tenable™
network security

Surveillance stratégique des programmes malveillants avec Nessus, PVS et LCE

19 mars 2013
(Révision 3)

Sommaire

Présentation

La suite Unified Security Monitoring (USM) de Tenable offre une flexibilité exceptionnelle pour la surveillance de la sécurité et de la conformité des réseaux dans de nombreux domaines, notamment l'inventaire des systèmes, les vulnérabilités et la conformité aux politiques d'entreprise. Le déploiement d'un dispositif de surveillance de bout en bout des systèmes en réseau donne des informations intéressantes et nécessaires sur votre présence en tant qu'entreprise. Avec la surveillance des processus système et du trafic réseau, et la mise en corrélation avec les résultats des audits de configurations antivirus et des analyses de programmes malveillants, la plate-forme USM de Tenable peut identifier une grande variété de menaces pesant sur une entreprise au-delà des analyses de vulnérabilités.

Nessus et SecurityCenter sont capables de détecter un large éventail de programmes malveillants s'exécutant sous Windows et même de plus en plus sur les systèmes Apple. Grâce à un flux d'informations externe à faible latence, Nessus peut recourir à une analyse avec authentification pour déterminer si les processus en cours d'exécution correspondent à des signatures de programmes malveillants connus. Associée à Passive Vulnerability Scanner (PVS) et Log Correlation Engine (LCE), la suite USM de Tenable peut ensuite vous aider à identifier et à déterminer l'étendue des infections par des programmes malveillants. Il est essentiel de savoir si un programme malveillant a infecté une machine parce qu'un employé a cliqué sur une pièce jointe dangereuse, ou s'il s'agit d'une infection généralisée qui nuit à l'intégrité d'une partie importante de votre environnement.

Les administrateurs informatiques sont supposés gérer eux-mêmes les logiciels de protection contre les programmes malveillants et installer sur leurs systèmes tout agent requis par ces logiciels.

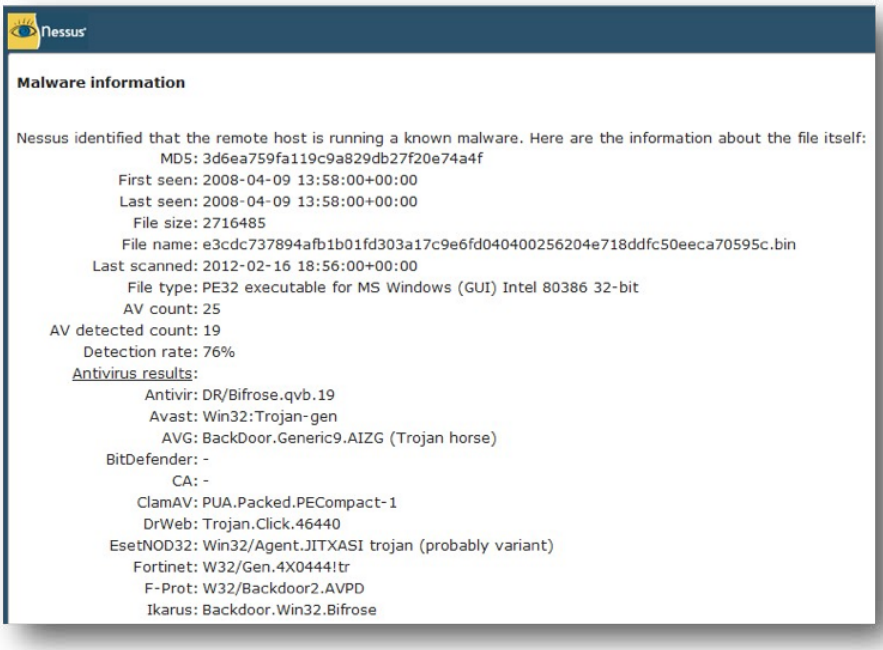
Nessus

L'analyseur de vulnérabilités Nessus fournit différentes méthodes pour détecter une grande variété de programmes malveillants. Selon le niveau d'accès dont dispose un analyseur Nessus sur l'hôte cible, ces méthodes peuvent permettre un examen approfondi de l'hôte pour la détection d'un nombre incroyable de programmes malveillants documentés et plus encore.

