Présentation de solution

Protection contre les exploits Adobe Flash

La plateforme logicielle et multimédia Adobe Flash est une solution très prisée pour la distribution de contenu web enrichi tel que des jeux, des sites web, des applications et bien plus encore. Malheureusement, sa popularité en fait une cible de choix pour les cybercriminels, qui exploitent sans relâche les nouvelles vulnérabilités non corrigées dans le but de compromettre des utilisateurs à leur insu.

Prévalence des exploits Adobe Flash

Les exploits Flash sont examinés en détail dans le ***Rapport de McAfee Labs sur le paysage des menaces de mai 2015***. Le nombre d'exploits conçus pour Flash a commencé à grimper en flèche au cours du dernier trimestre 2014. Les vulnérabilités de Flash captivent l'attention des auteurs d'exploits. McAfee Labs attribue le phénomène à une combinaison de facteurs : ces vulnérabilités sont toujours plus nombreuses ; des méthodes innovantes pour les exploiter voient le jour ; les utilisateurs mettent du temps à appliquer leurs correctifs ; les terminaux mobiles capables de lire les fichiers .swf de Flash foisonnent et les exploits Flash sont difficiles à détecter.

Parmi les kits de distribution d'exploits Flash, Angler est désormais le plus répandu. Ce kit d'une efficacité redoutable, abordé en détail dans le ***Rapport de McAfee Labs sur le paysage des menaces de février 2015***, est une boîte à outils prête à l'emploi et facile à utiliser, qui peut distribuer une large palette de charges actives grâce à l'exploitation de vulnérabilités.

Protection contre les exploits Flash

Voici quelques bonnes pratiques et procédures permettant de se protéger contre les exploits Flash :

- Activez les mises à jour automatiques de vos systèmes d'exploitation ou téléchargez-les régulièrement afin que ceux-ci bénéficient en permanence des derniers correctifs requis de leurs vulnérabilités connues.
- Configurez le logiciel antivirus de telle sorte qu'il bloque les pièces jointes portant l'extension .swf.
- Configurez les paramètres de sécurité du navigateur à un niveau moyen ou élevé.
- Utilisez un plug-in de navigateur pour bloquer l'exécution des scripts et des balises iFrame.
- N'installez pas de plug-ins de navigateur non approuvés.
- Soyez très prudent lorsque vous ouvrez des pièces jointes, surtout celles portant l'extension .swf.
- 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 des escroqueries par phishing utilisant le spam. Ne cliquez pas sur les liens figurant dans les e-mails ou les messages instantanés.

intel Security

- Saisissez ou copiez les URL dans la barre d'adresse du navigateur et vérifiez l'adresse au lieu de cliquer sur des publicités web.
- N'exécutez pas des vidéos Flash hébergées sur des sites non approuvés.

Comment Intel Security peut vous aider à vous protéger contre cette menace

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 qui tirent parti des exploits Flash. **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 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 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. Assurer à votre entreprise une protection optimale contre les applications vulnérables telles que les versions obsolètes de Flash est essentiel pour lutter contre la tendance actuelle à la multiplication des exploits Flash.

- **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 exploits Flash en veillant à ce que les versions non corrigées de Flash ne puissent pas s'exécuter dans votre environnement.
- **Réputation des fichiers —** L'intégration à 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 aider l'entreprise à identifier les vulnérabilités ainsi que les attaques émanant d'applications qui peuvent avoir été modifiées.
- **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 à fonction fixe tels que les terminaux de point de vente, qu'ils soient connectés ou non.

McAfee Vulnerability Manager

McAfee Vulnerability Manager aide votre entreprise à comprendre l'exposition qui peut résulter de la présence de versions obsolètes de Flash dans votre environnement et à prendre les mesures qui s'imposent pour la réduire efficacement.

- **Analyse complète des vulnérabilités —** McAfee Vulnerability Manager est un produit autonome hautement évolutif pour la découverte des hôtes, la gestion des actifs, l'évaluation des vulnérabilités et la génération de rapports sur tous les équipements réseau. Il peut évaluer l'exposition de votre environnement aux exploits Flash en recherchant les systèmes exécutant des versions vulnérables de Flash.

- **Rapports et corrections flexibles —** McAfee Vulnerability Manager et **McAfee Asset Manager** fonctionnent de concert pour assurer une gestion et une surveillance automatisées de l'analyse, de la correction, de la mise en œuvre et de la génération de rapports. Vous évitez ainsi les exercices d'alerte et les processus ponctuels fastidieux, vous éliminez les erreurs et vous protégez efficacement plus de systèmes.
- **Connaissance de votre niveau de risque —** McAfee Asset Manager indique à l'entreprise les systèmes vulnérables aux exploits Flash en mettant en corrélation des analyses de vulnérabilités avec des analyses de découverte des hôtes. L'identification en temps réel des systèmes précis qui exécutent des versions vulnérables de Flash permet de perdre moins de temps en spéculations et d'en consacrer davantage aux mesures correctives.

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 qui exploitent des vulnérabilités Flash dans l'environnement de votre entreprise.

- **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

Avec **McAfee VirusScan® Enterprise**, il est facile de détecter et d'éliminer les logiciels malveillants qui exploitent les vulnérabilités de Flash pour infiltrer votre environnement. 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 fonction de prévention des intrusions pour offrir une protection contre les exploits 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 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 exploits Flash et autres grâce aux fonctionnalités suivantes :

- **Renseignements par corrélation des vecteurs —** Collecte et corrèle les données relatives aux principaux vecteurs de menaces (fichiers, Web, messagerie et réseau) pour détecter les menaces combinées.
- **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.
- **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 exploits Flash.

McAfee VirusScan Mobile

McAfee VirusScan Mobile est un système de protection contre les logiciels malveillants (*malware*) qui analyse et assainit les données mobiles pour empêcher leur corruption par des virus, des chevaux de Troie et tout autre code malveillant. McAfee VirusScan Mobile assure la sécurité de vos terminaux mobiles en ciblant les points d'exposition les plus critiques, notamment les e-mails entrants et sortants, les SMS, les pièces jointes et les téléchargements Internet.

- Détection des menaces en temps réel — Bloquez les logiciels malveillants présents dans les e-mails, les SMS et les pièces jointes sans délai perceptible. McAfee VirusScan Mobile recherche tout un éventail de menaces en moins de 200 millisecondes, assurant ainsi une protection complète et automatique des smartphones.

La multiplication des vulnérabilités de Flash exploitées par les auteurs de logiciels malveillants ne montre aucun signe de ralentissement. Les technologies Intel Security peuvent aider votre entreprise à se protéger de manière proactive contre les menaces visant à exploiter ces vulnérabilités.

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