Présentation de solution

Protection contre les logiciels malveillants ciblant le GPU

Le **Rapport de McAfee® Labs sur le paysage des menaces — Août 2015** s'intéresse de près aux logiciels malveillants qui délaissent l'exploitation de la mémoire système ou processeur (CPU) d'un terminal pour cibler spécifiquement le processeur graphique (GPU, Graphics Processing Unit).

Les logiciels malveillants qui exploitent ou attaquent le GPU d'un terminal ne datent pas d'hier. Depuis au moins quatre ans, on observe la présence de chevaux de Troie conçus pour le minage des bitcoins. Ces menaces tirent parti du débit important du processeur graphique pour augmenter le « dividende » par système infecté. Toutefois, ce type de malware a reçu un coup de projecteur dernièrement avec la publication de code dans le cadre de plusieurs projets de preuve de concept prétendant exploiter la puissance et les fonctions du GPU à l'aide de méthodes inédites. Ces affirmations, décrites en détail dans le rapport, reposent principalement sur quatre principes :

- Accès à la mémoire hôte dédiée au CPU à partir du GPU
- Suppression ultérieure des fichiers hôte du CPU
- Persistance après les redémarrages à chaud
- Absence d'outils d'analyse du GPU

Les menaces ciblant le GPU sont effectivement préoccupantes même si, à ce stade, les logiciels malveillants à l'origine de telles attaques ne sont jamais que des preuves de concept. Aucune exploitation de ce type n'a encore été signalée ou observée en environnement réel jusqu'à présent. Compte tenu du manque d'outils d'investigation capables d'analyser le GPU, l'ingénierie inverse et l'analyse numérique de telles menaces représentent une tâche bien plus complexe et difficile que l'analyse des attaques exploitant la mémoire ou le CPU. Les attaquants ont réduit la surface de détection en exécutant le code malveillant ailleurs que dans le CPU et la mémoire, mais ils n'ont pas réussi à l'éliminer complètement car il reste souvent des traces de leurs activités sur le terminal.

Il ne fait aucun doute que les cybercriminels vont perfectionner les logiciels malveillants ciblant le GPU. Quant à savoir si ces attaques se multiplieront et connaîtront le succès qu'ils escomptent, seul l'avenir nous le dira.

intel Security

Mesures de protection contre les logiciels malveillants ciblant le GPU

Pour protéger les systèmes contre les attaques du GPU, McAfee Labs recommande ce qui suit :

- Activez les mises à jour automatiques du système d'exploitation ou téléchargez régulièrement ces mises à jour afin que vos systèmes bénéficient en permanence des derniers correctifs requis pour corriger leurs vulnérabilités connues.
- Installez les correctifs d'autres éditeurs de logiciels dès qu'ils sont disponibles.
- Installez un logiciel de sécurité complet sur tous les terminaux et mettez à jour les signatures antimalware.
- Envisagez de mettre en œuvre les listes blanches d'applications pour bloquer l'exécution des applications non autorisées.
- Évitez dans la mesure du possible d'exécuter des applications en mode administrateur.

Comment Intel Security peut vous aider à vous protéger contre les logiciels malveillants exploitant le GPU

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense est une solution multiniveau de détection des logiciels malveillants qui combine plusieurs moteurs d'inspection. Grâce à ces moteurs qui mettent en œuvre l'inspection basée sur les signatures et la réputation, l'émulation en temps réel, l'analyse statique complète du code et l'analyse dynamique en environnement restreint (*sandbox*), McAfee Advanced Threat Defense vous aide à vous protéger contre les logiciels malveillants avancés.

- **Détection basée sur les signatures —** Débusque les virus, les vers, les logiciels espions (*spyware*), les robots, les chevaux de Troie, les débordements de mémoire tampon et les attaques combinées. McAfee Advanced Threat Defense comprend une base de connaissances exhaustive, créée et gérée par McAfee Labs, qui compte actuellement plus de 150 millions de signatures.
- **Détection basée sur la réputation —** Tire parti du service McAfee Global Threat Intelligence (McAfee GTI) pour analyser la réputation des fichiers afin de détecter les nouvelles menaces émergentes.
- **Émulation et analyse statique en temps réel —** Permet de détecter rapidement les logiciels malveillants et les menaces « jour zéro » non identifiables au moyen des techniques basées sur les signatures ou la réputation.
- **Analyse statique complète du code —** Reconstitue la logique du code pour évaluer l'ensemble des attributs et des jeux d'instructions, et effectuer un examen approfondi du code source sans l'exécuter. En ouvrant tous les types de fichiers compressés afin d'effectuer une analyse minutieuse et une classification des logiciels malveillants qu'ils contiennent, les fonctionnalités de décompression permettent aux entreprises de mieux comprendre les risques posés par les logiciels malveillants auxquels elles ont affaire.
- **Analyse dynamique dans un environnement restreint de type « sandbox » —** Exécute le code du fichier suspect dans un environnement virtuel en temps réel et en observe le comportement. Les environnements virtuels peuvent être configurés de façon à correspondre à ceux des hôtes cibles et prennent en charge des images personnalisées des systèmes d'exploitation Microsoft Windows 7 (32/64 bits), Windows XP, Windows Server 2003 et Windows Server 2008 (64 bits), ainsi qu'Android.

