Présentation de solution

Logiciels légitimes infectés par des chevaux de Troie

Prévention des infections et blocage de la propagation grâce aux solutions Intel® Security

Les mécanismes de distribution de logiciels via Internet sont couramment utilisés comme vecteurs d'attaque par virus ou logiciel malveillant. Depuis les premiers binders malveillants identifiés il y dix ans jusqu'à la diffusion sophistiquée actuelle de logiciels légitimes infectés par des chevaux de Troie, avant ou pendant la phase de distribution, l'évolution est considérable.

Cela étant, quel que soit le degré de sophistication d'un cheval de Troie, le mode opératoire reste le même :

- Transformation en logiciel malveillant : insertion de code malveillant dans une application distribuable
- Distribution : transmission du logiciel infecté à la cible, sans détection
- Exploitation : activation du code du cheval de Troie, de façon à éviter la détection
- Installation : persistance et tentative de déplacement latéral du code malveillant dans le système

La toute dernière technique d'attaque repose sur un mécanisme sophistiqué qui consiste à injecter du code dans un logiciel légitime à la volée, au moment même où il est téléchargé, de sorte que l'infection passe inaperçue. Le principe de cette attaque est de fusionner le code malveillant à l'application originale.

Cette technique d'attaque peut recourir à deux composants pour trouver un point d'entrée dans la cible : un processus d'écoute, qui intercepte et modifie la demande de téléchargement HTTP, et un binder (programme de liaison), qui infecte et distribue les fichiers binaires.

Certains algorithmes actuels déploient même des routines d'infection par logiciel malveillant et des attaques par redirection réseau sans altérer le code de l'application. Cela ouvre grand la porte aux publicités et logiciels à code source libre infectés, susceptibles de contenir des exécutables avec signature incorporée. L'attaque réussit si la signature n'est pas vérifiée automatiquement et intégralement avant toute tentative d'exécution initiale.

Une fois que l'application infectée par cheval de Troie est lancée au niveau de la cible, un processus binder crée son propre fichier pour générer des exécutables incorporés supplémentaires. Tout le code injecté y est reconstruit en vue d'une exécution future, contournant ainsi tous les contrôles de sécurité. Comme l'application d'origine reste intacte, le logiciel malveillant peut passer inaperçu, quel que soit son fichier d'attachement et sa signature.

intel Security

Stratégies et procédures

Les meilleures pratiques de cybersécurité d'Intel Security recommandent l'adoption de stratégies générales de prévention des menaces, tant pour les réseaux que les terminaux :

- En cas de connexion à un réseau non approuvé, il est préférable d'utiliser un réseau privé virtuel (VPN). Il est recommandé aux administrateurs de maintenir leurs logiciels de sécurité à jour et de se fier à des indicateurs de fiabilité sûrs, plutôt qu'à ceux susceptibles d'avoir été falsifiés lors d'une attaque. Les applications doivent être signées et vérifiées à l'aide de chaînes de confiance. Les investigations numériques doivent inclure des hachages de mise en corrélation avec des sources fiables.
- Les logiciels de sécurité doivent pouvoir fournir des analyses dynamiques capables d'identifier les actions anormales, quelle que soit l'inspection binaire initiale, car les analyses statiques ont leurs limites. La surveillance des comportements, la réputation web et IP, l'analyse de mémoire et le confinement d'applications sont autant d'autres composants utiles au sein d'une solution de sécurité complète.
- Si vous téléchargez des applications directement auprès de fournisseurs, vous devez utiliser des connexions sécurisées et vous assurer que tous les codes sont signés. Cela réduira considérablement votre exposition aux attaques de type man-in-the-middle. En outre, les éditeurs de logiciels doivent veiller à joindre une auto-évaluation à leurs applications, à effectuer des audits de code réguliers, à utiliser des outils d'analyse de code statique et à se faire évaluer par leurs pairs. Il est toujours utile de disposer d'un référentiel central d'applications d'entreprise approuvées et d'autoriser uniquement le téléchargement des programmes d'installation fiables répertoriés dans ce référentiel.
- Les logiciels antimalware doivent être configurés de sorte à pouvoir déceler la présence de binders.
- Les applications de prévention et de détection des intrusions sur l'hôte doivent être utilisées pour inspecter les paquets et identifier les charges actives.
- Utilisez uniquement des architectures de virtualisation fiables combinées à une segmentation réseau adéquate. En effet, ces architectures ont recours à un processus de démarrage sûr et vérifiable. Une bonne segmentation réseau permet quant à elle de surveiller le trafic et d'isoler les applications en cas de compromission réussie. Cette combinaison assure en outre une protection contre le déplacement latéral des logiciels malveillants.
- Surveillez le trafic sortant, car celui-ci peut renfermer des logiciels malveillants, eux-mêmes transmis par des logiciels légitimes infectés par des chevaux de Troie. En effet, certaines machines infectées peuvent se voir davantage exposées aux menaces par leur trafic en direction d'Internet.

