McAfee
Together is power.

Protection contre WannaCry et Petya

Lancée en mai 2017, une cyberattaque à grande échelle basée sur la famille de logiciels malveillants WannaCry exploitait une vulnérabilité dans certaines versions de Microsoft Windows. Plus de 300 000 ordinateurs dans 150 pays auraient été infectés lors de l'attaque principale, demande de rançon à la clé.

Si les enquêteurs n'ont pas encore déterminé avec certitude le vecteur d'attaque initial, ils savent qu'un ver particulièrement agressif a permis de propager le logiciel malveillant. Dès le mois de mars, Microsoft avait mis en ligne un patch critique permettant de supprimer la vulnérabilité sous-jacente dans les versions prises en charge de Windows, mais de nombreuses entreprises ne l'avaient pas encore appliqué.

Quant aux ordinateurs qui exécutaient des versions non prises en charge de Windows (Windows XP, Windows Server 2003), ils n'avaient tout simplement pas de patch à disposition. Ce n'est qu'après l'attaque WannaCry que Microsoft a publié un patch de sécurité spécial pour Windows XP et Windows Server 2003.

Environ six semaines plus tard, une autre cyberattaque exploitait la même vulnérabilité. Petya n'a pas eu autant d'impact que WannaCry, mais ces attaques ont mis en évidence l'usage dans des domaines critiques de systèmes d'exploitation dépassés, à tel point qu'ils ne sont plus pris en charge par leurs éditeurs, mais aussi la négligence de certaines entreprises en matière d'application des correctifs. Vous trouverez une analyse détaillée de ces attaques dans le *Rapport sur le paysage des menaces de McAfee Labs — Septembre 2017*.

Stratégies et procédures de protection contre WannaCry et Petya

- **Sauvegarde des fichiers :** La mesure la plus efficace contre le ransomware consiste à sauvegarder régulièrement les fichiers de données et à vérifier les procédures de restauration réseau.
- **Information et sensibilisation des utilisateurs du réseau :** Comme d'autres logiciels malveillants, le ransomware infecte souvent un système grâce à des attaques de phishing par l'intermédiaire de pièces jointes, de téléchargements ou d'injections de scripts intersites lors de la navigation web.
- **Surveillance et inspection du trafic réseau :** Ces mesures permettent d'identifier le trafic réseau anormal associé à des ransomwares.
- **Utilisation de flux de cyberveille :** Cette pratique permet de détecter les menaces plus rapidement.
- **Limitation de l'exécution de code :** Le ransomware est souvent conçu pour s'exécuter dans des dossiers bien connus du système d'exploitation. S'il ne peut pas atteindre ces dossiers en raison du contrôle d'accès, le chiffrement malveillant des données peut être bloqué.
- **Limitation de l'accès aux comptes système et d'administrateur :** Certains types de ransomwares sont conçus pour utiliser des comptes par défaut pour exécuter leurs opérations. Dans ce cas, l'attribution de nouveaux noms aux comptes d'utilisateur par défaut et la désactivation des comptes inutiles (avec ou sans privilèges) permettent de renforcer la protection.
- **Suppression des droits d'administrateur local :** Cette mesure empêche le ransomware de s'exécuter sur un système local et bloque sa propagation favorisée par les privilèges administrateur. La suppression des droits d'administration locaux bloque également l'accès à tous les fichiers et ressources critiques que le ransomware cherche à chiffrer.
- **Autres pratiques de gestion des autorisations :** Envisagez de limiter l'accès en écriture des utilisateurs, par exemple en bloquant l'exécution à partir des répertoires des utilisateurs, en plaçant les applications sur des listes blanches et en limitant l'accès aux partages ou aux systèmes de stockage réseau. Certains ransomwares nécessitent un accès en écriture à des chemins de fichiers spécifiques pour s'installer et s'exécuter. Limiter les autorisations d'écriture à un nombre restreint de répertoires (par exemple Mes documents ou Téléchargements) peut arrêter certaines variantes. Les fichiers exécutables des ransomwares peuvent être également bloqués par la suppression de l'autorisation d'exécution sur ces répertoires. De nombreuses entreprises utilisent un ensemble limité d'applications pour réaliser leurs activités. Il est donc possible d'empêcher l'exécution d'applications non autorisées, y compris les ransomwares, en implémentant une stratégie de liste blanche. Une autre pratique en matière d'autorisations consiste à exiger un identifiant de connexion au niveau des ressources partagées, par exemple les dossiers réseau.
- **Gestion et mise à jour des logiciels :** Pour tenir les ransomwares en échec, une autre règle fondamentale consiste à gérer les versions et les mises à jour des logiciels, surtout les patchs du système d'exploitation, et celles des solutions de sécurité et antimalware.