Détection des programmes malveillants

Nessus peut utiliser une analyse avec authentification pour détecter les programmes malveillants sur les systèmes Windows. Grâce à un flux externe d'informations spéciales sur les programmes malveillants, Nessus peut inspecter les processus en cours d'exécution pour déterminer s'ils correspondent aux signatures de programmes malveillants connus, selon le catalogage établi par les principaux éditeurs de solutions antivirus.

Pour que cette détection ait lieu, un agent temporaire est chargé et s'installe en tant que service Windows. L'agent génère une liste d'empreintes numériques (ou hash) établie à partir des processus en cours d'exécution, les code et les envoie à un serveur Tenable qui transmet la requête au fournisseur externe de hachage ?? de programmes malveillants. Une fois ce processus terminé, l'agent est supprimé au moment de l'exécution de l'analyse. Nessus génère ensuite un rapport indiquant tous les programmes malveillants détectés, ainsi qu'un lien vers des informations complémentaires, notamment le hash MD5, la date/l'heure à laquelle le programme malveillant a été découvert pour la première fois, le nom que chaque éditeur d'antivirus lui a attribué ainsi que d'autres données détaillées pour chaque occurrence, comme l'illustre la capture d'écran ci-dessous :



En plus des contrôles approfondis multifournisseurs, Nessus peut souvent détecter une infection par un programme malveillant qui peut venir d'une défaillance au niveau d'un programme antivirus (par exemple, le fait de ne pas recevoir les mises à jour de signatures) ou du fait qu'un éditeur donné assure une couverture différente par rapport à ses pairs.

Cette approche constitue un complément idéal au déploiement d'une stratégie antivirus mono-niveau voire multi-niveau, car les pirates tendent à créer spécialement des charges utiles malveillantes pour échapper à la détection. Par exemple, une société peut déployer des agents antivirus de « marque X » sur des ordinateurs de bureau. Les pirates peuvent être au courant et préparer (ou « emballer ») tout spécialement leur programme malveillant de façon à ce qu'il ne soit pas détecté par la « marque X ». Toutefois, avec une analyse Nessus, les valeurs de hachage ?? de tous les processus en cours d'exécution sont comparées à un index professionnel répertoriant toutes les empreintes numériques des programmes malveillants connus (plug-in 59275 : Malicious Process Detection - détection des processus malveillants). Cela permet d'effectuer une détection secondaire des programmes malveillants sans avoir à exécuter plusieurs agents antivirus.

En plus de l'index conséquent des programmes malveillants détectés par le plug-in 59275, Nessus fournit plusieurs plug-ins et méthodes supplémentaires de détection des programmes malveillants connus :

- En utilisant le plug-in « Malicious Process Detection: User Defined Malware Running » (ID 65548), vous pouvez ajouter des empreintes numériques supplémentaires issues de vos propres recherches ou de tierces parties.
- Reposant sur un rapport Mandiant ??, le plug-in « Malicious Process Detection: APT1 Software Running » (ID 64687) détecte une grande variété de programmes malveillants utilisés par une entité étrangère surnommée « APT1 » qui semble opérer à partir de la Chine. Il est complété par le plug-in « APT1-Related SSL Certificate Detected » (ID 64688) qui est capable de détecter les certificats SSL erronés connus.
- Après un cas récent de compromission, Tenable a créé le plug-in « Malicious Process Detection: Malware Signed By Stolen Bit9 Certificate » (ID 64788) afin de détecter tout programme malveillant signé par un certificat volé.

