

Attacchi Informatici in Continua Evoluzione

Le tecniche e le metodiche di infezione via Internet cambiano nel tempo, costringendo l'utente a un costante aggiornamento delle proprie strategie di difesa. Luca Simonelli, Regional Director (Italy, Greece, Balkans and Turkey) di Fortinet Inc., ci parla delle ultime evoluzioni in tema di minacce e sicurezza.

Cos'è il mercato UTM (Unified Threat Management), di cui Fortinet è azienda leader?

L'utm è il mercato degli apparati che incorporano al loro interno più sistemi di sicurezza. Per essere classificate come aziende appartenenti a questa categoria bisogna produrre applicazioni di sicurezza con almeno quattro componenti quali "firewall", "VPN" (*Virtual Private Network*), "intrusion prevention" e "antivirus".

Perché il mercato UTM cresce così rapidamente?

I motivi che hanno portato all'affermarsi di questo mercato sono sostanzialmente due. Il primo, di natura economica, è stata la consapevolezza che nelle organizzazioni aziendali, acquisire un solo apparato che incorpora differenti soluzioni di sicurezza ("firewall", "antivirus", eccetera) risulta molto più conveniente rispetto all'acquisizione di elementi separati. Ciò risulta particolarmente evidente in *deployment* su larga scala quando occorre installare centinaia o migliaia di apparati di fascia medio/bassa. Il secondo, *di natura tecnologica*, è stata l'evoluzione del tipo di attacchi e di minacce informatiche. Prima, infatti, erano degli attacchi monotematici (o solo "virus", o solo "worm", eccetera) ben specifici; attualmente, invece, sono vere e proprie "combinazioni" di questi ultimi, definite "blended threats".

Cos'è una "blended threat"?

Letteralmente significa "minaccia combinata". In pratica è una minaccia che utilizza differenti mezzi di propagazione e richiede protezione e risposta da differenti soluzioni di sicurezza. Avere un approccio integrato, infatti, riesce a fornire una risposta più efficace. Inoltre, gli attacchi sono sempre più veloci e il tempo di reazione si è ridotto a ore, se non addirittura a minuti.

Come si stanno evolvendo gli attacchi di rete?

Stiamo assistendo a un nuovo fenomeno chiamato "pharming". Il "pharming" è una truffa molto simile al "phishing", che indirizza gli utenti a un sito fasullo con l'intenzione di carpire dati sensibili (come per esempio i numeri delle carte di credito, o le password). Un attacco di questo tipo colpisce tutti gli utenti che in un certo momento cercano di connettersi a un certo sito ed è molto difficile da individuare. Il sito web viene replicato in modo identico all'originale senza alterare l'indirizzo web (URL - *Uniform Resource Locator*). L'utente digita il nome del sito a cui vuole collegarsi e automaticamente viene rediretto su di un sito che è la copia speculare di quello cercato.

In cosa differisce dal "phishing"?

Praticamente il "pharming" ne è l'evoluzione. Con il "phishing" si carpiscono dati sensibili degli utenti tramite alcuni trucchi, come per esempio una finta pagina web. Con il

“pharming”, invece, pur essendoci sempre un falso sito, molto simile o del tutto identico all’originale, e il form di registrazione, nel quale gli utenti inseriscono i dati di cui ci si vuole appropriare, quello che cambia è la modalità di direzionamento al sito truffaldino. Il “phishing” attacca mediante posta elettronica e presuppone una certa azione da parte dell’utente, mentre il “pharming” attacca in maniera molto più insidiosa e senza che l’utente venga attirato in alcuna trappola.

Come ci si può proteggere dagli attacchi di nuova generazione?

La sicurezza dei moderni sistemi informativi aziendali è un problema comune a molte aziende che, sempre più frequentemente, sono vittime di attacchi di ‘pirati informatici’ sistematici e organizzati, che penetrano nell’azienda sfruttando i molteplici punti di connessione a Internet delle reti aziendali. Per fronteggiare il problema serve innanzi tutto avere qualche meccanismo di protezione. Un aiuto concreto viene dai certificati digitali che entrano in funzione quando si accede al sito home banking della propria banca. Il certificato serve a garantire il colloquio esclusivo con la banca e assicura che le informazioni scambiate non sono state modificate da soggetti terzi durante il tragitto.

Quale sistema di sicurezza bisogna adottare?

Non è possibile ipotizzare l’esistenza di un sistema di sicurezza valido per ogni tipo di impresa. La pianificazione delle politiche e degli strumenti da impiegare per la gestione della sicurezza dei sistemi informatici dipende direttamente dalla struttura organizzativa e dalla distribuzione geografica dell’impresa, da quali rischi essa intende difendersi e da quanto è disposta a investire nella sicurezza.

La tecnologia della sicurezza riesce sempre a mantenere il passo in termini di evoluzione?

Chi sviluppa “virus” o, più in generale, *malware* (cioè software creati con il solo scopo di arrecare danni più o meno estesi al computer su cui vengono eseguiti) sempre più sovente fa uso di algoritmi che sfruttano falle di sicurezza, vulnerabilità e *bug* più o meno noti, dei componenti software usati per operare in rete. L’obiettivo è sempre lo stesso, cercare di insediarsi il più facilmente possibile su un maggior numero di sistemi e diffondersi con rapidità e magari senza che l’utente possa accorgersene. È un po’ come giocare a guardie e ladri. Diciamo che l’industria cerca in tutti i modi di mantenersi al passo rispondendo agli *hacker* con tecniche sempre nuove e sempre più efficaci.

Cosa offre Fortinet?

La nostra famiglia di “firewall antivirus” rappresenta la nuova generazione di sistemi di protezione della rete “real time”. Questi prodotti consentono di rilevare ed eliminare le minacce più pericolose, provenienti da e-mail, web e traffico di trasferimento “file”, come “virus”, “worm”, “intrusioni”, “contenuto web dannoso” e molto altro. In tempo reale e senza compromettere le prestazioni della rete. I nostri sistemi, inoltre, sono gli *unici* prodotti di protezione a adottare una accelerazione hardware basata su di uno specifico microchip ASIC, capace di effettuare l’analisi dell’intero traffico in “real time”. I nostri apparati sono anche gli unici ad avere ottenuto per cinque volte la certificazione ICSA e offrono una gamma completa di servizi a livello applicazione e rete, su piattaforme integrate e di facile gestione.

Intervista a cura di Titti Acone