Documentazione

Protezione contro i password stealer

Dal momento che dipendiamo sempre più dai dispositivi elettronici personali e le aziende spostano informazioni preziose sul cloud, il valore delle credenziali d'accesso è aumentato. Oggi, gli aggressori utilizzano password rubate nelle fasi iniziali di quasi tutte le principali minacce avanzate persistenti.

I password stealer si concentrano sulla violazione della sicurezza di rete e sistemi per ottenere le credenziali critiche per l'accesso. Le solide capacità del password stealer Fareit lo rendono da oltre cinque anni il malware per il furto delle password più popolare. Sin dalla sua scoperta nel 2012, Fareit ha continuato ad evolversi per eludere le più recenti strategie di protezione informatica.

Inizialmente, Fareit si concentrava sul furto delle credenziali di accesso dai browser web per ottenere l'accesso ad applicazioni come il banking online, gli account di posta e per il furto di identità. Da allora, Fareit si è evoluto in un programma di intercettazione di informazioni più aggressivo che si nasconde utilizzando tattiche mimetiche come la modifica del proprio file hash con ogni infezione. Nel 2016, ha fatto la sua apparizione una nuova generazione di malware Fareit, utilizzando una risorsa di rete infetta per eseguire attacchi Denial of Service distribuiti. Inoltre, Fareit viene ora offerto come servizio pay-per-infection, che significa che i criminali informatici ora guadagnano denaro per distribuire malware. Maggiori sono le infezioni che riescono a perpetrare, più vengono pagati.

Nell'ultimo decennio, gli attacchi di phishing che rilasciano password stealer come Fareit sono risultati essere tra i principali vettori d'attacco iniziali.

Policy e procedure per proteggersi dagli attacchi password stealer

McAfee consiglia alle aziende di adottare le seguenti misure per proteggersi dagli attacchi password stealer:

- I programmi password stealer sono spesso distribuiti dal malware: come principio di sicurezza standard si consiglia di mantenere i prodotti antimalware sempre aggiornati.
- Il malware può essere scaricato da utenti inconsapevolmente durante la navigazione online. Mantenere aggiornati i browser web e gli add-on per aggiungere un livello ulteriore di protezione.

McAfee
Together is power.

- Eseguire le applicazioni come utente con privilegi limitati invece di utilizzare i diritti da amministratore.
- Mantenere protetto il perimetro della rete. I firewall possono impedire ad aggressori esterni di ottenere l'accesso ad applicazioni interne che sono state precedentemente violate da attacchi password stealer andati a buon fine.
- Utilizzare le credenziali di autenticazione aziendali (come quelle per i proxy web per la navigazione su Internet, le applicazioni database, le cartelle condivise, ecc.) solo quando si utilizzano risorse dell'azienda. Non autorizzare nella rete aziendale affidabile sistemi che non siano distribuiti e certificati dal gruppo di sicurezza informatica dell'azienda.
- Il malware che potrebbe contenere programmi password stealer può essere incorporato all'interno di software legittimo che è stato infettato da un Trojan da parte di un aggressore. Per prevenire un attacco di questo genere, consigliamo caldamente di rafforzare i meccanismi di recapito e distribuzione del software. È sempre una buona idea disporre in azienda di un archivio centrale di applicazioni, dal quale gli utenti possano scaricare il software approvato.
- Nei casi in cui gli utenti sono autorizzati a installare applicazioni non precedentemente convalidate dal gruppo di sicurezza informatica dell'azienda, istruire gli utenti a installare solo applicazioni con firme affidabili di fornitori noti. È molto comune che applicazioni "innocue" offerte online contengano programmi password stealer o altro malware.
- 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 P2P è molto alta. Anche i link ai siti web presenti su IRC e i messaggi istantanei puntano frequentemente a download infetti.
- Implementare un programma educativo per prevenire gli attacchi di phishing. I password stealer sono comunemente distribuiti attraverso il phishing.