Il est très important de réduire la surface d'attaque, surtout contre le phishing, l'une des techniques de prédilection des ransomwares. En ce qui concerne la messagerie électronique, il est conseillé d'appliquer les mesures suivantes :

- **Filtrage du contenu des e-mails :** La sécurisation du canal e-mail est une mesure essentielle. Les chances de réussite d'une attaque sont réduites si les utilisateurs du réseau reçoivent moins de messages de spam susceptibles d'inclure du contenu potentiellement malveillant et dangereux.
- **Blocage des pièces jointes :** L'inspection des pièces jointes joue un rôle clé dans la limitation de la surface d'attaque. Les ransomwares sont souvent distribués sous la forme d'une pièce jointe exécutable. Mettez en œuvre une stratégie interdisant l'envoi par e-mail de fichiers portant certaines extensions. Il est possible d'analyser ces fichiers joints dans une solution sandbox et de les faire supprimer par l'appliance de sécurité e-mail.

Comment les produits McAfee peuvent protéger contre WannaCry

McAfee Network Security Platform (NSP)

McAfee NSP assure un temps de réaction rapide dans la prévention des exploits et la protection des actifs installés sur un réseau. L'équipe McAfee NSP travaille sans relâche pour développer et déployer des signatures définies par l'utilisateur dans les cas critiques. Dans les 24 heures qui ont suivi l'attaque WannaCry, McAfee a créé et transmis plusieurs de ces signatures, que les clients ont pu déployer sur les capteurs de leur réseau.

Dans ce cas, les signatures ciblaient explicitement les outils d'exploit EternalBlue, Eternal Romance SMB Remote Code Execution et DoublePulsar. McAfee a également publié des indicateurs de compromission relatifs à ces exploits, à ajouter à une liste noire afin de bloquer les menaces potentielles associées au cheval de Troie original.

Pour en savoir plus sur les signatures NSP, cliquez ici.

McAfee Host Intrusion Prevention (HIPS)

McAfee HIPS 8.0 avec signature NIPS 6095 offre une protection contre les quatre variantes connues de WannaCry. Pour obtenir les dernières informations sur ces configurations, consultez l'article KB89335.

Signature personnalisée n° 1 : Règle de blocage du Registre pour contrer WannaCry
Utiliser une sous-règle standard
Type de règle = Registre
Opérations = Créer, Modifier, Modifier les autorisations, Inclure la clé de Registre
Clé de Registre = \REGISTRY\MACHINE\SOFTWARE\WanaCrypt0r
Fichier exécutable = *

Signature personnalisée n° 2 : Règle de blocage de fichier/dossier pour contrer WannaCry
Utiliser une sous-règle standard
Type de règle = Fichiers
Opérations = Créer, Écrire, Renommer, Modifier les attributs Lecture seule/Masqué, Inclure les fichiers
Fichiers = *.wnry
Fichier exécutable = *

Configuration de McAfee Endpoint Protection (ENS) et de McAfee VirusScan Enterprise (VSE) avec le module Protection adaptive contre les menaces

McAfee Endpoint Security 10.5 — Protection adaptive contre les menaces

McAfee Endpoint Security 10.5 avec les modules Protection adaptive contre les menaces, Real Protect et Confinement d'application dynamique offre une protection contre les exploits WannaCry connus et inconnus.

- Configurez les règles suivantes dans les options du module Protection adaptive contre les menaces :
  - Affectation de règle = Sécurité (La valeur par défaut est Equilibré.)
- Configurez les règles suivantes dans les options du module Protection adaptive contre les menaces — Confinement d'application dynamique :
  - Confinement d'application dynamique — Règles de confinement

Reportez-vous à l'article KB87843 : Liste des règles de confinement d'application dynamique Endpoint Security et meilleures pratiques pour leur utilisation, puis définissez les règles recommandées de confinement d'application dynamique sur Bloquer, comme indiqué.

McAfee Endpoint Security 10.1, 10.2 et 10.5 — Prévention contre les menaces

McAfee Endpoint Security 10.x — Prévention contre les menaces avec contenu AMCore 2978 ou version ultérieure offre une protection contre les quatre variantes actuellement connues de WannaCry.

McAfee VirusScan Enterprise 8.8

McAfee VirusScan Enterprise 8.8 avec contenu DAT 8527 ou version ultérieure offre une protection contre les quatre variantes actuellement connues de WannaCry.

