Présentation de solution

# Protection contre les voleurs de mots de passe

Notre dépendance croissante vis-à-vis des terminaux électroniques personnels et la migration des données d'entreprise stratégiques vers le cloud font monter en flèche la valeur des identifiants d'accès. De nos jours, les auteurs d'attaques utilisent des voleurs de mots de passe dans les premières phases de presque toutes les principales menaces persistantes avancées (APT).

Les voleurs de mots de passe ont pour but de déjouer la sécurité des réseaux et des systèmes pour obtenir des identifiants permettant d'accéder à des ressources critiques. Dans cette catégorie de malware, le voleur de mots de passe Fareit jouit d'une popularité inégalée depuis plus de cinq ans grâce à ses fonctionnalités robustes. Depuis sa découverte en 2012, il évolue sans cesse pour échapper aux stratégies de cyberdéfense les plus récentes.

Au départ, Fareit se concentrait sur les identifiants de connexion provenant des navigateurs web pour accéder à des applications (notamment des services bancaires ou comptes e-mail) et voler des identités. Au fil du temps, il s'est transformé en un voleur d'informations plus agressif qui recourt à des procédés de mimétisme, modifiant par exemple son hachage de fichier à chaque infection. En 2016, une nouvelle génération de malwares voleurs de mots de passe Fareit a vu le jour. Ceux-ci exploitent un actif réseau infecté pour lancer des attaques par déni de service distribué (DDoS). De plus, Fareit est désormais proposé sous la forme d'un service de facturation à l'infection. En d'autres termes, les cybercriminels gagnent de l'argent en distribuant les logiciels malveillants, leur rétribution étant proportionnelle au nombre d'infections.

Les attaques par phishing qui distribuent des voleurs de mots de passe tels que Fareit comptent parmi les principaux vecteurs d'attaque initiaux des dix dernières années.

## Stratégies et procédures de protection contre les attaques par voleurs de mots de passe

McAfee recommande aux entreprises de prendre les mesures suivantes pour se protéger contre les attaques par voleurs de mots de passe :

- Dans la mesure où les voleurs de mots de passe sont souvent distribués par des logiciels malveillants, veillez à toujours disposer de produits de protection antimalware à jour.
- Il arrive que des utilisateurs téléchargent sans le savoir des logiciels malveillants lors de la navigation. Conservez les navigateurs web et les modules complémentaires parfaitement à jour pour ajouter un niveau supplémentaire de protection.

McAfee™
Together is power.

- Exécutez les applications en tant qu'utilisateur ayant des privilèges limités plutôt que des droits d'administrateur.
- Sécurisez le périmètre réseau. Les pare-feux peuvent empêcher les auteurs d'attaques d'accéder à des applications internes compromises auparavant par des attaques par voleurs de mots de passe.
- Ne faites usage des identifiants d'authentification d'entreprise (p. ex. ceux des serveurs proxy web pour la navigation Internet, des applications de base de données, de dossiers partagés, etc.) que lorsque vous utilisez les actifs de l'entreprise. N'acceptez au sein du réseau d'entreprise fiable que les systèmes distribués et certifiés par l'équipe de sécurité informatique de l'entreprise.
- Des malwares susceptibles de contenir des voleurs de mots de passe peuvent se dissimuler dans des logiciels légitimes infectés par un cheval de Troie. Pour empêcher une attaque de ce type d'aboutir, nous vous recommandons vivement de renforcer les mécanismes de diffusion et de distribution de logiciels. Il est toujours intéressant de posséder un référentiel central d'applications d'entreprise à partir duquel les utilisateurs peuvent télécharger des logiciels approuvés.
- Si les utilisateurs sont autorisés à installer des applications qui n'ont pas été validées au préalable par l'équipe de sécurité informatique, informez-les qu'ils doivent uniquement installer des applications dotées de signatures approuvées provenant de fournisseurs connus. Il est très courant que des applications proposées en ligne, apparemment inoffensives, intègrent des voleurs de mots de passe ou d'autres logiciels malveillants.
- Évitez de télécharger des applications à partir d'autres types de sources que des sources web. La probabilité de télécharger des logiciels malveillants à partir de groupes Usenet, de canaux IRC, de clients de messagerie instantanée ou de réseaux peer-to-peer est très élevée. Les liens renvoyant à des sites web dans les canaux IRC et la messagerie instantanée pointent souvent vers des fichiers à télécharger infectés.
- Mettez en place un programme de formation sur la prévention des attaques par phishing. Les voleurs de mots de passe sont couramment distribués par cette technique.

Si vous pensez que des systèmes ont été compromis par un voleur de mots de passe, les meilleures pratiques suivantes vous aideront à contenir le déplacement latéral de l'infection :

- Réduisez la surface d'attaque en activant une authentification à deux facteurs pour les applications qui prennent en charge cette technologie. Ainsi, même si l'auteur de l'attaque dispose d'un mot de passe volé, le deuxième facteur bloque l'infiltration.
- L'utilisation d'un pare-feu pour terminaux peut freiner l'expansion des intrusions qui utilisent des mots de passe volés lorsque les règles de pare-feu limitent les trafics entrant et sortant sur l'ordinateur infecté.

## Comment les produits McAfee peuvent protéger contre les attaques par voleurs de mots de passe

### McAfee VirusScan® Enterprise 8.8 ou McAfee Endpoint Security 10

- Conservez les logiciels antimalware pour terminaux parfaitement à jour en leur appliquant les derniers patchs et la version la plus récente des fichiers DAT et du moteur d'analyse. Assurez-vous que McAfee Global Threat Intelligence (McAfee GTI) est activé.
- 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

Les outils de prévention des intrusions sont peu efficaces pour identifier une attaque par voleur de mot de passe. Toutefois, McAfee Host Intrusion Prevention permet d'empêcher le déplacement latéral de la charge active du logiciel malveillant, qui peut contenir un voleur de mots de passe.

- 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 McAfee 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 McAfee 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 « **\ » ou « ?:\ » avant le nom du fichier. Pour remplacer la lettre du lecteur, utilisez, par exemple, « **\nomdufichier.exe » ou « ?:\nomdufichier.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, 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 (p. ex. 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 (p. ex. 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 (p. ex. 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 voleurs de mots de passe.

### McAfee Threat Intelligence Exchange et McAfee Advanced Threat Defense

- Configuration des stratégies McAfee 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 McAfee 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 Advanced Threat Defense » (Envoyer les fichiers à Advanced Threat Defense) aux niveaux « Unknown » (Inconnu) et inférieurs.
  - Stratégie McAfee Threat Intelligence Exchange Server : Acceptez les réputations McAfee Advanced Threat Defense pour les fichiers qui n'ont jamais été rencontrés par McAfee Threat Intelligence Exchange.
- Intervention manuelle dans McAfee 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 :
  - Choisissez 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 : La collection de logiciels malveillants de McAfee Labs compte 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 des voleurs de mots de passe :
  - Systèmes d'exploitation courants tels que Windows 7, 8 et 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 McAfee Network Security Platform contiennent des signatures permettant d'identifier le réseau Tor, qui peut être utilisé pour transférer des fichiers associés aux voleurs de mots de passe.

- Intégration avec McAfee Advanced Threat Defense pour les nouvelles variantes des attaques :
  - Configurez l'intégration avec McAfee Advanced Threat Defense dans la stratégie pour les logiciels malveillants avancés.
  - Configurez McAfee Network Security Platform pour envoyer les fichiers .exe, Microsoft Office, Java Archive et PDF à McAfee Advanced Threat Protection pour inspection.
  - Vérifiez que la configuration de McAfee Advanced Threat Defense est appliquée au niveau des capteurs.
- Mettez à jour les règles de détection des rappels (pour contrer les botnets).

### McAfee Web Gateway

- Activez l'inspection antimalware de McAfee Web Gateway.
- 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.
- Vous pouvez modifier le script pour recouper les événements avec d'autres modules McAfee 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 McAfee.)

### McAfee Active Response

- McAfee Active 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 permettent de créer des outils spécifiques afin de rechercher et d'identifier les indicateurs de compromission associés aux voleurs de mots de passe.
- 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 particuliers sont détectés, une action de suppression peut être automatiquement exécutée.

## Autres lectures conseillées

Phishing Attacks Employ Old but Effective Password Stealer (Les attaques par phishing utilisent un voleur de mots de passe ancien, mais efficace)

Profil de virus - Fareit

Profil de virus - Fareit

McAfee™
Together is power.



**McAfee Ireland Ltd.**
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/fr