SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Febbraio 2014

Newsletter mensile di suggerimenti sulla sicurezza informatica

OUCH!

IN QUESTO NUMERO...

- Cos'è il Malware
- Chi e perché
- Come proteggersi

Cos'è il Malware

Introduzione

Avrete sicuramente già sentito parlare di virus, worm, cavalli di troia (trojan) e rootkit quando si parla di sicurezza digitale. Questi termini definiscono i tipi di programmi utilizzati dai criminali informatici per infettare e prendere il controllo di computer e dispositivi mobili, come tablet e smartphone. L'insieme di questi programmi prende oggi il nome di malware. In questa newsletter spiegheremo cos'è il malware, come e perché viene sviluppato e cosa potete fare per proteggervi da esso.

L'autore di questo numero

Lenny Zeltser si occupa della protezione delle attività IT dei clienti di NCR Corp e insegna come combattere il malware al SANS Institute. Lo potete seguire su Twitter (**@lennyzeltser**) e sul suo blog: **blog.zeltser.com**.

Cos'è il Malware

Il malware è un software, un programma per computer utilizzato per compiere azioni dannose: il termine è infatti una combinazione delle parole *malicious* e *software*. Lo scopo ultimo di molti criminali informatici è di diffondere il malware sui nostri computer, su tablet e smartphone: una volta installato permetterà ai criminali di prenderne il controllo. Molte persone credono erroneamente che il malware sia un problema che affligge solo i computer con sistema operativo Windows. Purtroppo non è così. Sebbene Windows sia molto diffuso, e quindi costituisca un obiettivo piuttosto importante, il malware può infettare qualsiasi tipo di dispositivo: anche i tablet e gli smartphone sono dei computer, anche se in un formato diverso e con funzioni peculiari e, infatti, la diffusione di software dannoso per i dispositivi mobili sta crescendo vertiginosamente.

Ognuno di noi è un obiettivo potenziale: maggiore è il numero di dispositivi che i criminali informatici possono infettare, maggiore sarà la quantità di denaro che potranno guadagnare. Ai criminali non importa chi viene infettato: basta solo che le vittime siano il maggior numero possibile.

Chi e perché

Il malware non viene più creato da hobbisti curiosi e hacker dilettanti, ma da criminali informatici esperti che vogliono raggiungere obiettivi specifici quali la sottrazione di dati confidenziali, la raccolta di utenti e password di collegamento, l'invio di email di spam, il lancio di attacchi di denial-of-service, l'estorsione o il furto d'identità. Il malware conosciuto come Cryptolocker, ad esempio, è usato per infettare e cifrare tutti i file presenti sul computer in modo che i criminali possano chiedere un riscatto per permettere alla vittima di riportare i propri file allo stato iniziale.

Cos'è il Malware

Le persone che creano, diffondono e beneficiano del malware sono sia individui che agiscono da soli sia organizzazioni criminali o governative. I gruppi dedicati allo sviluppo di software maligno sono spesso talmente specializzati da avere questo compito come loro unica attività: un virus, una volta creato, viene spesso venduto ad altre persone o organizzazioni che ricevono in seguito aggiornamenti regolari e supporto. Chi lo ha acquistato farà cassa installandolo su milioni di sistemi di ignare vittime, creando botnet di sistemi infetti, e costituendo così una sorta di esercito controllato a distanza utilizzabile dai criminali per i propri loschi scopi, che includono anche la rivendita di questo esercito ad altri gruppi di criminali.

Per proteggervi contro il malware assicuratevi che i vostri dispositivi e i relativi antivirus siano aggiornati e fate attenzione a possibili attacchi.

Come proteggersi

Il metodo più utilizzato per proteggere computer e dispositivi mobili dal malware è dotarli di un software anti-virus di un produttore di fiducia. Questi software, denominati anche anti-malware, sono programmi progettati per individuare e bloccare applicazioni dannose. Purtroppo tali soluzioni non sono in grado di bloccare tutto il malware poiché i criminali informatici innovano costantemente i loro approcci, sviluppando nuovi e più sofisticati attacchi in grado di scavalcare la protezione dell'anti-virus. Per questo motivo i creatori di software di sicurezza aggiornano costantemente i loro prodotti con nuove funzionalità per cui il rapporto che si è venuto a creare tra chi sviluppa malware e chi lo combatte è una sorta di corsa agli armamenti, in cui ogni parte cerca di superare in astuzia il concorrente. Sfortunatamente però i criminali hanno quasi sempre il sopravvento poiché, nonostante gli antivirus possano individuare e bloccare moltissimi tipi di programmi dannosi, ne vengono creati continuamente di nuovi che passeranno inosservati fino a quando non verrà sviluppato un rimedio contro di essi. Non è quindi possibile fare affidamento unicamente alla protezione dell'anti-virus: è necessario adottare ulteriori protezioni.

Come prima cosa, assicuratevi che il vostro sistema operativo e le applicazioni possano aggiornarsi automaticamente: più il software è aggiornato, più difficile sarà che il malware possa infettare computer, tablet e smartphone.

In secondo luogo, ricordate che la miglior difesa contro il malware siete voi: le infezioni spesso avvengono attraverso il social engineering, ad esempio quando il delinquente cerca di ingannarvi per farvi installare un'applicazione maligna. L'esempio più comune è l'attacco phishing, con cui dei messaggi email all'apparenza legittimi, ma in realtà assolutamente falsi, tentano di infettare il vostro computer: un criminale potrebbe inviarvi un messaggio fingendo di essere un impiegato della vostra banca e richiedendovi di cliccare su un link. Se

Cos'è il Malware

cascate nel tranello, verrete condotti a un sito web che cercherà di penetrare e infettare il vostro computer. Un'alternativa spesso utilizzata è costituita dal messaggio di avviso di una società di spedizioni che vi comunica che un vostro pacco non può essere consegnato e vi chiede di leggere il documento di tracciamento allegato che, una volta aperto, infetterà il vostro computer.

Gli attacchi di social engineering possono aver luogo anche con l'utilizzo di altre tecnologie: un criminale potrebbe telefonarvi spacciandosi per un tecnico Microsoft che vi informa che il vostro computer è stato infettato. La sua storia è naturalmente una menzogna e il vostro computer probabilmente è in buono stato. Il suo obiettivo è farvi credere di essere realmente stati infettati da malware allo scopo di permettergli di accedere remotamente al vostro computer o di acquistare un software di sicurezza, che altro non è che del malware reale. Usate il buon senso: se una chiamata o un messaggio vi sembrano strani, sospetti o troppo belli per essere veri, probabilmente costituiscono una minaccia.

Concludendo, il modo migliore per difendervi dal malware è di mantenere il vostro software aggiornato, installare anti-virus prodotti da aziende di fiducia e fare attenzione a chi tenta di ingannarvi per infettare il vostro computer.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
http://www.securingthehuman.org

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

OUCH - Email e Phishing:

http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_it.pdf

OUCH - Suggerimenti per avere un computer sicuro:

http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201212_it.pdf

Poster "Tu sei un bersaglio" :

http://www.securingthehuman.org/media/resources/planning/STH-Poster-YouAreATarget-Italian.zip

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis