Documentazione

Protezione dal malware evasivo

Come descritto nel Report sulle minacce McAfee Labs: giugno 2017, il malware evasivo si maschera per evitare di essere rilevato. Si nasconde facendosi trasportare o abusando di applicazioni legittime. Si accorge di quando lo stanno analizzando in una sandbox e ritarda l'esecuzione di giorni, settimane o anche mesi in attesa che si presenti l'opportunità di colpire.

La creazione di un programma di sicurezza per proteggersi dal malware evasivo deve basarsi su tre componenti fondamentali.

- **Persone**: i professionisti devono essere preparati per reagire correttamente agli eventi di sicurezza e per gestire correttamente la tecnologia di protezione in essere. Per infettare gli utenti gli autori degli attacchi usano comunemente il social engineering. Senza preparazione e sensibilizzazione interni, gli utenti spalancano di fatto le porte ai pirati informatici.
- **Processo**: bisogna porre in essere strutture chiare e processi interni in modo che gli addetti alla sicurezza operino in modo efficace. Le migliori pratiche di sicurezza (aggiornamenti, backup, governance, informazioni, piani di risposta agli eventi e molto altro) sono fondamentali per rendere efficace il team della sicurezza.
- **Tecnologia**: la tecnologia supporta persone e processi. Va mantenuta e potenziata in modo che si adatti alle nuove minacce.

Policy e procedure di pratico utilizzo per proteggere contro il malware evasivo.

- La difesa più importante contro le infezioni del malware rappresentata dagli utenti. Questi ultimi devono essere consapevoli del rischio di scaricare e installare le applicazioni provenienti da fonti potenzialmente rischiose. Gli utenti devono inoltre imparare che il malware può essere inavvertitamente scaricato durante la navigazione.
- Tenere sempre browser, componenti aggiuntivi e antimalware negli endpoint e gateway di rete aggiornati e all'ultima versione.

McAfee™
Together is power.

- Non autorizzare nella rete affidabile sistemi che non siano distribuiti e certificati dal gruppo di sicurezza informatica dell'azienda. Il malware evasivo può essere facilmente disseminato da sistemi non protetti e connessi alla rete affidabile.
- Il malware evasivo può nascondersi all'interno di software legittimo precedentemente infettato da un trojan. Per prevenire un attacco di questo genere, consigliamo caldamente di avere dei meccanismi ermetici 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 siano autorizzati a installare applicazioni che non siano state 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 del malware evasivo.
- Evitare di scaricare le applicazioni da fonti non del 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.
- Mettere in atto un programma istruttivo per la prevenzione degli attacchi di phishing, che comunemente distribuiscono il malware.
- Sfruttare i feed di informazioni sulle minacce combinati con la tecnologia antimalware. Questa combinazione permette di velocizzare il rilevamento delle minacce.

Come i prodotti McAfee possono proteggere dal malware evasivo

McAfee offre una nuova generazione di funzioni di sicurezza progettate per combattere le più elusive minacce moderne. Sfruttando la potente analisi dell'apprendimento automatico e gli strumenti di contenimento delle applicazioni, le aziende sono in grado di smascherare le minacce nascoste e stroncarle sul nascere molto più rapidamente e con molta meno fatica.

Tali funzionalità vengono rese disponibili tramite i seguenti prodotti McAfee:

Real Protect

Real Protect, parte della soluzione McAfee Endpoint Protection, unisce l'analisi statica pre-esecuzione e l'analisi comportamentale post-esecuzione per intercettare più malware di qualsiasi soluzione basata sulle firme o esclusivamente statica, il tutto integrato nell'ecosistema McAfee. Real Protect applica tecniche di apprendimento automatico all'avanguardia per identificare il codice dannoso sulla base sia di una valutazione approfondita delle sue caratteristiche statiche (analisi pre-esecuzione) sia di ciò che fa (analisi dinamica del comportamento), il tutto senza l'uso di firme. Real Protect rimuove le più recenti tecniche di occultamento per smascherare le minacce nascoste, affinché il malware zero-day non sappia dove nascondersi.

Contenimento dinamico delle applicazioni

Il contenimento dinamico delle applicazioni (DAC), anch'esso parte della soluzione McAfee Endpoint Protection , protegge gli endpoint "paziente zero"da nuove infezioni malware zero-day. Quando un endpoint rileva un file sospetto, la funzionalità DAC blocca immediatamente i comportamenti che il malware utilizza con maggiore frequenza (come la modifica del registro di sistema, il salvataggio in una directory temporanea o l'eliminazione di file). A differenza di altre tecniche che farebbero perdere tempo al file (e all'utente) per diversi minuti, la funzionalità DAC lascia che il file sospetto si carichi nella memoria senza tuttavia consentirgli di apportare determinate modifiche all'endpoint o di infettare altri sistemi mentre persiste il suo stato sospetto.

Documentazione

Real Protect e DAC sono integrati - l'uno con l'altro, con altre soluzioni di sicurezza di terze parti come SPLUNK, Avecto, ForeScout e con McAfee Endpoint Protection - per fornire una protezione multilivello contro le minacce più evasive. Esse mettono i team della sicurezza in condizioni di affrontare tutte le fasi del ciclo di vita della difesa contro le minacce: rilevamento, correzione e protezione proattiva, in modo rapido e automatizzato.

