Panoramica sulla soluzione

Software legittimo infettato dai trojan

Prevenire le infezioni e mitigarne la diffusione con i prodotti Intel® Security

I meccanismi utilizzati per la distribuzione del software attraverso Internet possono essere trasformati in vettori per attacchi virus e malware. Vi è una chiara evoluzione dal binder dannoso originale esposto un decennio fa alla sofisticata distribuzione di software legittimo che è infettato da trojan prima o durante la fase di distribuzione.

Indipendentemente dalla complessità del trojan, i passi fondamentali sono gli stessi:

- Trasformare il software in un'arma: inserire il malware in un'applicazione che può essere spedita.
- Consegna: trasmettere software infettato dal trojan all'obiettivo.
- Attuazione dell'exploit: attivare il codice del trojan e cercare di non essere rilevato.
- Installazione: diventare persistente e cercare di spostarsi lateralmente.

L'ultima tecnica di attacco è basata su un sofisticato meccanismo “al volo” che inietta codice all'interno di un download legittimo per non essere rilevato. Il principio d'attacco è quello di unire l'applicazione originale con il codice dannoso.

Questa tecnica d'attacco può utilizzare due componenti per trovare un punto d'ingresso favorevole verso l'obiettivo: un listener che cattura e modifica la richiesta di download HTTP e un binder che infetta e distribuisce i codici binari.

Gli algoritmi attuali distribuiscono routine di infezione malware e attacchi di reindirizzamento di rete senza modificare il codice dell'applicazione. Ciò apre un argine per il software commerciale o open-source trasformato in un'arma e può includere file eseguibili con una firma incorporata. L'attacco ha successo se la firma non viene verificata completamente e automaticamente prima di qualsiasi tentativo iniziale di esecuzione.

Una volta che l'applicazione infettata da trojan viene lanciata all'interno dell'obiettivo, un processo binder crea il proprio file per eseguibili incorporati aggiuntivi in cui tutto il codice iniettato viene ricostruito per essere eseguito ulteriormente, aggirando tutti i controlli di sicurezza. Poiché l'applicazione originale è intatta, il malware può essere allegato a qualsiasi file con qualsiasi firma e avere comunque successo.

intel Security

Policy e procedure

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

- Quando ci si collega a una rete non affidabile si dovrebbe usare una rete privata virtuale. Gli amministratori devono mantenere aggiornato il software e affidarsi a indicatori di affidabilità robusti, piuttosto che a quelli potenzialmente falsificati. Le applicazioni devono essere firmate e verificate con una catena di fiducia. Le analisi forensi devono includere la correlazione degli hash a origini affidabili.
- Il software di sicurezza deve includere l'analisi dinamica per segnalare le azioni ostili a prescindere dall'ispezione iniziale del file binario, data la limitazione della scansione statica. Il monitoraggio dei comportamenti, la reputazione di IP e web, la scansione della memoria e il contenimento delle applicazioni sono componenti preziosi di una soluzione completa.
- I download devono svolgersi attraverso connessioni sicure e tutto il codice dovrebbe essere firmato. Queste misure riducono drasticamente gli attacchi man-in-the-middle. I fornitori di sicurezza devono includere la convalida automatica nelle proprie applicazioni, devono verificare periodicamente il proprio codice, usare gli strumenti di analisi statica del codice ed eseguire revisioni paritarie. È sempre buona cosa disporre di un repository centrale di applicazioni aziendali affidabili e consentire agli utenti di scaricare solo programmi di installazione approvati da tale repository.
- Il software antimalware dovrebbe essere configurato per identificare la presenza di binder.
- Si dovrebbero utilizzare applicazioni di rilevamento e prevenzione delle intrusioni host per l'analisi dei pacchetti che possono identificare payload pericolosi.
- Utilizzare solo architetture di virtualizzazione affidabili combinate con un'adeguata segmentazione della rete. Le architetture di virtualizzazione affidabili utilizzano un processo di boot sicuro e verificabile. Una solida segmentazione delle rete permette di monitorare il traffico e mantenere le applicazioni isolate in caso di un exploit andato a buon fine. Questa combinazione protegge anche da movimenti laterali del malware.
- Identificare la presenza del malware distribuito da software infettato da trojan monitorando il traffico in uscita. È possibile esporre le macchine infette per ulteriori attività di remediation per il traffico che cercano di inviare a Internet.

