Présentation de solution

Bloquer les chevaux de Troie de type porte dérobée (backdoor)

L'outil d'administration à distance Adwind est un cheval de Troie de type porte dérobée (backdoor) écrit en langage Java, qui cible diverses plates-formes prenant en charge les fichiers Java. Adwind n'exploite aucune vulnérabilité. Dans la plupart des cas, pour qu'une infection réussisse, l'utilisateur doit exécuter le logiciel malveillant en double-cliquant sur le fichier .jar généralement distribué sous forme de pièce jointe, ou ouvrir un document Microsoft Word infecté. L'infection se propage si Java Runtime Environment est installé sur l'ordinateur de l'utilisateur. Une fois le fichier .jar malveillant exécuté sur le système cible, le malware s'installe silencieusement et se connecte à un serveur distant, via un port préconfiguré pour recevoir des commandes d'un attaquant distant et effectuer d'autres opérations illicites.

Bref historique

Adwind est une évolution de l'outil d'administration à distance Frutas. Frutas est un outil d'administration à distance Java découvert au début de l'année 2013. Il a été largement utilisé dans le cadre de campagnes de phishing menées contre des administrations et des sociétés financières, minières et de télécommunications de premier plan en Europe et en Asie.

Depuis le début du 1er trimestre 2015, McAfee® Labs a constaté une augmentation significative du nombre de soumissions des fichiers .jar identifiés en tant qu'Adwind.

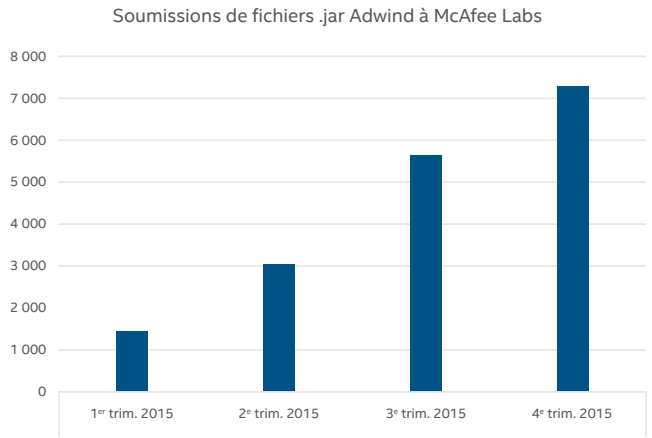

Figure 1. Le nombre de fichiers .jar Adwind envoyés à McAfee Labs est passé de 1 388 à 7 295 entre le 1er et le 4e trimestre 2015, soit une hausse de 426 %.

intel Security

Chaîne d'infection

Adwind se propage généralement au travers de campagnes de spam dont les pièces jointes contiennent des logiciels malveillants, de pages web altérées et de téléchargements à l'insu de l'utilisateur (drive-by download). Son mécanisme de distribution a évolué. Les premières campagnes de spam s'étalaient sur plusieurs jours, voire plusieurs semaines, et utilisaient le même objet d'e-mail ou le même nom de pièce jointe. Cette uniformité permettait aux éditeurs de solutions de sécurité de détecter et de neutraliser rapidement Adwind. Aujourd'hui, les campagnes de spam ont une durée réduite, les objets sont fréquemment modifiés et les pièces jointes sont élaborées avec soin, ce qui permet à Adwind d'échapper à la détection.

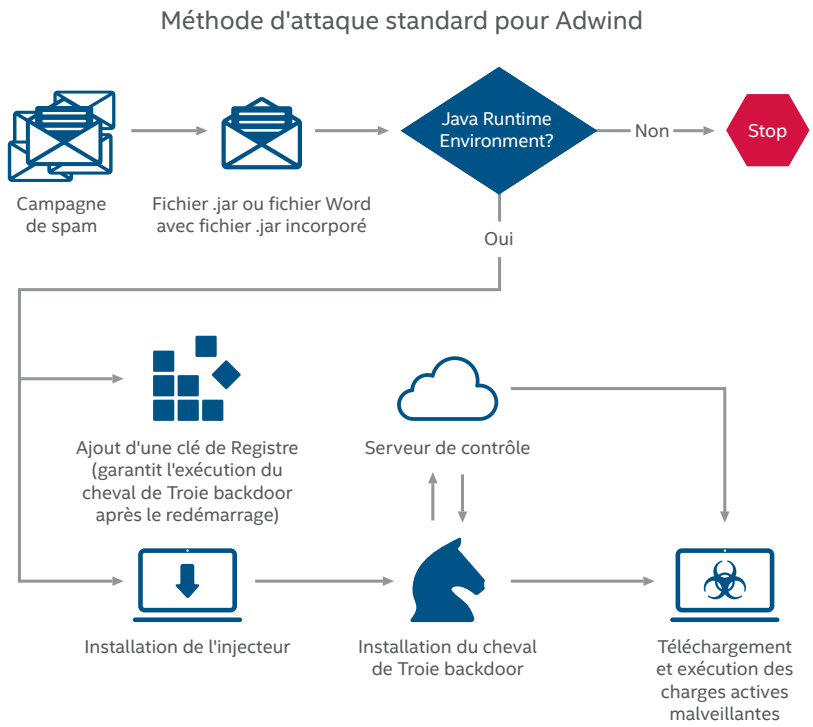

Figure 2. Chaîne d'infection d'Adwind

Nous avons constaté qu'après avoir infecté un système, Adwind peut enregistrer les frappes, modifier et supprimer des fichiers, télécharger et exécuter d'autres logiciels malveillants, créer des captures d'écran, accéder à la webcam du système, prendre le contrôle de la souris et du clavier, se mettre à jour automatiquement, etc.

