Panoramica sulla soluzione

Proteggersi dalla manipolazione di firmware e BIOS

Nel ***Report McAfee Labs sulle minacce: Maggio 2015***, analizziamo a fondo Equation Group e i loro attacchi contro il firmware delle unità a disco rigido e allo stato solido (SSD). "Equation Group", così chiamato per l'affinità con schemi di crittografia estremamente sofisticati e il malware associato al gruppo, è ora tra gli esempi più visibili e avanzati di attacco al firmware visti finora.

Una delle scoperte più significative della ricerca riguarda i moduli di riprogrammazione del firmware delle unità a disco rigido (HDD) e a stato solido (SSD). Le unità HDD/SSD il cui firmware è stato riprogrammato possono ricaricare il malware associato ogni volta che i sistemi infettati si avviano. Il malware poi persiste anche se le unità vengono riformattate o il sistema operativo reinstallato. Inoltre, dopo che hanno infettato l'unità, il firmware riprogrammato e il malware associato non sono rilevabili da parte del software di sicurezza.

Negli ultimi anni, Intel Security ha osservato molti esempi di malware con capacità di manipolazione del firmware o del BIOS. Sono stati osservati sia in scenari accademici/PoC e in-the-wild, tra cui **CIH/Chernobyl**, Mebromi e **BIOSkit**. Abbiamo inoltre previsto questo specifico tipo di attacco nel report *Previsioni sulle minacce nel 2012 di McAfee Labs*. I campioni specifici dell'Equation Group scoperti possono ora essere considerati come alcuni degli esempi di attacco firmware più visibili e avanzati mai osservati.

Proteggersi dagli attacchi di Equation Group

Di seguito policy e procedure consigliate per proteggersi dagli attacchi in stile Equation Group:

- Installare software di sicurezza su tutti gli endpoint.
- Attivare gli aggiornamenti automatici del sistema operativo oppure scaricare gli aggiornamenti regolarmente per mantenere il sistema coperto dalle patch per le vulnerabilità note.
- Installare le patch degli altri produttori software non appena vengono rese disponibili.
- Crittografare dati e dischi rigidi importanti.
- Eliminare le campagne di phishing di massa con il filtraggio dei messaggi email tramite gateway protetti.
- Implementare la verifica dell'identità dei mittenti per ridurre il rischio di scambiare criminali informatici per mittenti affidabili.

intel Security

- Rilevare ed eliminare gli allegati pericolosi con strumenti antimalware avanzati.
- Eseguire la scansione degli URL presenti nei messaggi alla ricezione, e nuovamente al clic di un utente.
- Eseguire la scansione del traffico web alla ricerca del malware quando il phishing induce un utente a fare clic più volte e a infettarsi.
- Educare gli utenti ad adottare pratiche ottimali per sapere come riconoscere e come trattare i messaggi email sospetti.
- Implementare la prevenzione della perdita di dati per arrestare la diffusione in caso di violazione.

Cosa può fare Intel Security per aiutarti a proteggerti dagli attacchi di Equation Group

La protezione contro gli attacchi di manipolazione di firmware e BIOS dovrebbe far parte dell'approccio alla sicurezza di ogni azienda. Le aree principali su cui concentrarsi sono due:

- Stabilire delle modalità di rilevamento dell'iniziale invio del malware dell'Equation Group. I vettori d'attacco noti sono phishing, CD e drive USB. Porre speciale attenzione in queste aree.
- Tutelare i sistemi dalle sottrazioni di dati. Anche se tuttora non è possibile rilevare il modulo di riprogrammazione del firmware, l'obiettivo complessivo di un attacco è molto probabilmente la ricognizione. Dato che quest'ultima dipende dalla comunicazione e sottrazione sistematiche dei dati con un server di controllo, bloccare questa fase è di fondamentale importanza.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense è una soluzione multilivello per il rilevamento del malware che riunisce molteplici motori di verifica che applicano controlli basati su firme e reputazione, emulazione in tempo reale, analisi completa del codice statico e sandboxing dinamico. McAfee Advanced Threat Defense aiuta a proteggersi dal malware avanzato che ha il compito di ricaricarsi dal firmware riprogrammato di Equation Group.

