Documentazione

Salvaguardare i dispositivi IoT per proteggersi dagli attacchi

Il riuscito attacco DDoS (Distributed Denial of Service) sostenuto contro l'infrastruttura DNS gestita di Dyn nell'ottobre 2016 è stato oggetto di un'analisi approfondita all'interno del *Report McAfee Labs sulle minacce: aprile 2017*.

L'attacco è stato eseguito utilizzando il protocollo DNS, che rende molto complicato per la tecnologia di sicurezza distinguere il traffico legittimo da quello ostile. Ad aggravare il problema, attacco e traffico legittimo provenivano da milioni di indirizzi IP in tutto il mondo.

Questo tipo di attacco DDoS è in aumento, alimentato da un'infrastruttura Internet of Things (IoT) protetta in modo non adeguato. Il malware Mirai utilizzato durante l'attacco Dyn ha sfruttato un'ampia gamma di dispositivi IoT non adeguatamente protetti quali videoregistratori, stampanti, videocamere di sorveglianza, frigoriferi, termostati, ecc. Una volta infettato il dispositivo IoT, il malware ha diffuso l'infezione ad altri dispositivi, formando una "botnet" per poi utilizzare la potenza di elaborazione aggregata per eseguire l'attacco DDoS.

Secondo il team di sicurezza di Dyn, erano decine di milioni i dispositivi IoT pericolosi che costituivano la botnet basata su Mirai durante il culmine dell'attacco.

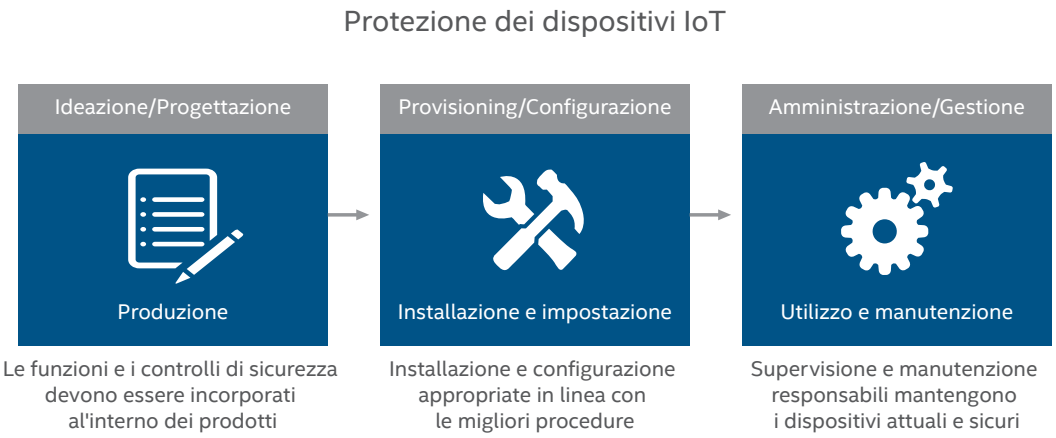
Non vi è alcun modo semplice per stabilire se un dispositivo di rete è stato infettato o il grado di infezione, che può variare da fasi iniziali di detonazione del codice, movimento laterale, o comunicazione del server di controllo al reclutamento di botnet per attacchi DDoS orchestrati. Ad ogni modo ci sono alcune raccomandazioni di sicurezza da seguire che aiutano a proteggere i dispositivi IoT e le reti affidabili.

Come proteggere i dispositivi IoT

Gli aggressori seguono il percorso che oppone meno resistenza per ottenere il controllo dei dispositivi IoT. Solitamente, ciò avviene attraverso credenziali poco sicure. Ma possono adattarsi a credenziali più efficaci e altri controlli di sicurezza. Questo è lo schema che abbiamo osservato con molti vettori d'attacco.

