PRÉSENTATION DE SOLUTION

Protection contre les logiciels malveillants basés sur des scripts

Les auteurs de logiciels malveillants sont parvenus à compliquer la détection au moyen de techniques telles que le polymorphisme, l'implantation d'agents de surveillance, la révocation des autorisations et bien d'autres.

Ces dix dernières années, les pirates ont exploité des fonctionnalités telles que Microsoft Windows Management Instrumentation (WMI) et Windows PowerShell pour compromettre des terminaux sans avoir besoin d'enregistrer un fichier binaire sur disque. Les attaques en deviennent difficiles à détecter, car le code malveillant peut être implanté directement dans le Registre d'un hôte compromis.

Les infections par scripts existent depuis des années. Même si elles sont considérées comme des menaces opérant sans fichier, les familles de malwares antérieures enregistraient tout de même un petit fichier binaire sur le disque lors de la phase d'attaque initiale, avant de se propager dans la mémoire principale d'un système.

Cependant, les dernières techniques de contournement utilisées par les logiciels malveillants avec scripts ne laissent aucune trace sur le disque. Cette nouvelle approche complique singulièrement la détection dans la mesure où celle-ci s'appuie généralement sur la recherche de fichiers statiques. Pour en savoir plus, lisez notre analyse approfondie des logiciels malveillants basés sur des scripts dans le *Rapport sur le paysage des menaces de McAfee Labs — Septembre 2017*.

Trois types de logiciels malveillants basés sur des scripts sont les plus courants :

- **Malwares résidant en mémoire :** Ce type de logiciel malveillant utilise l'espace mémoire d'un fichier Windows légitime. Il charge son code dans cet espace mémoire et y réside passivement jusqu'à ce qu'il soit accédé ou réactivé. Bien que l'exécution intervienne au sein de l'espace mémoire du fichier légitime, il existe un fichier physique dormant qui initie ou redémarre l'exécution.
- **Rootkits :** Certains logiciels malveillants dissimulent leur présence derrière une API utilisateur ou noyau. Un fichier est présent sur le disque, mais en mode furtif.
- **Malwares résidant dans le Registre Windows :** Certains types avancés de logiciels malveillants basés sur des scripts résident dans le Registre Windows. Par le passé, les auteurs de malwares ont exploité des fonctionnalités telles que le cache de miniatures servant à stocker des images pour l'affichage Miniatures de l'Explorateur Windows. Le cache de miniatures offre à l'attaque un mécanisme de persistance. Les malwares de ce type doivent toujours pénétrer dans le système de la victime par le biais d'un fichier binaire statique. Pour ce faire, la plupart d'entre eux utilisent les e-mails comme vecteurs d'attaque. Dès que l'utilisateur clique sur la pièce jointe infectée, le logiciel malveillant écrit l'intégralité du fichier de la charge active sous une forme chiffrée dans une ruche du Registre Windows. Ensuite, il s'efface de lui-même pour disparaître du système.

Très intelligemment conçues, les familles actuelles de logiciels malveillants basés sur des scripts peuvent exécuter des attaques sur le Registre Windows sans le moindre fichier et sans laisser aucune trace dans le système de fichiers. Bien que leurs auteurs préparent l'environnement destiné à lancer ces attaques en exécutant du code dans un fichier, ce dernier se supprime lui-même dès que le système est prêt pour l'attaque malveillante.

Stratégies et procédures de protection contre les logiciels malveillants basés sur des scripts

Les meilleurs pratiques de cybersécurité de McAfee recommandent l'adoption de stratégies générales de prévention des menaces, tant pour les réseaux que pour les terminaux :

- La façon la plus efficace de protéger votre système des infections par logiciels malveillants basés sur des scripts est de les arrêter avant qu'ils n'aient le temps de s'exécuter. En d'autres termes, la prévention est fondamentale. Dans cette optique, l'élément clé est l'utilisateur lui-même. Les utilisateurs doivent être au courant des risques qu'implique le téléchargement ou l'installation d'applications qu'ils ne comprennent pas ou dont ils se méfient. Il arrive aussi que des utilisateurs téléchargent des logiciels malveillants sans le savoir lors de la navigation.
- Appliquez les mises à jour et correctifs de sécurité destinés aux applications et au système d'exploitation.

