COMMUNIQUÉ DE PRESSE **18 mars 2014**

OPERATION WINDIGO : Plus de 500 000 ordinateurs infectés chaque jour par 25 000 serveurs UNIX piratés par un cheval de Troie

Les Pavillons-sous-Bois, le 18 mars 2013

L'équipe de chercheurs en sécurité d'ESET®, en collaboration avec le CERT-Bund (Allemagne), l'agence nationale suédoise de recherche sur les infrastructures réseau (SNIC) et d'autres agences en sécurité, ont découvert une vaste campagne d'attaques cybercriminelles qui a pris le contrôle de plus de 25 000 serveurs UNIX dans le monde entier.

Baptisée « Windigo » par les experts en sécurité informatique cette campagne d'une ampleur inédite a généré l'envoi de millions de pourriels par les serveurs infectés. Le piratage de ces serveurs n'est en réalité que la 1ère étape de cette opération complexe qui a pour finalité l'infection et le vol d'information des ordinateurs qui s'y connectent.

Parmi les victimes de Windigo, on compte notamment cPanel et Kernel.org.

L'équipe d'experts en sécurité d'ESET qui a mis à jour cette vaste campagne publie aujourd'hui un document technique détaillé présentant leur découverte ainsi qu'une analyse du malware. Ce document donne également la marche à suivre pour détecter si votre infrastructure est infectée et indique la procédure permettant de supprimer le code malveillant.

OPERATION WINDIGO : 3 ANNEES SOUS LES RADARS DES EXPERTS

Malgré la détection parcellaire de Windigo par certains experts en sécurité, cette vaste campagne cybercriminelle, en raison de son ampleur et de son architecture complexe, est parvenue à déjouer la vigilance de la communauté d'experts.

« Depuis 2 ans et demi, Windigo s'est renforcé en prenant le contrôle de 10 000 serveurs, sans être détecté par la communauté d'experts en sécurité » constate Marc-Etienne Léveillé, chercheur en sécurité chez ESET. « Plus de 35 millions de pourriels sont envoyés chaque jour à d'innocentes victimes, encombrant leur boîte de réception et menaçant la sécurité de leur ordinateur. Pire encore, chaque jour, plus d'un demi-million d'ordinateurs sont menacés par la simple visite d'un site Internet dont le serveur est infecté. L'internaute est alors redirigé vers des malwares ou des annonces publicitaires. »

Il est intéressant de noter que la menace varie en fonction du système d'exploitation de l'utilisateur. Ainsi, pour un ordinateur sous Windows visitant un site infecté, Windigo, tente d'installer un malware via un kit d'« exploit ». En revanche, Windigo affiche des publicités de sites de rencontres pour les utilisateurs sous MAC OS. Les possesseurs d'iPhone, quant à eux, sont redirigés vers des contenus pornographiques.

APPEL AUX ADMINISTRATEURS SYSTEMES POUR ERADIQUER WINDIGO

Plus de 60% des sites Internet à travers le monde sont hébergés sur un serveur Linux. C'est pourquoi l'équipe de chercheurs en sécurité d'ESET lance un appel aux webmasters et administrateurs systèmes pour qu'ils s'assurent que leurs serveurs n'aient pas été compromis.

« Nous sommes conscient que les webmasters et les équipes techniques ont déjà leurs propres problèmes à gérer sans avoir à rajouter une charge de travail supplémentaire, mais Windigo pose une réelle menace. Tout le monde souhaite contribuer à un Internet meilleur. Vous avez à présent l'occasion d'y prendre part en protégeant de manière très concrète des millions d'internautes. » déclare Marc-Etienne Léveillé.
« Face à une telle menace, ne rien faire c'est contribuer à l'expansion du malware et des pourriels. Quelques minutes de votre temps peuvent concrètement faire la différence. »

COMMENT SAVOIR SI VOTRE SERVEUR EST INFECTE PAR WINDIGO

Cette campagne a été surnommée « Windigo » par les chercheurs en sécurité d'ESET en référence à la créature maléfique et cannibale de la mythologie des Amérindiens algonquiens.

