Présentation de solution

Protection contre les programmes potentiellement indésirables (PUP)

Les programmes potentiellement indésirables ou PUP (*Potentially Unwanted Programs*) sont abordés en détail dans le **Rapport de McAfee sur le paysage des menaces — Février 2015**. Toute application présentant un risque sous-jacent tangible pour l'utilisateur, aussi avantageuse soit-elle pour ce dernier, peut être assimilée à un programme potentiellement indésirable. Les applications n'informent généralement pas les utilisateurs du risque encouru. Contrairement aux chevaux de Troie, aux virus, aux rootkits et autres formes de malware, les programmes potentiellement indésirables n'ont généralement pas pour fonction de collecter les informations d'identification d'utilisateurs (médias sociaux, banque ou autres) ni d'altérer les fichiers système dans un but malveillant. Ceux-ci se situent dans une « zone grise » dans la mesure où, à côté du risque qu'ils posent, ils présentent souvent un intérêt pour l'utilisateur. Ils sont souvent difficiles à détecter et à classer.

Voici une liste de comportements courants des PUP :

- Modification non autorisée des paramètres système (configuration du navigateur, par exemple)
- Dissimulation d'un programme non sollicité au sein d'une application légitime
- Collecte secrète d'informations sur les utilisateurs, les habitudes de navigation et la configuration système
- Dissimulation de l'installation d'une application
- Désinstallation complexe
- Distribution par le biais de publicités déroutantes ou trompeuses

Les PUP peuvent prendre différentes formes :

- **Logiciels publicitaires (adware)** : distribuent des publicités principalement par le biais des navigateurs.
- **Craqueurs de mot de passe** : affichent les mots de passe secrets des applications.
- **Outils d'administration à distance (RAT,** *Remote Administration Tool***)** : surveillent les activités des utilisateurs sur les machines infectées ou permettent le contrôle à distance du système à l'insu de l'utilisateur ou sans son consentement.

intel Security

- **Générateurs de clés** : génèrent des clés de produits pour des applications légitimes.
- **Outils de piratage de navigateurs** : modifient la page d'accueil ou de recherche, les paramètres du navigateur, etc.
- **Outils de piratage** : applications autonomes pouvant faciliter les intrusions système ou les fuites de données stratégiques.
- **Proxys** : redirigent ou dissimulent des informations liées aux adresses IP.
- **Outils de suivi :** logiciels espions (*spyware*) ou enregistreurs de frappe qui enregistrent les frappes de l'utilisateur, journalisent ses communications personnelles, surveillent ses activités en ligne ou capturent des écrans à son insu.

Le tableau suivant présente les principales différences entre les PUP et les autres logiciels malveillants (chevaux de Troie, *ransomware*, robots et virus, par exemple) :

Techniques	Programme potentiellement indésirable (PUP)	Autre logiciel malveillant : cheval de Troie, virus, robot, etc.
Méthode d'installation	Procédure d'installation standard, parfois accompagnée d'un accord de licence. L'installation complète sur un système nécessite souvent l'aval et l'intervention de l'utilisateur.	Installation autonome sans aucune intervention de l'utilisateur. Ce type de logiciel opère pour l'essentiel de manière totalement indépendante.
Présentation	Associé à une application légitime et installé clandestinement en même temps que celle-ci.	Fichier autonome avec peu de composants supplémentaires. Ne se présente pas sous la forme d'un programme d'installation.
Désinstallation	Le package contient parfois un programme de désinstallation permettant sa suppression. La procédure de désinstallation est souvent complexe.	Les fichiers exécutables compliquent la suppression du logiciel malveillant en raison d'imbrications dans d'autres processus, *handles* ou identifiants de processus et d'autres liens complexes. Comme il ne s'agit pas de packages d'installation, ces fichiers n'apparaissent pas dans le Panneau de configuration.
Comportement	Affiche des publicités indésirables et des fenêtres au-dessus (*pop-up*) ou en dessous (*pop-under*) de la fenêtre active. Modifie les paramètres du navigateur, collecte des données sur l'utilisateur et le système ou permet le contrôle à distance du système à l'insu de l'utilisateur ou sans son consentement.	Dérobe des informations d'identification personnelle ou des données bancaires, modifie les fichiers système, rend le système inutilisable, réclame une rançon, etc.
Furtivité	Son comportement n'est généralement pas furtif.	Peut dissimuler des fichiers, des dossiers, des entrées de Registre et du trafic réseau.

De toutes les catégories de PUP, les logiciels publicitaires sont ceux qui ont le plus attiré l'attention des éditeurs de solutions de sécurité, non pas pour le dérangement qu'ils occasionnent mais pour la manière dont ils abusent la confiance. Les logiciels publicitaires ont peaufiné leurs tactiques et mettent en œuvre diverses techniques pour assurer leur persistance sur les systèmes infectés, dont les suivantes :

- Exécution d'un processus autonome dans la mémoire
- Fichiers DLL de type COM (Component Object Model) et non COM avec fonctions spécialement conçues pour l'application
- Clés de Registre d'objets d'aide à la navigation (BHO, Browser Helper Object)
- Fichiers DLL accrochés à des processus système
- Extensions et plug-ins de navigateur
- Services système enregistrés
- Composants de pilotes de périphérique exécutant des fonctions de contrôle des équipements
- Pilotes de filtre de bas niveau
- Chevaux de Troie distribués sous forme de charge active

La propagation des PUP se fait généralement en abusant la confiance d'utilisateurs innocents, ainsi qu'expliqué dans le **Rapport de McAfee sur le paysage des menaces — Novembre 2014**. Les techniques de distribution de PUP les plus courantes sont les suivantes :

- Exploitation malveillante et secrète d'applications légitimes
- Ingénierie sociale
- Vente de mentions J'aime Facebook
- Publication de messages frauduleux sur Facebook
- Piratage de Google AdSense
- Extensions et plug-ins de navigateur non prévus
- Installation forcée en même temps que des applications légitimes

Comment Intel Security peut vous aider à vous protéger contre les PUP

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. Il peut ainsi vous aider à protéger votre entreprise contre les PUP.

