Présentation de solution

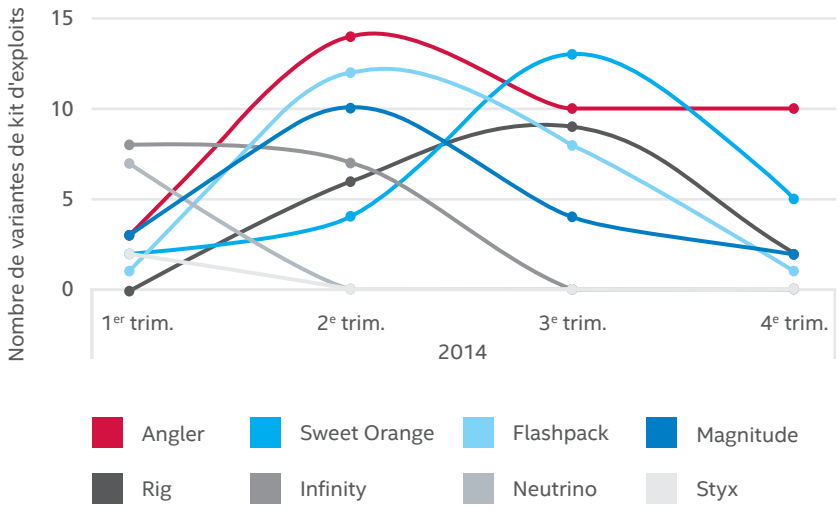
Mettre en échec le kit d'exploits Angler

Un kit d'exploits est un package logiciel commercialisé sur le marché noir, permettant d'élaborer facilement des attaques qui exploitent des vulnérabilités tant connues qu'inconnues (« jour zéro »). Ces ensembles d'outils exploitent des vulnérabilités côté client, ciblant généralement le navigateur web et les applications accessibles par celui-ci. Les kits d'exploits peuvent également enregistrer les statistiques d'infection et possèdent des fonctions de contrôle performantes.

Qu'est-ce que le kit d'exploits Angler ?

Angler est abordé en détail dans le **Rapport de McAfee sur le paysage des menaces — Février 2015**. Sa notoriété et sa prévalence se sont accrues au second semestre 2014 en raison de ses fonctionnalités particulièrement performantes. Citons par exemple l'infection sans fichier (injection de la charge active en mémoire), la détection des machines virtuelles et des produits de sécurité, ou encore sa capacité à distribuer un large éventail de charges actives — notamment des chevaux de Troie bancaires et de type porte dérobée (*backdoor*), des rootkits, des logiciels de demande de rançon (*ransomware*), CryptoLocker, etc. En outre, ce kit d'exploits s'utilise efficacement sans nécessiter de compétences techniques particulières et est disponible sur les marchés clandestins du Web :

Variantes parmi les kits d'exploits en 2014



Source : McAfee Labs, 2015

intel Security

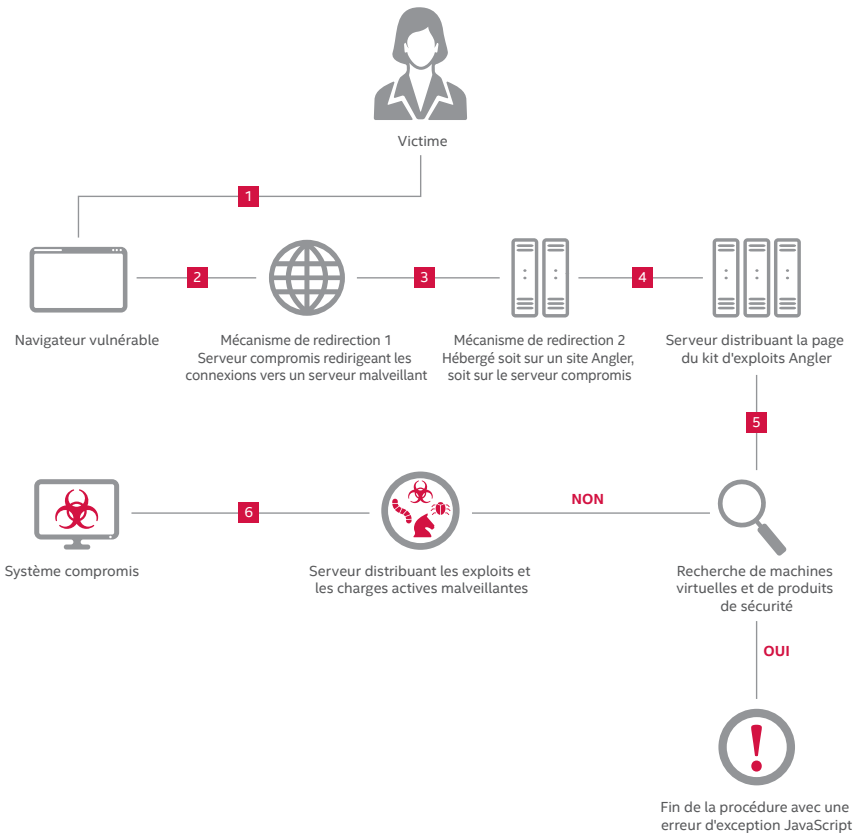
Angler modifie régulièrement ses comportements et ses charges actives afin d'échapper à la détection des produits de sécurité en dépit de son activité intense. Pour ce faire, il fait appel à plusieurs techniques de contournement :

