di eseguire un test della connessione SSL per verificare, prima di cominciare la comunicazione vera e propria, che il server sia davvero chi sostiene di essere.
Se, infatti, il server è davvero sé stesso, deve possedere la propria chiave privata, nota esclusivamente al server. In una normale richiesta effettuata mediante l'estensione Heartbeat, il client invia al server la seguente richiesta (cifrando il testo con la chiave pubblica del server): ***Rispondi con la parola di 5 lettere "hello".***
A questo punto il server (se è davvero riuscito a leggere la parola "hello" decifrandola con la propria chiave privata) risponde: ***hello***, dimostrando di possedere la chiave privata ed essere davvero chi dichiara di essere. Il bug sta nel fatto che il server non controlla che il numero di caratteri richiesto dal client sia corretto. Un malintenzionato potrebbe quindi inviare al server la richiesta: ***Rispondi con la parola di 20000 lettere "hello"***, ottenendo la risposta ***helloXYZ*** dove, ovviamente, ***XYZ*** è un insieme di 19995 caratteri prelevati dalla memoria del server stesso. Un pirata può, quindi, ottenere un dump (un'operazione di estrazione di informazioni da un database) di quasi tutta la memoria RAM del server, per l'esattezza a blocchi di 64 KB la volta. E, ovviamente, nella memoria del server è caricato anche il certificato di sicurezza, con tanto di chiave SSL privata.

Il pericolo che non ti aspetti

Come ogni esperto di sicurezza sa, "un falso senso di sicurezza è più pericoloso di nessuna sicurezza". A causa di Heartbleed, milioni di utenti in tutto il mondo sono stati vulnerabili proprio nei momenti in cui credevano di essere più protetti: mentre accedevano a pagine o servizi Web protetti mediante il protocollo HTTPS. Il bug consente ad un pirata la lettura delle informazioni inviate da un utente ad un server, comprese le password. I pirati che hanno scoperto il bug prima del suo annuncio pubblico possono, quindi, avere facilmente collezionato milioni e milioni di password di ignari utenti. Non si sa ancora se e quali account siano stati realmente violati sfruttando questa vulnerabilità. L'aggravante di tutta questa brutta storia è che tra i possibili attaccanti vi sono anche i servizi di informazione di alcuni governi nazionali che, neanche a dirlo, dispongono di sistemi di analisi del Web molto potenti. E la mente corre subito allo scandalo Datagate scoppiato dopo la scoperta delle migliaia di intercettazioni non autorizzate portate avanti per anni dalla NSA, l'agenzia di sicurezza nazionale degli Stati Uniti d'America. I servizi USA ovviamente negano tutto (www.winmagazine.it/link/2606),

```
s.send(create_hb(version[i]
                        [1]))
if hit_hb(s,create_
        hb(version[i][1])):
    break
```

IL CODICE DI ATTACCO È STATO INVIATO
Il pirata invia quindi la richiesta Heartbeat incriminata (generata dalla funzione *create_hbper* di OpenSSL). Bastano pochi bit di richiesta per generare, o meglio sfruttare, un errore di programmazione che lascerebbe di stucco ogni programmatore, anche quello alle prime armi.

```
hexdump(pay)
if len(pay) > 3:
    print 'WARNING: ser
     ver is vulnerable!'
else:
     print 'Server did
not return any extra data.'
return True
```

ECCO LA CHIAVE PRIVATA DEL SERVER
Per provare che il server sia davvero vulnerabile, basta verificare che abbia risposto (*pay*) con una parola di tre o più caratteri. Trovare la chiave privata del server non è un'operazione immediata perché potrebbe essere nascosta nelle migliaia di caratteri leggibili sfruttando Heartbleed.

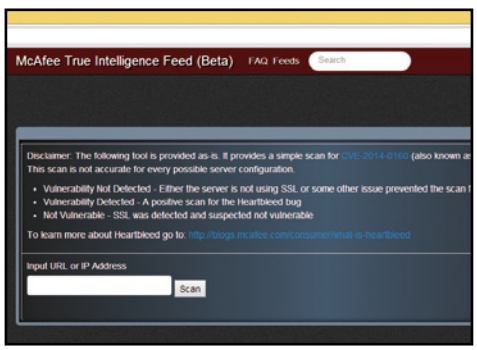
ma secondo alcune fonti anonime bene informate Heartbleed è stato scoperto dalla NSA anni addietro, forse poco dopo la sua erronea introduzione nel codice di OpenSSL (leggi a tal proposito il box **Svelati tutti i dettagli dell'attacco al cuore del Web**), e gli agenti dell'intelligence non si sarebbero fatti scrupolo di usare il bug del protocollo per catturare e decifrare quante più comunicazioni possibili tra privati cittadini. Secondo Sean Gallagher di ArsTechina, inoltre, se davvero l'NSA avesse scoperto l'esistenza di Heartbleed a pochi giorni dalla sua creazione, vorrebbe dire che l'agenzia di sicurezza americana avrebbe dedicato ingenti risorse per seguire e monitorare il progetto e che, pur di raggiungere i suoi scopi, avrebbe evitato di segnalare il pericolo lasciando milioni di internauti in balìa dei pirati informatici. Un'ipotesi incredibile, che però confermerebbe quanto in parte già descritto dai documenti riservati del caso Datagate: dalle carte si evince, infatti, che l'intelligence americana dispone di un budget di 1,6 miliardi di dollari da destinare all'analisi e allo sfruttamento dei dati che circolano su Internet e che gli esperti della NSA specializzati nella caccia alle vulnerabilità software sono un migliaio, con il compito ben preciso di scovare ogni falla nei sistemi di crittografia!

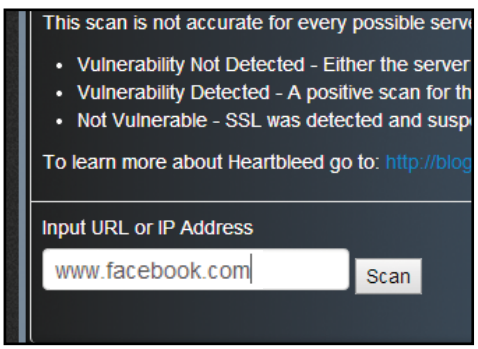
Un futuro incerto?

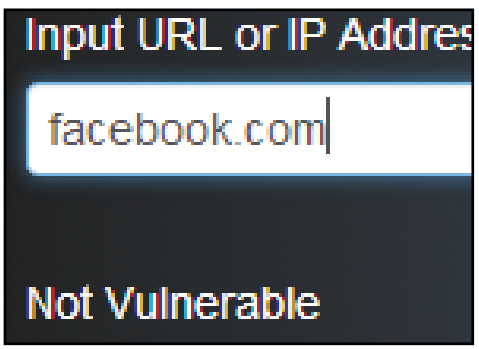
Lo scenario catastrofico generato da Heartbleed ha dunque riacceso nuove polemiche e argomenti di discussione relativi alla sicurezza su Internet. Ancora una volta sono coinvolti tutti, dalle grandi corporation, colpevoli di non aver supportato abbastanza il progetto OpenSSL, ai pirati informatici sempre a caccia di nuove vulnerabilità in stile Heartbleed. Sicuramente, il retroscena più inquietante è quello sull'impegno profuso nella gestione e nella cura di OpenSSL: un componente di sicurezza essenziale per la parte di Internet più frequentata dagli utenti ma che è stato sin qui curato da appena due sviluppatori (uno solo impegnato a tempo pieno) che possono contare su donazioni annuali di appena 2.000 dollari! Fortunatamente il caso Heartbleed sembra avere insegnato qualcosa alle grandi aziende e ora accanto a Steve Marquess e Stephen Henson (i due sviluppatori di cui sopra) dovrebbero arrivare un bel po' di forze fresche e OpenSSL dovrebbe giovarsi di finanziamenti sostanziosi gestiti da Linux Foundation con il contributo di colossi del calibro di Microsoft, Intel, Google, Facebook e Qualcomm. **Nel frattempo, ricordiamoci di cambiare tutte le password dei nostri account Web per impedire a qualche malintenzionato di trafugare i nostri dati personali.**

Verifichiamo la sicurezza dei siti

Grazie ad un tool messo a punto da McAfee possiamo testare la sicurezza o meno di qualunque servizio Web di nostro interesse. Basterà indicarne l'indirizzo e ci verrà dato un responso in merito al bug Heartbleed.







1 Andiamo sul sito

Il primo passo consiste nel visitare il sito Web allestito da McAfee per controllare l'eventuale presenza della vulnerabilità Heartbleed. Apriamo il browser e digitiamo http://tif.mcafee.com/heartbleedtest: il sito si presenta con un'interfaccia minimale.

2 Quale sito controllo?

Nel campo *Input URL or IP Address* inseriamo l'indirizzo del sito Web che vogliamo controllare. Possiamo inserire l'URL di Facebook, di Google, di Gmail, insomma di qualunque servizio di cui volessimo sincerarci in quanto ad affidabilità.

3 Siamo al sicuro!

Scelto il sito Web da controllare, dobbiamo semplicemente cliccare *Scan*. Pochi secondi di attesa e vedremo comparire il verdetto: nel nostro caso, il responso risulta negativo, segno che il sito ha provveduto ad aggiornare la versione di OpenSSL usata!

HEARTBLEED: TUTTO QUELLO CHE C'È DA SAPERE!

Il bug è stato introdotto in OpenSSL 1.0.1f, versione rilasciata nel dicembre del 2011, e reso pubblico lo scorso 7 aprile. È stato corretto il 14 marzo 2014 con il rilascio di OpenSSL 1.0.1g.

Sfruttando il bug del protocollo OpenSSL, i pirati informatici riescono a rubare dati trasmessi su Internet mediante connessioni di tipo SSL/TLS utilizzate da diverse applicazioni tra le quali:

- Browser
- Client e-mail
- Instant messagging
- Reti private VPN

La vulnerabilità consente ai pirati di accedere ai server Web ed entrare in possesso di:

- Password di accesso ai servizi on-line
- Numeri carte di credito
- Dati personali e sensibili

Dalle prime analisi, Heartbleed ha finora messo a rischio il 66% dei siti Web protetti mediante protocollo HTTPS: stiamo parlando di circa 500.000 siti vulnerabili!

Tra i siti e i servizi a rischio, per i quali è opportuno cambiare la password, ci sono:

Facebook • Pinterest • Tumblr • Twitter • Google • Apple • Yahoo • Gmail • Yahoo Mail • eBay

Sono invece immuni ad Heartbleed i seguenti siti e servizi:

LinkedIn • Microsoft • Hotmail/Outlook • Amazon • PayPal

Spetta ai responsabili della sicurezza dei singoli siti aggiornare il modulo OpenSSL alla nuova versione. Non bisogna installare alcun aggiornamento di sicurezza su PC, tablet e telefonini, ma chi ha un computer che ospita un sito Web oppure un NAS dovrà verificare se sta usando la versione vulnerabile di OpenSSL.

Tutti i sistemi operativi Mac OS, Linux, Windows, Android e iOS sono vulnerabili a Heartbleed

LE REGOLE D'ORO PER DIFENDERSI DA HEARTBLEED

1 Controlliamo se i siti Web che visitiamo più spesso sono vulnerabili testandoli su http://tif.mcafee.com/heartbleedtest

2 Evitiamo di collegarci ai siti che risultano vulnerabili. Aspettiamo quindi che il sito aggiorni la versione di **OpenSSL** e poi cambiamo immediatamente la **password**

3 Anche se un sito risulta non vulnerabile, è opportuno cambiare immediatamente la password

4 Non usiamo mai la stessa password per siti differenti

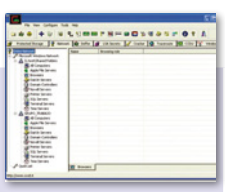
5 Diffidiamo delle e-mail che ci invitano a cliccare su un link per aggiornare le nostre password: **si tratta di attacchi di tipo phishing**

6 Per collegarsi ad un sito conviene sempre digitare a mano l'indirizzo e mai cliccare sui link che reindirizzano alla home page, in quanto potrebbero essere stati alterati

7 Se gestiamo un server Web che ospita un nostro sito o usiamo un NAS, aggiorniamoli appena possibile

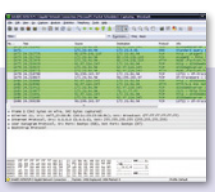
PIRATE CD: GLI STRUMENTI SEGRETI USATI DAGLI HACKER

I principali tool (li trovi sul WinDVD-Rom) preferiti dai malintenzionati per spiare via Web qualsiasi PC, collezionare password e numeri di carte di credito, clonare le identità altrui. Attenzione: usali solo sul tuo computer o su quello di un tuo amico.



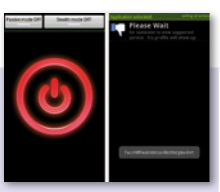
CAIN & ABEL

Permette di recuperare molti tipi di password sniffando la rete locale, usando tecniche di attacco basati su dizionari o di tipo brute force. In questo modo un eventuale malintenzionato riesce a recuperare le chiavi di acceso a siti e servizi Web di ogni genere.



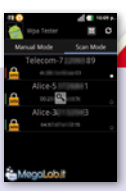
WIRESHARK

Uno degli strumenti di analisi di rete gratuito più famosi al mondo. Usando questo programma il pirata riesce a **filtrare, catturare e spiare i pacchetti e le informazioni che passano all'interno di una rete** di computer, spiando le comunicazioni via e-mail e chat.



FACENIFF

Un'app Android che permette ad un malintenzionato di portare a termine un attacco Man In The Middle (MITM): in pratica, **riesce ad inserirsi tra l'utente e il router in modo da "sniffare" la sessione aperta di Facebook, Twitter e Tumblr**.



WPA TESTER

Applicazione per dispositivi Android che consente di "testare" la sicurezza della nostra rete Wi-Fi. **Nel suo vasto database ha una lista di tutte le chiavi WPA e WEP predefinite di vari modelli di router appartenenti a circa 40 case produttrici** e forniti in comodato d'uso da provider come Alice, Fastweb, Vodafone e Infostrada.

AIRCRACKGUI

Funziona solo su dispositivi Android rootati. Per bucare le password WPA o WPA2 l'app effettua un attacco di tipo **Deauth** che farà disconnettere e riconnettere il client vittima. In questo modo il pirata potrà **sniffare la riautenticazione ed effettuare un attacco per identificare la password del Wi-Fi**.

Pirate CD

- Spia via Web qualsiasi PC
- "Colleziona" password, numeri di carta di credito&Co.
- Clona le identità sui Social
- Intercetta chat ed e-mail

Così si spia una spia

Rubare documenti personali è più facile di quanto si pensi. Scopri dove si nascondono le spie e… come spiarle!

Mano sul cuore: quante volte abbiamo pensato di mettere il naso nel PC di nostro figlio o in quello di un collega; oppure ci sarà capitato di pensare di spiare la babysitter o il dipendente attraverso una videocamera nascosta. Nonostante ci siano precise violazioni in merito, diverse persone praticano regolarmente azioni di spionaggio nei confronti dei propri familiari e colleghi. Naturalmente i fini possono essere diversi: si va dal controllo per scopi precauzionali sino a giungere ai casi più gravi, di furto di dati sensibili. Per evitare brutte sorprese e, soprattutto, proteggersi da occhi indiscreti occorre prendere coscienza degli strumenti utilizzati dagli spioni in modo da adottare opportune precauzioni. Insomma, come in tutte le attività, bisogna approfondire l'argomento e indagare su quelli che sono gli strumenti specifici in modo da poterli individuare e quindi neutralizzare. Nello speciale di queste pagine abbiamo raccolto una serie di utility con le quali registrare tutto ciò che viene digitato sulla tastiera del PC piuttosto che per offuscare dati sensibili in modo da poterli trasmettere in modo sicuro. In ultimo, abbiamo potuto testare alcune utility legate al mondo degli smartphone come la suite Oxigen Forensics, con la quale tenere traccia di tutto ciò che accade su uno smartphone.

Ragionare come un "spione"

Tra le utility maggiormente utilizzate dagli spioni figurano sicuramente i keylogger. Si

SULLE ORME DELLE SPIE CINEMATOGRAFICHE

Nella storia del cinema sono numerosi i titoli dedicati al mondo dello spionaggio. Uno di questi è The Lab, un film diretto dal regista di "Non aprite quella porta" e scritto da Shiban sceneggiatore di X-Files. La trama racconta le vicissitudini di Victor Helios che, in un laboratorio di New Orleans, è riuscito ad affinare la tecnica della cariogenesi (il congelamento di esseri umani). Una legione di superuomini sono sistemati in tutti i livelli della società e nei posti chiave con lo scopo di riuscire a conquistare il mondo. Ma il misterioso Deucalion vuole ostacolarlo. Per tutti Victor Helios è un insospettabile filantropo, ma O'Connor e Sloane sono convinti che sia il mandante di alcuni efferati omicidi...

SCHEDA TECNICA
TITOLO ORIGINALE: THE LAB
NAZIONE: USA
GENERE: HORROR
REGISTA: MARCUS NISPEL
CAST: MICHAEL MADSEN, VINCENT PEREZ, THOMAS KRETSCHMANN
DURATA: 90 MINUTI
ANNO: 2004

tratta, sostanzialmente, di software in grado di registrare tutto ciò che viene digitato sulla tastiera del computer. Ovviamente occorre che il software venga preventivamente installato sulla nostra macchina prima di poterlo mettere in funzione per "rubare i nostri dati". La sua installazione richiede, quindi, del tempo ed è pertanto buona regola proteggere sempre il proprio PC con password, in modo da rendere la vita difficile allo spione di turno. Genera-

Gli speciali bottoni con microspia incorporata possono essere applicati sulle bretelle di uno zaino e mimetizzarsi con una certa facilità (www.mondospy.com, € 97,75).

GADGET HI-TECH DA VERI 007

Affinché le operazioni di spionaggio siano veramente efficace, occorre munirsi degli strumenti giusti. Sul Web è possibile reperire diversi dispositivi utili a questo tipo di attività: Amazon, ad esempio, offre diversi oggetti da poter utilizzare per attuare efficaci tecniche di "intelligence". Al modico prezzo di 13,80 euro è possibile acquistare **Spy Pen 4 GB**, ovvero una penna in grado di registrare video e foto in formato HD. Sullo stesso portale di e-commerce, al prezzo di 68,50 euro, è possibile acquistare l'infallibile **orologio SC103 Spy Pro HD 1080P 4 GB IR** che, oltre ad effettuare riprese e registrazioni audio, permette anche le riprese notturne! Per attività da vero agente 007 segnaliamo la micro **spia per le intercettazioni ambientali**: acquistabile su eBay al prezzo di 32,99 euro, consente di ascoltare a distanza una conversazione. La microspia dispone, infatti, di una scheda SIM: pertanto, telefonando al numero associato alla scheda sarà possibile ascoltare tutto ciò che succede nell'ambiente in cui è posizionata la cimice. Non manca ovviamente la **sveglia con telecamera nascosta** in grado di rilevare il movimento e registrare video e foto: la si può acquistare sempre su eBay al prezzo di 23,42 euro.

SPY vs SPY TOOLKIT

- Nascondere informazioni nelle foto
- Offuscare i propri dati sensibili
- Scoprire le password di Windows
- Trasformare la webcam in telecamera di videosorveglianza

I migliori tool per spiare e non farsi spiare, da testare e utilizzare solo a fini personali. Li trovi tutti all'interno del DVD allegato a questo speciale.

Secure Eraser
Consente di eliminare i file dal PC senza che sia lasciata alcuna traccia e possibilità di recupero.

Refog Free Keylogger
Occorre tenere sotto controllo i figli o il partner? Se la risposta è affermativa, con Refog Free Keylogger è possibile intercettare le conversazioni in chat oppure scoprire i siti Web visitati ecc.

Shadow Explorer
Un software per Windows che rende possibile la visualizzazione e il ripristino dei file utilizzando le "copie Shadow" che il sistema operativo regolarmente esegue.

Hide my Windows
Non vogliamo farci sorprendere dal capo mentre navighiamo sul Web? Con questo tool possiamo simulare l'esecuzione di software gestionali e scambiare le schermate con un solo clic.

Exif Pilot
Permette di creare e personalizzare le informazioni associate ad un immagine come, ad esempio, il tipo di macchina fotografica data e ora dello scatto e tanto altro ancora.

SilentEye
Permette di nascondere messaggi segreti all'interno di file audio o immagini; i dati possono inoltre essere protetti con password.

Recuva
Utile a ripristinare i file cancellati accidentalmente dal computer o dalle periferiche esterne come hard disk e pendrive USB.

iSpy
Il programma giusto per trasformare la Webcam in una telecamera per sorvegliare casa o ufficio.

G Data Internet Security Suite
Tutto l'occorrente per proteggersi da virus&Co.

Casebook
Gioco composto da quattro episodi in stile CSI in cui dovremo vestire i passi di un vero detective che dovrà analizzare nei minimi dettagli la scena del crimine. **Il gioco lo trovi nell'interfaccia principale del Win DVD-Rom**.

ta una chiave di accesso al nostro account, poi, è importante ricordarci di premere sempre la combinazione di tasti Win+L prima di allontanarci dalla nostra postazione, in modo da bloccare la sessione attiva sul PC proteggendola proprio con la nostra password. Eviteremo così di lasciare incustodito il computer per molto tempo consentendo allo spione di agire indisturbato. Altro espediente potrebbe essere quello di anticipare le mosse dello spione installando sul proprio PC un software keylogger che in tal caso sarebbe sotto il nostro personale controllo e dunque andrebbe a registrare tutto ciò che accade sul PC quando siamo assenti. In merito ai documenti, il consiglio è quello di proteggerli con password e preferibilmente convertirli preventivamente in formato PDF, andando ad inserire all'interno del testo (magari nell'intestazione o nel pie' di pagina) la data di creazione del documento: in tal modo, se lo spione riesce a cambiare la data di creazione a livello di file, nel documento rimane quella originale.

Gli strumenti adatti

Come accennato, per proteggersi dalle spie informatiche occorre conoscere gli strumenti che usano e saperli, a nostra volta, sfruttare al meglio. Per tale motivo, all'interno del Win DVD abbiamo inserito una serie di tool utili per l'attività di controspionaggio. Nelle pagine che seguono troviamo le spiegazioni di molti dei software inclusi nel supporto: pertanto, non resta che armarci di buona pazienza e con una buona dose di curiosità esplorarli uno ad uno, magari effettuando qualche test: così facendo, lo spione avrà vita dura ma, soprattutto, sapremo affrontare e risolvere le varie situazioni di pericolo man mano che si dovessero presentare!

LO SPY SHOP PER VERI PROFESSIONISTI

Per chi volesse fare sul serio con le tecniche di spionaggio e controspionaggio occorrono strumenti all'altezza delle varie situazioni che man mano si possono presentare. Naturalmente, il costo di certi dispositivi sale man mano che le pretese di affidabilità e qualità crescono. Il mercato offre oggigiorno congegni a basso costo in grado di svolgere (almeno sulla carta) registrazioni e altre funzionalità che però non sempre si rilevano all'altezza. Scoprire di aver registrato audio di scarsa qualità oppure video a bassa risoluzione può significare compromettere tutto il lavoro svolto. Per evitare di sbagliare almeno negli acquisti dei dispositivi, ci si può rivolgere ai negozi specializzati che pullulano sul Web. Ecco cosa si trova.

Rilevatore di microspie

Tra gli strumenti che non dovrebbero mancare nella cassetta del perfetto agente 007 figura sicuramente il rilevatore di microspie (www.mondospy.com), ovvero un dispositivo in grado di rilevare se in una stanza si nascondono cimici; si tratta, in sostanza, di un localizzatore di frequenze in grado di intercettare le trasmissioni in un ambiente chiuso e dunque di rilevare la presenza o meno di apparecchiature elettroniche in grado di trasferire dati a nostra insaputa.

Valigetta di bonifica

Per maggiore affidabilità, al costo di qualche migliaio di euro possiamo procurarci una valigetta di bonifica (acquistabile sul sito www.microspie.org) capace di scoprire attraverso un'apposita e sofisticata apparecchiatura tutte le cimici nascoste in una determinata area.

Software di controllo

Per azioni di spionaggio sul PC ci si può affidare a Condor-KS (www.protezioneglobale.com) l'innovativo software realizzato da specialisti del settore che permette la sorveglianza nascosta di un PC. In pratica il software, una volta installato, registra tutti i dati digitati sulla tastiera, i siti Web visitati, le password, gli screenshot e quant'altro. Condor-KS non viene rilevato dagli antivirus e da antispyware e non crea rallentamenti in modo da destare il minimo sospetto. Tutte le azioni sono registrate con data e ora. Trascorso qualche giorno, lo spione, approfittando di una nostra temporanea assenza, connetterà una chiavetta USB al computer e con un clic trasferirà tutti i dati acquisiti. Non verrà lasciata mai nessuna traccia e con un altro clic sarà possibile disinstallare il programma.

Gli occhiali con binocolo incorporato possono rendersi utili per osservare a distanza i movimenti di persone senza l'uso delle mani.

La parola all'avvocato

Guido Scorza è uno dei massimi esperti in Diritto delle Nuove Tecnologie

SPIONAGGIO E CONTROSPIONAGGIO: COSA DICE LA LEGGE?

Oggigiorno si potrebbe spiare la donna delle pulizie per verificarne il comportamento oppure un dipendente per verificarne la resa sul posto di lavoro. L'attività di spionaggio assume molte sfaccettature: per chiarire la legalità di certe operazioni abbiamo quindi chiesto un parere all'avvocato Guido Scorza, uno dei massimi esperti italiani in diritto delle nuove tecnologie.

Qualora dovessimo forzare la password di Windows del PC dei nostri colleghi, in quali sanzioni possiamo andare incontro?
Direi che è meglio non provarci, neppure per scherzo. Accedere al PC o a qualsiasi altro dispositivo o rete altrui senza permesso costituisce reato (accesso abusivo a sistema informatico o telematico) e può costare caro: fino a tre anni di prigione. Specie nel 2014, in fondo, entrare nel PC altrui è un po' come violare il suo domicilio, entrare a casa sua o nel suo ufficio. Senza contare che se poi, una volta nel PC, si sbircia nei dati personali che vi sono contenuti, si possono commettere tutta una serie di altri reati connessi alla violazione della privacy che rischiano di "costare" altrettanto. Insomma mettere le mani nel barattolo della marmellata di una volta era, sicuramente, meno pericoloso.

Cosa ci può dire in merito alle videocamere di sorveglianza? È possibile installarle ovunque?
È possibile installarle laddove sussistano ragioni – normalmente di sicurezza – che ne giustifichino l'utilizzo e soprattutto giustifichino la limitazione dell'altrui privacy che certamente l'installazione di una telecamera comporta. Deve trattarsi di una reale necessità e, soprattutto, di una necessità proporzionata alla limitazione della privacy che si determina. In ogni caso, poi, le telecamere di sorveglianza devono essere installate nel rispetto delle regole dettate dal Garante per la privacy che, tra l'altro, stabiliscono che i soggetti che gravitano nell'area oggetto di telesorveglianza devono essere informati della circostanza che "non sono soli". Guai, peraltro, a pensare che basta un cartello e che poi si può fare ciò che si vuole delle immagini che si acquisiscono. Le immagini raccolte attraverso le telecamere devono essere conservate solo per il periodo strettamente necessario alla soddisfazione delle esigenze di sicurezza che ne hanno giustificato l'installazione e devono poi essere cancellate senza ritardo.

Un datore di lavoro potrebbe spiare i propri dipendenti attraverso videocamere nascoste?
Assolutamente no! Lo vieta la disciplina sulla privacy e lo vieta lo statuto dei lavoratori. In linea generale nessuno può "spiare" nessuno e men che meno i propri lavoratori. "Spiare", ovvero osservare di nascosto, specie attraverso strumenti a distanza, è legittimo solo se a farlo sono le forze dell'ordine previo idoneo provvedimento dell'Autorità giudiziaria e, in casi davvero particolari, gli investigatori privati ed i giornalisti. Spiare è sempre più facile grazie ad un'infinità di gadget tecnologici ma non per questo è anche sempre più legittimo.

Diversi software integrano al loro interno dei keylogger che spesso passano inosservati agli utenti, raccogliendo così dati preziosi circa le abitudini di chi usa il computer. I produttori di software possono monitorare i PC degli utenti senza previo consenso?
Il keylogger è uno dei più giovani membri della famiglia degli "spioni tecnologici". Valgono per questo tipo di software le considerazioni appena fatte per gli spioni a mezzo telecamere o analoghi dispositivi tecnologici. Spiare cosa faccio sul e con il mio computer è reato e trattare abusivamente – ovvero senza il mio permesso i dati così acquisiti – è un altro reato. Sarà amache facile ma proprio non lo si può fare se si tiene alla propria libertà e, soprattutto, se si ama la legalità.

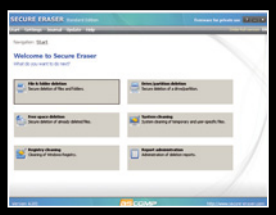
Come mai esistono tanti programmi liberamente scaricabili con i quali poter violare le leggi? Non dovrebbero essere vietati?
Se potessi rispondere alla domanda con una domanda, vi chiederei: perché si producono macchine che vanno tanto veloci se poi esistono limiti di velocità tanto stringenti? Fuor di battute, il punto è che la tecnologia non è mai né lecita, né illecita ma dipende sempre da come la si usa e, in taluni casi, da perché e chi la usa. Una pistola può essere usata per legittima difesa o per ammazzare qualcuno. Vale la stessa regola per queste tecnologie. Possono installarmi un keylogger trasparente sul mio PC per evitare che altri non lo usino a mia insaputa...

È possibile tracciare la posizione GPS di un persona per poi trasmetterla a terzi?
Sì, con il permesso della persona tracciata, nel rispetto delle regole dettate dal Garante privacy e, soprattutto, dopo aver notificato a quest'ultimo il trattamento che intende porre in essere. No, in assenza di questi requisiti. E' una delle sfide più delicate in termini di privacy. Ormai la tecnologia da indossare si sta diffondendo a macchia d'olio e, soprattutto, c'è un GPS in ogni smartphone. Una montagna di dati che fa e farà sempre più gola ai signori del marketing. Ma sapere dove si trova una persona e quale zona frequenta più spesso significa intromettersi pesantemente nella sua vita privata. Non è cosa che si possa fare solo perché tecnologicamente facile.

Il cavetto USB nasconde una micro camera in grado di registrare tutto ciò che avviene davanti al PC.

Questo dispositivo, dalle dimensioni di un pacchetto di sigarette, nasconde un trasmettitore in grado di registrare i movimenti di un veicolo.

I MIGLIORI TOOL PER LO SPIONAGGIO



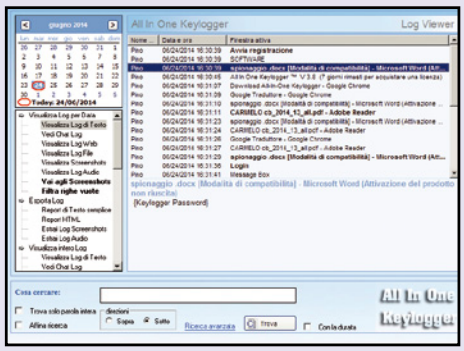
Dati "piccanti": cancellali così
Cancellare i file dal cestino di Windows non significa eliminarli definitivamente: per cancellare ogni traccia dei file possiamo affidarci a Secure Eraser. Dopo averlo installato clicchiamo *File & Folder deletion* dalla finestra che appare, aggiungiamo i file e/o le cartelle che vogliamo eliminare e scegliamo un metodo di cancellazione, ad esempio *Highest - Peter Gutmann Standard*.

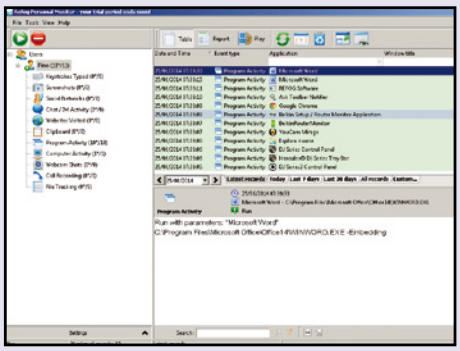
Nascondere le schermate
Per non farsi beccare in ufficio su Facebook possiamo usare Hide My Windows. Dopo avere installato il programma possiamo definire un'azione o una combinazione di tasti da premere, ad esempio *Ctrl+Alt+I*, per nascondere il browser o ridurre a icona le varie finestre aperte sul desktop. Volendo, dal menu *View / Option* possiamo anche impostare una password di protezione.

KEYLOGGER E TOOL DI MONITORAGGIO

I software keylogger possono registrare quello che viene digitato con la tastiera del PC. Una volta installato, il programma avvia la registrazione di tutto ciò che accade sul computer, compresi i testi digitati in Word, le password di accesso ai vari servizi on-line, le credenziali di accesso del conto corrente bancario, la cronologia dei siti Web visitati e tanto altro ancora. Lo spione potrà dunque impadronirsi di una serie di dati sensibili man mano che vengono digitati dall'utente ignaro. Tutto ciò che viene registrato potrà essere inviato via FTP oppure memorizzato su una chiavetta USB.

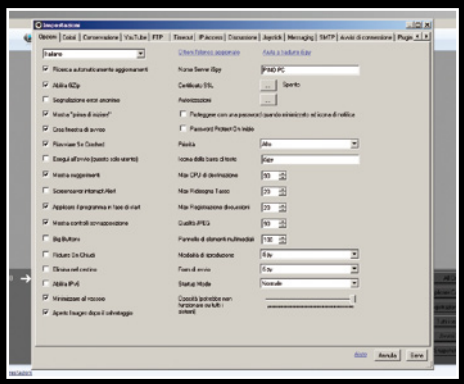
I tool di monitoraggio, invece, aggiungono ulteriori funzionalità all'azione di un semplice keylogger: permettono, infatti, di registrare quando vengono compiute determinate azioni e soprattutto consentono di inviare i dati di log via e-mail. Software come **Refrog Personal Monitor** permettono di impostare i parametri di un account e-mail e di inviare all'indirizzo specifico i dati di log ad intervalli di tempo stabiliti in fase di setup. Il file inviato potrà contenere tutto ciò che riguarda la cronologia Web piuttosto che i documenti aperti sul PC o ancora alcune foto scattate dalla Webcam.

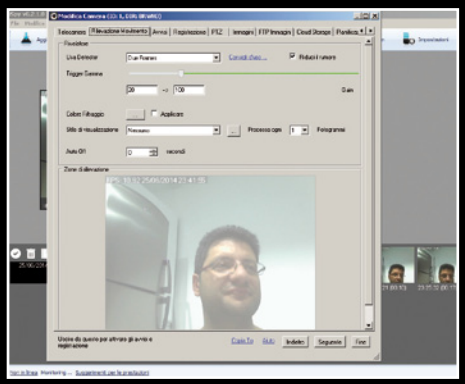


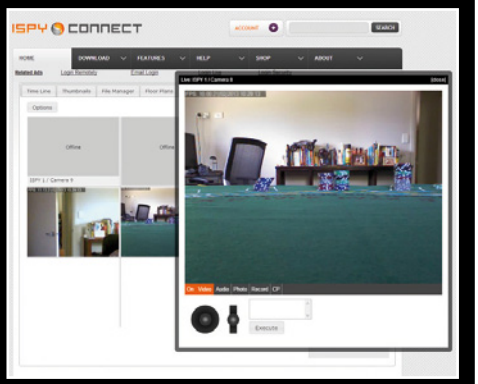


Ti spio con una Webcam

Vuoi scoprire chi usa di nascosto il tuo computer o mette mano sulla tua scrivania? Per farlo bastano una Webcam e un software in grado di trasformarla in una videocamera di sorveglianza. Ecco come.







1 Attiviamo le riprese

Installiamo innanzitutto il tool iSpy, avviamolo e dal menu *Options* scegliamo la lingua *Italiano*. Quindi clicchiamo *Aggiungi* e poi *Camera locale*: il software rileverà automaticamente la Webcam. Confermando con il pulsante *Bene* apparirà un riquadro con la nostra faccia in primo piano.

1 Se ti muovi, ti riprendo!

Per fare in modo che la registrazione inizi quando la Webcam rileva un movimento, clicchiamo nel riquadro *Video* e poi su *Modifica*. In *Rilevazione movimento*, senza cambiare le impostazioni di default, clicchiamo *Fine*. Per interrompere le registrazioni clicchiamo sul pulsante con il fulmine.

1 Riprese in diretta dal Web

Per controllare ciò che avviene sul PC possiamo connetterci alla Webcam da remoto. Da *Impostazioni Web/Impostazioni Web Server* creiamo un nuovo account. In seguito, con un semplice login possiamo prendere il controllo della videocamera e spiare chi utilizza il sistema.

SFIDA DI SPIONAGGIO CON LO SMARTPHONE

Gli smartphone hanno assunto un ruolo fondamentale nella vita di tutti i giorni: possiamo tenerci in contatto con amici e parenti e condividere quasi in tempo reale tutte le nostre emozioni mediante immagini, video e messaggi di testo. Al contempo, però, siamo molto più vulnerabili visto che le nostre abitudini possono rilevarsi con una certa facilità. Basta un software spia per registrare tutto ciò che facciamo e comunichiamo attraverso il cellulare. Ecco quindi la simulazione di un duello tra spione e spiato così da indicare a ciascuna azione di spionaggio una opportuna contromisura.

ATTACCO

CONTROLLO DEL CELLULARE

Lo spione potrebbe manomettere il cellulare in modo da assicurarsi il suo controllo: potrebbe, ad esempio, scoprire la posizione geografica e rubare altre informazioni strettamente personali come le password che solitamente memorizziamo nella memoria del dispositivo. Naturalmente lo spione dovrebbe impadronirsi dello smartphone a nostra insaputa e conoscere eventualmente la password di

ANALISI FORENSE

Se lo smartphone cade in mani sbagliate potrebbe essere sottoposto ad una analisi forense. In sostanza, lo spione potrebbe svolgere un'indagine in modo da risalire ad una serie di informazioni che riguardano, ad esempio, l'elenco delle telefonate inviate e ricevute, recupero dei messaggi di testo e altre informazioni strettamente personali. Per compiere una simile analisi, lo spione si avvale dell'applicazione gratuita Oxigen Forensics Suite (www.oxygen-forensic.com/en/). Una volta installata sul telefono dell'ignaro malcapitato, permette di estrarre con pochi passaggi tutte le informazioni che occorrono, comprese ad esempio le coordinate GPS, le foto ecc.

SPIARE I MOVIMENTI SUL TAXI

Se siamo soliti utilizzare le app per prenotare un taxi o altri servizi simili, lo spione potrebbe addirittura visualizzare su di una mappa tutti i nostri spostamenti risalendo così ad una serie di informazioni che ci riguardano, come ad esempio l'indirizzo di casa o ufficio e tanto altro ancora.

CONTROMISURA

IMPOSTIAMO ANTIFURTO E PASSWORD

Per evitare che lo smartphone cada in mani sbagliate occorre, anzitutto, impostare una password sicura composta da una stringa lunga almeno 8 caratteri composta da numeri, lettere minuscole e maiuscole. Per le password legate ad altri servizi, corre in nostro aiuto l'app Secure Vault, Password Manager. Le password memorizzate possono essere suddivise per categoria e, cosa importante, al momento della chiusura dell'app le informazioni vengono criptate sulla scheda SD del telefono.

CRIPTARE IL DISPOSITIVO

Si potrebbe ad esempio criptare il contenuto dello smartphone in modo da renderli inaccessibili se non dopo aver inserito una chiave di sblocco. Chi non conosce password o PIN non potrà accedere ai file crittografati contenuti nella memoria del dispositivo. Il rovescio della medaglia è una maggiore lentezza del cellulare nel rispondere ai comandi. La crittografia, inoltre, è un processo di sola andata: una volta che i file sono stati criptati non potranno più tornare al loro stato "originario". Solamente riportando il dispositivo alle impostazioni di fabbrica si potranno annullare gli effetti del criptaggio. Inoltre, se qualcosa dovesse andare storto nel corso del processo, si rischierebbe di perdere definitivamente tutti i dati.

PRENOTARE PERSONALMENTE I SERVIZI

Come contromisura possiamo semplicemente prenotare personalmente i servizi evitando di usare app specifiche: in tal modo, lo spione non ha modo di sapere cosa stiamo prenotando in un determinato momento e gli risulterà difficile seguire i nostri spostamenti. Un altro espediente potrebbe essere quello di lasciare volutamente a casa il cellulare durante gli spostamenti.

Lo scova password

Ti sveliamo le procedure segrete per scardinare PIN, impronte digitali e codici di accesso

Cosa ci occorre

30 MIN. DIFFICILE

KIT DI RECUPERO
LO SCOVA PASSWORD
SOFTWARE COMPLETO
Lo trovi su: ☑DVD
Sito Internet: www.winmagazine.it

"Mi serve un file, anzi, mi serve proprio quel file ma... dove l'ho salvato? Ah sì, è sul vecchio PC! Lo riaccendo ma è passato troppo tempo dall'ultima volta che l'ho usato e purtroppo non ricordo più la password di accesso a Windows! E adesso?". Tante volte ci siamo imbattuti in questa o in situazioni simili, in cui è necessario accedere a vecchi documenti o addirittura accendere dispositivi protetti da una password che, anche pensando e ripensando, proprio vuole tornarci in mente. Nemmeno i famosi "suggerimenti", le domande di sicurezza o gli innumerevoli tentatici di inserimento ci danno una mano, anzi spesso ci confondono e depistano ancora di più.

Accesso consentito: ecco le soluzioni software

Per fortuna abbiamo la possibilità di rimediare a questo fastidioso inconveniente. Le soluzioni per riottenere l'accesso al nostro sistema e alle cartelle in cui sono archiviati documenti e dati personali esistono, anche se non sempre risultano semplici da mettere in pratica. Con le dritte giuste, però, riusciremo a superare anche i più ostici sistemi di protezione. Grazie ad alcuni particolari strumenti software, infatti, in pochi e semplici passaggi

COME USARE LO SCOVA PASSWORD

Alcuni dei metodi illustrati nell'articolo sono gli stessi utilizzati dagli hacker per superare i diversi sistemi di protezione dei nostri dati, anche quelli "alternativi" che dovrebbero garantirci un maggiore grado di sicurezza, richiedendo per l'accesso al PC informazioni aggiuntive oltre alla classica password, come ad esempio i lettori di impronte digitali o gli scanner della retina, ma che eliminando appunto la password di accesso, perdono la loro validità. Mettiamo quindi in pratica le procedure indicate esclusivamente sul nostro computer oppure su quello dei nostri amici ma solo dopo avere ottenuto il loro consenso!

Il nostro esclusivo disco di emergenza per recuperare i codici di accesso di: Windows, Office, router Wi-Fi, archivi compressi e file PDF protetti e... tanto altro ancora.

TOOL DA UTILIZZARE	RECUPERA LE PASSWORD DI...	GUIDA PRATICA
NTPASSWORD	Windows (tutte le versioni tranne Windows 8.1 con account locale)	pag. 40
APPNIMI RAR PASSWORD UNLOCKER 2.02	Archivi compressi in formato RAR/ZIP protetti da password.	pag. 41
APPNIMI PDF UNLOCKER 2.0	Documenti PDF protetti da password.	pag. 41
APPNIMI WORD PASSWORD RECOVERY 2.5	Documenti Word/Excel protetti.	pag. 41
UFO WARDRIVING 4 INVASION	Router Wi-Fi (compresi quelli di Alice, DLink, Fastweb...).	pag. 42
WPA TESTER 4	Router Wi-Fi protetti con chiavi WPA e WEP.	pag. 42
WINDOWS STORE SERVICE CRACK	Applicazioni scaricabili dal Windows Store.	pag. 43
Nel DVD allegato a questo speciale sono presenti tanti altri tool specifici per il recupero password		

saremo in grado di accendere normalmente il nostro computer, senza dover inserire alcuna chiave di accesso. Utilizzando NTPassword, ad esempio, bastano pochi secondi per eliminare la richiesta di inserimento password quando accendiamo un computer con sistema operativo Windows. Funziona su qualsiasi versione, dalle più vecchie e diffuse come Windows XP, fino alle ultime versioni di Windows 8/8.1. E il bello è che in tutti i casi la procedura da seguire è sempre la stessa! L'unica circostanza in cui NTPassword non riesce a compiere il suo dovere è quando l'account utente è archiviato e sincronizzato direttamente on-line sui server Microsoft e non in locale sul computer: per fortuna questa particolare tipologia di accesso è disponibile solamente da Windows 8 in poi e comunque non è obbligatorio utilizzarla.