ESET recommande aux administrateurs systèmes sous UNIX et aux webmasters d'exécuter la ligne de commande suivante afin de vérifier l'intégrité de leur système :

```
$ ssh -G 2>&1 | grep -e illegal -e unknown > /dev/null && echo "System clean" || echo "System infected"
```

UN TRAITEMENT DE CHOC POUR LES VICTIMES DE WINDIGO

« En réalité, la backdoor (porte dérobée) "Ebury" propagée par la campagne de cybercriminalité Windigo n'exploite pas une vulnérabilité de Linux ou d'OpenSSH » poursuit Marc-Etienne Leveillé. « Elle est installée manuellement par les cybercriminels. Le fait qu'ils aient réussi à répliquer cette attaque sur des dizaines de milliers de serveurs différents est tout simplement effrayant. Si les solutions anti-virus et d'authentification forte sont désormais largement répandues sur les postes de travail, elles sont en revanche rarement employées pour protéger les serveurs. Ils sont, par conséquent, une cible vulnérable pour le vol d'identifiants et le déploiement de logiciels malveillants. »

Si les administrateurs systèmes constatent que leurs serveurs sont infectés, il est alors recommandé de formater les machines concernées et réinstaller les systèmes d'exploitation et les logiciels. La sécurité des accès étant compromise, il est également essentiel de changer tous les mots de passe et clés privées.

Il est recommandé d'intégrer des solutions d'authentification forte pour garantir un meilleur niveau de protection.

« Nous sommes conscients que formater votre serveur et repartir de zéro est un traitement radical. Mais, si des hackers sont en possession d'un accès distant à vos serveurs suite au vol de vos identifiants administrateur, il ne faut prendre aucun risque. » explique Marc-Etienne Leveillé. « Malheureusement, certaines victimes avec qui nous sommes en contact savent qu'elles sont infectées mais n'ont pour l'instant rien fait pour nettoyer leurs systèmes mettant ainsi en danger toujours plus d'internautes. »

Enfin, ESET rappelle qu'il ne faut jamais choisir ou réutiliser un mot de passe facile à casser.

PLUS D'INFORMATIONS

ESET a publié les détails de son enquête sur la campagne cybercriminelle Windigo et les nombreux logiciels malveillants composant cette menace.

Retrouvez le rapport d'enquête complet sur : welivesecurity.com/windigo

Pour suivre l'évolution de l'affaire sur Facebook, Google+ et Twitter, utilisez le hashtag **#windigo**

À propos d'ESET

Fondée en 1992, la société ESET est spécialisée dans la conception et le développement de logiciels de sécurité pour les entreprises et le grand public. Pionnier en matière de détection proactive des menaces véhiculées par l'Internet depuis 26 ans, ESET est aujourd'hui l'un des leaders dans ce domaine. En obtenant la 81ème récompense VB100 en août 2013, ESET NOD32 Antivirus détient le record mondial pour le nombre de récompenses Virus Bulletin (VB100), et n'a jamais manqué un seul ver ou virus « In-the-Wild » depuis le début des tests en 1998. ESET a été reconnue comme l'une des entreprises les plus innovantes en Europe pour 2011 au titre des HSBC European Business Awards et a été primée maintes fois par les laboratoires AV-Comparatives, AVTest et bien d'autres encore.
ESET NOD32, ESET Smart Security et ESET Cybersecurity pour Mac sont reconnus et appréciés par des millions d'utilisateurs dans le monde.
ESET a son quartier général à Bratislava (Slovaquie), possède des filiales à San Diego (U.S.), Buenos Aires, et Singapour et des bureaux à Jena (Allemagne), Sao Paulo et Prague. Ses centres de recherche sont établis à Bratislava, San Diego, Buenos Aires, Singapour, Prague, Košice (Slovaquie), Cracovie (Pologne), Montréal et Moscou. ESET est également représenté dans plus de 180 pays à travers un réseau de partenaires.

À propos d'Athena Global Services

Créée en 1997, ATHENA Global Services est une entreprise indépendante spécialisée dans la distribution de logiciels de sécurité informatique.

À travers un vaste réseau de distribution, constitué de VAR, revendeurs locaux professionnels et des plus importantes enseignes spécialisées dans la distribution de logiciels, Athena Global Services propose des logiciels et équipements de sécurité novateurs destinés aux particuliers et aux entreprises, pour protéger et gérer leur environnement informatique : antivirus, pare-feu, chiffrement, politique de sécurité, authentification, sauvegarde, migration des données, et contrôle du trafic Internet.
En outre, ATHENA Global Services propose une gamme de logiciels utilitaires également dédiés à la protection et à l'optimisation des parcs informatiques. Grâce à son savoir-faire, ATHENA Global Services entretient des relations privilégiées avec les éditeurs mondiaux qui lui confient la localisation et la distribution de leurs logiciels.

Ses principaux partenaires éditeurs de solutions de sécurité :
DeviceLock - ESET Antivirus - StorageCraft - SMSPasscode - 8Man - WhiteCanyon - EndSec Cloud Services - MDM

Ainsi que ses filiales Africa Global Services - Auxiliance - Marketing Land

Pour en savoir plus, veuillez visiter le site Internet : www.athena-gs.com

Contacts Presse Athena Global Services
François Groussard – francois.g@eset-nod32.fr - 01 55 89 09 22
Marion Lecrique - marion.l@athena-gs.com - 01 55 89 09 60