Intel Security

I prodotti Intel Security possono identificare il software legittimo infettato da trojan, identificare e bloccare le minacce malware incorporate, mostrare le violazioni e rispondere rapidamente:

McAfee VirusScan® Enterprise 8.8 o McAfee Endpoint Security 10

- Mantenere aggiornati i file DAT.
- Assicurarsi che McAfee Global Threat Intelligence (McAfee GTI) sia attivo; include oltre 600 milioni di firme di ransomware uniche.
- Sviluppare regole di protezione degli accessi per bloccare l'installazione e i payload del malware:
  - Fare riferimento agli articoli della base di conoscenza delle regole di protezione degli accessi: KB81095 e KB54812.
  - Fare riferimento alle migliori pratiche di configurazione per McAfee VirusScan 8.8 Enterprise: PD22940.
  - Fare riferimento alle migliori pratiche di configurazione per McAfee Endpoint Security: KB86704.

McAfee Host Intrusion Prevention

- McAfee Host Intrusion Prevention può aiutare a prevenire la diffusione del malware. Utilizzando firme IPS personalizzate, è possibile creare regole per prevenire operazioni di file generate da malware (creazione, scrittura, esecuzione, lettura, ecc.).
- Abilitare la firma 3894 di Host Intrusion Prevention, "Access Protection—Prevent svchost.exe executing non-Windows executables" (Protezione degli accessi - Prevenzione di svchost.exe utilizzando eseguibili non Windows).
- Abilitare le firme 6010 e 6011 di Host Intrusion Prevention per bloccare immediatamente l'iniezione.
- Due tipologie di sotto-regole possono raggiungere tale obiettivo:

1. Creare una firma IPS personalizzata utilizzando il motore Files e una sotto-regola con i seguenti criteri:
   - Name: <Inserire nome>
   - Rule type: Files
   - Operations: Create, Execute, Read, Write
   - Parameters: Include - Files - <percorso/nome file del malware>
     - Il nome del file deve includere un percorso. Se si desidera specificare con wildcard il percorso, iniziare il nome del file con "**\" or "?:\", se si desidera specificare con wildcard la lettera del drive (per esempio: "**\nomefile.exe" o "?:\nomefile.exe").
     - Non si possono utilizzare hash MD5 con il parametro "Files", solo percorso/nome file
     - È inoltre possibile utilizzare il tipo di drive per limitare il percorso a un drive specifico (per esempio, hard disk, CD-ROM, USB, rete, floppy disk).
   - Executables: può essere lasciato in bianco, a meno che si desideri limitare la firma a processi specifici che eseguono l'operazione del file (per esempio, explorer.exe, cmd.exe, ecc.).
2. Creare una firma IPS personalizzata utilizzando il motore Program e una sotto-regola con i seguenti criteri:
   - Name: <Inserire nome>
   - Rule type: Program
   - Operations: Run target executable
   - Parameters: <Lasciare vuoto>
   - Executables: può essere lasciato in bianco, a meno che si desideri limitare la firma a un processo specifico come l'eseguibile originario (per esempio, se si desidera impedire ad explorer.exe di eseguire un target executable (come notepad.exe)).
   - Target Executables: definire le proprietà dell'eseguibile per cui si desidera impedire l'esecuzione (per esempio, se si desidera impedire l'esecuzione di notepad.exe, specificare il percorso/nome file dell'eseguibile). L'eseguibile può essere definito utilizzando uno o più criteri (descrizione del file, nome file, impronta, firmatario).

McAfee SiteAdvisor® Enterprise o McAfee Web Protection

- Utilizza le reputazioni del sito web per prevenire o avvisare gli utenti dei siti web che distribuiscono software infettato dai trojan.

McAfee Threat Intelligence Exchange e McAfee Advanced Threat Defense

- Configurazione della policy di Threat Intelligence Exchange
  - Iniziare con la modalità di osservazione: Mano a mano che si scoprono endpoint con processi sospetti, usare i tag di sistema per applicare le policy di imposizione di Threat Intelligence Exchange.
  - Rimuovere se: file known malicious (notoriamente dannoso).
  - Blocca se: most likely malicious (molto probabilmente dannoso) (il blocco in caso di file unknown (sconosciuto) offrirebbe maggior protezione ma potrebbe anche aumentare il carico di lavoro amministrativo iniziale).
  - Submit files to McAfee Advanced Threat Defense (Invia i file a McAfee Advanced Threat Defense) in caso di livello unknown (sconosciuto) e inferiore.
  - Policy del server Threat Intelligence Exchange: accetta le reputazioni di Advanced Threat Defense per i file non ancora osservati da Threat Intelligence Exchange.
- Intervento manuale di Threat Intelligence Exchange:
  - Imposizione della reputazione dei file (in modalità operativa). Most likely malicious (Molto probabilmente dannoso): rimuovi/elimina.
  - Might be malicious (Probabilmente dannoso): blocca.
- La reputazione dell'impresa (organizzativa) può bypassare McAfee GTI:
  - Si può scegliere di bloccare un processo indesiderato, per esempio un'applicazione non supportata o vulnerabile.
  - Contrassegnare il file come might be malicious (probabilmente dannoso).
- Oppure scegliere di abilitare un processo indesiderato a fini di test:
  - Contrassegnare il file come might be trusted (probabilmente affidabile).

McAfee Advanced Threat Defense

- Capacità di rilevamento in-box:
  - Rilevamento basato sulle firme: Le firme mantenute da McAfee Labs sono oltre 600 milioni.
  - Rilevamento basato sulla reputazione: McAfee GTI
  - Analisi statica ed emulazione in tempo reale: utilizzata per il rilevamento senza firme
  - Personalizza le regole YARA
  - 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.
  - Analisi dinamica nella sandbox
- Crea profili nell'analizzatore per capire dove è probabile che venga eseguito il software infettato dai trojan:
  - Sistemi operativi comuni, Windows 7, Windows 8, Windows 10.
  - Installare applicazioni Windows (Word, Excel) e attivare le macro.
- Fornire un analizzatore per profilare l'accesso ad Internet:
  - Molti esempi eseguono uno script a partire da un documento di Microsoft che crea una connessione in uscita e può attivare il malware. Fornire un analizzatore profila la connessione a Internet e aumenta le percentuali di rilevamento.

McAfee Network Security Platform

- Network Security Platform dispone di firme all'interno delle sue policy di default per rilevare la rete TOR, che può essere utilizzata per trasferire i file associati al malware.
- Integrazione con Advanced Threat Defense per nuove varianti di attacchi:
  - Configurare l'integrazione di Advanced Threat Defense nella policy avanzata per il malware.
  - Configurare Network Security Platform per inviare file .exe, Microsoft Office, archivi Java e PDF ad Advanced Threat Protection per il controllo.
  - Verificare che la configurazione Advanced Threat Protection venga applicata a livello di sensore.
- Aggiornare le regole di rilevamento di callback (per combattere le botnet).

McAfee Web Gateway

- Attivare il controllo di McAfee Gateway Anti-Malware.
- Attiva GTI per la reputazione di URL e file.
- Integrazione con McAfee Advanced Threat Defense per l'analisi nella sandbox e il rilevamento delle minacce zero-day.

VirusTotal Convicter: intervento automatizzato

- Convicter è uno script Python attivato dal sistema di risposta automatico di McAfee ePolicy Orchestrator® (McAfee ePO) per avere un riferimento incrociato di un file che genera un evento legato a una minaccia in McAfee Threat Intelligence Exchange con VirusTotal.
- È possibile alterare lo script per far riferimento ad altri scambi di intelligence delle minacce come GetSusp.
- Se la soglia per la fiducia della comunità è soddisfatta, lo script imposta automaticamente la reputazione aziendale. Soglia suggerita: devono essere d'accordo il 30% dei vendor e 2 aziende leader.
- Filtro: Target file name does not contain (Il nome del file non contiene): McAfeeTestSample.exe.
- Questo è uno strumento gratuito supportato dalla comunità (non supportato da Intel Security).

McAfee Endpoint Threat Defense and Response

- McAfee Endpoint Threat Defense and Response individua e risponde alle minacce avanzate. Quando viene utilizzato unitamente ai feed sulle minacce di McAfee Labs, Dell SecureWorks o ThreatConnect, è possibile ricercare ed eliminare nuove minacce prima che abbiano la possibilità di diffondersi.
- Controllori personalizzati consentono di creare strumenti specifici per trovare e identificare indicatori di compromesso associati alle applicazioni infettate dai trojan.
- Attivatori e reazioni sono costruiti dall'utente per definire le azioni quando vengono soddisfatte determinate condizioni. Per esempio, quando vengono rilevati hash o nomi di file, può essere eseguita automaticamente un'azione di cancellazione.

Ulteriori letture

Best Practices for how to use McAfee Host Intrusion Prevention rules for a malware outbreak (Le migliori procedure su come utilizzare le regole di McAfee Host Intrusion Prevention per un attacco malware): KB84507

Questo articolo della base di conoscenza fornisce ai clienti informazioni dettagliate relativamente a Trojan-Powelike: Vettori di infezione e propagazione: PD25582

SIEM Orchestration: Orchestration Triggers Signs of Malware Infection and Anomalous Behaviors (Orchestrazione SIEM: l'orchestrazione attiva i segni dell'infezione malware e i comportamenti anomali): PD24830

White paper: *Sicurezza oltre la firma*

FAQs for Network Security Platform: Advanced Malware Detection (Domande frequenti per la soluzione Network Security Platform: Rilevamento avanzato del malware): KB75269

Guida prodotto di McAfee Web Gateway: Filtraggio web: PD26339

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com