Documentazione

Protezione dalle nuove minacce steganografiche

La steganografia, arte e scienza dell'occultamento, è utilizzabile per nascondere le informazioni anche nel mondo digitale. Un messaggio può essere nascosto all'interno di un'immagine, una traccia audio, un filmato o un file di testo. Può essere utilizzata per fini legittimi, ma più spesso la steganografia viene utilizzata dal malware.

Per evitare il rilevamento, alcuni malware usano la steganografia digitale per nascondere i propri contenuti ostili in un file di copertura, apparentemente innocente. Questa tecnica di evasione si avvantaggia del fatto che la maggior parte delle firme antimalware rileva il contenuto dannoso all'interno del file di configurazione del malware. Con la steganografia, il file di configurazione è incorporato nel file di copertura. Inoltre, il risultante file steganografico può decodificarsi nella memoria principale, riducendo ulteriormente le possibilità di rilevamento. Infine, è estremamente difficile rilevare la presenza di informazioni nascoste come un file di configurazione, un aggiornamento binario o un comando di bot all'interno di un file steganografico. Purtroppo, l'uso della steganografia negli attacchi informatici è facile da implementare e difficile da individuare.

Policy e procedure per proteggersi dagli attacchi steganografici

McAfee consiglia alle aziende di adottare le seguenti misure per proteggersi dalle minacce steganografiche.

- **Rafforzare i meccanismi di recapito e distribuzione del software per proteggersi dalle minacce interne.** È sempre una buona idea disporre di un repository centrale di applicazioni aziendali affidabili da cui gli utenti possono scaricare il software approvato, evitando così la pratica pericolosa di lasciare che gli utenti scarichino il software da fonti sconosciute che possono contenere codice steganografico.

McAfee
Together is power.

- **Guardare attentamente le immagini.** Con l'aiuto di un software per il ritocco delle immagini, cercare gli indizi che identificano la steganografia, come le lievi differenze di colore. Un gran numero di colori duplicati in un'immagine potrebbe indicare un attacco steganografico.
- **Controllare l'uso del software di steganografia.** La presenza del software steganografico in qualsiasi sistema aziendale dovrebbe essere proibita, se non specificamente richiesto per gli scopi aziendali. Impiegare questo tipo di software solo in un segmento di rete isolato.
- **Consentire solo firme affidabili.** Installare applicazioni solo con firme affidabili di fornitori affidabili.
- **Configurare l'antimalware per rilevare i binder.** Il software antimalware dev'essere configurato per identificare la presenza dei binder, che potrebbero contenere immagini steganografiche.
- **Segmentare la rete.** Nel caso indesiderato di un attacco steganografico andato a buon fine, architetture di virtualizzazione affidabili combinate con una corretta segmentazione della rete sono utili per contenere un focolaio perché il processo di avvio sicuro e verificabile che utilizzano e il monitoraggio continuo del traffico aiuteranno a mantenere isolate le applicazioni.
- **Monitorare il traffico in entrata.** Identificare la presenza degli attacchi steganografici monitorando il traffico in uscita.

Come i prodotti McAfee possono proteggere dal codice steganografico negli attacchi malware

McAfee Endpoint Security

Prevenzione delle minacce

Assicurarsi che McAfee Endpoint Security (ENS) sia configurato per prevenire qualsiasi minaccia nota dal malware che potrebbe contenere codice steganografico:

- Mantenere McAfee ENS aggiornato con le patch, versione dei file DAT e motore di scansione più recenti.
- Assicurarsi che tutti i sistemi all'interno del proprio ambiente siano protetti e aggiornati.
- Impostare la scansione in tempo reale (all'accesso) per analizzare tutti i file in lettura e in scrittura. Non disattivare mai la scansione in lettura, tranne quando si configurano processi a basso rischio.
- Le regole di esclusione per la scansione dovrebbero essere ridotte al minimo e utilizzate solo quando necessario. Se si sospetta la presenza di malware, assicurarsi che qualsiasi esclusione di scansione sia temporaneamente disabilitata. Scopri come impostare le esclusioni con un articolo della Knowledge Base KB88595.
- Comprendere le implicazioni per le prestazioni per l'utilizzo di configurazioni di "Processo ad alto rischio/Default/Basso rischio" per limitare l'esposizione alle minacce steganografiche in ambienti molto utilizzati o in quelli in cui la sicurezza hardware è minima. Maggiori informazioni su come migliorare le prestazioni con McAfee Endpoint Security KB88205.
- Configurare McAfee ENS per utilizzare la funzione di reputazione dei file di McAfee Global Threat Intelligence (GTI). Questa tecnologia aiuta a colmare il divario tra le minacce zero-day e i rilevamenti basati su firma. Scopri le impostazioni consigliate per la reputazione dei file di McAfee GTI nell'articolo KB74983, con maggiori informazioni nell'articolo KB53735.

- Configurare le regole di protezione dell'accesso di McAfee ENS per impedire la creazione di file autorun.inf.
- Utilizzare le regole di protezione dell'accesso per evitare l'installazione di minacce sconosciute.

Controllo del web

La funzione di controllo web di McAfee ENS è basata sui servizi di categorizzazione e di reputazione web di McAfee GTI. Il software infettato dalla steganografia spesso è localizzato in siti web di distribuzione del malware.

La funzione di controllo web di McAfee ENS identifica i siti - prima che vi si acceda - che ospitano malware o ne sono infetti, oppure includono contenuti inopportuni.

Controllo web McAfee:

- indica la sicurezza relativa dei siti web utilizzando uno scheda a colori:
  - Verde = Sicuro (rischio minimo o nullo)
  - Giallo = Cautela (rischio marginale)
  - Rosso = Allerta (rischio grave)
  - Grigio = Sconosciuto (non ancora classificato, fare attenzione)
  - McAfee Secure = testato quotidianamente per verificarne la vulnerabilità agli attacchi degli hacker
- Facile da distribuire e configurare tramite McAfee ePolicy Orchestrator.
- Fornisce un ulteriore livello di protezione endpoint. Può essere utilizzato con Internet Explorer, Firefox e Chrome.
- Utilizza un'efficace protezione antispam per impedire alle email dannose di entrare nelle reti.

Approfondisci: Guida di McAfee Endpoint Security - Utilizzare la funzione di controllo web di ENS

Protezione adattiva dalle minacce

- Abilitare McAfee Real Protect per applicare le tecniche di apprendimento automatico al fine di identificare le minacce avanzate sulla base sia del loro aspetto, di cosa potrebbe fare (analisi pre-esecuzione) e cosa fanno (analisi comportamentale dinamica), tutto senza firme. Approfondisci: Protezione adattiva dalle minacce—Real Protect
- Implementare il contenimento dinamico delle applicazioni di McAfee e segue le migliori procedure consigliate. Approfondisci: KB87843.

McAfee VirusScan Enterprise

I clienti che non hanno distribuito la versione più recente di McAfee ENS dovrebbero assicurarsi che McAfee VirusScan Enterprise (VSE) sia configurato per prevenire qualsiasi minaccia nota dal malware che potrebbe contenere codice steganografico:

- Mantenere McAfee VSE aggiornato con le patch, versione dei file DAT e motore di scansione più recenti.
- Assicurarsi che tutti i sistemi all'interno del proprio ambiente siano protetti e aggiornati.
- Impostare la scansione in tempo reale (all'accesso) per analizzare tutti i file in lettura e in scrittura. Non disattivare mai la scansione in lettura, tranne quando si configurano processi a basso rischio.