- **Rilevamento basato sulle firme:** rileva virus, worm, rootkit, trojan, buffer overflow e attacchi misti. La sua knowledgebase esaustiva, creata e mantenuta da McAfee Labs, include attualmente oltre 150 milioni di firme.
- **Rilevamento basato sulla reputazione:** controlla la reputazione dei file usando la rete McAfee Global Threat Intelligence per rilevare le nuove minacce emergenti.
- **Analisi statica ed emulazione in tempo reale:** consentono di individuare rapidamente minacce zero-day e malware non identificati dalle tecniche basate su firma o secondo la reputazione.
- **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. Le funzioni esaustive di decompressione aprono tutti i tipi di file compressi e di archivi per abilitare l'analisi completa e la classificazione del malware, consentendo alla tua azienda di comprendere la minaccia posta dallo specifico malware.
- **Analisi dinamica nella sandbox:** esegue il codice del file in un ambiente di runtime virtuale e osserva il comportamento che ne risulta. Gli ambienti virtuali si possono configurare in modo da riprodurre gli ambienti host della tua azienda e supportano immagini personalizzate dei sistemi operativi Windows 7 (32/64 bit), Windows XP, Windows Server 2003, Windows Server 2008 (64 bit) e Android.

Panoramica sulla soluzione

McAfee Threat Intelligence Exchange
Disporre di una piattaforma di intelligence in grado di adattarsi alle esigenze del tuo ambiente è importante. **McAfee Threat Intelligence Exchange** riduce considerevolmente l'esposizione a questi tipi di attacchi grazie all'individuazione delle minacce immediate come file o applicazioni sconosciute.

- **Informazioni complete sulle minacce:** personalizza facilmente le informazioni complete sulle minacce provenienti dalle fonti dislocate in tutto il mondo. Queste ultime possono essere costituite da feed McAfee GTI oppure di terze parti, contenenti le informazioni locali sulle minacce derivanti da eventi passati o in fase di svolgimento, inviate tramite endpoint, gateway e altri componenti della sicurezza.
- **Prevenzione dell'esecuzione e remediation:** McAfee Threat Intelligence Exchange può intervenire e impedire l'esecuzione di applicazioni sconosciute nell'ambiente. Se un'applicazione ammessa all'esecuzione viene in seguito giudicata dannosa, McAfee Threat Intelligence Exchange disattiva in tutto l'ambiente i processi in esecuzione a essa associati, grazie alle potenti capacità di gestione centralizzata e di imposizione delle policy.
- **Visibilità:** McAfee Threat Intelligence Exchange può rilevare tutti i file eseguibili compressi e la loro esecuzione iniziale all'interno dell'ambiente, oltre a tutte le modifiche che si verificano in seguito. Tale visibilità sulle azioni di un'applicazione o processo, dall'installazione fino al momento contingente, velocizza risposta e remediation.
- **Indicatori di compromissione (IoC):** importate gli hash dei file nocivi in McAfee Threat Intelligence Exchange per immunizzare l'ambiente da questi file di pericolosità nota mediante l'imposizione di policy. Se nell'ambiente viene attivato uno degli IoC, McAfee Threat Intelligence Exchange può interrompere tutti i processi e le applicazioni associati a quell'IoC.

McAfee VirusScan Enterprise
McAfee VirusScan® Enterprise utilizza il premiato motore di scansione McAfee per proteggere i file da virus, worm, rootkit, trojan e altre minacce avanzate.

- **Protezione proattiva contro gli attacchi:** integra la tecnologia antimalware e la prevenzione delle intrusioni per proteggere dagli attacchi che sfruttano gli exploit da overflow del buffer indirizzati alle vulnerabilità delle applicazioni.
- **Rilevamento ed eliminazione del malware imbattibili:** protegge da minacce come rootkit e trojan con l'analisi avanzata dei comportamenti. Blocca il malware sul nascere impiegando tecniche tra cui il blocco delle porte, dei nomi file, delle cartelle o directory e delle condivisioni dei file, rintracciando e risolvendo le infezioni.
- **Sicurezza in tempo reale tramite l'integrazione di McAfee GTI:** protegge contro le minacce note ed emergenti su tutti i vettori – file, web, email e rete – grazie al supporto della piattaforma di informazioni sulle minacce più esaustiva del mercato.