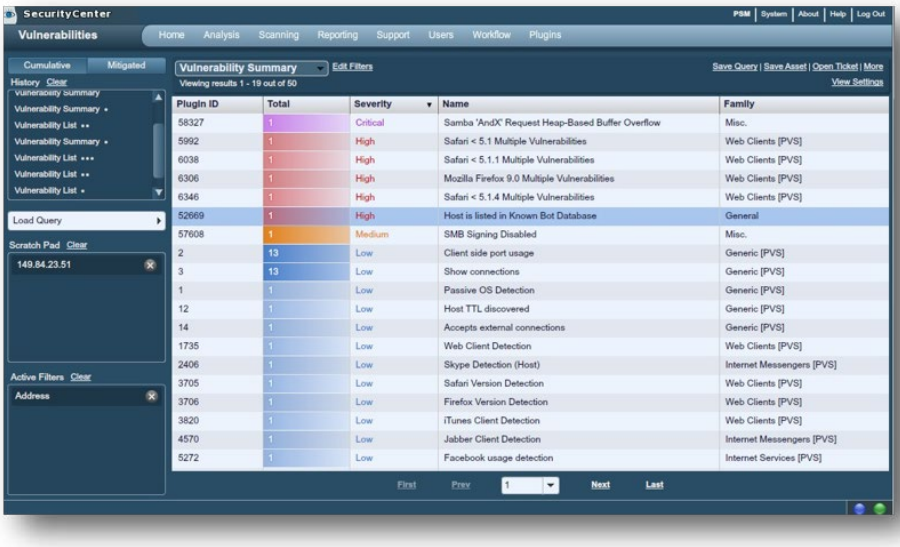
Nessus peut également détecter une grande variété de logiciels susceptibles d'enfreindre les politiques d'entreprise en comparant les processus en cours d'exécution à une liste de programmes douteux (plug-in 59641 : Malicious Process Detection: Potentially Unwanted Software).

Détection des réseaux de botnet

Grâce à un flux d'informations externe, Nessus offre plusieurs méthodes permettant de déterminer si un hôte fait partie d'un réseau de botnet actif. D'après les éditeurs de solutions de protection contre les programmes malveillants et de dépistage des réseaux de botnet, ces derniers représentent plusieurs millions d'hôtes sur Internet. Tout système faisant partie d'un réseau de botnet a été totalement infecté et constitue une menace sérieuse pour les entreprises. Grâce aux méthodes ci-dessous, Nessus peut souvent identifier les hôtes de ce type sur la base d'analyses de réputation et de contenu :

- Hôte répertorié dans la base de données des botnets connus (52669) : Nessus recherche l'adresse IP analysée dans une base de données contenant les adresses IP des réseaux de bots connus et signale toute occurrence trouvée.
- Liens de sites Web vers du contenu malveillant (52670) : tout en exécutant une analyse des applications Web, Nessus traite les listes d'URL externes pour rechercher toute correspondance avec la liste des noms DNS et sites Web connus qui sont associés à une activité de réseau de botnet.
- Connexion active à un hôte répertorié dans la base de données des botnets connus (58430) : Nessus évalue la liste des systèmes connectés pour déterminer si certains font partie d'un réseau de botnet connu. Ce contrôle nécessite des informations d'authentification ; il répertorie les connexions entrantes et sortantes avec les adresses IP de réseaux de botnet.
- Serveur DNS répertorié dans la base de données des botnets connus (58429) : comme pour le programme malveillant DNS Changer, si un système a été configuré avec une adresse IP DNS qui figure également sur la liste des réseaux de botnet connus, Nessus signale cette infection potentielle.

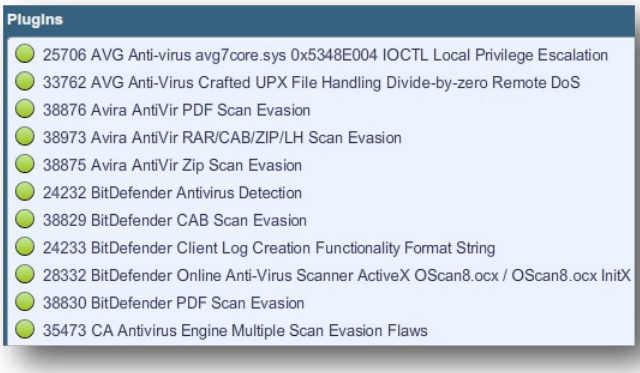
Il est important de réaliser que la détection des réseaux de botnet est totalement indépendante de tout dispositif antivirus, de détection des intrusions ou de mise en corrélation de type SIEM. Nessus dispose de toutes les informations dont il a besoin pour déterminer avec certitude si un système communique avec un réseau de botnet connu. La capture d'écran ci-dessous illustre une détection réelle par Nessus, telle qu'elle s'affiche lors de la consultation des résultats d'une analyse effectuée avec la solution SecurityCenter de Tenable :