- Le regole di esclusione per la scansione dovrebbero essere ridotte al minimo e utilizzate solo quando necessario. Se si sospetta la presenza di malware, assicurarsi che qualsiasi esclusione di scansione sia temporaneamente disabilitata. Scopri come impostare le esclusioni con un articolo della Knowledge Base KB50998.
- In ambienti molto utilizzati o in quelli in cui la sicurezza hardware è minima, utilizzare configurazioni "Processo ad alto rischio/Default/Basso rischio" per limitare l'esposizione alle minacce steganografiche. Scopri questa funzionalità nell'articolo KB55139 e impara a configurarla nell'articolo KB58692.
- Configurare McAfee VSE per utilizzare la funzione di reputazione dei file di McAfee Global Threat Intelligence (GTI) . Questa tecnologia aiuta a colmare il divario tra le minacce zero-day e i rilevamenti basati su firma. Scopri le impostazioni consigliate per la reputazione dei file di McAfee GTI nell'articolo KB74983, con maggiori informazioni nell'articolo KB53735.
- configurare le regole di protezione dell'accesso di McAfee VSE per impedire la creazione di file autorun.inf.
- Utilizzare le regole di protezione dell'accesso per evitare l'installazione di minacce sconosciute.

McAfee Application Control
McAfee Application Control è un modo efficace per bloccare le applicazioni e il codice non autorizzati su server, desktop aziendali e dispositivi a funzioni fisse a seguito di un attacco steganografico. McAfee Application Control evita la violazione dei file e che i programmi che infettano i file si diffondano sulla rete.

McAfee Application Control aiuta a proteggere due aree principali:

- **Protezione basata su file:** protezione contro attacchi basati su file, tipici delle minacce steganografiche. Questi attacchi possono cercare di eseguire nuove applicazioni o modificare le applicazioni correnti.
- **Protezione della memoria:** protezione contro attacchi basati sulla memoria, che possono provenire da Internet, dalla rete o verificarsi in locale come risultato dell'esecuzione di un file.

Protezione basata su file
Le applicazioni che non sono incluse nella whitelist non sono né autorizzate né protette. Al contrario, gli elementi inclusi nella whitelist sono sia autorizzati che protetti. Se un elemento non autorizzato viene introdotto in un endpoint (per esempio, attraverso un download, accesso dalla rete o in locale tramite un drive flash o un CD), potrebbe essere copiato sull'endpoint o modificato e spostato da una cartella ad un'altra sull'endpoint, ma non può mai essere eseguito. Di seguito, alcuni esempi di questo tipo di eventi.

Esecuzione negata	Un'applicazione che non appare nella whitelist cerca di andare in esecuzione, ma viene bloccata da McAfee Application Control.
Installazione di ActiveX impedita	McAfee Application Control impedisce i tentativi di installare controlli ActiveX non autorizzati.

Se un processo non autorizzato (per esempio, derivante dall'esecuzione di un file dannoso su un endpoint remoto) o un utente non autorizzato cerca di modificare, rinominare, spostare o cancellare un file consentito e quindi protetto, McAfee Application Control bloccherà tale modifica. Di seguito, alcuni esempi di questo tipo di eventi.

Scrittura file negata	McAfee Application Control previene un tentativo di modificare un'applicazione consentita da un processo non autorizzato.
Variazione pacchetto impedita	McAfee Application Control impedisce che un'applicazione che utilizza un programma di installazione basato su MSI effettui installazioni, modifiche o rimozioni utilizzando un meccanismo non autorizzato.

Approfondisci: Le migliori pratiche per McAfee Application Control

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) rileva programmi di compressione furtivi estremamente sofisticati, payload crittografati e malware zero-day con un innovativo approccio a più livelli. Riunisce firme antimalware a bassa manutenzione, reputazione e protezioni di emulazione in tempo reale con analisi approfondita del codice statico e analisi dinamica del malware (sandboxing) per analizzare il comportamento del malware.

Approfondisci: Domande frequenti su McAfee Advanced Threat Defense

Per ulteriori informazioni

McAfee Security Advice Center: Protezione antiphishing

Dashboard sul panorama delle minacce: il kit di exploit Sundown è stato aggiornato alla fine del 2016 e si è scoperto che utilizza la steganografia per nascondere codice exploit.

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