Osservatorio Sicurezza hi-tech

Volti Da Zeus a Stuxnet, i pericoli svelati dall'ex hacker Raoul Chiesa

Difese «Attenti ai pirati Attaccano in gruppo»

Il solo antivirus non basta più, serve protezione a 360 gradi
Mai aprire email da sconosciuti. La vulnerabilità dei browser

DI **UMBERTO TORELLI**

Sbaglia chi pensa di proteggere il computer, oggi, soltanto con un tradizionale antivirus. Perché in termini di sicurezza informatica il concetto del singolo virus che infetta il Pc è superato. Adesso si parla di «malware», vale a dire l'insieme dei software maligni come i «worm» (vermi), in grado di auto-replicarsi una volta insidiati nella memoria. Oppure ci sono i temibili «keylogger», i programmi che identificano password e identità di chi naviga in Rete.

Non bastasse, a sferrare gli attacchi non sono più hacker isolati, bensì strutture criminali. Che in squadra violano siti web, ma anche smartphone e tablet.

Per saperne di più sulle nuove minacce informatiche, abbiamo chiesto il parere di Raoul Chiesa (37 anni), un ex hacker torinese diventato cyber-poliziotto. Ora dirige @Mediaservice.net, un'azienda che si occupa di protezioni e sicurezza su web.

Da dove arrivano i pericoli maggiori per chi naviga online?

«Adesso gli attacchi più insidiosi utilizzano le vulnerabilità dei browser e dei programmi di posta elettronica. I cybercrminali violano i siti web, entrando direttamente nella home-page di quelli a maggiore concentrazione di visite. Quindi inseriscono un codice maligno nelle pagine, sfruttando le debolezze di software di navigazione come Internet Explorer, Firefox e Google Chrome».

E poi che cosa succede?

«Il resto avviene in modo automatico, all'insaputa degli utenti. Chi visita il sito sarà esposto al contagio e da quel momento il suo computer si trasformerà in un trampolino di lancio per compiere azioni fraudolente. Ad esempio, attacchi verso terzi, invio di spam, furto di informazioni personali, cattura dei login».

Quali sono i rischi per chi si connette con gli apparecchi mobili?

«Il "mobile malware", il software maligno per i dispositivi mobili, è in forte aumento. Negli ultimi cinque anni sono state individuate 516 tipi di minaccia per questo genere di apparecchi. Credo che le prossime insidie saranno proprio i malware progettati per smartphone e tablet. Già ora esiste una variante del programma maligno Zeus in grado di carpire informazioni bancarie. Inoltre sono stati rilevati software specifici sia per l'iPad, sia per i telefonini Android».

Le grandi organizzazioni criminali lavorano su scala globale e fatturano centinaia di milioni di dollari

Cyber-poliziotto Raoul Chiesa: già 516 minacce per i cellulari

In questo momento quali sono i virus più pericolosi?

«Il citato Zeus lo è, visto lo scopo: catturare le credenziali per operazioni di home banking, a differenza di altri virus che utilizzano il Pc della vittima per il generico furto di informazioni personali. C'è poi una nuova famiglia di malware, il cui capostipite si chiama Stuxnet. Per la prima volta è stato creato un worm auto-replicante, con il preciso compito di attaccare dispositivi elettronici dell'automazione industriale».

E le organizzazioni internazionali? Come si muovono i criminali informatici per operare in gruppo?

«Organizzazioni come Rbn, Russian business network, e l'ultima nata Imu, Innovative marketing ukraine, fatturano centinaia di milioni di dollari all'anno. Utilizzano modelli di business e schemi criminali innovativi, distribuiti a livello globale. Uno degli ultimi colpi, all'inizio dell'anno, è stato quello contro le carte di credito della Royal Bank of Scotland. Ha fruttato 9 milioni di dollari».

Come funzionava?

«Era prevista la presenza di oltre cento "e-mules". Sono gregari che fanno da tramite per la banda, recandosi fisicamente agli sportelli Bancomat per effettuare i prelievi con le carte clonate, dopo averne carpito i codici via Internet. Solo una piccola parte del prelievo veniva trattenuta da questi gregari, il resto era invece riciclato come denaro pulito ai capi dell'organizzazione con sedi a Mosca, San Pietroburgo e Kiev».

Come difendersi?

«Installando un software di protezione a 360 gradi, non più per il singolo virus. E usando il buon senso. Se arrivano mail da sconosciuti, con la richiesta di dati personali, bisogna insospettirsi. Allo stesso modo va prestata attenzione ai collegamenti via smartphone su reti wi-fi gratuite, ma sconosciute. Per questo, anche in ambito personale, stanno prendendo piede i protocolli crittografati di comunicazione».

L'iniziativa di Crif

Codice violato. Arriva il messaggino

Sono circa 20 milioni gli italiani che usano Internet da casa, e 16,5 milioni sono attivi su Facebook. La diffusione in Rete di dati anagrafici, recapiti personali o informazioni finanziarie, li espone al rischio di furto di identità e di frodi: sulle carte di credito o l'Internet banking, anche per l'abuso di password di posta elettronica e dei codici personali per i servizi.

L'Osservatorio sulle frodi creditizie di Crif, azienda bolognese specializzata nella gestione delle informazioni finanziarie, stima che nel primo semestre di quest'anno i casi di frode in Italia siano stati circa 11 mila, il 9% in più rispetto al 2009, per un importo complessivo di 92 milioni 158 mila euro. Per arginare il fenomeno, Crif ha ideato il servizio «Sicurnet», distribuito attraverso gli istituti bancari. Chi lo sottoscrive può registrare i dati personali che desidera vengano protetti sul web, nell'area riservata del sito www.mistercredit.it. Ogni volta che un dato oggetto di monitoraggio viene rilevato sul web, il cliente riceve un messaggio via mail o sms con i suggerimenti sull'azione da intraprendere. Come bloccare la carta di credito, se il messaggio è riferito al suo utilizzo.

C. S.

Memorie perse Tre aziende su quattro sbagliano procedure

Il Pc va in discarica? Occhio all'hard disk

Vanno cancellate tutte le informazioni archiviate. Per sempre. Ecco come fare

Dovete sostituire un vecchio computer? Si è rotto l'hard disk? Attenzione. Prima di rottamare la macchina, portandola al centro di raccolta dei rifiuti elettronici, assicuratevi che le informazioni archiviate all'interno siano cancellate per sempre.

Perché i dati sensibili come nomi, indirizzi e-mail, numeri di telefono e conti bancari, restano memorizzati nell'hard disk e possono essere violati da estranei.

Un sondaggio di novembre, condotto da Kroll Ontrack su 1.500 aziende americane, europee e dell'Est asiatico, ha rilevato che solo metà delle società intervistate mettono in pratica procedure per cancellare i dati dai dischi dismessi.

Il 75 per cento di queste ha comunque dichiarato di avere utilizzato sistemi che non garantivano la sicurezza totale dell'eliminazione.

Spiega Paolo Salin, direttore della sede italiana di Kroll Ontrack: «Tre aziende su quattro sono convinte di eliminare i file interni con un'operazione di formattazione, ma non è così. Questa procedura non garantisce la sicurezza della cancellazione totale». L'esempio può essere quello di una grande biblioteca in cui migliaia di volumi sono raccolti sugli scaffali. La certezza di eliminare un volume si ha soltanto quando questo viene tolto fisicamente dalla sua posizione e sostituito con uno nuovo. Se invece si distrugge la scheda che ne indica la posizione sullo scaffale, non viene distrutto il libro. Ebbene, l'operazione di formattazione fa invece proprio questo: cancella gli indici (le coordinate) che identificano i documenti sul disco, ma non il contenuto digitale del disco.

75%

La quota di aziende che ha rimosso i dati sensibili dal pc, senza però averli eliminati davvero

Dunque, per una rimozione sicura dei dati, bisogna riscrivere tutti i vecchi file, sostituendoli con nuovi. Un'operazione, di fatto, impossibile per chi deve cambiare decine o centinaia di computer aziendali. Che cosa fare allora? «La soluzione più semplice è usare software specifici — dice Salin —. Programmi che consentono di sovrascrive in modo definitivo tutti i dati presenti sul disco rigido. La cancellazione di un hard disk costa pochi euro». È un'operazione utile non solo per le grandi aziende, ma anche per le piccole e medie imprese e gli utenti domestici che desiderano mettere in sicurezza i dischi da eliminare. Per eseguirla, si può andare in un qualunque centro di assistenza computer.

In Italia, a livello legislativo, la riservatezza dati è regolamentata dal decreto legge 196/2003, noto come «legge sulla privacy». Fissa regole precise per l'archiviazione (anche digitale) dei dati sensibili. Il Garante ha poi specificato in un provvedimento dell'ottobre 2008 le misure per il corretto smaltimento dei supporti informatici con dati personali.

Nonostante queste indicazioni, dal rapporto Kroll Ontrack emerge che quattro aziende su dieci (italiane comprese) cedono direttamente a terzi i computer da dismettere, senza preoccuparsi della fine che faranno. Il pericolo maggiore? «Che il disco sia formattato e rivenduto sul mercato dell'usato — dice Salin — con il ripristino dei vecchi dati da parte di malintenzionati».

UMBERTO TORELLI