Le ransomware CryptoWall donne la migraine aux forces de l’ordre

	Le #ransomware CryptoWall donne la migraine aux forces de l’ordre

Bâti sur un labyrinthe de serveurs proxy, ce botnet est, pour l'instant, difficile à neutraliser. Pour se protéger, il faut faire des sauvegardes, mais pas n'importe comment.

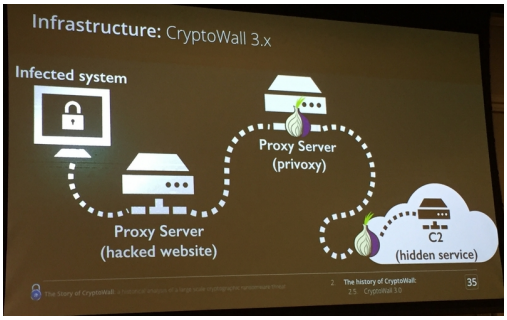
C'est l'un des plus importants « rançongiciels » du moment, et il le sera certainement encore pour un bout de temps. Car les pirates qui se cachent derrière ce néfaste malware ont mis en place un système pour l'instant assez inviolable et diaboliquement efficace. Bienvenue dans l'univers de CryptoWall.

Le chercheur en sécurité Yonathan Klijnsma de la société Fox IT est l'un de ceux qui essayent de pister ses auteurs. Il a profité de la conférence Botconf 2015, qui se déroule actuellement à Paris, pour présenter ses dernières analyses.

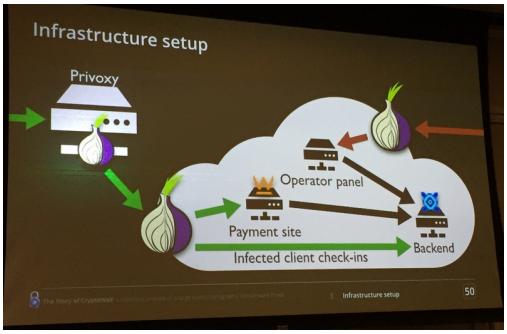
GK — Yonathan Klijnsma

Sur le principe, CryptoWall — qui existe actuellement dans sa version 4.0 — n'a rien d'original. Apparu pour la première fois en novembre 2013, ce code malveillant fonctionne un peu comme son aïeul Cryptolocker. Il infecte les ordinateurs et chiffre les fichiers qui s'y trouvent, ainsi que les noms de ces fichiers. Pour cela, il s'appuie sur les algorithmes AES 256bit et RSA 2048bit. Pour avoir une chance de récupérer ses données, il faut passer à la caisse. Plusieurs moyens de paiement sont acceptés : bitcoin, litecoin, UKash, moneypak, paysafecard, etc.
Ce qui rend ce malware si difficile à terrasser, c'est son infrastructure sous-jacente, composée d'une multitude de serveurs proxy en cascade, des intermédiaires qui servent essentiellement à brouiller les pistes. *« C'est un vrai labyrinthe. On ne sait jamais si la ressource que l'on a détectée est le véritable serveur de commande et contrôle, ou simplement un autre proxy »*, explique Yonathan Klijnsma.

Autre subtilité : le premier niveau de proxy est constitué de serveurs Web piratés. *« Ce sont de vrais sites totalement légitimes. Les propriétaires, évidemment, ne savent pas que leurs serveurs ont été détournés par des pirates. C'est assez malin de leur part, car cela complique le démantèlement du botnet. On ne peut pas simplement tirer le cordon. Il faut contacter chaque administrateur un par un »*, souligne le chercheur en sécurité.



© DR



© DR

Derrière le serveur Web piraté se trouve un autre proxy qui va faire le lien avec le réseau d'anonymisation Tor, dans lequel les pirates ont planqué toute leur infrastructure d'administration : les clés de chiffrement, le paiement, la diffusion de malware, etc. Tous ces « services » sont créés sous la forme de services Tor cachés (Tor Hidden Service). *« Pour les forces de l'ordre, c'est techniquement très difficile d'identifier les serveurs qui se cachent derrière »*, souligne Yonathan Klijnsma.
Pour avoir une chance de démanteler le réseau, il faut donc utiliser des méthodes d'investigation plus classiques, par exemple en infiltrant des forums de discussion. Mais cette méthode prend du temps et n'est pas forcément couronnée de succès.

Pour l'instant, ce cyberracket constitue donc quasiment le crime parfait. Les auteurs sont tellement insouciants qu'ils n'hésitent pas à se moquer ouvertement de leurs victimes, en les félicitant — sur l'un des écrans d'alerte — d'avoir rejoint *« la grande communauté CryptoWall »*.

Un malware d'origine russe ?

Certains éléments techniques semblent indiquer que les auteurs de CryptoWall — ou une partie d'entre eux — se trouvent en Russie. Un mécanisme dans le code évite, en effet, qu'il ne s'installe sur des ordinateurs qui se trouvent en Russie, en Biélorussie, en Ukraine ou au Kazakhstan. Ce type d'exception est typique pour des cybercriminels qui ne souhaitent pas avoir de problèmes avec les forces de l'ordre locales. *« En même temps, on ne peut jamais être sûr à 100 %. Cela pourrait être un faux indice »*, ajoute le chercheur.
En tant qu'utilisateur, pour se prémunir contre un fléau tel que CryptoWall ou consorts, le mieux c'est de faire des sauvegardes régulières de ses fichiers. Mais attention : pas n'importe comment. Il faut éviter les sauvegardes automatiques sur un disque en réseau sur lequel l'ordinateur est connecté en permanence. *« Dans ce cas, le malware ne va pas seulement chiffrer le contenu de l'ordinateur, mais aussi les sauvegardes »*, explique le chercheur. L'idéal, c'est donc de faire des sauvegardes régulières, mais à la main.

Réagissez à cet article
Source : http://www.01net.com/actualites/cryptowall-le-ransomware-qui-donne-la-migraine-aux-forces-de-l-ordre-934345.html
Gilbert KALLENBORN