Mesures proactives de protection par McAfee Endpoint Security (ENS) et de protection de l'accès par McAfee VirusScan Enterprise (VSE)

Les règles de protection McAfee ENS et de protection de l'accès McAfee VSE empêchent la création du fichier .wnry. Elles bloquent la routine de chiffrement qui crée les fichiers chiffrés contenant une extension .wncryt, .wncry ou .wcry. Le blocage du fichier .wnry rend inutile celui de ces types de fichiers chiffrés.

Cliquez ici pour en savoir plus sur la configuration de règles de protection de l'accès dans McAfee VSE.

Configuration d'un système de protection des terminaux contre le chiffrement de fichiers exécuté par WannaCry (et ses futures variantes, encore inconnues)

Les clients qui n'utilisent pas la sécurité McAfee ENS avec le module Protection adaptive contre les menaces ne disposent peut-être pas d'une protection de contenu McAfee contre les variantes encore inconnues. Dans ce cas, nous recommandons la configuration de tâches de mise à jour du référentiel avec un intervalle d'actualisation minimal, afin de garantir que le nouveau contenu est appliqué au moment de sa publication par McAfee.

D'autres protections contre la routine de chiffrement peuvent être configurées à l'aide des règles de protection de l'accès McAfee VSE/ENS ou à l'aide des règles personnalisées McAfee HIPS. Pour obtenir les dernières informations sur ces configurations, consultez l'article KB89335.

Les règles de protection de l'accès McAfee ENS et McAfee VSE, ainsi que les signatures McAfee HIPS personnalisées, empêchent la création du fichier .wnry.

Elles bloquent la routine de chiffrement qui crée les fichiers chiffrés contenant une extension .wncryt, .wncry ou .wcry.

Le blocage du fichier .wnry rend inutile celui de ces types de fichiers chiffrés.

Pour obtenir les dernières informations sur ces configurations, consultez l'article KB89335 (réservé exclusivement aux clients McAfee enregistrés).

McAfee Advanced Threat Defense (ATD)

La fonction d'apprentissage automatique de McAfee ATD permet d'identifier un échantillon via une analyse de type gravité moyenne.

McAfee ATD a permis de détecter les tendances suivantes :

Classification du comportement :

- Fichier dissimulé
- Propagation
- Exploitation via le shellcode
- Propagation sur le réseau

Analyse dynamique :

- Comportement déclenché du ransomware
- Chiffrement de fichiers
- Création et exécution de contenu de script suspect
- Comportement similaire à celui d'un injecteur de macro de cheval de Troie

Depuis l'existence de WannaCry, McAfee ATD a permis d'observer 22 opérations de processus, notamment cinq DLL d'exécution, 58 opérations sur fichiers, des modifications du Registre, des modifications de fichiers, des créations de fichiers (dll.exe), des injections de DLL et 34 opérations réseau.

McAfee Web Gateway (MWG)

McAfee Web Gateway (MWG) est une gamme de produits (appliance, cloud et hybride) composée de proxys web, qui offre une protection immédiate contre les variantes de WannaCry distribuées sur le Web (HTTP/HTTPS) à l'aide de différents moteurs d'analyse en temps réel.

Les fonctionnalités d'analyse de la réputation et antimalware de McAfee Global Threat Intelligence (GTI) bloquent les variantes connues au moment où le trafic web est traité dans le proxy.

Via son processus d'émulation comportementale appliqué sur les fichiers, le code HTML et les scripts JavaScript, le moteur Gateway Anti-Malware (GAM) Engine intégré à MWG bloque de façon efficace les variantes qui n'ont pas encore été identifiées à l'aide d'une signature (menaces « jour zéro »). Les modèles d'apprentissage automatique alimentent régulièrement les émulateurs en cyberveille sur les menaces. GAM s'exécute de concert avec les fonctionnalités GTI d'analyse de la réputation et antimalware à mesure que le trafic est traité.

En associant MWG et ATD, il est possible de bénéficier d'inspections plus poussées et d'une approche efficace en matière de prévention et de détection.

McAfee Threat Intelligence Exchange (TIE)

McAfee Threat Intelligence Exchange (TIE) renforce davantage encore le niveau de sécurité du client. Dotée de la capacité d'agréger les verdicts de réputation émis par ENS, VSE, MWG et NSP, la solution TIE est capable de partager rapidement des informations de réputation relatives à WannaCry avec n'importe quel vecteur intégré. En outre, étant donné que TIE permet d'utiliser GTI dans le cadre d'une demande de réputation au niveau mondial, les produits intégrés peuvent prendre une décision immédiate avant d'exécuter la charge active d'un ransomware, en exploitant les informations de réputation placées dans la mémoire cache de la base de données TIE.

Un terminal peut ainsi appliquer des mesures de protection, détecter les variantes associées et mettre à jour le score de réputation dans TIE. Cette approche à 360° offre un niveau de protection accru, car les informations sont disséminées à tous les terminaux intégrés à TIE. Ce partage bidirectionnel de la cyberveille sur les menaces est décuplé, car il existe également dans MWG et dans NSP. Par conséquent, lorsque la menace potentielle tente de s'infiltrer via un réseau ou le Web, MWG et NSP non seulement assurent un rôle de protection et de détection, mais partagent également ces informations avec TIE, qui va immuniser les terminaux. L'entreprise bénéficie d'une protection immédiate, la variante identifiée ne pouvant pas s'exécuter sur un « patient zéro » potentiel dans l'environnement.

Comment les produits McAfee peuvent protéger contre Petya

McAfee offre une protection contre l'attaque Petya initiale grâce à l'analyse comportementale antimalware avancée de Real Protect Cloud et à l'apprentissage automatique que permet le réseau neuronal dynamique de McAfee Advanced Threat Defense.

ATD 4.0 a introduit une nouvelle capacité de détection qui utilise un réseau neuronal multiniveau avec rétropropagation qui tire parti d'un apprentissage semisupervisé. Ce réseau neuronal dynamique analyse certaines fonctions du logiciel malveillant afin d'élaborer un verdict positif ou négatif quant à la malveillance du code.

Qu'elle soit installée en version autonome ou connectée aux terminaux ou capteurs réseau McAfee, la solution ATD associe cyberveille sur les menaces, analyse comportementale en sandbox et apprentissage automatique avancé pour offrir une protection de type « jour zéro » adaptable. Le module Real Protect, qui fait partie de la solution Dynamic Endpoint, utilise également l'apprentissage automatique et l'analyse des liens pour assurer une protection contre les malwares sans signature, et pour alimenter Dynamic Endpoint et le reste de l'écosystème McAfee en informations de qualité sur les menaces. Associé au module Confinement d'application dynamique, Real Protect a offert une protection contre Petya dès les premiers stades de l'attaque.

Les différents produits McAfee offrent une protection accrue, soit en bloquant l'attaque, soit en empêchant de nouvelles exécutions.

McAfee Endpoint Security

Prévention contre les menaces

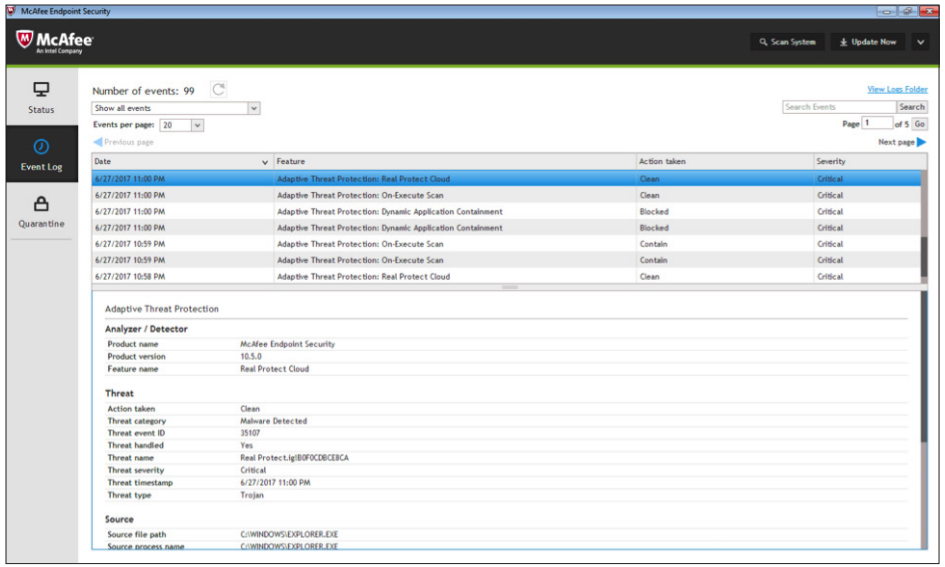
- En combinant McAfee Endpoint Security, McAfee Global Threat Intelligence et une stratégie d'analyse à l'accès avec niveau de sensibilité défini sur Faible, l'entreprise bénéficie d'une protection contre les échantillons et les variantes connus.
- Pour en savoir plus sur les paramètres recommandés de McAfee GTI en matière de réputation des fichiers, consultez l'article KB74983 du Knowledge Center. Vous trouverez également des informations complémentaires dans l'article KB53735.

