L'IMPORTANZA DELLE SANDBOX DI RETE PER BLOCCARE I RANSOMWARE

Perché è necessario utilizzare sandbox, firme e algoritmi euristici

Abstract

I firewall di nuova generazione sfruttano le firme e l'euristica con grande efficacia, ma quando si tratta di proteggersi dagli attacchi dannosi attualmente in circolazione, non sono più sufficienti. Gli attacchi mirati e le minacce zero-day rendono indispensabile utilizzare anche un sistema sandbox per garantire una protezione realmente efficace.

Capire dove sta la vera sfida per rispondere adeguatamente

Le minacce esterne si stanno evolvendo in modo sbalorditivo. Gli aggressori combinano il carattere opportunistico dell'automazione e l'approccio dei produttori di software per sviluppare costantemente le proprie minacce, con l'obiettivo di arrivare inosservati il più lontano possibile. Considerando i danni che un'azienda subisce nel caso di una violazione dei dati o di un attacco ransomware, individuare un codice maligno prima che entri e agisca nella propria rete è divenuto un imperativo per le organizzazioni IT.

La vera sfida non consiste tanto nel ransomware in sé, che magari è già diffuso su internet, bensì negli attacchi mirati e nelle minacce zero-day. Gli attacchi mirati vengono perpetrati con un codice mai visto prima, creato ad hoc per l'organizzazione presa di mira, mentre le minacce zero-day sfruttano le vulnerabilità appena scoperte per le quali non sono ancora disponibili patch correttive. Le aziende dovrebbero preoccuparsi soprattutto per questi tipi di aggressioni, che in genere sono ben più efficaci e dannose delle precedenti controparti. Dunque, qual è il modo migliore per impedire che una minaccia si diffonda all'interno della propria rete?

Si può scegliere tra più opzioni in termini di dove affrontare gli attacchi e come rilevarli ed eliminarli. L'obiettivo è riconoscere e rimuovere il codice maligno nel punto più vicino possibile alla fonte dell'aggressione. Per quanto riguarda il dove affrontare l'attacco, le organizzazioni adottano tipicamente due strategie: alcune si affidano alla sicurezza degli endpoint, lasciando che il codice maligno arrivi fino agli endpoint, dove viene rilevato e distrutto; altre scelgono le sandbox, dove questi codici vengono identificati ed eliminati prima che entrino in rete. In attesa di una soluzione efficace al 100%,

Gli attuali codici maligni sono talmente avanzati che per rilevarli occorre un approccio multilivello. Sia le firme che l'euristica hanno però dei limiti.

entrambe queste tecnologie continueranno probabilmente a fornire importanti livelli di difesa. Se implementata nel modo giusto, una sandbox può rappresentare un'ottima soluzione preventiva.

Tenere fuori i codici maligni

Se pensiamo a una rete aziendale come a un castello, il luogo migliore per bloccare un attacco è certamente l'entrata, un piccolo varco in cui qualsiasi persona o cosa può essere ispezionata prima di consentirne l'ingresso. Implementare una soluzione in grado di riconoscere un codice maligno già all'interno del firewall di nuova generazione (NGFW) è come mettere una guardia all'ingresso del castello. Niente e nessuno può entrare senza che la guardia lo sappia. Quando i dati entrano, sono sottoposti a diversi metodi di scansione per rilevare i codici dannosi:

- Firme
  Il traffico dati viene ispezionato in base a un database di firme digitali maligne per rilevare eventuali corrispondenze. In caso di corrispondenza, il codice in questione viene contrassegnato come dannoso.
- Euristica
  A differenza di quanto avviene con le firme, ossia una ricerca di corrispondenze specifiche all'interno di un database, la scansione di tipo euristico sfrutta regole e algoritmi per rilevare codici potenzialmente dannosi.
- Sandbox
  Anziché passare al vaglio tutti i codici per trovare firme maligne o potenzialmente dannose, la sandbox consente di far "detonare" i codici, ossia lasciare che si attivino e agiscano come previsto, monitorando la reazione per rilevare attività non regolari. Questo processo avviene in un ambiente creato appositamente, detto sandbox, nel quale nulla di grave può accadere.

