Le ransomware Locky mute pour multiplier ses victimes en France

« *Eteignez les ordinateurs immédiatement* ». C'est la consigne que s'est vue intimer la rédaction de *Silicon.fr* hier, vers 10h30. En cause : la découverte de fichiers comportant le suffixe .locky sur un des serveurs de fichiers partagés de NetMediaEurope, l'éditeur de notre publication. Le signe indiscutable d'une contamination naissante par le ransomware Locky, un malware apparu à la mi-février et qui multiplie les tentatives d'infection dans l'Hexagone.

Locky chiffre un grand nombre de fichiers, en particulier tous ceux ayant des extensions renvoyant à des vidéos, des images, des codes source et des fichiers Office. Une fois les données verrouillées, les cybercriminels demandent aux victimes de s'acquitter d'une rançon pour retrouver l'accès à leurs données devenues illisibles (entre **0,5 et 1 Bitcoin pour Locky**, selon les données publiées par l'éditeur Sophos, un Bitcoin valant aujourd'hui quelque 360 euros).

« Une nouvelle variante presque chaque jour »

Pour se propager, Locky se cache dans des e-mails (par exemple de fausses factures Free, l'opérateur vient d'ailleurs – tardivement – d'alerter ses abonnés du phénomène), mais également dans des **notifications semblant émaner d'imprimantes ou de scanners situés sur le réseau de l'entreprise**. Ces dernières comportent un fichier PDF renfermant du code Javascript déclenchant le téléchargement du malware. « *Ce n'est malgré tout pas une attaque ciblée au sens où on l'entend habituellement*, explique **Vincent Nguyen**, le responsable technique du CERT (le centre de réponse aux incidents de sécurité) de la société de conseil Solucom. *Cette technique peut s'automatiser à partir de l'adresse du destinataire. La diversification des techniques de diffusion de l'infection témoigne par contre de la volonté des cybercriminels d'échapper aux filtres anti-spam*. »

Le ransomware se diffuse aussi via des sites infectés par les cybercriminels, méthode qui semble être celle exploitée pour contaminer l'éditeur de *Silicon.fr*. « *Le site va utiliser un 'Exploit Kit' (en ce moment, principalement Angler), qui consolide plusieurs codes d'exploitation de vulnérabilités pour des produits web (navigateurs web, plug-in Flash, Java, Silverlight…)* », détaille Vincent Nguyen. Objectif : repérer une des vulnérabilités ciblées par le kit dans le navigateur web des visiteurs pour exécuter un code malveillant qui va déclencher l'innoculation du ransomware.

Et ça marche, comme peut en témoigner Apicomm, le prestataire chargé de la gestion du parc de NetMediaEurope. « *Une nouvelle variante de Locky apparaît presque chaque jour afin d'échapper aux outils de détection* », confirme **Rémy Fontaine**, son responsable entreprise. Qui précise : « *depuis ce matin (hier le 10 mars), une nouvelle variante est apparue et n'est détectée que par 5 antivirus sur 57. Cette variante est plus dangereuse, car elle chiffre tout sur le partage réseau en utilisant la découverte réseau de Windows, alors que la précédente mouture du malware se basait sur les lettres des lecteurs réseaux* ». Pour Apicomm, en cas d'infection, la première chose à faire consiste à débrancher le câble réseau et même à éteindre les PC. « *En effet, sur les dernières variantes, le fait de couper le réseau empêche la communication entre Locky et le serveur des hackers et donc interrompt le chiffrement. Normalement, le fait de relancer la machine suffit à désactiver le malware* », détaille Rémy Fontaine, dont la société est déjà intervenue sur

5 serveurs infectés par les premières variantes et sur deux autres touchés par les dernières moutures. Pour tenter d'enrayer le malware, la société a développé une stratégie de groupe (GPO,Group Policies Object) sur les serveurs permettant de bloquer l'exécution de Locky dans APPDATA, le répertoire où il a l'habitude de se loger.

« *Le phénomène touche toutes les entreprises, les plus grandes y compris* », assure Vincent Nguyen. Solucom, dont l'activité se concentre sur les grandes entreprises, a ainsi reçu une dizaine de sollicitations sur le sujet et est intervenu, sur site, chez deux de ses clients. « *L'un d'entre eux était touché par 5 souches de ransomwares différentes en même temps. C'est ce qui rend la situation complexe, car on n'a pas affaire à une menace unique : aux multiples variantes de Locky s'ajoutent celles de Teslacrypt par exemple. Et les antivirus ont toujours un coup de retard* », explique le responsable technique du CERT de Solucom, société qui vient de publier quelques conseils sur les façons de réagir à une infection par ransomware.

Locky mute par algorithme

Comme l'explique **Cyrille Badeau**, le directeur régional de l'éditeur ThreatQuotient, spécialisé dans l'intelligence sur la menace, les malwares mutent en permanence pour contourner les lignes de défense, ce qui explique pourquoi des entreprises même à jour sur leurs technologies de lutte contre les menaces sont piégées… pour peu qu'un utilisateur clique sur un fichier malicieux. « *Si on compare une attaque complexe à une molécule composée d'atomes, même si les méthodologies d'attaque, soit la structure des molécules, évoluent très lentement du fait de l'importance du coût associé, les hackers sont capables de faire évoluer de nombreux atomes à bas coût. Ainsi depuis plusieurs années, de campagne en campagne, ils remplacent certains atomes devenus trop facilement détectables par de nouveaux éléments ayant le même rôle, mais apparaissant pour la première fois.* »

Et Cyrille Badeau de noter que, dans le cas de Locky, l'automatisation des attaques s'est accentuée avec l'utilisation de serveurs de contrôle et de commande (serveurs dits C&C qui pilotent les virus) générés par algorithme. « I*mpossible pour les défenseurs de prévoir le prochain C&C à surveiller* », résume-t-il. Un site comme RansomwareTracker les référence au fil de l'eau, mais une fois les premières infections détectées.

Un Javascript à la place des macros Office

Si la France figure parmi les principaux pays victimes du rançongiciel, le phénomène est global. Les laboratoires SpiderLabs de la société Trustwave estiment que 18 % des 4 millions de spams qu'ils ont analysé dans le courant de la semaine dernière sont liés à des ransomware. Et Locky est la star actuelle dans cette famille d'infections. Les SpiderLabs notent une **accélération importante de l'envoi de spams renfermant des ransomware** au cours des derniers jours. « *Ces campagnes (d'envoi de spams visant à diffuser l'outil de téléchargement du virus) ne sont pas continues, mais concentrées, avec des pics à 200 000 e-mails infectieux arrivant sur nos serveurs en une seule heure* », écrit Rodel Mendrez, un chercheur de Trustwave.

Et la société de mettre en garde contre la diffusion par spam de scripts Javascript (encapsulés dans des fichiers Zip) déclenchant le téléchargement de Locky, une autre technique exploitée par les

cybercriminels. Objectif de la compression en .zip et de l'envoi d'un fichier de petite taille : laisser penser que ledit fichier est bénin.« *Nous pensons que le passage au Javascript vise à esquiver les technologies antimalware* », renchérit McAfee dans un billet de blog. Cette méthode, aux côtés de celles basées sur de fausses notifications de scanners ou imprimantes et sur la diffusion par des sites infectés, semblent avoir supplanté la première technique de dissémination employée par les cybercriminels, une approche exploitant les macros Office.

500 000 connexions venant de France

Les statistiques fournies par un autre fournisseur d'outils de sécurité, Fortinet, témoignent aussi de la large diffusion de Locky. Sur la base des connexions aux serveurs de commande et contrôle des ransomware détectées par ses sondes de détection d'intrusion (soit 18,6 millions de connexions entre le 17 février et le 2 mars), la société estime que 16,5 % d'entre elles sont liées à Locky. C'est certes beaucoup moins que les connexions dues à la famille Cryptowall (plus de 83%), mais Locky est, contrairement à son aîné, clairement **surreprésenté en France**, l'Hexagone pesant quelque 15 % des connexions totales dues à la nouvelle terreur des services IT. Ce qui représente, pour les seules sondes Fortinet, pas loin de 500 000 connexions aux serveurs de commande et contrôle Locky issues de France, dans le courant de seconde moitié de février.

Locky a récemment fait la démonstration de sa dangerosité outre Atlantique, en bloquant les systèmes d'un hôpital de Los Angeles, le Hollywood Presbyterian Medical Center. Selon le *New York Post*, ce dernier a été contraint de verser 17 000 $ aux pirates – après négociation, les criminels réclamaient au départ plus de 3,5 M$ – pour obtenir les clefs de déchiffrement et retrouver l'accès à ses données. Comme l'explique Vincent Nguyen, de Solucom, aucun outil ne permet à ce jour de restaurer les fichiers chiffrés par Locky sans posséder la clef que vendent les cybercriminels, même si des travaux sont en cours pour tenter de trouver des solutions de contournement.

A lire aussi :

Le ransomware Locky inonde la France, via de fausses factures Free Mobile

Le ransomware prospère grâce à l'apathie des autorités

Ransomware : un retour sur investissement très lucratif

Crédit photo : Carlos Amarillo / Shutterstock