Intel Security consiglia di bloccare gli exploit noti e probabili future mosse da parte degli aggressori e di seguire i tre seguenti passaggi per proteggere i dispositivi IoT, dalla produzione al ritiro:

intel Security



1. **Progettare dispositivi IoT tenendo ben presente la sicurezza.** I produttori di soluzioni IoT devono incorporare la sicurezza all'interno dell'architettura, delle interfacce e dei progetti dei loro prodotti. Stabilire e testare concetti e funzionalità di sicurezza di base come la compartimentazione dei dati e del codice, la comunicazione tra parti affidabili, la protezione dei dati sia in uso che a riposo e l'autenticazione degli utenti. I prodotti in futuro saranno più potenti, archivieranno più dati e disporranno di maggiori funzionalità. Ciò significa che i prodotti dovrebbero avere la possibilità di eseguire aggiornamenti di sicurezza, bloccare le funzioni, convalidare la compilazione, controllare accuratamente il software e impostare configurazioni di default che seguono le migliori procedure del settore. Ha tutto inizio con chi produce; la solidità per il futuro parte dalle basi. Hardware, firmware, sistemi operativi e software devono essere progettati per essere inseriti in un ambiente ostile e sopravvivere. Coloro che acquistano un dispositivo IoT dovrebbero tenere ben presente questi punti in fase di acquisto. Il produttore ha ideato e progettato il dispositivo IoT pensando alla sicurezza?
2. **Provisioning e configurazione in modo sicuro.** La maggior parte dei dispositivi IoT richiedono un certo tipo di configurazione e provisioning in fase di installazione. L'identità e l'autenticazione del dispositivo sono una parte essenziale di questo processo a due fasi. Configurazioni predefinite adeguate che aderiscono alle migliori procedure di sicurezza sono importanti e dovrebbero essere facili da comprendere da parte degli utenti. Le regole non dovrebbero autorizzare password di default, esigere la firma di patch e aggiornamenti, la crittografia dei dati e solo connessioni web sicure. Per le aziende, la limitazione dell'accesso alla rete, l'applicazione delle patch in modo tempestivo e l'autorizzazione ad eseguire solo software approvato saranno di grande aiuto per mantenere protetti i dispositivi IoT. Per quei dispositivi che sono in grado di farlo, l'implementazione di software di sicurezza come antimalware, sistemi per la prevenzione delle intrusioni e anche firewall locali miglioreranno lo stato di protezione di un dispositivo. Rilevamento e telemetria dovrebbero essere configurati in modo da rilevare quando i sistemi sono sotto attacco o vengono utilizzati in modo improprio. Devono essere stabilite policy per la privacy, la conservazione dei dati, l'accesso remoto, la sicurezza primaria e le procedure di revoca.
3. **Attività adeguate di amministrazione e gestione.** Per i dispositivi di proprietà dei consumatori finali, solo questi ultimi devono avere l'ultima parola sul modo in cui il dispositivo è gestito. I produttori e fornitori di servizi online hanno un loro ruolo in fase di provisioning, ma i proprietari devono mantenere il controllo di ciò che il dispositivo farà. Il provisioning è diverso dall'amministrazione. Per esempio, durante l'installazione di videocamere domestiche ha senso collegarsi al produttore per le patch più recenti e impostare magari uno storage in cloud. Ma i clienti non desiderano che le videocamere siano controllate dai produttori, che non dovrebbero avere la possibilità di controllare i dispositivi al di fuori dell'autorità dell'acquirente. I possessori devono mantenere la facoltà di accendere o spegnere i propri prodotti e scegliere a quali servizi online possono collegarsi. Questa capacità richiede un'adeguata identificazione

