Présentation de solution

Protection contre la manipulation du BIOS et des micrologiciels

Dans le ***Rapport trimestriel de McAfee Labs sur le paysage des menaces de mai 2015***, nous nous penchons sur Equation Group et sur les attaques qu'il a lancées à l'encontre des micrologiciels de disques durs et de disques électroniques. Equation Group, ainsi baptisé pour sa prédilection pour les modèles de chiffrement ultracomplexes et les logiciels malveillants (*malware*) associés, fait désormais partie des exemples d'attaques de micrologiciels les plus visibles et les plus avancés jamais observés.

Les recherches ont mis au jour un élément capital de leur méthodologie : des modules de reprogrammation de micrologiciels de disques durs (HDD) et de disques électroniques (SSD). Les disques durs/électroniques dont le micrologiciel a été reprogrammé peuvent charger à nouveau le malware associé chaque fois que les systèmes infectés démarrent. Le malware persiste même si les disques sont reformatés ou le système d'exploitation réinstallé. En outre, le micrologiciel reprogrammé et son malware ne peuvent pas être détectés par les logiciels de sécurité une fois le disque infecté.

Ces dernières années, Intel Security a observé de nombreux exemples de logiciels malveillants capables de manipuler le BIOS ou les micrologiciels. Ces logiciels malveillants, dont **CIH/Chernobyl**, Mebromi et **BIOSkit**, ont été observés aussi bien dans un contexte universitaire et de preuve de concept que dans des scénarios bien réels. Nous avions également annoncé l'émergence de ce type d'attaques dans le rapport de *McAfee Labs Prévisions 2012 en matière de menaces*. Avec la découverte des échantillons propres à Equation Group, on peut affirmer qu'il s'agit d'une des attaques de micrologiciels les plus évoluées jamais observées.

Se protéger contre les attaques d'Equation Group

Voici quelques stratégies et procédures recommandées pour se protéger contre les attaques analogues à celles d'Equation Group :

- Installez un logiciel de protection des terminaux sur l'ensemble du parc informatique.
- Activez les mises à jour automatiques du système d'exploitation ou téléchargez régulièrement ces mises à jour afin que vos systèmes d'exploitation 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.
- Chiffrez les données et les disques durs importants.

intel Security

- Éliminez les campagnes de phishing en masse grâce au filtrage des e-mails au niveau d'une passerelle sécurisée.
- Implémentez la vérification de l'identité des expéditeurs pour limiter le risque de confondre les cybercriminels avec des parties fiables.
- Détectez et éliminez les pièces jointes malveillantes grâce à un composant antimalware avancé.
- Analysez les URL contenues dans les e-mails au moment de la réception et à nouveau lors du clic.
- Analysez le trafic web pour détecter les logiciels malveillants lorsque l'e-mail de phishing incite l'utilisateur à cliquer sur divers liens afin de l'infecter.
- Sensibilisez les utilisateurs aux meilleures pratiques en matière de détection et de neutralisation des e-mails suspects.
- Implémentez la prévention des fuites de données pour empêcher l'exfiltration en cas de compromission.

Comment Intel Security peut vous aider à vous protéger contre des attaques analogues à celles d'Equation Group

La protection contre toute manipulation du BIOS et des micrologiciels doit faire partie de la stratégie de sécurité de toutes les entreprises. L'accent doit être mis sur deux points :

- Mettre en place des mesures capables de détecter la distribution initiale des logiciels malveillants d'Equation Group — Les vecteurs d'attaque connus sont le phishing, les CD et les clés USB. Il convient donc d'y être particulièrement attentif.
- Sécuriser les systèmes contre l'exfiltration des données — Bien que le module de reprogrammation ne puisse pas être détecté à l'heure actuelle, l'objectif premier de l'attaque est vraisemblablement la reconnaissance. Comme la reconnaissance dépend d'une communication systématique avec un serveur de contrôle et de l'exfiltration des données par celui-ci, le blocage de cette phase est particulièrement important.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense est une solution de détection des logiciels malveillants multiniveau qui combine plusieurs moteurs d'inspection. Ces derniers 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 conçus pour être rechargés par le micrologiciel reprogrammé par Equation Group.

- **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. La solution utilise 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 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 Windows 7 (32 ou 64 bits), Windows XP, Windows Server 2003 et Windows Server 2008 (64 bits), ainsi qu'Android.

