Présentation de solution

Échec et mat aux logiciels de demande de rançon : ne laissez pas vos données se faire prendre en otage

Les logiciels de demande de rançon (*ransomware*) sont des logiciels malveillants qui ont recours au chiffrement asymétrique pour prendre en otage les données d'une victime. Le chiffrement asymétrique (public-privé) est une technique cryptographique utilisant une paire de clés pour chiffrer et déchiffrer un fichier. La paire de clés publique et privée est générée de façon unique par le pirate à l'intention de la victime, la clé privée servant à déchiffrer les fichiers stockés sur le serveur du pirate. Ce dernier communique la clé privée à la victime après paiement de la rançon, bien que ce ne soit pas toujours le cas, comme nous avons pu le constater lors de récentes campagnes de demande de rançon. Sans accès à la clé privée, il est pratiquement impossible de déchiffrer les fichiers pris en otage.

Gros plan sur les logiciels de demande de rançon

Pour une analyse technique approfondie des logiciels de demande de rançon, lisez le ***Rapport de McAfee Labs sur le paysage des menaces de mai 2015***. Dans le *Rapport de McAfee Labs sur le paysage des menaces de novembre 2014*, nous avions prédit l'apparition de neuf grandes menaces en 2015. À propos des logiciels de demande de rançon, McAfee Labs disait à l'époque qu'ils « connaîtraient une évolution en termes de modes de propagation, de chiffrement et de cibles visées. » Peu de temps après, ces logiciels ont effectivement enregistré une hausse considérable, accompagnée de l'émergence de nouvelles familles, telles que TeslaCrypt, et de nouvelles variantes de familles existantes, notamment CTB-Locker, CryptoWall et TorrentLocker.

intel Security

La plupart des campagnes de demande de rançon commencent par une attaque de phishing. Au fil du temps, elles ont gagné en sophistication et sont aujourd'hui soigneusement adaptées aux particularités régionales des victimes prises pour cible.

Par ailleurs, de nouvelles technologies ont été adaptées pour renforcer l'efficacité des logiciels de demande de rançon :

- **Monnaie virtuelle —** En utilisant la **monnaie virtuelle** comme moyen de paiement d'une rançon, les pirates évitent le système bancaire traditionnel et le traçage des virements.
- **Réseau Tor —** Grâce au **réseau Tor**, les cybercriminels peuvent plus facilement dissimuler l'emplacement de leur serveur de contrôle, qui stocke les clés privées des victimes. Tor permet de maintenir l'infrastructure criminelle en place pendant longtemps, voire de louer l'infrastructure à d'autres pirates afin qu'ils puissent lancer des campagnes affiliées.
- **Transition vers les plates-formes mobiles —** En juin 2014, les chercheurs ont découvert la première famille de ransomware chiffrant des données sur Android[1]. Pletor utilise le chiffrement AES, verrouille les données sur la carte mémoire du téléphone et utilise Tor, le service SMS ou HTTP pour communiquer avec les cyberpirates.
- **Ciblage des périphériques de stockage en masse —** En août 2014, Synolocker a commencé à cibler les boîtiers et racks NAS de Synology[2]. Le logiciel malveillant exploite une vulnérabilité présente dans les versions non corrigées des serveurs NAS pour chiffrer à distance toutes les données des serveurs à l'aide de clés RSA de 256 ou 2 048 bits.

Protection contre les logiciels de demande de rançon

Voici quelques bonnes pratiques et stratégies pour renforcer votre protection et celle de votre entreprise contre la menace posée par les logiciels de demande de rançon.

- **Informez régulièrement vos utilisateurs.** C'est nécessaire et même crucial dans la mesure où la plupart des attaques par logiciel de demande de rançon débutent par l'envoi d'e-mails de phishing. Les statistiques prouvent que, sur dix e-mails envoyés par les auteurs d'attaques, au moins un fera mouche. N'ouvrez pas des e-mails et des pièces jointes si leur expéditeur vous est inconnu ou sans avoir vérifié son identité.
- **Maintenez les patchs système à jour.** De nombreuses vulnérabilités exploitées par les logiciels de demande de rançon peuvent être corrigées. Installez les derniers correctifs disponibles pour les systèmes d'exploitation, Java, Adobe Reader, Flash et les différentes applications. Mettez en place une procédure de déploiement des patchs et vérifiez que les correctifs requis ont été correctement appliqués.
- **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. Vérifiez que l'ouverture des pièces jointes ne soit 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. 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.

Comment Intel Security peut vous aider à vous protéger contre les logiciels de demande de rançon

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 les logiciels de demande de rançon. **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. 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 Email Gateway

Pouvoir déterminer si le courrier dans les boîtes de réception des employés est inoffensif ou s'il s'agit d'une attaque de phishing cherchant à distribuer un ransomware constitue une préoccupation importante des entreprises. **McAfee Email Gateway** possède plusieurs fonctionnalités capables de vous protéger contre ces types d'attaques de phishing toujours plus sophistiquées.

- **ClickProtect —** Élimine les menaces transmises par des URL incorporées dans les e-mails en les analysant au moment où l'utilisateur clique dessus. L'inspection comprend un contrôle de la réputation des URL et une émulation proactive assurée par McAfee Gateway Anti-Malware Engine.
- **Intégration avec McAfee Advanced Threat Defense —** Détecte les logiciels malveillants sophistiqués et difficiles à identifier grâce à l'analyse statique approfondie du code et à l'analyse dynamique appliquées aux fichiers suspects joints aux e-mails. Cette méthode permet de bloquer les fichiers malveillants avant qu'ils ne puissent atteindre la boîte de réception.
- **Intégration avec McAfee GTI —** La combinaison des informations réseau locales et des données sur la réputation fournies par McAfee Global Threat Intelligence permet d'offrir la protection la plus complète contre les menaces entrantes, le spam et les logiciels malveillants.

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense est une solution de détection des logiciels malveillants multiniveau qui combine plusieurs moteurs d'inspection. Ces derniers 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 vous protège contre les logiciels de demande de rançon les plus répandus, à savoir CTB-Locker, CryptoWall et bien d'autres.

- **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, qui compte actuellement plus de 150 millions de signatures, notamment des signatures pour CTB-Locker, CryptoWall et leurs variantes.
- **Détection basée sur la réputation —** Tire parti du service 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. 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 —** 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 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 exécutés dans l'environnement. Le blocage de fichiers exécutables inconnus ou nouveaux garantit une protection proactive contre les logiciels de demande de rançon.

- **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

McAfee VirusScan® Enterprise assure la détection et le blocage des logiciels de demande de rançon en toute simplicité. McAfee VirusScan Enterprise fait appel au moteur d'analyse primé de McAfee pour protéger les 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 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 renseignements sur les menaces la plus complète du marché.

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 complète des protocoles, l'analyse basée sur la réputation, l'analyse du comportement et l'analyse des logiciels malveillants avancés, pour détecter et prévenir les attaques, dont les logiciels de demande de rançon tentant de communiquer via les protocoles réseau, tels que Tor, IRC et d'autres.

- **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.

Empêcher que les précieuses données de votre entreprise ne soient prises en otage n'est pas une sinécure, surtout face à la hausse constante des logiciels de demande de rançon en tant que vecteur d'attaque. Les technologies Intel Security peuvent aider votre entreprise à se protéger de façon proactive contre les menaces, telles que les logiciels de demande de rançon, tant au niveau des terminaux que du réseau.

1. **https://threatpost.com/android-ransomware-first-to-encrypt-data-on-mobile-devices/106535**
2. **http://forum.synology.com/enu/viewtopic.php?f=108&t=88770**

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