Una memoria aggiuntiva

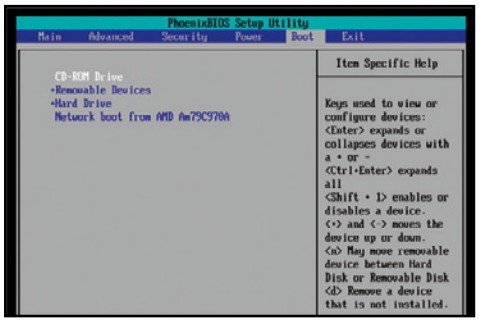
Non esiste solo Windows, però: ormai siamo circondati da password, codici e nomi utente su ogni dispositivo! Anche i nostri soldi gestiti mediante bancomat e carte di credito sono protetti da una password. Ecco quindi nascere la necessità di una memoria aggiuntiva che ci aiuti a sopperire alle nostre dimenticanze. Da internauti "esperti", ad esempio, utilizziamo sempre più spesso la funzione integrata in tutti i browser per il salvataggio delle password di accesso ai vari siti Web. Una comodità, certo, ma basta cambiare computer o anche solo il browser e la frittata è fatta: vai a ricordartela poi la password! Ma non finisce qua e non ci sono solo le password da tenere a memoria. Sempre più spesso, ad esempio, acquistiamo on-line il codice seriale per l'attivazione di un software che avevamo scaricato in versione trial: cosa succede se dobbiamo reinstallarlo e non troviamo più l'e-mail in cui era indicato il seriale? Anche a questo per fortuna c'è rimedio. Grazie ad altri potenti tool (tutti gratuiti) saremo in grado di recuperare informazioni sull'installazione di molti programmi. Altri strumenti specializzati, invece, ci danno la possibilità di togliere ogni protezione da documenti Word, cartelle Excel, archivi RAR e file PDF protetti da password. Questi software utilizzano il metodo del brute force, ovvero un attacco di tipo brutale che prova tutte le possibili password ad una ad una, fino a trovare quella corretta. È opportuno far notare, però, che i tool descritti nell'articolo, per la loro natura intrinseca di "scova password", potrebbero essere captati dai software antivirus come file potenzialmente dannosi e quindi bloccati. In realtà, non si corre alcuni rischio utilizzandoli e, consapevoli di ciò, prima di utilizzarli è opportuno disattivare temporaneamente la protezione in tempo reale del nostro antivirus, riattivandolo solo una volta terminata la procedura di recupero della password.

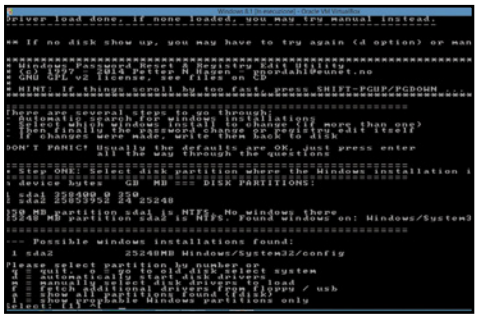
Non solo software!

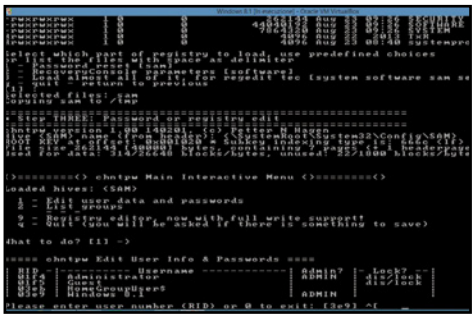
Nell'articolo analizzeremo, inoltre, i metodi utilizzati da hacker e smanettoni per recuperare le password delle reti Wi-Fi o dei router protetti dal sistema WPS. Scopriremo poi come fanno ad effettuare in-app purchase, ovvero ad acquistare oggetti aggiuntivi come le vite, l'energia o le armi nei vari giochi presenti nel Market Place di Microsoft Windows (il tutto in maniera gratuite) e a scaricare gratis giochi ed applicazioni dal Play Store di Google. Insomma, ce n'è davvero per tutti i gusti!

Password di Windows ko!

Inserendo il nostro Win DVD-Rom nell'apposito lettore ed effettuando il boot da CD, possiamo caricare il tool NTPassword che permette di disattivare la richiesta di password all'avvio del sistema operativo. Ecco come procedere.







1 Il disco di avvio è pronto!

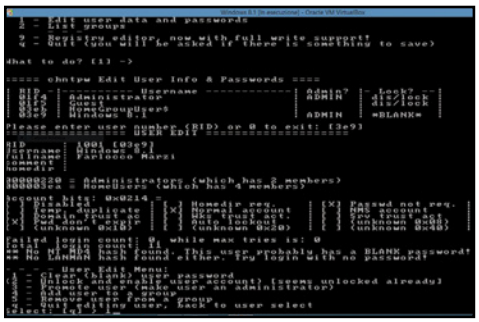
Abilitiamo il boot da CD/DVD (l'operazione varia in base al computer): all'accensione del PC premiamo *F2* o *ESC* per accedere al BIOS: spostiamoci in *Boot/Boot Device Priority* e settiamo *CD/DVD-ROM Drive* come periferica d'avvio. Inseriamo il Win DVD nel lettore e riavviamo.

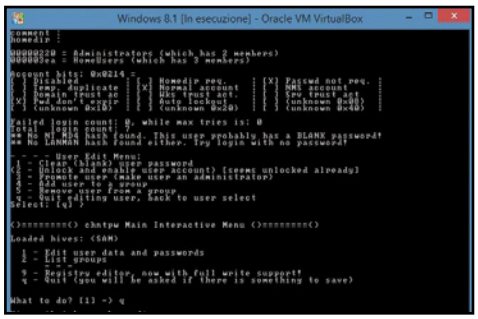
2 Facciamo la scelta giusta

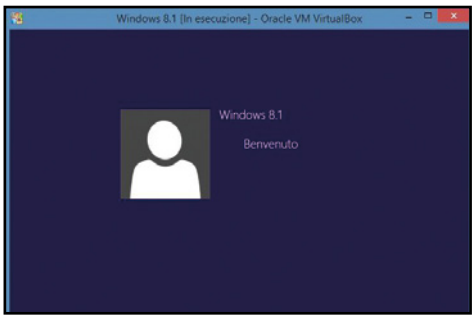
All'avvio di NTPassword premiamo *Invio* al prompt *Boot*. Il software effettua una scansione per individuare le installazioni di Windows. Selezioniamo la versione corretta del sistema operativo premendo *Invio* (in pratica selezionando *1*, che è la scelta predefinita di NTPassword).

3 Questione di utente

Scegliamo l'opzione *1* per il reset delle password e attendiamo che il software rilevi gli account utente attivi. Digitiamo di nuovo *1* per selezionare *Edit user data and password* e premiamo *Invio*. Scegliamo il nostro account digitando in *RID* corrispondente e premiamo *Invio*.







4 Cancelliamo la password

Digitiamo ancora *1* (confermando con il tasto *Invio*) per eliminare la password dell'utente in questione. Questa scelta quindi non recupererà la password di Windows, ma eliminerà l'obbligo di inserire la password quando si accende il computer, permettendoci così accesso ai file.

5 Confermiamo le modifiche

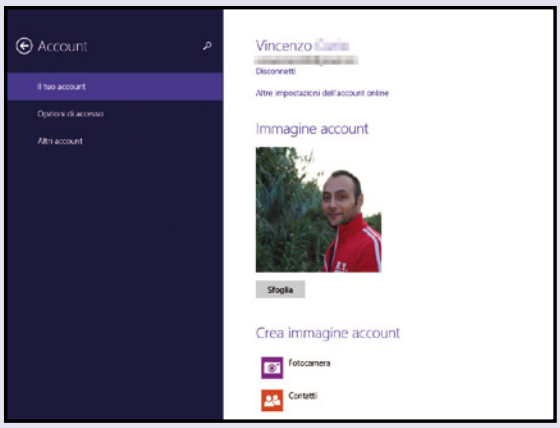
A lavoro ultimato, confermiamo le modifiche effettuate al sistema: selezioniamo la voce *q* per uscire, confermiamo con *Invio*, salviamo premendo *y* e *Invio*. Il programma ci chiederà se vogliamo ricominciare da capo: digitiamo *n* e premiamo *Invio*. Rimuoviamo il CD e riavviamo il PC.

6 L'accesso è libero!

Al nuovo avvivo saremo in grado di accedere al computer senza dover inserire alcuna password, recuperando così l'accesso completo a Windows, per poter effettuare altre operazioni come recuperare seriali di altri software come Windows e Office, o accedere alla nostra Mailbox.

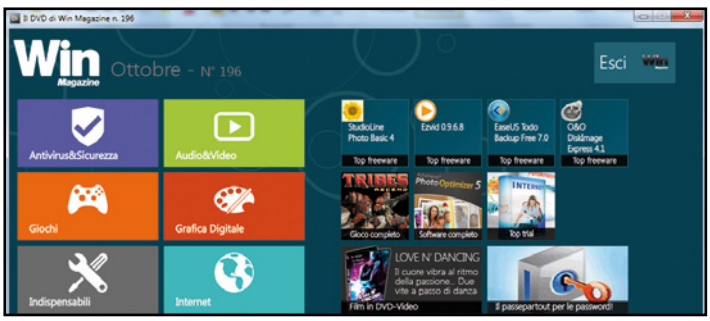
ACCOUNT ON-LINE: IL RECUPERO È IMPOSSIBILE!

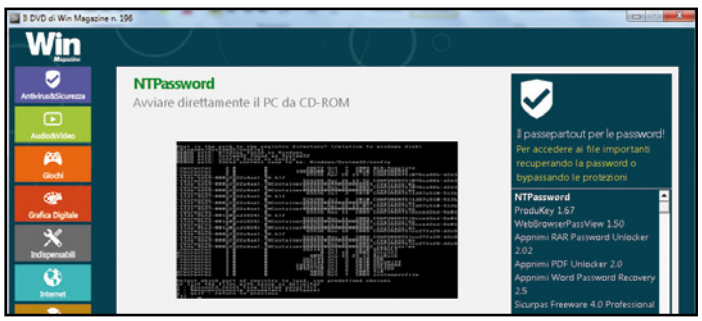
Con Windows 8 Microsoft ha introdotto una nuova tipologia di account. Denominata remota, prevede che sul PC venga utilizzato un account Microsoft on-line (un po' come succede sugli smartphone): di conseguenza, la password e le impostazioni dell'account sono salvate su un server Microsoft e non più fisicamente sul computer. Quando accediamo al PC con un account remoto, possiamo scaricare app dal Windows Store, eseguire il backup dei nostri dati usando spazio di archiviazione cloud gratuito (OneDrive) e mantenere aggiornati e sincronizzati dispositivi, foto, amici, giochi, impostazioni, musica e così via. Pertanto, nei PC in cui è attivato un account remoto al posto di uno locale, non saremo in grado di disattivare la password di accesso al sistema con i metodi appena illustrati. Per controllare se abbiamo usato un account Microsoft per l'accesso, oppure uno locale, puntiamo con il mouse sul bordo destro dello schermo, clicchiamo su ***Impostazioni*** e quindi ***Modifica impostazioni*** PC. Andiamo su ***Account/Il tuo account***. Se compaiono le parole ***Account locale***, insieme al link ***Collega a un account Microsoft***, sul PC è in esecuzione un account locale; se invece vi è l'indirizzo e-mail con tanto di immagine del profilo, allora stiamo utilizzando un account on-line Microsoft.



Codici seriali: recuperali così

Grazie allo "Scova password" di Win Magazine possiamo recuperare anche i codici seriali smarriti dei software commerciali già installati sul computer. Vediamo assieme come procedere.





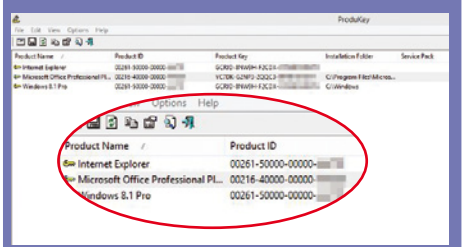
1 Tutti i tool necessari

All'interno del DVD allegato a questo speciale troveremo tutti i software necessari al recupero delle informazioni sull'installazione di software commerciali come Office o Windows, oppure utili per bypassare le password memorizzate nei browser e nei client di posta elettronica.

2 Con e senza installazione

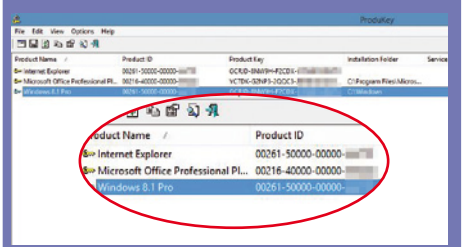
Clicchiamo sul nome del tool che ci interessa per visualizzarne la recensione, poi su *Salva/Installa* per archiviare il corrispondente archivio ZIP sull'hard disk. Scompattiamolo ed eseguiamo l'EXE contenuto all'interno per installare o avviare (qualora non richieda installazione) il software.

Il seriale di Office



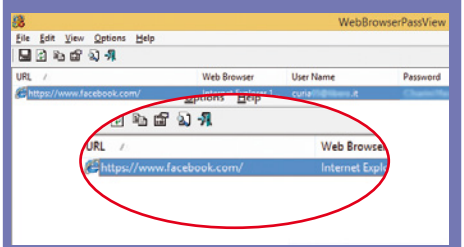
A seconda della versione di Windows installata sul nostro PC (32 o 64 bit), eseguiamo il file per il recupero del seriale di Office corretto (*productKeyOffice_32* o *productKeyOffice_64.exe*). Una volta avviato, comparirà il seriale di installazione della suite: annotiamolo per riusarlo in seguito.

Il seriale di Windows



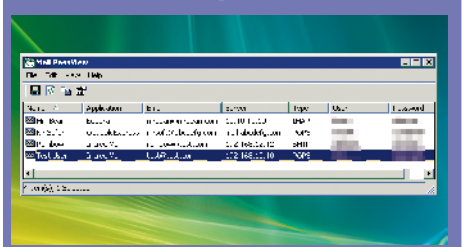
Il seriale di installazione del sistema operativo è generalmente stampato su un adesivo attaccato sul case del nostro computer, ma con il tempo può deteriorarsi e scollarsi: per recuperarlo, quindi, avviamo il file *productkey.exe* e annotiamoci in un posto sicuro il seriale mostrato in chiaro.

Password del browser



Per scovare le password salvate nel browser preferito, usiamo *WebBrowserPassView*, che ci restituirà tutte le password in un istante. Eseguiamo dunque il file EXE corrispondente con un doppio clic del mouse: dalla schermata principale recuperiamo le password che avevamo dimenticato.

Password della posta



Eseguiamo il file *mailpv.exe*: appena avviato mostrerà subito tutti gli account salvati nel client di posta elettronica, con le relative password. Funziona con tutti i maggiori software come Outlook, Mozilla Thunderbird, Yahoo! Mail, Hotmail/MSN, Windows Live e Gmail di Google.

Password file RAR/PDF

Per superare le password usate a protezione dei file RAR, ZIP e PDF installiamo *Appnimi RAR Password Recovery* oppure *Appnimi PDF Password Recovery*. Al termine, avviamo il tool che ci interessa, selezioniamo il file protetto da password e clicchiamo *Start* per visualizzarla in chiaro.

Password file Word/Excel

Per sbloccare i file DOC e XLS installiamo *Appnimi Word Password Recovery*. Avviamolo, selezioniamo con *Select* il file da sproteggere, clicchiamo *Start* e attendiamo. Se ricordiamo alcuni dettagli della nostra password come la sua lunghezza, possiamo impostarla per risparmiare tempo.

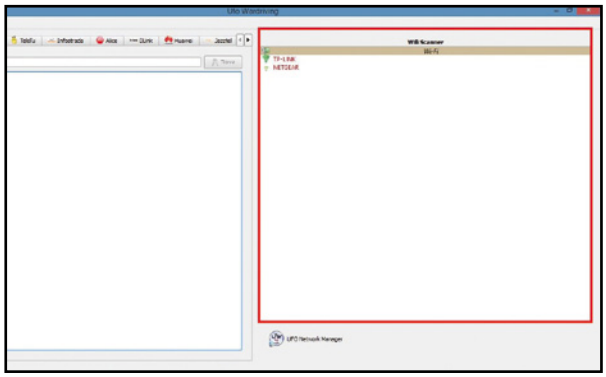
PER SAPERNE DI PIU'

IL WI-FI SI APRE CON ANDROID

Se non ricordiamo più la password del nostro router di casa, è possibile recuperarla anche grazie al nostro smartphone e all'applicazione gratuita WPA Tester, che può essere scaricata gratuitamente da www.winmagazine.it/link/2795. Installiamola tappando sull'APK appena scaricato e avviamola. Accettiamo il disclaimer e attendiamo che termini la scansione automatica delle reti. Tra tutte le Wi-Fi disponibili, cerchiamo la nostra. Se appare di colore verde, possiamo tentare di recuperare la password semplicemente tappando sul nome corrispondente. Se invece la rete è di colore rosso, non abbiamo alcuna possibilità. Se non abbiamo mai cambiato la password del router (lasciando quella di default) e il nostro router appartiene ad una marca/serie di cui si conosce l'algoritmo di generazione dei codici, l'app genererà la password e ci connetterà direttamente alla rete Wi-Fi.

Accesso consentito al Wi-Fi

Per alcuni modelli di router, la password del pannello di controllo può essere facilmente recuperata grazie al software gratuito Ufo-Wardriving. Ecco la procedura per utilizzarlo al meglio.

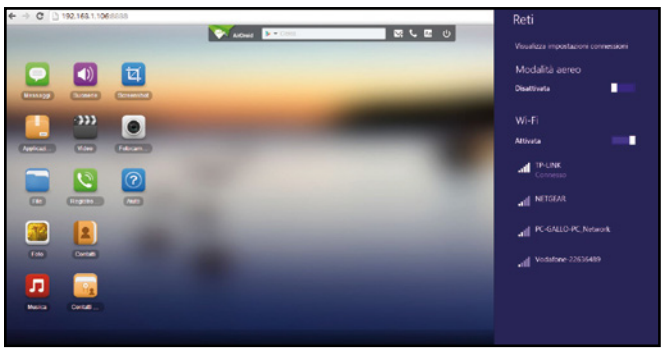


1 Il segugio delle password

Installiamo Ufo-Wardriving (lo trovi nel DVD allegato a questo speciale). Questo programma ci permetterà di recuperare la password di default di alcuni modelli di modem/router conosciuti e molto diffusi. Se la password del router è stata cambiata, però, non sarà più possibile ottenerla.

2 La scansiona è automatica

Avviamo il software e dal menu *Strumenti* in alto (oppure premiamo *Ctrl+S* sulla tastiera), selezioniamo la voce *Scanner*: in questo modo attiveremo la modalità di scansione che ci permetterà di visualizzare tutte le reti wireless nelle immediate vicinanze della nostra scheda di rete.



3 Ecco visualizzati i dati di accesso alle reti Wi-Fi

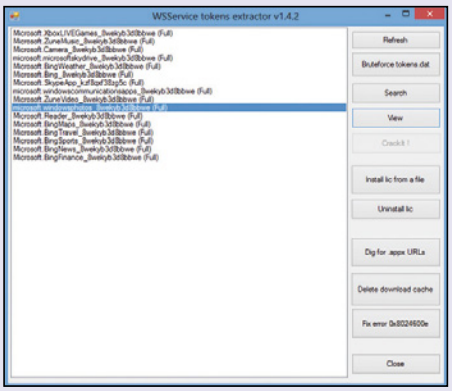
Occhio alla parte destra della schermata, nella sezione *Reti*, verranno identificate le connessioni disponibili con i seguenti colori: in rosso o arancio quelle con la password non recuperabile, in verde quelle facilmente accessibili. Ovviamente verranno generate le password di default: se è stata cambiata, non saremo più in grado di recuperarla.

NON TUTTO È COSÌ SEMPLICE COME SEMBRA

La password della nostra rete Wi-Fi viene generata in automatico da un particolare algoritmo, durante l'installazione del router da parte del gestore telefonico. È facile intuire che, se conosciamo tale algoritmo, saremo in grado anche noi di generare la password. Tale algoritmo però, varia in base al modello, alla marca del router e al nome della rete (SSID): per questo motivo, è stato svelato e reso noto solo per alcune serie di router. Per i restanti modelli, o quelli in cui la password è stata cambiata dall'utente, è necessario l'utilizzo della tecnica cosiddetta di attacco brute force. Tale tecnica utilizza dei file di testo, detti dizionari, che contengono tutte le password possibili, provandole ad una ad una, fino a trovare la parola chiave corretta. Il brute force, presenta però almeno due grossi problemi: il primo è derivante dal fatto che la password può essere ricavata se e solo se è presente in questo set di chiavi (dizionario) che, pertanto, deve ospitare migliaia di combinazioni possibili, raggiungendo spesso dimensioni spropositate. Il dizionario delle possibili password dei router Alice/Telecom, ad esempio, hanno una dimensione di circa 3 TB: per aprire un file di testo di queste dimensioni avremo bisogno di un hardware certamente superiore ad un normale PC. Il secondo problema derivante dall'utilizzo dei dizionari deriva dal tempo in cui gli attuali computer sono in grado di scovare la password corretta. Sempre prendendo come esempio una rete Alice (di una serie non nota) e supponendo di avere a disposizione una macchina con hardware di ultima generazione, il tempo necessario per ottenere la password può variare da pochi secondi (nel caso in cui la password sia tra le prime parole del file) fino a 150 anni (se la password corretta è tra le ultime del file dizionario)!

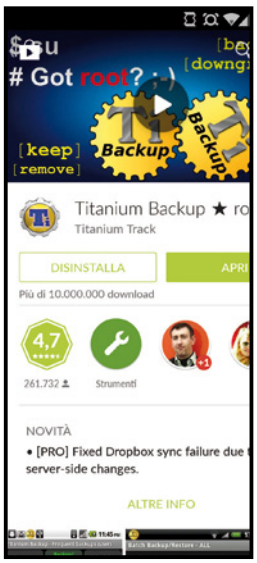
COSÌ GLI HACKER SUPERANO LE PROTEZIONI DEL WINDOWS STORE

Con la versione 8 di Windows, Microsoft ha introdotto molte novità tra cui uno Store on-line che ci permette di scaricare e installare, direttamente sul computer, giochi e applicazioni, proprio come accade sugli smartphone. Ovviamente gli hacker non sono rimasti a guardare e hanno scovato un metodo per scaricare gratis le app a pagamento. In pratica, sfruttano il software Windows Store Service Crack (WSService Tokens Extractor) che, utilizzando un algoritmo di brute force, permette loro di validare l'acquisto fittizio di un'applicazione. Il funzionamento è abbastanza semplice: quando si acquista un'applicazione all'interno dello store viene generato un "token", ovvero un codice univoco che attesta l'avvenuta transazione e che quindi delibera il download dell'app in versione complete. Per ottenere in maniera "illecita" il token, l'hacker scarica la versione di prova dell'applicazione da "acquistare", quindi, avvia il software WSService, che tramite attacco brute force estrae la chiave d'acquisto e l'app passerà da versione di prova a versione completa. A quanto pare Microsoft ha scoperto la falla ed è subito corsa ai ripari: infatti il software WSService Tokens Extractor non funziona con la più aggiornata versione di Windows, la 8.1. Ma intanto sul sito ufficiale di Tokens Extractor è comparso un annuncio in cui i pirati sostengono che entro il 2015 rilasceranno la nuova versione del loro software.



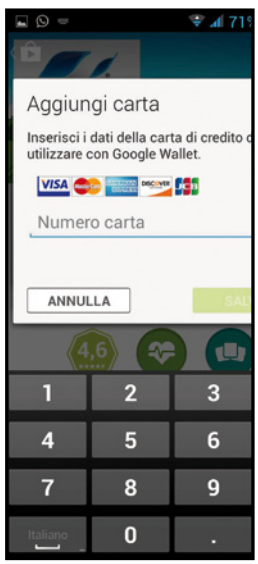
Crack dei giochi Android

Utilizzando un semplice escamotage, i pirati riescono ad utilizzare gratuitamente e senza alcun limite le app altrimenti scaricabili a pagamento dal Google Play Store. Ecco in che modo.



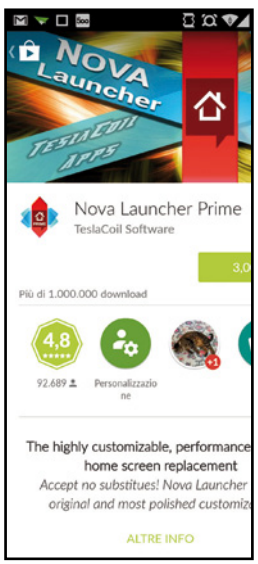
1 Il tool per il backup

Innanzitutto, i pirati installano l'app Titanium Backup in versione gratuita: la utilizzeranno per effettuare i backup delle app scaricate. Verificano, inoltre, che sullo smartphone siano attivi i permessi di root, in modo da potere effettuare anche il backup delle impostazioni di sistema.



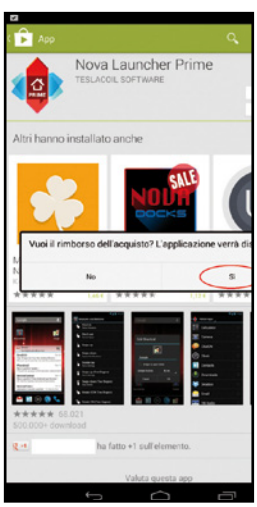
2 Serve la carta di credito

I pirati associano quindi una carta di credito al Play Store di Google e simulano l'acquisto di un'app a pagamento per accedere al pannello di configurazione del Google Wallet. Quindi seguono le istruzioni a video e inseriscono i dati della carta di credito e del legittimo proprietario.



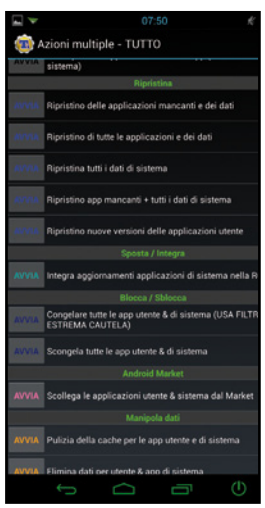
3 Shopping sfrenato

A questo punto, i pirati possono acquistare l'applicazione che gli interessa senza preoccuparsi della spesa sostenuta: sanno, infatti, che hanno 15 minuti di tempo per completare la procedura, effettuare il backup dell'app stessa e, successivamente, richiedere il rimborso per… acquisto errato!



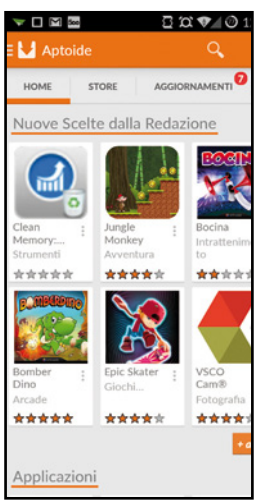
4 I soldi tornano indietro

Avviano quindi Titanium Backup ed effettuano il backup dell'applicazione appena installata, in modo da averne una copia "completa". Tornano quindi sul Play Store e dalla pagina dell'app cliccano *Rimborso*, seguendo i passi della procedura guidata mostrata a video.



5 Un'app da ripristinare

Ottenuto il rimborso, il pirata ripristina il backup dell'applicazione che, non essendo più "di suo gradimento", era stata disinstallata. Per ripristinare il backup contenente l'applicazione, avviano Titanium Backup e, dalla voce *Ripristina*, selezionano il backup creato in precedenza.



6 Meglio gli store unofficial

In alternativa, i pirati installano un market alternativo, che permettono di scaricare le app a pagamento in maniera gratuita, semplicemente cercandole e installandole. Il più diffuso è Aptoide, un multistore che effettua la ricerca in più market fino a recuperare l'app desiderata.

La chiavetta aspira password

Ecco il tool che trasforma qualsiasi pendrive in un passpartout: basta collegarla a un PC per avere le chiavi d'accesso in chiaro

Cosa ci occorre

20 MIN. DIFFICILE

TOOL RECUPERO PASSWORD
WMPASSWORD HOOVER
SOFTWARE COMPLETO
Lo trovi su: ☑DVD
Sito Internet: www.winmagazine.it

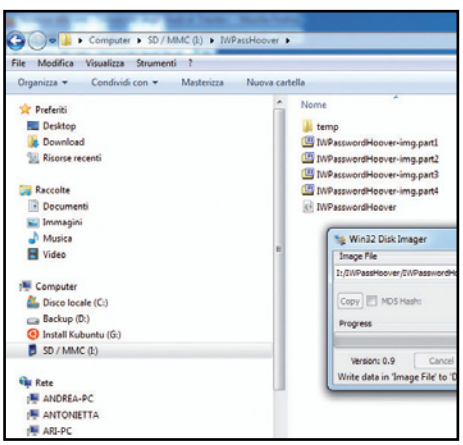
Password, dati di accesso, PIN... ogni giorno dobbiamo mettere in moto il cervello decine di volte per ricordare un qualche codice di sicurezza. Ognuno ha la sua strategia: c'è chi usa sempre lo stesso account e la stessa password (un invito a nozze per qualsiasi malintenzionato) o chi, più furbescamente, diversifica le utenze con dati differenti. La soluzione più usata è sicuramente quella di salvarle sul PC per non scervellarsi ogni volta. Quando ci logghiamo a un sito Web, ad esempio, il browser ci chiede se può memorizzare la password per liberarci dall'obbligo di inserirla anche le volte successive. Così facendo superiamo l'ostacolo della memoria, ma di fatto ci esponiamo a ulteriori rischi: basta infatti un tool ad hoc per aspirarle tutte!

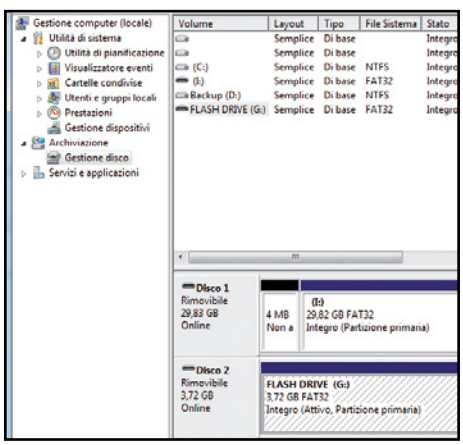
Password in chiaro

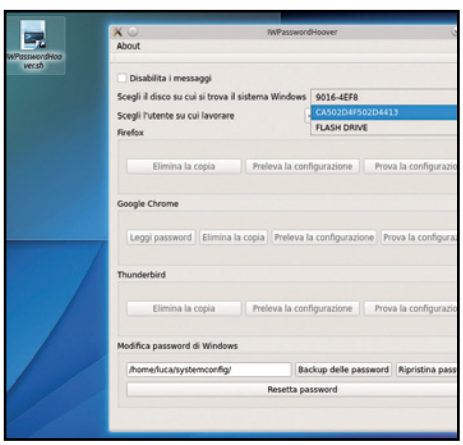
Per dimostralo abbiamo realizzato un programma che fa esattamente questo: lo abbiamo chiamato WMPasswordHoover, "l'aspira password". Seguendo i passi del tutorial otterremo una chiavetta USB avviabile che permette di prelevare facilmente le password memorizzate in un computer. Vediamo in che modo. Prima di procedere, però, è bene ricordare che rubare password altrui è illegale! Le procedure mostrate di seguito servono esclusivamente a scopo illustrativo. Se decidiamo di seguire il tutorial, facciamolo solo ed esclusivamente sui nostri PC o al massimo per aiutare un amico in difficoltà!

A Prepariamo la pendrive

La nostra applicazione è pronta all'uso: basta semplicemente copiare i file di configurazione di WMPasswordHoover e "flashare" una chiavetta da 4 GB per renderla avviabile. Ecco come procedere.







1 Prepariamo l'occorrente

Scompattiamo il file *IWPasswordHoover.zip* (lo trovi nel DVD allegato a questo speciale) e carichiamo su una chiavetta USB vuota il contenuto del file *.img* ricorrendo a Win32 Disk Imager: è sufficiente indicare il percorso del file, la lettera della chiavetta e premere Write.

2 Partizioniamo la pendrive

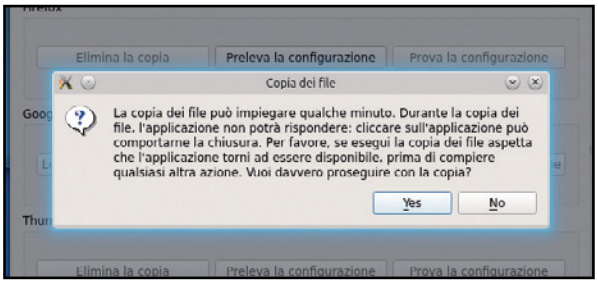
Il tool è progettato per chiavette da 4 GB. Se abbiamo usato una pendrive più capiente, verrà vista come una da 4 GB. Andiamo in *Pannello di controllo/Strumenti di amministrazione/Gestione Computer/Gestione disco* ed espandiamo la partizione esistente sulla chiavetta.

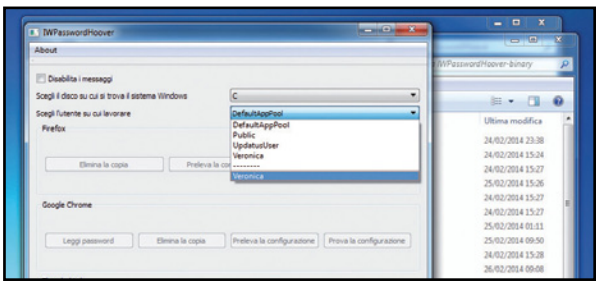
3 Il boot da chiavetta

Colleghiamo la pendrive al PC e avviamolo da USB: potrebbe essere necessario abilitare tale funzione nel BIOS (*Canc*, *F2* o *F12*). Alla schermata di avvio della chiavetta scegliamo *Prova Kubuntu* e attendiamo il caricamento. Quindi avviamo WMPassvordHoover presente sul *Desktop*.

B Accendiamo l'aspiratutto!

Password, cronologia e preferiti: bastano pochi clic per copiare tutto sulla pendrive USB appena realizzata. Ecco come usare la versione "bootable" di Win Magazine Password Hoover.



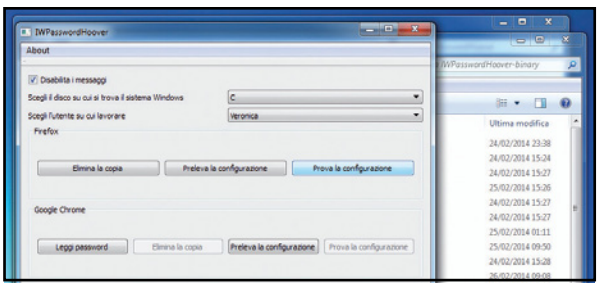


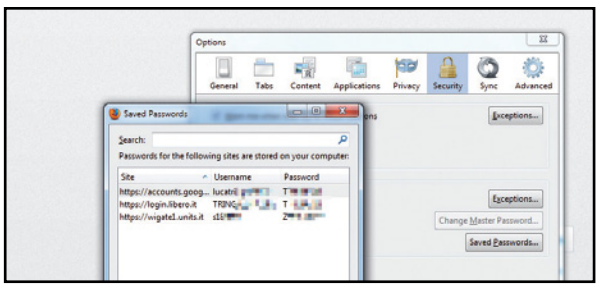
1 Prepariamo la copia

L'applicazione ha bisogno di sapere su quale disco si trova il sistema operativo: scegliamolo dal menu a discesa e indichiamo pure il nome dell'utente su cui lavorare. Per copiare la configurazione di Firefox (Thunderbird o Chrome) premiamo il pulsante *Preleva la configurazione*.

2 Cambiamo computer

La copia dei file può durare diversi minuti. Al termine, chiudiamo tutto e spegniamo il PC. Inseriamo la chiavetta USB su un altro computer Windows (con Windows già caricato): avviamo *WMPasswordHoover.exe* e selezioniamo il nome utente da cui abbiamo prelevato le configurazioni.





3 Dimmi che utente sei

Il programma ci dice cosa possiamo fare (le funzioni attive sono quelle cliccabili): per leggere i dati personali precedentemente copiati clicchiamo *Prova la configurazione*. Prima, però, spuntiamo *Disabilita i messaggi* così non apparirà più il messaggio informativo sulla copia dei file.

4 È un clone perfetto

I file verranno copiati in un'altra locazione della chiavetta. Al termine, verrà avviata una versione portable di Firefox (o di Thunderbird) con precaricati i dati di configurazione dell'altro computer. Possiamo scorrere i preferiti, la cronologia e addirittura vedere le password in chiaro.

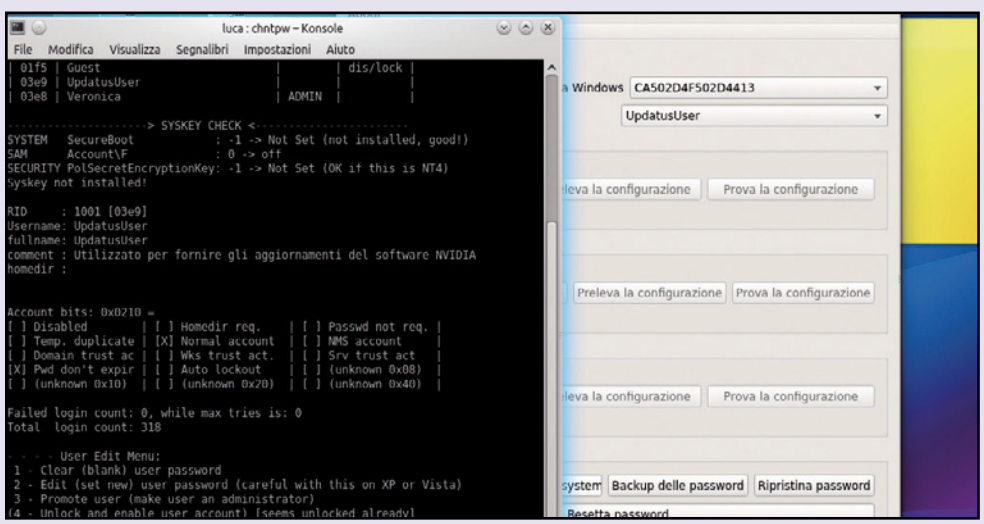
PER SAPERNE DI PIU'

BYPASSARE LA CHIAVE DEL BIOS

Se non ricordiamo più la password di accesso al BIOS, armiamoci di cacciavite, apriamo il case del computer e rimuoviamo per qualche minuto la batteria tampone della scheda madre. In questo modo resetteremo le preferenze impostate, password comprese. Un altro metodo consiste nello spostare l'apposito jumper di solito identificato dalla scritta *CLR_CMOS* (Clear Cmos) presente sempre sulla scheda madre.

CAMBIARE E CANCELLARE LA PASSWORD DI WINDOWS

Con WMPasswordHoover è possibile resettare persino la password del sistema operativo e crearne una nuova! Dopo avere avviato il computer dalla chiavetta USB e poi WMPasswordHoover dal Desktop di Kubuntu, possiamo eseguire un backup delle password esistenti, in modo da poterle ripristinare. Per farlo dobbiamo selezionare il disco e l'utente su cui lavorare e cliccare ***Backup delle password***. La copia dei file non dovrebbe durare molto. Eseguito il backup, clicchiamo ***Resetta password***. Nella finestra che appare scegliamo 1 per cancellare la password (o 2 per cambiarla) e premiamo ***Invio***. Per confermare, rispondiamo con ***Y*** e premiamo ***Invio***.



Password del Web a portata di clic!

Il motore di ricerca che, in mani sbagliate, porterebbe il caos nel Mondo... Ecco come funziona e come difendersi

Cosa ci occorre 15 MIN. FACILE

MOTORE DI RICERCA
SHODAN
Quanto costa: Gratuito
Sito Internet: www.shodanhq.com

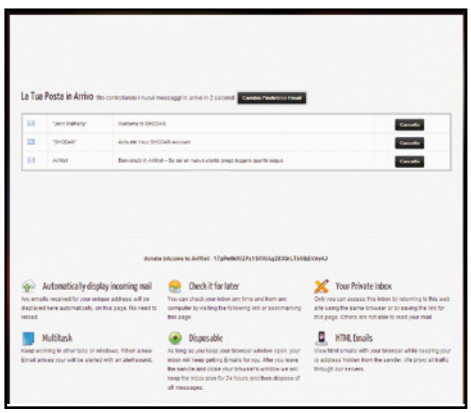
Su Internet, ormai, si trova davvero di tutto! Quello che sembrava essere un abusato luogo comune è ora diventato realtà: un nuovo e sconcertante servizio sta infatti facendo parlare di sé in Rete. Questa volta non si tratta dell'ennesimo social network, ma di un rivoluzionario search engine da molti ribattezzato come "il Google dei pirati". Di che stiamo parlando? Di Shodan, il motore di ricerca più pericoloso del mondo, raggiungibile da tutti all'indirizzo www.shodanhq.com. Perché è così sconvolgente? Perché consente di violare facilmente qualsiasi dispositivo connesso a Internet, dalle telecamere di sicurezza ai sistemi industriali più avanzati.

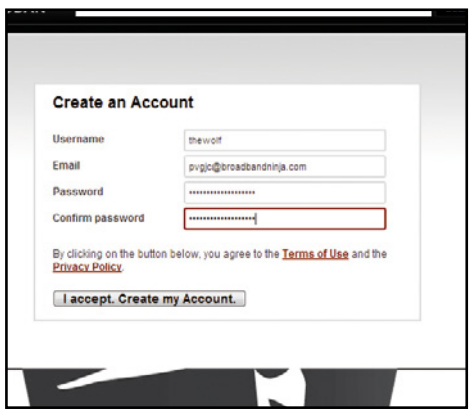
Ricerche mirate

I normali motori di ricerca come Google o Bing indicizzano i siti Web così da consentirne l'individuazione mediante parole chiave; Shodan fa un lavoro simile, ma sui cosiddetti "banner". Tutti i server e i dispositivi di Rete, quando vengono interrogati da un client su un'apposita porta, rispondono con una serie di informazioni testuali, che comprendono lo stato del servizio, un eventuale messaggio di benvenuto, dati sul tipo di autenticazione e sui protocolli di comunicazione utilizzati. Questi messaggi sono i "banner". Shodan effettua periodicamente una scansione dell'intera Rete, individua i dispositivi connessi e ne archivia i banner. Quando l'utente utilizza Shodan di fatto esegue una ricerca sui contenuti dei banner. Con questo incredibile search engine è

Così i pirati prendono il controllo

Le stampanti di rete, specialmente nei contesti aziendali, possono finire nel mirino di Shodan. Se non adeguatamente protette, che danni può provocare un hacker malintenzionato? Scoprilo con noi!





1 Protetto dall'anonimato

L'hacker scarica l'archivio *TorBrowser.zip* dal Web, lo scompatta ed esegue il file *Start Tor Browser.exe*: il browser anonimo non richiede installazione. All'avvio vengono aperti un pannello di controllo e un'istanza di un browser basato su Firefox, ma opportunamente modificato.

2 Un'e-mail temporanea

Per registrarsi a Shodan e sfruttarne le potenzialità, l'hacker deve fornire principalmente un indirizzo e-mail valido. Invece di utilizzare il proprio, ne crea uno temporaneo su http://getairmail.com. Anche in questo caso, per non lasciare tracce accede alla posta temporanea utilizzando Tor.

