La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per tutti

Stop ai Malware

Overview

Probabilmente avrete sentito parlare di virus, Trojan, ransomware o rootkit quando si tratta di sicurezza informatica. Questi termini si riferiscono a diversi tipi di programmi malevoli, chiamati malware, che i cyber criminali utilizzano per infettare computer e dispositivi. Una volta installati, possono fare tutto ciò che vogliono. Scoprite cos'è il malware, che pericoli rappresenta e, soprattutto, cosa potete fare per proteggervi da esso.

Cos'è il Malware?

In poche parole, il malware è un software, un programma per computer, utilizzato per eseguire azioni dannose. Il termine è una combinazione delle parole malevolo e software. I cyber criminali installano malware sui vostri computer o dispositivi per averne il controllo. Una volta installato, il malware può consentire ai criminali di spiare le vostre attività online, rubare password, file o utilizzare il vostro sistema per attaccarne altri. Il malware può persino prendere il controllo dei vostri file, chiedendovi poi di pagare un riscatto per riaverli. Molte persone credono che il malware sia un problema solo per i computer Windows. Sfortunatamente il malware può infettare qualsiasi dispositivo, dai computer Mac, agli smartphone, ai DVR e alle telecamere di sicurezza. Più computer e dispositivi si infettano più cresce il denaro che i cyber criminali possono guadagnare. Pertanto, ognuno di noi è un obiettivo.

Proteggi te stesso - Stop ai Malware

Sareste portati a pensare che tutto ciò che dovete fare è semplicemente installare un programma come un software anti-virus per evitare di essere infettati. Sfortunatamente, l'anti-virus non può fermare tutti i malware. I cyber criminali stanno costantemente sviluppando nuovi e più sofisticati malware che possono eludere il rilevamento. A loro volta, i produttori di antivirus aggiornano costantemente i loro prodotti con nuove funzionalità per rilevare il malware. Per molti versi è diventata una corsa agli armamenti, e i cattivi di solito sono un passo avanti. Dal momento che non potete fare affidamento solo sull'antivirus, ecco i passaggi aggiuntivi da eseguire per proteggervi:

I cyber criminali spesso infettano computer o dispositivi sfruttando vulnerabilità nel software. Più il vostro software è aggiornato, meno vulnerabilità sono presenti nei vostri sistemi e più è difficile per i cyber-criminali infettarli. Assicuratevi che i vostri sistemi operativi, applicazioni, browser, plug-in del browser e dispositivi siano sempre aggiornati. Il modo più semplice per garantire ciò è abilitare l'aggiornamento automatico quando possibile.

Un modo molto usato con il quale i cyber criminali infettano computer o dispositivi mobili è creando falsi programmi per computer o app mobili, pubblicandoli su Internet e inducendovi a scaricarli e installarne uno. Attenzione a scaricare e installare programmi o app solo da negozi online di fiducia. Inoltre, state alla larga dalle app per dispositivi mobili che sono nuove di zecca, che hanno poche recensioni positive, che sono raramente aggiornate o sono state scaricate da un piccolo numero di persone. Non usate più un programma o un'app mobile? Cancellatelo.

I cyber criminali spesso inducono le persone a installare malware al posto loro. Ad esempio, potrebbero inviarvi un'email che sembra legittima e contiene un allegato o un link ad esempio potrebbe provenire dalla vostra banca o da un amico. Tuttavia, se si dovesse aprire il file allegato o fare clic sul collegamento, si attiverà il codice dannoso che installerà il malware sul vostro sistema. Se un messaggio crea un forte senso di urgenza, o sembra troppo bello per essere vero, potrebbe essere un attacco. Siate sospettosi, il buon senso è spesso la vostra migliore difesa.

Effettuate regolarmente il backup di sistema e dei file su servizi basati su cloud, archiviate i backup offline come ad esempio unità esterne. Questo protegge i vostri backup nel caso in cui il malware tenti di crittografarli o cancellarli. I backup sono fondamentali, spesso sono l'unico modo per recuperare da un'infezione da malware.

In definitiva, il modo migliore per difendersi dai malware è mantenere aggiornati tutti i tuoi software e dispositivi, installare un software anti-virus affidabile quando possibile e fare attenzione a chiunque tenti di ingannarvi per infettare il vostro sistema. Quando tutto il resto fallisce, i backup regolari sono spesso l'unico modo per recuperare.

Versione Italiana

Italtel è una società multinazionale che progetta e realizza soluzioni e servizi di Information & Communication Technology basati su prodotti propri e di partner. Offre un ricco catalogo di servizi professionali di ingegneria, di servizi gestiti e soluzioni di Cybersecurity, collaboration, IoT, digitalizzazione delle reti e servizi di comunicazione.
Per maggiori informazioni www.italtel.com e seguici su Twitter (@Italtel)

L'autore di questo numero

Lenny Zeltser *combatte i malware creando prodotti per la security degli endpoint presso Minerva Labs e insegnando presso il SANS Institute. Lenny è attivo su Twitter come @lennyzeltser e scrive un blog sulla sicurezza su zeltser.com.*

Risorse

Ransomware:	https://www.sans.org/u/EdI
Backups:	https://www.sans.org/u/EdN
Stop That Phish:	https://www.sans.org/u/EdS