OUCH! | Marzo 2016

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

- La rete wireless
- I dispositivi

Il malware

Introduzione

Sicuramente avrete già sentito parlare di concetti come virus, Trojan, ransomware o rootkit nelle discussioni sulla sicurezza informatica. Questi vocaboli descrivono tipi di programmi utilizzati dai criminali per infettare computer e dispositivi mobili. Un termine comune usato per descriverli tutti quanti è malware. In questa newsletter illustreremo cos'è il malware, chi lo crea e perché, e naturalmente cosa potete fare per proteggervi.

L'autore di questo numero

Lenny Zeltser si occupa della protezione delle IT Operation dei client di NCR Corp e insegna come combattere il malware al SANS Institute. Potete seguire Lenny su Twitter (**@lennyzeltser**) o attraverso il suo blog presso **zeltser.com**.

Cos'è il malware?

Si tratta di un software, e quindi di un programma per computer, usato per svolgere azioni maligne. Il termine stesso è la combinazione delle parole malicious e software. I criminali informatici installano il malware in computer e dispositivi per ottenerne il controllo o l'accesso ai loro contenuti. Una volta installato, il malware potrà essere usato per spiare le vostre attività online, sottrarvi password e file o usare il vostro sistema per attaccarne altri. Il malware può inoltre negarvi l'accesso ai vostri stessi file, richiedendovi di pagare un riscatto per ritornarne in possesso.

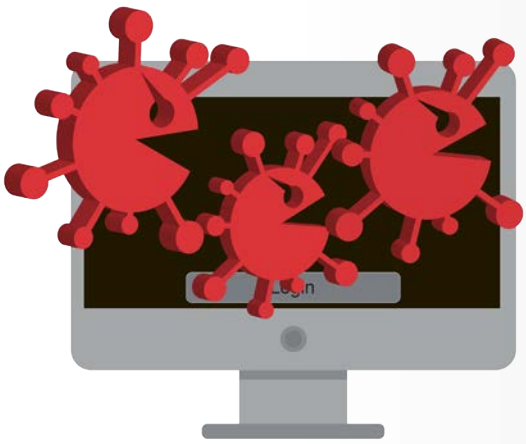
Molte persone sono convinte che il malware sia un problema esclusivo dei computer con sistema operativo Windows. Sebbene questo sistema operativo sia molto diffuso e costituisca quindi un obiettivo primario, il malware può infettare anche altri dispositivi come computer Mac, smartphone e tablet. Più dispositivi vengono infettati, più denaro potrà guadagnare un criminale informatico. Ognuno di noi costituisce, quindi, un obiettivo.

Chi crea il malware?

Ai giorni nostri, il malware non viene più creato da hobbisti curiosi o hacker dilettanti, ma da criminali informatici estremamente competenti il cui scopo è guadagnare denaro attraverso computer o device infetti, da quali sono stati sottratti dati confidenziali, o che possono essere utilizzati per inviare email spam, lanciare attacchi di denial of service (DOS) o, ancora, attraverso l'estorsione. Le persone che creano, distribuiscono e beneficiano del malware sono individui che agiscono per

Il malware

proprio conto, ma anche organizzazioni criminali vere e proprie oppure organizzazioni governative. Spesso chi crea il sofisticato malware dei giorni nostri è spesso dedicato a questo unico scopo. Il nuovo software maligno viene poi rivenduto ad altri individui o organizzazioni, insieme a un "contratto" di aggiornamento e supporto.



Proteggetevi dal malware esercitando un sano scetticismo nei confronti dei messaggi sospetti e mantenendo i vostri dispositivi e il vostro anti-virus sempre aggiornati.

Come proteggersi

Uno dei modi per proteggervi è installare un anti-virus proveniente da un produttore di fiducia. Questo strumento, chiamato anche software anti-malware, è stato progettato per individuare e fermare i programmi maligni. Purtroppo un anti-virus non è in grado di bloccare o rimuovere tutto il malware. I criminali informatici si innovano costantemente, sviluppano nuove e sempre più sofisticate soluzioni in grado di evadere i tentativi di individuazione. I venditori di anti-virus, a loro volta, aggiornano costantemente i loro prodotti con nuove caratteristiche. Per molti aspetti, tutto questo somiglia a una corsa alle armi, dove ognuna delle parti cerca di superare in astuzia l'altra. Sfortunatamente i cattivi sono spesso un passo avanti. Dal momento che, quindi, non possiamo fare affidamento unicamente agli anti-virus, ecco altri modi con cui possiamo proteggerci.

- I criminali informatici infettano computer e dispositivi mobili sfruttando le vulnerabilità del loro software. Più un software è aggiornato, meno vulnerabilità avrà un sistema e più difficile sarà per un hacker poterlo infettare. Assicuratevi che il vostro sistema operativo, le applicazioni e i dispositivi siano aggiornati automaticamente e regolarmente
- Uno dei modi più comuni con cui i criminali infettano i dispositivi è di creare una app mobile falsa, pubblicarla su Internet e convincere le persone a scaricarla e installarla. Per questo motivo è necessario scaricare e installare app solo da app store di fiducia. Installate app mobili che siano state pubblicate da lungo tempo, scaricate da un vasto numero di persone e che abbiano ricevuto recensioni positive
- Sui computer, usate un account standard che abbia privilegi limitati piuttosto che un account privilegiato come "amministratore" o "root". Questo fornisce una protezione ulteriore, prevenendo che molti tipi di malware possano installarsi
- I criminali informatici spesso riescono a condurre le vittime a installare malware usando, ad esempio, stratagemmi come messaggi email all'apparenza legittimi che contengono un allegato o un link. Le email appaiono provenire,

Il malware

ad esempio, dalla vostra banca o da un amico, ma se aprirete l'allegato o selezionerete il link, attiverete del codice maligno che installerà malware sul vostro sistema. Se un messaggio crea un forte senso di urgenza, se vi confonde, o vi porta un messaggio troppo bello per essere vero, potrebbe trattarsi di un attacco informatico. Usate sempre molta cautela: il buon senso è la vostra miglior difesa

- Effettuate salvataggi regolari dei vostri sistemi e dei file su servizi cloud, o conservate i vostri salvataggi offline, ad esempio su dischi esterni. Questo proteggerà i vostri backup in caso che un malware cancelli o cifri i vostri dati. I backup sono critici, costituendo spesso l'unico modo per ripristinare il sistema dopo un'infezione

Il miglior modo per difendervi dai pericoli è di mantenere il software costantemente aggiornato, installare anti-virus di produttori riconosciuti e stare allerta da chiunque tenti di ingannarvi allo scopo di infettare il vostro sistema.

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

Il Phishing:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_it.pdf
Social Engineering:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201411_it.pdf
Usare le app in modo sicuro:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201501_it.pdf
Tablet e sicurezza:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_it.pdf
Salvataggi e ripristino:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_it.pdf

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