La combinazione di queste strategie è la soluzione più efficace ed efficiente: i malware più facili da riconoscere e affrontare possono essere gestiti con le tecnologie tradizionali, più rapide e meno onerose, permettendo alla sandbox di concentrarsi sui restanti contenuti, quelli che davvero richiedono i suoi livelli di analisi.

Perché firme ed euristica non bastano

L'efficacia del rilevamento basato su firme è direttamente proporzionale alla qualità e completezza del database utilizzato per identificare i codici maligni. Anche se il database è aggiornatissimo, un attacco potrebbe comunque sfuggire a questo tipo di rilevamento perché i fornitori di antivirus impiegano del tempo per identificare i malware, aggiornare i database e distribuirli ai clienti. Inoltre, chi crea codici dannosi conosce i sistemi di rilevamento basati su firme e quindi utilizza codici che li evitano.

Persino l'euristica può rivelarsi inaccurata. Alcuni codici o parti di codice possono essere semplicemente traffico che non rispecchia lo schema previsto e perciò possono dar luogo a falsi positivi. A volte, un codice maligno non sembra inizialmente dannoso finché non viene riassemblato alla fine, rendendo inefficace la tecnologia euristica.

Basti pensare ai ransomware. Il codice inizialmente scaricato non è dannoso, ma lo diventa nel momento in cui si connette a un server di comando e controllo (C2) e scarica un codice aggiuntivo. Un altro esempio è una macro all'interno di un documento di Microsoft Word. A meno che la macro dannosa non utilizzi un metodo di attacco noto o sospetto, né il rilevamento basato su firme né l'euristica sono in grado di stabilire se la macro sia di per sé innocua o dannosa.

L'utilizzo di firme o di algoritmi euristici per effettuare una scansione passiva del traffico presenta dei limiti. La scansione non permette al codice di attivarsi e gli aggressori sono abili nell'occultare i loro codici maligni (alla scansione) celandoli all'interno di codici "benigni". Pertanto, la maniera più efficace di individuarli è interagire con la loro versione completamente "armata".

Giocare col fuoco

L'unico modo per rilevare i codici maligni avanzati è "farli detonare".

Si tratta di un processo totalmente diverso dalla semplice scansione, è come realizzare

la coltura di un microbo pericoloso in un laboratorio di biosicurezza, o far brillare una bomba in una camera di contenimento. La sandbox è un ambiente sicuro in cui lasciare che i dati intercettati si attivino e facciano il loro corso sotto stretta osservazione. Nel caso in cui il comportamento sospetto o dannoso venga confermato, il file in questione e la minaccia in esso contenuta possono essere eliminati.

La sandbox cerca di far detonare tutti i tipi di file:

- File con contenuto attivo
  Questi file, che includono contenuti eseguibili, script e DLL, sono lasciati liberi di attivarsi e interagire normalmente con la sandbox, in modo da monitorarne eventuali azioni dannose come la modifica alle impostazioni del firewall del sistema operativo o il collegamento verso l'esterno a Internet.
- File con contenuto passivo
  Questi file includono qualunque tipo di documento, tra cui PDF, file compressi (ad es., ZIP, JZIP, RAR) e persino file d'immagine. Vengono analizzati utilizzando la loro applicazione di default per verificarne eventuali attività pericolose, come ad es. una macro di Word che tenta di scaricare un codice supplementare da Internet. Se la sandbox non è dotata di tutti i software necessari, è impossibile analizzare tutti i file passivi. Quindi è bene configurarla in modo che sia in grado di verificare il maggior numero possibile di tipi di file.

Malware nelle immagini

Essendo la tipologia di dati apparentemente più innocua, ci si potrebbe chiedere quale sia la necessità di esaminare i file d'immagine. Eppure anche questi file possono contenere dati di payload dannosi. Consideriamo ad esempio il recente attacco avvenuto in Brasile, dove un allegato in formato PDF conteneva un link a un file ZIP, al cui interno erano presenti un eseguibile e un file PNG (Portable Network Graphics). Il PNG era piccolo (meno di 64 pixel quadrati), ma il file aveva una dimensione di oltre 1 MB. Analizzando l'eseguibile accluso, è apparso chiaro che il codice era progettato per estrarre dal PNG un codice binario dannoso nascosto e attivarlo.

Migliorare le firme con la sandbox

Come già accennato, un approccio su più livelli è il modo migliore per rilevare i codici dannosi. Anche migliorando il metodo di scansione passiva si può contribuire

Le notevoli energie che vengono spese per celare i codici maligni dimostrano quanto è necessario dotarsi di una sandbox in cui far detonare tutti file che entrano nella propria rete.

a rendere più efficiente il processo di rilevamento, poiché servono molti meno cicli di CPU per eseguire il controllo in base a un database di firme di quanti ne servano per generare e supportare una sandbox in grado di far detonare un solo codice maligno.

Oltre che per la detonazione, la sandbox è utilizzabile per generare firme una volta stabilito che un codice è maligno. Dopotutto, il vantaggio di eseguire il codice consiste proprio in questo. Una volta identificato un codice dannoso viene creata anche la firma corrispondente, che può essere aggiunta al database delle firme, incrementando così la rapidità e l'accuratezza di rilevamento di futuri codici dannosi.

Ma le tecniche di scansione passiva hanno anch'esse delle criticità di rilevamento. È quindi lecito chiedersi se una sandbox sia realmente più efficace.

Come funziona una sandbox

La sandbox è un ambiente che, come un "agnello sacrificale", monitora il codice maligno e il modo in cui esso interagisce con il sistema operativo. Le sandbox cercano:

- Chiamate del sistema operativo, incluso il monitoraggio delle chiamate di sistema e delle funzioni API.
- Modifiche al file system: qualsiasi azione compresa la creazione, la modifica, la cancellazione e la criptazione dei file.
- Modifiche di rete: qualunque connessione anomala che viene stabilita verso l'esterno.
- Modifiche di registro: qualsiasi modifica volta rendere persistenti o a modificare le impostazioni di sicurezza o della rete.
- Altre variazioni, anche temporanee: monitoraggio delle istruzioni che un programma esegue tra una chiamata del sistema operativo e l'altra, per integrare o completare il contesto di altre osservazioni.

Quanto è efficace una sandbox?

Un sistema di rilevamento basato sulle firme è perfetto per scoprire i codici maligni già noti, ma è totalmente inefficace contro gli attacchi zero-day o attuati con una semplice mutazione (ossia con un malware specifico che, per via di una mutazione, non corrisponde ad alcuna firma). L'euristica rappresenta un passo avanti nella giusta direzione, in quanto cerca anomalie nei codici. È stato però dimostrato che, se si utilizza un file d'immagine per veicolare payload, i file iniziali (ad es. un PDF con un link a un file ZIP esterno) non suscitano alcun sospetto.

Ecco perché le sandbox sono un metodo di rilevamento così efficace: sono l'unico modo per rilevare i comportamenti dannosi anche in caso di attacco zero-day senza firma e di un codice mai visto prima. In fin dei conti un codice maligno esegue poche azioni, tra cui connettersi all'esterno, scaricare payload aggiuntivi, collegarsi a un server C2 e tentare di apportare modifiche al sistema operativo. Nessuna di queste azioni è normale per i comuni file di lavoro.

Conclusioni

Esistono diverse soluzioni per proteggere la propria organizzazione dai codici maligni. Proteggere gli endpoint è certamente importante, ma lasciando entrare questi codici nella propria rete si può esporre l'azienda a rischi notevoli. L'utilizzo di una sandbox consente di bloccare le minacce ancora prima che entrino nella propria rete.

Maggiori informazioni. Scopri gli elementi distintivi da considerare nella tua strategia d'uso delle sandbox. Leggi il nostro documento "*Putting a solid sandbox strategy in place*" (Come realizzare una solida strategia di sandboxing).

Informazioni su SonicWall

Da oltre 25 anni SonicWall è il partner di fiducia nel campo della sicurezza. Dalla protezione di rete alla sicurezza degli accessi fino alla protezione dell'email, SonicWall ha costantemente ampliato la sua gamma di prodotti permettendo alle aziende di fare innovazione, accelerare e crescere. Con oltre un milione di dispositivi di sicurezza in quasi 200 paesi e aree del mondo, SonicWall consente ai suoi clienti di guardare al futuro con fiducia.

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

ExecBrief-WhyNetworkingSandboxing-US-VG-24857

SONICWALL™