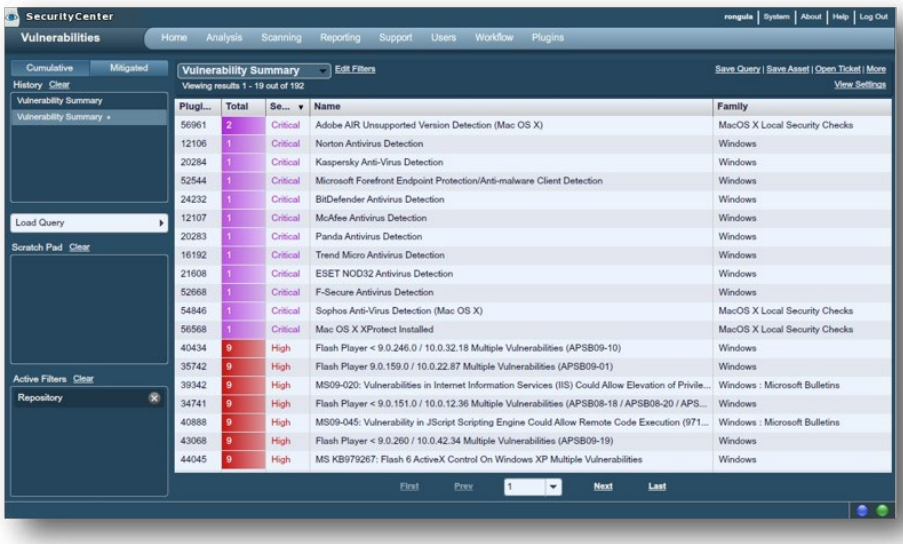
Dans ce cas, le plug-in Nessus 52669 s'est déclenché car l'adresse IP analysée figurait dans une base de données extrêmement fiable et pertinente de réseaux de botnet connus.

Audits des antivirus

Nessus dispose de plus de 100 plug-ins qui examinent les logiciels antivirus pour rechercher les vulnérabilités, ainsi que les signatures manquantes ou obsolètes. Cela concerne de nombreux éditeurs, dont Trend Micro, McAfee, ClamAV, Bitdefender, Kaspersky, ESET, F-Secure et bien d'autres encore. La possibilité de réaliser un audit des serveurs pour vérifier si les signatures antivirus sont mises à jour correctement offre un second niveau de protection à l'entreprise. La capture d'écran ci-dessous montre un exemple d'écran de création d'une politique d'analyse Nessus, qui permet de sélectionner des contrôles pour différents éditeurs de solutions antivirus de premier plan.



Liste partielle de plug-ins liés aux antivirus

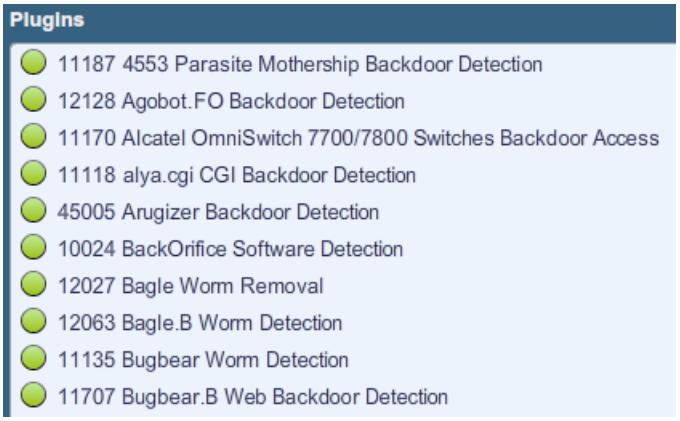


Nessus considère que les agents antivirus sans signature à jour présentent un niveau de gravité Critique.

En plus des plug-ins Nessus, Tenable propose 11 politiques d'audit que Nessus peut utiliser pour déterminer si le logiciel antivirus d'un éditeur donné est installé, exécuté et/ou configuré de manière à se lancer après le démarrage du système. Ces contrôles permettent de s'assurer que n'importe quel type de programme antivirus à l'échelle du réseau fonctionne correctement et offre le niveau de défense approprié.