- Maintenez à jour les navigateurs web et les modules complémentaires. De même, les solutions antimalware sur les terminaux et les passerelles réseau doivent disposer des versions les plus récentes.
- N'utilisez jamais des systèmes qui ne sont pas distribués et certifiés par l'équipe de sécurité informatique de l'entreprise. Les logiciels malveillants basés sur des scripts peuvent être facilement propagés par des actifs non sécurisés connectés au réseau de l'entreprise.
- Si certains utilisateurs disposent de droits d'administrateur local et sont par conséquent autorisés à installer des applications de leur propre chef, informez-les qu'ils doivent uniquement installer des applications dotées de signatures approuvées provenant de fournisseurs connus. Il est très courant que des applications proposées en ligne, apparemment inoffensives, intègrent des rootkits ou d'autres logiciels malveillants basés sur des scripts.
- Évitez de télécharger des applications à partir d'autres types de sources que des sources web. Le risque de télécharger des logiciels infectés à partir de groupes Usenet, de canaux IRC, de clients de messagerie instantanée ou de réseaux peer-to-peer est très élevé. Les liens renvoyant à des sites web dans les canaux IRC et la messagerie instantanée pointent souvent vers des fichiers à télécharger infectés.
- Mettez en place un programme de formation sur la prévention des attaques de phishing. Il est en effet fréquent que les logiciels malveillants soient distribués dans des e-mails ciblés.
- Utilisez des flux de cyberveille conjointement avec vos technologies antimalware. Cette association est idéale pour améliorer le temps de détection des menaces émergentes ou déjà connues.

Comment McAfee vous aide à vous protéger contre les logiciels malveillants basés sur des scripts

La détection d'un logiciel malveillant basé sur des scripts, qui n'implique l'installation d'aucun fichier binaire initial, peut s'avérer ardue. Elle est souvent le fruit d'un long travail d'enquête de la part de l'équipe de sécurité de l'entreprise. Il existe cependant une méthode incontournable permettant de bloquer ce type d'infection : déployer les contrôles appropriés afin de priver les pirates d'un point d'entrée.

McAfee Endpoint Security

McAfee Endpoint Security (ENS) offre un cadre de sécurité collaboratif qui réduit la complexité des environnements de protection des terminaux, assure une visibilité accrue sur les menaces avancées (comme les logiciels malveillants basés sur des scripts) et accélère la détection et l'application de mesures correctives. Son architecture extensible permet aux équipes de sécurité d'appréhender et de gérer plus facilement le cycle de défense contre les menaces dans des environnements comportant une multitude de solutions de sécurité.

McAfee ENS intègre de nouvelles technologies et améliorations :

- **Real Protect.** Applique des techniques d'apprentissage automatique qui permettent d'identifier le code malveillant en évaluant ses activités potentielles (analyse pré-exécution) et réelles (analyse comportementale dynamique) — le tout sans signatures. Real Protect est un élément clé d'une stratégie de défense efficace contre les logiciels malveillants basés sur des scripts.
- **Confinement d'application dynamique.** Cette fonction permet notamment d'isoler une instance unique d'un processus.
- **Intégration de McAfee Client Proxy.** McAfee Endpoint Security peut désormais être associé à la protection multiniveau des passerelles web. Celle-ci assure une sécurisation continue de l'utilisateur dans tous ses déplacements, en conservant la couverture même en cas de sortie du réseau grâce à la connexion des terminaux au service de cloud Web Gateway.
- **Module Pare-feu.** Dans une stratégie de sécurité proactive, le niveau de protection suivant consiste à bloquer la communication entre l'ordinateur et les serveurs contrôlés par les cybercriminels.
- **Module Prévention contre les menaces.** Les analyses à la demande incluent désormais une option d'analyse du Registre, particulièrement utile pour se protéger contre les logiciels malveillants basés sur des scripts. Dans le cadre de la Protection de l'accès, les administrateurs peuvent créer des règles personnalisées relatives aux services, qui prennent maintenant en charge les services Windows. La fonctionnalité Prévention contre les exploits peut être personnalisée de même que les signatures IPS fournies par McAfee. Enfin, la protection des applications Windows a été ajoutée aux règles Prévention contre les exploits.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) est une solution multiniveau de détection des logiciels malveillants qui combine divers moteurs d'inspection. Avec ces moteurs combinés, qui effectuent une inspection basée sur les signatures et la réputation, une émulation en temps réel, une analyse statique complète du code et une analyse dynamique en environnement sandbox, McAfee ATD assure une protection contre les logiciels malveillants basés sur des scripts qui déposent initialement un fichier binaire sur les systèmes cibles.