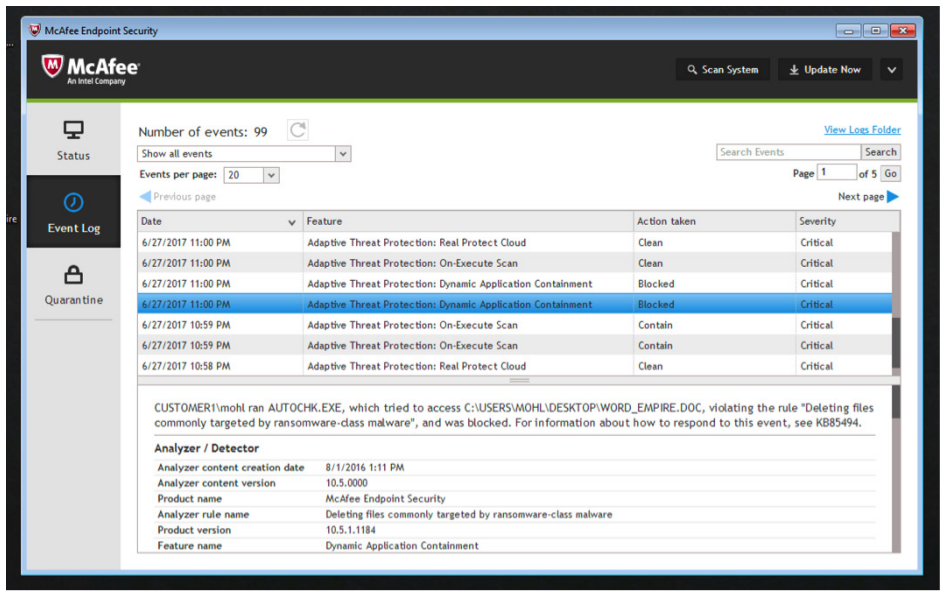
- McAfee Threat Intelligence Exchange associé à GTI assure une protection contre les échantillons et les variantes connus.

Les systèmes qui utilisent McAfee ENS 10 bénéficient d'une protection contre les échantillons et les variantes connus, qui se base à la fois sur les signatures et sur la cyberveille sur les menaces.

Protection adaptive contre les menaces

- Le module Protection adaptive contre les menaces (avec affectation de règle définie sur Équilibré, soit la valeur par défaut du paramètre Protection adaptive contre les menaces\Options\Affectation de règle) assure une protection contre les variantes connues et inconnues du ransomware Petya.
- Ce module offre une protection contre cette menace inconnue à l'aide de plusieurs couches de protection et de confinement avancés :
  - Le composant Real Protect Static utilise une analyse comportementale pré-exécution côté client afin de surveiller les menaces malveillantes inconnues avant leur lancement.
  - Le composant Real Protect Cloud exploite une fonction d'apprentissage automatique assisté par le cloud pour identifier et éradiquer la menace, comme illustré sur la capture d'écran en haut à droite.
- Le composant Confinement d'application dynamique permet de confiner la menace et d'éviter les éventuels dégâts. (Des événements liés à ce composant sont illustrés sur la capture d'écran en bas à droite.)