3 Una veloce registrazione

Per effettuare la registrazione a Shodan l'hacker si collega con TorBrowser a www.shodanhq.com e clicca *Register*. Inserisce una login, l'indirizzo e-mail (temporaneo) e una password. Letti i *Terms of use* e la *Privacy Policy*, preme *I accept. Create my Account*. Adesso è tutto pronto!

PROTEGGERSI DA SHODAN IN 5 MOSSE

1 Evitiamo di esporre su Internet le nostre periferiche senza prima sostituire la password predefinita con una parola chiave lunga che contenga anche numeri e segni speciali. Facciamolo per le stampanti di rete, le IP-Cam, i router, gli access point, i range extender e per qualsiasi altro dispositivo apparentemente innocuo connesso alla Rete. Chi andrebbe a dormire con la porta di casa senza serratura? E non usiamo la stessa parola per tutte le periferiche: violata una, si avrebbe libero accesso anche alle altre.

2 Cambiamo periodicamente le password di accesso a tutti i nostri dispositivi: in questo modo, anche se qualcuno riuscisse a violare i nostri sistemi, prima o poi si ritroverebbe comunque tagliato fuori.

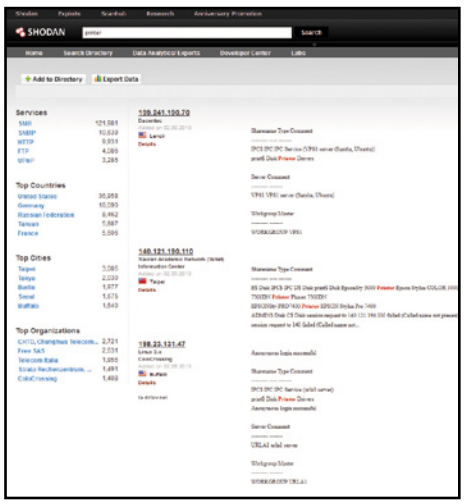
3 Se abbiamo bisogno di accedere dall'esterno ai nostri sistemi, invece che esporli pericolosamente sulla rete, utilizziamo una Virtual Private Network ricorrendo ad esempio al software OpenVPN (lo trovi nel DVD allegato a questo speciale).

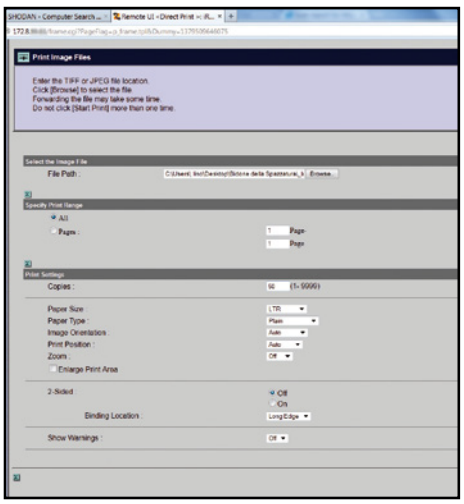
4 Se abbiamo un nostro server FTP, evitiamo di renderlo accessibile con l'utente anonymous.

5 Tentiamo noi stessi di violare i nostri sistemi usando Shodan! Essere in grado di scoprire da sé le proprie carenze è la protezione migliore!

possibile cercare con estrema facilità server FTP, video server, router, stampanti, Web server... insomma, tutto quanto è connesso in Rete ed è dotato di un indirizzo IP. Per sfruttare appieno le potenzialità di Shodan è necessaria la registrazione, che è gratuita se ci si accontenta dei primi 50 risultati di ricerca (più che sufficienti per chi non è un hacker di professione). Altrimenti, con una piccola quota di adesione è possibile sbloccare tali limiti. Secondo l'ideatore di Shodan, John Matherly (https://twitter.com/achillean), queste scelte consentono di limitare significativamente i potenziali rischi di sicurezza: con "soli" 50 risultati è difficile attuare attacchi massivi alla Rete. E chi, invece, effettua il pagamento, non potrà lanciarsi in attività particolarmente pericolose, in quanto si rende identificabile tramite i dati della carta di credito.

delle stampanti





4 Iniziano le ricerche
L'hacker digita printer o inserisce il modello di una stampante e preme *Search*. Cliccando su uno dei link visualizzati accede alla pagina di autenticazione del pannello di controllo della stampante associata a quell'IP e tenta la connessione con login e password predefinite (admin e admin).

5 Accesso effettuato!
Se l'hacker è fortunato (il proprietario della stampate ha lasciato login e password di fabbrica) riesce ad accedere al pannello di controllo della periferica. Cliccando *Direct Print* (se presente) può eseguire l'upload di un'immagine dal proprio computer e stamparla in un'infinità di copie!

Cosa c'è di vero?

Ma Shodan è davvero così pericoloso? Un hacker ci ha mostrato il suo funzionamento! Da quanto abbiamo avuto modo di vedere, i rischi sono concreti, ma solo per chi non protegge bene i propri sistemi collegati in Rete. Se non cambiamo la password del nostro dispositivo e lasciamo quella predefinita (di fabbrica), allora potremo essere vittime di Shodan. Se invece seguiamo alcuni semplici accorgimenti, chiunque dovesse individuare il nostro dispositivo tramite Shodan non potrà che restare inerme a guardare la pagina di accesso. Gli algoritmi di forza bruta per l'individuazione delle password, le cui potenzialità sono spesso decantate dai loro sviluppatori, non sono particolarmente rischiosi se siamo abituati a utilizzare stringhe lunghe e poco intuibili per proteggere l'accesso ai nostri sistemi: senza nessun indizio sul tipo di parola chiave utilizzata, un programma del genere potrebbe impiegare decenni prima di arrivare al suo obiettivo.

Shodan e la legalità

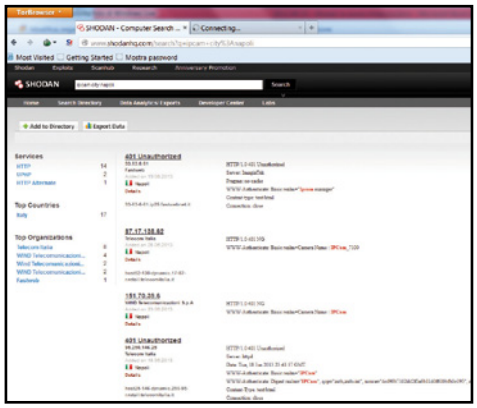
Quel che bisogna chiedersi è se l'utilizzo di Shodan sia legale o meno. Cercando un dispositivo collegato alla Rete non si commette alcun reato. Diverso è il caso in cui si cerca di forzare una password, anche quella predefinita, o di creare danni. Quando operiamo in Rete, la nostra identità reale è facilmente individuabile a partire dall'indirizzo IP, assegnato dall'Internet Service Provider (ISP) al momento della connessione, e anche tramite il MAC Address, che è un indirizzo univoco attribuito dal produttore alla scheda di rete e a qualsiasi dispositivo che può connettersi a Internet. Pertanto, se vogliamo curiosare è importante non andare oltre i limiti del consentito.

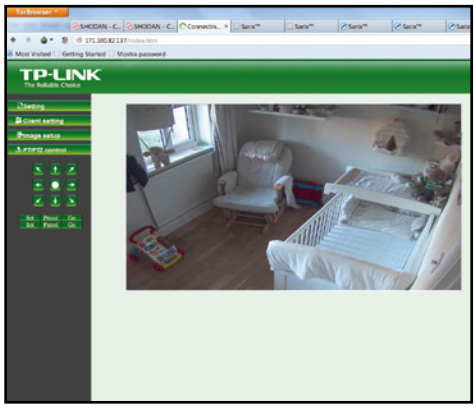
ATTENTI AI WI-FI EXTENDER!

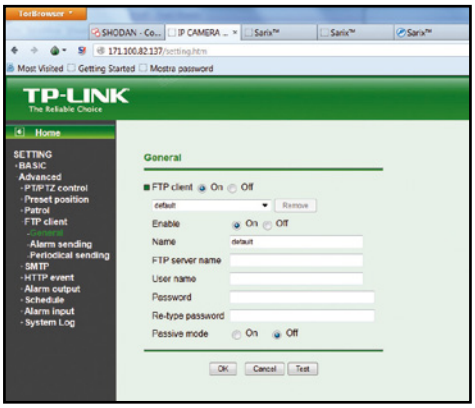
Alcuni dispositivi di rete sono più a rischio di altri perché non ci si preoccupa della loro sicurezza. I Range Extender, ad esempio, utilizzati per ampliare la copertura di segnale di un router Wi-Fi in un appartamento grande o su più livelli, sono utilizzati quasi sempre con la password predefinita. Un esempio tipico è dato dagli RE1000 della Linksys/Cisco. Digitando RE1000 nella casella di ricerca di Shodan, l'hacker ci ha mostrato come la maggior parte dei dispositivi sia accessibile lasciando la login vuota e inserendo admin come password. Avuto accesso al pannello di controllo, l'hacker potrebbe creare danni disattivando il dispositivo o modificando le impostazioni e la password. Addirittura si potrebbe eseguire un aggiornamento usando un firmware modificato ad hoc.

Ci spiano dalla Webcam

Le IPCam usate per sorvegliare gli ambienti domestici (e non solo) possono essere una finestra spalancata sulla vita privata di tutti quanti noi. Così, in pochi secondi, la nostra privacy va in malora!







1 Hacker a caccia di IPCam

L'hacker si connette a Shodan usando Tor Browser per non essere rintracciato. Eseguito il login effettua una ricerca filtrandola per area geografica e inserendo una parola chiave adeguata, tipo *ip-cam*, *webcam* ecc. (la ricerca mostrataci dall'hacker è *ip-cam city:napoli*). Esamina quindi i risultati cercando una cam non protetta da password o con password predefinita.

2 Così spia di tutto e di più

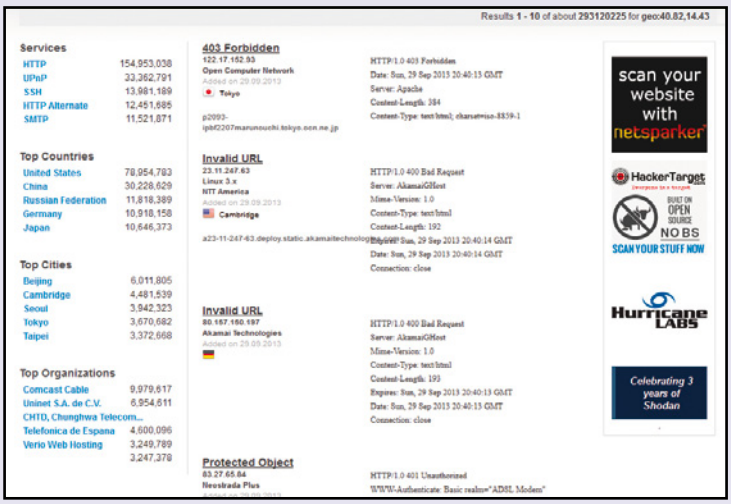
L'IP Cam incustodita è ora sotto il controllo dell'hacker. Se il dispositivo è motorizzato, l'hacker usa i pulsanti direzionali per orientarlo e puntare l'obiettivo in altri punti della stanza, con buona pace della privacy. Alcuni sistemi, inoltre, gestiscono più Webcam contemporaneamente: tramite il pannello di controllo l'hacker potrà passare da un canale all'altro.

3 Immagini dirottate

Le IPCam usate come sistema di sicurezza prevedono il trasferimento delle riprese (a intervalli regolari o al rilevamento di un movimento) su server remoti, di solito con protocollo FTP. Accedendo all'apposita sezione del pannello di controllo l'hacker può modificare queste impostazioni disabilitando la funzione o cambiandone i parametri per puntare a un proprio server.

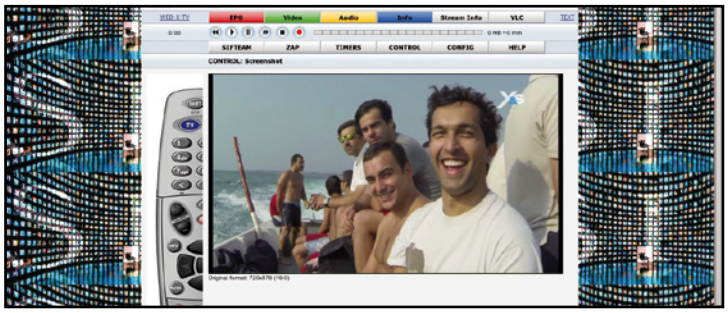
PERCHÉ VIOLARE UN ROUTER CON SHODAN?

Usare Shodan per accedere a un router può servire a un hacker non solo per fare danni, ma anche per trarne un vantaggio pratico. Shodan può effettuare ricerche geografiche: questo significa che è in grado di filtrare i risultati rispetto a una data città o ad esatte coordinate geografiche. Se si esegue una ricerca aggiungendo il filtro geo seguito da latitudine e longitudine (ad esempio geo:40.82,14.43), Shodan elencherà gli IP che soddisfano la stringa di ricerca e che sono nelle vicinanze delle coordinate fornite. In questo modo un hacker potrebbe identificare un router preciso e accedervi per rendere la connessione Wi-Fi non protetta (disattivando la chiave di sicurezza), così da poterla utilizzare liberamente.



Decoder sotto attacco!

Il Dreambox è un decoder che gli smanettoni modificano per fare card sharing degli abbonamenti alle Pay TV e guardare a scrocco i canali SAT. Ma integra anche un server Web che potrebbe essere indicizzato da Shodan...

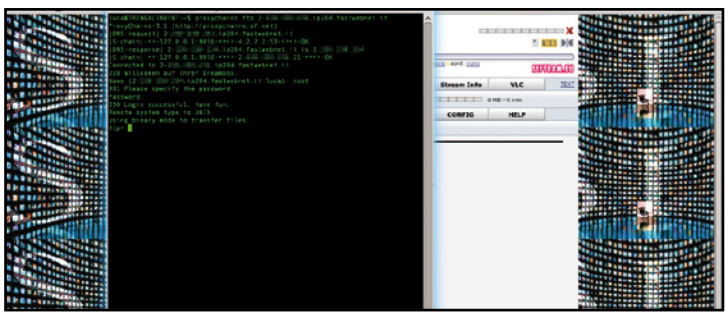


1 Direttamente dal browser

Quando il pirata trova su Shodanhq un dispositivo Dreambox, prova ad entrare visitando direttamente il suo indirizzo IP con il browser. Inserendo le credenziali di default (root e dreambox) dovrebbe poter accedere all'interfaccia (se la password della Web interface non è stata modificata): il pulsante *CONTROL* fa apparire un menu per gestire il dispositivo.

2 Come col telecomando

Nel menu di controllo, i pulsanti più interessanti sono due: *Screenshot* e *Remote Control*. Il primo serve a mostrare un'istantanea di ciò che appare al momento sullo schermo del televisore collegato al Dreambox. L'altro fa apparire un telecomando molto realistico e comodo. Se il Dreambox è in standby, il pirata lo attiva col pulsante Wakeup.

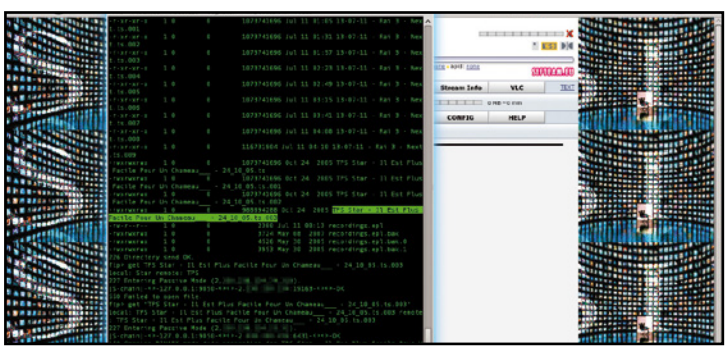


3 Lo zapping è virtuale

La sezione ZAP permette al criminale di scorrere l'elenco dei canali (facendo zapping). Cliccando sul nome di un canale qualsiasi, questo viene selezionato ed è possibile vederlo in tempo reale cliccando sul link WEB-X-TV (necessita di una vecchia versione di VLC player). Il pirata può anche registrare la trasmissione, usando l'apposito pulsante.

4 Accesso diretto ai file

Registrato il programma che gli interessa, il criminale cerca di trasferirlo sul proprio computer. Per questo apre una finestra del terminale di Windows (il Prompt dei comandi) e dà il comando *ftp* seguito dall'indirizzo IP del Dreambox vittima. Inserendo le credenziali di accesso (le stesse della Web Interface) ha ormai il completo controllo sulla vittima.



5 Ecco dove sono i film

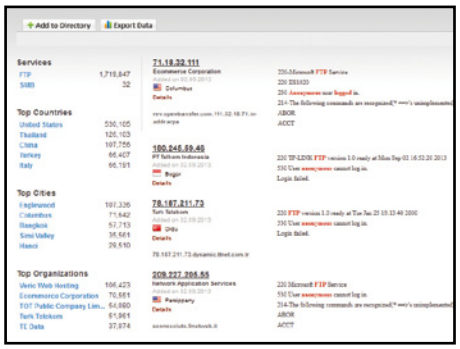
Per prima cosa il pirata dà il comando passive e poi dir per avere una lista di file e cartelle. Poi scrive *cd /media/hdd* per entrare nell'hard disk del Dreambox. Il comando dir elenca tutte le cartelle: con i comandi *cd movie* e *dir* ottiene l'elenco dei film registrati. Il pirata sceglie uno dei video presenti, per esempio "*TPS Star*".

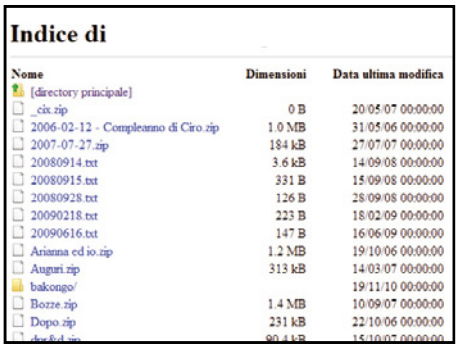
6 Senza destare sospetti

Il pirata può spedirsi il video col comando *get "TPS Star"*. Trattandosi di FTP, può addirittura interrompere l'invio e riprenderlo il giorno seguente per non destare sospetti. Per evitare che il proprietario si accorga che il Dreambox è stato acceso, infatti, il criminale lo mette in standby dall'interfaccia Web, usandolo per poco tempo al giorno.

Server FTP pieni di MP3

I pirati informatici usano molto spesso il File Transfer Protocol per scambiare file illegali sul Web in gran segreto. Un eventuale malintenzionato riesce a scovare questi FTP con Shodan e... scarica tutto!





1 L'FTP è anonimo

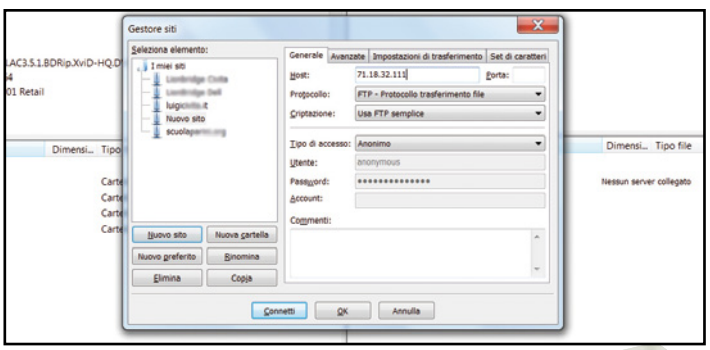
L'hacker si collega a Shodan usando Tor-Browser e dà il via alle sue ricerche. Poiché vuole individuare un server FTP con accesso anonimo, digita nella casella di ricerca la stringa *FTP anonymous*. Tra i risultati della ricerca presta attenzione a quelli che riportano la dicitura *Anonymous user logged in*. Gli altri vengono scartati perché non consentono l'accesso anonimo.

2 Accesso diretto dal browser

Individuato l'indirizzo IP del server FTP con accesso anonimo, *71.18.32.xxx* nell'esempio mostratoci dall'hacker, cerca di accedere ai file in esso archiviati. Apre il browser e *digita ftp://71.18.32.xxx*. Effettuata la connessione, sul PC dell'hacker viene visualizzata una struttura a cartelle. Se il server non consentisse l'accesso anonimo, verrebbero richieste login e password.

3 Serve anche un client FTP

L'hacker si procura un client che gli renda più semplici le operazioni su file e cartelle. Scarica FileZilla da https://filezilla-project.org. Fa doppio clic su *Download Filezilla Client* e poi su *Download Now*. Fa clic due volte sul file *SFInstaller_SFFZ_filezilla_8992693_.exe* e segue la procedura guidata.



4 File in trasferimento

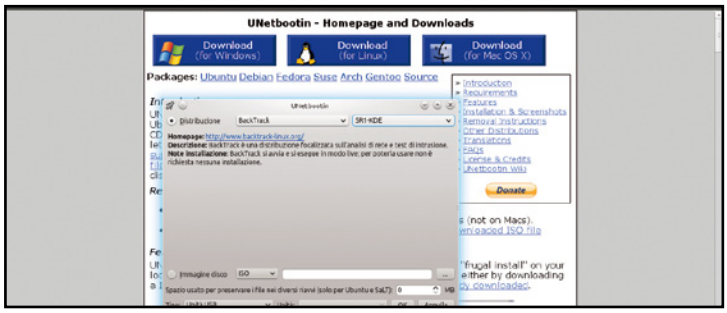
L'hacker avvia FileZilla e fa clic su *File/Gestore siti*. Preme *Nuovo sito*, inserisce come host l'indirizzo IP del server FTP e come tipo di accesso sceglie la voce *Anonimo*. Fa clic su *Connetti* e attende qualche secondo. FileZilla si è connesso al server e l'hacker inizia ad esplorare agevolmente file e cartelle: quando trova qualcosa di suo interesse lo trascina sul Desktop del suo PC.

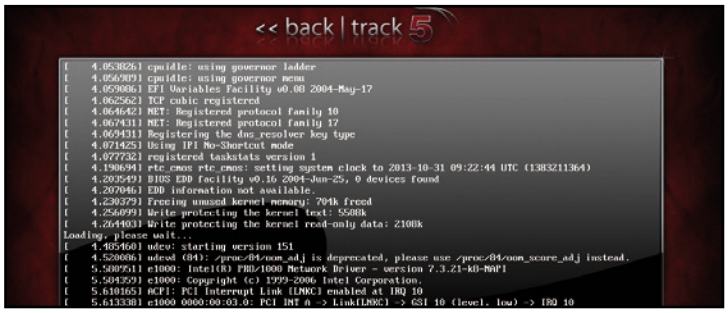
L'APP CHE PORTA IL CAOS NEL MONDO

Unendo la logica di Shodan ai Google Hacks abbiamo realizzato un'applicazione Web che permette di cercare di tutto e di più da PC, smartphone e tablet. Non devi fare altro che collegarti alla pagina www.winmagazine.it/link/2359 e cliccare o tappare sulla ricerca desiderata... Troverai cose davvero pazzesche!

La forza bruta del pirata

Entrare in un sistema di cui si conosce la password è estremamente facile. ma anche se la chiave d'accesso è stata cambiata, i veri pirati ci riescono lo stesso e con la tecnica del "brute force" controllano a distanza anche i nostri PC.



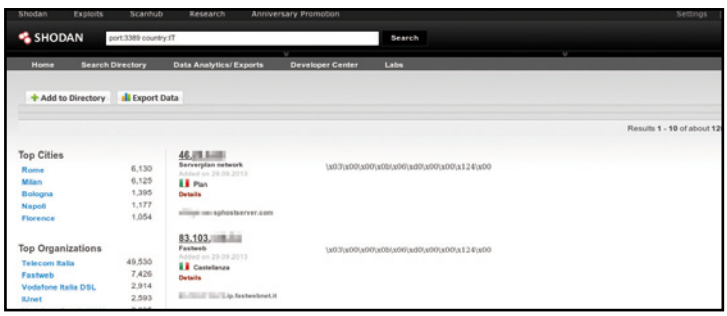


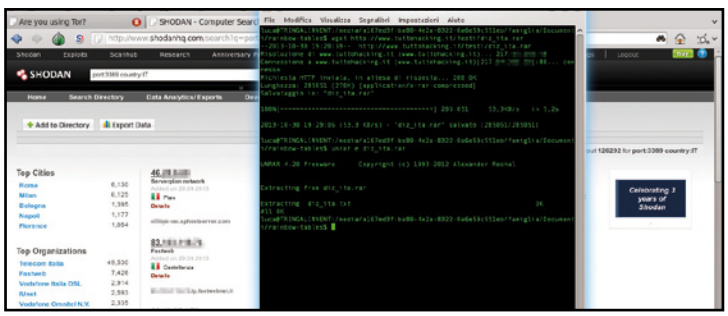
1 Con Linux è più semplice

La prima cosa che il pirata fa è scaricare l'applicazione open source UNetBootIN dal sito http://unetbootin.sourceforge.net. Con questo programma può creare una pendrive avviabile scegliendo, dal menu, la distribuzione BackTrack 5R1 con KDE. Avviando il computer da pendrive si presenta, al pirata, una schermata in cui sceglie la versione *BackTrack Text*.

2 Dentro la rete Tor

Appena appare il prompt dei comandi, scrive *startx* e preme *Invio* per accedere all'ambiente grafico. Il pirata apre il menu *K*, voce *System*, avvia la Konsole e digita il comando *wget http://tinyurl.com/vidalia-linux && tar xvf vidalia-linux && chown -R root*; con *sudo nano /etc/proxychains.conf* aggiunge la riga *socks4 127.0.0.1 9050*.



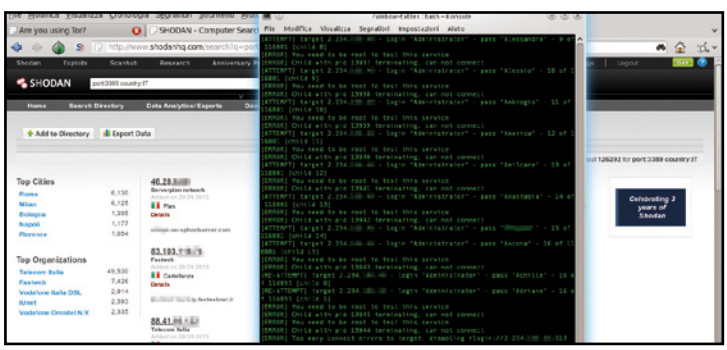


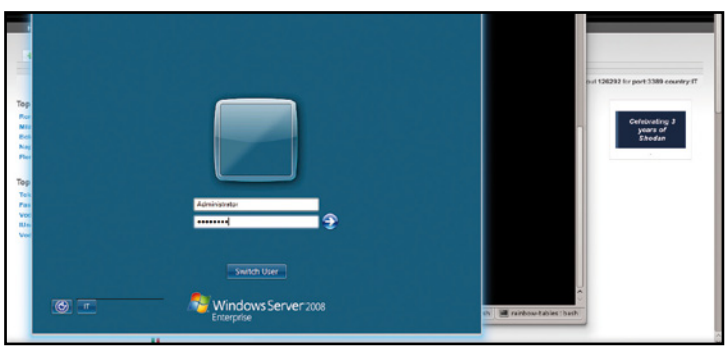
3 L'elenco delle vittime…

Dalla Konsole il pirata avvia TorBrowser col comando *cd ./tor-browser_en-US && ./App/vidalia --datadir Data/Vidalia -style Cleanlooks*. Poi si reca sul sito *www.shodanhq.com* e cerca la query *port:3389 country:IT* che gli fornisce la lista dei server italiani che consentono accesso remoto a Windows. Usando la porta *21* si potrebbero ottenere i server FTP.

4 … e quello delle password

A questo punto il pirata apre un'altra finestra della Konsole e scarica un elenco di possibili password con il comando *wget http://www.tuttohacking.it/testi/diz_ita.rar*, estraendone poi il contenuto con il comando *unrar diz_ita.rar*. A questo punto si ritrova col file chiamato *diz_ita.txt*, che contiene varie parole in italiano.





5 Una porta da scardinare

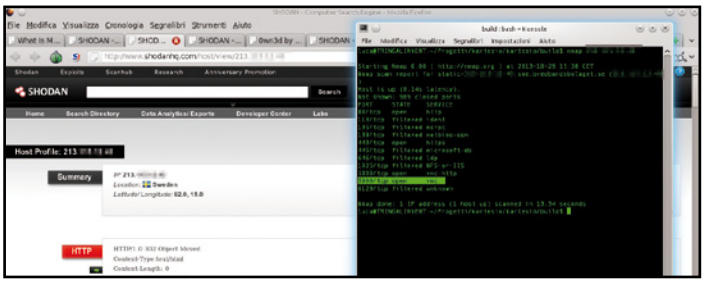
È tutto pronto affinché il criminale avvii la ricerca delle password con il comando *proxychains hydra 2.234.XXX.XX rlogin -l Administrator -P ./diz_ita.txt -V*. Dove, naturalmente, *2.234.XXX.XX* è l'IP della vittima, e *Administrator* l'utente di cui si vuole scoprire la password. Il programma proverà tutte le parole del file *diz_ita.txt*.

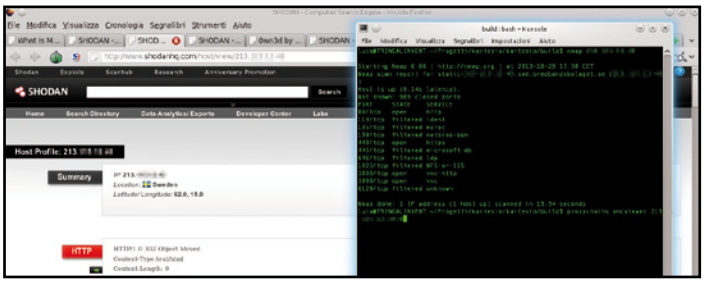
6 Accesso ottenuto

Quando una parola non funziona, il programma risponde *can not connect*. Se non dice niente, significa che la password è corretta. Appena viene trovata, il pirata dà il comando *proxychains rdesktop -m 2.234.XXX.XX* per collegarsi al server e fa login con nome utente e password che ora conosce. Esattamente come se si trovasse davanti al computer della vittima.

Se l'automazione non è sicura

Entrare in una caldaia a gas, una piscina, o una catena di robot che costruiscono oggetti vari? Grazie a Shoda, i pirati possono fare anche questo, se non ci si protegge adeguatamente.



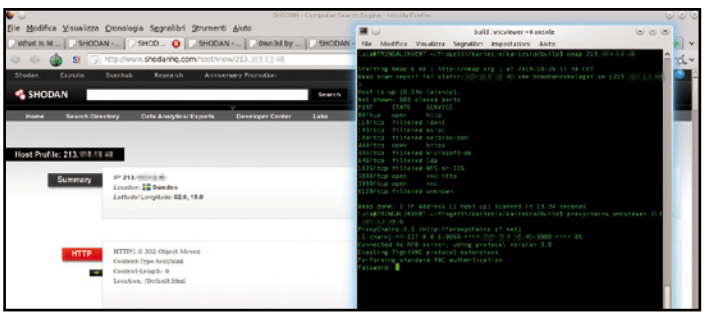


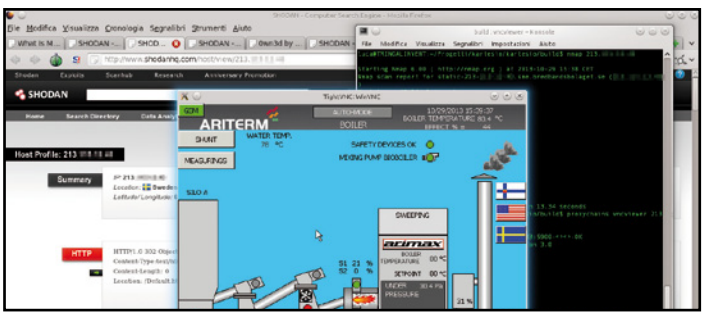
1 Obiettivi identificati

Il pirata può trovare facilmente su Shodan degli impianti industriali controllati con il sistema Siemens usando la query di ricerca *siemens hmi*. Quando ne ha trovato uno, apre un terminale su Backtrack e digita il comando *nmap 213.115.XX.XX* (dove *213.115.XX.XX* è l'IP del sistema vittima) per ottenere una lista delle porte di accesso disponibili.

2 Connesso allo schermo

Se tra le varie porte disponibili è presente la porta *5900* significa che il server *VNC* è disponibile. Al pirata non resta quindi che provare a collegarsi al server: per fare questo il criminale dà il comando *vncviewer 213.115.XX.XX:0*. Lo zero finale rappresenta il display standard usato sui dispositivi Siemens.



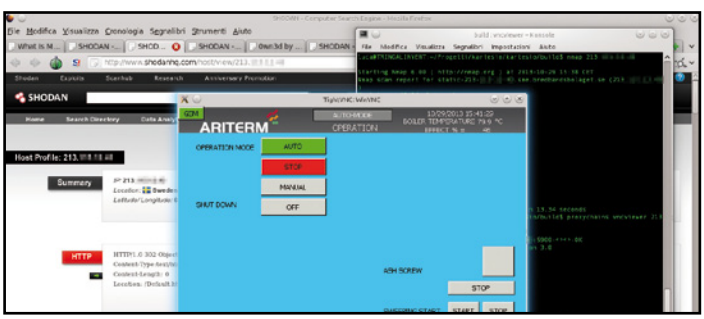


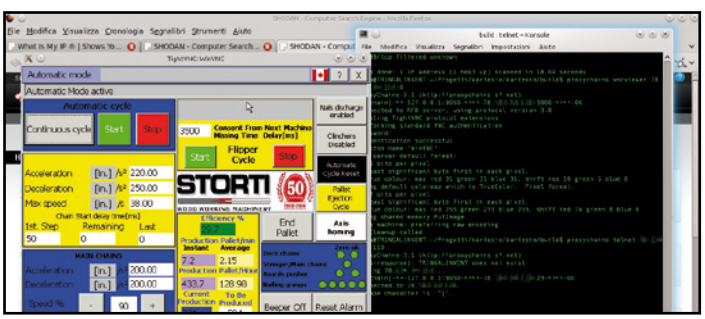
3 Ecco la password

Ovviamente il sistema richiede una password, ma visto che spesso gli utenti non la cambiano, il pirata prova ad entrare con la parola chiave di default, cioè *100*. Se non dovesse essere quella giusta potrebbe sempre ricorrere alla tecnica del "brute force", visto che VNC non limita il numero di tentativi di accesso (come fa invece SSH).

4 Controllo assoluto

Ottenuto l'accesso al sistema della vittima, il pirata si trova di fronte una finestra che simula lo schermo del dispositivo di gestione in cui è entrato. Ovviamente, la finestra è interattiva, quindi il criminale ha il completo controllo del dispositivo. Nell'esempio che vediamo in figura, si tratta di una caldaia a metano che porta l'acqua a 80° C.





5 Il pirata burlone!

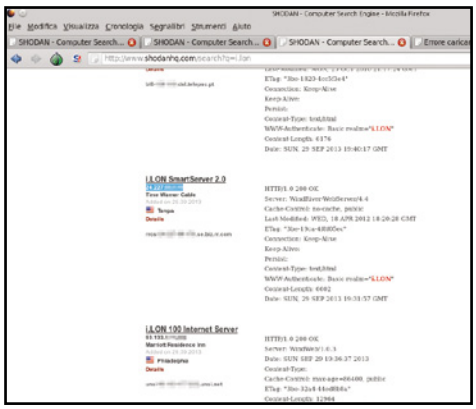
Il criminale, quindi, può carpire informazioni importanti sulla sua vittima ma può anche creare qualche disagio. Per esempio, può spegnere la caldaia, lasciando al freddo l'edificio. Uno scherzo piuttosto di cattivo gusto, anche considerando che difficilmente le vittime potranno capire cosa effettivamente abbia spento la caldaia.

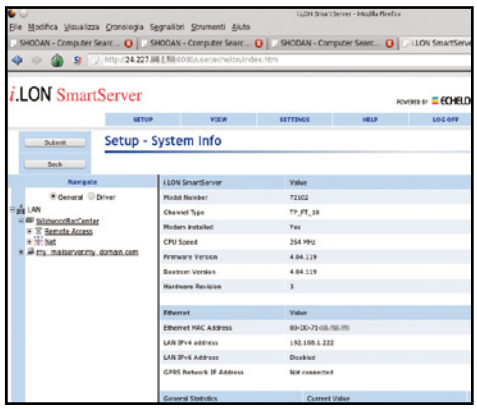
6 Anche da remoto

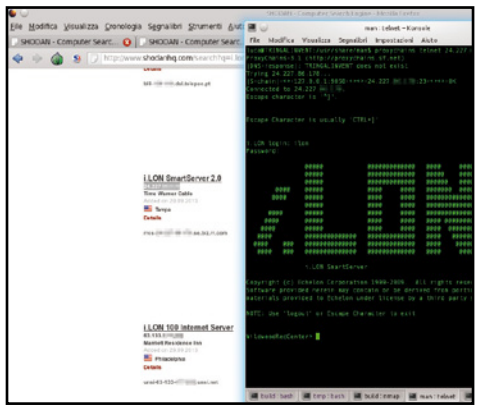
Si trovano veramente molti dispositivi e alcuni di questi sono accessibili anche tramite telnet. L'accesso telnet sui sistemi Siemens non è protetto da password, quindi il pirata può avere un controllo completo sul file system (e infatti i Web server vengono spesso "defacciati"). Nell'immagine si vede l'accesso a un impianto di produzione di pedane in legno.

Altri "giocattoli" per il pirata

Alcuni Web server vengono utilizzati per gestire gli impianti di interi edifici. È facile immaginare che se questi non sono sicuri, i pirati possono "entrare" facilmente e creare tanti disagi.







1 Il pirata cerca la vittima

Gli smartserver i.Lon prodotti da Echelon sono utilizzati per controllare edifici o addirittura complessi di edifici. Per trovarli il pirata cerca su Shodanhq la parola *i.lon*, in modo da ottenere una lista. L'immagine si riferisce a un centro ricreativo con una palestra da basket in Florida, ma si trovano anche strutture più grandi.

2 A volte basta una parola

Appena trova un indirizzo IP, il pirata prova a entrare tramite l'interfaccia web, che lavora sulla porta *8080*. Quindi aprendo col proprio browser l'indirizzo *http://24.227.XX.XXX:8080/* ed inserendo *ilon* sia come nome utente che come password, il criminale dovrebbe avere accesso al server, controllando tutti i dispositivi collegati.

3 Controllo dal terminale

Gli smart server possono essere controllati tramite telnet: con il comando *proxychains telnet 24.227.XX.XXX* e inserendo le stesse credenziali di accesso, il criminale riesce a disattivare alcune funzioni del server. Per esempio, disattivando il sistema di congelamento di una pista di pattinaggio sul ghiaccio può far fondere il ghiaccio stesso!

GOOGLE HACKS: LO SHODAN SECONDO IL MOTORE DI RICERCA BIG G

No, non è un nuovo prodotto della serie Google Maps e Google Docs: i Google Hacks sono dei trucchi (in inglese "hack") che permettono ai pirati di trovare con il motore di ricerca di Mountain View cose che, normalmente, dovrebbero essere nascoste... Un pirata può decidere di bombardare centinaia di persone con e-mail contenenti trojan. Eseguendo la query di ricerca **allintext:email OR mail +*gmail.com filetype:txt**, invece, fa incetta di file .txt con indirizzi e-mail privati. Si possono ottenere anche elenchi di clienti di varie aziende usando la query **allintext:email OR mail +*gmail.com AND client AND postal filetype:csv**. Carpire password di accesso ai siti nei database SQL? La stringa di ricerca **allintext:email AND pass AND "insert into" filetype:sql** fornisce risultati sconvolgenti. Le password potrebbero essere cifrate con algoritmo MD5, ma con un semplice programma di confronto stringhe di tipo "brute force" il pirata può risalire alla password in un paio d'ore. Per leggere la password di accesso a un database MySQL il pirata cerca su Google **intext:mysql_connect filetype:inc** e spulcia tra i vari risultati… Per scoprire le chiavi RSA private delle persone, invece, la query è **intitle:index.of intext:.ssh:** la ricerca restituisce alcune cartelle **/.ssh/**; il file id_rsa contiene la chiave privata con la quale si possono leggere i messaggi della vittima oppure firmare digitalmente false e-mail. È un furto di identità digitale, si tratta di qualcosa di estremamente pericoloso: è inutile lamentarsi con l'NSA del fatto che leggono la nostra posta, se poi siamo noi stessi a fornire loro la chiave crittografica per la nostra posta privata! Accedere a Webcam gestibili da remoto con Google? Basta utilizzare la query di ricerca **inurl:"viewerframe?mode=refresh"**. Entrare nel pannello di controllo on-line delle stampanti? Con la stringa **inurl:page=printerInfo** si ottiene facile accesso alle impostazioni di una stampante di rete. Trovare server VNC? I server VNC (come quelli che abbiamo visto nel caso degli impianti industriali Siemens) hanno spesso una interfaccia Web, a cui si può accedere usando la porta 5800 e cercando su Google **intitle:vnc.desktop inurl:5800**.

Password svelate grazie al PC

Cosa ci occorre
30 MIN. DIFFICILE
TOOL DI RECUPERO PASSWORD
WIN PASSWORD FINDER
Lo trovi su: ✔DVD
SOFTWARE COMPLETO

I nostri esperti ti svelano i trucchi unofficial e i software proibiti per scovare qualsiasi codice di accesso

In un mondo sempre più digitale e interconnesso la protezione dei dati personali e della nostra identità on-line è diventata un'esigenza basilare che non può in alcun modo essere sottovalutata. Ormai tutti, ogni giorno, abbiamo a che fare con password e, più in generale, codici di accesso: li usiamo per accedere al nostro computer, al diario su Facebook, alla casella di posta elettronica piuttosto che ai documenti riservati con le relazioni di lavoro da presentare in ufficio. E ogni volta dobbiamo fare uno sforzo mnemonico non indifferente per ricordarli tutti. Dimenticarli significherebbe essere tagliati fuori dalla nostra stessa vita digitale!

Accesso garantito

Per evitare che ciò accada abbiamo realizzato una raccolta di potenti tool tutti gratuiti con i quali sarà impossibile "restare fuori" dai servizi più importanti. Perfino rimuovere la password (dimenticata) del BIOS non sarà più un problema! E questo varrà anche per i documenti Word che ci siamo premurati di proteggere da occhi indiscreti; stesso discorso per i file PDF. E se lo ZIP colmo delle foto delle nostre vacanze è anch'esso protetto da una chiave che abbiamo dimenticato? Abbiamo la soluzione perfino per gli archivi compressi. Quando invece ci troviamo a dover maneggiare un vecchio computer stipato in cantina da tanti anni, cosa succede se all'accensione ci viene chiesta la password dell'account? Spesso non ci si ricorda cosa si mangia a pranzo, figuriamoci una sequenza di lettere "pensata" anni addietro. Basterà OphCrack, la distribuzione Linux preferita dai pirati per ovviare a quest'ultimo inconveniente: sarà necessario avviarla da Live USB e tutte le password appariranno in chiaro. Per saperne di più... continua con la lettura dell'articolo!

TUTTE LE SOLUZIONI PER METTERE IN CHIARO I CODICI DI ACCESSO

Windows, BIOS, documenti e archivi compressi: TI sveliamo i trucchi e i software usati dai pirati per scovare qualsiasi password.

