Présentation de solution

Mesures de protection contre les logiciels malveillants diffusés par macro

Le ***Rapport de McAfee® Labs sur le paysage des menaces — Novembre 2015*** s'intéresse de près aux logiciels malveillants diffusés par macro. Reliques des années 90, ceux-ci renaissent de leurs cendres en raison de l'utilisation intensive des macros par les entreprises et de la sophistication accrue des attaques d'ingénierie sociale qui propagent de nouveaux malwares encore plus furtifs par le biais des macros. Une macro est un raccourci permettant d'automatiser une tâche fréquemment exécutée. Il s'agit d'un segment de code incorporé dans un document, le plus souvent un document Microsoft Office, généralement écrit dans le langage de programmation VBA (Visual Basic for Applications). Lorsqu'une macro est enregistrée, elle génère en réalité un programme en VBA. Pour contrer les logiciels malveillants diffusés par macro, Microsoft a conçu une étape d'activation des macros, avec une procédure d'autorisation qui sert de vérification. Microsoft Office désactive désormais toutes les macros par défaut de sorte qu'elles ne puissent pas s'exécuter sans l'autorisation de l'utilisateur. Cette intervention a tempéré les ardeurs des auteurs de logiciels malveillants diffusés par macro, et l'influence des macros malveillantes a fini par décliner. Cependant, au cours des douze derniers mois, les cyberpirates ont eu recours à de nouvelles macros malveillantes plus furtives utilisées dans le cadre d'attaques d'ingénierie sociale pour cibler les entreprises de façon persistante. Le nombre d'échantillons de logiciels malveillants diffusés par macro est à son plus haut niveau depuis six ans.

Les cyberpirates qui ont recours aux macros malveillantes à l'heure actuelle exploitent principalement les pièces jointes aux messages de phishing, ainsi que les campagnes de spam, les pages web compromises et les téléchargements involontaires pour distribuer leur malware. Ces techniques sont aujourd'hui bien plus sophistiquées qu'elles ne l'étaient dans les années 90, époque où sont apparus les premiers logiciels malveillants diffusés par macro. Les utilisateurs éprouvent de plus en plus de difficultés à identifier ces campagnes du fait qu'elles sont ciblées, de courte durée, et contiennent des pièces jointes soigneusement élaborées pour échapper à la détection.

intel Security

Voici quelques stratégies et procédures recommandées pour se protéger contre les attaques de logiciels malveillants diffusés par macro :

- Activez les mises à jour automatiques de vos systèmes d'exploitation ou téléchargez-les régulièrement afin de bénéficier en permanence des derniers correctifs pour les vulnérabilités connues.
- Utilisez une suite Microsoft Office à jour pour bénéficier d'une meilleure protection contre ces types d'attaques.
- Assurez-vous que le paramètre de sécurité des macros par défaut est défini sur Élevé sur tous les produits Microsoft Office.
- Configurez votre logiciel antimalware pour qu'il analyse automatiquement tous les fichiers joints aux e-mails et aux messages instantanés. Vérifiez que l'ouverture des pièces jointes n'est pas automatique dans vos programmes de messagerie, pas plus que l'affichage des images. Assurez-vous par ailleurs que le volet d'aperçu est désactivé.
- Configurez les paramètres de sécurité du navigateur à un niveau moyen ou élevé.
- Soyez très prudent lorsque vous ouvrez des pièces jointes, surtout celles portant l'extension .doc ou .xls.
- 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.
- Établissez une surveillance réseau permettant d'identifier les requêtes ping inattendues envoyées par les ordinateurs internes aux adresses IP telles que 1.3.1.2 ou 2.2.1.1.
- Sachez que les reçus ou les documents de facturation ne nécessitent généralement pas des macros.
- Soyez prudent lorsque vous manipulez des documents vides qui invitent les utilisateurs à activer les macros pour afficher le contenu du document.

Comment Intel Security peut vous aider à vous protéger contre les logiciels malveillants diffusés par macro

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 sont quelques-unes des principales méthodes d'attaque utilisées pour distribuer les logiciels malveillants diffusés par macro. **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 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 utilisant des réseaux publicitaires malveillants.

McAfee VirusScan® Enterprise

McAfee VirusScan Enterprise assure la détection et la suppression en toute simplicité des logiciels malveillants diffusés par macro. McAfee VirusScan Enterprise fait appel au moteur d'analyse primé de McAfee Labs pour protéger vos fichiers contre les virus, les vers, les rootkits, les chevaux de Troie et d'autres menaces avancées. Renforcez la protection de votre entreprise grâce aux multiples fonctions de McAfee VirusScan Enterprise, dont le blocage de ports, 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.

- **Protection proactive contre les attaques** — Intègre une technologie antimalware avec prévention des intrusions pour offrir une protection contre les exploits tirant parti du débordement de mémoire tampon et visant les vulnérabilités des applications Microsoft.
- **Performances inégalées dans la détection et la neutralisation des logiciels malveillants** — Protège contre des 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 cyberveille sur les menaces la plus complète du marché.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense est une solution multiniveau de détection des logiciels malveillants qui combine divers moteurs d'inspection. Grâce à plusieurs moteurs appliquant une 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 non seulement détecte les documents qui exploitent les macros pour diffuser des logiciels malveillants, mais assure également la détection et la protection contre le malware qu'ils téléchargent après leur exécution.

- **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.
- **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 logiciels malveillants diffusés par macro 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 les logiciels malveillants auxquels elles ont affaire.

- **Analyse dynamique dans un environnement sandbox** — En présence d'un fichier dont les moteurs d'inspection ci-dessus 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 Windows XP SP2 et SP3, Windows 7 (32 et 64 bits), Windows 8 (32 et 64 bits), Windows Server 2003, Windows Server 2008 (64 bits) ainsi qu'Android.

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 logiciels malveillants diffusés par macro, grâce à la visibilité qu'il offre 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 informations locales sur les menaces, issues de données d'événements historiques et en temps réel fournies par les solutions de sécurité des terminaux, de passerelle, etc.
- **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 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.

Outre ces produits Intel Security, nous recommandons deux autres technologies de sécurité.

- **Sécurité de la passerelle de messagerie** — La plupart des logiciels malveillants diffusés par macro 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.
- **Pare-feu** — Une technologie de pare-feu performante est la pierre angulaire de tout système de sécurité. Un pare-feu peut détecter de nombreuses menaces au niveau du périmètre, avant qu'elles n'accèdent au réseau.

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