- Il utilise deux niveaux de mécanismes de redirection avant d'atteindre la page de destination.
- Les serveurs web compromis qui hébergent la page de destination ne sont accessibles qu'une seule fois à partir d'une même adresse IP. Il est donc évident que les auteurs d'attaques surveillent activement les hôtes.
- Il détecte la présence de machines virtuelles et de produits de sécurité sur le système.
- Son code contient des appels parasites et destinés à brouiller les pistes pour que sa logique soit difficile à reconstituer.
- Il chiffre toutes les charges actives au moment du téléchargement et les déchiffre sur l'ordinateur compromis.
- Il recourt à l'infection sans fichier (déploiement direct de la charge active en mémoire).

L'infection des systèmes par Angler se déroule en plusieurs étapes :

- La victime accède à un serveur web compromis par l'intermédiaire d'un navigateur vulnérable.
- Le serveur web compromis redirige la connexion vers un serveur intermédiaire.
- Le serveur intermédiaire redirige à son tour la connexion vers un serveur web malveillant qui héberge la page de destination du kit d'exploits.
- La page de destination recherche ensuite la présence de plug-ins vulnérables (Java, Flash et Silverlight) ainsi que leurs informations de version.
- Si un navigateur ou plug-in vulnérable est détecté, le kit d'exploits distribue la charge active voulue et infecte le système.

Chaîne d'infection du kit d'exploits Angler



Protection contre le kit d'exploits Angler

Voici quelques mesures recommandées pour protéger les systèmes contre Angler :

- Faites appel à un fournisseur d'accès Internet attentif à la sécurité qui met en œuvre des procédures strictes en matière de lutte contre le spam et le phishing.
- Activez les mises à jour automatiques de vos systèmes d'exploitation ou téléchargez-les régulièrement afin que ceux-ci bénéficient en permanence des derniers patchs requis pour corriger leurs vulnérabilités connues. Installez les patchs d'autres développeurs de logiciels dès qu'ils sont disponibles. Doter son ordinateur de tous les patchs nécessaires et le protéger au moyen d'un pare-feu constitue la meilleure approche pour se prémunir contre les logiciels espions (*spyware*) et les chevaux de Troie.
- Soyez extrêmement prudent au moment d'ouvrir des pièces jointes. Configurez votre logiciel antivirus pour qu'il analyse automatiquement tous les fichiers joints aux e-mails et aux messages instantanés. Assurez-vous que l'ouverture des pièces jointes ne soit pas automatique dans vos programmes de messagerie, pas plus que l'affichage des images. Vérifiez par ailleurs que le volet d'aperçu est désactivé. N'ouvrez jamais des e-mails non sollicités ou des fichiers joints que vous n'attendez pas, même s'ils proviennent de personnes que vous connaissez.
- Méfiez-vous du spam, susceptible de masquer des tentatives de phishing. Ne cliquez pas sur les liens figurant dans les e-mails ou les messages instantanés.
- Utilisez un plug-in de navigateur pour bloquer l'exécution des scripts et des balises iframe.

Comment Intel Security peut vous aider à vous protéger contre le kit d'exploits Angler

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 de confiance ne sont que quelques-unes des méthodes d'attaque utilisées pour distribuer le kit d'exploits Angler. **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 assurent une protection 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 Global Threat Intelligence (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 VirusScan® Enterprise

Grâce à **McAfee VirusScan Enterprise**, la détection et l'éradication des logiciels malveillants tels que ceux diffusés par Angler sont d'une grande 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 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 exploits tirant parti du débordement de mémoire tampon et visant 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.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense est une solution de détection des logiciels malveillants multiniveau 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 garantit une protection contre les kits d'exploits les plus répandus, dont Angler, et les logiciels malveillants qu'ils déploient.

- **Détection basée sur les signatures** — Débusque les virus, les vers, les logiciels espions, 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, notamment des signatures pour Angler et ses variantes.
- **Détection basée sur la réputation** — Tire parti du réseau 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. 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 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 (32/64 bits), Windows XP, Windows Server 2003 et Windows Server 2008 (64 bits), ainsi qu'Android.

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 avec McAfee GTI** — 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 Threat Intelligence Exchange

Une plate-forme de renseignements capable de s'adapter aux besoins de votre 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 kits d'exploits, grâce à la visibilité offerte sur les menaces immédiates, notamment les applications ou fichiers 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.
- **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** — 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.

La prolifération de kits d'exploits simples d'emploi tels qu'Angler nous rappelle une dure réalité : le paysage des menaces est en constante évolution. Les technologies Intel Security peuvent aider votre entreprise à se protéger de façon proactive contre les menaces comme Angler, tant au niveau des terminaux que du réseau.

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