Intel Security

Les solutions Intel Security permettent d'identifier les logiciels légitimes infectés par des chevaux de Troie, de détecter et de bloquer les logiciels malveillants incorporés, de déceler les compromissions et d'intervenir immédiatement :

McAfee VirusScan® Enterprise 8.8 ou McAfee Endpoint Security 10

- Maintenez les fichiers DAT à jour.
- Assurez-vous que McAfee Global Threat Intelligence (McAfee GTI) est activé, car ce système reconnaît plus de 600 millions de signatures de logiciels malveillants uniques.

- Développez des règles de protection de l'accès pour bloquer l'installation et les charges actives des logiciels malveillants.
  - Reportez-vous aux articles de la base de connaissances consacrés aux règles de protection de l'accès : KB81095 et KB54812.
  - Reportez-vous aux meilleures pratiques de configuration de McAfee VirusScan Enterprise 8.8 : PD22940.
  - Reportez-vous aux meilleures pratiques de configuration de McAfee Endpoint Security : KB86704.

McAfee Host Intrusion Prevention

- La solution McAfee Host Intrusion Prevention peut empêcher la propagation des logiciels malveillants. Par l'utilisation de signatures IPS personnalisées, vous pouvez créer des règles empêchant les opérations sur fichiers (création, écriture, exécution, lecture, etc.) générées par les logiciels malveillants.
- Activez la signature 3894 de Host Intrusion Prevention, Access Protection—Prevent svchost.exe executing non-Windows executables (Protection à l'accès - Empêcher le lancement de fichiers exécutables non-Windows par svchost).
- Activez les signatures 6010 et 6011 de Host Intrusion Prevention pour bloquer immédiatement les injections.
- Deux types de sous-règles permettent cela :

1. Créez une signature IPS personnalisée à l'aide du moteur Files et d'une sous-règle répondant aux critères suivants :
   - Name: <Insérer le nom>
   - Rule type: Files
   - Operations: Create, Execute, Read, Write
   - Parameters: Include - Files - <chemin d'accès/nom de fichier du logiciel malveillant>
     - Le nom de fichier doit inclure un chemin d'accès. Pour remplacer le chemin d'accès par un caractère générique, insérez « **\ » avant le nom du fichier, et pour remplacer la lettre du lecteur, insérez « ?:\ » (par exemple « **\nom_de_fichier.exe » ou « ?:\nom_de_fichier.exe »).
     - Le paramètre « Files » ne prend pas en charge les hachages MD5 ; uniquement le format chemin d'accès/nom de fichier.
     - Vous pouvez également indiquer le type de lecteur si vous souhaitez limiter le chemin d'accès à un lecteur spécifique (par exemple disque dur, CD-ROM, USB, réseau, disquette).
   - Executables: Ce critère peut rester vide, sauf si vous souhaitez limiter la signature à des processus spécifiques qui exécutent l'opération sur fichier (par exemple explorer.exe, cmd.exe, etc.).
2. Créez une signature IPS personnalisée à l'aide du moteur Program et d'une sous-règle répondant aux critères suivants :
   - Name: <insérer le nom>
   - Rule type: Program
   - Operations: Run target executable
   - Parameters: <laisser vide>
   - Executables: Ce critère peut rester vide, sauf si vous souhaitez limiter la signature à un processus spécifique comme l'exécutable source (par exemple pour empêcher explorer.exe d'exécuter un fichier Target Executable tel que notepad.exe).