- **Détection basée sur les signatures :** Débusque les virus, les vers, les logiciels espions (spywares), 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.
- **Détection basée sur la réputation :** Tire parti de McAfee Global Threat Intelligence (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 des logiciels malveillants précis.
- **Analyse dynamique dans un environnement restreint de type « sandbox » :** En présence d'un fichier dont les moteurs d'inspection précités sont incapables de déterminer l'innocuité, McAfee ATD offre la possibilité d'exécuter son code dans un environnement d'exécution virtuel et d'observer ainsi son comportement. Les environnements virtuels peuvent être configurés de façon à correspondre à ceux des hôtes cibles.

McAfee Threat Intelligence Exchange

Une plate-forme de cyberveille capable de s'adapter aux besoins de l'environnement au fil du temps constitue un outil de première importance. McAfee Threat Intelligence Exchange (TIE) réduit considérablement les risques d'attaques menées à l'aide de logiciels malveillants basés sur des scripts, grâce à la visibilité offerte sur les menaces immédiates, notamment les applications ou fichiers inconnus exécutés dans l'environnement.

- **Cyberveille complète sur les menaces :** Créez aisément une base personnalisée de cyberveille enrichie par 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 d'exécution et actions correctives :** McAfee TIE peut intervenir pour empêcher l'exécution d'applications inconnues dans l'environnement. Si une application dont l'exécution était auparavant autorisée se révèle par la suite malveillante, McAfee TIE peut, grâce à ses fonctions performantes de gestion centralisée et de mise en œuvre des stratégies, désactiver les processus en cours d'exécution associés à l'application coupable dans l'ensemble de l'environnement.
- **Visibilité :** McAfee TIE 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 des informations sur les hachages de fichiers dangereux, de manière à immuniser l'environnement contre ces menaces connues par l'application des stratégies adéquates. Si l'un des indicateurs déclenche une alerte dans l'environnement, McAfee TIE peut bloquer tous les processus et applications associés à cet indicateur de compromission.

McAfee Web Gateway

Les téléchargements involontaires et les URL malveillantes incorporées à des e-mails de phishing sont les principales méthodes d'attaque utilisées pour distribuer les logiciels malveillants basés sur des scripts. McAfee Web Gateway (MWG) est un produit robuste qui optimise la protection de votre entreprise contre ce type de menace.

- **McAfee Gateway Anti-Malware Engine :** L'analyse des intentions sans signatures élimine, en temps réel, le contenu malveillant du trafic web. L'émulation et l'analyse comportementale protègent de manière proactive contre les attaques ciblées et de type « jour zéro ». McAfee Gateway Anti-Malware Engine inspecte les fichiers et empêche leur téléchargement s'ils sont malveillants.
- **Intégration avec McAfee GTI :** McAfee GTI propose des flux de cyberveille en temps réel sur la réputation des fichiers, la réputation web et les catégories de sites web. Ces flux contribuent à assurer une protection efficace contre les dernières menaces, car MWG bloque les tentatives de connexion à des sites web malveillants connus ou à des sites utilisant des réseaux publicitaires malveillants. Outre ces produits McAfee, nous vous recommandons deux catégories de technologies de sécurité supplémentaires :
  - **Sécurité de la passerelle de messagerie :** La plupart des logiciels malveillants infiltrent les systèmes par le biais de pièces jointes à des e-mails. Un produit efficace de protection de la passerelle de messagerie, capable d'analyser toutes les pièces jointes, constitue dès lors un élément essentiel d'une défense à toute épreuve contre ce type d'attaque.
  - **Pare-feu :** La technologie de pare-feu est le fondement même de tout système de sécurité. Un pare-feu peut détecter de nombreuses menaces au niveau du périmètre avant qu'elles n'entrent dans le réseau approuvé. Les logiciels malveillants basés sur des scripts envahissent un système via des fichiers binaires statiques. Pour cette raison, nombre de ces attaques peuvent être arrêtées avant qu'elles n'affectent les systèmes situés dans le réseau approuvé.

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr