Spear Phishing: eliminare il veleno dai documenti infetti

Date : 10 ottobre 2016

Cosa collega le massicce violazioni di dati compiute a danno di grandi retailer come Target e Neiman Marcus, del gigante delle assicurazioni sanitarie Anthem e di Sony Pictures?

Hanno tutte avuto inizio con un attacco phishing costruito in modo ingegnoso, usando messaggi email con allegati infetti da malware, progettati per sembrare legittimi pren10dendo di mira dipendenti specifici all'interno dell'organizzazione.

Questo tipo di attacco mirato si chiama spear phishing: è la tecnica più comune per una ragione molto semplice: funziona, spesso ingannando persino gli utenti più esperti di sicurezza e permettendo agli hacker di entrare fisicamente nelle reti.

Una ricerca di Check Point condotta su oltre 10.000 organizzazioni in tutto il mondo ha messo in luce come l'84% di esse avesse scaricato un documento infetto nei precedenti 12 mesi.

Questo perché è relativamente semplice per un hacker profilare un'organizzazione o un individuo partendo dalla loro presenza online, e creare un'email capace di ingannare persino il dipendente più attento, inducendolo ad aprire quel documento infetto e a scatenare l'attacco malware.

ELUDERE IL RILEVAMENTO

Il problema nasce dal modo in cui funzionano gli antivirus tradizionali basati su signature. Sono veloci, ma possono solo rilevare malware che è già stato identificato: non possono rilevare le nuove infezioni da malware zero-day.

Questo è un problema perché, se il codice per la gran parte delle nuove infezioni è nascosto nei tipi di file più comuni che tutti usiamo per lavoro - email, documenti Word, PDF, fogli Excel e così via – esistono toolkit che possono oscurare questi script eseguibili, per mascherare le loro azioni malevole e aiutare a eluderne il rilevamento. Questo riduce al 93% circa l'accuratezza di un antivirus convenzionale.

Le soluzioni di sandboxing rappresentano un metodo utile per fermare malware zero-day non

identificato, ma possono richiedere anche diversi minuti prima che la minaccia venga rilevata, esponendo di fatto la rete ai rischi di un'infezione. Per questo, l'efficacia di alcune soluzioni di sandboxing arriva solo al 95%.

E se la formazione a una maggiore consapevolezza può certo mitigare la minaccia spear phishing, non può eliminarla del tutto: le persone tendono a fidarsi, e vogliono fare il loro lavoro nel modo più efficiente possibile.

Così quando ricevono un documento PowerPoint via email inaspettato, che sembra provenire da un altro dipartimento o da un'azienda con cui già collaborano, non per forza penseranno alla possibilità che si tratti di un potenziale attacco.

È quindi necessario un nuovo approccio per affrontare queste minacce ed eliminare il malware prima che abbia l'opportunità di raggiungere la casella di posta dei dipendenti.

MAI FIDARSI

Come detto prima, la stragrande maggioranza del malware si nasconde all'interno delle più comuni tipologie di file – documenti Microsoft Office Word, Excel, PowerPoint e Adobe PDF – e per l'attivazione attende che l'utente clicchi sul file. Le tecniche convenzionali anti-malware comportano un approccio 'fidati, ma verifica' di ispezione dei file allegati per vedere se questi contengono malware, e poi bloccarli. Ma questo non fornisce la precisione totale di rilevamento necessaria per proteggere completamente le reti da rischi potenziali.

Non è meglio da un punto di vista della sicurezza invertire questo pensiero, e assumere che qualsiasi documento allegato sia sempre infetto – e pulirlo da qualsiasi potenziale minaccia prima di passarla all'utente, in modo da eliminare completamente il rischio di attacco attraverso questo vettore?

Questo approccio è chiamato threat extraction. Funziona a livello del gateway di rete dell'organizzazione, ispezionando in tempo reale le email nel momento in cui vengono inviate all'azienda.

Quando al messaggio email è allegato un documento, la soluzione lo scompone e rimuove qualsiasi contenuto o codice identificabile come malware o potenzialmente sfruttabile in questo senso, come macro, oggetti e file embedded e link esterni.

Il documento viene poi ricostruito con elementi riconosciuti come sicuri e inoltrato al destinatario, nel suo formato file originale o come PDF non modificabile, seguendo le richieste del team IT dell'organizzazione. L'intero processo richiede meno di un secondo, eliminando preventivamente ogni rischio dai file infetti.

Per la maggioranza dei file il processo è del tutto trasparente, poiché la maggior parte dei documenti non hanno contenuti embedded o macro. Per questo, i dipendenti non noteranno alcun ritardo nel ricevere i file.

Può esserci il caso di un documento complesso (come una presentazione PowerPoint) che arrivi da una fonte legittima e sia assolutamente innocuo, pur contenendo macro e file integrati che il processo di Threat Extraction rimuoverebbe. In questi casi, oltre a inoltrare il documento pulito, la soluzione Threat Extraction conserva il file originale, in modo che possa essere analizzato dagli antivirus e dai sistemi sandboxing tradizionali per determinare se è sicuro e se l'utente può accedervi. La soluzione tiene anche traccia delle istanze malware identificate nei file ricevuti, consentendo ai team di sicurezza di identificare modelli potenzialmente in grado di indicare una campagna specificamente mirata a un'organizzazione.

Threat Extraction offre alle aziende un livello ulteriore di protezione contro forme distruttive di malware in arrivo tramite email mirate. Se gli hacker continueranno a lanciare attacchi utilizzando questo vettore, Threat Extraction consente alle aziende di eliminare il veleno dai documenti infetti.

Articolo a cura di **Noam Green**, Product Manager di Check Point