- **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. McAfee Application Control réduit votre exposition aux PUP en bloquant l'exécution des logiciels publicitaires connus.
- **Réputation des fichiers** — L'intégration à **McAfee Global Threat Intelligence** (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 faciliter l'établissement de listes blanches et à aider l'entreprise à identifier les applications connues pour être des PUP.
- **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 fixes tels que les terminaux de point de vente, qu'ils soient connectés ou non.

McAfee Web Gateway

Les publicités malveillantes, les téléchargements à l'insu de l'utilisateur (*drive-by*) et les URL malveillantes incorporées à des sites web légitimes ne sont que quelques-unes des méthodes d'attaque utilisées pour distribuer des programmes potentiellement indésirables. **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 filtre, en temps réel, le contenu malveillant du trafic web. 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 renseignements en temps réel sur la réputation des fichiers, la réputation web et les catégories de sites web. Ceux-ci 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 utilisant des réseaux publicitaires malveillants.

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence (McAfee GTI) est un service complet de renseignements sur les menaces, délivré en temps réel et basé dans le cloud, qui permet aux produits McAfee de bloquer les cybermenaces sur tous les vecteurs : fichiers, Web, messagerie électronique et réseau. Il assure une protection proactive contre les PUP grâce aux fonctionnalités suivantes :

- **Renseignements par corrélation des vecteurs** — Collecte et met en corrélation des données en provenance de tous les vecteurs de menaces principaux, dont les fichiers, le Web, la messagerie électronique et le réseau, afin de détecter les menaces combinées telles que les réseaux publicitaires distribuant des logiciels malveillants signés.
- **Plate-forme de renseignements complets sur les menaces** — Recueille des données sur les menaces au départ de millions de sondes sur les produits McAfee déployés par des clients tels que les solutions de protection des terminaux, de l'environnement web, de la messagerie électronique, sans oublier les systèmes de prévention des intrusions sur le réseau et les pare-feux.
- **Réputation des certificats** — Le système interroge les flux de données en temps réel qui renseignent les certificats dont la bonne ou mauvaise réputation est connue, dans le but de protéger votre entreprise contre des menaces telles que les logiciels malveillants signés qui peuvent être transmis par le truchement de réseaux publicitaires malveillants.
- **Security Connected** — McAfee GTI est intégré aux produits de sécurité McAfee pour fournir les informations les plus détaillées sur les menaces, la corrélation des données la plus précise et l'intégration aux produits la plus complète de façon à assurer une protection optimale contre les logiciels publicitaires.

McAfee SiteAdvisor® Enterprise

Ne pas se laisser distancer par le paysage des menaces en évolution perpétuelle constitue un défi de taille. En particulier lorsqu'il s'agit de protéger les utilisateurs en ligne contre des menaces telles que les PUP, sans pour autant imposer des stratégies trop restrictives qui gâchent l'expérience utilisateur.

- **Identification aisée de menaces telles que des sites web malveillants se présentant comme légitimes** — Fondé sur un système de classification intuitif avec codes de couleur, **McAfee SiteAdvisor Enterprise** offre une couche de protection supplémentaire au niveau du poste de travail. Il bloque les connexions vers les sites malveillants connus et informe les utilisateurs du danger.
- **Sécurité optimisée par McAfee GTI** — McAfee GTI procure des renseignements sur les menaces en temps réel à McAfee SiteAdvisor Enterprise, qui peut ainsi évaluer les sites web en s'appuyant sur les informations les plus récentes.

McAfee Threat Intelligence Exchange

Une plate-forme de renseignements capable de s'adapter aux besoins de votre environnement au fil du temps constitue un outil essentiel. **McAfee Threat Intelligence Exchange** réduit considérablement l'exposition à ces types d'attaques grâce à sa visibilité sur les menaces immédiates telles que les fichiers ou applications inconnus exécutés dans l'environnement.

- **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.

- **Réputation des certificats** — L'intégration à McAfee GTI protège votre entreprise en temps réel contre les attaques qui exploitent le code malveillant signé, en interrogeant les flux d'informations en temps réel sur la bonne ou mauvaise réputation des certificats. McAfee Threat Intelligence Exchange peut protéger vos terminaux contre les certificats malveillants au travers de stratégies gérées de manière centralisée, qui peuvent être déployées pour protéger à la fois les terminaux connectés et déconnectés.

McAfee VirusScan® Enterprise

McAfee VirusScan Enterprise assure la détection et la suppression des logiciels malveillants, dont les logiciels publicitaires, en toute simplicité. McAfee VirusScan Enterprise fait appel au moteur d'analyse primé de McAfee pour protéger vos fichiers contre les virus, les vers, les rootkits, les chevaux de Troie et autres menaces avancées.

- **Protection proactive contre les attaques** — Intègre une technologie antimalware avec fonction de prévention des intrusions pour vous protéger contre les exploits par débordement de mémoire tampon dirigés contre 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 des 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.

Il est compliqué de lutter contre les PUP qui cherchent à contourner le modèle de confiance traditionnel par l'adoption de comportements sournois et indésirables. La combinaison des recherches de pointe de McAfee Labs et de la technologie Intel Security peut vous aider à protéger votre entreprise contre ces PUP.

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