BIOS
La password del BIOS può essere resettata, e quindi cancellata, rimuovendo e reinserendo la batteria dalla scheda madre del PC (sia desktop sia notebook)
PAG. 55

RAR/ZIP
Appnimi RAR Password Unlocker è un'ottima soluzione per recuperare le password degli archivi ZIP e RAR perdute. Offre diverse possibilità di "attacco" per la ricerca
PAG. 57

DOC/PDF
Appnimi DOC Password Unlocker rappresenta una valida soluzione per scovare le password usate per proteggere i nostri documenti Word e quelli in formato PDF
PAG. 57

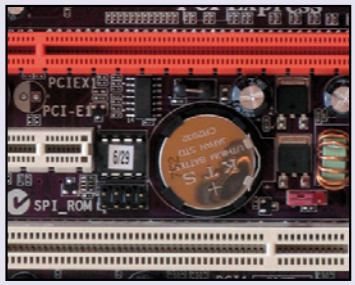
WINDOWS
Grazie a **OphCrack** potremo recuperare le password di accesso a Windows con relativa facilità, a meno che non siano molto complicate e composte da molti caratteri particolari (ad esempio: %, &, /, !, ?, >, <, ecc…)
PAG. 55

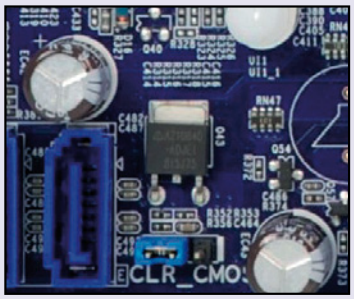
E-MAIL & WEB
Asterisk Key è una soluzione molto semplice da utilizzare per recuperare le password usate nel Web: rimuove infatti gli asterischi e mostra in chiaro le lettere che compongono i dati di login
PAG. 57

CELLULARI & TABLET
Con le nuove versioni del sistema operativo Android è diventato impossibile recuperare le password di accesso senza formattare il dispositivo, che rimane quindi l'unica alternativa possibile
PAG. 58

RECUPERA LA PASSWORD DEL BIOS

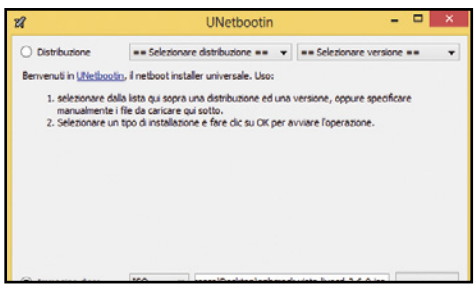
Qualora il nostro primo ostacolo sia rappresentato dalla richiesta della password del BIOS non appena acceso il PC, la soluzione (non l'unica, ma la più veloce) è rappresentata dalla rimozione e il reinserimento della batteria tampone dalla scheda madre del PC. Il BIOS è infatti un "mini sistema operativo" che fa un controllo di tutte le periferiche di cui è composto il computer e viene alimentato dalla batteria. Qualora il PC non dovesse disporre più di alimentazione, entrerà in funzione la batteria, presente in tutti i computer sia desktop sia notebook. Rimuovendola, però, tute le impostazioni salvate nel BIOS (password, data, ora…) verranno resettate! Ecco perché questo espediente è efficace nel caso in cui abbiamo dimenticato la chiave di accesso al computer. Se la batteria non può essere rimossa, è comunque possibile riprogrammare il BIOS spostando il jumper di reset presente sulla scheda madre e indicato dalla sigla ***CLR CMOR***. Bisogna poi tenere conto che molti produttori hardware inseriscono nel BIOS la Master Password che consente ai tecnici dell'assistenza di accedere alle impostazioni del PC bypassando quella inserita dall'utente. Per conoscere le chiavi di accesso dei principali modelli di motherboard, colleghiamoci al sito www.winmagazine.it/link/795.

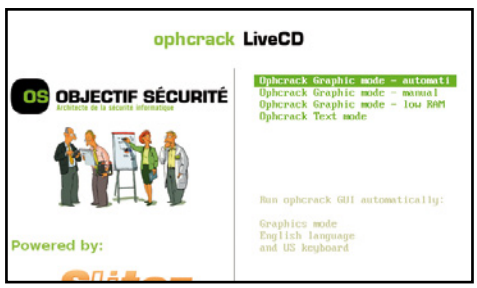




Codice di Windows in chiaro

Per accedere al sistema operativo è sufficiente creare un pennetta "bootable" con dentro la distribuzione Linux OphCrack che "scardina" il PC alla ricerca della password dell'account bloccato.





1 Recuperiamo il grimaldello

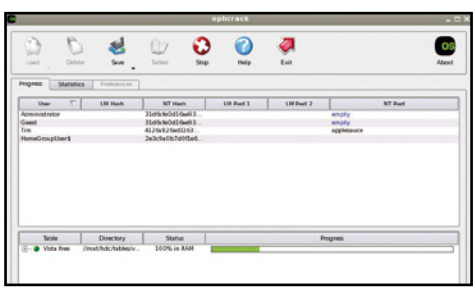
Dal DVD allegato a questo speciale scarichiamo l'archivio compresso *OphCrack.zip* e scompattiamolo in una qualsiasi cartella del nostro hard disk (ad esempio sul *Desktop*). Al suo interno troveremo l'immagine ISO della distro Linux che copieremo sulla chiavetta USB.

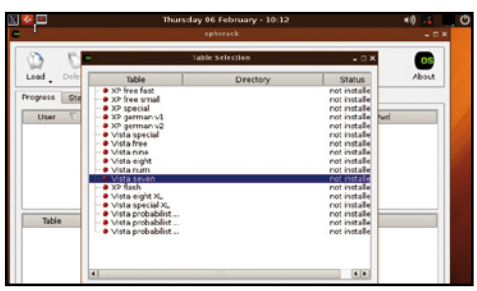
2 Tutto nella pennetta

Sempre dal DVD allegato a questo speciale scarichiamo il tool *Unetbootin* e avviamolo. Inseriamo nel PC una pennetta da almeno 4 GB: nell'interfaccia del software spuntiamo *Immagine disco* e selezioniamo l'immagine ISO di OphCrack. Premiamo *OK* per avviare la procedura.

3 Passiamo sul PC da recuperare

Pronta la chiavetta, inseriamola nel PC di cui vogliamo recuperare la password. Se non viene riconosciuto il boot da chiavetta, entriamo nel BIOS e impostiamo la priorità di boot sui dispositivi removibili. Apparsa la schermata di OphCrack premiamo *Invio* per avviare il mini OS.





4 Ecco le password!

Caricato il sistema operativo, dal desktop avviamo il tool *OphCrack*: si aprirà un'interfaccia che scansionerà gli hard disk del computer alla ricerca di un'installazione di Windows e dell'account di cui scovare la password che, dopo qualche secondo, sarà visibile nel campo *NT Pwd*!

5 Se la password non c'è…

Se la password è complessa, da OphCrack colleghiamoci a www.winmagazine.it/link/2412 per scaricare le tables contenenti dizionari più forniti. Dalla precedente schermata di Ophcrack clicchiamo *Tables*, *Vista Seven* e poi *Install*: cerchiamo il file scaricato e diamo *OK*.

6 L'accesso adesso è libero

Installate le nuove tabelle, chiudiamo e riavviamo OphCrack (come nel **Passo 4**). Avremo ora molte più probabilità che la password venga individuata! Non ci resta che scriverla da qualche parte, riavviare il PC e controllare di riuscire ad accedere nuovamente al nostro account!

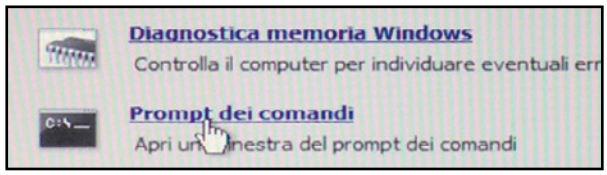
BUONI CONSIGLI

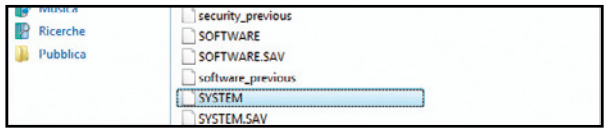
ECCO LA PASSWORD DEL ROUTER

È sempre buona norma cambiare la password predefinita del router ADSL: se la dimentichiamo, però, non potremmo più accedere al pannello di controllo per configurare, ad esempio, il port forwarding per le porte di accesso di eMule. In questi casi, possiamo resettare il dispositivo alle impostazioni di fabbrica per riuscire a loggarci con la chiave predefinita. Basta premere e tenere premuto per almeno 20 secondi il pulsante *Reset* posto sul retro del dispositivo. La procedura per recuperare la password di accesso alla rete Wi-Fi è invece più semplice. Nel caso del router Pirelli Alice Gate VoIP 2 Plus WiFi colleghiamoci al pannello di controllo digitando *192.168.1.1* nel browser e nella sezione *Wi-Fi* prendiamo nota della password indicata in *Chiave di cifratura*.

Nuova chiave per Windows

Se nel PC sono installati Vista o 7 possiamo sfruttare il tool integrato che permette di resettare la password di accesso al sistema operativo e crearne all'occorrenza una nuova. Ecco come.



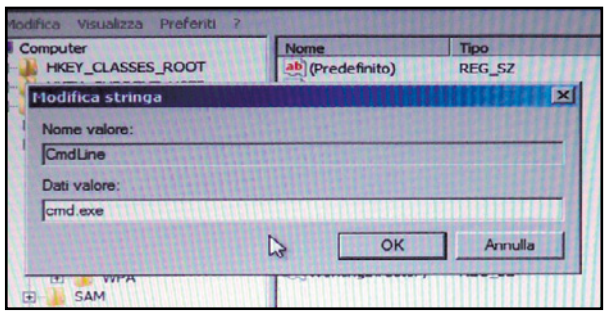


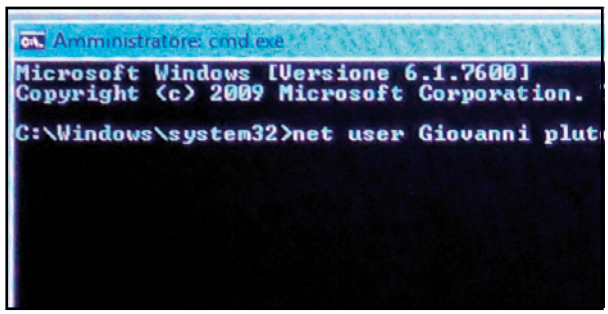
1 Gli strumenti di recupero

Inseriamo il DVD di Windows nel lettore del PC ed effettuiamo il boot dal drive ottico. Proseguiamo nelle varie schermate come se dovessimo installare il sistema operativo: giunti nella finestra *Installa*, clicchiamo *Ripristina il computer*. Selezioniamo l'OS presente sul PC e premiamo *Avanti*.

2 Mettiamo mano al registro

Clicchiamo *Prompt dei comandi*, digitiamo *regedit* e diamo *Invio* per avviare l'editor del registro. Individuiamo la chiave *HKEY_LOCAL_MACHINE* e clicchiamo *File/Carica hive*. Da *C:\Windows\System32\config* selezioniamo il file *SYSTEM* e diamo *Apri*. Verrà creata una chiave che chiameremo *reset*.





3 Il valore giusto della chiave

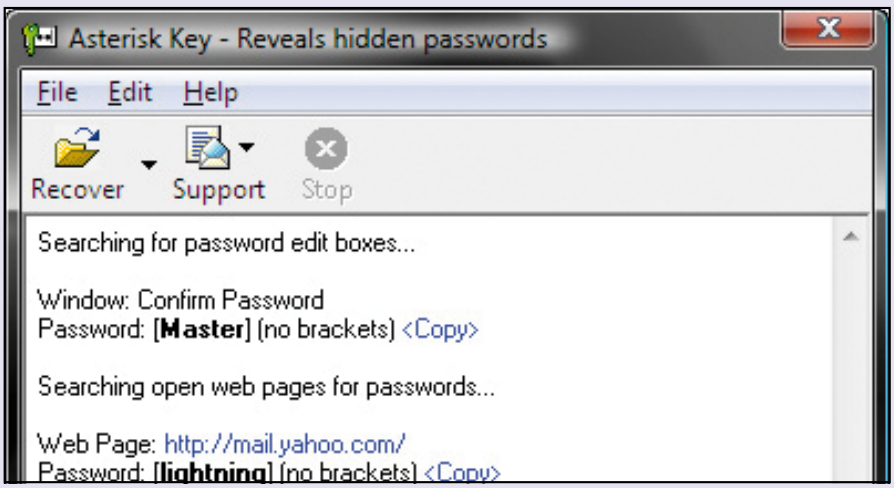
Selezioniamo la voce *HKEY_LOCAL_MACHINE\reset\Setup*. Clicchiamo due volte su *SetupType* e assegniamogli valore *2*. Doppio clic sulla chiave *CmdLine* e assegniamole valore *cmd.exe*. Selezioniamo *HKEY_LOCAL_MACHINE\reset*, andiamo nel menu *File* e clicchiamo *Scarica hive*.

4 Una password nuova di zecca

Riavviamo il PC. Verrà mostrato il Prompt dei comandi. Digitiamo *net user* seguito dal nome utente e dalla nuova password (ad esempio net user *Giovanni pluto*). Se il nome utente è composto da più parole, racchiudiamolo tra virgolette. Premiamo *Invio*, digitiamo *exit* e premiamo nuovamente *Invio*.

PASSWORD NASCOSTE DIETRO GLI ASTERISCHI? SCOPRILE COSÌ!

Tutti i browser permettono (ma anche il sistema operativo e i client di posta elettronica) permettono di memorizzare le password digitate nei vari form di accesso: una funzionalità sicuramente molto utile. Purtroppo, però, sono pochissime le possibilità di recuperarle, soprattutto nel caso dei servizi online che, il più delle volte per cambiare la password richiedono di inserire quella "vecchia", che ovviamente non ricordiamo! In questi casi, un aiuto inaspettato ci arriva da Asterisk Key, un tool molto "leggero" che resta attivo in background e ci rivela in chiaro le credenziali di accesso "nascoste" dietro gli asterischi. Il programma, semplicissimo da utilizzare, funziona con molti servizi Web tra cui Mailbox, Facebook, Twitter e forum, ma anche con i form precompilati del sistema operativo. Basta cliccare sul pulsante ***Recover*** per mettere le password in chiaro.

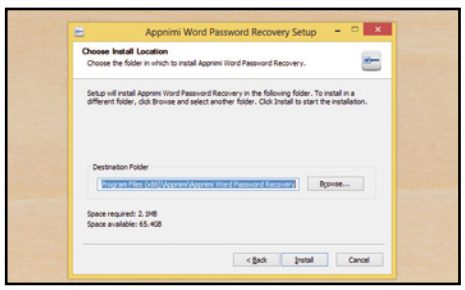


BROWSER, E-MAIL E CHAT: ECCO LO SCOVA PASSWORD

Grazie ad alcuni software specializzati possiamo recuperare facilmente le password degli account di posta memorizzate sul computer, del programma di messaggistica istantanea e quelle utilizzate per loggarci ai servizi Web salvate nel browser. Per recuperare quella della posta elettronica possiamo usare ***Mail PassView***: basta eseguire il file mailpv.exe e attendere che il programma faccia il suo dovere. Analogamente, possiamo usare ***MessenPass*** per risalire al nome utente e alla password utilizzati con i principali client di chat. Infine, per recuperare le password del browser possiamo ricorrere a ***IE PassView*** per Internet Explorer e ***PasswordFox*** per Firefox.

Così apri file DOC e PDF protetti

Con Appnimi Word Password Recovery e Appnimi PDF Password Recovery recuperi facilmente le password dei tuoi file DOC e PDF, anche quelle abbastanza complesse. Ecco come usarli al meglio.



1 Pronti a installare

Avviamo l'installazione di Word Password Recovery dal Win DVD-Rom. Durante l'installazione ci viene proposto per due volte di installare una toolbar: entrambe le volte clicchiamo su *Decline*. Procediamo premendo due volte *Next* per terminare la procedura.

2 Semplici impostazioni

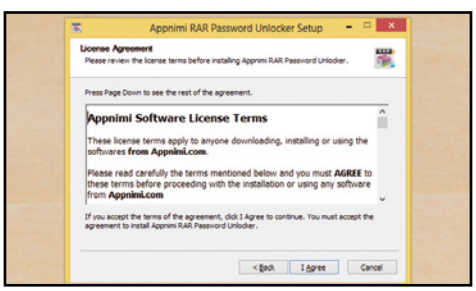
I comandi da usare sono pochi. Cliccando *Select* scegliamo il file DOC di cui recuperare la password. Con *Min Length* e *Max length* settiamo il numero minimo e massimo di lettere di cui la chiave potrebbe essere composta. Clicchiamo *Start* per avviare la procedura.

3 Non resta che attendere

La procedura di recupero della password potrebbe durare diversi minuti. Il tutto comunque dipende anche dalla potenza del processore del PC. Il risultato è garantito, anche se con chiavi di accesso particolarmente "complicate" il risultato potrebbe non essere quello sperato.

File compressi: li scardini così!

Appnimi RAR Password Recovery è un'ottima scelta se stiamo cercando una valida soluzione per recuperare le password perdute dei nostri archivi RAR e ZIP. Impariamo ad usarlo al meglio.



1 Iniziamo con l'installazione

Avviamo l'installazione di Appnimi RAR Password Recovery presente all'interno del DVD allegato a questo speciale. Durante il processo ci verrà chiesto di installare una toolbar per due volte: rifiutiamo cliccando *Decline*. Clicchiamo *Next* fino ad arrivare al termine della procedura.

2 Interfaccia ricca di funzioni

In *Input* scegliamo il file ZIP/RAR che desideriamo analizzare. In *Min Length* e *Max length* inseriamo il numero minimo e massimo di lettere di cui dovrebbe essere composta la password. In *Destination* scegliamo la cartella nella quale verranno estratti i file al termine della procedura.

3 Ce l'abbiamo quasi fatta!

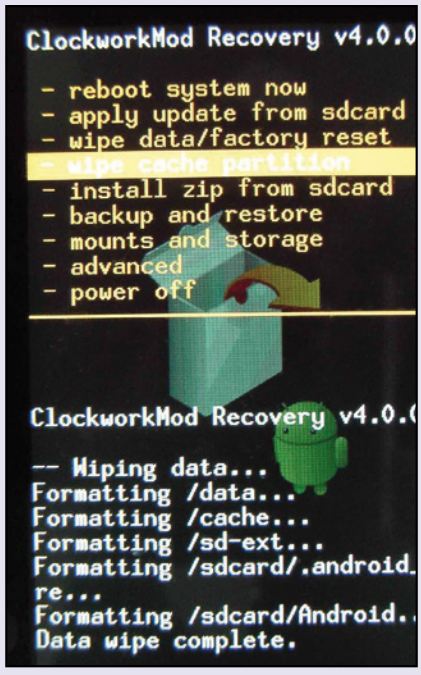
Possiamo eseguire un attacco Brute Force o Dictionary: il primo "mescola" tutti i caratteri fino a comporre la password cercata; il secondo si avvale di migliaia di chiavi di accesso contenute in un file di testo integrato nel programma che vengono provate fino a trovare quella giusta.

CELLULARI E TABLET: SERVE IL RESET DEL DISPOSITIVO!

Se per i PC il recupero delle password può sembrare relativamente semplice, non è per niente così se invece consideriamo gli smartphone e i tablet Android. Se con le vecchie versioni del sistema operativo di Google era possibile intervenire (seppur in maniera un po' macchinosa) sul reset delle password di sistema modificando alcuni file, con i nuovi aggiornamenti non è più così. E forse è anche un bene, dato che è molto più alta la probabilità che un dispositivo portatile ci venga sottratto con la reale possibilità che questo finisca nelle mani sbagliate: inutile dire che in questo caso la nostra privacy viene messa davvero a dura prova! Sostanzialmente, ora le uniche soluzioni che si possono attuare dopo essersi completamente dimenticati la password di sblocco sono due: una è la totale formattazione del device. Quindi dobbiamo stare molto attenti nel caso in cui usassimo una sequenza numerica facile da dimenticare. Stesso discorso se invece usiamo il sistema di sblocco con la sequenza da "disegnare" sullo schermo. L'altro metodo è provare e riprovare delle possibili combinazioni finché, al quindicesimo tentativo, ci verranno richieste le credenziali del nostro account di Google per poter sbloccare il dispositivo. Le ricordiamo quelle, vero? Se così non fosse, l'unica soluzione è rappresentata dalla formattazione del cellulare o tablet.

UNA RECOVERY PROVVIDENZIALE

In questo caso possiamo procedere con un hard reset tramite la recovery presente in ogni dispositivo Android. Per prima cosa bisogna spegnere il dispositivo per poi riaccenderlo tramite una combinazione di tasti che però è differente in base alla marca: sui dispositivi Nexus, ad esempio, è sufficiente usare la combinazione ***Volume su*** + ***Volume giù*** + ***Tasto accensione***; per i Samsung dovremo premere ***Volume su*** + ***Home*** + ***Tasto accensione***; su HTC basta tenere premuto il tasto ***Volume giù*** + ***Tasto accensione***. Entrati a questo punto nella recovery di sistema, sarà sufficiente individuare la voce ***wipe data/factory reset*** e selezionarla per avviare la procedura che "raderà al suolo" tutta la memoria interna del nostro dispositivo, eliminando sì tutte le credenziali di accesso ma anche tutti i file in esso contenuti!



La parola all'avvocato

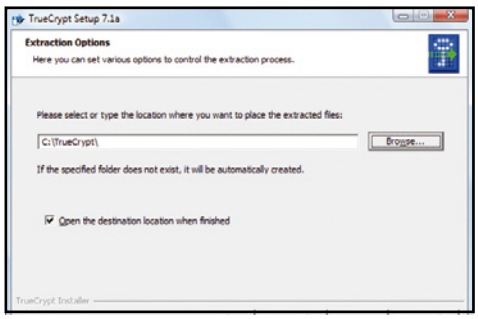
Guido Scorza è uno dei massimi esperti in Diritto delle Nuove Tecnologie

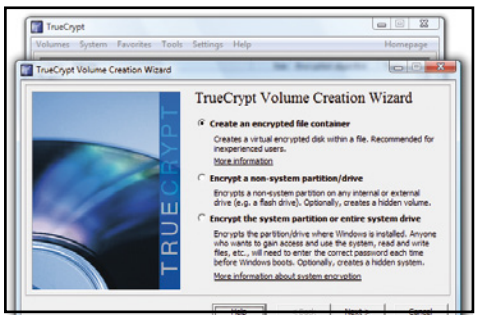
NON DESIDERARE LA PASSWORD D'ALTRI

Lo si dice e scrive spesso, ma mai abbastanza: la tecnologia non è né buona né cattiva, né lecita né illecita! Tali caratteristiche appartengono all'uso che ciascuno sceglie di farne. Tale considerazione è particolarmente calzante in relazione alle decine e decine di software diffusi in Rete e sul mercato che consentono, ormai anche ad utenti poco esperti, di cimentarsi con il recupero di password smarrite o dimenticate. Si tratta di soluzioni utili, preziose e legittime a condizione di usarle per il recupero della propria password e, dunque, per garantirsi l'accesso al proprio PC o all'account di posta elettronica. L'uso di tali soluzioni, invece, diviene certamente illegittimo laddove le password che si cerca di recuperare appartengano ad altri o comunque valgano a garantirci l'accesso ad un sistema o ad un account che non ci appartiene. In tal caso, salvo che sia stato il proprietario del sistema in questione a chiederci una mano per recuperare la password, corriamo il rischio di ritrovarci invischiati in guai piuttosto seri. L'art. 615 quater del codice penale, infatti, stabilisce che ***"Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164"***. Se poi, oltre a procurarsi la password per l'accesso ad un sistema o ad un account di posta che non ci appartengono, decidessimo addirittura di usarli per accedere a tali sistemi, la situazione potrebbe aggravarsi ulteriormente. L'art. 615 ter dello stesso Codice Penale, stabilisce, in tal caso che ***"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni"***. Inutile, poi, dire che se non ci si accontenta né di mettere alla prova la propria abilità per recuperare la password altrui né di accedere all'altrui sistema o account di posta ma, dopo averlo fatto, ci si diverte anche a prendere visione del contenuto del sistema o della corrispondenza elettronica a noi non diretta, si pongono le Autorità nell'imbarazzo della scelta circa l'elenco di reati da contestarci: dalla violazione della disciplina sulla privacy sino ad arrivare alle ipotesi di reato a tutela della segretezza della corrispondenza. L'utilizzo di tali soluzioni può, insomma, costarci davvero molto caro. Meglio, dunque, non dimenticare mai che entrare nel PC altrui senza permesso equivale a entrare nell'altrui abitazione o ufficio e impossessarsi - anche solo momentaneamente - dell'altrui account di posta elettronica equivale ad aprire la corrispondenza ad altri indirizzata. Meglio pensarci due volte prima di procedere…

Mettiamo al sicuro le password

Preferiamo annotare le nostre password in un file di testo da tenere sempre a portata di clic? Ecco come metterlo al sicuro in un'unità virtuale criptata creata con TrueCrypt e archiviata nel nostro spazio cloud su Dropbox.





1 Strumenti di sicurezza

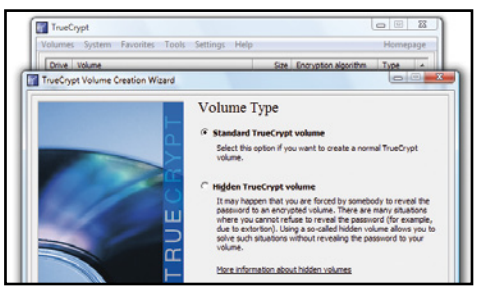
Installiamo il client Dropbox (lo trovi nel DVD allegato a questo speciale) e creiamo, se non ne abbiamo già uno, un account gratuito da 2 GB. Al termine, scompattiamo l'archivio *TrueCrypt.zip* (sezione *Antivirus&Sicurezza*) ed eseguiamo il file *TrueCrypt Setup 7.1a.exe*.

2 Estraiamo tutti i file

Selezioniamo *Extract* per installare la versione portabile e premiamo *Next*. Confermiamo i messaggi di avviso con *OK* e *Sì*. Clicchiamo *Browse* per selezionare una cartella in cui estrarre i file del programma (ad esempio *C:\TrueCrypt*) e premiamo *OK*. Al termine diamo *OK* e *Finish*.

3 Un'unità "inaccessibile"

Verrà aperta automaticamente la cartella con i file di TrueCrypt. Facciamo doppio clic sul file *TrueCrypt.exe* e nella schermata principale del programma clicchiamo su *Create Volume*. Assicuriamoci che sia selezionata l'opzione *Create an encrypted file container* e premiamo *Next*.



4 Creiamo il file del volume

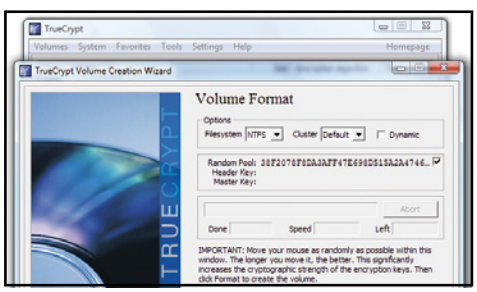
Nella schermata successiva selezioniamo *Standard TrueCrypt volume* e clicchiamo *Next*. In *Volume Location* premiamo *Select File*, andiamo nella cartella di Dropbox e indichiamo il nome da assegnare all'unità criptata (*Personale*), premiamo *Salva* e clicchiamo su *Next*.

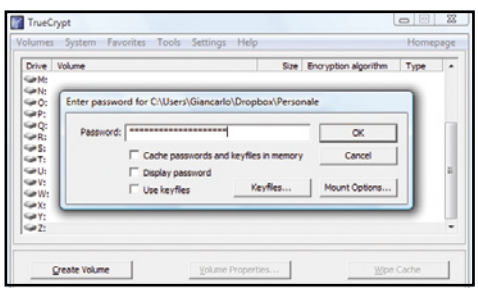
5 La scelta della dimensione

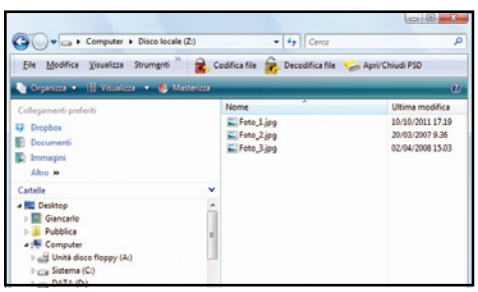
Da *Encryption Algorithm* selezioniamo l'algoritmo di crittografia (ad esempio *AES-Twofish*) per criptare i dati dell'unità virtuale e premiamo *Next*. Digitiamo la dimensione dell'unità virtuale tenendo conto che lo storage di base disponibile su Dropbox è pari a 2 GB e premiamo *Next*.

6 Password di 20 caratteri

Digitiamo quindi negli appositi box una password di accesso (e la relativa conferma) all'unità virtuale. Scegliamola con cura in modo che sia sufficientemente complessa e assicuriamoci che la sua lunghezza sia di almeno 20 caratteri. Proseguiamo cliccando sul pulsante *Next*.







7 E adesso formattiamo!

Selezioniamo il file system con cui formattare l'unità virtuale, ad esempio *NTFS* e muoviamo il puntatore in modo random all'interno della finestra per aumentare la forza delle chiavi di crittografia. Clicchiamo su *Format*, Attendiamo che venga creato il file e al termine premiamo *Exit*.

8 Un nuovo disco sul PC

Dall'interfaccia principale di TrueCrypt selezioniamo dall'elenco dei drive l'unità *Z:*, premiamo *Select File*, indichiamo il volume appena creato e premiamo *Apri*. Clicchiamo quindi su *Mount*. digitiamo la password del volume e premiamo *OK*.

9 È tutto sincronizzato!

La nuova unità (*Z:*) sarà accessibile da *Esplora risorse* e dalle applicazioni installate. Possiamo già salvarvi dentro dei file. Per smontare l'unità virtuale, selezioniamola in TrueCrypt e premiamo *Dismount*. Una volta smontato il file, verrà aggiornato in remoto su Dropbox.

Giù le mani dai miei dati!

Vuoi vendere un PC o un cellulare? Ecco come eliminare per sempre i file salvati nei dispositivi

Cosa ci occorre

30 MIN. FACILE

TOOL DI SICUREZZA
DISKWIPE
Lo trovi su: ✔DVD
SOFTWARE COMPLETO
Sito Internet: www.diskwipe.orgc

SOFTWARE DI OTTIMIZZAZIONE
CCLEANER
Lo trovi su: ✔DVD
SOFTWARE COMPLETO
Sito Internet: www.piriform.com

TOOL DI RECUPERO FILE
RECUVA
Lo trovi su: ✔DVD
SOFTWARE COMPLETO
Sito Internet: www.piriform.com

PROGRAMMA DI RECUPERO FILE
WONDERSHARE DR.FONE
Lo trovi su: ✔DVD
Quanto costa: € 37,19,00
Sito Internet: www.wondershare.net

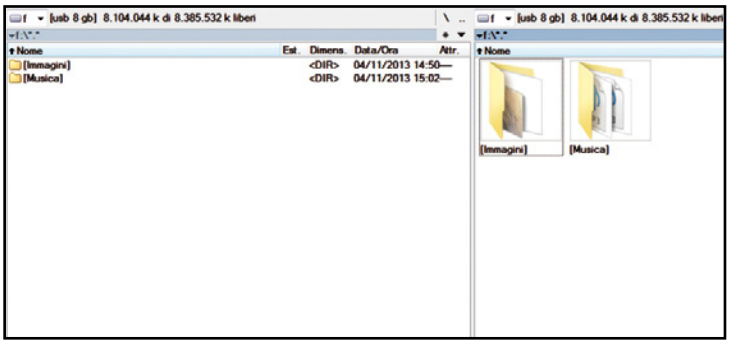
Quando si vuole vendere un PC, un notebook, uno smartphone, un tablet o in generale un dispositivo dotato di una unità di memorizzazione (oppure anche soltanto un hard disk o una scheda di memoria SD), è bene assicurarsi di eliminare i dati memorizzati al loro interno in maniera definitiva. Non è sufficiente, infatti, una formattazione per "svuotare" un disco rigido o una memoria di massa portatile. Adoperando appositi tool, infatti, il nuovo proprietario del dispositivo da noi venduto potrebbe riuscire a recuperare tutti (o almeno buona parte) i dati presenti in esso. E visto e considerato che l'abitudine comune è quella di conservare su PC, cellulari e tablet documenti personali, credenziali di accesso a conti corrente on-line e altri dati sensibili, è fondamentale assicurarsi, prima di cedere un dispositivo, di aver eliminato i dati contenuti e di fare in modo di non renderli recuperabili neanche con l'uso di programmi atti allo scopo.

Cancellare tutto per sempre

Per ottenere questo risultato dobbiamo pertanto ricorrere ad alcuni software specifici, come CCleaner, che effettuano il "wipe" del disco, scrivendo dati random e rendendo praticamente impossibile il recupero delle informazioni. Questa operazione può essere effettuata non solo sui dischi rigidi, ma anche sulle chiavette USB, sulle SD Card e alle memorie dei telefoni cellulari. Cosa un po' diversa, invece, è la cancellazione dei dati dalla memoria principale degli smartphone. In questo caso dobbiamo effettuare il root del telefono, quindi entrare nel recovery mode e infine procedere con il wipe. La procedura cambia a seconda del modello, ma possiamo ugualmente utilizzare delle app che si occupano di eliminare i dati nel modo più sicuro possibile. Vediamo quindi come effettuare una cancellazione sicura dei dati dalle memorie e verificare che siano stati effettivamente eliminati.

Cancellazioni a prova di hacker

Utilizzando in sequenza due appositi tool possiamo eliminare in maniera definitiva tutti i dati presenti su una chiavetta USB. Questo procedimento vale anche per hard disk e schede SD e MicroSD.

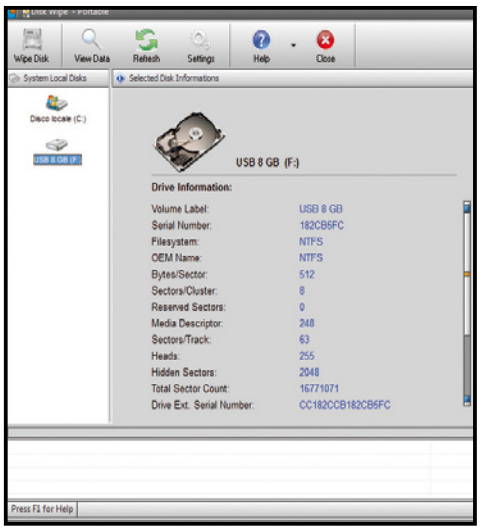


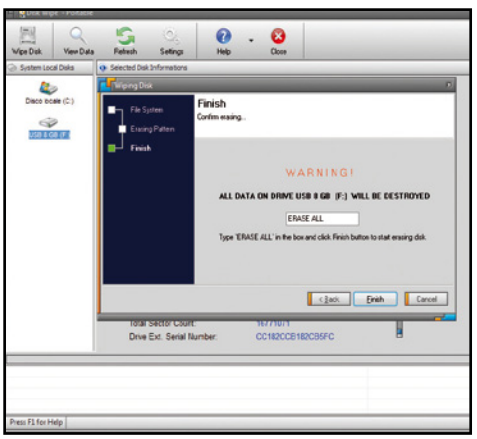
1 Esploriamo la pendrive

Inseriamo la nostra chiavetta USB nell'apposita porta del computer e visualizziamone il contenuto con Esplora Risorse o con qualunque altro file manager. Nel nostro caso file come immagini e brani musicali si trovano all'interno delle cartelle *Immagini* e *Musica*.

2 Il tool cancella tutto

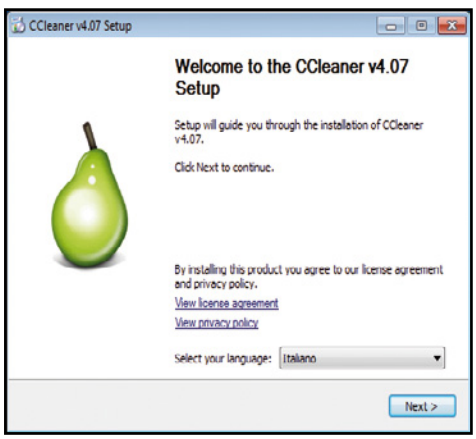
È il momento di effettuare il "wipe" del supporto. Per massima sicurezza cancelliamo i dati utilizzando due software. Cominciamo con DiskWipe (lo trovi nel DVD allegato a questo speciale). Non necessita di installazione: per avviarlo facciamo doppio clic sul file eseguibile.





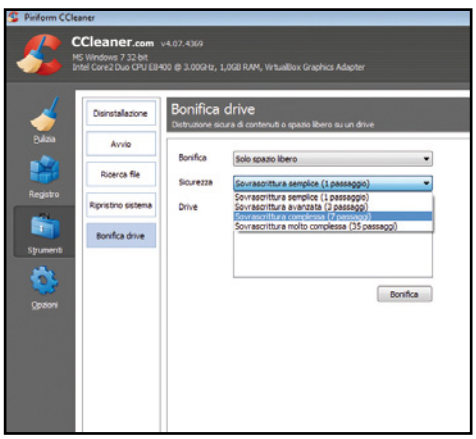
3 Il giusto numero di passate

Selezioniamo il disco da cancellare, clicchiamo *Wipe Disk*, quindi premiamo *Next*. Scegliamo quante passate effettuare (nel caso di una memoria USB o una scheda SD non esageriamo perché potrebbe danneggiarsi). Confermiamo nella schermata successiva e premiamo *Finish*.



4 Rifacciamo tutto con CCleaner

Scompattiamo sul disco rigido l'archivio compresso *CCleaner.zip* (lo trovi nel DVD allegato a questo speciale) e facciamo doppio clic sul file eseguibile. Selezioniamo *Italiano* come lingua e seguiamo la procedura d'installazione guidata.

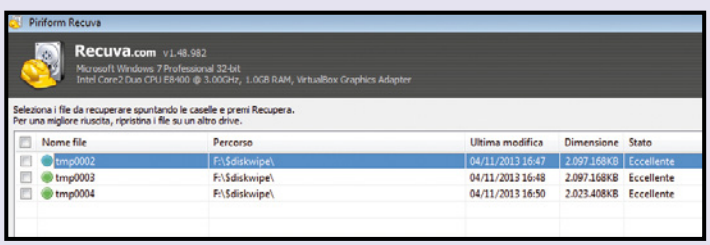


5 Bonifichiamo la chiavetta

Avviato CCleaner, a sinistra clicchiamo *Strumenti*, quindi *Bonifica*. Scegliamo il disco da bonificare e il numero di passaggi da effettuare (selezioniamo almeno 7 passaggi (*Sovrascrittura complessa*) solo nel caso di hard dask) e premiamo il pulsante *Bonifica*.

LA PROVA DEL NOVE

Dopo aver eseguito il wipe del disco, è bene verificare se i dati risultano ancora recuperabili o meno. Per farlo installiamo il software Recuva (lo trovi nel DVD allegato a questo speciale), avviamo il programma tramite l'icona creata sul desktop e seguiamo il wizard proposto da Recuva. Scegliamo la voce Tutti i file e la posizione (il disco) sulla quale effettuare il ripristino dei file. In redazione abbiamo effettuato dei test di recupero subito dopo aver eliminato i dati sia con l'uno sia con l'altro software. Nel caso del wipe effettuato con Wipe Disk, Recuva ha recuperato soltanto 3 file dei 77 che erano memorizzati nel disco, sia effettuando la scansione veloce sia quella approfondita. I file recuperati, però, non sono risultati utilizzabili, come spesso capita eseguendo questo tipo di operazione in caso di recupero. Ancora meglio le cose sono andate dopo il wipe effettuato con CCleaner: il programma Recuva non è infatti riuscito a ripristinare neanche un file.



Ripuliamo smarthone e tablet

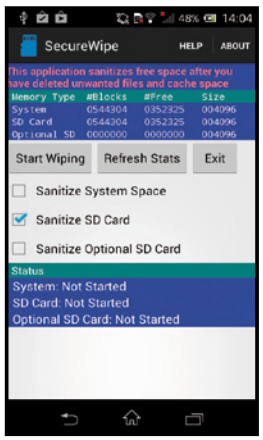
Nei seguenti passi abbiamo utilizzato un Sony Xperia M. Se vogliamo eliminare tutti i dati da un dispositivo diverso facciamo riferimento al box a fondo pagina. Ecco come fare.

1 Un Android come nuovo

Per riportare alle impostazioni di fabbrica la memoria principale di uno smartphone o tablet Android andiamo in *Impostazioni/Backup e ripristino/Ripristino dati di fabbrica*. In questo modo il sistema sarà in grado di eliminerà definitivamente gli account impostati e tutte le applicazioni installate.

2 "Svuotiamo" la memoria aggiuntiva

Per eliminare in maniera definitiva tutti i dati presenti nella scheda di memoria SD installata nello smartphone scarichiamo l'app SecureWipe dal Play Store. Avviamola, togliamo la spunta dalla voce *Sanitize System Space* e infine tocchiamo su *Start Wiping*,

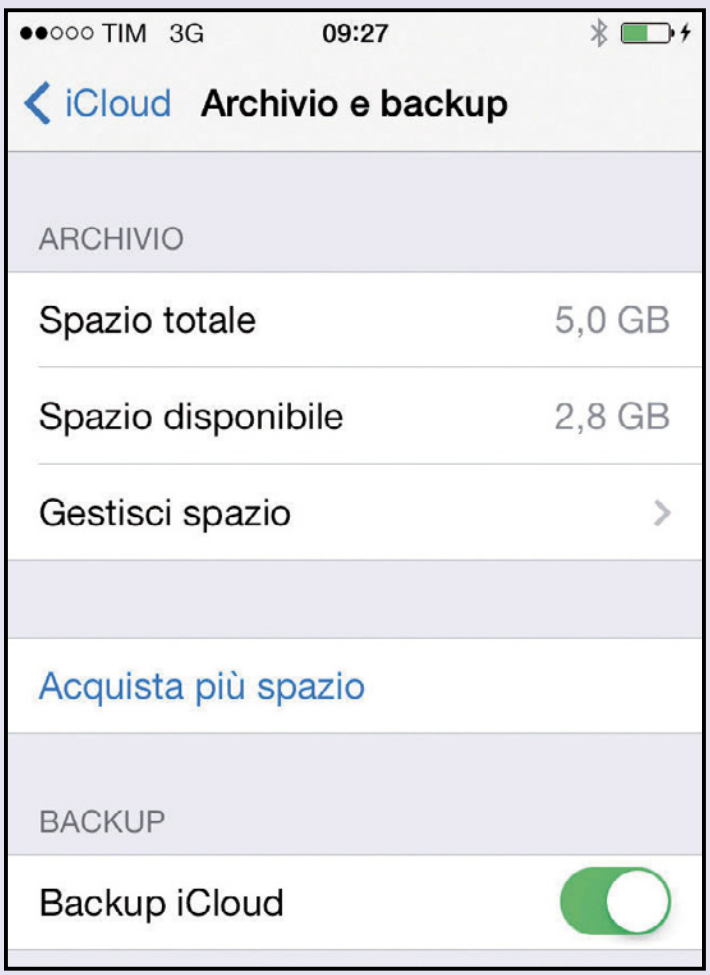


3 Cancellazione effettuata

Per controllare una memoria esterna inseriamola nel lettore del PC e seguiamo la procedura nel box **La prova del nove**. Altrimenti, installiamo il software Wondershare Dr.Fone (lo trovi nel DVD allegato a questo speciale), colleghiamo il telefono via USB e seguiamo le istruzioni.

