La Newsletter Mensile di sensibilizzazione alla sicurezza informatica per te

Sono stato hackerato?

Introduzione

Non importa quanto sei sicuro, è come guidare una macchina, prima o poi potresti avere un incidente. In questo articolo sono riportati gli indizi per capire se sei stato hackerato e se sì, cosa fare. Perché prima ti rendi conto che qualcosa di anomalo è successo e più è probabile che tu possa risolvere il problema.

Indizi di potenziali attacchi

Il tuo programma anti-virus genera un avviso che il tuo sistema è infetto. Assicurati che sia effettivamente il tuo software anti-virus a generare l'avviso e non una finestra comparsa da un sito Web che cerca di ingannarti spingendoti a chiamare un numero o ad installare qualcos'altro. Non sei sicuro? Apri il tuo programma antivirus.

Viene visualizzata una finestra pop-up che dice che il tuo computer è stato crittografato e devi pagare un riscatto per riavere i tuoi file.

Il tuo browser ti sta indirizzando verso tutti i tipi di siti web che non vuoi visitare.

Il computer o le applicazioni si bloccano costantemente, sono presenti icone per app sconosciute oppure finestre di pop-up sconosciute.

La tua password non funziona più sebbene tu sia sicuro che è corretta.

Gli amici ti chiedono perché li stai inondando di e-mail che sai di non aver mai inviato.

Ci sono addebiti sulla tua carta di credito o prelievi dal tuo conto bancario che non hai mai effettuato.

Come rispondere

Se sospetti di essere stato hackerato prima agisci meglio è. Se la violazione è correlata al lavoro, non provare a risolvere il problema da solo, ma segnalalo immediatamente. Se invece si tratta di un dispositivo o un account personale, ecco alcuni passaggi che è possibile eseguire.

Cambio delle tue password: questo significa non solo la modifica delle password sui tuoi computer e dispositivi mobili, ma anche per i tuoi account online. Non utilizzare il computer compromesso per modificare le password, utilizza un sistema diverso che ritieni sicuro. Se hai molti account inizia prima con quelli più importanti. Se non riesci a tenere traccia di tutte le password, utilizza un gestore di password.

Supporto della Banca: per problemi con la tua carta di credito o con qualsiasi tuo account bancario, chiama subito la tua banca o la tua compagnia di carte di credito. Utilizza un numero di telefono fidato per chiamarli, di solito sono presenti sul retro della carta bancaria e nei rendiconti finanziari oppure consulta il loro sito Web da un computer sicuro. Inoltre, considera la possibilità di mettere un blocco sul credito.

Anti-virus: se il tuo software anti-virus ti informa della presenza di un file infetto, segui le azioni che raccomanda. La maggior parte dei software antivirus dispone di collegamenti che è possibile seguire per avere ulteriori informazioni sull'infezione specifica.

Reinstallazione: se non sei in grado di riparare un computer infetto o se desideri essere più certo del fatto che il sistema sia sicuro, reinstalla il sistema operativo. Non reinstallare dai backup, usa invece i backup solo per il recupero dei tuoi file personali. Se non ti senti confidente nel fare il ripristino del tuo dispositivo, considera l'opzione di utilizzo di un servizio professionale che possa supportarti. Nel caso il tuo computer o dispositivo fosse vecchio, potrebbe essere più facile acquistarne direttamente uno nuovo. Infine, una volta che hai ricostruito il tuo sistema o ne hai acquistato uno nuovo, assicurati che sia aggiornato e abilita l'aggiornamento automatico quando possibile.

Backup: un passo fondamentale per proteggersi è prepararsi in anticipo con backup regolari. Molte applicazioni eseguiranno automaticamente il backup dei tuoi file ogni giorno o anche ogni ora. Indipendentemente dalla soluzione che usi, periodicamente controlla di essere in grado di ripristinare quei file. Molto spesso il ripristino dei backup dei dati è l'unico modo in cui è possibile rimediare ad eventuali attacchi.

Applicazione della legge: se ti senti in qualche modo minacciato, segnala l'incidente alle forze dell'ordine locali. Se sei vittima di Identity Theft e hai sede in Italia, visita https://www.commissariatodips.it/

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 articolo

Il Dr. Johannes Ullrich *(@johullrich). Decano della ricerca per il SANS Technology Institute è il direttore del SANS Internet Storm Center e un SANS Fellow. Ha creato la rete DShield basata sulla collaborazione di sensori e ospita il podcast quotidiano di notizie sulla sicurezza della rete dell'Internet Storm Center.*

Bibliografia

Backups: https://www.sans.org/u/JGP
Passphrases: https://www.sans.org/u/JGU
Password Managers: https://www.sans.org/u/JGZ
What Is Malware: https://www.sans.org/u/JH4
Credit Freeze: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/