Protezione dal malware basato sugli script

Gli autori di malware hanno reso arduo il rilevamento utilizzando tecniche come il polimorfismo, l'installazione di watchdog, la revoca delle autorizzazioni e molti altri metodi.

Nel corso di questo decennio, abbiamo osservato gli aggressori sfruttare funzionalità come Microsoft Windows Management Instrumentation (WMI) e Windows PowerShell per compromettere gli endpoint senza mai memorizzare un file binario su disco, assicurandosi che un attacco rimanesse difficile da tracciare, dal momento che il codice dannoso può essere inserito direttamente nel registro di un host compromesso.

Le infezioni basate sugli script circolano ormai da anni. Sebbene fossero considerate senza file, famiglie di malware precedenti avrebbero depositato un piccolo file binario sul disco nell'attacco iniziale prima di passare alla memoria principale di un sistema.

Tuttavia, le ultime tecniche di evasione usate malware di scripting non lasciano tracce sul disco, rendendo più difficile il rilevamento, che si basa generalmente sulla ricerca di file statici. Leggi la nostra analisi approfondita del malware basato sugli script nel *Report McAfee Labs sulle minacce: settembre 2017.*

Sono tre le tipologie comuni di malware basato sugli script:

- **Residente in memoria:** questo tipo di malware utilizza lo spazio della memoria di un file Windows legittimo. Carica il suo codice in quello spazio di memoria e rimane lì finchè qualcuno non vi accede o lo riattiva. Sebbene l'esecuzione avvenga all'interno dello spazio di memoria di un file legittimo, esiste un file fisico dormiente che avvia o riavvia l'esecuzione.
- **Rootkit:** alcuni malware nascondono la loro presenza dietro un'API (Application Programming Interface) di un utente o a livello di kernel. È presente un file su disco ma in modalità furtiva.
- **Registro di sistema di Windows:** alcuni tipi avanzati di malware basato sugli script risiedono all'interno del registro di sistema di Windows. Gli autori di malware hanno sfruttato caratteristiche in passato come la cache anteprime di Windows, utilizzata per archiviare immagini per la visualizzazione anteprima di Explorer. La cache anteprime opera come un meccanismo di persistenza per l'attacco. Il malware di questo tipo deve ancora entrare nel sistema della vittima attraverso un codice binario statico. La maggior parte utilizza l'email come vettore d'attacco per raggiungere il sistema. Una volta che l'utente ha fatto clic sull'allegato, il malware scrive il file di payload completo in una forma crittografata nell'hive del registro di sistema di Windows. Quindi scompare dal sistema cancellandosi.

Oggi, gli autori del malware creano intelligentemente le famiglie di malware basate sugli script per eseguire attacchi completamente senza file al registro di sistema di Windows senza lasciare alcuna traccia sul file system. Sebbene l'ambiente per eseguire questi attacchi venga preparato eseguendo il codice contenuto in un file, il file si cancella automaticamente una volta che il sistema è pronto per perpetrare l'azione dannosa.

Policy e procedure per proteggersi dal malware basato sugli script

Le migliori e più recenti procedure di McAfee in termini di protezione informatica raccomandano l'adozione delle seguenti strategie generali per la mitigazione delle minacce per rete ed endpoint:

- Il modo migliore per proteggere il proprio sistema dalle infezioni causate da malware basato sugli script è bloccarli prima che colpiscano. La prevenzione è la chiave di volta. Il principale fattore per prevenire qualsiasi tipo di infezione malware su un computer è l'utente. Gli utenti devono essere consapevoli dei rischi legali allo scaricare e installare le applicazioni provenienti da fonti di cui non si fidano o non comprendono. Inoltre, il malware potrebbe essere scaricato inavvertitamente da utenti ignari mentre navigano online.
- Applicare aggiornamenti e patch di sicurezza per le applicazioni e il sistema operativo.