e autenticazione dell'utente. Autorizzare una comune password di default non va bene perché chiunque potrebbe diventare amministratore. Immaginiamo se Windows fosse fornito con una password di login di default per ogni sistema. Si verrebbe a creare un incubo di sicurezza dal momento che molti utenti non la cambierebbero e gli aggressori potrebbero accedere come utenti. I sistemi IoT devono prima essere in grado di autenticare i propri proprietari. Le funzionalità di gestione devono estendersi anche per consentire ai proprietari per impostare i limiti, le policy per i dati e i parametri di tutela della privacy che sono più restrittivi di quelli di qualsiasi potenziale fornitore terza parte. Gli aggiornamenti di sicurezza firmati dovrebbero essere installati automaticamente nel momento in cui si rendono disponibili. I proprietari esperti dovrebbero essere in grado di configurare i limiti per le connessioni in entrata e uscita, i tipi di dati, le porte e le impostazioni di sicurezza. I registri che possono essere inviati ad un sistema affidabile o visionati a livello locale dovrebbero catturare gli errori, così come le attività impreviste e insolite. Un sistema per le notifiche di allarme da remoto, via email o messaggio di testo, è una funzione ben accetta su alcuni dispositivi. Infine, la possibilità di reset è necessaria in caso di una volazione irrecuperabile o trasferimento di possesso.

Policy e procedure fruibili per proteggere i dispositivi IoT

- **Esaminare le precedenti prestazioni del dispositivo IoT in termini di sicurezza.** Prima di acquistare un dispositivo IoT, verificare se lo stesso, o l'azienda che lo offre, abbia avuto dei problemi. Una veloce ricerca su Internet può essere sufficiente. Una ricerca sul sito web della Federal Trade Commission rivelerà eventuali procedure esecutive precedenti. Eseguendo una ricerca di base, si potrebbe scoprire che alcune aziende non pongono attenzione alle preoccupazioni per la sicurezza dei loro prodotti, mentre altre sono più proattive.
- **Mantenere aggiornati tutti i software del dispositivo IoT.** Questa semplice procedura spesso elimina le vulnerabilità, in particolare quelle più recenti e messe in evidenza pubblicamente. Implementare una procedura di applicazione delle patch e verificarne la corretta applicazione.
- **Per i dispositivi IoT che non possono essere corretti con le patch, mitigare il rischio** tramite il whitelisting delle applicazioni, che mette in sicurezza i sistemi e previene l'esecuzione dei programmi non autorizzati.
- **Isolare i dispositivi IoT dalle altre parti della rete** usando un firewall o un sistema di prevenzione delle intrusioni. Disattivare in questi sistemi le porte e i servizi non necessari per ridurre l'esposizione ai possibili punti di ingresso delle infezioni. Mirai sfrutta le porte inutilizzate.
- **Modificare le impostazioni di default e utilizzare password sicure.** Le impostazioni di default e password deboli rappresentano la principale minaccia per i dispositivi IoT. Adottare buone abitudini in merito alle password, come l'utilizzo di frasi lunghe, caratteri speciali, un mix di maiuscole e minuscole e numeri. Le password devono essere efficaci e difficili da indovinare.
- **Sfruttare le impostazioni di sicurezza IoT.** Alcuni dispositivi IoT offrono configurazioni avanzate e si dovrebbero sfruttare al massimo. Alcuni prodotti IoT offrono networking separato, analogamente a una rete Wi-Fi guest insieme alla connessione principale. Questa è solo una funzione, altri prodotti potrebbero offrirne altre ancora.
- **Collegare i dispositivi IoT utilizzando una rete Wi-Fi sicura.** Creare password solide e utilizzare i protocolli di sicurezza più recenti, come WPA2.
- **Limitare l'accesso fisico ai dispositivi IoT.** La manomissione diretta di un dispositivo può portare a una violazione del dispositivo IoT.
- **Disabilitare il supporto Universal Plug and Play (UPNP).** Molti dispositivi supportano UPnP, che permette di individuare il dispositivo su Internet rendendolo vulnerabile alle infezioni malware. Disabilitare tale funzione quando possibile.
- **Spegnere e riavviare periodicamente i dispositivi IoT.** Il malware viene solitamente archiviato in una memoria volatile e può essere cancellato spegnendo e riavviando il dispositivo.

