OUCH! | Aprile 2016

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Hanno violato i miei sistemi!

Introduzione

Di certo saprete già come proteggere il vostro computer e i vostri dispositivi mobili e come mantenerli sicuri, ma nonostante questo potrebbe capitare anche a voi, prima o poi, che la loro sicurezza venga compromessa. In questa newsletter imparerete a capire se i vostri sistemi sono stati violati e cosa fare per porvi rimedio. Più velocemente riuscirete a capire che c'è qualcosa che non va, meglio potrete ridurre il danno che potrà essere causato da un attacco informatico.

L'autore di questo numero

Samantha Davison (**@sam_e_davison**) è Program Manager nell'ambito della Security Awareness and Education presso Uber e si occupa della formazione dei dipendenti nelle 350 città del mondo dove è presente l'azienda.

Capire se i vostri sistemi sono stati violati

Potrebbe essere difficile capire di essere stati hackerati, perché non esiste un unico modo per determinarlo. Gli hacker spesso lasciano vari indizi, chiamati anche indicatori: se li individuerete nei vostri sistemi, significherà probabilmente che essi sono stati violati. Ecco i principali:

- è scattato un avviso del vostro sistema antivirus segnalando un'infezione e indicando di non essere in grado di rimuovere o mettere in quarantena dei file infetti;
- l'home page del browser è cambiata all'improvviso oppure il browser vi porta a visitare siti che non volete consultare;
- sono stati creati nuovi account sul computer o sul dispositivo e non siete stati voi a farlo. O ancora, trovate programmi che non avete installato;
- il vostro computer o le applicazioni vanno in crash costantemente, ci sono nuove icone di app sconosciute o appaiono strane finestre;
- un programma richiede la vostra autorizzazione per apportare cambiamenti al sistema, sebbene non abbiate installato o aggiornato nessuna applicazione;
- la password che usate per collegarvi al Sistema o a un account online non funziona più, anche se sapete che è corretta;

Hanno violato i miei sistemi!

- gli amici vi chiedono perché state inviando spam con messaggi email che sapete di non aver mai inviato;
- vi vengono segnalati pagamenti a servizi SMS in abbonamento;
- il vostro dispositivo mobile segnala un alto uso della batteria o un consumo di banda fuori dal normale.

Potrebbe capitare che il computer o i dispositivi mobili vengano violati da un attacco hacker: in questo caso, è meglio agire il più in fretta possibile.

Come reagire

Se credete che un Vostro Sistema sia stato hackerato, prima reagirete meglio sarà: se vi è stato fornito dalla vostra azienda o se viene usato per lavoro, non tentate di rimediare al problema da soli. Potreste causare ancora più danni e distruggere evidenze utili per condurre investigazioni. Comunicate invece l'incidente al vostro datore di lavoro, contattando l'help desk, il dipartimento sicurezza o i supervisori. Se per qualche ragione non potete contattare la vostra organizzazione, scollegate il sistema dalla rete e mettetelo in ibernazione o in modalità aereo. Anche se non siete sicuri di essere stati hackerati, è comunque meglio segnalarlo, per sicurezza. Se invece il sistema è usato per scopi personali, ecco alcuni suggerimenti su cosa fare.

- **Cambiate le password**, non solo quelle del computer e dei dispositivi mobili, ma anche quelle degli account online. Non usate il sistema violato per farlo, però, ma un computer o un dispositivo diverso che sapete sicuro.
- **Anti-virus**. Se l'anti-virus vi informa di un file infetto, seguite le indicazioni che vi raccomanda. Normalmente si tratta di mettere il file in quarantena, ripulirlo o cancellarlo. Molti software anti-virus mostrano dei link a pagine che si possono consultare per avere più informazioni sull'infezione. Nel dubbio, mettere il file in quarantena, ma se non fosse possibile, cancellatelo.
- **Ricostruire il sistema**. Se non siete in grado di rimediare all'infezione o volete essere assolutamente sicuri che il sistema sia sicuro, l'opzione più sicura è di ricostruirlo. Per i computer, seguite le istruzioni del fornitore. In molti casi questo significherà utilizzare le utility disponibili per reinstallare il sistema operativo. Se questi programmi non sono disponibili, corrotti o infetti, contattate il produttore del sistema o visitate il suo sito web per capire come procedere. Non reinstallate il sistema operativo dai salvataggi che avete effettuato in precedenza, poiché potrebbero essere affetti dagli stessi problemi che volete eliminare. I salvataggi devono essere usati solo per recuperare i dati. Per i dispositivi mobili, seguite le istruzioni del produttore o del fornitore del servizio, che troverete sul suo sito.

Hanno violato i miei sistemi!

Potreste dover ripristinare il dispositivo ai dati di fabbrica. Se avete difficoltà con questo processo, fatevi aiutare da un servizio professionale. Se il sistema ha qualche anno, potrebbe essere più semplice ed economico comprarne uno nuovo. Infine, una volta che avete ripristinato il computer o il dispositivo, oppure ne avete comprato uno nuovo, aggiornatelo e impostate gli aggiornamenti automatici.

- **Salvataggi**. Il passo più importante da seguire per proteggersi è di prepararsi con dei salvataggi regolari. Più frequentemente li effettuerete, meglio sarà. Alcune soluzioni vi permetteranno di salvare automaticamente ogni ora i file nuovi o modificati. Indipendentemente da quale soluzione di backup userete, controllate periodicamente di essere in grado di ripristinare questi file. Molto spesso l'unico modo per recuperare i vostri dati dopo un attacco saranno proprio i salvataggi.
- **Autorità giudiziarie**. Se, in qualsiasi modo, vi sentite minacciati, contattate le autorità giudiziarie.

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

Salvataggio e ripristino:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_it.pdf
Le Passphrase:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_it.pdf
Il malware:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_it.pdf
Tablet e sicurezza:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_it.pdf

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