Cryptolocker : quand un virus prend vos données en otage contre rançon

	**Cryptolocker : quand un virus prend vos données en otage contre rançon**

Depuis quelques jours, une campagne d'attaque utilisant CryptoLocker (logiciel malveillant de type cheval de Troie) semblerait être en cours. La société d'antivirus Trend Micro a été alertée par de nombreux appels et messages de la part de ses clients et partenaires. Loïc Guézo, évangéliste Sécurité de l'Information pour l'Europe du Sud chez Trend Micro et administrateur du Clusif, livre quelques pistes pour lutter contre ce ransomeware (logiciel malveillant prenant les données personnelles de l'utilisateur en otage) particulièrement nuisible.

Vous cliquez sur le lien d'un e-mail reçu. Le fond d'écran change. Une fenêtre s'ouvre. Un avis apparaît, vous informant que vos fichiers importants sont cryptés. Vous tentez de cliquer ailleurs. Impossible de quitter la fenêtre. L'écran est verrouillé. Un cauchemar nommé "Cryptolocker".
Ce "ransomware" (ou rançongiciel) est un logiciel malveillant qui piège l'ordinateur de ses victimes et prend en otage leurs données personnelles. Il est précisé que le chiffrage des données du disque par le logiciel malveillant les rend inutilisables jusqu'au versement de la rançon demandée. Le pirate promet de fournir la clé capable de déchiffrer les données en échange d'une somme de quelques centaines d'euros, à régler en ligne via Paypal ou un virement en bitcoins. Le tout avec un compteur de temps bien visible, qui signifie que la décision doit être prise rapidement.
Bien sûr une clé unique est utilisée pour chaque machine piégée. Si la rançon demandée n'est pas versée dans le temps imparti, la clé de chiffrement ne sera pas communiquée et les données chiffrées définitivement perdues. Et si la rançon est payée, rien ne garantit pour autant la suite des opérations…
Ce scénario digne d'un thriller a fait son apparition fin 2013 et revient en force depuis quelques semaines. S'il est encore trop tôt pour connaître précisément le nombre de systèmes infectés par le programme malveillant, Le Monde Informatique du 6 janvier 2014 rapporte que Cryptolocker 2.0 aurait infecté 200 à 300 000 PC et qu'environ 0,4 % des victimes ont probablement payé la rançon réclamée, même si payer ne garantit absolument pas le déblocage du système.
Ce banditisme virtuel est basé sur un chantage avec comme otage les données de la victime. Il a été jugé suffisamment grave pour que des policiers, spécialement formés, enquêtent pour retrouver ces malfaiteurs du Net et les poursuivent. Des unités spéciales américaines et européennes ont, par exemple, travaillé ensemble et uni leurs efforts pour démanteler le 2 juin dernier le réseau criminel GameOver Zeus qui, entre autres, pouvait distribuer Cryptolocker.

L'INGÉNIERIE SOCIALE, VECTEUR DE L'INFECTION
Les malfaiteurs s'appuient sur des techniques d'ingénierie sociale. Ils procèdent à l'envoi initial de leurres sous forme de vagues d'e-mails ciblés. D'où l'importance de vérifier la légitimité de chaque message. Il convient de toujours faire preuve d'une extrême prudence lorsque nous ouvrons la pièce jointe à un message électronique dont la source nous est inconnue.
Ce sont principalement aujourd'hui les utilisateurs de PC qui sont visés (des versions visant les mobiles apparaissent déjà). Mais le point de départ est bien le geste de l'utilisateur lui-même, piégé par un message avec pièce jointe. L'hameçon psychologique est celui de l'inquiétude naturelle, de la surprise ou de l'intérêt du destinataire du message. Il peut s'agir de faux courriers paraissant provenir d'un organisme social, d'une banque, d'une assurance, d'e-commerçants, de logisticiens ou de transporteurs, etc. La pièce jointe est censée être un document lié à un litige, une facture impayée, un avis de livraison en suspens, un remboursement sur trop-perçu…
L'éducation et la vigilance des utilisateurs isolés sont donc indispensables. Sur un réseau d'entreprise, l'information d'alerte doit être donnée et pourra plus facilement être souvent répétée : "n'ouvrez pas les mails de provenance inconnue sans vérification, ne cliquez jamais sur un lien si vous avez le moindre doute", etc.

COMMENT SE DÉFENDRE ET PRÉVENIR LE BLOCAGE ?
Il existe plusieurs moyens pour gérer cette menace, tant pour les particuliers que pour les entreprises. Il a été largement démontré que la sécurité basée sur les signatures a atteint ses limites, mais il existe cependant d'autres solutions avec des fonctions d'alerte plus évoluées. Ce sont par exemple des solutions basées sur les éléments environnementaux (comme la réputation d'adresses IP, les noms de domaine…). Un service de réputation va en particulier permettre de bloquer l'accès à certaines adresses IP correspondant à des C&C de botnets, empêchant tout simplement le Cryptolocker de s'initialiser et donc de chiffrer la cible !
Revoir la politique de sécurité des pièces jointes est urgent pour de nombreuses entreprises. L'adoption des bonnes pratiques permettra d'éviter une contamination très rapide.
Posons-nous les bonnes questions pour contrer Cryptolocker. Est-ce que l'entreprise dispose bien d'une politique de blocage des pièces jointes aux messages, empêchant par exemple le déclenchement d'un fichier exécutable ? Peut-on analyser "en amont" le comportement des pièces jointes ? Utilise-t-on un service avancé de réputation ? Surveille-t-on le comportement des pièces jointes sur la durée? A-t-on simplement le moyen de contrôler que la solution de sécurité reste activée ? Ces quelques premières précautions permettront d'éviter les catastrophes, en particulier pour les PME.
Il faut bien sûr toujours être sur ses gardes, ne pas négliger de mettre à jour les logiciels de sécurité installés et vérifier que le navigateur utilise la réputation de sites Web avant de cliquer sur un lien ou bien utiliser un service gratuit comme Trend Micro Site Safety Center.
Quant aux grandes entreprises, qu'elles se préparent à recevoir des attaques type Cryptolocker mais désormais ciblées. Et bien sûr, toujours communiquer en interne sur les risques, et communiquer, c'est répéter…

LES SYSTÈMES INFORMATIQUES DOIVENT ÊTRE PRÉPARÉS POUR RÉSISTER
On ne soulignera jamais assez que la formation des utilisateurs, la mise à jour régulière des logiciels et de bonnes pratiques d'utilisation de l'ordinateur individuel restent le socle de défense contre Cryptolocker ou toutes les nouvelles menaces similaires. Il est désormais nécessaire d'introduire des outils d'analyses plus complets (vision en temps réel de la menace ou exécution en environnement contrôlé – sandboxing – par exemple).
Si les cybercriminels perfectionnent chaque jour leurs logiciels malveillants qui deviennent ainsi de plus en plus sophistiqués, alors les systèmes informatiques doivent également être préparés pour résister mais surtout être cyber-résilients face à ces attaques. Cette lutte doit être globale pour non seulement réduire le taux de l'infection, mais également briser la chaîne de transmission des logiciels malveillants par une stratégie de défense en profondeur, y compris lors de son déroulement.
L'autre aspect fondamental reste la lutte policière et judiciaire contre ces nouvelles formes de criminalité dont les dernières semaines ont montré l'ampleur et le dynamisme.

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

Source : http://www.usine-digitale.fr/article/cryptolocker-quand-un-virus-prend-vos-donnees-en-otage-contre-rancon.N302748
par Loïc Guézo, Evangéliste Sécurité de l'Information pour l'Europe du Sud chez Trend Micro & Administrateur du Clusif