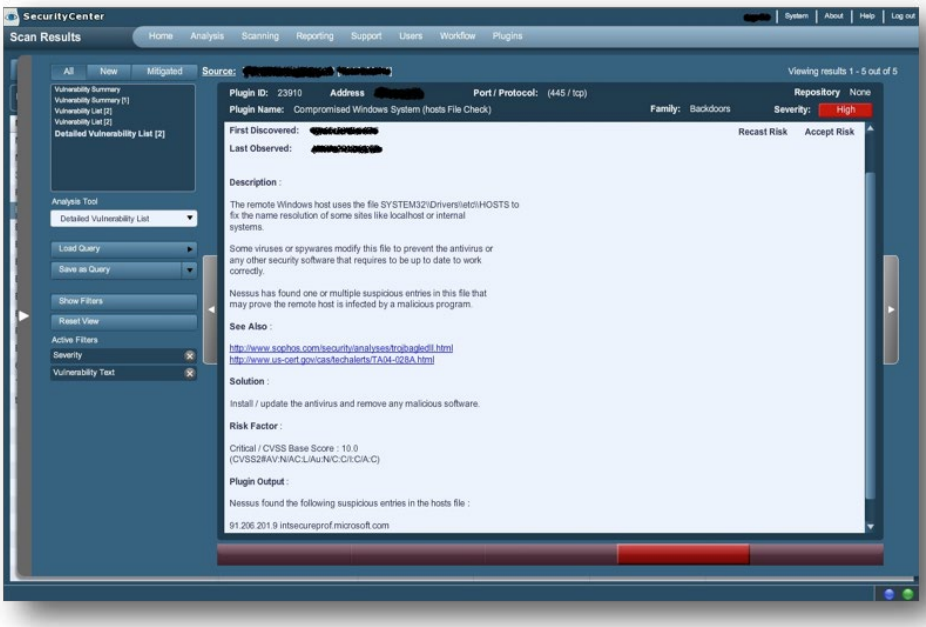
Portes dérobées et comptes par défaut

L'une des familles de plug-ins Nessus facilitant la détection des programmes malveillants est appelée « **Backdoors** » (Portes dérobées). Les différents plug-ins disponibles dans cette famille recherchent les portes dérobées et les logiciels publicitaires connus, ainsi que certaines infections notoires telles que Conficker, Stuxnet et Zeus. Dans la mesure du possible, Nessus tente de détecter à distance la présence de ces types de programmes malveillants. Certains des plug-ins sont conçus de telle manière qu'une authentification est nécessaire pour que Nessus accède aux fichiers sur un système (par exemple, 'hosts') afin de détecter tout signe de compromission ou de programme malveillant. Par ailleurs, Nessus peut détecter certains rootkits (par exemple, D13HH et wh00t) via la présence de comptes par défaut laissés pour un accès ultérieur.



Liste partielle de plug-ins de la famille Backdoors (Portes dérobées)

La capture d'écran ci-dessous présente une occurrence trouvée par le plug-in Nessus 23910 qui analyse le contenu d'un fichier « hosts » Windows pour vérifier s'il a été modifié de manière à intégrer un contenu suspect :



