# Ransomwares : ingéniosité, perversité et persévérance

Tout d'abord un chiffre délivré par Kaspersky Lab. Au 1er trimestre 2016, les ransomwares ont représenté 30% des attaques et devancent les APT (Advanced Persistent Threat). Les experts de la firme russe ont dénombré 2900 variantes de rançongiciel sur les trois premiers mois de l'année, en hausse de 14% par rapport au trimestre précédent. Kaspersky recensait près de 185 000 attaques en mars dernier. L'Italie, les Pays-Bas et la Belgique étaient les pays les plus touchés. La société donne aussi son palmarès des ransomwares les plus utilisés : Teslacrypt, CTB-Locker et Cryptowall. Les victimes du premier peuvent néanmoins espérer se sortir d'affaire après un revirement de la part des pirates qui ont rendu publique la clé de chiffrement.

Tous les observateurs sont unanimes, la vague des ransomwares ne fait que commencer et elle progresse très rapidement. Et surtout les rançongiciels laissent la place à l'ingéniosité machiavélique des cybercriminels. Les exemples sont nombreux, mais voici un échantillon des dernières trouvailles.

## L'ajout d'un botnet pour des attaques DDoS

Des chercheurs d'Invincea ont découvert une variante du rançongiciel baptisé Cerber. Celle-ci place, en même temps que le chiffrement des fichiers, un botnet capable de mener des attaques DDoS. Il peut ainsi usurper le trafic réseau sur différentes adresses IP. Le ransomware est diffusé par un fichier RTF à travers du spear phishing (mail ciblé) avec une macro activable.

Pour l'utilisateur, c'est donc la double peine, s'il ne peut pas ou ne veut pas régler la rançon, non seulement ses fichiers continueront à être chiffrés, mais en plus son ordinateur sera enrôlé dans un botnet capable de mener des attaques par saturation sur des ordinateurs cibles. Une autre manne pour les cybercriminels, car les DDoS constituent une source de revenus. « Un idée diabolique », constate les chercheurs d'Invincea, car ce couplage pourrait devenir une tendance dans les prochains mois.

## De faux techniciens pour de faux écrans Windows

Sur le blog de Malwarebytes, on découvre une technique de faux techniciens Microsoft pour installer un ransomware. A la base, le PC de l'utilisateur est infecté par un malware qui lance une fausse mise à jour de l'OS en maquillant un écran similaire à Windows Update. Mais l'installation est arrêtée pour des questions de licence Windows et l'utilisateur doit fournir une clé pour continuer. La clé ne fonctionne pas et l'utilisateur est invité à appeler un numéro de téléphone du support.

Un faux technicien demande alors à la personne de taper les commandes CTRL + Shift + T pour faire apparaître une fenêtre qui lance une session TeamViewer pour contrôler l'ordinateur à distance. Le faux technicien peut ainsi activer le ransomware et demander en direct le paiement de la rançon. Sur son blog, Malwarebytes donne quelques exemples de clés de déchiffrement, mais

sans être sûr qu'elles fonctionneront à nouveau.

## Rançonner pour la bonne cause

En début de mois, des experts de Heimdal Security tombaient sur le ransomware « Cryptmix » qui combine des souches de CryptoWall 4.0 and CryptXXX. Particularité de ce virus, il réclame le paiement d'une obole de 5 bitcoins soit environ 1500 dollars. Un montant relativement élevé pour un rançongiciel qui soutire en général des sommes plus modestes (300 à 500 dollars en bitcoin). Mais là, les cybercriminels promettent que les fonds extorqués permettent dans un premier temps d'acheter un logiciel capable d'éviter à l'avenir ces désagréments, une protection garantie pendant 3 ans ! Et surtout l'argent devrait servir à financer des œuvres de charité pour les enfants pour leur apporter des cadeaux et une aide médicale. Un poil comédien, le cybercriminel en rajoute : « *Votre nom sera en tête de la liste des donneurs et restera dans l'histoire des bienfaiteurs.* » Mais prévient à la fin du message, le montant demandé sera doublé sans réponse dans les 24h.

## DMA Locker 4.0 en attente de distribution massive

Le rançongiciel DMA Locker n'en finit pas de muter. Une première version a été dénichée en janvier dernier avec de telles imperfections que les spécialistes ont cru à une blague. La clé de déchiffrement était codée en dur dans le binaire du ransomware, rendant très facile la récupération des fichiers. Une version 2 est apparue en février avec encore des faiblesses, mais les cybercriminels avait changé et amélioré certaines parties du logiciel. A la fin février, la version 3 montre un tournant, car les spécialistes n'ont plus réussi à le déchiffrer, ce qui signifie un meilleur système de cryptage.

Aujourd'hui, selon l'expert Hasherazade de Malwarebytes, le ransomware est passé dans une autre dimension avec sa version 4. Alors que ces prédécesseurs travaillaient offline, DMA Locker se connecte maintenant à un serveur de C&C pour générer des clés de chiffrement. Idem pour le paiement, les versions précédentes demandaient l'envoi d'un mail. Maintenant, tout se passe depuis un site web. Ce dernier n'est pas pleinement opérationnel, mais cela montre que les cybercriminels peaufinent leur ransomware pour une diffusion massive dans les prochaines semaines. L'objectif est d'intégrer un kit d'exploit. C'est déjà le cas pour Neutrino.

**A lire aussi :**

Les ransomwares tirent et réclament à tout va
Une faille JBoss ouvre la porte des serveurs au ransomware SamSam