Comment Intel Security peut vous aider à vous protéger contre Adwind et d'autres chevaux de Troie de type portée dérobée (backdoor)

Les technologies Intel Security peuvent vous aider à vous protéger contre les chevaux de Troie backdoor tels qu'Adwind. Voici quelques produits qui peuvent vous prémunir contre ce type d'attaque.

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** réduit considérablement les risques d'attaques menées à l'aide de chevaux de Troie de type porte dérobée (backdoor), grâce à la visibilité 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 Global Threat Intelligence** (McAfee GTI) ou des flux externes avec des informations locales sur les menaces, issues de données d'événements historiques et en temps réel que fournissent les solutions de sécurité des terminaux, de passerelle, etc.
- **Prévention d'exécution et actions correctives :** 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 se révèle 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 coupable 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 des informations sur les hachages de fichiers dangereux, de manière à immuniser l'environnement contre ces menaces connues grâce à la mise en œuvre des stratégies adéquates. Si l'un des indicateurs déclenche une alerte dans l'environnement, McAfee Threat Intelligence Exchange peut bloquer tous les processus et applications associés à cet indicateur de compromission.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense est une solution multiniveau de détection des logiciels malveillants qui combine divers moteurs d'inspection. Les moteurs 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 sur les objets suspects. Ainsi, la solution assure une protection contre les logiciels malveillants qui déposent initialement un fichier binaire sur les systèmes cibles.

- **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.
- **Détection basée sur la réputation :** Tire parti de 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 chevaux de Troie de type porte dérobée (backdoor) 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 Advanced Threat Defense 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 Advanced Threat Defense prend en charge des images personnalisées des systèmes d'exploitation Microsoft Windows XP (32 et 64 bits), Windows 7 (32 et 64 bits), Windows 8 (32 et 64 bits), Windows Server 2003, Windows Server 2008 (64 bits) et Android.

McAfee Network Security Platform

McAfee Network Security Platform est une solution de sécurité dont l'intelligence unique lui permet d'identifier et de bloquer des menaces sophistiquées sur le réseau. Grâce à diverses techniques avancées de détection et d'émulation, elle va au-delà de la simple mise en correspondance de modèles pour offrir une protection très performante contre les attaques furtives. Notre approche ouverte et intégrée de la gestion de la sécurité rationalise les opérations de sécurité en combinant les flux en temps réel McAfee GTI avec des données contextuelles riches sur les utilisateurs, les équipements et les applications. Cela permet ainsi une réponse rapide et précise aux attaques propagées par le réseau.

- **Défense sans signatures :** Les menaces avancées et inconnues telles que les logiciels malveillants furtifs, les menaces APT, les robots et les attaques « jour zéro » échappent souvent aux systèmes de défense basés sur les signatures. McAfee Network Security Platform combine plusieurs moteurs avancés qui ne nécessitent pas de signatures pour assurer la protection contre ces types de menaces. La détection sans signatures recourt à l'émulation pour analyser le comportement d'éléments tels que le contenu web, les fichiers PDF, les objets Flash et les scripts JavaScript quasiment en temps réel.
- **Endpoint Intelligence Agent :** McAfee Network Security Platform assure la mise en corrélation du trafic des terminaux, en temps réel et pour chaque flux. Endpoint Intelligence Agent allie l'analyse comportementale des flux de trafic réseau à plusieurs sources de cyberveille sur la réputation. Cette technologie tire parti de la cyberveille au niveau du réseau et de chaque hôte Windows pour identifier les relations entre les fichiers exécutables sur les terminaux et les flux de trafic réseau. Cette approche offre divers avantages. Ainsi, l'agent intègre des informations contextuelles détaillées sur les processus des attaques, bloque les communications malveillantes, prévient la propagation des logiciels malveillants avancés et, enfin, met en quarantaine et corrige les systèmes hôtes compromis.

McAfee Web Gateway
Les publicités malveillantes, les téléchargements à l'insu de l'utilisateur (drive-by) et les URL malveillantes incorporées à des e-mails de phishing ne sont que quelques-unes des méthodes d'attaque utilisées pour distribuer les chevaux de Troie backdoor. **McAfee Web Gateway** est un produit robuste qui optimise la protection de votre entreprise contre ce type de menaces.

- **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 une cyberveille en temps réel basée 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 McAfee Web Gateway bloque les tentatives de connexion à des sites web malveillants connus ou à des sites agissant en tant que serveurs de contrôle.

Outre ces produits Intel Security, nous vous recommandons une catégorie de technologies de sécurité supplémentaire.

- **Sécurité de la messagerie électronique :** La plupart des chevaux de Troie backdoor compromettent les systèmes par l'entremise d'une pièce jointe à un message. Dès lors, une stratégie de défense bien conçue contre ce type d'attaques doit prévoir une solution efficace pour sécuriser la passerelle de messagerie.

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