Virus e antivirus: una battaglia infinita

I tradizionali software per la sicurezza sono disarmati di fronte agli attacchi informatici sempre più sofisticati. Ma altre risorse sono pronte a scendere in campo.

Tom Simonite

Questa estate i laboratori che si occupano di sicurezza informatica in Iran, Russia e Ungheria hanno annunciato la scoperta di Flame, che il centro di ricerca ungherese CrySyS ha definito «il più complesso malware mai incontrato».

Per almeno due anni, Flame ha copiato documenti, ha "catturato" schermate di file, registrazioni audio, sequenze di battute di tasti e chiamate telefoniche su Skype da computer infettati. Tutti questi dati sono stati trasmessi ai server controllati dagli hacker. Fino a oggi, nessun software per la sicurezza aveva lanciato l'allarme.

La scoperta di Flame è solo l'ultima che indica come il tradizionale software antivirale sia un sistema ormai superato per proteggere i computer dai malware. «Flame è stata la Caporetto dell'industria degli antivirus», ha scritto Mikko Hypponen, il fondatore dell'azienda di antivirus F-Secure. «Avremmo dovuto fare molto di più, ma non ne siamo stati capaci. Siamo chiusi nell'angolo».

I programmi per la sicurezza dei computer di aziende, governi e consumatori funzionano allo stesso modo: le minacce vengono rilevate confrontando i codici dei programmi e le loro attività con una banca dati di malware conosciuti. Le aziende per la sicurezza come F-Secure e McAfee sono alla ricerca costante di nuovi malware per aggiornare la loro lista. L'obiettivo è di creare un muro invalicabile per i malintenzionati.

In realtà, negli ultimi anni gli attacchi a governi e aziende hanno utilizzato software che, sia pure non sofisticati come Flame, hanno aggirato il sistema di difesa basato sul riconoscimento delle tracce. Alcuni esperti e aziende sostengono che sia giunto il momento di modificare questa forma di protezione. «Gli antivirus tradizionali rimangono una componente importante della difesa dai malware, ma devono venire affiancati da altri rimedi», afferma Nicolas Christin, ricercatore della Carnegie Mellon University. «Dobbiamo cambiare logica e non intestardirci a costruire una specie di linea Maginot, che viene regolarmente elusa dagli hacker».

Christin e diverse startup che si occupano di sicurezza, sono impegnati nella creazione di nuove strategie difensive per rendere gli attacchi più difficili e aiutare chi li subisce.

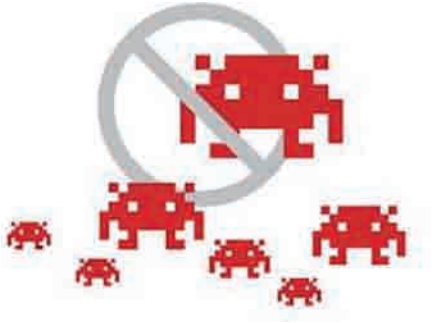
Un ottimo esempio della nuova linea di azione è costituito da CrowdStrike, un'azienda fondata da esperti del settore antivirus, che ha raccolto 26 milioni di dollari di fondi d'investimento. Dmitri Alperovitch, responsabile tecnologico e cofondatore di CrowdStrike, sostiene che l'azienda ha intenzione di presentare un sistema intelligente di allarme per segnalare qualsiasi tipo di attacco e la sua provenienza.

Questo sistema è realizzabile, dice Alperovitch, perché l'hacker, oltre a modificare facilmente il codice di un virus come Flame per sfuggire agli scanner dell'antivirus, dovrebbe avere un obiettivo primario: accedere ed estrarre dati di valore. Comprensibilmente, CrowdStrike non vuole rivelare dettagli della sua tecnologia, ma è verosimile che prenda in considerazione le attività del sistema dell'utente per individuare una eventuale infiltrazione.

Le nuove strategie del chi e non del come

La strategia è quella di ostacolare le tattiche più diffuse e di rendere la vita più dura ai malintenzionati, invece di concentrarsi sugli strumenti, in continua evoluzione, impiegati dagli hacker. «Dobbiamo guardare a chi spara, non alla pistola», come sostiene Alperovitch.

Altre aziende la pensano nello stesso modo. «È necessario convincersi che, come direbbe un tutore dell'ordine, "il crimine non paga"», afferma Sumit Agarwal, cofondatore della startup Shape Security. L'azienda ha raccolto 6 milioni di dollari dagli investitori, tra cui Eric Schmidt, presidente di Google. Anche Shape Security mantiene uno stretto riserbo sulla sua tecnologia, ma Agarwall dice che l'obiettivo è quello di alzare il costo dell'attacco informatico rispetto al ritorno economico, vanificandolo.



Alperovitch dice che la sua azienda collaborerà con le vittime, nei limiti delle leggi, per identificare chi si trova dietro gli attacchi. «Azioni di "difesa attiva" possono sconfinare nell'illegalità, ma non è illegale intraprendere iniziative nei confronti delle persone che traggono vantaggi dai dati "rubati", alzando in tal modo i costi commerciali di chi attacca un sistema», spiega Alperovitch. Si può, per esempio, chiedere al governo di sottoporre il caso alla Organizzazione Mondiale per il Commercio e rendere di dominio pubblico quanto è successo, per denunciare chi ha condotto l'operazione di spionaggio industriale.

Christin e i suoi colleghi universitari hanno evidenziato come si possano intraprendere azioni legali relativamente semplici per neutralizzare le operazioni di crimine informatico. La loro ricerca ha preso in considerazione le tecniche di manipolazione dei risultati della ricerca, volte a promuovere prodotti farmaceutici illeciti, arrivando a concludere che l'inganno si sarebbe potuto bloccare operando su un esiguo numero di servizi che reindirizzano i visitatori da una pagina Web a un'altra. Lo scorso anno, alcuni ricercatori dell'Università della California, a San Diego, hanno dimostrato che una larga parte dello spam passa attraverso tre sole banche dati.

Comunque Agarwal mette in guardia sui "pericoli" della denuncia legale. «Immaginate di essere una grande azienda e di entrare accidentalmente in rotta di collisione con la mafia russa. Potreste mettere in moto un meccanismo incontrollabile». ■

Tom Simonite lavora nella redazione di San Francisco come responsabile dell'area software e hardware della edizione americana di MIT Technology Review.