Come proteggersi dal ransomware

Prevenire le minacce ransomware odierne con McAfee®

Il ransomware è un malware che utilizza la crittografia asimmetrica per tenere sotto sequetro le informazioni di una vittima. La cifratura asimmetrica (pubblica-privata) è una crittografia che utilizza una coppia di chiavi per cifrare e decifrare un file. La coppia di chiavi pubblica-privata viene generata in modo univoco dall'aggressore per la specifica vittima. La chiave privata, necessaria per decifrare i file, viene memorizzata nel server dell'aggressore stesso. Quest'ultimo mette la chiave privata a disposizione della vittima solo dopo il pagamento del riscatto, anche se non è sempre così, come si è visto in recenti campagne di ransomware. Senza l'accesso alla chiave privata, decifrare i file tenuti in ostaggio è pressoché impossibile.

Esistono diverse varianti di ransomware. Spesso il ransomware (e altro malware) viene distribuito utilizzando campagne di email spam o attraverso attacchi mirati. I prodotti McAfee® sfruttano varie tecnologie che aiutano a prevenire il ransomware. I seguenti prodotti McAfee e le configurazioni associate sono progettati per bloccare molti tipi di ransomware.

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 8 milioni di firme di ransomware uniche.
- Sviluppare regole di protezione degli accessi per bloccare l'installazione di payload ransomware: fare riferimento agli articoli della base di conoscenza delle regole di protezione degli accessi: **KB81095** e **KB54812**.

McAfee Host Intrusion Prevention

- **Guarda il video** su come configurare McAfee Host Intrusion Prevention per prevenire il payload di CryptoLocker.
- Abilitare la firma 3894 di McAfee 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 McAfee Host Intrusion Prevention per bloccare immediatamente le iniezioni.

Le regole di McAfee Host Intrusion Prevention

McAfee Host Intrusion Prevention supporta il monitoraggio della creazione, lettura, scrittura, esecuzione, cancellazione, ri-denominazione dei file, modifica degli attributi e creazione di un hard-link. Definire per quale percorso/tipo di file si desidera o non si desidera ricevere un avviso e quali eseguibili si desidera includere (fonti notoriamente pericolose) o escludere (noti creatori di falsi positivi). Questa regola ha il potenziale di essere intrusiva, perciò prendere in considerazione di utilizzare la regola in modalità informativa/log per un periodo di prova. Notare che le regole per la protezione dei file richiedono la creazione del proprio database di applicazioni affidabili.

Rule: Cryptolocker—block EXE in AppData
Rule type: files
Operations: create, execute, write
Parameters:
- Include: Files: **\AppData*.exe
- Include: Files: **\AppData\Local*.exe
- Include: Files: **\AppData\Roaming*.exe

Executables: Include *.*

Notare che il seguente esempio ha omesso molte estensioni dei file a causa dei limiti di spazio. Assicurarsi di verificare tutte le estensioni di file valide per le proprie applicazioni.

```
Rule {
tag “Blocking a Non-Trusted program attempt to write to protected data file extensions”
Class Files
Id 4001
level 4
files {Include “*\\*.3DS” “*\\*.7Z” “*\\*.AB4” “*\\*.AC2” “*\\*.ACCDB” “*\\*.ACCDE” “*\\*.ACCDR” “*\\**.ACCDT” “*\\*.ACR” “*\\*.ADB” “*\\*.AI” “*\\*.AIT” “*\\*.al” “*\\*.APJ” “*\\*.ARW” “*\\*.ASM” “*\\*.ASP” “*\\*.BACKUP” “*\\*. BAK” “*\\*.BDB” “*\\*.BGT” “*\\*.BIK” “*\\*.BKP” “*\\*. BLEND” “*\\*.BPW” “*\\*.C” “*\\*.CDF” “*\\*. CDR” “*\\*. CDX” “*\\*.CE1” “*\\*.CE2” “*\\*.CER” “*\\*.CFP” “*\\*.SRF” “*\\*.SRW” “*\\*.ST4” “*\\*.ST5” “*\\*.ST6” “*\\*.ST7” “*\\*. ST8” “*\\*.STC” “*\\*.STD” “*\\*. STI” “*\\*.STW” “*\\*.STX” “*\\*.SXC” “*\\*.SXD” “*\\*.SXG” “*\\*.SXI” “*\\*.SXM” “*\\*. SXW” “*\\*.TXT” “*\\*.WB2” “*\\*.X3F” “*\\*.XLA” “*\\*. XLAM” “*\\*.XLL” “*\\*. XLM” “*\\*.XLS” “*\\*.XLSB” “*\\*. XLSM” “*\\*.XLSX” “*\\*.XLT” “*\\*.XLTM” “*\\*. XLTX” “*\\*. XLW” “*\\*.XML” “*\\*.ZIP”}
Executable {Include “*”}
user_name{Include “*”}
directives files:writefiles:renamefiles:delete
}
```

- Regole di protezione dell’accesso: puoi anche utilizzare regole di protezione dell’accesso per rafforzare la regola di Host Intrusion Prevention con l’utilizzo di una wildcard flessibile: **\Users**\AppData***.exe

Nota: con le nuove versioni di SYSCore fornite dalle versioni aggiornate di McAfee VirusScan® Enterprise, McAfee Agent, McAfee Host Intrusion Prevention e McAfee Data Loss Prevention, gli ** non funzionano più all’inizio del campo “File or folder name to block” (Nome di file o cartella da bloccare). Con le versioni più recenti, è necessario utilizzare il seguente formato:

```
C:\**\AppData\**.exe
```

Questo formato è studiato per bloccare qualsiasi .exe casuale alla radice e tutte le sotto-directory di una cartella denominata AppData ovunque sul drive C:.