BACKUP E RIPRISTINO SU IPHONE

Se prima di vendere un dispositivo Apple vogliamo effettuare una copia di backup dei dati memorizzati su di esso, dobbiamo solo scegliere se utilizzare iCloud o se farlo direttamente sul nostro computer. Se optiamo per la copia sul Mac dobbiamo avviare il player multimediale iTunes, selezionare il dispositivo da vendere e, nella sezione ***Backup*** fare clic su ***Questo computer***. Subito dopo scegliamo ***Effettua backup adesso***. Se dovessimo invece scegliere di effettuare il salvataggio su iCloud, andiamo nelle ***Preferenze*** dell'iPhone e selezioniamo ***iCloud/Archivio e Backup*** e, infine, ***Effettua backup adesso***. Nel caso ci trovassimo nella necessità impellente di effettuare il ripristino, dobbiamo collegare lo smartphone direttamente al computer tramite il cavo Dock/Lightning e n seguito lasciamo avviare iTunes. Terminata questa operazione, clicchiamo sul pulsante ***iPhone***. Se possediamo invece più di un dispositivo, al posto del pulsante iPhone dobbiamo selezionare ***Dispositivi*** e poi il nome del melafonino. Premiamo poi ***Ripristina iPhone*** e facciamo clic su ***Backup e Ripristina***. Prima che il ripristino giunga al termine scarichiamo sul Mac l'ultima versione di iOS. Alla fine del download dovremo solo aspettare ancora qualche minuto e il gioco sarà fatto. Completata correttamente la procedura di ripristino, iTunes chiederà se configurare il telefono come un nuovo dispositivo o se ripristinare le applicazioni e i dati del backup effettuato in precedenza. Nel nostro caso non bisogna fare altro: sarà il nuovo proprietario a configurarlo come meglio desidera. Per evitare che lui continui a ricevere messaggi indirizzati a noi, disabilitiamo iMessage. Spuntiamo l'apposita opzione nelle ***Preferenze di Sistema*** e sotto la voce ***Messaggi*** e avvisiamo Apple del passaggio di proprietà. Logghiamoci con le nostre credenziali Apple ID, selezioniamo il telefono nella lista disponibile e facciamo clic su ***Annulla la registrazione***.



ABBONATI A
WIN MAGAZINE

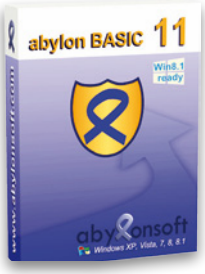
Collegati all'indirizzo http://abbonamenti.edmaster.it/winmagazine
e scopri le nostre offerte di abbonamento

Giù le mani dai miei file

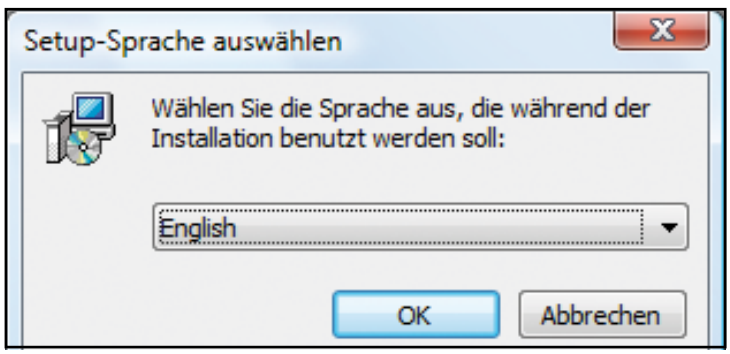
Così puoi crittografare i dati salvati su disco e pendrive per renderli inaccessibili a spioni e ficcanaso

Cosa ci occorre 30 MIN. FACILE

SOFTWARE DI CRITTOGRAFIA
ABYLON BASIC 11
Lo trovi su: ☑DVD
Quanto costa: Gratuito
Sito Internet: www.abylonsoft.com



Documenti, filmati, foto: i nostri dati non sono mai al sicuro da occhi indiscreti. Durante una pausa di lavoro, ad esempio, qualora ci allontanassimo dal PC, qualcuno potrebbe provare ad accedervi e sbirciare tra file e cartelle del disco rigido. Immaginiamo poi cosa potrebbe succedere se dimenticassimo incustodita da qualche parte una chiavetta USB sulla quale abbiamo salvato file personali. La soluzione per evitare questo tipo di evenienze è criptare i propri dati in modo tale che nessuno possa riuscire ad accedere al loro contenuto. Per farlo possiamo utilizzare un programma specifico come abysoft BASIC 11, in regalo per i lettori di questo numero di Win Magazine, che consente di proteggere i file e criptarli mediante l'uso di password e persino di certificati digitali. Ecco come fare.

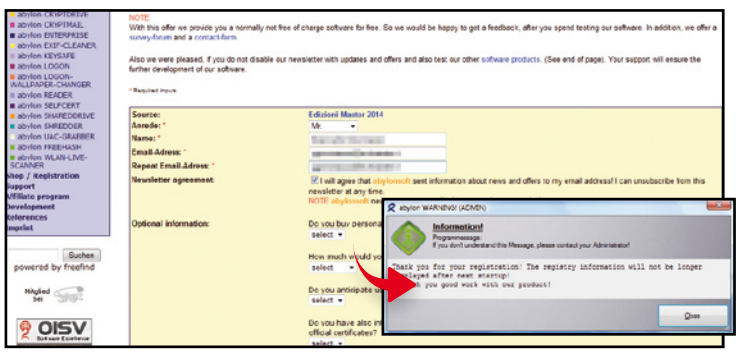


Si parte con il setup

1 Scompattiamo sul disco rigido l'archivio compresso *Basic11.zip* (lo trovi nel DVD allegato a questo speciale) e facciamo doppio clic sul file *Basic11.exe*. Nella schermata di setup selezioniamo *English* dal menu a tendina, quindi premiamo *OK*.

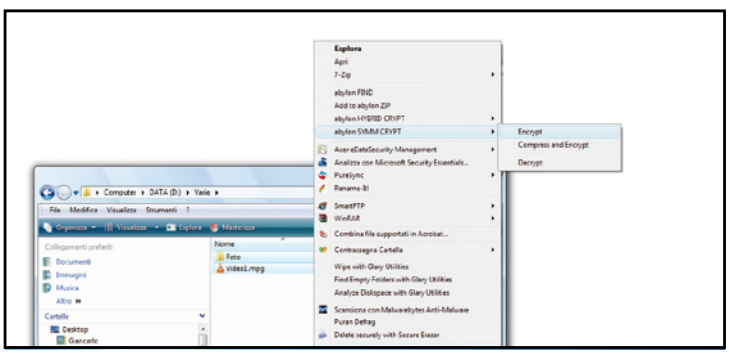
Richiediamo il codice

2 Seguiamo la procedura guidata: al termine leviamo tutte le spunte delle opzioni visualizzate e premiamo *Close*. Quando compare il messaggio del completamento dell'installazione clicchiamo su *No*. Nella schermata di registrazione facciamo clic invece su *Request registration data*.



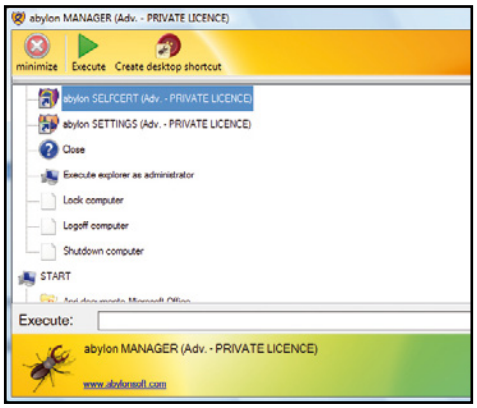
Una veloce registrazione

3 Si aprirà una pagina Web con un form in cui inserire il nostro nome e la nostra e-mail, quindi clicchiamo su *Request registry key!* e su *OK*. Riceveremo un'e-mail contenente *CD-Key* e *Registry – Key*: copiamoli nei box della schermata del programma e premiamo *Activate*, quindi su *Close*.



Criptiamo usando una password

4 A questo punto possiamo subito procedere con la crittografia dei file. Per criptare con una password una cartella o un gruppo di file selezioniamoli, clicchiamo su di essi con il tasto destro del mouse e clicchiamo sulla voce *abylon SYMM CRYPT*, quindi su *Encrypt*. Clicchiamo su *Yes* e poi su *Continua*.



Una parola chiave complessa

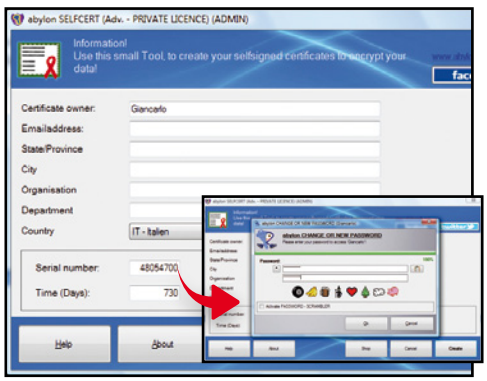
5 Nella schermata successiva digitiamo una password (la lunghezza della striscia verde in alto ne indica la complessità) in entrambi i campi, quindi premiamo il pulsante *Ok*. Al termine confermiamo con *Yes all*. Al termine, tutti i file saranno criptati e protetti da sguardi indiscreti.

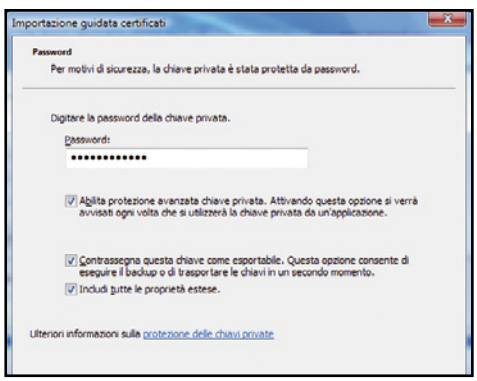
Decriptiamo tutto in un clic

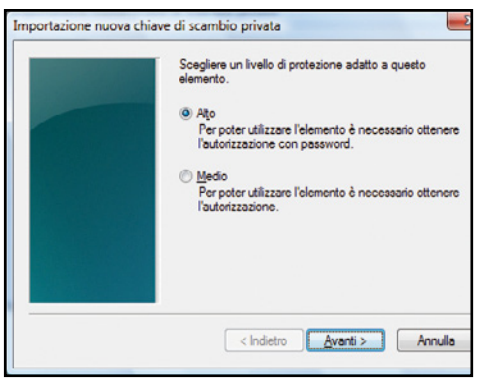
6 Per decriptare uno o più file, selezioniamoli, clicchiamo su di essi con il tasto destro e facciamo clic sulla voce *abylon SYMM CRYPT/Decrypt*. Ci verrà chiesto questa volta di inserire la password usata per la criptazione: digitiamola nell'apposito box e premiamo *Ok*.

Un certificato di sicurezza

7 Per criptare invece dei file utilizzando un certificato di sicurezza, dobbiamo prima crearlo e importarlo in Windows. Clicchiamo due volte sull'icona di abylon BASIC presente in basso sulla system tray e poi facciamo doppio clic sulla voce *abylon SELFCERT*.







Inseriamo i dati e la validità

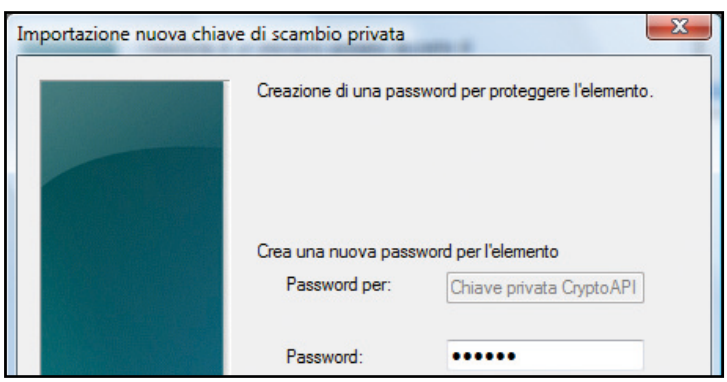
8 Riempiamo i vari campi della schermata con i nostri dati, selezioniamo *IT-Italien* in *Country*, in *Time (Days)* indichiamo i giorni di validità del certificato e proseguiamo con *Create*. Clicchiamo *Yes*, digitiamo in entrambi i box di testo una password per il certificato e diamo *Ok*.

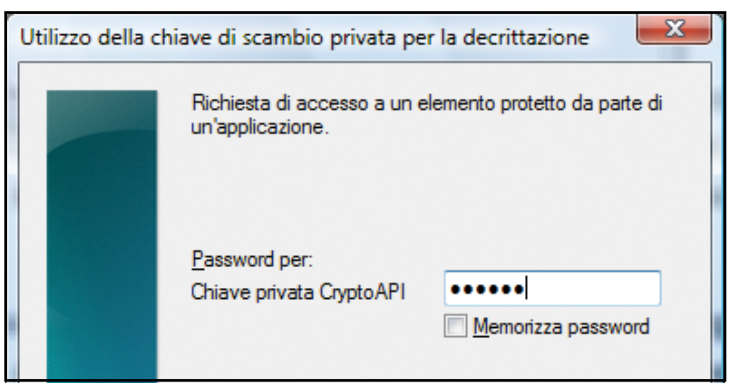
L'importazione del certificato

9 Scegliamo una cartella in cui salvare il certificato, digitiamo un nome e premiamo *Salva*. Clicchiamo *Yes* per importare il file in Windows, quindi premiamo *Avanti*, poi ancora *Avanti*, digitiamo la password del certificato, selezioniamo tutte le opzioni presenti e clicchiamo *Avanti*.

Un livello di protezione elevato

10 Selezioniamo la voce *Mettere tutti i certificati nel seguente archivio* e premiamo *Sfoglia*. Scegliamo *Personale*, quindi confermiamo con *OK* e premiamo *Avanti*, quindi *Fine*. Clicchiamo su *Imposta livello protezione*, selezioniamo *Alto* e premiamo *Avanti*.





Aggiungiamo anche una password

11 A questo punto dobbiamo digitare in *Password* e in *Conferma password* una ulteriore password di protezione che ci verrà chiesta quando decripteremo un elemento. Fatto ciò, completiamo questa fase premendo il tasto *Fine*, quindi clicchiamo su *OK* e poi ancora su *OK*.

E ora criptiamo ogni cosa!

12 Selezioniamo con il tasto destro i file da criptare e clicchiamo su *abylon HYBRID CRYPT/Encrypt*. Per decriptare elementi crittografati con questo metodo, selezioniamoli col tasto destro e clicchiamo su *abylon HYBRID CRYPT/Decrypt*, digitiamo la password del certificato e premiamo *OK*.

Metti al sicuro il tuo Facebook!

Cosa ci occorre

30 MIN. DIFFICILE

SOCIAL NETWORK
FACEBOOK
Quanto costa: **Gratuito**
Sito Internet: **www.facebook.com**

Scopri le tecniche usate dai pirati informatici per violare il social network e impara a difendere la tua identità

Facebook è divenuto negli anni un servizio Web così popolare che sono ormai rimasti davvero in pochi gli internauti che non possiedono un account al social network più famoso del mondo. Del resto questa piattaforma risulta molto comoda agli iscritti per tenersi in contatto tra di loro, postare e condividere immagini e informazioni di ogni genere, ricevere notizie mirate dal Web e molto altro ancora. Come era però facile prevedere, proprio l'enorme successo di Facebook, anche grazie alla diffusione sempre più capillare di dispositivi mobili connessi alla Rete, ha finito per attirare l'attenzione dei pirati informatici che hanno trovato in questa piattaforma un universo sconfinato in cui poter scorrazzare per rubare dati personali e non solo.

I pericoli di Facebook

Forse non ci abbiamo mai pensato, ma la cosa più semplice che ci possa capitare sul social network è, ad esempio, che un malintenzionato ci attiri con un trucco su una finta pagina Facebook per rubarci le credenziali di accesso e poi spiare le nostre attività on-line e utilizzare come più gli pare e piace il profilo e i contenuti in esso presenti. Un'eventualità questa neanche troppo remota, soprattutto per quegli utenti della Rete un po' distratti che non fanno troppo caso alle pagine Web che visitano. Immaginiamo solamente i danni che un estraneo può creare al nostro profilo cancellando e modificando i post in bacheca o semplicemente violando la nostra privacy leggendo cose che prima erano accessibili solo ad un numero ristretto di amici. Viceversa può anche accadere che a nostra insaputa qualcuno, utilizzando uno dei nostri indirizzi di posta elettronica, registri un account su Facebook compiendo un vero e proprio furto d'identità, ovvero spacciandosi per noi sul social network. C'è poi chi, addirittura, si piglia la briga di creare un falso profilo Facebook che viene disattivato dopo qualche ora, giusto il tempo per richiedere e ottenere la nostra amicizia per poter parlare male di noi con tutti i nostri contatti e rovinarci la reputazione. Come difendersi allora da questi pericoli? La soluzione è semplice: basta seguire il famoso adagio che recita "se lo conosci, lo eviti". In ogni caso Win Magazine ti da le indicazioni e gli accorgimenti per evitare di cadere in una di queste "trappole 2.0" e riportare tutto alla normalità nel caso in cui siamo divenuti inconsapevolmente vittime dei pirati di Facebook.

COSÌ I PIRATI METTONO SOTTO SCACCO IL TUO DIARIO

Dal furto del profilo alla creazione di un account a tempo: ecco come uno smanettone può impossessarsi di un profilo Facebook per mettere a repentaglio la nostra privacy e rovinarci la reputazione sul social network.

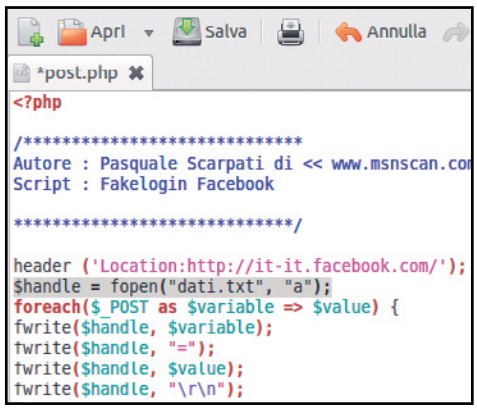
Furto del profilo Facebook
Un pirata informatico può prepararci una trappola sul Web e rubarci con l'inganno le credenziali di accesso al social network. Scopriamo quali sono le tecniche adottate per entrare nel nostro account Facebook e come riprenderne il controllo. pag. 67

Un account non autorizzato
Su Facebook malintenzionati o sistemi automatizzati possono utilizzare un nostro indirizzo e-mail per registrare un falso profilo a noi intestato. In pochi passi possiamo segnalare questo abuso al social network e disattivare l'account. pag. 68

Nuove amicizie, ma a tempo!
C'è chi crea un account temporaneo su Facebook con il solo scopo di fare scherzi o rovinare la reputazione di altri utenti. Per farlo il pirata esegue una registrazione falsa e incompleta al social network. Vi sveliamo tutti i retroscena. pag. 69

Furto del profilo Facebook

Uno dei trucchi più utilizzati dai pirati informatici per rubare le credenziali di accesso al social è quello di creare una falsa home page del sito. Svelati i retroscena.



1 I ferri del mestiere

Il pirata informatico si collega alla pagina http://goo.gl/tLq5Gz ed effettua il download di una falsa home page di Facebook già pronta all'uso, così da non scrivere neanche una riga di codice. Al termine del download estrae il contenuto dell'archivio in formato ZIP sul *Desktop* del suo PC.

2 Tutto all'interno di un file

Il pirata accede quindi alla directory nella quale ha scompattato l'archivio e apre il file post.php con un editor di testo non formattato (ad esempio il *Blocco Note* di Windows) per assegnare un nome al file nel quale verranno memorizzati i dati delle vittime (nel caso in figura *dati.txt*).

3 Una home page fasulla

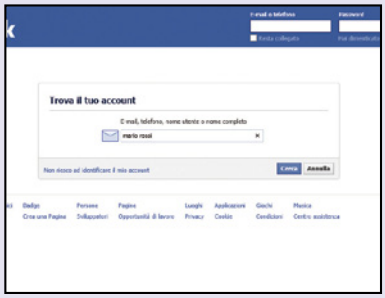
Al pirata non resta quindi che caricare i tre file scompattati nel suo spazio Web (ad esempio uno gratuito su Altervista) e inviare alla vittima un'e-mail col link da raggiungere. La pagina visualizzata, però, non è quella di Facebook, quindi occhio all'indirizzo mostrato nel browser!

COSÌ RECUPERIAMO L'ACCESSO AL NOSTRO DIARIO

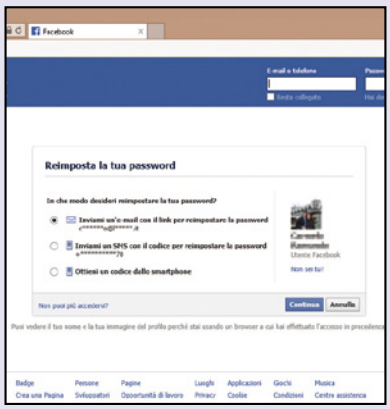
Per quanto il nostro account Facebook possa rivelarsi blindato (dopo aver adottato opportune misure di sicurezza, come ad esempio il passaggio al protocollo HTTPS per l'indirizzo), al mondo esisterà sempre almeno un pirata capace di impossessarsi della nostra identità virtuale. E, nel caso in cui qualcuno sia riuscito a rubarla, non dobbiamo far altro che sperare che non abbia già proceduto al cambio della e-mail di registrazione o del numero di cellulare collegato all'account stesso. Già, perché come ben sappiamo, ad ogni account Facebook è associato un indirizzo di posta elettronica (utilizzato durante la registrazione) sul quale è possibile ricevere oltre che a notifiche di tutti i tipi, anche il modulo che ci permetterà di resettare la nostra password. La stessa procedura può essere effettuata confermando un SMS ricevuto sul nostro telefonino.

PROCEDURA DI RECUPERO

1 Raggiungiamo la pagina di login di Facebook e clicchiamo sul pulsante ***Hai dimenticato la password?***. Compiliamo il campo presente indicando il nostro indirizzo di posta elettronica o, in alternativa, il numero di cellulare fornito a Facebook al momento della registrazione e confermiamo con Cerca. Supponiamo di avere inserito l'indirizzo di posta elettronica e che, dunque, il pirata non abbia variato l'e-mail associata all'account Facebook.



2 Nella nuova pagina che appare possiamo scegliere se ricevere un messaggio nella mailbox contenente un link che ci permetterà di reimpostare con estrema facilità la nostra password o, nel caso di un indirizzo di posta elettronica di Gmail, se verificare la nostra identità tramite il Google Account. Effettuata la nostra scelta proseguiamo con ***Continua*** e apriamo il messaggio che abbiamo appena ricevuto. Il nostro consiglio è quello di settare una password abbastanza complessa (alterniamo numeri a caratteri alfabetici e teniamoci sempre su una lunghezza non inferiore ai 12 caratteri).



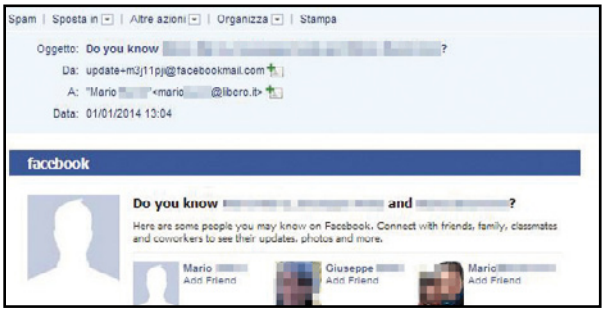
PER SAPERNE DI PIU'

ATTACCHI CON LO SMARTPHONE

All'interno di una rete locale è sufficiente usare un telefonino Android e un'app come FaceSniff per scoprire i dati di accesso a Facebook degli utenti connessi nella LAN che usano il social network. Dal suo telefonino, il malintenzionato, avvia il browser e si sposta in Impostazioni per ripulire Cronologia e cookie. Installa FaceNiff.apk e si connette ad una rete Wi-Fi e avvia FaceSniff. La ricerca di una potenziale vittima ha inizio: se qualche altro utente connesso alla stessa rete senza fili è connesso a Facebook, apparirà nella lista dopo soli pochi secondi. Al pirata basta tappare su uno dei nomi visualizzati per loggarsi con i dati dell'ignaro utente.

Account non autorizzato!

Se qualcuno utilizza un nostro indirizzo e-mail per registrare un falso profilo a noi intestato, dobbiamo subito segnalare l'abuso e disattivare l'account. Ecco come



1 L'e-mail del falso profilo

Un'e-mail che può insospettirci è quella spedita ad un indirizzo non usato per iscriverci a Facebook: cita un nostro profilo e ha contenuti social. Effettuiamo il login a Facebook con il nostro account personale, nella barra di ricerca digitiamo l'e-mail usata per il profilo falso e clicchiamo sulla lente.

2 Facciamo la segnalazione

Sul falso profilo clicchiamo sulla rotellina, scegliamo *Segnala/Blocca*, *Invia una segnalazione/Segnala l'account di NomeUtente* e *Questo diario finge di essere me...* Riceveremo un'e-mail: clicchiamo su https://www.facebook.com/recover/initiate e seguiamo le istruzioni.

3 La password dell'account

Una volta trovato l'account, richiediamo un'e-mail per reimpostare la password. Selezioniamo l'opzione *Inviami un'e-mail con un link per reimpostare la password* e premiamo *Continua*. Riceveremo per posta elettronica un codice: inseriamolo nella nuova pagina e premiamo *Continua*.

4 Prima entriamo nel profilo…

Nella successiva schermata in *Nuova password* digitiamo una nuova password per il profilo. Digitiamo la stessa password anche nel box *Conferma password* e premiamo *Continua*. Quando compare la pagina del falso profilo clicchiamo sulla voce *Disattiva il tuo account* in basso.

5 … e poi disattiviamolo!

In basso selezioniamo l'opzione relativa alla motivazione della disattivazione dell'account, digitiamo nel box di testo una breve spiegazione più dettagliata, spuntiamo la voce *Non ricevere e-mail da Facebook in futuro* e premiamo il pulsante *Conferma*.

6 L'account è fuori uso!

Digitiamo la password scelta al **Passo 4** e facciamo clic su *Disattivare ora*. A questo punto il falso profilo Facebook è disattivato. Riceveremo anche un'e-mail che ci confermerà la disattivazione (l'account sarà comunque riattivabile in qualunque momento cliccando su *Riattiva l'account*).

BUONI CONSIGLI

CAMBIAMO LA PASSWORD!

Quando ci accorgiamo che qualcuno ha usato il nostro indirizzo e-mail per registrare un falso profilo Facebook, è buona norma cambiare immediatamente la password che utilizziamo per accedere all'account di posta elettronica. Oltre ad averci registrato a nostra insaputa su Facebook, infatti, un malintenzionato potrebbe aver violato anche la nostra mailbox!

BACKUP TOTALE DEL PROFILO

Per essere pronti a qualsiasi evenienza, è bene effettuare periodicamente un backup del nostro account Facebook. Per farlo, dalla home page del profilo, in alto a destra, clicchiamo su Impostazioni account, quindi su Impostazioni generali dell'account/ Scarica una copia dei tuoi dati di Facebook/ Avvia al mio archivio. In alternativa possiamo utilizzare la versione free di SocialSafe (lo trovi nel DVD allegato a questo speciale) che fornisce, appena installato e avviato, una chiave di licenza da usare due volte per procedere con l'attivazione del software su due diversi PC. Effettuata l'attivazione, dobbiamo poi installare Adobe Air (seguendo la procedura indicata) e inserire le credenziali del nostro account Facebook. Il backup impiega un tempo variabile in base alle dimensioni e al numero di documenti caricati sul profilo.

Nuove amicizie, ma a tempo!

Incredibile ma vero! Abbiamo scoperto che esiste addirittura la possibilità di aprire e utilizzare, anche se per un tempo limitato, un nuovo account senza completare le registrazione al social network.

1 Impostiamo un profilo facebook a tempo

Colleghiamoci a www.facebook.com e nella sezione *registrazione* inseriamo un indirizzo e-mail qualsiasi (anche fasullo), una password di accesso, impostiamo una data di nascita e dopo aver scelto il sesso clicchiamo su *Registrazione*. Nella schermata successiva clicchiamo su *Salta*.

2 Il falso profilo è stato creato!

Ci verrà data la possibilità di impostare la nostra immagine del profilo. Proseguiamo cliccando su *Salta*. Anche se il processo di registrazione non è stato comletato, potremo fin da subito accedere alla bacheca e utilizzare il falso profilo creato per postare messaggi o chiedere amicizie.

COME SCOVARE UN ACCOUNT FAKE SU FACEBOOK

Ecco una serie di indizi che possono esserci utili per smascherare falsi profili sul social network.

1 IMMAGINI SENZA L'UTENTE

Cerchiamo la persona che ci ha chiesto l'amicizia nell'immagine di copertina e nelle foto del suo profilo. Se riusciamo a scorgerlo solo in pochissime foto, probabilmente vuol dire che le ha rubate dal Web". Per scoprirlo con certezza possiamo ricorrere al software FbChecker (lo trovi sul DVD) che consente di effettuare automaticamente l'analisi delle foto dei profili dei nostri amici e controllare se sono state prese da Internet.

2 AMICI DA TUTTO IL MONDO

Diamo un'occhiata alla lista dei suoi amici: tanto più un account può essere falso quanto più in essa sono presenti persone delle nazionalità più disparate senza un gruppo ben definito. Controlliamo anche quanti amici abbiamo in comune: non averne neanche uno può essere indice di profilo fake.

3 UNA BACHECA QUASI VUOTA

Leggiamo attentamente la bacheca del profilo che ci ha contattato. Se i post, i link e i commenti inseriti dall'utente si contano sulle dita di una mano, probabilmente si tratta di un falso account.

4 IDENTITÀ MISTERIOSE

Sbirciamo tra le informazioni personali dell'account. Generalmente chi crea un account fake lascia tutti i campi in bianco e non perde tempo a compilarli uno ad uno.

5 LA DATA DI NASCITA

Scorriamo la timeline del profilo fino a visualizzare la data di nascita dell'utente. Se è impostata al 1 gennaio oppure al 31 dicembre è probabile che si tratti di un account fake.

6 DOMANDE NEI POST

Se in bacheca sono presenti molte domande del tipo "Per favore, mi dici chi sei?" postate da più utenti, quasi sicuramente l'account che ci ha contattato è fasullo. Eventualmente facciamogli anche noi, tramite messaggio privato, delle domande dirette sulla sua identità. Se non riceviamo nessuna risposta, cominciamo ad insospettirci.

7 CATTIVI BUGIARDI

Chi crea uno o più falsi account di solito dimostra poca coerenza nei contenuti che posta. Può capitare ad esempio che faccia confusione e dica di essere prima di una città e poi di un'altra, oppure si spacci per una persona giovane e dimostri invece una conoscenza approfondita di un'epoca antecedente a quella della data di nascita dichiarata.

8 NESSUN TAG

Chi ci ha chiesto l'amicizia non è stato mai taggato? Una persona reale generalmente è taggato in qualche foto. Se non lo è, allora cominciamo a pensare che si potrebbe trattare di un account falso.

9 MAI AVERE FRETTA

Se non abbiamo la certezza che un profilo Facebook sia reale, non siamo precipitosi a concedergli l'amicizia. Se si tratta infatti di un nostro amico, non tarderà a contattarci tramite messaggio privato per identificarsi di persona e sollecitare la concessione dell'amicizia.

10 GLI AMICI DEGLI AMICI

Se non conosciamo chi ci ha chiesto l'amicizia, prima di rifiutare l'amicizia, verifichiamo se abbiamo un amico in comune sul social network. Potrebbe essere infatti semplicemente un amico di un nostro amico che ha pensato di contattarci perché condividiamo gli stessi gusti musicali.

Antivirus 2015 gratis per te!

Ti regaliamo la miglior suite di sicurezza e la guida pratica per proteggere al meglio il tuo PC

Cosa ci occorre

20 MIN. FACILE

SOFTWARE ANTIVIRALE
G DATA INTERNET SECURITY 2015
SOFTWARE COMPLETO
Lo trovi su: ☑DVD
Sito Internet: www.gdata.it

BUONI CONSIGLI

RIMUOVI IL VECCHIO ANTIVIRUS

Prima di procedere con l'installazione di G Data InternetSecurity 2015 è opportuno rimuovere tutti i software antivirali presenti nel PC. Possiamo direttamente con Windows da *Pannello di controllo/Disinstalla un programma*. In alternativa, possiamo utilizzare i tool di rimozione specifici per ogni antivirus nel DVD-Rom. Al termine della disinstallazione è sempre buona norma ripulire il registro di configurazione di Windows con un programma come CCleaner (lo trovi nel DVD allegato a questo speciale), cliccando su *Registro/Trova Problemi* e poi su *Ripara selezionati*.

Passano gli anni, i computer diventano a mano a mano più potenti e sofisticati, ma il pericolo virus è sempre dietro l'angolo. Avere un sistema operativo sempre aggiornato con le ultime patch rilasciate, fare attenzione a non aprire allegati ricevuti con le e-mail, non eseguire mai file .exe di cui non conosciamo l'autore e la provenienza sono sicuramente precauzioni che possono aiutarci ad evitare disastrose infezioni. Il problema è però che le trappole e le possibilità di beccare un virus o un trojan navigando su Internet sono tante e tali che basta poco per divenire vittima di un malware. In caso di infezione, lo sappiamo bene, le conseguenze possono essere le più diverse, dal "semplice" blocco del PC all'impossibilità di connettersi ad Internet, se non addirittura la corruzione e la cancellazione definitiva di documenti importanti e file di sistema o il furto di dati sensibili come informazioni di accesso bancari e numeri di carte di credito, con tutte le conseguenze del caso.

Protezione massima per il PC

Senza un buon programma antivirus il nostro computer è pertanto esposto a ogni genere di minaccia esterna. Per questo motivo noi di Win Magazine abbiamo deciso di regalare ai nostri lettori la suite G Data InternetSecurity 2015, gratuita per 180 giorni, utile per blindare il PC e renderlo praticamente invulnerabile ad ogni attacco di virus e hacker. Utilizzando questo programma potremo infatti analizzare i messaggi di posta elettronica alla ricerca di allegati dannosi e link di phishing, bloccare automaticamente tutte le e-mail di spam, attivare un potente firewall che renda inaccessibile ogni accesso non autorizzato al nostro computer ed eseguire un efficace controllo parentale per proteggere i bambini dai siti Internet pericolosi. Vediamo subito come fare.

G DATA: LA MIGLIOR DIFESA POSSIBILE DA VIRUS E MALWARE

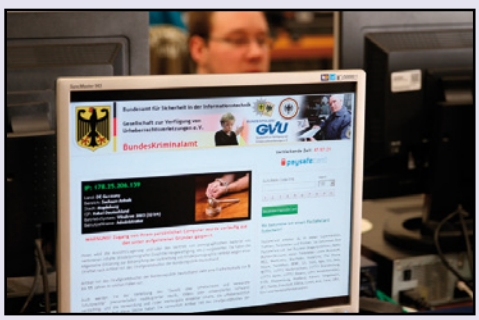
Per scegliere l'antivirus in grado di offrire la protezione migliore al nostro computer e ai dati in esso archiviati abbiamo messo sotto torchio, nei nostri laboratori, le migliori suite di sicurezza disponibili sul mercato, sia quelle commerciali sia quelle gratuite. I risultati sono stati molto interessanti, ma alla fine la vincitrice come miglior rapporto qualità/prezzo è stata proprio la suite G Data InternetSecurity 2015. L'efficiente protezione antivirus consente di assegnare un 10 e lode al programma di G Data, che non lascia scampo neppure ai virus più insoliti. Nessun altro programma ha bloccato in modo così veloce le nuove minacce. Nel corso del test, la suite ha riconosciuto immediatamente la maggior parte dei virus sconosciuti o solo dopo alcune ore dalla loro comparsa. Il programma è in grado di offrire queste straordinarie prestazioni grazie all'impiego di due scanner per virus che interagiscono perfettamente tra loro.

- Rischio di infezione con prevalenza di virus attuali (10.231 campioni) **0%**
- Rischio di infezione con virus finora sconosciuti **20,00%**
- Percentuale di riconoscimento di virus datati (283.987 campioni) **99,51%**
- Protezione da siti Web infetti, download, e-mail e pendrive USB **98,15%**
- Percentuale di riconoscimento **99,73%**
- Falsi allarmi attivi con programmi / falsi allarmi per i file **0%/0,001%**

I TEST DI WIN MAGAZINE

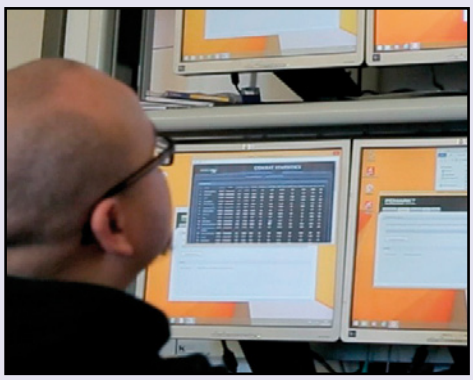
ANALISI DI QUASI 300.000 VIRUS

Per quattro settimane,abbiamo sottoposto a test severissimi le funzioni antivirus di programmi e app per la sicurezza. Sono stati utilizzati complessivamente 294.307 virus, impiegandone 10.231 per infettare i PC usati per il test. L'aspetto importante non era il corretto riconoscimento dei virus, bensì verificarne la loro efficace rimozione.



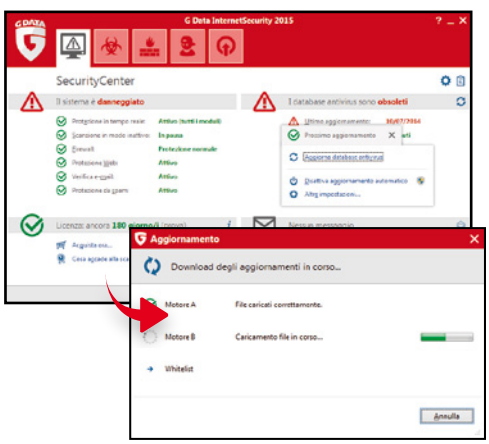
OLTRE 2.500 ORE DAVANTI AL PC

I programmi antivirus, si sa, rallentano la velocità del computer. Per quantificare il reale consumo di risorse di sistema abbiamo tenuto sotto controllo questo aspetto su otto PC per oltre due settimane. Sono stati eseguiti svariati benchmark, sono stati analizzati i tempi necessari per le copie di riserva ed è stata bloccata la possibilità di richiamare pagine Internet.



Installa e attiva la suite di sicurezza

Ecco la procedura da seguire per configurare la versione a 180 giorni di G Data InternetSecurity 2015. Al termine è necessario attivare via Internet il programma per usare tutte le sue funzioni senza limiti.



1 Una semplice installazione

Scompattiamo l'archivio *GData.zip* che troviamo nel DVD allegato a questo speciale ed eseguiamo il file *EXE* contenuto al suo interno. Nella prima schermata del Wizard di installazione selezioniamo l'opzione *Installazione standard* e clicchiamo *Avanti* per proseguire.

2 Attiviamo la nostra copia

Clicchiamo sul pulsante *Accetta & Installa* per proseguire con la procedura di installazione completamente automatica e che durerà soltanto pochi minuti. Al termine, clicchiamo sul pulsante *Attiva versione di prova* e, quando richiesto, clicchiamo *Esci* per riavviare il computer.

3 Aggiornamento in corso

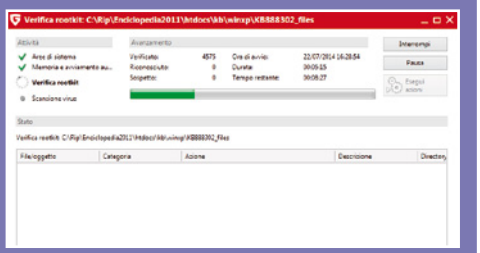
Al successivo riavvio di Windows clicchiamo due volte sull'icona di G Data InternetSecurity 2015 nella system tray per avviare il pannello di controllo della suite. A destra selezioniamo *Prossimo aggiornamento* e poi *Aggiorna database virus*. Al termine, clicchiamo *Chiudi*.

FUNZIONI DI PROTEZIONE

PROTEZIONE ANTIVIRUS

Da qui è possibile eseguire una scansione completa del computer o sapere quali sono i file in quarantena

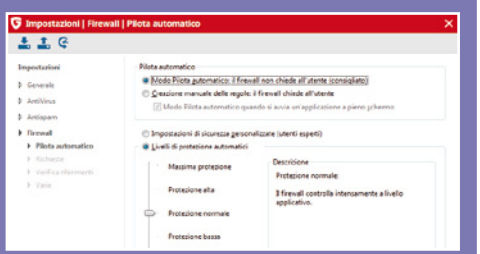
Pagina 73



FIREWALL

Permette di configurare un vero e proprio sistema di sicurezza contro ogni intrusione non autorizzata al computer

Pagina 74



PROTEZIONE MINORI

Grazie al parental control è possibile proteggere i nostri bambini dai contenuti inadeguati pubblicati su Internet

Pagina 74

AUTOSTART MANAGER

È possibile configurare Microsoft Windows scegliendo quali applicazioni caricare all'avvio e quali no

Pagina 75

ECCO COME METTERE AL SICURO IL NOSTRO PC

Diamo uno sguardo all'interfaccia principale di G Data InternetSecurity 2015 per conoscere e imparare ad utilizzare al meglio i principali comandi.

LICENZA

Indica il periodo di validità del software. Qualche giorno prima della scadenza, un messaggio ci ricorderà di rinnovare la registrazione del software

EFFETTUIAMO UNA PRIMA

Terminata l'installazione e l'attivazione della suite di sicurezza è opportuno effettuare un primo controllo del sistema per individuare e debellare eventuali virus e malware che si nascondono tra le cartelle e i file dell'hard disk. La procedura da seguire è semplicissima e al termine avremo la certezza di un sistema "pulito" e sicuro. Avviamo il Pannello di controllo di G Data InternetSecurity 2015 cliccando due volte sull'icona della suite che troviamo nella system tray di Windows,

STATO
Da qui è possibile monitorare il corretto funzionamento dell'antivirus

IMPOSTAZIONI
Cliccando su questo pulsante accediamo a tutti i menu di configurazione della suite G Data

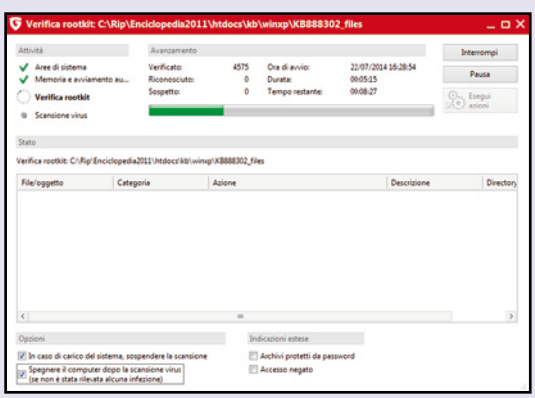
LOG
In ogni momento è possibile avere un resoconto dettagliato sull'attività dell'antivirus e degli altri moduli della suite

AGGIORNAMENTI
Basta un clic per scaricare le nuove firme dei virus

MESSAGGI
Permettono di ricevere costantemente informazioni sulla sicurezza del computer e altre utili notizie inviate direttamente da G Data

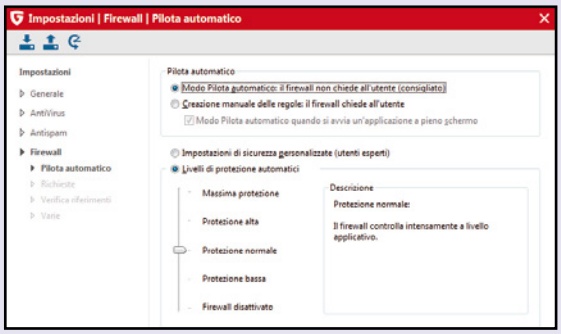
SCANSIONE DEL NOSTRO HARD DISK

vicino all'orologio di sistema. Spostiamoci quindi nella sezione ***Protezione antivirus*** e clicchiamo su ***Verifica computer (tutti i dischi fissi locali)***. Partirà automaticamente la scansione di tutti gli hard disk installati nel PC. La procedura potrebbe richiedere molto tempo e consumare parecchie risorse di sistema. Conviene quindi eseguirla quando non utilizziamo il PC: in questo caso, attiviamo la voce ***Spegnere il computer dopo la scansione virus*** (se non è stata rilevata alcuna infezione). Nella stessa schermata di controllo della scansione spuntiamo, inoltre, anche l'opzione In caso di carico del sistema, sospendere la scansione così da evitare eventuali surriscaldamenti o blocchi del sistema. Qualora venissero individuati virus o altre minacce, G Data InternetSecurity 2015 ci suggerirà come procedere: nella schermata di rimozione sarà sufficiente selezionare l'Azione consigliata per eliminare il virus o spostarlo in quarantena.



NESSUNO PUÒ ENTRARE DI NASCOSTO NEL MIO COMPUTER

Il Firewall integrato nella suite G Data InternetSecurity 2015 è attivato di default. Possiamo comunque personalizzarne il funzionamento per adattarlo alle nostre esigenze. Dalla schermata principale del modulo clicchiamo su ***Protezione*** e poi su ***Modifica impostazioni di sicurezza*** nel menu contestuale che appare. Nella nuova schermata possiamo scegliere la ***Creazione manuale delle regole*** oppure lasciare attivo il ***Modo Pilota automatico***: nel primo caso, il firewall ci chiederà quale azione intraprendere ogni qualvolta verrà individuato un tentativo di intrusione nel nostro sistema. Il ***Pilota automatico***, invece, procederà in totale autonomia. Dalla sezione ***Livelli di protezione automatici***, invece, possiamo scegliere l'opzione ***Firewall disattivato*** (ovviamente non consigliata) oppure scegliere il livello di protezione preferito, scegliendo un buon compromesso tra un efficace controllo e una buona libertà di navigazione su Internet.



Bambini protetti su Internet

Impariamo a configurare correttamente il parental control di G Data InternetSecurity 2015 per fare in modo che i nostri figli possano navigare al sicuro da contenuti Web non adatti alla loro età.

1 Un account per ogni figlio

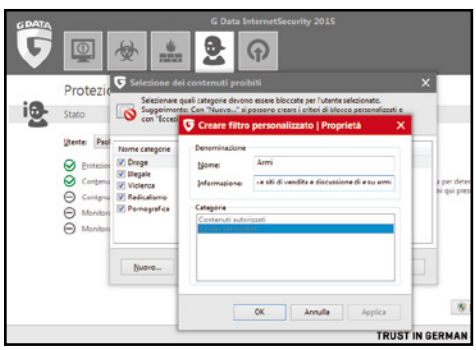
Per usare il modulo *Protezione minori* è opportuno creare un account di Windows per ogni utente. Possiamo farlo dal menu *Start* di Windows selezionando *Pannello di controllo/Account utente e protezione famiglia/Account utente*) oppure direttamente da G Data cliccando *Nuovo utente*.

2 Ad ognuno il suo accesso

In *Aggiungi nuovo utente* scegliamo un *Nome utente*, assegniamogli una *Password*, digitiamola per sicurezza anche in *Ripeti password* e clicchiamo *Applica*. Ripetiamo la procedura per ogni nostro figlio. Il modulo di protezione verrà automaticamente attivato su questi nuovi utenti.

3 Filtri su misura

Tornati nella schermata di *Protezione bambini* selezioniamo l'account da proteggere dal menu a tendina *Utente*. Il modulo risulta già configurato: se vogliamo personalizzarlo ulteriormente, clicchiamo su una delle voci presenti (ad esempio *Contenuti proibiti*) e poi su *Modifica*.

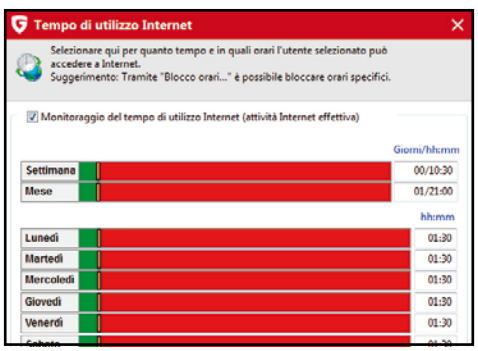


4 Blocchiamo altri contenuti

In *Selezione dei contenuti proibiti* sono già selezionate le categorie di contenuti Web potenzialmente pericolosi per i minori. Per creare un *Filtro personalizzato* clicchiamo *Nuovo*, scegliamo una *Denominazione* e la categoria di appartenenza (nel nostro caso: *Contenuti proibiti*).

5 Ricerche impossibili

Clicchiamo *OK*. In *Modifica dei contenuti proibiti* diamo un nome al *Filtro*. Da *Luogo per la ricerca* spuntiamo le opzioni per bloccare le ricerche on-line in base all'URL, al *Titolo della pagina Web* o al suo contenuto e clicchiamo *Aggiungi*. Confermiamo le modifiche con *Applica* e *OK*.

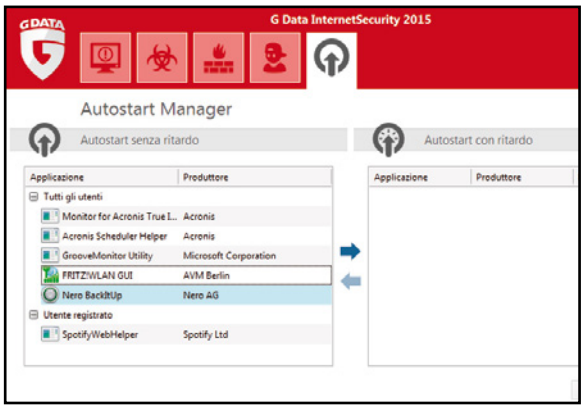


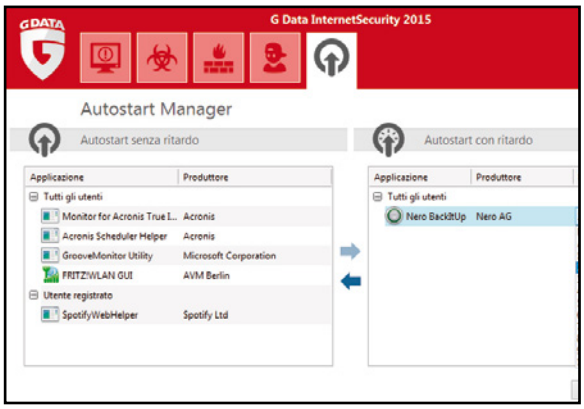
6 L'uso del PC è limitato

Possiamo anche limitare l'uso del computer o di Internet ai nostri figli. Clicchiamo, ad esempio, su *Monitorare il tempo di utilizzo di Internet* e poi *Modifica*. Spuntiamo *Monitoraggio del tempo* e impostiamo le ore e i minuti di utilizzo massimo per ogni giorno, settimana o mese.

Windows al fulmicotone

Grazie all'Autostart Manager del software è possibile configurare le applicazioni che vengono caricate automaticamente da Windows, così da ottimizzare la fase di boot del PC.





1 L'elenco dei programmi

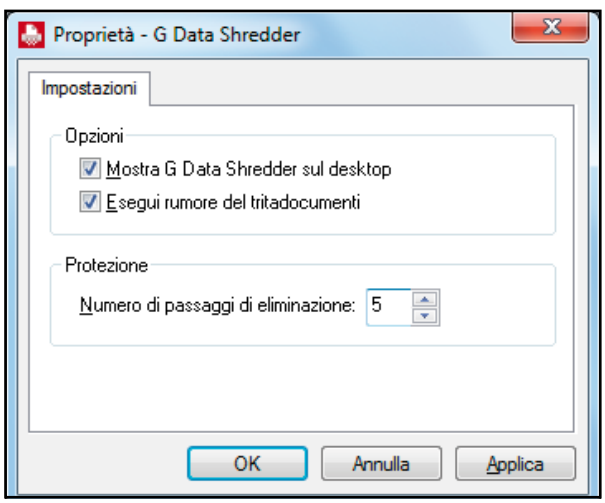
Spostiamoci nella sezione *Autostart Manager* e concentriamo la nostra attenzione sull'elenco di programmi in *Autostart senza ritardo*: sono tutti quelli che vengono caricati all'avvio di Windows rallentando inutilmente il sistema. Selezioniamo quello che non ci interessa e clicchiamo sulla freccia blu verso destra.

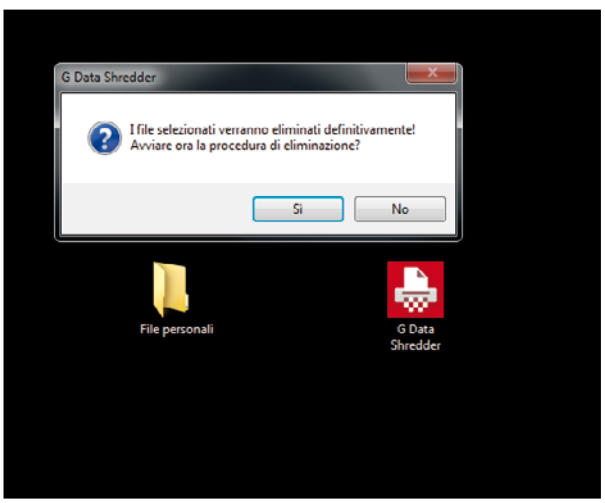
2 Esecuzione ritardata

Spostiamoci in *Autostart con ritardo*: per ogni software aggiunto a questo elenco sarà disponibile la voce *Ritardo*. Clicchiamo sul menu a tendina corrispondente e selezioniamo il ritardo con cui avviare il programma stesso: *Non avviare* ne bloccherà completamente l'esecuzione automatica. Al termine clicchiamo *Salva*.

Cancellazioni sicure

Insieme alla suite G Data viene installato anche il tool Shredder che permette di eliminare file e cartelle dal disco in maniera sicura, impedendo ogni tentativo di recupero. Ecco come utilizzarlo.





1 Attiviamo il "tritatutto"

Terminata l'installazione della suite G Data InternetSecurity 2015, sul Desktop di Windows comparirà l'icona G Data Shredder. Cliccandoci sopra due volte apparirà la sua semplice interfaccia grafica. Lasciamo i due segni di spunta sulle voci presenti all'interno della sezione *Opzioni*.

2 Cancellazione in corso

Scegliamo il *Numero di passaggi di eliminazione* (cioè quante volte i file verranno sovrascritti per cancellarne ogni traccia): quanto più è alto, tanto più difficile sarà il recupero. Clicchiamo *OK*. Basta ora trascinare un file sull'icona di Shredder per cancellarlo definitivamente!

BUONI CONSIGLI

E-MAIL SENZA SPAZZATURA

Come ogni buona suite che si rispetti, anche G Data InternetSecurity 2015 integra un ottimo modulo antispam, che si attiva automaticamente al primo avvio dell'antivirus. I filtri predefiniti riescono a bloccare praticamente tutta la spazzatura proveniente dal Web, ma è possibile comunque personalizzarli ulteriormente o configurarli secondo le proprie esigenze. Dal Pannello di controllo della suite clicchiamo *Impostazioni*, spostiamoci nella sezione *Antispam* e, nella relativa schermata, definiamo le modalità di filtraggio delle e-mail ricevute con il proprio client di posta elettronica.

UN BACKUP DELLE IMPOSTAZIONI

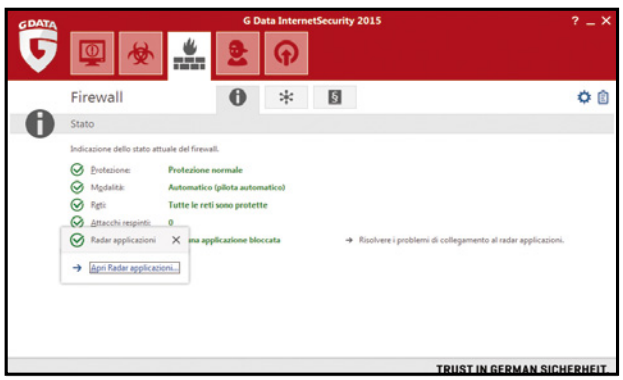
G Data InternetSecurity 2015 permette di creare un backup dei file di configurazione, così da ripristinarli velocemente in seguito ad una nuova installazione del software. Per crearlo, dal Pannello di controllo della suite clicchiamo su *Impostazioni*. Nella nuova schermata premiamo il pulsante in alto a destra *Salva impostazioni*. Scegliamo dove archiviare il file *GDataSettings.gds* e clicchiamo *Salva*. Per ripristinarlo basterà, ovviamente, cliccare sul pulsante *Carica impostazioni*. Con *Ripristina impostazioni*, invece, possiamo riportare la suite alla configurazione di default.

TRUCCHI VELOCI PER G DATA INTERNETSECURITY 2015

1 ACCESSO CONSENTITO A INTERNET

Dopo l'installazione di G Data InternetSecurity 2015 alcuni programmi non riescono più ad accedere al Web. Cosa può essere successo?

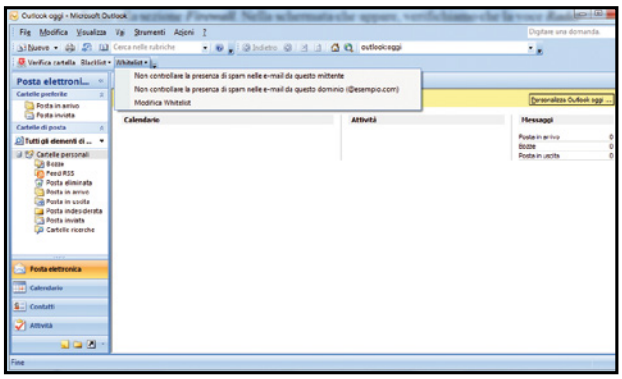
È probabile che il firewall integrato nella suite G Data abbia modificato i permessi di esecuzione del programma bloccando di fatto l'accesso a Internet. Avviamo il *Pannello di controllo* della suite e accediamo alla sezione *Firewall*. Nella schermata che appare, verifichiamo che la voce *Radar applicazioni* sia impostata su *Nessuna applicazione bloccata*. In caso contrario, clicchiamoci su e poi selezioniamo *Apri Radar applicazioni*. Quindi, nell'elenco che appare individuiamo l'applicazione che non accede più a Internet, selezioniamola e clicchiamo su *Autorizza*.



2 RIPULIRE LA MAILBOX DAI VIRUS

Una scansione eseguita con G Data InternetSecurity ha rilevato un virus nel file Outlook.pst, che però non è stati rimosso. Ho allora provato a spostare il file in quarantena, ma così facendo non riesco più ad accedere alle mie e-mail. Come faccio a sbarazzarmi del virus senza perdere i miei messaggi di posta?

Il file *PST* rappresenta l'intero archivio di posta elettronica gestito da Outlook: spostandolo in quarantena eliminiamo, di fatto, tutta la posta scaricata dal client. Non serve, quindi, eseguire una scansione su tutto il database, ma sulle singole e-mail. Per risolvere il problema, avviamo Outlook: nella barra dei menu dovrebbe essere presente la toolbar di G Data InternetSecurity 2015. Clicchiamo quindi sul pulsante *Verifica cartella*. L'antivirus avvierà un controllo approfondito di tutta la Mailbox: eventuali messaggi infetti verranno individuati e segnalati prontamente. Per eliminarli, selezioniamoli e clicchiamo *Elimina*. Le e-mail infette verranno

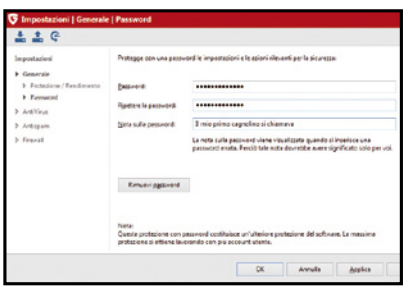


spostate nel cestino e la mailbox verrà completamente ripulita.

3 UNA PASSWORD PER LA SUITE

Il mio computer viene utilizzato da più persone e ho il timore che qualcuno, anche involontariamente, possa modificare la configurazione di G Data InternetSecurity 2015 esponendo così i miei dati a virus e malware di ogni genere. Posso proteggere l'accesso alla suite con una password?

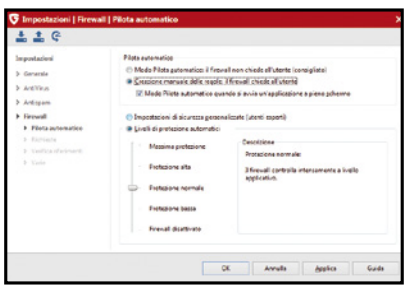
È sempre buona norma proteggere l'accesso alla suite di sicurezza con una password. È possibile farlo anche con G Data InternetSecurity 2015. La procedura da seguire è semplicissima. Dal *Pannello di controllo* della suite (avviabile cliccando due volte sull'icona che appare nella system tray, vicino all'orologio di sistema) clicchiamo su *Apre le impostazioni* (il pulsante a forma di ingranaggio in alto a destra). Nella nuova schermata spostiamoci nella sezione *Generale* e clicchiamo su *Password*. Compiliamo quindi i campi *Password* e *Ripetere la password con una chiave di accesso a nostra scelta*. Nel campo *Nota sulla password* indichiamo una domanda segreta alla quale solo noi sappiamo rispondere e che ci verrà posta qualora, effettuando in futuro l'accesso al pannello di controllo della suite, dovessimo dimenticare la chiave di accesso, aiutandoci così a ricordare la password. Quindi, clicchiamo *Applica* e *OK* per tornare al pannello di controllo della suite.



4 UN FIREWALL SU MISURA

È possibile personalizzare il funzionamento del firewall di G Data InteretSecurity 2015 per monitorare l'accesso a Internet dei programmi installati nel computer?

La suite G Data offre una configurazione predefinita del firewall che garantisce già una protezione efficace contro eventuali accessi non autorizzati al sistema. È comunque possibile personalizzare il funzionamento del programma secondo le proprie esigenze. Dal *Pannello di controllo* della suite clicchiamo su *Apre le impostazioni* (l'icona a forma di ingranaggio in alto a destra) e, nella schermata che appare, spostiamoci nella sezione *Firewall*. Quindi, in *Pilota automatico*, attiviamo la voce *Creazione manuale delle regole*: il firewall chiede all'utente. In questo modo, ogni volta che un programma tenterà di accedere a Internet, il firewall chiederà all'utente di fornire o meno l'autorizzazione.



5 NIENTE SPAZZATURA NELLA POSTA

Capita di ricevere e-mail di spam nonostante il filtro per il controllo della posta elettronica sia attivo. Come fare a bloccare questi messaggi spazzatura dalla mailbox?

Gli spammer e i pirati informatici cercano sempre nuovi modi per invadere le nostre caselle di posta elettronica con inutili e-mail spazzatura. Il filtro antispam di G Data InternetSecurity 2015 viene costantemente aggiornato con l'elenco di nuove parole chiave che permettono di identificare correttamente lo spam, ma ovviamente non è possibile avere un controllo preciso al 100%. Possiamo però intervenire manualmente aggiungendo manualmente a questo elenco le keyword che riteniamo opportune. Dal *Pannello di controllo* della suite clicchiamo su *Apre le impostazioni* (l'icona a forma di ingranaggio in alto a destra) e, nella schermata che appare, spostiamoci nella sezione *Antispam/Filtro antispam*. Clicchiamo su *Usa parole chiave* (testo messaggio). Nella finestra che appare clicchiamo *Nuovo* e aggiungiamo la keyword nel campo *Parola chiave*, confermando con *OK*. ■

Questa foto è stata ritoccata!

✓ Come faccio a capire se un'immagine digitale è stata manomessa ad arte utilizzando Photoshop?

✓ Posso scoprire i tool usati per modificare uno scatto?

SERVE A CHI...
... vuole analizzare col computer una foto per verificare se si tratta di un fake

Quella foto è vera oppure si tratta di un fotomontaggio? È questa la domanda che sicuramente molte volte ci siamo posti quando abbiamo visto la foto di un personaggio famoso in TV, su una rivista oppure su un sito Internet. Oggi grazie alla tecnologia è sempre più facile creare delle immagini manipolate che sembrano in tutto e per tutto realistiche, capaci di ingannare anche gli occhi dei più esperti. La falsificazione delle immagini non è però solo esclusiva del mondo dello spettacolo, in cui si pratica quasi sempre il fotoritocco per nascondere le imperfezioni fisiche delle celebrità, ma viene sempre più usato anche dai politici che vogliono dare una "ripulita" alla propria immagine.

Come individuare i "fake"

Come fare allora per riconoscere una foto falsa da una vera? A tale scopo nasce Izitru, il sistema di verifica che si applica solamente al formato di compressione JPEG, il più usato in commercio. Izitru impiega una combinazione di sei criteri per scovare un'eventuale intervento manipolativo. Il software controlla che tipo di macchina fotografica o fotocamera è stata usata, come il file è stato compresso e se sia stato salvato più volte e, quindi, contraffatto. Una volta terminata l'analisi, il programma restituisce una valutazione che varia da un punteggio massimo di conformità al test ***high trust*** ad un rating ***no trust***, che indica un'immagine con chiari segni di alterazione. Ogni foto che viene inserita resta conservata sul sito in una pagina con un indirizzo univoco che è possibile condividere tramite e-mail o attraverso i social network. Gli utenti, peraltro, possono collaborare ai risultati segnalando con il pulsante ***Challenge*** anomalie e particolari sospetti che sono sfuggiti all'esame della macchina. Izitru, tuttavia, non ha efficacia in caso di contraffazione della scena al momento dello scatto e di immagine ricatturata, cioè nel caso ci si trovi davanti ad una fotografia di un'altra foto modificata. Certo, una sicurezza che la foto sia genuina al 100% è impossibile: anche analizzando tutti i metadati a disposizione resta comunque difficile avere una certezza granitica. Grazie a questi strumenti però ci si può avvalere di un'ottima base sui cui fondare un'eventuale indagine.

UN'ANALISI APPROFONDITA DELLE FOTO
I metadati EXIF contenuti nelle foto digitali sono un'ottima fonte di indizi per cercare indizi su un eventuale uso di software di editing. Un ottimo tool in grado di esaminare a fondo questo tipo di dati è sicuramente JPEGsnoop (www.winmagazine.it/link/2642). Questo software infatti, analizzando anche la compressione, l'istogramma dei colori e altri parametri, consente di verificare con ragionevole certezza se una foto che ad occhio nudo non mostra alcuna manipolazione è stata modificata per correggere delle imperfezioni o anche solo per migliorarne il contrasto. Terminata l'analisi, il software ci rivelerà se la foto è classificabile come ritoccata o meno.

Così scopri se una foto digitale ha subito qualche ritocco con Photoshop

1 Per analizzare una foto sarà sufficiente andare sul sito www.izitru.com. Come funziona? Semplice, una volta caricata, la foto 'incriminata' verrà inviata ai server di Izitru che eseguiranno una serie di controlli per scoprire eventuali manomissioni al file tramite Photoshop.

2 Come prima cosa clicchiamo ***Upload Image*** per aprire una finestra dalla quale scegliere l'immagine che vogliamo sottoporre al controllo anticontraffazione. Basteranno pochi secondi (dipenderà dalla linea ADSL e dalla grandezza della foto) e inizierà lo scanning del file.

3 Ecco il verdetto: notiamo la scritta ***High Trust-Original file from camera*** con un bollino verde che testimonia la "purezza" dell'immagine. Ciò vuol dire che nessuna modifica è stata apportata con Photoshop. Nel caso di fake apparirà la scritta ***Potential file modification***.

L'e-mail più furba che c'è!

Ecco il trucco per scoprire se i tuoi messaggi di posta vengono effettivamente letti

Cosa ci occorre

30 MIN. FACILE

SERVIZIO WEB
streak
Quanto costa: Gratuito
Sito Internet: www.streak.com

SERVIZIO WEB
BANANATAG
Quanto costa: Gratuito
Sito Internet: http://bananatag.com

APP IOS
MAILTRACKER
Quanto costa: Gratuito
Sito Internet: ttps://itunes.apple.com

Internet consente a miliardi di utenti di tutto il pianeta di comunicare e scambiare tra di loro informazioni in tempo reale. Uno degli strumenti più utilizzati a tale scopo è sicuramente la posta elettronica. Il problema è però che non sempre si può essere sicuri che i messaggi inviati tramite e-mail siano stati letti dai destinatari. Con alcuni client è possibile inserire una notifica di lettura, ma non è detto che il ricevente la invii al mittente una volta letto il messaggio. Ci sono, però, diversi servizi che permettono di monitorare le e-mail e ci avvisano quando queste vengono aperte dal destinatario. Se abbiamo bisogno di sapere se i destinatari hanno ricevuto comunicazioni importanti, questi servizi di monitoraggio sono in grado di fornirci tutte le informazioni di cui abbiamo bisogno. Alcuni sono totalmente gratuiti, altri, invece, prevedono piani di abbonamento cui solitamente aggiungono altre funzionalità come la pianificazione dei messaggi, il monitoraggio di link e allegati, e altro ancora.

I servizi pronti sul Web

Se abbiamo un account Gmail, tra i migliori servizi che ci permettono di tracciare le e-mail c'è sicuramente Streak che si usa attraverso il browser installando un'estensione gratuita. Si tratta di un servizio completo che offre diverse funzionalità studiate per migliorare la produttività dei professionisti. Una di queste è appunto quella chiamata Email Tracking che permette di sapere quando qualcuno ha letto le nostre e-mail. Streak ci permette quindi di sapere quando un destinatario ha aperto la nostra e-mail. È anche possibile vedere l'intera storia di quando, dove e quante volte i riceventi hanno aperto il messaggio. Possiamo monitorare gratuitamente fino a 200 e-mail al mese, ma condividendo Streak con almeno 5 amici avremo un monitoraggio illimitato.

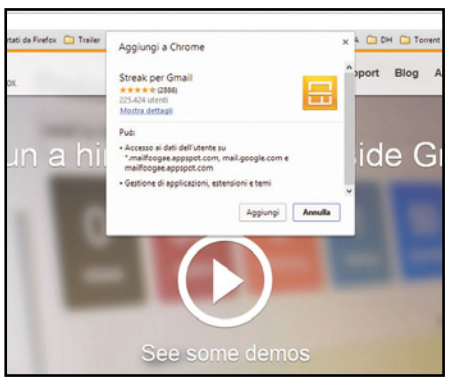
Ci sono anche altre utili funzioni come Send Later che consente di programmare le e-mail per inviarle in futuro. Se invece utilizziamo Microsoft Outlook, allora possiamo servirci del plug-in Bananatag.

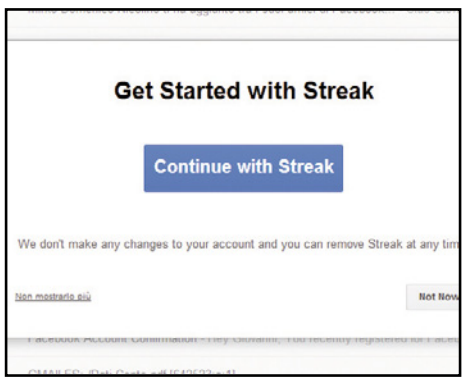
Il tracciamento è mobile!

Sono sempre di più le persone che utilizzano il proprio smartphone per inviare i messaggi di posta elettronica. Se anche noi siamo tra questi e abbiamo un iPhone, possiamo controllare la lettura delle e-mail utilizzando l'applicazione gratuita per iOS MailTracker. Una volta installata e configurata, potremo continuare a utilizzare sempre l'applicazione nativa Mail per inviare i messaggi mentre MailTracker ci servirà solo per controllare l'apertura delle e-mail da parte dei destinatari. Quando questo avviene, riceveremo sul nostro dispositivo una notifica che poi ci permetterà di conoscere maggiori dettagli come informazioni sulla località e sul dispositivo utilizzato per la lettura del messaggio, il numero di volte che è stata letto e altro. Nella versione gratuita MailTracker ci permette di monitorare un massimo di due account. Vediamo subito come fare.

Tracciamo la posta di Gmail

Installando l'estensione gratuita Streak per Google Chrome e Safari possiamo monitorare direttamente dal browser l'invio di una nostra e-mail e verificare se è stata letta dal destinatario.





1 Un'estensione per il browser

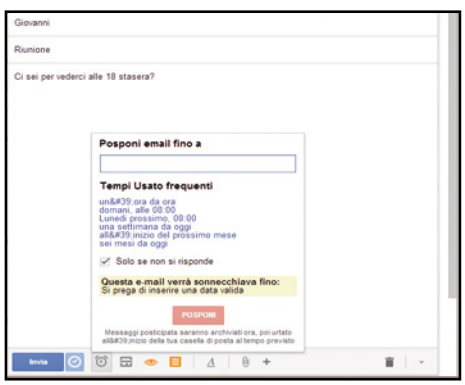
Avviamo il browser (al momento sono supportati Chrome e Safari), andiamo su www.streak.com e clicchiamo su *Install Streak for Gmail*. Nella finestra *Aggiungi a Chrome* confermiamo cliccando su *Aggiungi*: in pochi secondi l'estensione sarà aggiunta e verremo reindirizzati su Gmail.

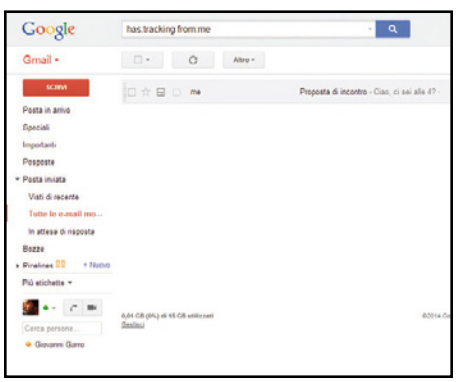
2 Attiviamo il plug-in

Eseguiamo l'accesso con l'account di Gmail da tracciare inserendo l'indirizzo di posta elettronica e la password. Una volta entrati nella nostra casella di posta, ci comparirà una finestra al centro con scritto *Get Started with Streak*. Clicchiamo quindi su *Continue with Streak*.

3 Questione di autorizzazioni

Una nuova finestra ci mostrerà i dati a cui cerca di accedere l'estensione. Per proseguire clicchiamo su Accetto per fornire i permessi e accedere definitivamente alla nostra casella di posta. Una finestra ci chiederà in cosa Streak può aiutarci: clicchiamo su *Blank* e proseguiamo.





4 Un nuovo messaggio

Ora possiamo tracciare le e-mail che inviamo. Per farlo, clicchiamo su *Scrivi* per creare un nuovo messaggio. Accanto al tasto *Invia*, sono disponibili una serie di nuovi pulsanti. Cliccando su quello a forma di occhio facendolo diventare arancione abilitiamo il monitoraggio per l'e-mail.

5 Posporre l'invio

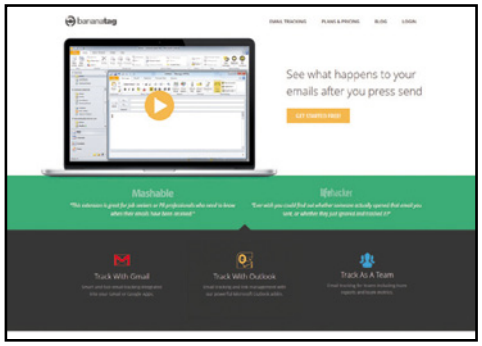
Con Streak è anche possibile posporre l'invio di un messaggio a una data specifica. Dopo averlo composto, non dobbiamo far altro che cliccare sul tasto con la sveglia e impostare il giorno e l'ora. Fatto ciò, clicchiamo su *Invia* per completare l'invio del messaggio di posta.

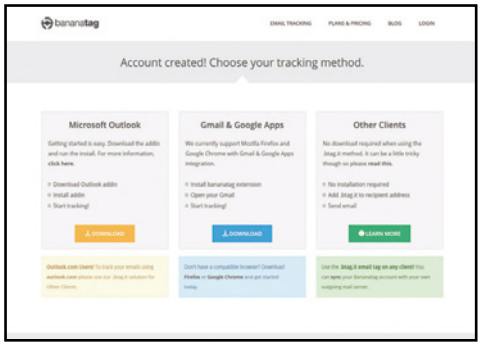
6 Notifiche di lettura

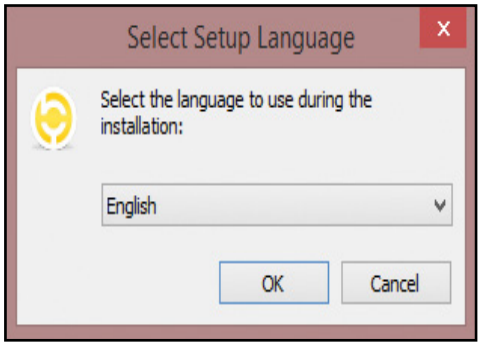
Se abbiamo attivato le notifiche nel browser, quando il messaggio verrà letto, comparirà una notifica nella taskbar di Windows. Possiamo monitorare la ricezione delle e-mail andando nella cartella *Posta inviata*. Se l'occhio accanto al messaggio è colorato, l'e-mail è stata letta.

Monitorare le e-mail da Outlook

Installando il plug-in Bananatag possiamo controllare con il client Microsoft tracciare i messaggi di posta elettronica da noi inviati e ricevere automaticamente le conferme di lettura.







1 Effettuiamo la registrazione

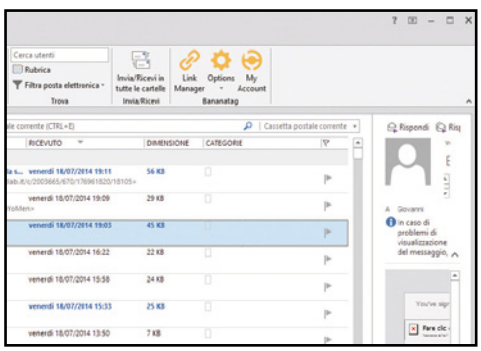
Andiamo su http://bananatag.com e clicchiamo su *Get Free Account*. Saremo reindirizzati alla pagina di registrazione. Compiliamo i campi con il nostro nome e cognome, l'indirizzo e-mail e scegliamo una password di almeno 8 caratteri. Clicchiamo su *Sign Up* per proseguire.

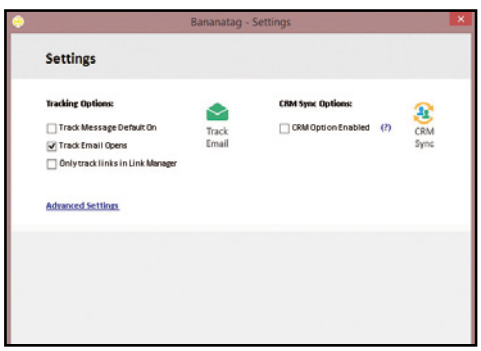
2 Scegliamo la tipologia

Un messaggio ci informerà che l'account è stato creato con successo. Verremo quindi reindirizzati alla pagina per scegliere il metodo per il tracciamento. Possiamo usare anche un'estensione per Chrome e Firefox ma noi scaricheremo il componente per Outlook cliccando su *Download*.

3 Ora tocca al plug-in

Salviamo il file *Bananatag-1.3.9.exe* sul PC. Al termine del download, assicuriamoci di non aver avviato Outlook sul computer e facciamo doppio clic sul file eseguibile per avviarne l'installazione. Non essendo presente la lingua italiana, scegliamo quella inglese e proseguiamo con *OK*.





4 Un componente necessario

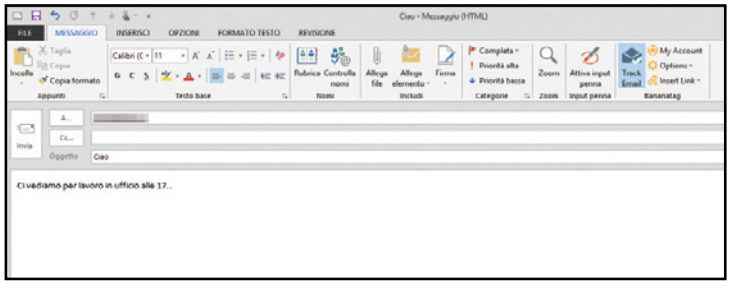
Clicchiamo su *Next*, accettiamo la licenza e proseguiamo con l'installazione. Se ci viene chiesto di scaricare e installare il tool Visual Studio 2010 confermiamo ed eseguiamo il download e l'installazione dei componenti necessari. Al termine potremo installare Bananatag.

5 Ecco i nuovi strumenti

Avviamo Outlook e confermiamo il setup di Bananatag con *Installa*. Se tutto è andato come dovrebbe, nel pannello degli strumenti di Outlook comparirà anche il set contenente quelli di Bananatag tra cui il *Link manager* e il tasto *Options* per accedere alle impostazioni del plug-in.

6 Stop all'autotracciamento

Bananatag è configurato di dafault per tracciare tutte le e-mail che inviamo. Poiché l'account gratuito ci permette di tracciare fino a un massimo di 5 e-mail al giorno, conviene disabilitare il tracciamento automatico: da *Options/Settings* togliamo la spunta in *Track Message Default On*.

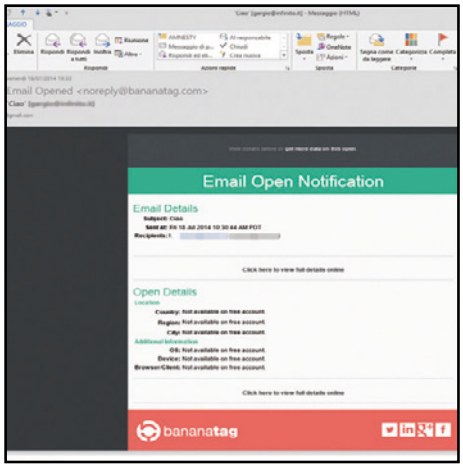


7 Un'azione manuale

Creiamo un nuovo messaggio di posta elettronica come siamo soliti fare abitualmente. Se vogliamo tracciarlo, prima di spedirlo clicchiamo sul tasto *Track E-mail* presente nella barra degli strumenti per selezionarlo e poi completiamo l'invio del messaggio.

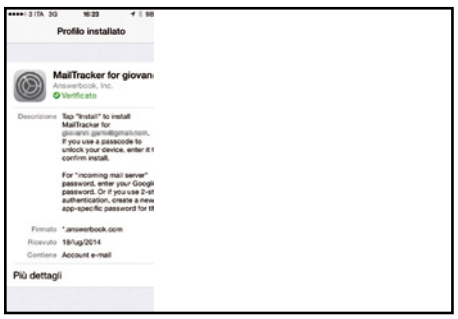
8 Lettura effettuata!

Ora non dobbiamo far altro che attendere. Quando il ricevente aprirà l'e-mail, riceveremo da parte di Bananatag un messaggio con oggetto *E-mail Opened* che ci conferma la lettura. Cliccando sul link *Click here to view full details online* potremo visualizzare maggiori dettagli.



Faccio tutto dallo smartphone

Possediamo unMelafonino? Se sì, installando sul dispositivo l'app Mailtracker possiamo verificare anche in mobilità l'apertura delle nostre e-mail da parte dei destinatari.



1 Selezioniamo l'account

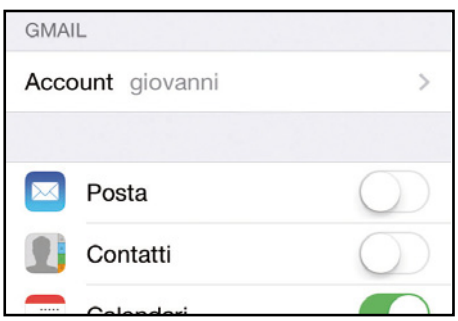
Scarichiamo e installiamo l'applicazione MailTracker dall'App Store. Una volta avviata, ci viene mostrata la procedura di configurazione. Per prima cosa eseguiamo l'accesso col nostro account e-mail. Utilizzeremo quello di Google ma l'applicazione è compatibile anche con altri servizi.

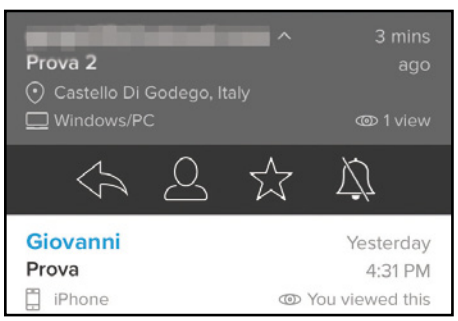
2 Installiamo il profilo

Effettuato l'accesso, ci viene mostrato il tipo di dati cui accederà l'applicazione. Confermiamo con *Accetto* e proseguiamo. L'applicazione ci chiederà di installare sul nostro iPhone un profilo: proseguiamo con *Installa* e confermiamo toccando nuovamente il tasto *Installa*.

3 Serve la password

Ci viene ora chiesto di inserire la password per il server della posta in arrivo, ovvero la password dell'account di Gmail che stiamo configurando. Inseriamola e tocchiamo la voce *Seguente* in alto a destra. La procedura di configurazione iniziale è terminata, tocchiamo *Fine* per proseguire.





4 La configurazione

Tocchiamo *Next* per passare alle istruzioni che ci illustreranno come utilizzare MailTracker. In sostanza dobbiamo ora andare in *Impostazioni/Posta, contatti, calendari*, toccare l'account che abbiamo precedentemente configurato in MailTracker e mettere la linguetta *Posta* su *Off*.

5 Inviamo il messaggio

Ora siamo pronti a inviare una e-mail tracciabile. Per farlo andiamo sempre in *Mail*, l'applicazione di posta dell'iPhone, e compiliamo il nuovo messaggio. Assicuriamoci che nel campo *Da* come mittente sia selezionato l'account di posta che abbiamo configurato con MailTracker.

6 Notifica ricevuta

Quando il destinatario aprirà il messaggio, riceveremo una notifica sull'iPhone dell'avvenuta lettura. Potremo controllare lo stato dei messaggi inviati andando in *MailTracker*. In *Feed* visualizzeremo le notifiche di lettura con informazioni sull'ora e il luogo da cui è stata visualizzata.

E-MAIL: LE TRACCIO SUL WEB

Esistono servizi del tutto gratuiti, come WhoReadMe, che consentono di tracciare l'invio delle e-mail senza installare nulla. Per utilizzarlo andiamo su http://whoreadme.com ed effettuiamo la registrazione. Dopo aver confermato il nostro account cliccando sul link ricevuto per e-mail, siamo pronti a tracciare i messaggi con qualsiasi client di posta. Basterà infatti aggiungere il suffisso ***whoreadme.com*** all'indirizzo di posta del destinatario (ad esempio ***giovanni@gmail.com.whoreadme.com***). Per conoscere l'avvenuta ricezione basterà invece loggarsi al sito di ***WhoReadMe*** e andare nella sezione ***Reports***.

