Panoramica sulla soluzione

Protezione contro il malware delle GPU

Nel **Report McAfee® Labs sulle minacce: agosto 2015**, prediamo approfonditamente in esame il malware che si distacca dallo standard dello sfruttamento della memoria di sistema degli endpoint o della CPU anziché attaccare l'unità di elaborazione grafica (GPU).

Il malware che attacca o sfrutta le unità di elaborazione grafica degli endpoint non è una novità. I trojan per il mining di Bitcoin che sfruttano il throughput delle unità di elaborazione grafica per incrementare i potenziali pagamenti da parte dei sistemi compromessi sono in circolazione da almeno quattro anni. Tuttavia, la pubblicazione del codice Proof of Concept che si vanta di sfruttare le capacità delle GPU in modi mai sperimentati prima ha nuovamente acceso i riflettori sul malware basato sulle unità di elaborazione grafica. Tali affermazioni, che verranno illustrate approfonditamente nel report, si possono riassumere in quattro punti principali:

- Accesso alla memoria dell'host CPU dalla GPU.
- Successiva eliminazione dei file dall'host CPU.
- Persistenza in caso di riavvio a caldo.
- Assenza di strumenti di analisi della GPU.

Le minacce dirette alle GPU sono un problema reale, anche se il malware che sferra questo tipo di attacchi è ancora soltanto Proof of Concept. Non abbiamo ancora assistito infatti ad una proliferazione "in the wild". L'assenza di strumenti in grado di condurre analisi forensi sulle unità di elaborazione grafica ha condotto a una situazione in cui la decompilazione e l'analisi forense delle minacce alle GPU sono un'attività assai più complessa e impegnativa rispetto all'analisi degli attacchi che sfruttano memoria o CPU. Gli aggressori hanno ridotto la superficie di rilevamento spostando il codice dannoso fuori dalla CPU e dalla memoria, anche se non completamente poiché alcuni infinitesimali elementi della loro attività restano spesso sull'endpoint.

Ci saranno senza dubbio ulteriori progressi nel malware basato sulle unità di elaborazione grafica da parte degli aggressori e potremo scoprire quanto saranno prolifici questi tipi di attacchi soltanto vivendo.

Tutela contro il malware delle GPU

McAfee Labs consiglia diversi modi per proteggere i sistemi dagli attacchi alle GPU.

- Abilitare gli aggiornamenti automatici del sistema operativo o scaricarne regolarmente gli aggiornamenti per mantenerlo aggiornato con le patch più recenti contro le vulnerabilità note.
- Installare le patch degli altri produttori software non appena vengono rese disponibili.

intel Security

- Installare il software di sicurezza per endpoint su tutti gli endpoint e mantenere aggiornate le firme antimalware.
- Considerare la possibilità di adottare il whitelisting per bloccare l'esecuzione delle applicazioni non autorizzate.
- Evitare il più possibile di eseguire le applicazioni in modalità amministratore.

Che cosa può fare Intel Security per aiutarvi a proteggervi dal malware delle GPU

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense è una soluzione di rilevamento del malware multilivello che si avvale di più motori di ispezione. Combinando l'analisi basata sulle firme e sulla reputazione eseguita da una serie di motori di ispezione, l'emulazione in tempo reale, l'analisi completa del codice statico e il sandboxing dinamico, McAfee Advanced Threat Defense protegge dal malware avanzato.

- **Rilevamento basato sulle firme:** rileva virus, worm, spyware, bots, trojan, buffer overflow e attacchi misti. McAfee Advanced Threat Defense comprende una knowledgebase esaustiva, creata e mantenuta da McAfee Labs, che include attualmente oltre 150 milioni di firme.
- **Rilevamento basato sulla reputazione:** cerca la reputazione dei file usando il servizio McAfee Global Threat Intelligence (McAfee GTI) 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 statica completa del codice:** 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.

McAfee VirusScan Enterprise

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

- **Protezione proattiva contro gli attacchi:** integra la tecnologia antimalware con la prevenzione delle intrusioni per proteggerti contro gli attacchi che sfruttano gli exploit da overflow del buffer mirati alle vulnerabilità delle applicazioni.
- **Rilevamento ed eliminazione del malware imbattibili:** protegge contro le minacce come rootkit e trojan grazie all'analisi comportamentale avanzata. Neutralizza il malware all'istante mediante diverse tecniche come il blocco delle porte, il blocco in base al nome dei file, il blocco di cartelle/directory e delle condivisioni di file e la traccia e il blocco delle 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 Threat Intelligence Exchange

Una piattaforma intelligente in grado di adattarsi alle esigenze del tuo ambiente è essenziale. **McAfee Threat Intelligence Exchange** riduce notevolmente l'esposizione a questi tipi di attacchi grazie alla sua visibilità sulle minacce immediate, come file o applicazioni sconosciuti.

- **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 allo stato attuale, accelera risposta e remediation.
- **Indicatori di compromissione (IoC):** gli IoC importano spesso hash dei file nocivi. McAfee Threat Intelligence Exchange è in grado di immunizzare il tuo ambiente da questi file di pericolosità nota mediante l'imposizione delle 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 Application Control

McAfee Application Control permette di controllare le applicazioni di cui è autorizzata l'esecuzione nel tuo ambiente mediante policy di whitelisting dinamico e di imposizione sia sugli endpoint connessi che su quelli offline, garantendo alla tua azienda di essere protetta contro le applicazioni dannose vulnerabili o note.

- **Whitelisting dinamico:** consente alla tua organizzazione di gestire con efficienza le applicazioni presenti nella whitelist, compilandola automaticamente via via che i sistemi vengono aggiornati e dotati di patch.
- **Reputazione dei file:** l'integrazione con McAfee GTI permette a McAfee Application Control di interrogare flussi di informazioni in tempo reale sui tipi di file noti (innocui, pericolosi e sconosciuti) per facilitarne l'inserimento nella whitelist e mantenere la tua azienda sempre al corrente delle vulnerabilità o degli attacchi di applicazioni che potrebbero essere state alterate.
- **Protezione per dispositivi connessi e non connessi:** imposizione di controlli su tutti i dispositivi, connessi e non connessi: server, macchine virtuali, endpoint e dispositivi a funzionalità fissa come i terminali POS.

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