- Target Executables: Définissez les propriétés du fichier exécutable dont vous souhaitez empêcher l'exécution (par exemple si vous souhaitez bloquer l'exécution de notepad.exe, indiquez le chemin d'accès/nom du fichier exécutable). Vous pouvez définir l'exécutable à l'aide d'un ou de plusieurs critères (description du fichier, nom du fichier, empreinte, signataire).

McAfee SiteAdvisor® Enterprise ou McAfee Web Protection

Utilisez les informations sur la réputation des sites web pour signaler aux utilisateurs les sites distribuant des logiciels infectés par des chevaux de Troie.

McAfee Threat Intelligence Exchange et McAfee Advanced Threat Defense

- Configuration des stratégies Threat Intelligence Exchange :
  - Commencez en mode d'observation. Lorsque des processus suspects sont identifiés sur des terminaux, utilisez des marqueurs système pour appliquer les stratégies de mise en œuvre de Threat Intelligence Exchange.
  - Nettoyez au niveau « Known malicious » (Malveillant connu).
  - Bloquez au niveau « Most-likely malicious » (Très probablement malveillant). (Un blocage au niveau « Unknown » (Inconnu) offrirait une meilleure protection mais peut également alourdir la charge administrative initiale.)
  - Configurez l'option « Submit files to McAfee Advanced Threat Defense » (Envoyer les fichiers à McAfee Advanced Threat Defense) aux niveaux « Unknown » (Inconnu) et inférieurs.
  - Stratégie Threat Intelligence Exchange Server : Acceptez les réputations Advanced Threat Defense pour les fichiers qui n'ont jamais été rencontrés par McAfee Threat Intelligence Exchange.
- Intervention manuelle dans Threat Intelligence Exchange :
  - Appliquez les règles en matière de réputation des fichiers (selon le mode de fonctionnement). « Most likely malicious » (Très probablement malveillant) : choisissez de nettoyer/supprimer.
  - « Might be malicious » (Potentiellement malveillant) : bloquer.
- La réputation d'entreprise (organisationnelle) peut outrepasser McAfee GTI :
  - Vous pouvez choisir de bloquer un processus indésirable, par exemple une application non prise en charge ou vulnérable.
  - Marquez le fichier comme « Might be malicious » (Potentiellement malveillant).
- Vous pouvez également choisir d'autoriser un processus indésirable à des fins de test.
  - Marquez le fichier comme « Might be trusted » (Potentiellement approuvé).

McAfee Advanced Threat Defense

- Fonctionnalités de détection prédéfinies :
  - Détection basée sur les signatures : McAfee Labs dispose actuellement de plus de 600 millions de signatures.
  - Détection basée sur la réputation : McAfee GTI
  - Émulation et analyse statique en temps réel : utilisées pour la détection sans signature.
  - Règles YARA personnalisées.
  - Analyse statique complète du code : Reconstitue la logique du code pour évaluer les attributs et les jeux d'instructions, et effectuer un examen approfondi du code source sans l'exécuter.
  - Analyse dynamique dans un environnement restreint de type sandbox

- Créez des profils d'analyse sur les systèmes et programmes susceptibles d'être ciblés par les logiciels infectés par des chevaux de Troie :
  - Systèmes d'exploitation courants, Windows 7, Windows 8, Windows 10
  - Applications Windows installées (Word, Excel) avec macros activées
- Autorisez les profils d'analyse à accéder à Internet :
  - De nombreux échantillons exécutent un script à partir d'un document Microsoft, qui établit une connexion sortante et active le logiciel malveillant. Autoriser les profils d'analyse à accéder à Internet permet d'améliorer les taux de détection.