Se si ritiene che i sistemi siano stati compromessi da un password stealer, alcune best practice aiuteranno a contenere il movimento laterale dell'infezione:

- Ridurre la superficie d'attacco abilitando l'autenticazione a due fattori per le applicazioni che la supportano. L'aggressore potrebbe aver rubato una password, ma il secondo fattore bloccherà l'infiltrazione.
- L'utilizzo di un firewall endpoint ridurrà l'espansione delle intrusioni con le password rubate se il computer infetto ha un traffico in ingresso e in uscita limitato imposto da regole del firewall.

Come i prodotti McAfee possono proteggere da attacchi password stealer

McAfee VirusScan® Enterprise 8.8 o McAfee Endpoint Security 10

- Mantenere il software antimalware dell'endpoint aggiornato con le patch, versione dei file DAT e motore di scansione più recenti. Assicurarsi che McAfee Global Threat Intelligence (McAfee GTI) sia in uso.
- 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 Enterprise 8.8: PD22940.
  - Fare riferimento alle migliori pratiche di configurazione per McAfee Endpoint Security: KB86704.

McAfee Host Intrusion Prevention

Gli strumenti per la prevenzione delle intrusioni non sono efficaci al fine di rivelare un attacco password stealer andato a buon fine. Tuttavia, McAfee Host Intrusion Prevention può aiutare a prevenire il movimento laterale del payload del malware, che potrebbe contenere un password stealer.

- 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 McAfee 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 assegnare un carattere jolly al percorso, iniziare il filename con "**\" or "?:\". Se si desidera assegnare un carattere jolly alla lettera del drive, utilizzare, per esempio, "**\nomedelfile.exe" or "?:\nomedelfile.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

- Utilizzano le reputazioni dei siti per prevenire o avvisare gli utenti dei siti web che distribuiscono password stealer.

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 McAfee Threat Intelligence Exchange.
  - Rimuovere se: Known malicious (Notoriamente dannoso).
  - Bloccare 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 Advanced Threat Defense (Inviare i file a Advanced Threat Defense) in caso di livello Unknown (Sconosciuto) e inferiore.
  - Policy di McAfee Threat Intelligence Exchange Server: accettare 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): cancella/elimina.
  - Might be malicious (Probabilmente dannoso): blocca.
- La reputazione dell'impresa (organizzativa) può scavalcare McAfee GTI:
  - 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

- Funzionalità di rilevamento in-box:
  - Rilevamento basato sulle firme: Lo "zoo" di malware di McAfee Labs mantiene oltre 600 milioni di firme.
  - Rilevamento basato sulla reputazione: McAfee GTI.
  - Analisi statica ed emulazione in tempo reale: utilizzata per il rilevamento senza firme.
  - Personalizzazione delle 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 malware per il furto di password:
  - sistemi operativi comuni come Windows 7, 8, 10.
  - Installa applicazioni Windows (Word, Excel) e attivare le macro.
- Fornisce 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. Fornisce 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 ai password stealer.

- 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 Defense venga applicata a livello di sensore.
- Aggiornare le regole di rilevamento di callback (per combattere le botnet).

McAfee Web Gateway

- Attivare il controllo antimalware di McAfee Web Gateway.
- 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 da 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 altre analisi McAfee Threat Intelligence Exchange come GetSusp.
- Se la soglia per considerare affidabile la community viene rispettata, 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 McAfee).

McAfee Active Response

- McAfee Active Response individua e reagisce 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.
- Possono essere utilizzati controllori personalizzati per creare strumenti specifici per trovare e identificare indicatori di compromesso associati ai password stealer.
- Attivatori e reazioni vengono creati dall'utente per definire le azioni quando vengono soddisfatte determinate condizioni; per esempio, quando vengono rilevati hash o nomi di file, può verificarsi automaticamente un'azione di cancellazione.

Per ulteriori informazioni

Phishing Attacks Employ Old but Effective Password Stealer (Gli attacchi di phishing utilizzano password stealer vecchi ma efficaci)

Profilo del virus Fareit

Profilo del virus Fareit

McAfee™
Together is power.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/it