Real Protect e DAC possono essere sfruttati per:

- Smascherare gli attacchi rimuovendo le tecniche di occultamento per vedere altre minacce malware.
- Limitare l'impatto di un attacco: contenere, schermare e prevenire danni ai sistemi, sia prima che si verifichi un attacco, sia prima che tale attacco possa causare un danno irreversibile.
- Rilevare e adattare: utilizzare difese automatizzate e integrate per eseguire una più ampia gamma di operazioni di sicurezza senza doverci pensare o senza doverle attivare manualmente.

Guarda un video dimostrativo di un'attività di contenimento di malware evasivo utilizzando Real Protect e DAC.

Le migliori procedure di configurazione del contenimento dinamico delle applicazioni
Le regole DAC nella policy McAfee Default sono impostate solo ai fini della segnalazione, riducendo perciò i falsi positivi. La protezione dalle minacce adattive offre due ulteriori policy DAC predefinite: McAfee Default Balanced e McAfee Default Security. Queste policy impostano le regole consigliate per il blocco, sulla base del profilo di sicurezza:

- McAfee Default Balanced fornisce un livello basilare di protezione minimizzando i falsi positivi per molti programmi di installazione e applicazioni comuni.
- McAfee Default Security fornisce una protezione decisa, ma potrebbe causare falsi positivi più frequentemente su programmi di installazione e applicativi privi di firme.

Valutare l'impatto delle regole DAC utilizzando la policy McAfee Default con le regole impostate per la segnalazione. Per stabilire se impostare le regole al blocco, monitorare i registri e i report. Dopo aver acquisito la violazione DAC consentita (evento ID 37280), impostare reputazioni di livello enterprise o esclusioni DAC prima di applicare la policy McAfee Default Balanced.

La funzionalità DAC può escludere i processi dal contenimento sulla base di nome, hash MD5, dati della firma e percorso. Se l'azienda dispone di strumenti di firma distribuiti internamente, aggiungere tali firme come esclusioni per ridurre i falsi positivi.

Le regole DAC dispongono di controllo di flusso che limita il numero di eventi generati per ora, regola e processo. Il controllo di flusso DAC traccia i processi in base all'ID del processo. Quando un processo riparte, il sistema operativo gli assegna un nuovo ID, che resetta il controllo di flusso anche se il nome del processo è lo stesso. Per esempio, se il Processo A viola la regola A DAC 100 volte all'ora, si riceverà un evento all'ora. Se il Processo A riparte durante quell'ora, il controllo di flusso resetta il Processo A e si riceverà un altro evento se continua a violare la regola A DAC. Se il Processo B viola la stesso regola A DAC, si riceverà un secondo evento (con i dettagli del Processo B). Leggere questo documento per maggiori informazioni sulle migliori procedure specifiche per le regole DAC definite da McAfee.

Eseguire lo strumento McAfee GetClean sulle immagini base di distribuzione per assicurarsi che vengano inviati file puliti a McAfee Global Threat Intelligence (GTI) ai fini della categorizzazione. Questo strumento aiuta a garantire che McAfee GTI non fornisca un valore di reputazione errato per i file. Per maggiori informazioni, consultare la Guida di Prodotto GetClean (PD23191).

McAfee Cloud Threat Detection
Migliora facilmente le protezioni McAfee per giudicare dannoso il malware avanzato e svelare le minacce evasive sfruttando McAfee Cloud Threat Detection (CTD). Ottieni l'accesso a McAfee ePO Cloud, abilita McAfee CTD e integralo con i tuoi prodotti McAfee.

Per utilizzare la funzionalità McAfee CTD con i tuoi prodotti di sicurezza McAfee, segui quanto sotto:

- Abilitare McAfee CTD in McAfee ePO Cloud.
- Abilitare McAfee CTD all'interno dell'interfaccia del proprio prodotto di sicurezza McAfee e ottenere la chiave di provisioning.
- Utilizzare la chiave di provisioning per generare una chiave di attivazione all'interno dell'interfaccia di McAfee ePO Cloud.
- Utilizzare la chiave di attivazione per attivare il proprio prodotto di sicurezza McAfee.

Le istruzioni dettagliate per ottenere la chiave di provisioning e attivare un prodotto variano. Fare riferimento alla guida di prodotto per informazioni dettagliate sull'integrazione di McAfee CTD con i propri prodotti McAfee.

Quando i prodotti integrati iniziano a inviare i file da analizzare a McAfee CTD, è possibile visualizzare le informazioni sull'utilizzo nella pagina Abbonamenti all'interno di McAfee ePO Cloud.

McAfee Active Response

- McAfee Active Response è stato creato appositamente per individuare e rispondere alle minacce avanzate. Quando viene utilizzato unitamente ai feed sulle minacce come McAfee GTI, Dell SecureWorks o ThreatConnect, è possibile ricercare ed eliminare le minacce evasive prima che abbiano la possibilità di diffondersi.
- Possono essere utilizzati controllori personalizzati per creare strumenti specifici per trovare e identificare indicatori di compromesso associati alle applicazioni infettate dai trojan.
- Attivatori e reazioni possono essere costruiti 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

Neutralize Advanced Threats: Adapt Layered Defenses for Comprehensive Malware Protection (Neutralizzare le minacce avanzate: adattare le difese a più livelli per una protezione completa dal malware)

McAfee Security Advice Center: i 10 metodi più efficaci per difendersi da malware e trojan

McAfee Endpoint Security: Domande frequenti

McAfee
Together is power.

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