	SITO INTERNET	COSTO MENSILE	NUMERO E-MAIL TRACCIATE	COMPATIBILITÀ
YESWARE	www.yesware.com	$ 10	Illimitato con pianificazione; invio e tracciamento degli allegati	Chrome e Firefox
BANANATAG	http://bananatag.com	$ 5	100 e-mail al giorno	Chrome, Firefox, Microsoft Outlook e altri client
SIGNALS	www.getsignals.com	$ 10	Illimitato	Gmail, Microsoft Outlook, Apple Mail

Abbiamo scoperto il Web segreto

C'è una porta nascosta del Web dalla quale si accede ad un archivio di comunicazioni private

Cosa ci occorre

30 MIN. FACILE

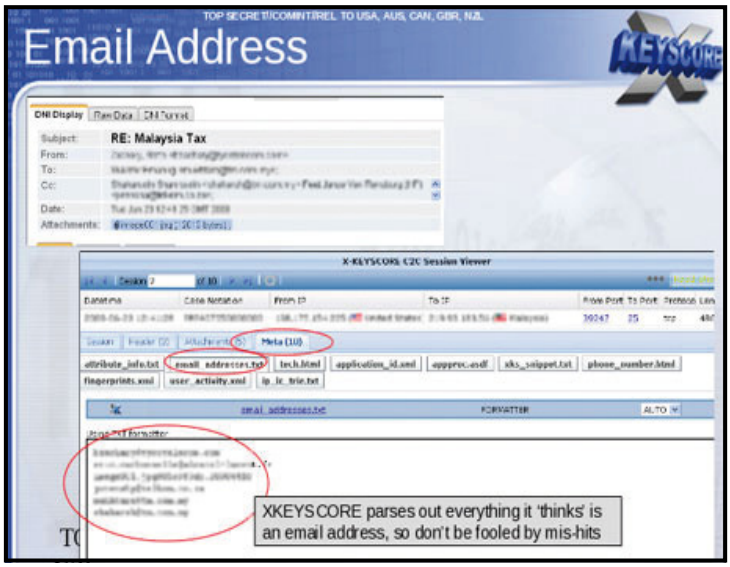
BROWSER DI NAVIGAZIONE ANONIMA
TOPSECRET EXPLORER
☑DVD
SOFTWARE COMPLETO
Note: Il software che ci permette di accedere agli archivi segreti del Web si chiama Tor Browser, che noi abbiamo ribattezzato come Top Secret Explorer

Durante questi ultimi mesi, i media di tutto il mondo hanno parlato almeno una volta dello scandalo NSA, la National Security Agency, ovvero l'organismo governativo degli Stati Uniti d'America che, insieme alla CIA e all'FBI, si occupa della sicurezza nazionale. A gridare allo scandalo è stato l'ex tecnico della CIA Edward Snowden, il quale ha dichiarato, con ingenti quantitativi di prove, che il sistema per la sicurezza nazionale è sempre andato ben oltre i limiti imposti all'interno degli accordi Internazionali e le attività di "controllo" si estendevano anche, senza permesso, ad intercettazioni di telefonate, fax e dati anche su altri paesi ed in particolar modo su politici esteri di un certo spessore (ultima saltata alla ribalta dello scandalo NSA è stata la Cancellieria dell Germania, Angela Merkel)

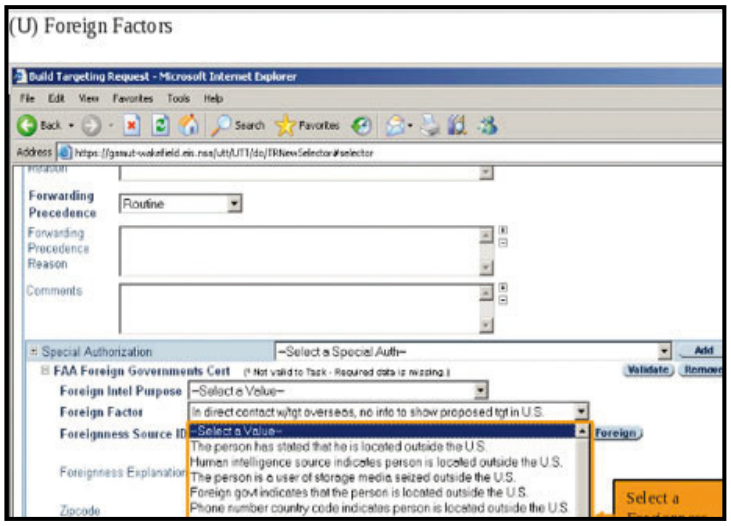
Xkeyscore: il software per le intercettazioni

Spesso può sembrare quasi impossibile che informazioni così riservate, come possono essere le telefonate di alti capi di Stato, siano intercettate così facilmente da enti esterni. Ma le prove rilasciate da Snowden, e pubblicate anche all'interno di archivi come WikiLeaks e Cryptome, non lasciano dubbi sull'invasione dei sistemi utilizzati principalmente dagli Stati Uniti per garantire una sicurezza nazionale quanto più possibile. **Il software utilizzato dall'agenzia NSA per le intercettazioni è saltato allo scoperto grazie ad un articolo apparso sul giornale "The Guardian" il 31 Luglio 2013. Tale programma prende il nome di Xkeyscore e permette di accedere ai dati della cronologia di navigazione, di quella di ricerca, alle mail, alle telefonate ed alle conversazioni private su Facebook.**

I documenti messi on line dal Guardian e da altri quotidiani, tra cui Le Monde, mettono in luce il suo funzionamento. La NSA lo definisce come



Il software Xkeyscore in azione per il filtraggio delle e-mail.



I filtri di Xkeyscore permettono di indicare la tipologia di persona da filtrare (è possibile selezionare se l'utente sta parlando "in codice", se si trova all'esterno o all'interno del territorio USA).

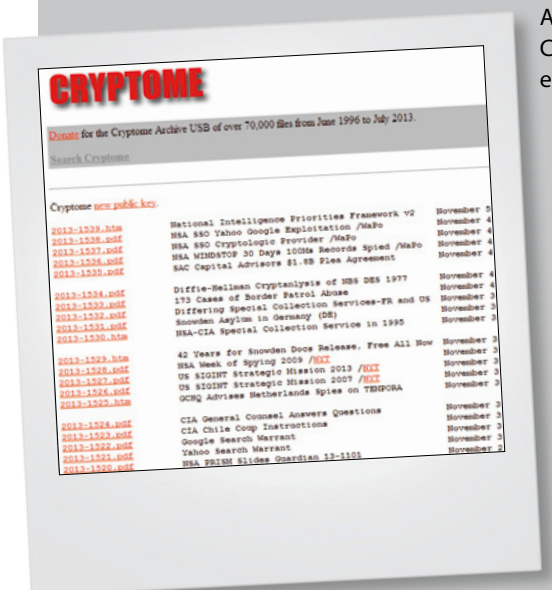
un strumento che permette di esaminare «quasi tutto quello che un individuo fa su Internet». Secondo le rivelazioni diffuse da Snowden il software Xkeyscore è in grado di analizzare anche le conversazioni cifrate. Sulla base di alcuni screenshot rilasciati sembrerebbe possibile, infatti, poter risalire a tutte le informazioni che vengono trasmesse in forma nascosta per poi successivamente decifrare in maniera del tutto automatica. Secondo la documentazione ufficiale NSA i dati vengono memorizzati per un massimo di 5 giorni, tranne quelli ritenuti di estrema importanza. Dopo la divulgazione di queste molteplici informazioni la NSA ha pubblicato la seguente dichiarazione sul quotidiano "The Guardian": *«Le affermazioni secondo le quali ci sarebbe un accesso generalizzato e senza controllo alcuno dei nostri analisti ai dati raccolti dalla Nsa è falsa. L'accesso a Xkeyscore è limitato al personale che ne ha bisogno nello svolgimento del suo lavoro».*

Gli Stati Uniti D'America affermano che l'intercettazioni di ingenti quantità di dati sia effettivamente reale, ma che la loro analisi venga effettuata solamente verso individui che potrebbero mettere a rischio la sicurezza Nazionale e non.

Cryptome: l'antenato di wikileaks

Quando WikiLeaks, la creatura di Julian Assange su cui in questi giorni è uscito un film nelle sale cinematografiche di tutto il mondo dal titolo "Il Quinto Potere", saltò alla ribalta nel 2009 (in realtà il sito era online dal 2006) pochi sapevano che fin dal 1996 esisteva un portale, chiamato Cryptome, dove informazioni riservate ad analoghe, i cosidetti "leaks", venivano pubblicati alla portata di tutti senza alcun tipo di censura.Ancora oggi Cryptome è online e continua a riscuotere moltissimo successo pur non essendo mai balzato sui media come invece è successo su WikiLeaks. Grazie ad una serie di ricerche siamo riusciti a recuperare documenti inediti riguardanti l'Italia. In queste pagine vogliamo mostrarvi delle foto in esclusiva riguardanti la tragedia della Costa Concordia, foto mai divulgate pubblicamente e scattate direttamente dalle aziende che hanno avuto l'incarico di assicurare il relitto e procedere allo smaltimento di quest'ultimo. Accedere a Cryptome è un'operazione che non richiede alcun tipo di conoscenza tecnica ed il suo utilizzo è molto più intuitivo di WikiLeaks. Basterà infatti accedere con il proprio browser all'indirizzo http://cryptome.org/ per essere proiettati all'interno di migliaia di documenti strettamente riservati che mai avrebbero dovuto vedere la luce. **L'archivio di Cryptome al momento contiene oltre 70.000 documenti inviati in forma anonima da attivisti di tutto il mondo**. Le fonti rimangono sempre sconosciute grazie alla possibilità di inviare messaggi anonimi allo staff del portale grazie ad una

SU CRYPTOME DOCUMENTI INEDITI SUL NOSTRO PAESE

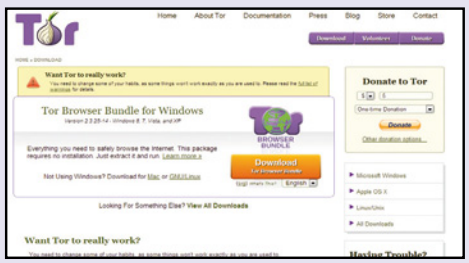


All'interno dell'archivio italiano disponibile su Cryptome sono state trovate anche delle foto esclusive e ad alta risoluzione sul naufragio della Concordia, scattate direttamente dai responsabili della messa in sicurezza del relitto e mai divulgate sui media.

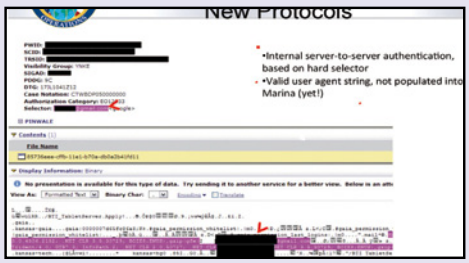
NASCE IRPILEAKS: IL "WIKILEAKS" ITALIANO

Dopo Cryptome e WikiLeaks sono nati in tutti gli stati dei portali che hanno come scopo quello di collezionare i documenti riservati della propria nazione. Anche in Italia abbiamo un progetto analogo ed il suo nome è "IrpiLeaks" (accessibile da: https://irpi.eu/irpileaks/?lang=it). Il progetto è stato realizzato ed è sostenuto dal Centro Studi Hermes per la Trasparenza e Diritti Umani Digitali (http://logioshermes.org/). L'intero sistema si basa sull'utilizzo di Tor, già integrato nella piattaforma, che risulta essere la miglior tecnologia di anonimato a disposizione degli utenti su Internet, ed è costantemente soggetto a revisioni da parte di esperti della sicurezza. Tor garantisce che nessuna traccia personale rimanga su IrpiLeaks. vIrpi suddivide le informazioni in diverse categorie al fine di renderle accessibili più facilmente sulla base dei propri interessi personali: Spesa pubblica, Frodi, Finanza, Criminalità organizzata ed Ambiente. Il portale pubblica materiale anche in lingua Inglese al fine di poter rendere internazionale la diffusione delle notizie sopra-riportate. Come per WikiLeaks e Cryptome anche Irpi permette di caricare, per chi lo desidera, qualsiasi tipo di materiale senza dover compromettere la propria identità. All'interno dello stesso portale è disponibile un'ampia guida per aiutare i "whistleblower", ovvero coloro che vogliono diffondere una notizia di cui sono a conoscenza e che è reputata "Top Secret", ad effettuare l'upload del materiale.

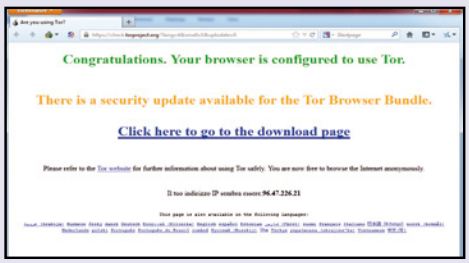
ECCO COME USARE IRPILEAKS PER TROVARE DOCUMENTI TOP SECRET



1 Il primo passo consiste nello scaricare il software TOR Browser presente nel DVD allegato a questo speciale



2 Scompattiamo l'archivio sul Desktop o in qualsiasi altra cartella all'interno del computer. Non sono necessarie installazioni.



3 Per poter avviare il browser TOR basterà adesso fare doppio click sull'applicazione "Start Tor Browser" e al termine inserire l'indirizzo https://irpi.eu/irpileaks/?lang=it

chiave pubblica ed una chiave privata.
Gli ultimi documenti che appaiono all'interno della Homepage del portale riguardano quasi esclusivamente lo scandalo NSA ed in particolar modo una serie di slide Powerpoint che mostra nei dettagli i sistemi utilizzati dall'ente governativo per mantenere sotto controllo le conversazioni di moltissimi Stati stranieri.

MafiaLeaks per combattere la mafia Italiana

Se CryptoMe, WikiLeaks e IRPILeaks sono portali in cui è possibile inviare o leggere documentazioni riservata a livello generale, MafiaLeaks (www.mafialeaks.org) è il primo portale al mondo verticale di questa tipologia. Il servizio, basato anch'esso sulla rete TOR, permette di divulgare in forma completamente anonima qualsiasi informazione inerente alla Mafia italiana. Lo scopo di MafiaLeaks è quello di funzionare da intermediario tra coloro che possiedono determinate informazioni riservate e le "persone fidate" in grado di combattere oppure aiutare le vittime di mafia. Sul portale MafiaLeaks si legge:
«Le persone fidate sono le persone che riceveranno la tua segnalazione. Le informazioni che tu deciderai di svelare attraverso la nostra piattaforma non verranno inviate indiscriminatamente a tutti ma sarai tu a scegliere a chi farle pervenire. Il nostro elenco di persone fidate è in continuo aggiornamento e stiamo lavorando per aumentare il loro numero.»

La lista al momento comprende: Forze dell'ordine (per agire), giornalisti (per informare) e associazioni antimafia (per aiutare).

COSÌ I DOCUMENTI RISERVATI VIAGGIANO NELLA RETE

1 Scarica Tor

Scarica il browser Tor Bundle dal link che trovi sopra.

Salva la Cartella Tor sul tuo Desktop.

2 Apri Tor & IRPILEAKS

Apri la Cartella Tor e fai doppio click sul file Start Tor Browser.exe.

Copia l'indirizzo di IRPILEAKS che trovi sopra e incollalo nella barra di navigazione di Tor.

3 Invia una Segnalazione

Se vuoi inviare una Segnalazione clicca sul tasto Invia una Segnalazione.

Se invece hai già inviato una Segnalazione, digita il codice della Ricevuta per modificarla.

4 Argomento & Destinatario

Scegli l'Argomento più pertinente alla tua Segnalazione e indica il Destinatario della stessa.

5 Compila il form

Compila il form nel modo più dettagliato possibile.

Qualora desideraste venire contattati, aggiungete dei contatti di riferimento..

6 Carica i file

Clicca su Aggiungi FIle per condividere documenti a sostegno della tua Segnalazione.

Per noi è fondamentale poter provarne la genuinità.

7 Accetta & invia

Clicca su Accetto soltanto dopo aver letto attentamente le istruzioni.

Invia la tua Segnalazione.

8 Conserva la Ricevuta

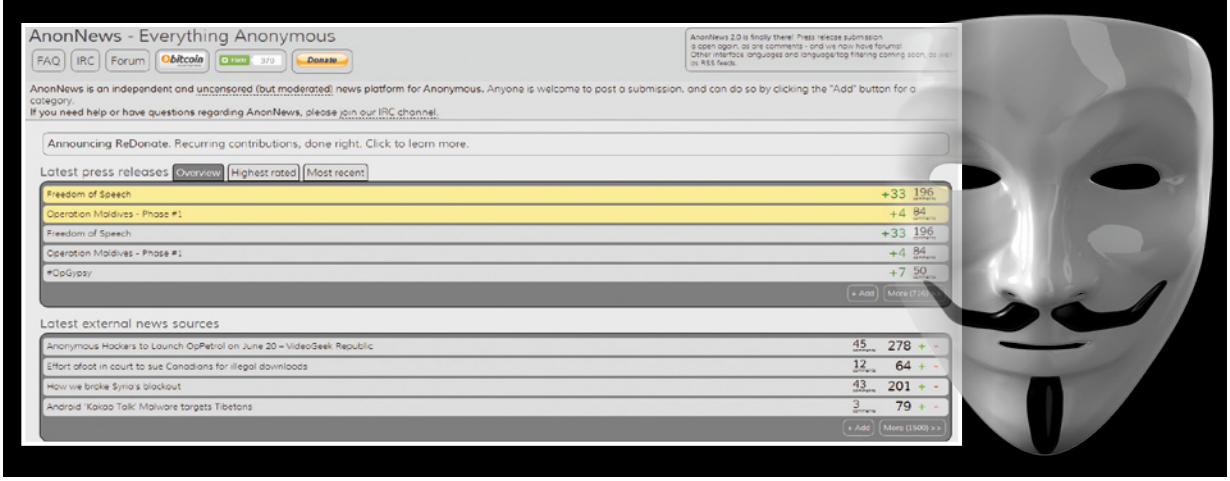
Conserva la Ricevuta che appare sullo schermo ma ***non salvarla sul tuo computer***!

La Ricevuta ti consentirà di accedere alla tua Segnalazione in futuro.

ANONNEWS: PER CHI RIMANE NEL SILENZIO

Molte fughe di notizie o di Hacktivism rimangono spesso nel silenzio: questo accade perchè spesso i Media non danno l'importanza di un attacco Hacktivism quanto ad una fuga di notizie come quanto avvenuto per l'NSA, ma in Rete il portale AnonNews (www.anonnews.org) ha lo scopo di raccogliere gli attacchi portati a termine da parte dei gruppi Anonymous.

All'interno di AnonNews sono riportate notizie che, a causa della censura, non vengono spesso pubblicate all'interno di molti quotidiani, principalmente legati alle questioni Siriane. AnonNews è, infatti, anche un canale di comunicazione che, grazie alla rete TOR su cui si basa come tutti i servizi visti in precedenza, permette di bypassare i filtri che i diversi stati abilitano per il controllo delle notizie.



COSA VUOL DIRE

NSA: National Security Agency, organismo degli USA che si occupa della sicurezza nazionale.

CIA: Central Intelligence Agency, l'agenzia di spionaggio degli USA, responsabile dell'ottenimento e dell'analisi delle informazioni sui governi stranieri, sulle società ed individui

FBI: Federal Bureau of Investigation, ente investigativo di polizia federale, principale braccio operativo del Dipartimento della Giustizia degli Stati Uniti

Edward Snowden: Ex tecnico della CIA ed ex collaboratore della Booz Allen Hamilton (azienda di tecnologia informatica consulente della NSA, la National Security Agency) noto per aver rivelato pubblicamente dettagli di diversi programmi di sorveglianza di massa del governo statunitense e britannico, fino ad allora tenuti segreti

Cryptome: Portale nato nel 1996 con lo scopo di raccogliere e pubblicare i documenti TopSecret

WikiLeaks: Portale nato nel 2006 da Julian Assange saltato alla ribalta dei media dopo la pubblicazione dei "War Log" americani e di video militari riservati

NoForn: Dicituar utilizzata all'interno dei documenti Americani per indicare il materiale che non deve essere condiviso con Stati stranieri, anche se amici.

TOR: Sistema che permette di navigare completamente anonimi sfruttando dei proxy

Whistleblower: Utenti che sono in possesso di materiale riservato e decidono di renderlo pubblico.

Gli hacker ci spiano dalla TV!

Cosa ci occorre 30 MIN. FACILE

PACKET SNIFFER
WIRESHARK
Lo trovi su: ☑DVD
SOFTWARE COMPLETO
Sito Internet:
www.wireshark.org

Abbiamo analizzato tutto il traffico Internet che circola nelle nuove Smart TV e scoperto che…

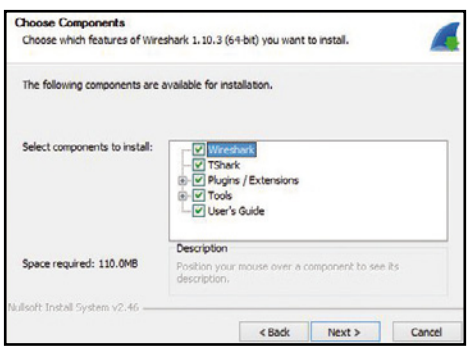
"Se stasera in TV non danno nulla di interessante, perché non colleghiamo l'hard disk al televisore e guardiamo qualche film da lì?" Sono frasi che chissà quante volte pronunciamo la sera in salotto. Ma abbiamo mai pensato che c'è qualcuno che potrebbe sapere tutto quello che facciamo con il televisore? Potrebbe ad esempio conoscere quali film vediamo, quali dispositivi colleghiamo, i dati di accesso usati per guardare YouTube o per navigare sui sociali network. Un'ipotesi surreale? Tutt'altro!

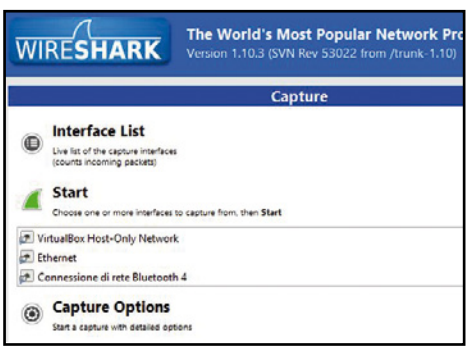
Il caso dei dati "rubati"

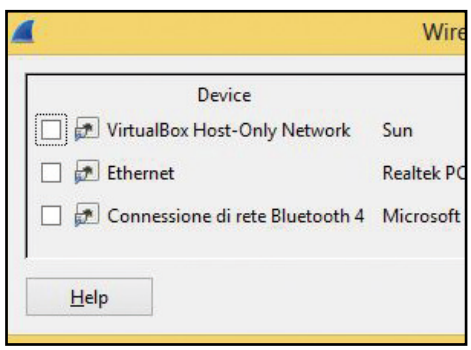
Considerando che si tratta di dispositivi connessi ad Internet, già da tempo in redazione ci stavamo occupando di controllare quali dati venissero generati e scambiati dalle Smart TV verso i server dei vari servizi di cui dispongono, senza mai notare nulla di anomalo e totalmente ignari invece di quello che di lì a poco avrebbe fatto scalpore tra le maggiori testate giornalistiche on-line che si occupano di hi-tech. Nelle ultime settimane, infatti, è scoppiato uno scandalo che vede coinvolta la casa coreana LG, accusata di "conservare" e far viaggiare in chiaro i dati dei propri utenti che utilizzano un suo modello di Smart TV. Davanti ad una notizia del genere chiunque storcerebbe il naso, mostrando da una parte curiosità e desiderando di ottenere maggiori delucidazioni sulla faccenda, dall'altra incre-

È il momento di sniffare la nostra rete

Servendoci del tool Wireshark possiamo passare al setaccio tutto il traffico di pacchetti generato nella LAN di casa nostra, alla ricerca di potenziali tracce di spionaggio attraverso la Smart TV. Ecco come fare.







1 Installiamo il tool di rete

Scompattiamo l'archivio *Wireshark.zip* (lo trovi nel DVD allegato a questo speciale) e avviamo il file *EXE* contenuto in esso. Accettiamo le condizioni di utilizzo e clicchiamo sempre su *Next*. Se ci viene chiesto di installare anche WinPcap, accettiamo e attendiamo il termine della procedura.

2 A tu per tu con l'interfaccia

L'interfaccia di Wireshark appare a molti alquanto incomprensibile, ma non è del tutto così. Ricordiamo infatti che il tool da noi scovato è pure sempre uno strumento professionale col quale si può veramente fare di tutto in ambito di reti informatiche.

3 Compatibilità Wi-Fi

Dal menu in alto clicchiamo su *Capture*, poi su *Interfaces*: controlliamo se la nostra scheda Wi-Fi supporta la *Capture Mode*, che ci permette di intercettare una maggior quantità di pacchetti, selezionando la casella corrispondente e cliccando *Options*.

dulità per quanto sia diventato ormai pericoloso perfino guardare la TV. Addirittura qualcuno ha gridato al complotto, considerati i recenti fatti che hanno portato alla luce le indagini a tutto campo condotte dall'agenzia americana NSA che spiava tutto e tutti senza alcun controllo. Sicuramente questo non è il caso di LG, ma effettivamente l'idea di fare un confronto verrebbe a chiunque. In pratica, è emerso che un modello di Smart TV, prodotta appunto da LG, memorizza la maggior parte delle operazioni che l'utente compie, anche le più semplici, e le invia ad una serie di server. Tra i dati trasmessi ci sono le impostazioni salvate, i canali TV visti, le periferiche USB collegate al televisore, il tutto senza la benché minima traccia di codifica.

La risposta di LG

Avremmo voluto verificare di persona il tutto ma, dopo una nostra richiesta, LG non ha accettato che ci venisse inviato un suo modello di Smart TV affetta da questo tipo di "problema". Un loro riscontro però non si è fatto attendere: ***"La privacy dei nostri clienti è una priorità assoluta per LG Electronics, perciò prendiamo la questione molto seriamente. Stiamo considerando con attenzione le segnalazioni pervenuteci sulla possibilità che alcuni dati sull'utilizzo delle Smart TV di LG siano stati condivisi senza consenso. Stiamo approfondendo la questione e prevediamo di avere a breve maggiori informazioni"***. Sappiamo però che i prodotti della casa coreana non sono gli unici a generare sospetti di tentato spionaggio; abbiamo scoperto infatti che anche le Smart TV prodotte da Samsung (a quanto pare tutti i modelli delle generazioni recenti) soffrono di problemi di intercettazione. Una società maltese di sicurezza informatica, la ReVuln, ha infatti spiegato che è possibile prendere il totale controllo da remoto di una Smart TV Samsung, scoprendo i canali visti, password, le impostazioni del televisore, ed è perfino possibile salvare tutto il contenuto di un eventuale hard disk collegato. Per ora ReVuln non ha comunicato le procedure adottate per mettere in atto l'hack alle aziende, per cui si aspettano ancora importanti risvolti.

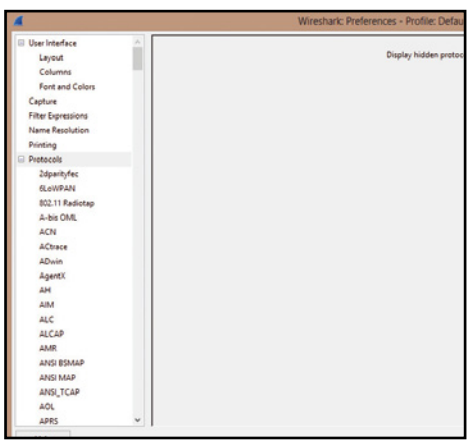
Proteggiamo la nostra privacy

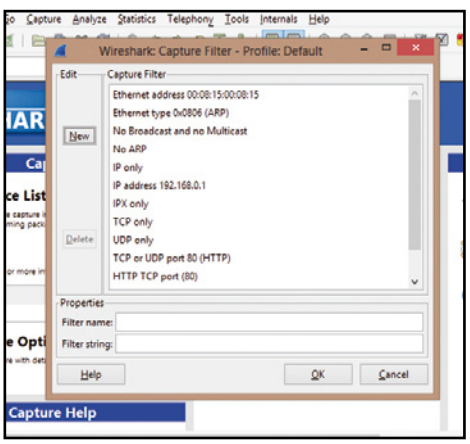
Com'è possibile che sia diventato pericoloso perfino guardare la TV e ci si debba preoccupare che la nostra privacy possa essere violata? È il prezzo da pagare, purtroppo, per avere dispositivi sempre più connessi ad Internet. Ma forse non è il caso di allarmarsi, perché comunque ci sono contromisure adottabili. Vediamo insieme quindi come verificare se la nostra Smart TV collegata alla rete Wi-Fi di casa sta generando del traffico anomalo e, se così è, la soluzione è presto detta: scollegarla definitivamente da Internet!

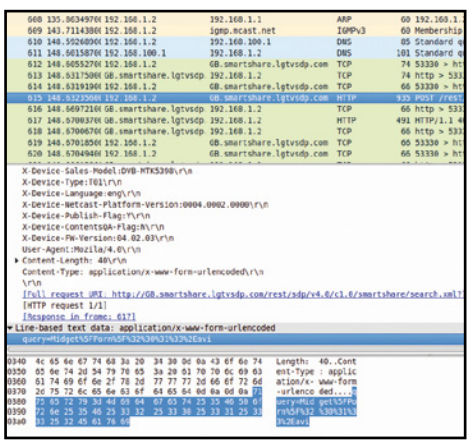
IL FIREWALL FATTO IN CASA

Esistono soluzioni, per veri smanettoni, che possono aiutarci a proteggere la nostra privacy su Internet. Una di queste può essere ad esempio un servizio costantemente attivo che analizzi e filtri ogni singolo byte scambiato sulla rete di casa nostra e che intercetti collegamenti potenzialmente pericolosi e li blocchi in automatico. C'è infatti chi, servendosi di un vecchio PC desktop, installa un vero e proprio firewall hardware in casa. Per realizzarlo bisogna installare su questo PC una distribuzione Linux creata ad hoc (scaricabile dal sito www.ipcop.org) e montare una seconda scheda di rete che servirà alla trasmissione della rete Internet a tutti i dispositivi che dovranno usufruirne. Il router andrà così collegato al PC-firewall e a quest'ultimo potranno essere collegati a cascata (tramite Wi-Fi o tramite un semplice ed economico switch) tutti i dispositivi (TV, PC, notebook, smartphone, tablet ecc.) presenti in casa. Il firewall si gestisce facilmente da un'interfaccia Web semplice ed intuitiva ed è possibile creare una lista di siti da inserire in una blacklist.

per testarne la sicurezza







4 Tutti i protocolli in chiaro

Per abilitare la visualizzazione di tutti i protocolli utilizzati è necessario spostarsi nelle preferenze di Wireshark *Edit\Preferences\Protocols*. Da qui, attiviamo l'opzione *display hidden protocol items* per abilitare la visualizzazione di tutti i protocolli di rete, inclusi quelli nascosti.

5 Impostiamo i filtri!

Per filtrare la visualizzazione del solo traffico generato dalla SmartTV spostiamoci su *Capture\Capture filter* e compiliamo *Filter name* con *IP address 192.168.1.10* (dove 192.168.1.10 è l'indirizzo della SmartTV) e *Filter string* con *host 192.168.1.10*. Confermiamo con *OK*.

6 Vai con lo sniffing!

Clicchiamo *Capture* e poi *Start*: teniamo d'occhio la colonna in corrispondenza di *Destination*; se notiamo stringhe o link che si riferiscono a servizi che non stiamo usando, significa che qualcosa non va! Clicchiamo sul link per visualizzare maggiori dettagli.

La card intelligente di Win Magazine

Ci nascondi tutto quello che vuoi e per leggerla basta avvicinarla allo smartphone. Ecco i mille usi dei tag NFC

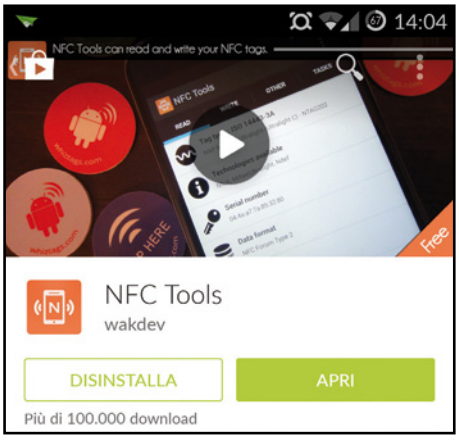
Wi-Fi, Bluetooth, infrarossi e alla fine NFC. Tra le tante tecnologie disponibili per il trasferimento di dati senza fili tra vari dispositivi, l'NFC è l'ultima (in ordine cronologico) arrivata. A differenza delle precedenti, questa tecnologia permette a due dispositivi di scambiarsi informazioni quando si trovano ad una brevissima distanza l'uno dall'altro. In pratica, quando due smartphone si toccano (o più in generale due dispositivi dotati di chip NFC), possono trasferirsi qualsiasi tipo di informazioni, come documenti, foto, contatti e altro.

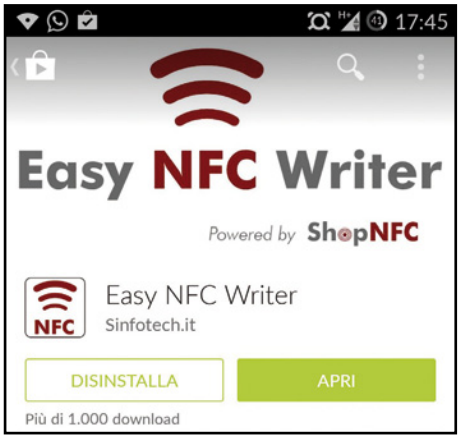
Utilizzi senza limiti

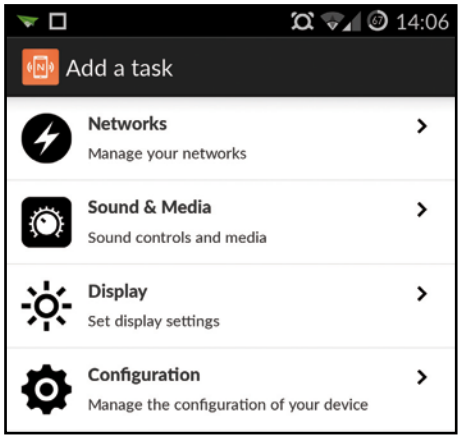
La tecnologia NFC (acronimo di Near Field Communication), è utilizzata anche per accettare pagamenti dai POS in mobilità: in molte città è possibile pagare il biglietto dei mezzi pubblici semplicemente avvicinando il proprio smartphone ad un dispositivo NFC appositamente progettato. Per non dire che sono stati sviluppati piccoli dispositivi magnetici, detti TAG, in grado di memorizzare pochi Kilobyte di informazioni in modo continuativo e permanente.
Anche se lo spazio a disposizione sembra poco, in realtà 32 KB (per i tag versione 4) sono più che sufficienti a salvare indirizzi Web, contatti o righe di codice relative ai processi da avviare. Questi tag, quindi, possono poi trasferire le informazioni salvate ad un qualsiasi altro smartphone o dispositivo

Programmiamo il nostro tag NFC

Se disponiamo di uno smartphone Android con tecnologia NFC, possiamo utilizzare un'apposita app gratuita per programmare i chip in tre semplici passaggi. Ecco come procedere.







1 L'app per programmare

Per impostare le funzionalità desiderate sul nostro tag NFC, abbiamo bisogno di un'apposita applicazione. Colleghiamoci al *Play Store* di Google e cerchiamo l'app gratuita Easy NFC Writer, sviluppata direttamente da Sinfotech.it. Tocchiamo prima *Installa* e poi *Apri* per avviarla.

2 Aggiungiamo un task

Per scrivere un Tag NFC, è sufficiente compilare i campi richiesti e avvicinare il Tag al proprio dispositivo. Con Easy NFC Writer possiamo scrivere e programmare Tag NFC di qualsiasi tipo. Possiamo nasconderci indirizzi di pagine Web, contatti in formato V-Card, testo semplice e tanto altro ancora.

3 Scriviamo la card

Una volta completata la scrittura, è possibile bloccare la riscrittura dei tag rendendoli di sola lettura. Ti ricordiamo che questa operazione è irreversibile. Nell'app è presente una comodissima funzione, che ci permette di acquistare direttamente i Tag NFC a prezzi davvero vantaggiosi.

NFC. In sostanza possiamo programmare un tag NFC così che quando poggiamo su di esso uno smartphone, su quest'ultimo si abilitino delle impostazioni precedentemente configurate nel tag.
Ad esempio, possiamo far sì che quando poggiamo il telefono sul tag adesivo incollato sul comodino, questo abiliti sullo smartphone la modalità silenzioso e attivi la sveglia per il giorno seguente! Nei nostri test, invece, ne abbiamo utilizzato uno su cui abbiamo registrato una funzione che avvia le mappe di Google e mostra la nostra posizione sullo schermo dello smartphone. Considerando che un tag NFC può essere acquistato on-line a meno di 1 euro e riprogrammato tutte le volte che vogliamo, ci sarà davvero di che divertirsi!

COSA SI PUÒ FARE CON UN TAG NFC

- Effettuare e ricevere pagamenti
- Salvare prenotazioni e/o biglietti di ingresso
- Operazioni di marketing come flayer o cataloghi
- Memorizzare le informazioni di un'attività
- Trasferire qualsiasi tipologia di file tra dispositivi NFC
- Monitorare e controllare gli accessi

AZIONI PROGRAMMABILI SUI TAG NFC

- Modificare impostazioni di rete Wi-Fi, Bluetooth
- Attivare/disattivare modalità aereo, GPS e dati
- Variare il volume e i toni di notifica
- Modificare le impostazioni del display
- Controllare e pubblicare sui social media
- Avviare, terminare o installare applicazioni
- Apertura di URL, direttamente tramite browser
- Impostare sveglie o creare eventi sul calendario

Ti regaliamo le applicazioni per chiamare tutti e inviare messaggi impossibili da rintracciare. Ecco come usarle

Il mio cellulare è anti-spia

Cosa ci occorre 10 MIN. FACILE

APP TELEFONICA
REDPHONE
DVD
SOFTWARE COMPLETO
Sito Internet:
https://play.google.com

APP DI MESSAGGISTICA
CRYPTOSMS
DVD
SOFTWARE COMPLETO
Sito Internet:
https://play.google.com

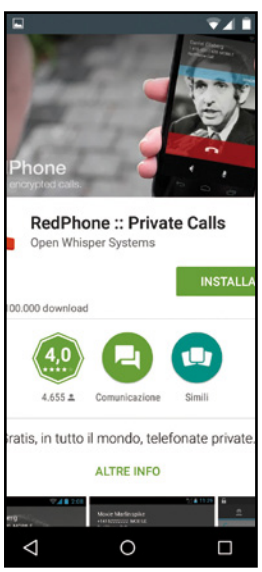
"Il telefono. La tua voce": recitava così la campagna pubblicitaria di fine anni '70 di Telecom Italia (cha allora si chiamava ancora SIP). Uno spot che anticipava e raccontava la passione degli italiani per le comunicazioni telefoniche. A distanza di tanti anni sono cambiati gli apparecchi telefonici ma non le abitudini: nel 2014, infatti, nel nostro Paese sono stati venduti 15,6 milioni di smartphone e inviati quasi 40 milioni di messaggi SMS! Numeri da capogiro che ovviamente non potevano non attirare le attenzioni dei tanti cacciatori di dati personali sempre pronti a carpire ogni nostro segreto. Proprio per dare una soluzione al problema delle intercettazioni telefoniche abbiamo messo a punto un kit composto da due applicazioni tanto potenti quanto semplici da utilizzare che permettono di criptare tutte le nostre telefonate e i messaggi inviati e ricevuti col nostro telefonino.

App su misura per la privacy

La prima, RedPhone, permette di instaurare un collegamento tra due smartphone su un canale criptato e impossibile da intercettare: per l'utente questo si traduce nell'effettuare una semplicissima telefonata da avviare dall'applicazione invece che dal dialer predefinito del telefono. CryptoSMS è invece un sistema di cifratura con password che abbiamo appositamente realizzato nei nostri laboratori e permette realmente di mettere "sotto chiave" tutti i nostri messaggi. La chiave di codifica del testo dell'SMS, infatti, viene creata e condivisa esclusivamente tra i due interlocutori: non ci sono server remoti che memorizzato queste password e sui quali transitano i messaggi. Ma non perdiamo altro tempo e scopriamo insieme come configurare il nostro sistema anti intercettazione.

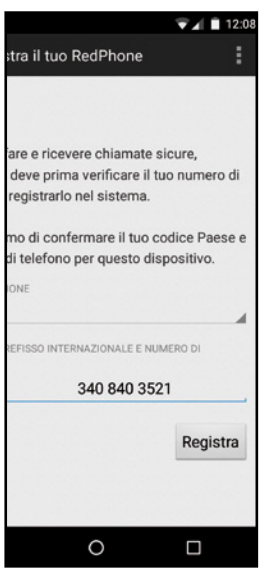
Telefonate criptate col cellulare

Ecco la procedura da seguire per configurare correttamente RedPhone: in pochi minuti saremo in grado di criptare le nostre conversazioni ed evitare che qualche malintenzionato possa origliarle di nascosto.



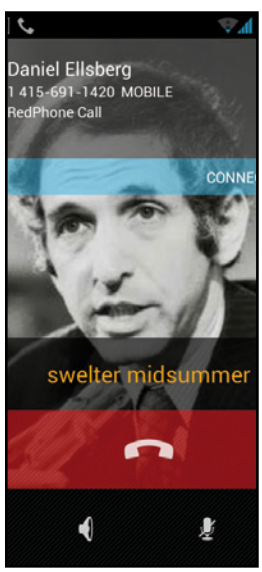
Installiamo subito l'app

1 La prima cosa da fare è procurarci l'app RedPhone. Avviamo il *Play Store* dal nostro smartphone e cerchiamo, scegliamo l'icona a forma di lente di ingrandimento, *redphone*. Tocchiamo la relativa icona e poi *Installa* per avviare il download e la successiva installazione.



Registriamo il numero

2 Dal menu del telefono avviamo l'applicazione: la schermata relativa alla registrazione del nostro numero al servizio di RedPhone serve essenzialmente per essere rintracciabile dagli altri utenti: il numero sarà come un nickname univoco, per cui inseriamolo e tocchiamo *Registra*.

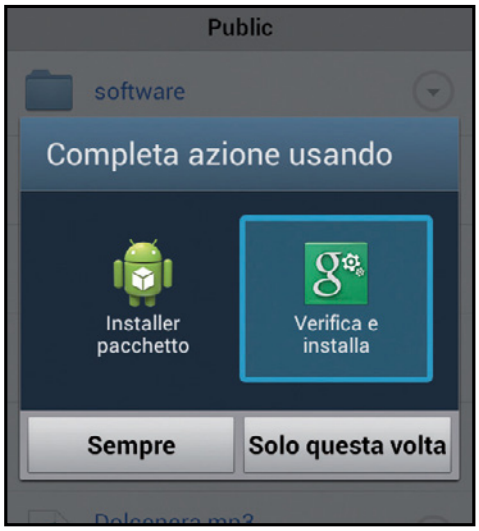


Nessuno ci può ascoltare…

3 Riceveremo un SMS col codice di convalida da copiare e incollare nell'interfaccia di RedPhone. Automaticamente, la rubrica mostrerà tutti i nostri contatti iscritti anch'essi al servizio. Basta selezionarne uno per avviare una comunicazione a prova di intercettazione!

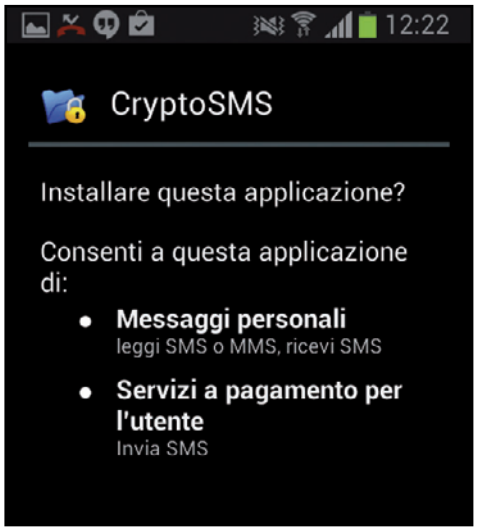
I miei SMS non li legge nessuno

Grazie all'app CryptoSMS potremo inviare e ricevere messaggi di testo criptati: basterà semplicemente creare una password di accesso e condividerla con il nostro interlocutore. Ecco come utilizzarla al meglio.



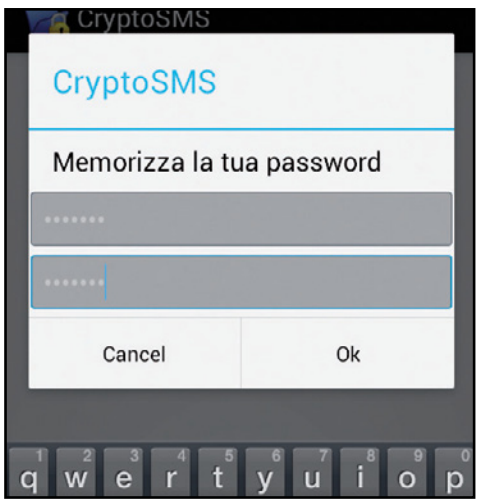
Ecco l'app esclusiva

1 CryptoSMS è un regalo esclusivo per i lettori di Win Magazine e non si trova sul Play Store di Google: per installarla, scarichiamo l'archivio *CryptoSMS.zip* dal DVD allegato a questo speciale, scompattiamolo e copiamo l'APK nella memoria dello smartphone. Tappiamo quindi su questo file e selezioniamo *Verifica e installa*.