Le possibili iterazioni di una regola di questo tipo sono pressoché illimitate, perciò considerare attentamente tutti gli aspetti di questa regola. Si vorranno prendere in considerazione tutti gli aspetti della regola, tutte le possibili voci per la sua funzione prevista e anche come configurare le regole come un insieme (esempio di seguito):

```
Process to include: *
Process to exclude: [Lasciare in bianco]
File or folder name to block: <percorso o directory>
File actions to prevent: [Qualsiasi azione si desideri (si consiglia di iniziare con azioni meno aggressive per minimizzare il possibile danno all’endpoint)]
```

McAfee SiteAdvisor® Enterprise o Endpoint Security Web Protection

- Utilizza le reputazioni del sito web per prevenire o avvisare gli utenti dei siti web che il ransomware è stato distribuito.

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 McAfee Threat Intelligence Exchange.
  - Rimuovere se: known malicious (notoriamente dannoso).
  - Blocca se: most likely malicious (olto 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:
  - Esecuzione della reputazione del file (soggetto alla modalità di funzionamento) - Most likely malicious (Molto probailmente dannoso) - Ripulire/Eliminare
  - Might be malicious (probabilmente dannoso) - Bloccare.
- 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 pericoloso).
- Oppure scegliere di abilitare un processo indesiderato a fini di test:
  - Contrassegnare il file come might be trusted (probabilmente affidabile).

McAfee Advanced Threat Protection

- Capacità di rilevamento in-box:
  - Rilevamento basato su firme - Le firme mantenute da McAfee Labs includono oltre 8 milioni di firme ransomware, comprese quelle di CTB-Locker, CryptoWall e delle loro varianti.
  - Rilevamento basato sulla reputazione - McAfee GTI.
  - Analisi statica in tempo reale ed emulazione - 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 ransomware:
  - Sistemi operativi comuni, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows XP.
  - 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 include delle firme nelle sue policy di default per rilevare quanto segue:
  - Verificare di disporre della firma id=0x4880f900 (specifica per il ransomware).
  - McAfee Network Security Platform dispone anche di firme per identificare TOR, ce può essere utilizzato 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, Java Archive 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 (botnet).

McAfee Web Gateway

- Attivare il controllo di McAfee Gateway Anti-Malware.
- Attivare 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.
- Notare che 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 McAfee).

McAfee Active Response

McAfee Active Response individua e reagisce alle minacce avanzate. Quando viene utilizzato unitamente ai feed sulle minacce come McAfee GTI, Dell SecureWorks o ThreatConnect, è possibile ricercare ed eliminare nuove minacce - ransomware incluso - prima che abbiano la possibilità di diffondersi.

- Controllori personalizzati consentono di creare strumenti specifici per trovare e identificare indicatori di compromesso associati al ransomware.
- 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 intrapresa automaticamente un'azione di cancellazione.

Ulteriori letture

Protecting Against Ransomware (Proteggersi contro il ransomware)

Quest'articolo della base di conoscenza fornisce ai clienti le ultime informazioni dettagliate per proteggersi contro il ransomware all'interno di un ambiente McAfee.

Per informazioni approfondite sulle diverse varianti del ransomware CryptoLocker, sintomi, vettori di attacco e tecniche di prevenzione, consultare i seguenti video:

- **CrytpoLocker Malware Session (Sessione sul malware CryptoLocker)**
- **CryptoLocker Update (Aggiornamento di CryptoLocker)**

Avviso sulle minacce McAfee Labs: X97M/Downloader

Quest'articolo fornisce ai clienti un'analisi dettagliata della più recente versione del ransomware.

Sconfiggi il ramsomware: assicurati che i tuoi dati non siano presi in ostaggio

Documento di quattro pagine che delinea cos'è il ransomware e come alcune (ma non tutte) delle soluzioni McAfee aiutano a proteggersi.

Advice for Unfastening CryptoLocker Ransomware (Suggerimento per sbloccare il ransomware CryptoLocker)

Dettagliato articolo sul blog dedicato a quanto un cliente dovrebbe fare dopo un attacco ransomware.

Il ritorno del ransomware: la vendetta delle nuove famiglie

Articolo del report sulle minacce di McAfee Labs (pagina 14) evidenzia il ransomware nuovo e in evoluzione.

McAfee
Together is power.

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

1938_1016
OTTOBRE 2016