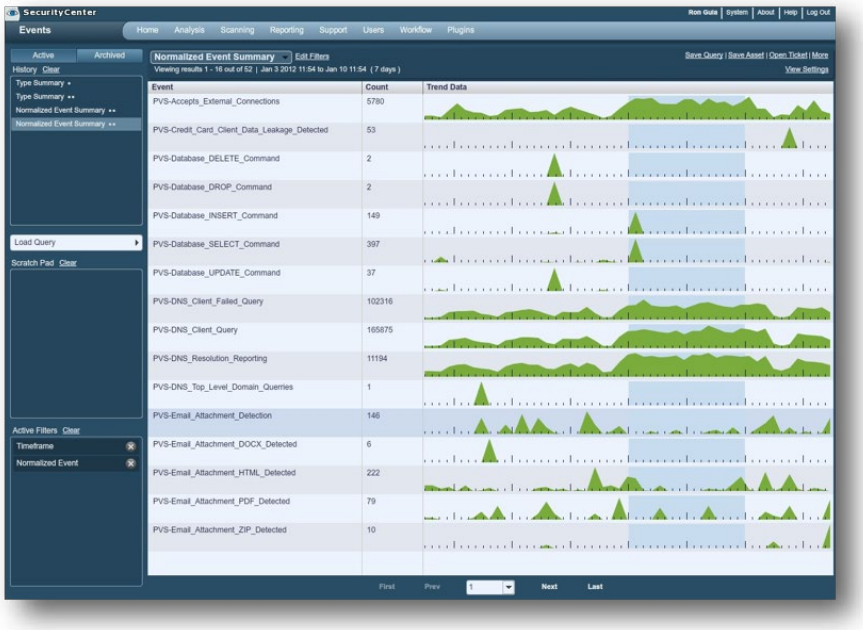
Trafic en temps réel et surveillance des systèmes

Pour renforcer la lutte contre les programmes malveillants, Tenable propose deux solutions, Passive Vulnerability Scanner et Log Correlation Engine, qui sont axées sur la surveillance du réseau et des événements système.

La solution Passive Vulnerability Scanner (PVS) est conçue pour analyser passivement le trafic réseau afin de rechercher un large éventail d'événements et de vulnérabilités. Sont notamment concernés l'exploration des fichiers, les recherches DNS, les protocoles logiciels utilisés, les agents utilisateurs de navigateurs Web, les violations potentielles de politiques et bien plus encore. Grâce à tous ces événements collectés, PVS peut vous aider à déterminer la présence ou l'étendue d'une infection par un programme malveillant. La solution Log Correlation Engine (LCE) peut collecter et prendre en charge un nombre incroyable de journaux générés par chacun des systèmes présents sur un réseau. LCE peut mettre en corrélation ces entrées de journaux pour en faire un outil utile à la compréhension des activités des utilisateurs ou des programmes malveillants sur le réseau.

Consignation des activités réseau

PVS consigne tout type de trafic en vue d'une analyse approfondie et de l'émission d'alertes. La capture d'écran ci-dessous indique les différents types de flux de trafic réseau en temps réel qui sont ensuite consignés vers LCE :



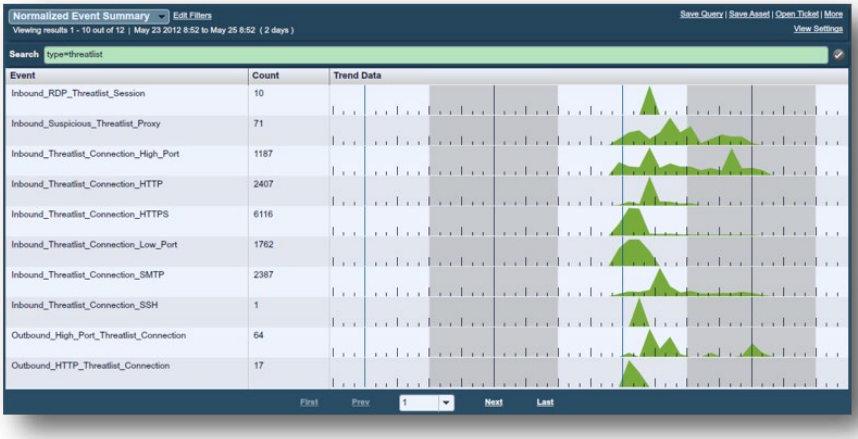
La conversion des sessions réseau en journaux exploitables présente d'immenses avantages pour l'analyse des infections par des programmes malveillants :

- Elle fournit la preuve de la présence d'infections.
- Elle permet de compléter les journaux de détection des intrusions avec une véritable analyse approfondie du trafic réseau.
- Elle offre un accès aisé aux sites Web, aux requêtes DNS exécutées et aux certificats SSL utilisés dans un échange.
- Tous les transferts de fichiers via SMB, NFS, FTP et d'autres protocoles à l'intérieur et à l'extérieur du réseau sont consignés dans des journaux.
- Ces journaux sont mis en corrélation avec les ID utilisateur réseau internes, qu'ils s'agissent de terminaux mobiles ou de systèmes dans des environnements DHCP dynamiques.