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 menées à l'aide de kits d'exploits, 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 accélère la réponse et la correction.
- **Indicateurs de compromission —** Il est possible d'importer dans McAfee Threat Intelligence Exchange des informations sur les hachages de fichiers dangereux, de façon à ce que la solution immunise 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 VirusScan Enterprise

McAfee VirusScan® Enterprise fait appel au moteur d'analyse primé de McAfee 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 les menaces telles que les rootkits et les chevaux de Troie grâce à l'analyse avancée des comportements. Arrête net les logiciels malveillants grâce à diverses 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 Network Security Platform

McAfee Network Security Platform est conçu pour inspecter le trafic réseau de façon approfondie. La solution associe diverses techniques d'inspection évoluées, dont l'analyse de protocoles complète, l'analyse basée sur la réputation, l'analyse du comportement et l'analyse des logiciels malveillants avancés pour détecter et prévenir tant les menaces connues que les menaces de type « jour zéro » sur le réseau.

- **Protection antimalware complète —** Conjugue le service d'évaluation de la réputation des fichiers de McAfee GTI, l'analyse approfondie des fichiers avec inspection du code JavaScript et l'analyse sans signatures des logiciels malveillants avancés afin de détecter et de neutraliser les menaces de type « jour zéro », les logiciels malveillants personnalisés et d'autres attaques furtives.
- **Utilisation de techniques d'inspection avancées —** Recourt à l'analyse complète des protocoles, l'analyse basée sur la réputation et l'analyse des comportements pour détecter et bloquer les attaques connues et de type « jour zéro » lancées sur le réseau.
- **Intégration à McAfee Global Threat Intelligence —** Associe l'analyse en temps réel de la réputation des fichiers, l'analyse des adresses IP et les flux de géolocalisation à un riche éventail de données contextuelles sur les utilisateurs, les équipements et les applications pour des réponses précises et rapides aux attaques propagées via le réseau.
- **Security Connected —** McAfee Network Security Platform bénéficie d'une intégration avec McAfee Advanced Threat Defense, ce qui permet l'application d'actions pertinentes. Cette intégration lui permet de soumettre à McAfee Advanced Threat Defense les fichiers suspects détectés au sein du trafic surveillé et de les bloquer ou de les autoriser en fonction des résultats obtenus.

McAfee DLP Monitor

McAfee Data Loss Prevention (DLP) Monitor collecte et suit les données en mouvement sur l'ensemble du réseau et génère les rapports correspondants. Cette solution détecte facilement les menaces inconnues pesant sur vos données et prend les mesures requises pour les protéger, de manière à ce que votre entreprise n'ait pas à pâtir d'une compromission massive de données.

- **Examen du trafic réseau —** La technologie performante de balayage et d'analyse des données de McAfee DLP Monitor effectue un examen du trafic réseau approfondi.
- **Identification rapide des données —** La détection en temps réel permet de déterminer rapidement l'usage fait des données, les personnes qui les utilisent et la destination des données, de sorte que vous disposez d'informations permettant de prendre les mesures qui s'imposent. McAfee DLP Monitor est à même de détecter rapidement plus de 300 types de contenu transitant par n'importe quel port ou employant n'importe quel protocole, les empêchant ainsi de passer inaperçus aux yeux de votre entreprise.
- **Exécution d'analyses post-mortem détaillées —** Investigations numériques permettant de mettre en corrélation les événements de risque passés et présents, de détecter les tendances des risques et d'identifier les menaces. McAfee DLP Monitor vous permet de comprendre rapidement ce qui se passe, et d'élaborer des règles et stratégies pour remédier à la situation.

McAfee DLP Prevent

McAfee Data Loss Prevention (DLP) Prevent vous protège contre les fuites de données en s'assurant que les données ne quittent le réseau que lorsqu'elles y sont autorisées — que ce soit par le biais de la messagerie électronique, de la messagerie web, de la messagerie instantanée, de wikis, de blogs, de portails, de sites HTTP/HTTPS ou de transferts FTP. Toute la différence entre garder vos précieuses données à l'abri et faire la une des journaux réside dans la capacité à rapidement identifier les tentatives d'exfiltration et à y remédier.

- **Visibilité sur les incidents de sécurité —** Les vues personnalisées et les rapports sur les incidents offrent des vues synthétiques et détaillées sur les incidents de sécurité et les mesures correctives prises.
- **Mise en œuvre proactive de stratégies pour tous types d'informations —** Mettez en œuvre des stratégies de protection pour les informations sensibles que vous connaissez et pour celles dont vous ignorez peut-être l'existence. Grâce à l'éventail étendu de stratégies intégrées, régissant notamment la conformité, l'utilisation acceptable ou encore la propriété intellectuelle, vous pouvez mettre en correspondance des documents entiers ou partiels avec un ensemble complet de règles, de façon à protéger la totalité de vos données sensibles.

McAfee. Part of Intel Security.
Tour Pacific
13, Cours Valmy - La Défense 7
92800 Puteaux
France
+33 1 47 62 56 09 (standard)
www.intelsecurity.com