McAfee VirusScan Enterprise

McAfee VirusScan® Enterprise fait appel au moteur d'analyse primé d'Intel Security pour protéger les fichiers contre les virus, les vers, les rootkits, les chevaux de Troie et d'autres menaces avancées.

- **Protection proactive contre les attaques —** Intègre une technologie antimalware avec le système de prévention des intrusions pour offrir une protection contre les attaques par débordement de mémoire tampon ciblant les vulnérabilités des applications.
- **Performances inégalées dans la détection et la neutralisation des logiciels malveillants —** Protège contre des menaces telles que les rootkits et les chevaux de Troie grâce à l'analyse avancée des comportements. Arrête net les logiciels malveillants grâce à plusieurs techniques dont le blocage de ports ou le blocage en fonction des noms de fichiers, le verrouillage de dossiers, de répertoires ou de partages de fichiers, ainsi que le suivi et le blocage des infections.
- **Sécurité en temps réel grâce à l'intégration de McAfee GTI —** Assure une protection contre les menaces connues et émergentes sur tous les vecteurs (fichiers, Web, messagerie électronique et réseau) grâce au soutien de la plate-forme de renseignements sur les menaces la plus complète du marché.

McAfee Threat Intelligence Exchange

Une plate-forme de renseignements capable de s'adapter aux besoins de votre environnement constitue un outil de première importance. **McAfee Threat Intelligence Exchange** réduit considérablement les risques d'attaques grâce à la visibilité offerte sur les menaces immédiates, notamment les applications ou fichiers inconnus.

- **Renseignements complets sur les menaces —** Créez aisément une base personnalisée de renseignements sur les menaces issus de plusieurs sources mondiales. Il est possible de combiner les flux McAfee GTI ou des flux externes avec des renseignements locaux tirés de données d'événement historiques et en temps réel, obtenues par le biais de composants de sécurité pour terminaux, au niveau de la passerelle et autres.
- **Prévention de l'exécution et correction —** McAfee Threat Intelligence Exchange peut intervenir pour empêcher l'exécution d'applications inconnues dans l'environnement. Si une application dont l'exécution était auparavant autorisée s'avère par la suite malveillante, McAfee Threat Intelligence Exchange peut, grâce à ses fonctions de gestion centralisée et de mise en œuvre des stratégies, désactiver les processus en cours d'exécution associés à l'application en question dans l'ensemble de l'environnement.
- **Visibilité —** McAfee Threat Intelligence Exchange est capable de surveiller tous les fichiers exécutables compressés et leur première exécution dans l'environnement, de même que l'ensemble des modifications survenant par la suite. Cette visibilité sur les actions effectuées par une application ou un processus depuis son installation accélèrent la réponse et la correction.
- **Indicateurs de compromission —** Les indicateurs de compromission importent souvent des hachages de fichiers dangereux connus. McAfee Threat Intelligence Exchange peut immuniser l'environnement contre ces fichiers dommageables grâce à la mise en œuvre des stratégies adéquates. Si l'un des indicateurs de compromission déclenche une alerte dans l'environnement, McAfee Threat Intelligence Exchange peut bloquer tous les processus et applications associés à cet indicateur.

McAfee Application Control

McAfee Application Control permet à votre entreprise de contrôler les applications autorisées à s'exécuter dans votre environnement par le truchement de listes blanches dynamiques et de stratégies de mise en œuvre, qui s'appliquent tant aux terminaux connectés qu'à ceux hors connexion. Votre société est ainsi assurée d'être protégée contre les applications vulnérables ou malveillantes connues.

- **Listes blanches dynamiques —** Cette fonction permet à l'entreprise de gérer efficacement les applications sur liste blanche en développant automatiquement cette dernière à mesure que les systèmes sont corrigés et mis à jour.
- **Réputation des fichiers —** L'intégration à McAfee GTI permet à McAfee Application Control d'interroger les flux d'informations en temps réel définissant les types de fichiers dont la réputation est bonne, mauvaise ou inconnue, de façon à aider l'entreprise à créer des listes blanches et à identifier les vulnérabilités ainsi que les attaques émanant d'applications qui peuvent avoir été modifiées.
- **Protection des équipements, qu'ils soient connectés ou hors connexion —** Les contrôles sont mis en œuvre sur les serveurs, les machines virtuelles, les terminaux et les équipements à fonction fixe tels que les terminaux de point de vente, qu'ils soient connectés ou non.

62072brf_protect-against-gpu-malware_0815

McAfee. Part of Intel Security.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com