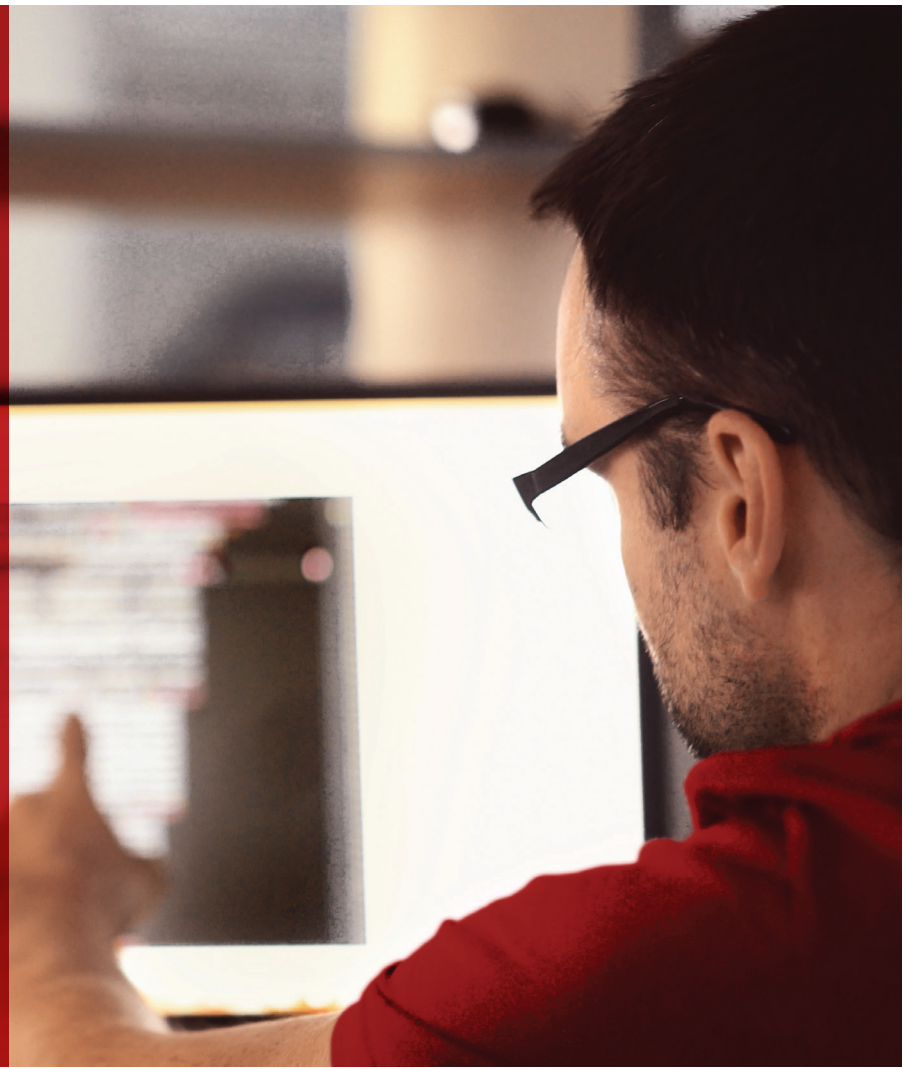
Protection contre Pinkslipbot

W32/Pinkslipbot est une famille de logiciels malveillants à propagation automatique, conçue pour voler les données personnelles et financières de ses victimes. Le logiciel malveillant permet en outre un contrôle total sur ces machines grâce à deux portes dérobées (backdoor), l'une basée sur les commandes transmises par un serveur de contrôle et l'autre sur un utilitaire VNC (Virtual Network Computing). Pinkslipbot peut également se propager à d'autres systèmes de l'environnement via des partages réseau et communiquer avec son serveur de contrôle pour télécharger des versions mises à jour de lui-même.



Pinkslipbot est apparu pour la première fois en 2007. Depuis, le groupe à l'origine de sa conception procède à des mises à jour incrémentielles de sa base de code avant de distribuer de nouvelles versions à intervalles de quelques mois.

Les données volées par Pinkslipbot permettent à l'auteur de l'attaque de déterminer l'emplacement, l'entreprise et l'utilisateur du système infecté. Le cyberpirate pourrait ensuite vendre ces informations à un tiers (en particulier si des entreprises de renom ont été infectées) et déployer un logiciel malveillant ciblé sur la machine compromise une fois le paiement reçu.

Pour une analyse technique approfondie de Pinkslipbot, lisez le *Rapport de McAfee Labs sur le paysage des menaces — Juin 2016*. Le rapport passe en revue le processus d'infection initial, les mécanismes de propagation, les détails techniques et les méthodes de protection générales.

Stratégies et procédures de protection contre Pinkslipbot

Les procédures et stratégies générales expliquées ci-après permettent de vous protéger contre Pinkslipbot.

Pour sécuriser le périmètre, il convient de bloquer les ports inutilisés au niveau de tous les points de sortie du réseau et les demandes de connexion depuis et vers des adresses IP malveillantes associées connues, de même que l'utilisation de partages réseau afin d'empêcher le déplacement latéral de Pinkslipbot. Dans la plupart des environnements, il est également essentiel de désactiver la fonction d'exécution automatique AutoRun de Microsoft Windows. Il est par ailleurs primordial d'appliquer les derniers patchs disponibles aux systèmes d'exploitation et applications Windows, ainsi que de mettre à niveau les logiciels antimalware de façon à disposer de la version la plus récente.

Les systèmes dépourvus de patchs permettent l'exploitation des vulnérabilités. Une gestion efficace des patchs est dès lors indispensable dans tout environnement. Les patchs doivent être testés, vérifiés et implémentés dès leur distribution par le fournisseur. Lorsqu'il est impossible d'appliquer un patch en raison de dépendances à l'égard d'une version plus ancienne, un autre mécanisme doit être mis en place pour limiter l'exploitation des vulnérabilités connues. La gestion rigoureuse des patchs est l'une des solutions les plus efficaces pour limiter les conséquences de Pinkslipbot et d'autres logiciels malveillants.

Bien que Pinkslipbot soit essentiellement distribué au moyen de téléchargements à l'insu de l'utilisateur (drive-by) sur des sites web compromis par des kits d'exploit, les victimes sont généralement dirigées vers ces sites par des e-mails de phishing. En faisant la distinction entre e-mails internes et externes, les utilisateurs ont plus de chances d'identifier les e-mails frauduleux ou de phishing. Ils réfléchiront ainsi à deux fois avant de cliquer sur des liens inconnus, potentiellement malveillants.

Comme Pinkslipbot s'exécute en partie dans la mémoire, l'application de patchs au système, la réalisation d'une analyse complète et l'exécution d'un outil de suppression antimalware ne suffisent pas. Il est indispensable de procéder à un redémarrage des systèmes infectés pour supprimer le logiciel malveillant de la mémoire,

de même qu'à une nouvelle analyse pour s'assurer que le système a été correctement nettoyé. Il est par ailleurs recommandé d'utiliser des mots de passe forts pour mettre fin aux attaques par dictionnaire, de désactiver la fonction AutoRun et d'appliquer le principe du droit d'accès minimal.

Pinkslipbot est un cheval de Troie particulièrement agressif, héritier du célèbre cheval de Troie Zeus. Un mot de passe de connexion faible lui suffit pour infecter un système Windows, même sans aucune exposition à un kit d'exploit ou interaction d'un utilisateur. Une fois le système infecté, toutes les opérations réalisées sur le système sont enregistrées et envoyées aux cyberpirates responsables de l'attaque. Compte tenu de l'établissement d'une communication sécurisée personnalisée avec ses serveurs de contrôle, Pinkslipbot est de plus en plus difficile à détecter et à analyser. Au vu de ses antécédents, chaque nouvelle itération devrait renforcer sa dangerosité. Une parfaite connaissance de votre environnement et la mise en œuvre des stratégies et procédures recommandées vous permettront de limiter les dégâts que peut occasionner Pinkslipbot.

Comment les technologies McAfee peuvent vous aider à vous protéger contre Pinkslipbot

McAfee VirusScan Enterprise (VSE) et McAfee Endpoint Security (ENS) 10

McAfee VirusScan Enterprise et McAfee Endpoint Security 10 offrent une protection antimalware avancée aux terminaux. McAfee VirusScan Enterprise a été remplacé par McAfee Endpoint Security 10, une plate-forme optimisée, plus performante et plus rapide.

Les fichiers DAT de McAfee pour McAfee VirusScan Enterprise et McAfee Endpoint Security 10 incluent des fonctions de détection et de nettoyage des composants de Pinkslipbot. McAfee VirusScan Enterprise et McAfee Endpoint Security 10 offrent une protection multiniveau grâce à des mécanismes de détection en mémoire et d'analyse statique, comportementale et antirootkit. Si vous souhaitez bénéficier d'une protection supplémentaire contre les nouvelles variantes, vous pouvez mettre en œuvre des règles de protection de l'accès qui empêchent Pinkslipbot d'infecter les systèmes.

- Créez et testez une règle de protection de l'accès pour empêcher tout processus de s'exécuter et de créer des fichiers exécutables dans C:\Users*\AppData\Roaming\Microsoft**.exe.
- Créez et testez une règle de protection de l'accès pour empêcher les processus cscrpit.exe et wscript.exe de lire, d'exécuter et de créer des fichiers WPL à partir du dossier %LOCALAPPDATA%\Microsoft\. Il s'agit généralement de fichiers JavaScript. Le blocage de ces fichiers peut empêcher le logiciel malveillant de télécharger ses nouvelles versions.
- Lorsque c'est possible, créez et testez une règle de protection de l'accès pour empêcher les processus cscrpit.exe et wscript.exe de lire et d'exécuter des fichiers du dossier %UserProfile%.
- Créez et testez une règle de protection de l'accès pour empêcher les fichiers « updates_*new.cb », « upd_*.cb » et « updates*_new.cb » d'exécuter et de créer des nouveaux fichiers. Ceux-ci sont généralement utilisés par les fichiers de configuration de Pinkslipbot. Le blocage de ces fichiers peut empêcher le logiciel malveillant de se mettre à jour.