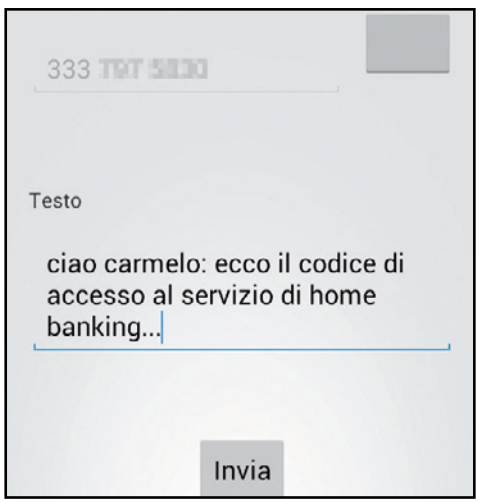
Una semplice installazione

2 Nella nuova schermata tappiamo su *Installa* per procedere con l'installazione dell'applicazione. La procedura durerà solo pochi secondi. Al termine tappiamo *Apri* per avviare direttamente la semplice interfaccia grafica di CryptoSMS. Tappando *Fatto*, invece, l'app sarà avviabile direttamente dal menu *Applicazioni* dello smartphone.



Impostiamo la password

3 Al primo avvio di CryptoSMS creiamo la password che verrà usata per criptare i messaggi e che dovremo comunicare alla persona con cui comunicare in tutta sicurezza (e che, ovviamente, dovrà installare l'app con la procedura vista finora). Creiamo un nuovo messaggio tappando sul + in alto a destra e compiliamo il campo *Destinatario*.



I messaggi sono criptati

4 Digitiamo il *Testo* e tappiamo *Invia*. Il destinatario dovrà inserire la password (**Passo 3**) per leggere l'SMS! Per chiudere l'app premiamo il tasto *Indietro* dello smartphone: in questo modo ad ogni successivo avvio ci verrà chiesto di inserire nuovamente la password di decodifica, per avere sempre il massimo della sicurezza!

ECCO COME FUNZIONA L'INVIO DI UN MESSAGGIO CON CRYPTOSMS

Sorveglia casa anche in vacanza

Ecco come usare browser e Webcam per controllare il tuo appartamento anche a distanza

Cosa ci occorre

30 MIN. FACILE

BROWSER WEB
GOOGLE CHROME
SOFTWARE COMPLETO
Lo trovi su: ✔DVD
Sito Internet: https://chrome.google.com

APP PER BROWSER
CHROME REMOTE DESKTOP
SOFTWARE COMPLETO
Lo trovi su: ✔DVD
Sito Internet: https://chrome.google.com

ENCODER AUDIO/VIDEO
WINDOWS MEDIA ENCODER
SOFTWARE COMPLETO
Lo trovi su: ✔DVD
Sito Internet: www.microsoft.com

APP PER VIDEOSORVEGLIANZA
IVIDEON
SOFTWARE COMPLETO
Lo trovi su: ✔DVD
Sito Internet: www.ivideon.com

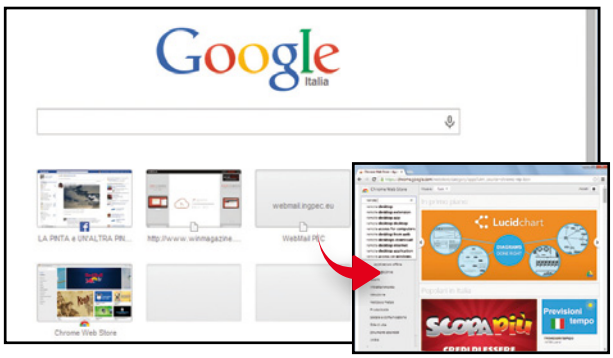
Le statistiche parlano chiaro: è proprio durante il periodo delle vacanze quello in cui si verifica il maggior numero di furti in appartamento, complice proprio il fatto che tante famiglie sono fuori e lasciano incustodita la propria abitazione. Per ovviare a questo problema molti installano nei propri appartamenti dei sofisticati e costosi sistemi di videosorveglianza che spesso, però, non sono proprio alla portata di tutti.

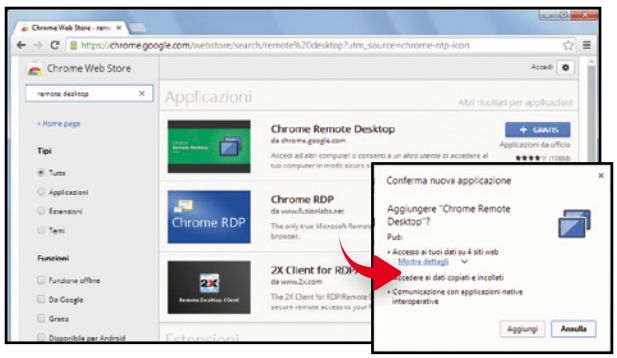
Lo smartphone controlla casa anche a distanza

Esiste un modo veloce per mettere in sicurezza il nostro appartamento senza spendere un capitale e senza installare complicate centrali tecnologiche di controllo che, solo a sfogliare il manuale di istruzioni, fanno venire il mal di testa! Il segreto consiste nello sfruttare e configurare in maniera opportuna la Webcam collegata al computer, al quale potremo accedere da remoto installando una semplice estensione per il browser. Niente software di telecontrollo e complicate configurazioni dei protocolli di comunicazione: basterà semplicemente avere un collegamento a Internet, in qualunque posto ci troviamo, per ritrovarci virtualmente davanti al nostro desktop (avendo quindi la possibilità di usare anche tutti i nostri file e i software preferiti). Proprio durante le vacanze, però, è difficile avere un PC a portata di mano. Nessun problema! Il nostro sistema di videosorveglianza potrà essere gestito e controllato a distanza anche con uno smartphone o con un tablet. Prepariamo le valigie, dunque, e partiamo sereni, certi che la nostra bella casetta sarà protetta e al riparo dai pericolosi topi di appartamento!

A Accesso remoto al PC

Grazie ad un plug-in per Chrome è possibile accedere da remoto al computer usando il browser. Il software è molto semplice da utilizzare ma, allo stesso, tempo potente e funzionale.



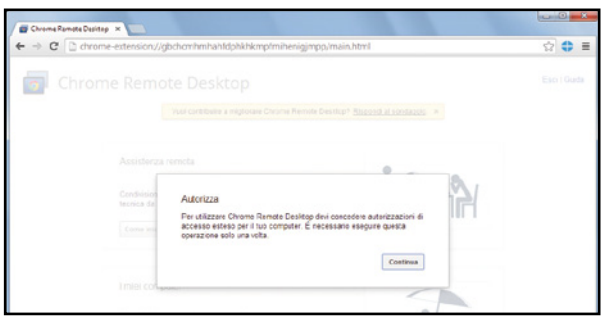


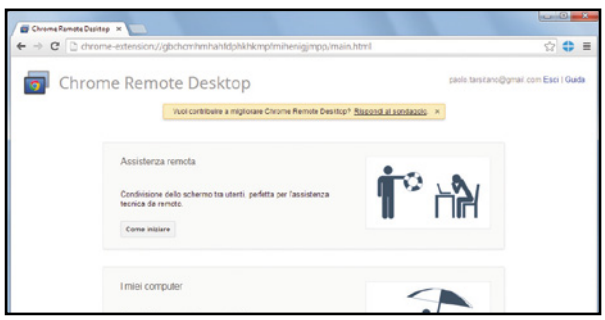
1 Prepariamo l'occorrente

Avviamo Google Chrome e, in alto a sinistra, clicchiamo su *Applicazioni*, quindi sull'icona *Store* per accedere al negozio on-line da cui scaricare le estensioni per il browser. Nella nuova schermata digitiamo *Remote desktop* nel campo di ricerca in alto a sinistra e premiamo *Invio*.

2 Installiamo il plug-in giusto

Nella nuova schermata *Applicazioni* clicchiamo sul pulsante *+ Gratis* in corrispondenza della voce *Chrome Remote Desktop*. Se non lo abbiamo già fatto, eseguiamo il login al nostro account Google. Quindi clicchiamo su *Aggiungi* per installare automaticamente il nuovo plug-in di Chrome.



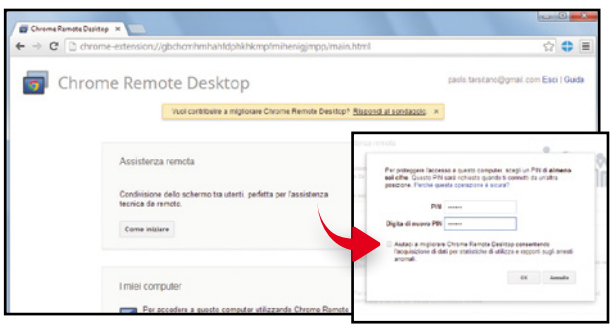


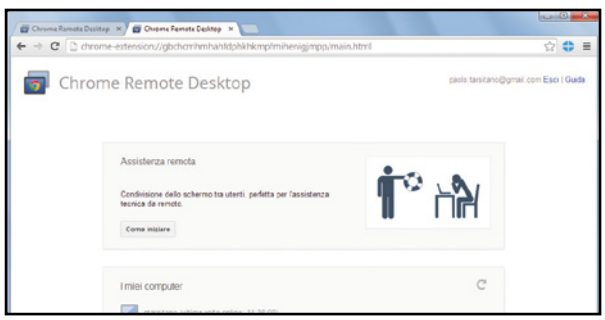
3 Il primo avvio

Tornati nella pagine iniziale di Chrome, clicchiamo di nuovo in alto a sinistra su *Applicazioni*. Nella nuova schermata troveremo ora anche l'icona di Chrome Remote Desktop: clicchiamoci sopra. Ci verrà chiesto di autorizzare l'accesso al computer: confermiamo con *Continua* e *Accetto*.

4 Ecco il pannello di controllo

Ci ritroveremo nella schermata di configurazione del plug-in. Se non ci interessa, chiudiamo il messaggio che ci chiede di partecipare al miglioramento di Chrome Remote Desktop. Clicchiamo quindi *Come iniziare* nel tab relativo a *I miei computer* per rendere il PC accessibile da remoto.





5 Attiviamo l'accesso in remoto

Clicchiamo su *Attiva connessioni remote*. Il browser provvederà a scaricare automaticamente anche il Chrome Remote Desktop Host: terminato il download installiamolo. Ci verrà quindi richiesto un PIN di sei cifre: digitiamone uno a nostra scelta e clicchiamo su *OK* per confermare.

6 Accediamo al nostro PC

Il PC è pronto per ricevere connessioni dall'esterno! Da un altro computer connesso a Internet e su cui sono installati Chrome e il suo plug-in, avviamo il browser, clicchiamo *Applicazioni* e avviamo Chrome Remote Desktop: nell'elenco dei PC accessibili sarà presente anche il nostro.

BUONI CONSIGLI

TI AIUTO DA REMOTO

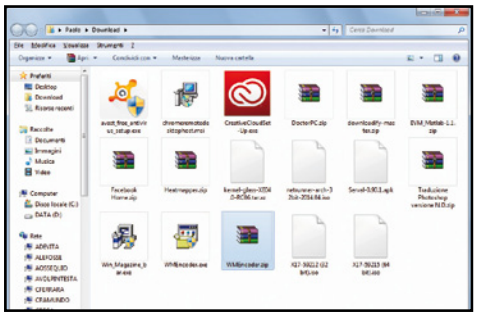
Tra le altre funzioni, Chrome Remote Desktop offre anche quella per la condivisione del desktop del proprio PC. In questo modo, se siamo in difficoltà con Windows possiamo chiedere aiuto ad un amico più esperto che può darci una mano a risolvere eventuali problemi, senza per questo dargli l'accesso a tutto il sistema. Per attivare la funzione, avviamo Chrome Remote Desktop dal menu *Applicazioni* di Chrome e, nella sua home page clicchiamo su *Come iniziare* nella sezione *Assistenza remota*, quindi seguiamo le indicazioni mostrate a video per attivare la funzionalità di assistenza remota.

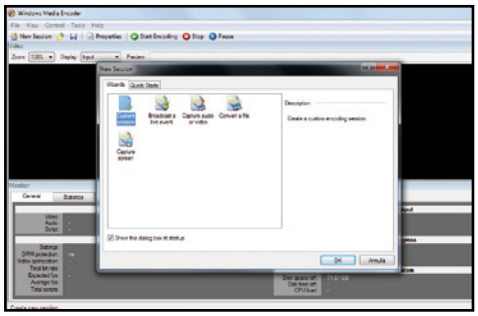
UNA RICERCA SU MISURA

Il browser Chrome usa, come motore di ricerca predefinito, quello di Google che, ovviamente, si integra perfettamente con il programma. Ciò non toglie che è possibile comunque sceglierne un altro in base alle proprie preferenze. Avviato Chrome, clicchiamo in alto a destra su *Personalizza* e controlla Google Chrome (il pulsante con le tre linee orizzontali), poi su Impostazioni e, nella schermata che appare, scegliamo il motore di ricerca che preferiamo dal menu a tendina presente nella sezione *Ricerca*.

B Videosorveglianza… fatta in casa

Siamo adesso pronti a configurare un efficiente sistema di sicurezza che ci servirà per tenere sotto controllo, anche a distanza, quello che succede nel nostro appartamento. Ecco la procedura da seguire.





1 Il tool per le riprese video

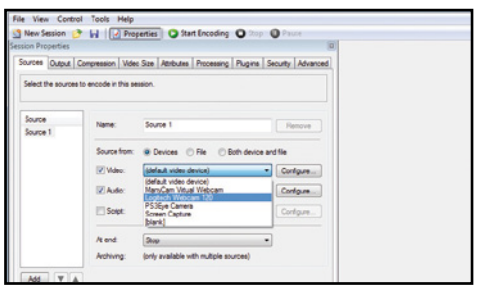
Per registrare mediante la Webcam quello che succede all'interno della nostra casa installiamo il Windows Media Encoder, che troviamo nel DVD allegato a questo speciale. Copiamo l'archivio *WMEncoder.zip* in una cartella dell'hard disk.

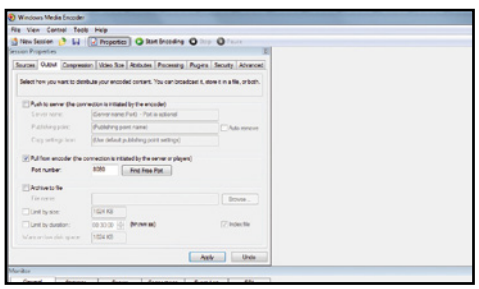
2 Una semplice installazione

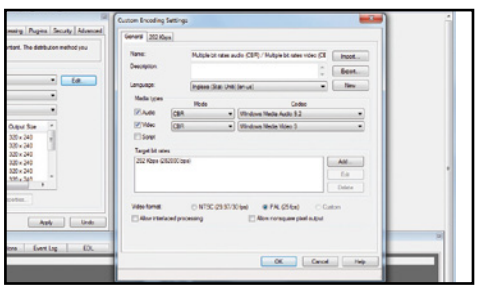
Scompattiamo l'archivio *ZIP* ed eseguiamo il file *WMEncoder.exe* contenuto al suo interno. Rispondiamo *Sì* al *Controllo dell'account utente* e proseguiamo con la procedura guidata di installazione dell'encoder. Bastano pochi clic e l'encoder audio/video è pronto all'uso.

3 Creiamo una nuova sessione

Una volta avviato il Windows Media Encoder, nella schermata *New session* selezioniamo *Custom session* per creare la nostra sessione di streaming personalizzata e poter modificare tutti i parametri di funzionamento del programma. Quindi clicchiamo *OK* per proseguire.







4 Prendi i video dalla Webcam

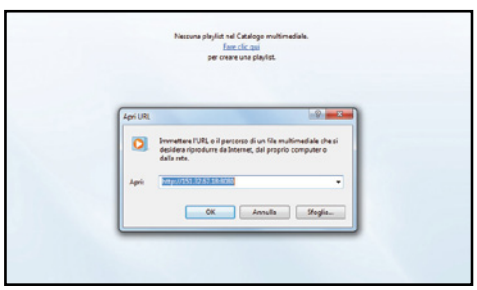
Dal tab *Sources* spuntiamo *Video e Audio* nella sezione *Source from* lasciando attiva la voce *Devices*. Dai rispettivi menu a tendina selezioniamo il modello della Webcam che useremo per le riprese. In *Audio* è possibile selezionare un eventuale microfono esterno collegato al PC.

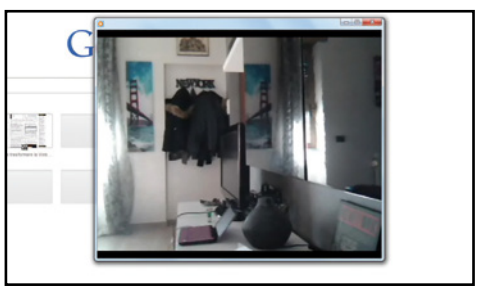
5 Apriamo la porta giusta

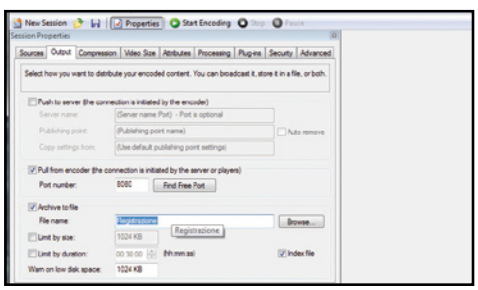
Spostiamoci adesso nel tab *Output*. Lasciamo invariate tutte le opzioni presenti verificando soltanto che sia spuntata la casella di controllo *Pull from encoder*. Nel relativo campo *Port number* digitiamo il numero di porta *8080* e confermiamo le modifiche con *Apply*.

6 Attenti alla qualità video

In *Compression* impostiamo *Windows Media server* come *Destination*. Clicchiamo *Edit* per modificare il *Video format* da *NTSC* a *PAL*. Scegliamo il *Bit rates* in base alla nostra connessione (*282 kbps* è un buon equilibrio tra qualità e velocità di caricamento). Clicchiamo *OK* e *Apply*.







7 La Webcam è live!

Il server è pronto: clicchiamo *Start Encoding*. Per "vedere" la Webcam da qualunque posto ci troviamo usiamo Windows Media Player. Avviamolo, selezioniamo *File/Apri URL* e inseriamo l'indirizzo IP del nostro PC seguito da *:8080*.

8 Inizia lo streaming

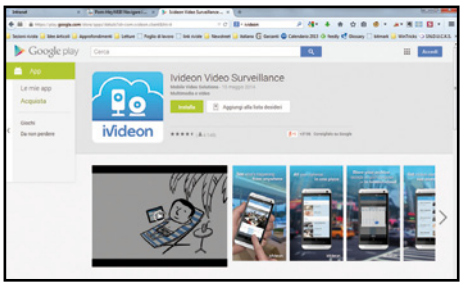
Dopo qualche secondo di caricamento, avremo il segnale video proveniente dalla nostra Webcam disponibile all'interno di una finestra di Windows Media Encoder dalla quale potremmo controllare, istante per istante, tutto ciò che accade all'interno della nostra abitazione.

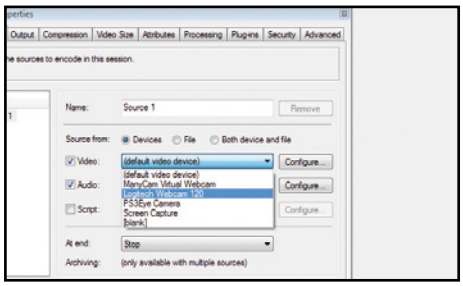
9 Registrazioni senza problemi

Se vogliamo registrare quello che accade in casa, come in un vero sistema di videosorveglianza, basterà spuntare il campo *Archive to file* dal tab *Output* e dare un nome al file della registrazione. Il programma archivierà automaticamente sul PC le immagini della Webcam.

C Fai tutto con lo smartphone

Con un semplice escamotage è possibile tenere sotto controllo la propria casa accedendo alla Webcam collegata al computer direttamente dal nostro cellulare o dal tablet. In che modo? Scopriamolo assieme!





1 Prepariamo il guardiano

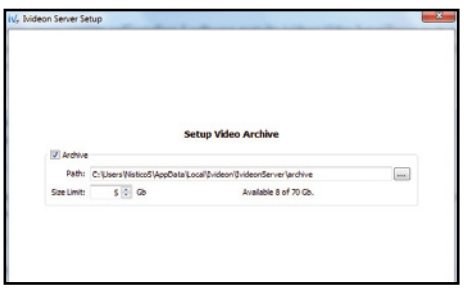
Installiamo innanzitutto il software gratuito Ivideon Video Surveillance su PC e smartphone. La versione per PC la troviamo nel DVD allegato a questo speciale, mentre l'applicazione per Android e iOS può essere scaricata dal *Play Store* o da *iTunes*.

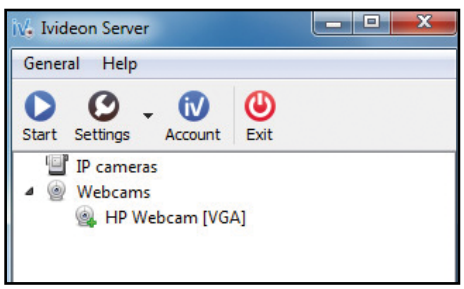
2 Un account pronto all'uso

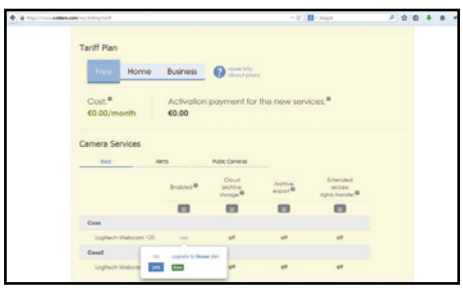
Durante la procedura d'installazione su PC ci verrà chiesto di creare un account personale. La procedura per farlo è semplicissima e completamente gratuita: basta infatti inserire un indirizzo e-mail valido, scegliere una password e dare un nome alla nostra Webcam.

3 Configuriamo la Webcam

Clicchiamo *Next* per proseguire al passo successivo della procedura di installazione guidata di Ivideon Video Surveillance. Il wizard mostrerà l'elenco di tutte le Webcam eventualmente collegate al PC. Selezioniamo quella da usare per le nostre riprese e clicchiamo *Next*.







4 Possiamo anche registrare

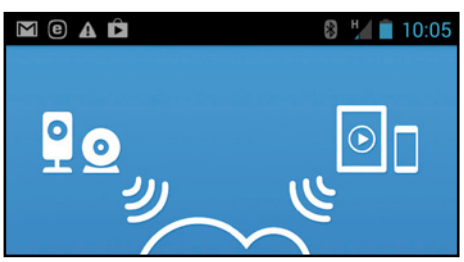
Nel caso in cui volessimo utilizzare la funzione di registrazione sul PC, nella schermata successiva selezioniamo l'opzione *Archive* e scegliamo in quale cartella dell'hard disk andare a salvare il video, prestando attenzione ad impostare un limite massimo alla dimensione.

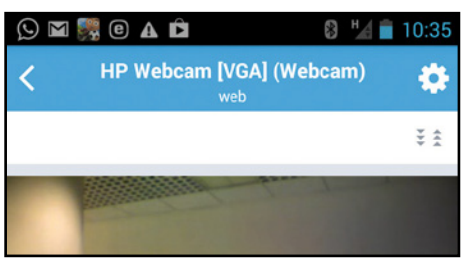
5 Ecco il pannello di controllo

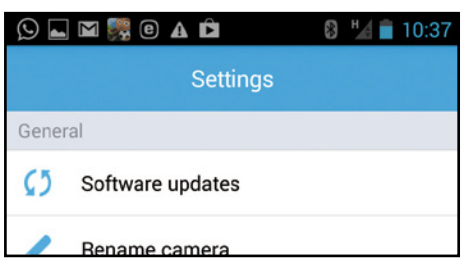
Procediamo con *Next* lasciando invariate tutte le altre opzioni. Terminata la configurazione di Ivideon Video Surveillance, ci ritroveremo davanti alla schermata principale del programma. Premendo il pulsante *Start* la nostra Webcam inizierà le registrazioni video.

6 Attiviamo la Webcam

Colleghiamoci ora al sito www.ivideon.com ed effettuiamo il login al servizio utilizzando l'account precedentemente creato. Andiamo su *My Services* e clicchiamo sul pulsante *Free* per attivare l'account. Più in basso attiviamo la nostra Webcam selezionando *Enabled/Yes*.







7 Configuriamo lo smartphone

Spostiamoci ora sul nostro telefonino Android o sull'iPhone e avviamo l'applicazione di Ivideon. Effettuiamo quindi il login utilizzando l'account creato precedentemente (**Passo C2**). Una volta effettuato il login, apparirà la Webcam attiva con il suo nome associato.

8 Inizia la videosorveglianza

Accendiamo la Webcam: dopo una breve fase di caricamento, vedremo le immagini della nostra casa in diretta sul display dello smartphone. Tramite un doppio tocco sul video sarà possibile anche zoomare sulle immagini per controllare al meglio gli angoli di casa ripresi.

9 Le opzioni dell'applicazione

L'app per smartphone offre numerose opzioni tramite l'apposito menu. Possiamo rinominare la webcam, aggiungerne di nuove ed eliminare sessioni inutilizzate. Inoltre tramite l'opzione *Show events* possiamo vedere la cronologia dell'attivazione delle nostre webcam.

Accesso remoto con noi è gratis

Il servizio DynDNS diventa a pagamento? Ecco il trucco per continuare ad accedere da remoto al nostro computer senza sborsare un centesimo

Cosa ci occorre

20 MIN. FACILE

SERVIZIO DI DND DINAMICI
NO-IP.COM
Quanto costa: gratuito
Sito Internet: www.no-ip.com

MINIPC
RASPBERRY PI MODEL B
Quanto costa: € 34,99
Sito Internet: www.amazon.it

DynDNS, il più famoso servizio di DNS dinamici, è diventato a pagamento. Ma a cosa serve un DNS dinamico? Semplice: a rendere raggiungibile qualsiasi dispositivo della nostra rete locale da qualunque postazione remota connessa a Internet. In realtà, i nostri dispositivi (per esempio il decoder satellitare o il computer) sono già raggiungibili dall'esterno conoscendo l'indirizzo IP di casa nostra. Ma è molto scomodo, perché l'IP varia in continuazione (attivando una linea ADSL, infatti, i provider ci assegnano un indirizzo diverso ogni qualvolta ci colleghiamo a Internet con il router). Un nome di dominio, invece, è sempre lo stesso: se scegliamo "casamia.sito.it", questo sarà sempre associato alla nostra casa. Potremo così raggiungere facilmente il decoder SAT casalingo dal computer dell'ufficio, oppure la Webcam collegata al PC di casa.

Non serve un nuovo router

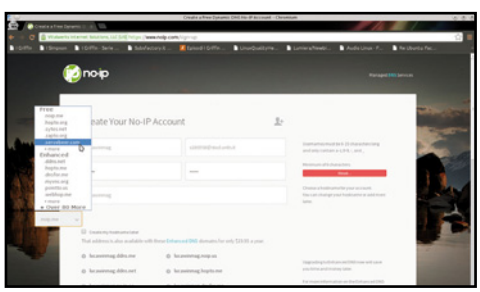
Per fortuna esistono alcuni siti che offrono tale servizio in modo gratuito. DynDNS era il più usato, ed ora che non è più gratuito molti utenti si ritrovano privi di un DNS dinamico. La soluzione? Passare ad un altro servizio simile come No-Ip.com. C'è però un problema: per poter funzionare, il nome di dominio dinamico deve essere impostato nel router oppure in un NAS collegato alla nostra rete locale, in modo da mantenere automaticamente la corrispondenza tra l'indirizzo IP assegnatoci dal provider ed il nome del dominio. La maggioranza dei router non ha problemi con No-Ip, ma alcuni modelli sono predisposti per funzionare esclusivamente con DynDNS. Comprare un altro router? Se disponiamo del mini computer Raspberry Pi, è possibile realizzare un NAS che risolverà il nostro problema. Ecco come fare.

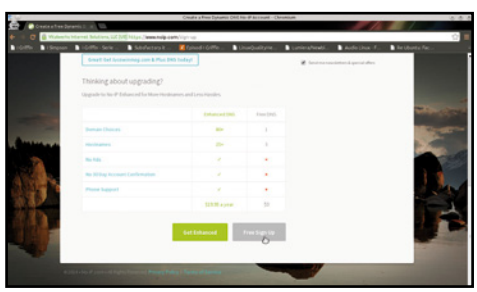
LEGGI ANCHE...

A pagina 92 di questo speciale trovi il tutorial per realizzare un perfetto sistema di videosorveglianza casalingo

A Registriamoci su No-Ip

Prima di poter utilizzare il servizio di DNS dinamici gratuiti è necessario creare un account utente. Ecco la semplice procedura da seguire per ottenere un nome di dominio ed essere subito operativi.





1 L'iscrizione al sito

Per ottenere un nome di dominio di terzo livello gratuito è necessario iscriversi al servizio. Avviamo il nostro browser e raggiungiamo il sito www.noip.com. In alto a destra nella pagina è presente il pulsante *Sign Up*: clicchiamoci sopra per avviare la procedura di registrazione al servizio.

2 Creiamo l'account

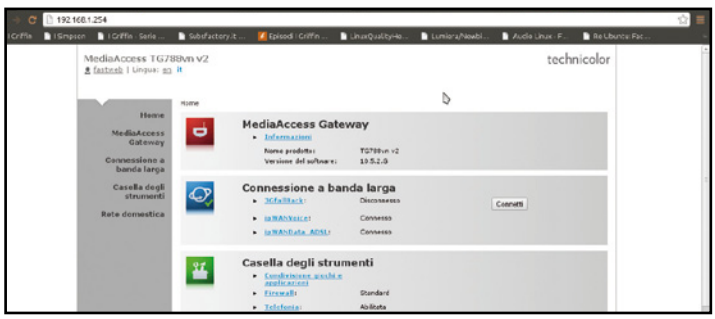
Nella finestra che appare compiliamo i campi di testo specificando il nome utente, la password e l'indirizzo e-mail da assegnare al nostro account. Non solo: possiamo già scegliere l'*hostname*, cioè il nome del dominio che vogliamo ottenere (si tratta dell'ultima casella di testo del form).

3 La registrazione è gratuita

Rimane soltanto da scegliere, tramite l'apposito menu a tendina, il dominio di secondo livello. Per concludere la procedura, clicchiamo sul pulsante *Sign Up Free* in fondo alla pagina. Ci verrà quindi inviata una email con un link su cui cliccare per confermare l'attivazione del nostro account.

B La soluzione più semplice

I principali modelli di router in circolazione permettono di usare i DNS dinamici di No-Ip. In alternativa, possiamo anche configurare il NAS per ottenere lo stesso risultato. Vediamo in che modo.



1 Usiamo l'interfaccia Web

Per raggiungere l'interfaccia Web del router o del NAS scriviamo il suo indirizzo IP nel browser: di solito è *192.168.1.1* oppure *192.168.1.254*. Se non lo ricordiamo, l'indirizzo IP è scritto nel libretto di istruzioni del router, così come l'eventuale password predefinita di accesso.

2 Il pannello degli strumenti

Ogni router, anche se della stessa marca, ha un'interfaccia Web di controllo differente, ma più o meno tutti hanno una sezione chiamata *Impostazioni* o *Pannello degli strumenti*. Ciò che conta, alla fine, è trovare la scheda *DNS dinamico* (oppure *DDNS* o ancora qualcosa di simile).

3 Una semplice configurazione

Se non abbiamo mai usato prima d'ora il router od il NAS in questione per impostare un nome di dominio dinamico, probabilmente questa funzione sarà disabilitata. Clicchiamo quindi sul pulsante *Configura* per impostare il nuovo dominio appena ottenuto con la registrazione a No-Ip.

4 I nuovi dati di accesso

È quindi necessario inserire i dati di accesso del nostro account registrato su No-Ip: l'indirizzo e-mail, che funge da nome utente, la password che abbiamo scelto per l'accesso al servizio, e il nome completo del dominio di terzo livello (l'hostname, ad esempio *lucawinmag.servebeer.com*).

5 Vai su No-Ip, grazie!

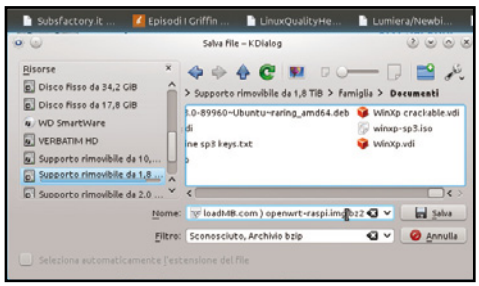
In ultimo, dobbiamo anche specificare il gestore del dominio che stiamo utilizzando: un menu a tendina ci consentirà di scegliere il servizio *No-Ip*. Nel caso in cui non fosse presente nell'elenco dei servizi supportati dal nostro router, dovremo seguire la procedura del *Macropasso C*.

6 Un veloce riepilogo

Dopo avere completato l'inserimento dei dati di accesso necessari, possiamo cliccare sul pulsante *Applica* per attivare il servizio di DNS dinamico. Se controlliamo nuovamente l'apposita sezione dell'interfaccia Web del router, dovremmo notare che il servizio risulta effettivamente attivo.

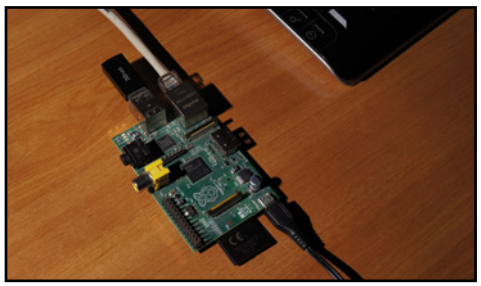
C Accesso remoto col Raspberry!

Configurando opportunamente il mini-computer riusciamo a realizzare con pochi clic un disco di rete che potremo utilizzare come punto di accesso per il nostro dominio registrato su No-Ip. Ecco come.



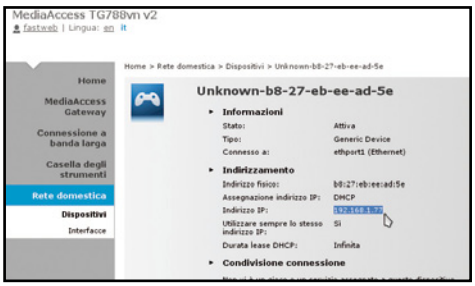
1 L'immagine e la scheda

Scompattiamo l'archivio *openwrt-raspi.img.bz2* (nel DVD allegato a questo speciale) contenente l'immagine del sistema operativo OpenWRT. Scriviamo il file IMG su un scheda SD usando il programma Win32DiskImager (anch'esso presente nel DVD allegato).



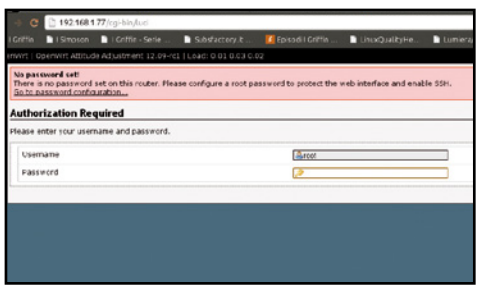
2 Il Raspberry è pronto!

Appena Win32DiskImager termina la procedura di scrittura dell'immagine di OpenWRT sulla scheda di memoria SD, possiamo inserirla nell'apposito slot sul nostro Raspberry. Colleghiamo quindi il mini PC al router tramite un cavo Ethernet e accendiamolo collegando l'alimentatore.



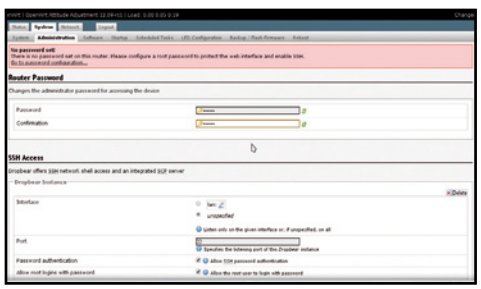
3 Come ti chiami?

Nel giro di 30 secondi o poco più, il Rapsberry dovrebbe avviarsi. Per poter accedere alla sua interfaccia Web dobbiamo scoprire il suo indirizzo IP: solitamente l'interfaccia del nostro router presente un elenco dei dispositivi connessi e qui troviamo l'indirizzo del Raspberry.



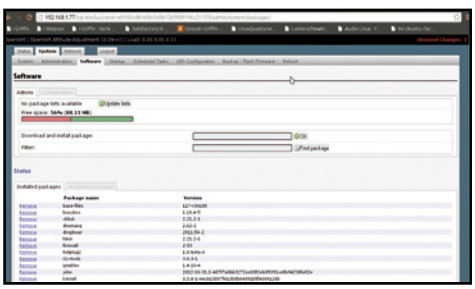
4 Il primo accesso

Se l'indirizzo IP del nostro mini PC è, ad esempio, *192.168.1.77*, non dovremo fare altro che inserire questo indirizzo nel browser per veder apparire LUCI, l'interfaccia del Web. Al primo accesso, il nome utente da utilizzare è *root*, mentre la password va lasciata vuota.



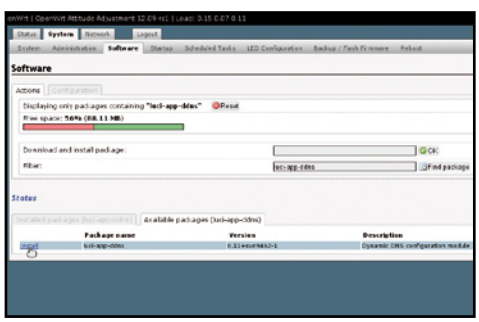
5 Prima la sicurezza

È fondamentale cambiare immediatamente la password predefinita del Raspberry, cliccando sul link *Go to password configuration*. Se non lo facessimo, chiunque potrebbe accedere da remoto al Raspberry rubando i nostri dati e infettando la nostra rete con malware di vario genere.



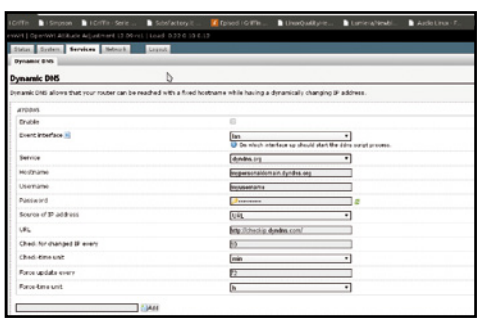
6 L'elenco dei plug-in

Essendo open source, esistono decine di utili estensioni per questo sistema operativo. Nella sezione *System*, scheda *Software*, possiamo gestire tutti i plug-in di OpenWRT. La prima volta, però sarà necessario aggiornare l'elenco completo cliccando sul pulsante *Update lists*.



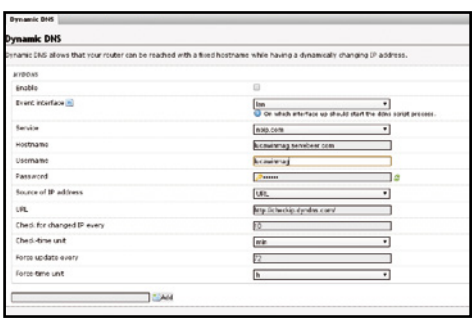
7 Installazione in corso

Se la lista del plug-in risulta già aggiornata, possiamo facilmente cercare il *plug-in luci-app-ddns* tramite la casella di ricerca *Find Package*. Appena il nome compare nei risultati sotto la voce *Available packages*, possiamo installarlo semplicemente cliccando sul link *Install*.



8 La configurazione giusta

Dopo l'installazione del plug-in basta aggiornare la pagina (tasto *F5*) per vedere apparire la sezione *Services*. All'interno troveremo le opzioni di configurazione del *Dynamic DNS*. Qui dovremo inserire tutte le informazioni di accesso a No-Ip come visto nel Macropasso precedente.



9 Abbiamo finito!

La sorgente dell'IP predefinita è uno speciale URL e conviene mantenerla tale, dal momento che funziona piuttosto bene. Cliccando su *Save & Apply* confermiamo il nostro DNS. Per sicurezza è meglio riavviare il Raspberry, in modo da essere certi di attivare subito il servizio.

TP-LINK®
The Reliable Choice

Vuoi viaggiare a tutta velocità fino a 1900Mbps?

Scegli *Archer* D9

Modem Router Gigabit ADSL2+ Wireless Dual Band AC1900

- Supporto standard 802.11ac
- Dual band simultaneo 600Mbps a 2.4GHz e 1300Mbps a 5GHz
- Tecnologia Beamforming
- Processore dual-core da 1GHz
- 1 Porta USB 3.0 e 1 USB 2.0
- 3 antenne esterne permettono la copertura anche di grandi ambienti

Scopri tutta la gamma Modem Router Gigabit ADSL2+ Wireless Dual Band AC

AC1750 Archer D7
- Fino a 1750Mbps
- 4 Porte Gigabit Ethernet

AC750 Archer D2
- Fino a 750Mbps
- 4 Porte Gigabit Ethernet

AC1200 Archer D5
- Fino a 1200Mbps
- 4 Porte Gigabit Ethernet

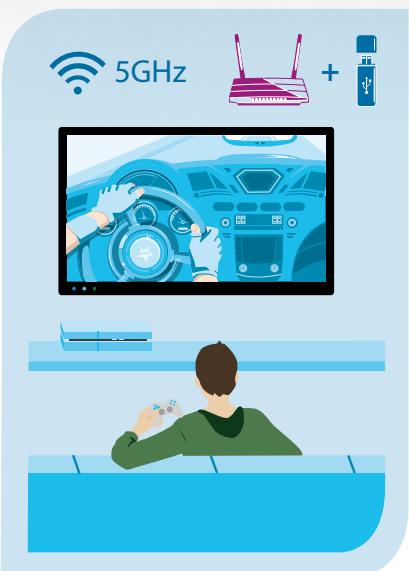
Espandi il segnale Wi-Fi

Pocket Range Extender AC750 RE200
- Dual Band fino a 750Mbps
- Porta WPS compatibile con Modem Router Archer

5 GHz

Massimizza le prestazioni della rete a 5GHz

Scheda di rete AC1200 Archer T4U
- Dual Band fino a 1200Mbps
- Compatibile con Modem Router Archer



TP-LINK ITALIA s.r.l.
www.tp-link.it | support.it@tp-link.com

TP-LINK è fornitore a livello mondiale di prodotti di networking SOHO e uno dei maggiori player sul mercato globale, con prodotti disponibili in oltre 120 paesi e decine di milioni di clienti.

Non ti sei **mai** accorto...

...di avere una palla al piede?

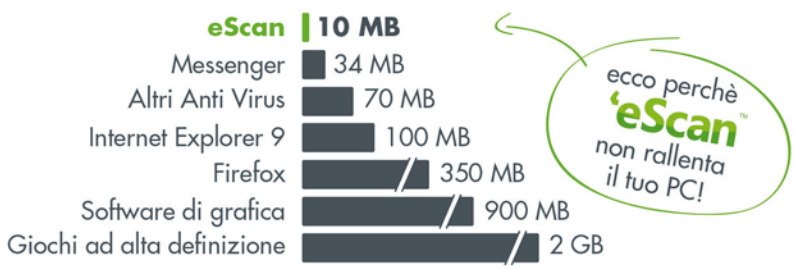
Computer **protetto** e finalmente libero di essere **veloce** con

'eScan™ Anti Virus

Per sistemi Windows®, Linux e OS X

www.escanantivirus.it

Utilizzo medio della memoria RAM



Anti Virus | *Anti Spyware* | *Anti Spam* | *Anti Phishing* | *Firewall* | *Monitoraggio della rete* | *Protezione drive USB*

Testato e certificato da:

Diventa rivenditore di eScan Anti Virus

partners.escanantivirus.it

Distributore esclusivo per l'Italia.