Come i prodotti Intel Security possono proteggere sistemi e reti dagli attacchi dei dispositivi IoT

Oltre al precedente elenco delle migliori procedure per i dispositivi IoT, i prodotti Intel Security possono contribuire a mitigare i rischi delle infezioni malware all'interno dei dispositivi IoT e bloccare le attività dannose delle botnet. Le seguenti configurazioni di prodotto Intel Security possono essere d'aiuto per salvaguardare i dispositivi IoT e proteggere sistemi e reti dagli attacchi provenienti dai dispositivi IoT:

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:
  - Consulta l'articolo della knowledgebase sulle regole di protezione dell'accesso: KB81095 e KB54812.
  - Fare riferimento alle migliori pratiche di configurazione per McAfee VirusScan Enterprise 8.8: 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 McAfee Host Intrusion Prevention: Access Protection—Prevent svchost.exe executing non-Windows executables (Protezione dell'accesso: impedisce a svchost.exe di lanciare eseguibili non Windows).
- Abilitare le firme 6010 e 6011 di Host Intrusion Prevention per bloccare immediatamente l'iniezione.
- Due tipologie di sotto-regole raggiungono 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, 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 dei siti per prevenire o avvisare gli utenti dei siti web che distribuiscono malware.

McAfee Threat Intelligence Exchange e McAfee Advanced Threat Defense

- Configurazione della policy di McAfee 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: 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 McAfee Threat Intelligence Exchange: accetta le reputazioni di McAfee Advanced Threat Defense per i file non ancora osservati da McAfee Threat Intelligence Exchange.
- Intervento manuale di McAfee 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 scavalcare 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).

Documentazione

McAfee Advanced Threat Defense

- Funzionalità di rilevamento:
  - Rilevamento basato sulle firme: McAfee GTI contiene oltre 600 milioni di firme.
  - Rilevamento basato sulla reputazione: McAfee GTI.
  - Analisi statica in tempo reale ed emulazione: utilizzata per il rilevamento senza firme.
  - Regole YARA personalizzate.
  - 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 malware:
  - 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 attiva il malware. Fornire un analizzatore profila la connessione a Internet e aumenta le percentuali di rilevamento.

McAfee Network Security Platform

- McAfee 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 McAfee Advanced Threat Defense per nuove varianti di attacchi:
  - Configurare l'integrazione di McAfee Advanced Threat Defense nella policy avanzata per il malware.
  - Configurare McAfee Network Security Platform per inviare file .exe, Microsoft Office, archivi Java e PDF ad McAfee Advanced Threat Protection per il controllo.
  - Verificare che la configurazione McAfee 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 McAfee 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 filtro non contiene): McAfeeTestSample.exe."
- Questo è uno strumento gratuito supportato dalla comunità (non supportato da Intel Security).

Documentazione

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 GTI, 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 al malware.
- 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

White paper: *More Confidence, Safety, and Security in the Digital World (Maggior fiducia, sicurezza e protezione nel mondo digitale)*

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

SIEM Orchestration. How McAfee Enterprise Security Manager can drive action, automate remediation, and increase situational awareness (Orchestrazione SIEM. Come McAfee Enterprise Security Manager può indirizzare l'azione, automatizzare la remediation e incrementare la consapevolezza della situazione): PD24830

White paper: *Sicurezza oltre la firma*

FAQs for Network Security Platform. Advanced malware detection (Domande frequenti per Network Security Platform. Rilevamento avanzato del malware): KB75269

Guida prodotto di McAfee Web Gateway. Filtraggio web: PD26339

Intel e i loghi Intel e McAfee sono marchi di Intel Corporation o McAfee, Inc. negli Stati Uniti e/o in altri Paesi. Altri marchi e denominazioni potrebbero essere rivendicati come proprietà di terzi. Copyright © 2017 Intel Corporation. 2729_0217_brf-secure-iot-devices-protect-attacks
Marzo 2017

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