Consignation des activités des réseaux de botnet

LCE met en corrélation les journaux d'intrusions, les événements liés au pare-feu, aux connexions, à NetFlow, à l'authentification et les journaux PVS en temps réel avec une liste extrêmement précise d'adresses IP de réseaux de botnet. La solution émet des alertes sur la base du sens et du type de la connexion. De cette manière, les entreprises peuvent savoir quand elles font l'objet d'un balayage par des réseaux de botnet malveillants et quand un serveur interne entre en contact avec un site de réseau de botnets.

La capture d'écran ci-dessous présente des événements de réseaux de botnets collectés par LCE :



LCE identifie les événements de réseaux de botnets avec le terme « threat list ». Dans la capture d'écran ci-dessus, il existe diverses connexions réseau, y compris d'applications reconnues telles que RDP (Windows Remote Desktop), en provenance d'adresses IP connues pour leur appartenance à un réseau de botnets.

Consignation des processus système

LCE collecte également des journaux issus des systèmes Windows et Linux, et notamment sur l'exécution d'applications sur ces systèmes.

La collecte des données d'application de l'ensemble de l'entreprise se révèle utile pour l'analyse approfondie des systèmes infectés. LCE peut également utiliser ces données pour réaliser une synthèse et générer des alertes lorsque certaines conditions clés sont réunies, notamment :

- Lorsqu'un système exécute un nouveau fichier exécutable pour la première fois
- Lorsqu'un nouveau fichier exécutable est exécuté sur le réseau pour la première fois
- Lorsqu'un fichier exécutable connu est exécuté selon une nouvelle

méthode pour la première fois Tous ces événements peuvent potentiellement être associés à des infections virales.

Par exemple, si Nessus détecte un programme malveillant s'exécutant sous la forme d'un processus appelé 1738d.exe, LCE offre la possibilité de rechercher ce nom de processus dans les journaux d'événements de chaque système. Une requête de ce genre permet d'avoir une bonne idée de l'étendue de l'infection.

Mieux encore, LCE peut interroger les journaux pour rechercher les erreurs, les comportements de connexion inhabituels, les insertions de périphériques USB et d'autres événements liés au système infecté. Avec quelques requêtes rapides, il est souvent possible d'isoler l'endroit où le programme malveillant a trouvé prise sur le réseau pour la première fois et de savoir où il s'est propagé.

Conclusion

Il est essentiel de déployer un logiciel de protection contre les programmes malveillants dans l'ensemble de l'entreprise afin de garantir un niveau de sécurité de base. Quel que soit l'éditeur, ce type de logiciel n'est pas infaillible. Les entreprises doivent accepter le fait qu'une infection sera inévitable. L'utilisation des composants de la suite USM de Tenable procure un second niveau de validation et de protection. Plus important encore, il est de plus en plus vital d'inclure plusieurs niveaux de protection contre les programmes malveillants dans la stratégie de sécurité de l'entreprise.

A propos de Tenable Network Security

Tenable Network Security, leader de la surveillance unifiée de la sécurité, est à l'origine de l'analyseur de vulnérabilités Nessus et le créateur de solutions professionnelles sans agent pour la surveillance continue des vulnérabilités, des faiblesses de configuration, des fuites de données, de la gestion des enregistrements et de la détection des compromissions, et ce afin d'assurer la sécurité des réseaux et la conformité aux réglementations FDCC, FISMA, SANS CAG et PCI. Les produits primés proposés par Tenable sont utilisés par de nombreuses entreprises figurant parmi les 2 000 plus grandes firmes internationales, ainsi que par de nombreuses administrations afin de minimiser les risques liés au réseau de façon proactive. **Pour plus d'informations, visitez le site** http://www.tenable.com/.

SIÈGE INTERNATIONAL

Tenable Network Security
Corporate Head office
amer@tenable.com
+1.410.872.0555

EMEA Head office
emea@tenable.com
+44 (0)203.178.4247

APAC Head Office
apac@tenable.com

www.tenable.com

tenable™ network security