Le malware XOR.DDoS utilise la force brute pour contrôler les systèmes Linux

	Le malware XOR.DDoS utilise la force brute pour contrôler les systèmes Linux

L'éditeur de sécurité FireEye a identifié deux autres versions du malware XOR.DDoS découvert en septembre 2014. Faisant partie d'une famille de logiciels malveillants particulièrement sophistiqués, il a la particularité de cibler différents systèmes Linux sous architectures x86 et ARM.

Les systèmes Linux sont toujours sous pression. Une dizaine de jours après l'alerte de Qualys portant sur la découverte de la faille « Ghost » relative à la librairie GNU C (http://www.lenetexpert.fr/une-faille-critique-permet-de-prendre-le-controle-des-routeurs-des-nas-des-systemes-linux), c'est au tour du spécialiste en sécurité FireEye de tirer la sonnette d'alarme. Cette fois au sujet d'un malware conçu pour cibler les systèmes Linux, incluant les terminaux à base d'architecture ARM et utilisant un noyau rootkit sophistiqué qui présente une grande menace.
Connu sous l'appellation XOR.DDoS et découvert une première fois en septembre par des chercheurs de Malware Must Die, ce cheval de Troie a depuis évolué et de nouvelles versions se sont retrouvées dans la nature depuis le 20 janvier selon un rapport publié vendredi par FireEye qui a analysé en détail cette menace.
XOR.DDOS est installé sur des systèmes cibles via des attaques SSH par force de brute lancées principalement depuis des adresses IP émanant d'une société hong-kongaise appelée Hee Thai Limited. Ces attaques essaient de deviner le mot de passe de démarrage en usant de différentes techniques basées sur des dictionnaires et des listes de mots de passe issues de précédentes violations de données. FireEye a observé plus de 20 000 tentatives de login SSH par serveur visé en 24 heures et plus d'1 million par serveur entre mi-novembre 2014 et fin janvier 2015.
Lorsque les attaquants tentent de deviner le mot de passe de démarrage, ils envoient une commande SSH complexe à distance pouvant parfois atteindre plus de 6 000 caractères, qui se compose de plusieurs commandes shell séparées. Ces commandes téléchargent et exécutent différents scripts dans le cadre d'une chaîne d'infection sophistiquée s'appuyant sur un système de construction de malware à la demande. L'utilisation de commandes SSH distantes est significative car OpenSSH ne liste pas de telles commandes « même lorsque la connexion est configurée dans la plus verbeuse de ses configurations », ont indiqué les chercheurs de FireEye. « Comme une commande distante ne créé par de terminal session, les systèmes de connexion TTY ne retiennent pas non plus ces événements, pas plus que les dernières commandes de logs ».
Cette infrastructure à la demande de construction sophistiquée d'automatisation de création de rootkits LKM s'appuie sur différents noyaux et architectures, sachant que les architectures de chaque Loadable Kernel Modules (LKM) doivent être compilées pour le noyau particulier sur lesquel il est prévu de tourner. « Contrairement à Windows qui dispose d'une API noyau stable permettant de créer du code qui est portable entre différentes versions de noyaux, le noyau Linux ne dispose pas d'une telle API », expliquent les chercheurs de FireEye. « Comme les changements internes de noyau changent d'une version à une autre, un LKM doit être binairement compatible avec le noyau ».

Chiffrer les serveurs SSH et désactiver le démarrage de comptes à distance
L'objectif de ce rootkit est de cacher des processus, des fichiers, et des ports associés avec XOR.DDoS. « Contrairement à des attaques DDoS typiques de robots, XOR.DDoS est l'une des familles de malware les plus sophistiquées ciblant les OS Linux », a précisé FireEye. « Il est également multi-plateformes avec du code source C/C++ pouvant être compilé pour cibler x86, ARM et d'autres plateformes ». XOR.DDoS peut également télécharger et exécuter des fichiers binaires arbitraires lui donnant la capacité de se mettre tout seul à jour.
FireEye a identifié jusqu'à présent deux versions majeures de XOR.DDoS, le second ayant été repéré fin décembre. Le nombre de systèmes accessibles via SSH et utilisant des mots de passe faibles pouvant être vulnérables à des attaques par force brute complexe comme celles utilisées par les pirates derrière XOR.DDoS, pourrait être très élevé. Pour éviter d'être une cible trop facile, il faut absolument veiller à ce que les serveurs SSH soient configurés pour utiliser des clés de chiffrement au lieu de mots de passe pour l'authentification, et la connexion à distance pour démarrer des comptes devrait être désactivée, a précisé FireEye. « Particuliers et utilisateurs en PME peuvent installer l'utilitaire fail2ban qui fonctionne avec iptables pour détecter et bloquer les attaques par force brute ».

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.lemondeinformatique.fr/actualites/lire-le-malware-xorddos-utilise-la-force-brute-pour-controler-les-systemes-linux-60175.html
Par Dominique Filippone avec IDG News Service