SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Dicembre 2014

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Cos'è un Anti-Virus?

Introduzione

Un anti-virus è un programma di sicurezza che potete installare sul vostro computer o dispositivo mobile per proteggerlo da infezioni da malware. La parola "malware" sta a indicare qualsiasi tipo di software maligno, come virus, worm, Trojan e spyware. Il termine deriva, infatti, dalla combinazione delle parole malicious (maligno) e software. Se il vostro computer venisse infettato da malware potrebbe permettere a un attaccante di catturare tutto ciò che digitate, rubare i vostri documenti o usare il vostro computer per attaccarne altri. Al contrario di ciò che pensano in molti, ogni sistema operativo può essere infettato, anche il Mac OS X e Linux. Potete acquistare un software anti-virus come soluzione a sé stante oppure incluso in un pacchetto di sicurezza.

L'autore di questo numero

Jake Williams è il fondatore di Rendition Infosec (**www.renditioninfosec.com**) ed è anche un istruttore certificato nonché autore di corsi per il SANS Institute. Lo potete seguire su Twitter (**@MalwareJake**) e sul suo blog **malwarejake.blogspot.com**.

Purtroppo, uno dei problemi degli anti-virus è che essi non possono stare al passo con i criminali informatici, che costantemente sviluppano e rilasciano nuovi tipi di malware. Esistono così tante nuove versioni di malware rilasciate ogni giorno che nessun programma anti-virus può individuarle e proteggerle tutte insieme: ecco perché è fondamentale che capiate che sebbene gli anti-virus possano proteggere il vostro computer, non potranno fermare qualsiasi tipo di malware. Per comprenderne il motivo, cerchiamo di capire come funzionano questi programmi.

Come funzionano gli anti-virus

Esistono due modi principali in cui gli anti-virus identificano il malware: basandosi sulle firme o sul suo comportamento. L'individuazione basata su firme funziona come il sistema immunologico umano: viene effettuata una scansione del computer alla ricerca delle caratteristiche di programmi maligni conosciuti facendo riferimento a un dizionario di malware conosciuti. Nel caso che un file del vostro computer contenga una firma corrispondente a una voce del dizionario, il programma cercherà di neutralizzarlo. Come accade nel sistema immunitario umano con i sieri antiinfluenzali, l'approccio a dizionario richiede continui aggiornamenti, per poter far fronte a nuovi ceppi di malware. Gli anti-virus possono proteggere contro ciò che riconoscono come dannoso. Purtroppo i criminali informatici sviluppano nuovo malware così velocemente che i produttori di anti-virus non riescono a farvi fronte; non importa quanto recentemente il vostro anti-virus sia stato aggiornato: ci sarà sempre una nuova variante di malware che potrà potenzialmente evitarlo.

Cos'è un Anti-Virus?

Attraverso l'individuazione del comportamento, un anti-virus non tenta di identificare malware conosciuti, ma controlla il comportamento del software installato sul vostro computer. Quando un programma si comporta in modo anomalo, tentando ad esempio di accedere a un file protetto o di modificare un altro programma, gli anti-virus di questo tipo individuano il comportamento sospetto e inviano un avviso. Questo approccio offre una protezione contro i nuovi tipi di malware non ancora presenti nei dizionari. Purtroppo anche questo approccio non è infallibile poiché uno dei problemi è la generazione di falsi positivi: potreste non essere sicuri di ciò che dovete permettere o bloccare e, a un certo punto, potreste perdere la sensibilità di fronte a questi avvisi e clicare su "Accetta" su ogni finestra di avviso, lasciando così il computer aperto a ogni genere di attaco e infezione. Una volta che il comportamento è stato individuato, il malware è già stato eseguito dal vostro sistema e voi potreste non sapere quali attività ha svolto prima che l'anti-virus sia stato identificato.

Sebbene l'anti-virus sia un componente importante della sicurezza, non è in grado di individuare e bloccare tutti gli attacchi. La miglior difesa non è la tecnologia: siete voi.

Gli anti-virus costituiscono una parte importante della sicurezza di computer e dispositivi mobili: laddove possibile vi raccomandiamo di installarli e usarli. In ogni caso, sebbene il punto fondamentale sia ricordarsi che non è possibile proteggersi da qualsiasi tipo di malware, sappiate che siete voi, e non la tecnologia, la migliore difesa contro gli attacchi informatici di oggi.

Alcuni suggerimenti

1. Ottenete il software anti-virus solo da fonti conosciute e di fiducia, meglio se da un rivenditore: è uno stratagemma comune tra i criminali distribuire programmi anti-virus falsi che, al contrario, sono del vero e proprio malware.
2. Assicuratevi che l'anti-virus installato sia aggiornato, che il vostro abbonamento annuale sia stato pagato e attivo e che il programma sia configurato per aggiornarsi automaticamente. Se il computer è rimasto offline o spento per un certo tempo, il vostro anti-virus avrà bisogno di aggiornarsi al momento dell'accensione. Non ritardate questo importante aggiornamento.
3. Verificate che l'anti-virus scansioni automaticamente i dispositivi rimovibili, come le chiavette USB, e che la protezione in tempo reale (real time protection) sia attiva.
4. Fate attenzione agli avvisi a schermo generati dall'anti-virus: molti di essi prevedono la possibilità di ottenere maggioni informazioni o racomandazioni su cosa fare. Se ricevete un avviso sul vostro computer al lavoro, contattate l'helpdesk o il vostro responsabile.

Cos'è un Anti-Virus?

5. Non disabilitate o disinstallate l'anti-virus perché ritenete che stia rallentando il computer, bloccando un sito web o impedendovi dall'installare un'app o un programma. Disabilitare l'anti-virus vi esporrebbe a un rischio non necessario e potrebbe provocare un grave incidente di sicurezza. Se state lavorando in azienda e il problema persiste, contattate il vostro helpdesk. Nel caso che invece ciò accada sul vostro computer personale, cercate di contattare il produttore dell'anti-virus, visitando il sito web per trovare maggiori informazioni o sostituendo l'anti-virus con un altro prodotto.
6. Non installate più di un anti-virus sul computer, poiché ciò potrebbe causare conflitti tra le vostre applicazioni e ridurre la sicurezza del vostro computer.
7. Imparate a riconoscere i segnali prodotti dal vostro anti-virus. I criminali informatici possono creare siti web maligni dai quali diffondere avvisi prodotti da anti-virus falsi per aiutarvi a sistemare il vostro computer. Cliccare su questi link può causare seri danni al vostro computer.

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

Confronto tra Anti-Virus:	http://www.av-test.org/en/
Social Engineering:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_it.pdf
Email e Phishing:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_it.pdf
Il computer è stato compromesso. E Ora?:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-2014-05_it.pdf

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