McAfee Network Security Platform
McAfee Network Security Platform è studiato per eseguire ispezioni approfondite del traffico di rete. Il prodotto combina una serie di tecniche di ispezione avanzate (tra cui l'analisi completa del protocollo, la reputazione delle minacce, l'analisi del comportamento e l'analisi avanzata del malware) per rilevare e prevenire sia gli attacchi noti che quelli zero-day sulla rete.

- **Difesa completa contro il malware:** combina la reputazione dei file di McAfee GTI, l'analisi approfondita dei file con ispezione di JavaScript e l'analisi avanzata e senza firma del malware per rilevare e neutralizzare le minacce zero-day, il malware personalizzato e altri attacchi di virus occulti.

- **Sfrutta tecniche di ispezione avanzate:** comprende analisi completa dei protocolli, reputazione delle minacce e analisi del comportamento per rilevare e prevenire sia gli attacchi di rete di tipo noto, sia quelli zero-day.
- **Integrazione con McAfee Global Threat Intelligence:** abbina i feed di reputazione dei file in tempo reale, di reputazione degli indirizzi IP e di localizzazione geografica a dati contestuali completi su utenti, dispositivi e applicazioni per rispondere rapidamente e con precisione agli attacchi veicolati tramite la rete.
- **Security Connected:** grazie all'utile integrazione fra i due prodotti, McAfee Network Security Platform può inviare i file sospetti scoperti nel traffico monitorato a McAfee Advanced Threat Defense e negarne o consentirne l'esecuzione a seconda dei risultati ottenuti da McAfee Advanced Threat Defense.

McAfee DLP Monitor

McAfee Data Loss Prevention (DLP) Monitor acquisizione, traccia e crea report sui dati in movimento sull'intera rete. Scopre facilmente le minacce sconosciute ai dati e agire per proteggerli per assicurare che la tua azienda non subisca la prossima violazione ai big data.

- **Esamina il traffico di rete:** la funzionalità di scansione e analisi dei dati di McAfee DLP Monitor esamina il traffico di rete a un livello approfondito.
- **Identificazione rapida dei dati:** il rilevamento in tempo reale dettaglia in modo rapido come vengono usati i dati, chi li utilizza e dove sono diretti, fornendo le informazioni utili all'azione. McAfee DLP Monitor può identificare rapidamente oltre 300 tipi di contenuti che attraversano qualsiasi porta o protocollo, assicurando visibilità alla tua azienda.
- **Esegue analisi scientifiche forensi dettagliate:** conduci un'analisi forense per correlare gli eventi di rischio attuali e passati, individuare le tendenze di rischio e identificare le minacce. Consente di comprendere rapidamente la situazione e sviluppare regole e policy per affrontarla.

McAfee DLP Prevent

McAfee Data Loss Prevention (DLP) Prevent protegge dalla perdita di dati, garantendo che i dati lascino la rete solo nei casi appropriati, a prescindere che si tratti di email, webmail, messaggi istantanei, wiki, blog, portali, HTTP/HTTPS o trasferimenti FTP. Essere in grado di identificare e mitigare rapidamente i tentativi di esfiltrazione fanno la differenza tra il mantenere i tuoi dati preziosi al sicuro ed essere il prossimo caso di cronaca.

- **Ottieni visibilità sugli eventi di sicurezza:** visualizzazioni personalizzate e report sugli incidenti forniscono viste di riepilogo e dettagliate sugli incidenti di sicurezza e le azioni di mediazioni eseguite.
- **Implementare le policy in modo proattivo per tutti i tipi di informazioni:** implementa le policy per le informazioni che sai essere sensibili e per le informazioni non ovvie di cui non sei a conoscenza. Con un'ampia gamma di policy incorporate - dalla conformità all'utilizzo accettabile fino alla proprietà intellettuale - puoi far corrispondere documenti interi e parziali con una serie di regole completa per proteggere tutte le informazioni sensibili.

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