OUCH! | Maggio 2014

La newsletter mensile sulla sicurezza informatica per gli utenti di

OUCH!

IN QUESTO NUMERO...

Il computer è stato compromesso. E Ora?

Introduzione

Tutti ci preoccupiamo di proteggere il computer e le informazioni in esso contenute, adottando le necessarie contromisure. Purtroppo, come accade anche per le auto, non importa quanta prudenza adottiamo nella guida: presto o tardi potrebbe capitarci di avere un incidente. In questa newsletter vi indicheremo cosa guardare per capire se il vostro computer è stato compromesso e, nel caso che lo sia stato, come porvi rimedio. Prima riuscite a capire che il vostro computer è stato compromesso e più rapidamente rispondete, meglio potrete mitigare ogni danno a voi e alla vostra azienda.

L'autore di questo numero

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) è Chief Scientist presso la CSRgroup Computer Security Consultants, nonché coautore dei corsi SANS "Memory Forensics (FOR526)" e "Malware Reverse Engineering (FOR610)".

Come capire se siete stati attaccati

Per prima cosa dovete sapere che in molti casi non esiste un unico modo per determinare se il vostro computer è stato compromesso. Esistono invece diversi indicatori: identificare la combinazione di alcuni di essi potrebbe indicare che siete stati attaccati. Ecco alcuni esempi:

- L'anti-virus ha fatto scattare un allarme comunicandovi che il vostro computer è stato infettato. Questa comunicazione arriva in particolare se comunica che non è stato in grado di rimuovere o mettere in quarantena i file interessati;
- la homepage del vostro browser è improvvisamente cambiata, oppure vi porta in siti web che non volevate vedere;
- sul vostro computer sono presenti account che non avete creato;
- ci sono dei programmi che non vi sembra di avere installato; il vostro computer continua ad andare in crash oppure funzions molto lentamente;
- un progrmamma vi chiede l'autorizzazione ad apportare modifiche al sistema, sebbene voi non abbiate installato o aggiornato nessuna applicazione
- il vostro firewall vi avvisa che un programma sconosciuto sta richiedendo il permesso di accedere Internet.

Il computer è stato compromesso. E Ora?

Cosa fare

Se pensate che il vostro computer sia stato compromesso, prima reagite meglio sarà. Se il sistema che state usando vi è stato assegnato dalla vostra azienda o viene utilizzato per lavoro, è consigliabile che non tentiate di sistemarlo da soli e che non lo spegniate: non solo potreste causare più danni che benefici, ma distruggereste delle evidenze che potrebbero essere utilizzate per un'investigazione. Comunicate invece l'incidente all'helpdesk, all'ufficio sicurezza o a un vostro superiore. Se per qualche ragione non potete contattare la vostra azienda o nel caso la reazione sia tardiva, disconnettete il computer dalla rete e mettetelo in modalità sospensione o ibernazione. Anche se non avete la certezza di essere stati attaccati, per precauzione è comunque consigliabile contattare l'ufficio interessato. La vostra azienda è certamente organizzata per gestire situazioni come queste.

Presto o tardi il vostro computer potrebbe venire compromesso: prima individuate l'incidente, meglio sarà.

Se invece utilizzate il computer per uso personale, ecco alcune azioni che potete compiere.

- **I salvataggi**. La più importante attività da svolgere è prepararsi per tempo con i salvataggi: salvate i vostri dati in modo regolare e controllate periodicamente di essere in grado di ripristinare i file dai backup. Spesso, quando un computer è stato compromesso, la sola opzione a disposizione è di riformattare il disco fisso e reinstallare il sistema operativo, o comprare un nuovo computer. In ogni caso, avrete bisogno dei salvataggi per ripristinare i vostri dati.
- **Cambiare la password**. Cambiate le password, non solo quelle del vostro computer o dei dispositivi mobili , ma anche quelle dei servizi online. Eseguite questa operazione da un computer diverso che considerate sicuro.
- **Anti-virus**. Se il vostro software anti-virus vi informa della presenza di un file infetto, potete eseguire le azioni che vi consiglia: normalmente si parla di porre il file in quarantena, eliminare il virus o cancellare il file. Molti software anti-virus presentano dei link a risorse che offrono spiegazioni dettagliate sulla specifica infezione. Nel dubbio, mettete il file in quarantena, ma se ciò non è possibile, eliminatelo.
- **Re-installare**. Se non siete in grado di ripulire il computer con un anti-virus, uno dei modi più sicuri per ripartire è ricostruire il computer da zero. Per prima cosa disconnettete il computer dalla rete; in seguito, seguite le istruzioni del produttore: in molti casi si tratta di utilizzare la partizione di ripristino

Il computer è stato compromesso. E Ora?

per reinstallare il sistema operativo. Se tale partizione non è utilizzabile, è corrotta o infetta, contattate il produttore e richiedete che vi invii un DVD di ripristino. Non reinstallate il sistema operativo dai backup, perché potrebbero essere soggetti alle stesse vulnerabilità che hanno permesso agli hacker di avere accesso al vostro computer. I salvataggi devono essere utilizzati unicamente per ripristinare i vostri dati personali. Infine, se il vostro computer è vecchio e datato, potrebbe essere più semplice (e forse anche economico) comprarne uno nuovo piuttosto che impiegare ore e ore per tentare di ripristinarlo.

- **Un supporto professionale**. Se credete che il computer sie astato infettato, ma non avete le capacità e le conoscenze per porvi rimedio, sarebbe opportuno chiedere l'aiuto di un professionista. Supponiamo, ad esempio, che vi rendiate conto che i vostri backup siano obsoleti o che siate tentati dal trasferire i vostri file personali (documenti, foto, video) dal sistema infetto al nuovo computer e che, nel fare questa operazione, trasferiate inavvertitamente anche il malware che vi ha infettato. Un'alternativa più sicura è di portare il computer infetto a un tecnico qualificato in grado di ripristinare i file senza rischiare di trasferire anche l'infezione.

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! Il salvataggio dei dati: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_it.pdf

OUCH! Le password: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201305_it.pdf

OUCH! Cos'è il Malware: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201402_it.pdf

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