McAfee Network Security Platform

- Les stratégies par défaut de Network Security Platform contiennent des signatures permettant d'identifier le réseau Tor, qui peut être utilisé pour transférer des fichiers associés aux logiciels malveillants.
- Intégration avec Advanced Threat Defense pour les nouvelles variantes des attaques :
  - Configurez l'intégration avec Advanced Threat Defense dans la stratégie pour les logiciels malveillants avancés.
  - Configurez Network Security Platform pour envoyer les fichiers .exe, Microsoft Office, Java Archive et PDF à Advanced Threat Protection pour inspection.
  - Vérifiez que la configuration d'Advanced Threat Protection est appliquée au niveau des capteurs.
- Mettez à jour les règles de détection des rappels (pour contrer les réseaux de robots).

McAfee Web Gateway

- Activez l'inspection McAfee Gateway Anti-Malware.
- Activez McAfee GTI pour tirer parti du service de réputation des fichiers et des URL.
- Intégrez la solution avec McAfee Advanced Threat Defense pour bénéficier de fonctions sandbox et de détection des menaces de type « jour zéro ».

VirusTotal Convicter : intervention automatisée

- Convicter est un script Python déclenché par le système de réponse automatisée de McAfee ePolicy Orchestrator® (McAfee ePO) pour référencer un fichier générant un événement de menace McAfee Threat Intelligence Exchange avec VirusTotal.
- Notez que vous pouvez modifier le script pour recouper les événements avec d'autres modules Threat Intelligence Exchange, tels que GetSusp.
- Si le seuil de confiance dans la communauté est atteint, le script définit automatiquement la réputation de l'entreprise. Seuil d'identification positive suggéré : 30 % des éditeurs, dont deux éditeurs majeurs, doivent confirmer.
- Filtre : « Target File Name Does Not Contain (Le nom du fichier cible ne contient pas) : McAfeeTestSample.exe ».
- GetSusp est un outil gratuit dont le support est assuré par la communauté. (Le support n'est pas pris en charge par Intel Security.)

McAfee Endpoint Threat Defense and Response

- McAfee Endpoint Threat Defense and Response détecte et neutralise les menaces avancées. Lorsqu'il est utilisé en association avec des flux d'informations sur les menaces tels que McAfee Labs, Dell SecureWorks ou ThreatConnect, les nouvelles menaces peuvent être recherchées et éliminées avant qu'elles n'aient l'occasion de se propager.
- Les collecteurs personnalisés vous permettent de créer des outils spécifiques afin de rechercher et d'identifier les indicateurs de compromission associés aux applications infectées par des chevaux de Troie.
- L'utilisateur intègre des déclencheurs et des réactions pour définir les actions exécutées lorsque des conditions spécifiques sont remplies. Par exemple, lorsque des hachages ou des noms de fichiers sont détectés, une action de suppression peut être automatiquement exécutée.

Autres lectures conseillées

Best Practices for how to use McAfee Host Intrusion Prevention rules for a malware outbreak (Meilleures pratiques pour utiliser les règles McAfee Host Intrusion Prevention en cas d'attaque par logiciel malveillant) : KB84507

Cet article de la base de connaissances fournit des informations détaillées sur Trojan-Powelike, dont les vecteurs d'infection et de propagation : PD25582

SIEM Orchestration: Orchestration Triggers Signs of Malware Infection and Anomalous Behaviors (L'orchestration déclenche des signes d'infection par logiciels malveillants et de comportements anormaux) : PD24830

Livre blanc : *La sécurité au-delà des signatures*

FAQs for Network Security Platform: Advanced Malware Detection (Questions fréquentes sur McAfee Network Security Platform : Détection des logiciels malveillants avancés) : KB75269

Guide produit McAfee Web Gateway : Filtrage de contenu web : PD26339

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