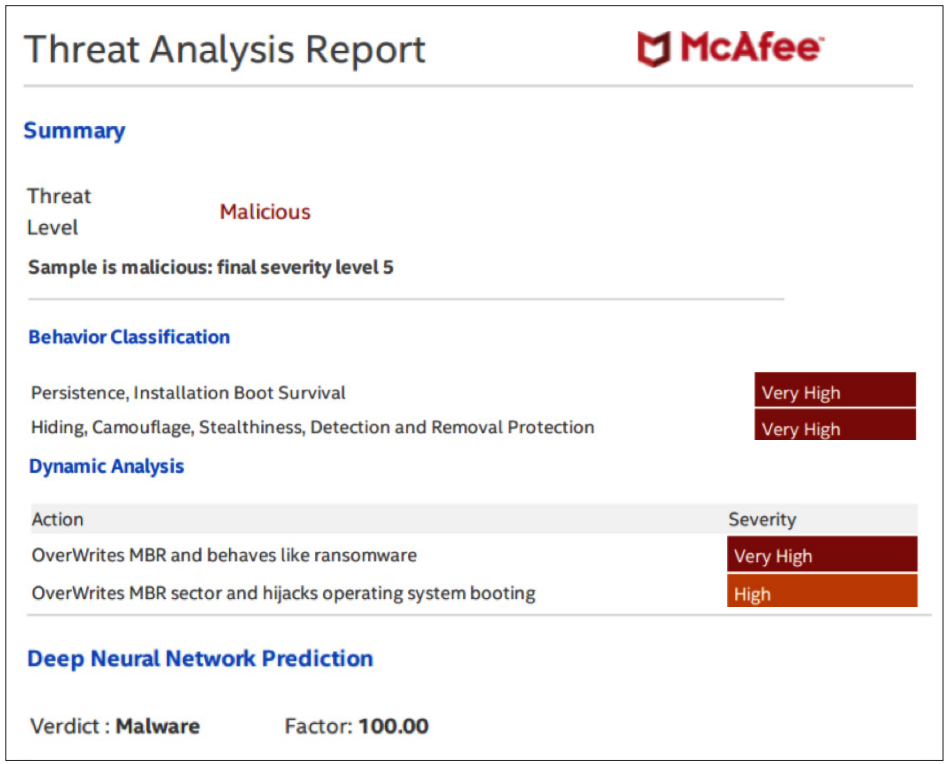
McAfee Advanced Threat Defense

- La solution McAfee Advanced Threat Defense 4.0, dotée d'un réseau neuronal pour apprentissage profond et d'une fonction d'analyse dynamique en sandbox, a identifié la menace et mis à jour son écosystème de cybersécurité de façon proactive. (Voir ci-dessous.)

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) est une solution SIEM qui propose une cyberveille sur les menaces directement exploitable et des intégrations pour prioriser, analyser et neutraliser efficacement les menaces.

Les packs de contenu Suspicious Activity Content Pack et Exploit Content Pack pour McAfee ESM ont été mis à jour avec l'ajout de règles, alarmes et listes de surveillance propres à WannaCry, ce qui rend possible la détection et l'identification d'éventuelles infections. Ces mises à jour offrent également une protection contre Petya. Ces deux packs sont disponibles au téléchargement dans la console McAfee ESM, gratuitement. Par ailleurs, les règles de corrélation par défaut intégrées à McAfee ESM peuvent alerter les utilisateurs si davantage d'analyses SMB horizontales sont détectées.



De même que pour WannaCry, une attaque Petya représente une occasion d'en apprendre davantage sur le fonctionnement des logiciels malveillants, au profit des analystes SOC. Comprendre les malwares et automatiser les meilleures pratiques permettront aux professionnels de la sécurité de gérer aux mieux les prochaines attaques fulgurantes.

McAfee Web Gateway

McAfee Web Gateway (MWG) est une gamme de produits (appliance, cloud et hybride) composée de proxys web, qui offre une couche supplémentaire de protection contre les variantes de Petya distribuées sur le Web (HTTP/HTTPS) à l'aide de différents moteurs d'analyse en temps réel. Les fonctionnalités d'analyse de la réputation et antimalware de GTI bloquent les variantes connues au moment où le trafic web est traité dans le proxy.

Via son processus d'émulation comportementale appliqué sur les fichiers, le code HTML et les scripts JavaScript, le moteur Gateway Anti-Malware Engine intégré à MWG bloque de façon efficace les variantes de type « jour zéro » qui n'ont pas encore été identifiées à l'aide d'une signature. Les modèles d'apprentissage automatique alimentent régulièrement les émulateurs en cyberveille sur les menaces. GAM s'exécute de concert avec les fonctionnalités GTI d'analyse de la réputation et antimalware à mesure que le trafic est traité.

En associant MWG et ATD, il est possible de bénéficier d'inspections plus poussées et d'une approche efficace en matière de prévention et de détection.

Produits McAfee utilisant des fichiers DAT

McAfee a publié un fichier Extra.DAT qui couvre Petya, ainsi qu'un fichier DAT d'urgence qui traite lui aussi cette menace. Les fichiers DAT successifs feront de même. Les fichiers DAT les plus récents sont disponibles via l'article du Knowlegde Center KB89540.

Autres lectures conseillées

Les articles suivants du McAfee Knowledge Center offrent des détails techniques régulièrement mis à jour : KB89335, KB87843, KB74983, KB53735 et KB89540.

McAfee
Together is power.

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