- Mantenere browser web, componenti aggiuntivi, antimalware negli endpoint e gateway di rete aggiornati e all'ultima versione.
- Non utilizzare mai computer che non sono distribuiti e certificati dal gruppo di sicurezza IT dell'azienda. Il malware basato sullo script può essere facilmente disseminato da risorse non protette e connesse alla rete aziendale.
- In caso gli utenti abbiano privilegi da amministratore locale per installare le applicazioni in autonomia, è importante istruirli ad installare solo applicazioni con firme affidabili di fornitori noti. È molto comune che applicazioni "innocue" offerte online incorporino rootkit e altri tipi di malware basato sugli script.
- Evitare di scaricare le applicazioni da fonti non web. Le probabilità di scaricare il malware infetto da gruppi Usenet, canali IRC, client di messaggistica istantanea o reti peer è molto alta. Anche i link ai siti web presenti su IRC e i messaggi istantanei puntano frequentemente a download infetti.
- Mettere in atto un programma istruttivo per la prevenzione degli attacchi di phishing. Il malware viene comunemente distribuito da email mirate.
- Utilizzare i feed di informazioni sulle minacce combinati con la tecnologia antimalware. Tale combinazione aiuterà a ridurre il tempo necessario per rilevare minacce malware emergenti e note.

Come McAfee aiuta a proteggere dal malware basato sugli script

L'individuazione immediata di malware basato sugli script che non coinvolge un codice binario iniziale può essere difficile e spesso è guidata dagli sforzi investigativi delle organizzazioni di sicurezza. Tuttavia, per bloccare questo tipo di malware è fondamentale assicurare l'impiego di controlli appropriati per negare un punto di accesso agli aggressori.

McAfee Endpoint Security

McAfee Endpoint Security (ENS) mette a disposizione un'infrastruttura di sicurezza collaborativa che riduce la complessità degli ambienti di sicurezza degli endpoint e offre visibilità sulle minacce avanzate, come il malware basato sugli script, che velocizza il rilevamento e gli interventi di remediation. La sua architettura flessibile offre un'infrastruttura per i team della sicurezza che sono oppressi da molteplici soluzioni per poter visualizzare, rispondere e gestire più facilmente il ciclo di vita di protezione dalle minacce.

McAfee ENS introduce numerose nuove tecnologie e miglioramenti:

- **Real Protect.** Applica tecniche di apprendimento automatico per identificare il codice pericoloso in base sia a cosa sembra, cosa potrebbe fare (analisi pre-esecuzione) che a cosa fa (analisi comportamentale dinamica); il tutto senza firme. Real Protect fa parte di una strategia di difesa efficace contro il malware basato sugli script.

- **Contenimento dinamico delle applicazioni.** Include l'abilità di contenere una singola istanza di un processo.
- **Integrazione di McAfee Client Proxy.** McAfee Endpoint Security può essere combinato con una sicurezza web gateway multilivello, che fornisce protezione pervasiva ovunque si viaggi, eliminando la mancanza di protezione quando si è scollegati dalla rete collegando gli endpoint al servizio cloud Web Gateway.
- **Modulo firewall.** Il livello successivo di protezione assicurata da una strategia di sicurezza proattiva è il blocco delle comunicazioni tra il proprio computer e i server controllati dai criminali informatici.
- **Modulo di prevenzione delle minacce.** Le scansioni on-demand ora includono un'opzione di scansione del registro di sistema, utile per proteggere dal malware basato sugli script. Gli amministratori possono creare regole personalizzate per la protezione degli accessi ai servizi, che ora includono anche i servizi Windows. La prevenzione personalizzata dagli exploit delle applicazioni è disponibile unitamente alle firme IPS (Intrusion Prevention System) fornite da McAfee. Infine, la protezione per le applicazioni Windows è stata aggiunta alle regole di prevenzione dagli exploit.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) è un prodotto per il rilevamento del malware multilivello che si avvale di più motori di ispezione. Combinando molteplici motori di analisi che applicano un controllo basato su firme e reputazione, emulazione in tempo reale, analisi completa del codice statico e sandboxing dinamico, McAfee ATD protegge dal malware basato sugli script che inizialmente deposita un file binario nel sistema preso di mira.

- **Rilevamento basato sulle firme:** rileva virus, worm, spyware, bot, trojan, buffer overflow e attacchi misti. La knowledgebase completa viene creata e sostenuta da McAfee Labs.
- **Rilevamento basato sulla reputazione:** controlla la reputazione dei file usando McAfee Global Threat Intelligence (GTI) per rilevare le nuove minacce emergenti.
- **Analisi statica ed emulazione in tempo reale:** consentono di individuare rapidamente minacce zero-day e malware non identificati dalle tecniche basate su firma o secondo la reputazione.
- **Analisi completa del codice statico:** esegue il reverse engineering del codice del file per valutarne tutti gli attributi e i gruppi di istruzioni, oltre che per analizzarne in modo completo il codice sorgente senza eseguirlo. Le funzioni esaustive di decompressione aprono tutti i tipi di file compressi e di archivi per abilitare l'analisi completa e la classificazione del malware, consentendo all'azienda di comprendere la minaccia posta da malware specifico.
- **Analisi dinamica nella sandbox:** per un file la cui sicurezza non può essere stabilita attraverso i motori di ispezione precedenti, McAfee ATD può eseguire il codice del file in un ambiente di runtime virtuale e osservare il comportamento risultante. Gli ambienti virtuali possono essere configurati per soddisfare gli ambienti host.

McAfee Threat Intelligence Exchange

È importante disporre di una piattaforma di intelligence in grado di adattarsi nel tempo alle esigenze di un ambiente. McAfee Threat Intelligence Exchange riduce considerevolmente l'esposizione agli attacchi di malware basato sugli script grazie all'individuazione delle minacce immediate come file o applicazioni sconosciute in esecuzione nell'ambiente.

- **Informazioni complete sulle minacce:** personalizza facilmente informazioni complete sulle minacce provenienti dalle fonti dislocate in tutto il mondo. Queste ultime possono essere costituite da feed McAfee GTI oppure di terze parti, contenenti le informazioni locali sulle minacce derivanti da eventi passati o in fase di svolgimento, inviate tramite endpoint, gateway e altri componenti della sicurezza.
- **Prevenzione dell'esecuzione e remediation:** McAfee TIE può intervenire e impedire l'esecuzione di applicazioni sconosciute nell'ambiente. Se un'applicazione ammessa all'esecuzione viene in seguito giudicata dannosa, McAfee TIE disattiva in tutto l'ambiente i processi in esecuzione a essa associati, grazie alle potenti capacità di gestione centralizzata e di imposizione delle policy del prodotto.
- **Visibilità:** McAfee TIE può rilevare tutti i file eseguibili compressi e la loro esecuzione iniziale all'interno dell'ambiente, oltre a tutte le modifiche che si verificano in seguito. Tale visibilità sulle azioni di un'applicazione o processo, dall'installazione fino al momento contingente, velocizza risposta e remediation.
- **Indicatori di violazione:** importazione degli hash dei file nocivi e immunizzazione dell'ambiente da queste minacce note mediante l'imposizione di policy. Se nell'ambiente scatta uno degli indicatori, McAfee TIE è in grado di terminare tutti i processi e le applicazioni associati agli indicatori di compromissione.

McAfee Web Gateway

Download guidati e URL pericolosi incorporati in email di phishing sono alcuni dei metodi di attacco principali utilizzati per distribuire malware basato sugli script. McAfee Web Gateway (MGW) è un prodotto efficace con cui ottimizzare la protezione dell'azienda da questo tipo di minaccia.

- **McAfee Gateway Anti-Malware Engine:** l'analisi senza firma degli intenti filtra in tempo reale i contenuti dannosi dal traffico web. L'emulazione e l'analisi del comportamento proteggono in modo proattivo contro gli attacchi mirati e zero-day. McAfee Gateway Anti-Malware Engine ispeziona i file e ne blocca il download nel caso in cui siano pericolosi.

DOCUMENTAZIONE

- **Integrazione con McAfee GTI:** i feed di intelligence in tempo reale sulla reputazione di file e siti web e la classificazione dei siti di McAfee GTI garantiscono protezione dalle minacce più recenti perché MWG blocca i tentativi di connessione ai siti web di cui è nota la pericolosità o ai siti che utilizzano reti pubblicitarie malevole. Oltre a questi prodotti McAfee, suggeriamo due categorie aggiuntive di tecnologie di sicurezza.
  - **Protezione del gateway email:** la maggior parte del malware basato sugli script penetra in un sistema attraverso un allegato di un messaggio email, perciò un prodotto efficace per la protezione del gateway email che analizza tutti gli allegati alla ricerca di malware rappresenta una difesa solida contro questo tipo di attacco.
  - **Firewall:** la tecnologia firewall è fondamentale per qualsiasi sistema di sicurezza. Un firewall è in grado di rilevare molte minacce a livello perimetrale, prima che possano introdursi nella rete affidabile. Poiché il malware basato sugli script si introduce in un sistema tramite codici binari statici, molti di questi attacchi possono essere bloccati prima che riescano ad introdursi all'interno della rete affidabile.

McAfee
Together is power.

Via Fantoli, 7
20138 Milano, Italy
(+39) 02 554171
www.mcafee.com/it

3529_0917
SETTEMBRE 2017