La menace des rançongiciels s'est intensifiée en 2016

written by Françoise Laugée | 16 mai 2017

Infectant un système bancaire aussi bien qu'un téléviseur connecté, les rançongiciels (*ransomwares*) s'immiscent partout. À tel point que ces logiciels malveillants (*malwares*) ont marqué l'année 2016 pour ce qui concerne le piratage informatique, selon certains experts en cybersécurité, qui avaient du reste annoncé ce phénomène.

Apparus dans les années 1990 sous la forme d'une fenêtre invitant à acheter un logiciel anti-virus, les rançongiciels permettent de prendre le contrôle d'un équipement informatique, en cryptant toutes les données qu'il contient, avec pour objectif d'obtenir une rançon en échange de la clé de déchiffrement. Des millions d'attaques dues à des virus comme Petya, Locy ou Cerber, transmis par courriel ou en cliquant sur un lien, affectent les particuliers comme les entreprises : 43 % visent le monde du travail en 2016 contre 99 % le grand public un an auparavant, d'aprés l'américain Symantec. Au troisième trimestre 2016, une entreprise était touchée toutes les 40 secondes à l'échelle de la planète, selon Kaspersky Lab, qui a dénombré pas moins d'une soixantaine de familles inédites de logiciels malveillants pour l'année entière. McAfee Labs annonce, quant à lui, 1,3 million nouveaux rançongiciels au deuxième trimestre 2016, et plus de 7 millions d'exemplaires en circulation pendant cette période. Le montant de la rançon demandée atteint en moyenne 300 dollars. Parfois beaucoup plus, comme l'a révélé l'affaire d'une clinique située en Californie qui a dû se résoudre à verser 17 000 dollars en *bitcoins* pour reprendre la main sur ses ordinateurs et la totalité de leurs fichiers. L'anonymat des transactions avec les cryptomonnaies encouragerait les malfaiteurs. Logiciels malveillants les plus répandus, les rançongiciels sont aussi *« les plus rentables de l'histoire de la cybercriminalité »*, observe la société Cisco System.

En France, les rançongiciels constituent la forme d'attaque informatique la plus répandue : 80 % des entreprises déclarent en avoir été victimes en 2016, contre 61 % un an auparavant, selon le Cesin (Club des experts de la sécurité de l'informatique et du numérique) qui regroupe les responsables de la sécurité informatique de 280 entreprises françaises. Plutôt bien équipées pour lutter contre le piratage informatique, elles utilisent en moyenne chacune une dizaine d'outils différents. Néanmoins, l'efficacité de leurs mesures de protection dépend notamment de leur cohérence ainsi que de la qualité de la maintenance des systèmes mis en place, devenus très complexes et coûteux, notamment pour les PME, avec le développement des terminaux mobiles, de l'informatique en nuage et des objets connectés.

Pour Intel Security, le nombre des attaques par rançongiciels devrait toutefois décliner au cours du second semestre 2017 grâce aux progrès effectués dans le domaine de la cybersécurité, mais cette forme de piratage va s'étendre davantage encore avec les smartphones. De même, la multiplication des objets connectés comportant des failles de sécurité (voir *La rem* n°40, p.27) laisse présager un bel avenir à la piraterie informatique, notamment au *drone-jacking*, (détourner un drone). *« Le phénomène continue de grossir et choisit ses victimes avec plus de précisions »*, prévient Steven Wilson, chef du centre européen de lutte contre le crime en ligne au sein d'Europol. Sur le *darknet* (voir *La rem* n°33, p.63), la vente de rançongiciels est un commerce profitable rémunéré à la commission prélevée sur la rançon obtenue. Pour Trend Micro, spécialiste japonais de cybersécurité, la moitié des entreprises françaises accepte de payer une rançon – en moyenne de 638 euros et pour un quart dépassant 1 000 euros –, mais seulement un tiers d'entre elles récupère effectivement leurs données. Toutefois, tous les spécialistes conseillent de ne pas céder au chantage.

Parmi les équipements numériques touchés par l'épidémie de rançongiciels, sont concernés désormais les téléviseurs connectés, susceptibles d'être infectés par les mêmes virus que ceux qui attaquent les smartphones. De nombreux cas ont été recensés en Asie, où le taux d'équipement en *smart tv* est important.

Une histoire relatée sur Twitter par un ingénieur en informatique américain est éloquente. En décembre 2016, un téléviseur connecté de la marque LG, appartenant à l'un de ses proches, s'est trouvé bloqué sur la page d'accueil du logiciel rançonneur Cyber.Police (nommé également Flocker, Frantic Locker ou Dogspectus) au cours du visionnage d'un film sur un site de *streaming*. Sans pouvoir déterminer si l'attaque était survenue par le biais de la plate-forme ou si elle provenait d'un site tiers, l'ingénieur n'est pas parvenu à réinitialiser l'appareil pour en effacer toutes les données. En l'absence d'instructions fournies par le fabricant pour faire redémarrer le téléviseur connecté, le service client LG l'a renvoyé vers un service spécialisé facturant son intervention 340 dollars, tandis que la rançon demandée était de 500 dollars ! L'ingénieur a finalement communiqué sur internet la procédure à suivre que le fabricant coréen s'est résolu à lui indiquer. Éradiquer un rançongiciel, constatent les experts de Symantec, se révèle être une opération beaucoup plus complexe sur un téléviseur connecté que sur un smartphone ou un ordinateur.

En décembre 2016, la Malware Hunter Team, qui rassemble des chercheurs en cybersécurité du monde entier, a révélé l'existence d'un rançongiciel d'un genre nouveau. Baptisé Popcorn Time (sans rapport avec le logiciel pirate de *streaming*, voir *La rem* n°37, p.54), ce virus permet un double chantage qui invite à sa prolifération : soit payer un *bitcoin* de rançon

(environ 736 euros), soit transmettre le lien infecté à au moins deux internautes de son entourage. Selon la seconde option, la victime ne récupérera ses données qu'à la condition que les deux autres paient dans le délai imposé. Cette méthode inédite est qualifiée par les pirates eux-mêmes de *« méthode sale »*, sachant que les victimes successives peuvent elles-mêmes choisir de passer leur tour… En outre, dans leur grande malveillance, les pirates n'accordent que quatre essais pour saisir la longue série de chiffres et de lettres qui sert à débloquer le système, les données étant effacées au-delà.

La Malware Hunter Team alerte également sur le fait que les pirates créateurs du virus Popcorn Time se présentent indûment comme un groupe d'étudiants syriens en quête d'argent pour venir en aide aux habitants d'un État oublié aux yeux du monde. La parole des pirates n'est jamais d'or, insiste le groupe de chercheurs qui confirme qu'il ne faut ni payer la rançon ni transmettre le lien infecté. *« L'exploitation de chaîne (comme la chaîne de Ponzi) est une des dérives à laquelle il fallait s'attendre en tant qu'alternative à la rançon. Participer à la diffusion du* ransomware *et infecter ses connaissances est finalement pire que de payer la rançon. La cybercriminalité expérimente ainsi l'affiliation sous une forme inédite par la corruption des victimes et par la menace. Ce nouveau type de diffusion est, il faut le reconnaître, assez malin »*, explique Régis Bénard, consultant chez Vade Secure. En décembre 2016, plus de 160 rançongiciels sont listés sur le site ID Ransomware.

Début décembre 2016, la plate-forme Avalanche, active depuis 2009 et fournissant des outils numériques en tout genre aux cybercriminels, notamment une large gamme de logiciels malveillants dont des rançongiciels, a été démantelée à la suite de quatre années d'une enquête menée conjointement par Europol, la police allemande et le FBI. Avalanche enrôlait chaque jour environ un demi-million de machines, à l'insu de leurs utilisateurs. Pour parvenir à leurs fins, les enquêteurs ont réussi à rediriger le trafic entre les ordinateurs infectés et les serveurs utilisés par les criminels vers des serveurs administrés par la police, une technique appelée *« sinkholing »*. Résultat : 37 sites ont été perquisitionnés, 39 serveurs saisis, 221 autres mis hors ligne et cinq personnes arrêtées.

La forte croissance de la piraterie informatique rappelle que la France manque d'experts en cybersécurité. À l'occasion du Forum international de la cybersécurité (FIC) qui s'est tenu en janvier 2017 à Lille, le groupe Orange a inauguré son second centre consacré à la cyberdéfense, qui abrite un centre de formation professionnelle et initiale. Réalisant un chiffre d'affaires de 250 millions d'euros dans cette activité en croissance d'au moins 20 % par an, l'opérateur télécoms a annoncé son ambition de devenir *« l'un des leaders européens du secteur »*, et le recrutement de 200 spécialistes en cybersécurité en 2017, qui

s’ajouteront aux 180 déjà employés en 2016.

La cybermalveillance est devenue un fléau ordinaire. Baptisé Acyma, un dispositif d’assistance aux victimes de ce nouveau banditisme a été annoncé par le gouvernement et l’Agence nationale de sécurité des systèmes d’information (Anssi). Tout objet numérique est susceptible d’être piraté. Des règles élémentaires sont à observer, répètent à l’envi les experts : utiliser un logiciel de protection, ne pas ouvrir les messages électroniques dont l’intitulé est suspect, ne pas télécharger des programmes sans en vérifier l’origine. Ou encore, être équipé d’un logiciel de décryptage pour éviter d’avoir à payer une rançon pour récupérer sa voiture.

Sources :

- « Le “ransomware”, fléau de l’année de la piraterie informatique », AFP, tv5monde.com, 6 octobre 2016.
- « Une opération de police internationale fait tomber un large réseau de cybercriminalité », Sébastien Dumoulin, *Les Echos*, 5 décembre 2016.
- « Les logiciels extorqueurs ont exploré en 2016 », Anaëlle Grondin, *Les Echos*, 8 décembre 2016.
- « Popcorn Time, le virus vicieux qui vous pousse à contaminer vos amis », Sylvain Rolland, LaTribune.fr, 13 décembre 2016.
- « Un *ransomware* désactive un téléviseur connecté LG », Corentin Durand, numerama.com, 29 décembre 2016.
- « Orange veut devenir un leader européen de la cybersécurité », AFP, tv5monde.com, 24 janvier 2017.
- « Cyberattaques : deux fois plus de cas en France en 2016 », Sébastien Dumoulin, *Les Echos*, 24 janvier 2017.
- « Les pirates informatiques innovent pour causer davantage de dégâts », Lucie Ronfaut, *Le Figaro*, 26 janvier 2017.