- Créez et testez une règle de protection de l'accès aux ports 65200 à 65400 pour les processus iexplorer.exe et explorer.exe. Comme Pinkslipbot s'injecte dans ces processus, interdire aux processus l'utilisation de ces ports bloque les communications de Pinkslipbot avec son serveur de contrôle.
- Implémentez et testez des règles de protection de l'accès pour empêcher l'exécution à distance des fichiers autorun.inf.

McAfee Host Intrusion Prevention (HIPS)

McAfee Host Intrusion Prevention protège les systèmes contre les menaces de type « jour zéro » en alliant un système de prévention des intrusions (IPS) basé sur les signatures et l'analyse des comportements à un pare-feu dynamique. Les mises à jour planifiées protègent les systèmes des vulnérabilités présentes dans les applications et le système d'exploitation avant même que des patchs soient disponibles. Renforcez la sécurité d'un environnement en activant des signatures. Celles-ci permettent de bloquer un grand nombre des méthodes généralement utilisées par un logiciel malveillant pour exploiter des applications courantes.

- Testez et activez la signature McAfee HIPS 6010 (Protection d'accrochage d'applications génériques).
- Testez et activez la signature McAfee HIPS 6011 (Protection contre l'invocation d'applications génériques).
- Isolez les systèmes infectés par Pinkslipbot en leur attribuant une stratégie dans laquelle la règle de pare-feu bloque tous les ports autres que les ports d'administration.

McAfee Endpoint Security 10 et McAfee Host Intrusion Prevention sont inclus dans la suite McAfee Complete Endpoint Protection.

McAfee Web Gateway (MWG)

Les téléchargements involontaires (drive-by) et les liens incorporés aux e-mails sont deux méthodes courantes de propagation de Pinkslipbot. McAfee Web Gateway assure une sécurité renforcée à l'environnement web et protège les systèmes contre les sites web malveillants. Il peut être déployé en tant qu'appliance matérielle dédiée ou image de machine virtuelle.

- Configurez McAfee Web Gateway pour le filtrage antispam.
  - Le filtrage antispam offre une protection contre les éléments suivants :
    - Adresses IP malveillantes
    - URL malveillantes
    - E-mails de spam
- Activez l'inspection GAM.
- 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 ».

McAfee Active Response (MAR)

McAfee Active Response assure des fonctions continues de détection et réponse aux systèmes ciblés par des menaces avancées telles que Pinkslipbot. La surveillance automatique des événements vous permet d'identifier des indicateurs de compromission, signes d'une infection par un logiciel malveillant.

- La présence des domaines suivants dans un cache DNS peut être le signe d'une infection par Pinkslipbot :
  - gpfbvtuz.org
  - hsdmoyrkeqpcyrtw.biz
  - lgzmtkvnijeaj.biz
  - mfrlilcumtwieyzbfdmpdd.biz
  - hogfpicpoxnp.org
  - qrogmwmahgcwil.com
  - enwgzzthfwhdm.org
  - vksslxpxaoql.com
  - dxmhcvxcmdewthfbnaspnu.org
  - mwtfngzkadeviqtlfrrio.org
  - jynsrklhmaqirhjrtygjx.biz
  - uuwgdehizcuuucast.com
  - gyvwkxfxqdargdooqql.net
  - xwcjchzq.com
  - tqxllcfn.com
  - feqsrxswnumbkh.com
  - nykhliicqv.org
  - ivalhlotxdyvzyxrb.net
  - bbxrsgsuwksogpktqydlkh.net
  - rudjqypvucwwpfejdxqsv.org
- Effectuez la requête de cache DNS suivante pour déterminer si des systèmes ont communiqué avec l'un des domaines Pinkslipbot connus répertoriés ci-dessus.
  - DNSCache where DNSCache hostname equals "[domaine Pinkslipbot]"
- Cette requête renvoie une liste des communications entre des domaines Pinkslipbot et des systèmes de l'environnement. Vous pouvez facilement identifier les systèmes en communication avec ces domaines en cliquant sur l'entrée et en affichant les systèmes connectés.
- Utilisez un pare-feu local comme McAfee ENS 10 ou McAfee HIPS pour mettre en quarantaine les systèmes infectés par Pinkslipbot. Pour mettre un système en quarantaine, attribuez-lui une stratégie de pare-feu verrouillé dans McAfee ePO.

Exécutez une analyse McAfee ENS 10 ou McAfee VSE complète à la demande du système en lui attribuant une tâche d'analyse à la demande à exécuter immédiatement dans McAfee ePO. Activez l'agent afin de lancer l'analyse.

Autres lectures conseillées

Série de webinars McAfee sur les logiciels malveillants : Pinkslipbot

Cette vidéo propose une présentation de Pinkslipbot, la répartition des infections par région et secteur d'activité, ses caractéristiques et les symptômes, sans oublier des recommandations de prévention.

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr