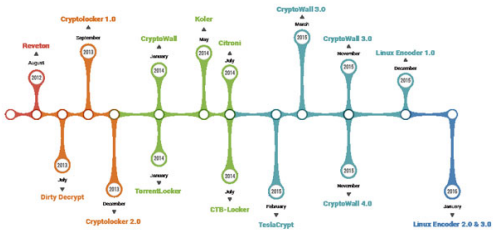
Ransomware – Les Français disposés à payer 190 euros pour récupérer leurs données

Ransomware – Les Français disposés à payer 190 euros pour récupérer leurs données

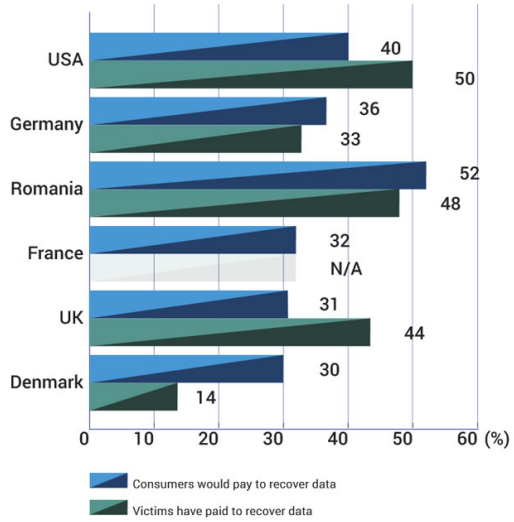
Le ransomware est une catégorie de programme malveillant qui une fois installé chiffre les données du PC et exige de son propriétaire qu'il paie une rançon pour les récupérer. Et les victimes seraient, pour une bonne partie d'entre eux, disposées à payer cette rançon.
Si vous étiez victime d'un ransomware (ou rançongiciel), paieriez-vous la rançon exigée pour récupérer vos fichiers ou enverriez-vous les cybercriminels promener ? Le fait que vous soyez au travail ou à votre domicile ferait-il une différence ?

Selon une étude, le comportement des victimes de ransomware pourrait bien dépendre du lieu où celles-ci se trouvent lorsque la demande de rançon leur parvient. Ce qui varierait également, c'est le montant de cette rançon.



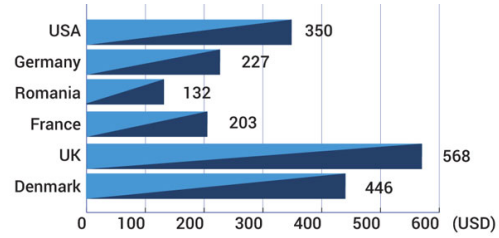
32% des sondés français paieraient pour leurs fichiers.
Comme son nom le suggère, le ransomware va chiffrer les fichiers enregistrés sur l'ordinateur compromis. Menaçant les utilisateurs de l'impossibilité de récupérer ces documents, les cybercriminels exigent le versement d'une rançon. Une fois celle-ci versée, promesse serait faite de déchiffrer les données des victimes.

Et d'après une étude de l'éditeur de sécurité Bitdefender, tous les internautes, en fonction de leur nationalité, ne sont pas égaux face à ces logiciels malveillants. Ainsi aux Etats-Unis, 50% des victimes de ransomware ont accepté de payer.
En France ? Cette donnée n'est pas disponible. En revanche, 32% des internautes français interrogés déclarent qu'ils paieraient en cas d'infection. Cette part dépend aussi, très logiquement, de l'importance accordée aux fichiers devenus inaccessibles en raison du chiffrement.



Par exemple, 18% des répondants du Royaume-Uni paieraient pour les documents personnels, 17% pour les photos personnelles et seulement 10% pour les documents liés au travail » détaille BitDefender.

Accepter de payer est une chose, mais quel montant ? Sur ce point aussi, les sommes varient très significativement d'un pays à un autre. Au Royaume-Uni, une victime accepterait de verser jusqu'à 568 dollars, contre 203 dollars en France.



Payer la rançon aide juste les cybercriminels
Un tel comportement consistant à céder aux cybercriminels est-il cependant recommandé ? Catalin Cosoi, responsable de la stratégie sécurité de BitDefender, déconseille de payer. « Alors que les victimes sont généralement enclines à payer la rançon, nous les encourageons à ne pas à se livrer à de telles actions, car cela contribue uniquement à soutenir financièrement les développeurs du malware. »
En janvier, à l'occasion du FIC 2016, le directeur de l'Anssi a évoqué l'infection du ministère des Transports par un ransomware. Et Guillaume Poupard était formel : « On ne paie pas, ce n'est pas une solution raisonnable. »
Pourquoi ? Notamment, car le cybercriminel peut tout à fait choisir de ne pas livrer les clefs nécessaires au déchiffrement des fichiers, et rien ne garantit non plus qu'il ne relancera pas une nouvelle attaque ultérieurement. Les sauvegardes restent donc la meilleure parade face à ces malwares, préconise l'Anssi … ***[Lire la suite]***

Réagissez à cet article

Source : *Ransomware – Les Français disposés à payer 190 euros pour récupérer leurs données*

The Current State of Ransomware

The Current State of Ransomware

In the past year or two, one of our most popular technical topics, for all the wrong reasons, has been ransomware.
Ransomware, as we're sure you know, is the punch-in-the-face malware that scrambles your files, sends the only copy of the decryption key to the crooks, and then offers to sell the key back to you.
Even Linux has ransomware these days, although fortunately we've only seen one serious attempt at Linux-based extortion so far, presuambly because cybercriminals haven't yet figured out how to make money in that part of the IT ecosystem.
Let's hope it stays that way for Linux sysadmins, because the crooks are still attacking Windows users heavily, and are still raking in lots of ill-gotten gains.

THE CRYPTOLOCKER YEARS
Two years ago, one strain of ransomware known as CryptoLocker dominated the demanding-money-with-menaces malware scene.
The US Department of Justice (DoJ) suggested that the crew behind CryptoLocker raked in $27,000,000 in September and October 2013 alone, in the first two months that the malware was widely reported.
And a 2014 survey by the University of Kent in England estimated that 1 in 30 British computer users had been hit by CryptoLocker, and that 40% of those coughed up, paying hundreds of dollars each in blackmail money to recover their data.
But in mid-2014, the DoJ co-ordinated a multi-country takedown of a notorious botnet called Gameover Zeus that targeted victims while they were doing online banking.
And, would you believe it: while the cops were raiding the Gameover servers, they came across the CryptoLocker infrastructure as well, and took down those servers at the same time, pulling off a neat double play.
CryptoLocker doesn't start its data scrambling until after it has called home for an encryption key, so killing its servers pretty much neutralised the warhead of the malware: it would get right to the very brink of detonation and then freeze, waiting for data that never came.
But any celebration about the damage done to the ransomware scene as a whole was short-lived.

RANSOMWARE REDUX
Cybercrime, if you will tolerate a clumsy metaphor, abhors a vacuum, and new ransomware soon appeared to fill the multi-million-dollar void left by the demise of CryptoLocker.
CryptoWall, and its close derivative CryptoDefense, were early pretenders to CryptoLocker's throne, but many others have appeared, too.
Threats like TorrentLocker, CTB-Locker and TeslaCrypt are big names these days, joined by other intriguing threats such as VirLock, ThreatFinder (an ironic name, considering that it is itself the threat) and CrypVault.

WHAT TO DO?
When it comes to malware of this sort, the dictum "know your enemy" is worth remembering.
With this in mind, James Wyke and Anand Ajjan, who are Senior Threat Researchers in SophosLabs, have recently published a thorough and well-written paper entitled The Current State of Ransomware.
This paper is a highly-recommended read – and it's a free download, no registration required.
https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-current-state-of-ransomware.pdf?la=en

You'll learn about the history of ransomware, the latest threats, how they work, and what you can do to defend yourself.
Great stuff from SophosLabs!

Réagissez à cet article

Source : *The Current State of Ransomware – a new paper from SophosLabs |*

Quelques pistes en prévention ou en curation d’attaque par ransomwares

Quelques pistes en prévention ou en curation d’attaque par ransomwares

Un de vos clients est victime d'un ransomware. Cryptolocker, Cryptowall, Supercrypt, TeslaCrypt, … Peut importe le malware, le résultat est à peu prêt le même. Ses fichiers sont cryptés, et l'impact est énorme. Dans l'urgence, il convient de procéder correctement, en prenant certaines précautions. Je vais donc ici vous donner quelques pistes (un peu en vrac) afin de traiter au mieux le problème.

Sauvegarde

J'imagine que si vous consultez cet article, aucune sauvegarde de votre client n'est exploitable. Sinon, vous l'auriez remontée.
Cependant, avant d'envisager toute action sur le/les systèmes infectés, pensez à procéder à une sauvegarde. Je recommande d'arrêter immédiatement ces systèmes infectés. Ensuite, qu'il s'agisse d'un serveur, ou d'un simple client, clonez le disque dur.
Pour cela, effectuez un clone en mode hors ligne, avec un de ces outils par exemple : Acronis, Veeam, AOMEI.
Ca vous permettra d'effectuer les tests que vous voulez sur le clone, sans aucun risque.

Lister les fichiers cryptés

Un outil bien pratique permet de lister les fichiers cryptés par Cryptowall. En effet, cette infection stocke la liste des fichiers qu'elle crypte dans le registre. L'outil ListCWall permet de localiser et utiliser ces infos afin de vous sortir une liste des fichiers, et permet aussi de les exporter afin de les stocker par exemple sur un média externe avant de formater la machine si besoin.

Utilitaires de décryptage

Ce qu'il faut retenir de ce paragraphe, ce n'est pas autant la liste des outils (non exhaustive) que je vous propose, mais que de tels outils voient le jour périodiquement. Pensez à regarder du côté des éditeurs d'antivirus (ou sur Tech2Tech!!), si un nouvel outil existe concernant l'infection que vous avez à traiter en particulier. En effet, suite à des enquêtes internationales, parfois, des réseaux tombent. Et lorsque les services en charge de ces enquêtes découvrent un lot de clés de cryptages, les éditeurs d'antivirus peuvent les exploiter afin de les intégrer dans des outils de décryptage. Pas sur que ca fonctionne donc (si la clé utilisée ne fait pas partie de celles qui ont été découvertes) mais vous pouvez le tenter…
On peut lister par exemple :
RectorDecryptor chez Kaspersky (pour le ransomware Rector)
XoristDecryptor chez Kaspersky (pour le ransomware Xorist/Vandev)
ScatterDecryptor chez Kaspersky (pour le ransomware Scatter)
ScraperDecryptor chez Kaspersky (pour le ransomware Scraper)
RakhniDecryptor chez Kaspersky (pour le ransomware Rakhni)
Ransomware Decryptor chez Kaspersky (pour le ransomware Coinvault/Bitcryptor)
Decryptor 0-1.3 chez Bitdefender (pour le ransomware Linux.Encoder.1)
DecryptCryptoLocker par FireEye et Fox IT (pour le ransomware CryptoLocker)
TeslaDecrypt par Cisco Talos Security Intelligence (pour le ransomware TeslaCrypt)

Récupérer les fichiers

A ma connaissance, si vous n'avez pas de sauvegardes, et que le ransomware n'a pas d'outil de décryptage dédié ayant été élaboré, il y a peu de chances de retrouver les fichiers.
Cependant, deux pistes peuvent s'avérer intéressantes :

Shadow Volume Copies

Les shadow copies (service de clichés instantanés), peuvent s'avérer utiles dans le cas d'un ransomware. Cependant, il faut déjà que le service soit activé et configurée correctement. Ensuite, la majorité des ransomware un peu élaborés et récents désactivent ce service, et vont effacer les snapshots déjà présents. S'ils s'avèrent utilisables, le logiciel Shadow Explorer sera pratique pour récupérer les fichiers.

Récupération de données

Il semblerait que, dans le cas de certains ransomware, les fichiers soient copiés, cryptés, puis supprimés. Il serait alors envisageable, si la machine est arrêtée au plus vite, de récupérer des fichiers à l'aide d'un utilitaire de récupération de données.
Pour cela, clonez d'abord le disque par précaution, en mode hors ligne (Live CD).

Se protéger des ransomwares

Plusieurs éditeurs de solutions de sécurité proposent des utilitaires plus ou moins élaborés afin de se protéger contre un cryptage de données.
Il y a d'abord une approche qui consiste à interdire le lancement d'exécutables situés dans %APPDATA%. C'est en effet un mode de fonctionnement courant de ce type de malwares. Cette fonction est proposée par Bitdefender à travers son outil gratuit Anti-Cryptowall. Personnellement cet utilitaire ne m'a pas vraiment convaincu lorsque je l'ai essayé, puisque j'ai pu lancé des exe situés dans %APPDATA%…
CryptoPrevent, utilitaire développé par Foolish IT permet de se prémunir d'une attaque par un CryptoLocker. Cependant, la version gratuite nécessite des mises à jours manuelles visiblement. Voyez plutôt vos besoins sur les différentes versions commerciales.
BitDefender a intégré dans sa version grand public 2016 un moteur d'analyse de cryptage. Le but est d'analyser en temps réel une éventuelle activité de cryptage sur la machine, et de la stopper. Cette fonction sera intégrée dans les antivirus pro maximum en début d'année 2017.
Pour ma part, je suis distributeur des solutions Panda Security Cloud. Et un outil a été mis au point durant l'été : Adaptive Defense 360. Venant en renfort de n'importe quel antivirus, ce produit permet de bloquer tous les logiciels que l'entreprise n'a pas décidé explicitement de laisser fonctionner sur son parc. Il en résulte une protection quasi parfaite, même si ca a un coût. Et comme il faut bien manger, je me fais au passage une petite pub : n'hésitez pas à me contacter si vous désirez vous équiper de cette solution!
Ce ne sont évidement que des exemples, non exhaustifs. Mais ils traduisent la diversité des solutions élaborées afin de contrer les ransomwares et cryptolockers, qui sévissent actuellement de manière dramatique.

Réagissez à cet article
Source : http://www.tech2tech.fr/ransomware-avec-cryptage-quelques-pistes/

Le pire des ransomwares vous fait perdre vos données à vie

Le pire des ransomwares vous fait perdre vos données à vie

Dans la famille des logiciels malveillants, on trouve de tout : les virus, les trojans, les rootkits, les spywares… Et puis il a aussi les ransomwares, aussi appelés rançongiciels, qui consistent à chiffrer les données d'un utilisateur, et à lui réclamer une certaine somme en échange de la clé de déchiffrage.

Mais récemment est apparu un nouveau ransomware appelé Power Worm.
Sa particularité ? Être tellement mal codé qu'il est impossible de déchiffrer ensuite les données corrompues, même en mettant la main au porte-monnaie.
Power Worm s'en prend aux fichiers Word et Excel en les chiffrant sans que l'utilisateur ne s'en aperçoive.
En théorie, lorsqu'il souhaite ensuite accéder à ces données, celui-ci est alors contraint de payer la coquette somme de 700 euros pour les récupérer. Mais dans sa toute dernière version, Power Worm détruit littéralement l'une des clés qui permettraient de déchiffrer les données.
En conséquence, il est totalement impossible d'accéder au contenu des fichiers chiffrés. Inutile donc de payer les 700 euros réclamés par l'auteur de ce malware, cela ne sert à rien. Le chercheur Lawrence Abrams, expert en malwares, explique sur le site Bleeping Computer qu'il « n'y a malheureusement rien qui puisse être fait pour les victimes de cette infection. Si vous avez été infecté par ce ransomware, votre seule option est de restaurer une sauvegarde de vos données ».

C'est visiblement une carence dans le code la part de l'auteur qui est à l'origine de ce gros bug : ça n'était pas volontaire d'après le chercheur Nathan Scott, qui a découvert ce défaut de conception. L'unique moyen de se préserver d'une telle situation reste de laisser constamment en place un antivirus sur sa machine. Ici, peu importe qu'ils soient gratuits ou payants : ils devraient tous remplir leur office et empêcher n'importe quel ransomware de s'installer, et en particulier interdire Power Worm de chiffrer les données de l'utilisateur.

Source : http://www.tomsguide.fr/actualite/power-worm-ransomware,49134.html

Un rançongiciel Linux s’attaque aux webmasters, en chiffrant les données des répertoires contenant les pages web | Le Net Expert Informatique

Un rançongiciel Linux s’attaque aux webmasters, en chiffrant les données des répertoires contenant les pages web

Un nouveau rançongiciel s’attaque aux machines Linux et cible en particulier les dossiers contenant les pages web. Le procédé du logiciel malveillant appelé Linux.Encoder est simple. Le rançongiciel crypte les répertoires de MySQL, Apache ainsi que le répertoire home/root. Le système demande alors de payer un seul bitcoin pour déverrouiller les fichiers.

Une fois que la rançon est payée, le système reçoit une instruction lui faisant parcourir les répertoires pour déchiffrer leurs contenus. Pour s’exécuter, la ransomware a besoin des privilèges d’administrateur et éventuellement d’une autorisation de la part d’un administrateur système pour qu’un tel programme puisse s’exécuter sans restriction. Selon le site drweb.com, une fois que le rançongiciel est lancé avec les privilèges d’administrateur, le logiciel télécharge le contenu des dossiers ciblés et crée un ficher contenant le lien vers une clé RSA publique. Le rançongiciel commence alors à supprimer les fichiers originaux et la clé RSA est utilisée pour générer une clé AES qui sera utilisée pour chiffrer les fichiers sur l’ordinateur infecté.

Source : Dr.WEB

Source :
http://www.developpez.com/actu/92220/Un-rancongiciel-Linux-s-attaque-aux-webmasters-en-chiffrant-les-donnees-des-repertoires-contenant-les-pages-web/

Toulouse attaqué par le virus «Rançongiciel» | Le Net Expert Informatique

Toulouse attaqué par le virus «Rançongiciel»

Ce mardi 10 mars, le système informatique de la ville de Toulouse a été attaqué par le virus «Rançongiciel», a confirmé hier une source municipale à La Dépêche du Midi3.

Vendredi 6 mars, les services informatiques municipaux avaient été mis en garde sur une éventuelle attaque par une autre collectivité de l'agglomération, qui avait elle-même été la cible de ce virus. «Rançongiciel» se propage par l'ouverture de pièces jointes dans les courriels, le téléchargement de fichiers infectés, la navigation sur internet. Il s'installe silencieusement dans l'ordinateur contaminé dont il crypte certains types de documents qui deviennent alors illisibles. Les pirates adressent alors un message dans lequel ils demandent une rançon en échange de la clé de déchiffrement des données. Généralement, cette clé n'est jamais fournie, même en cas de paiement.

Ce mardi 10 mars, un «Rançongiciel» a été détecté dans le système informatique de la ville de Toulouse qui avait été placé sous surveillance. Des mesures de précaution, comme l'interruption du travail en réseau, ont été prises immédiatement pour éviter sa propagation. De source interne, aucun fichier n'a été endommagé. Le réseau a été rétabli ce jeudi à 15 heures.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.ladepeche.fr/article/2015/03/13/2065766-le-reseau-de-la-ville-attaque-par-le-virus-rancongiciel.html

---

Trend Micro dresse le bilan de l'année écoulée dans son rapport annuel de sécurité | Le Net Expert Informatique

Trend Micro dresse le bilan de l'année écoulée dans son rapport annuel de sécurité

Les cyber-attaques réussies contre Sony, avec environ 100 Téraoctets de données piratées et des dommages estimés à près de 100 millions de dollars, sont venues couronner une année mémorable en termes de cyber-sécurité. Le rapport de sécurité annuel de Trend Micro, intitulé « The High Cost of Complacency » (Le coût élevé de la négligence), revient sur ce piratage ainsi que sur les événements de sécurité majeurs qui ont de nouveau illustré l'obstination des cybercriminels et la sophistication de leurs attaques en 2014.

« L'essentiel d'une stratégie de cyber-sécurité repose sur l'identification de ce qui est le plus important, le déploiement de technologies adéquates et la sensibilisation des utilisateurs », explique Raimund Genes, CTO de Trend Micro. « C'est le rôle de tout un chacun, pas seulement des informaticiens, que de préserver les données sensibles de l'entreprise. »
Les informations rassemblées au sein de ce rapport confirment notamment la prédiction formulée par Trend Micro fin 2013, selon laquelle un piratage majeur de données se produirait en moyenne une fois par mois. Pour les entreprises, le besoin de déployer des dispositifs de protection des réseaux et de détection des intrusions se fait d'autant plus sentir.
« A l'image du piratage de Sony, l'envergure et la portée des attaques perpétrées l'année dernière se sont avérées dramatiques », commente Tom Kellermann, Chief Cybersecurity Officer de Trend Micro. « Malheureusement, il ne s'agit sans doute que d'un aperçu de ce que l'avenir nous réserve. »

Parmi les principaux éléments traités dans ce rapport de sécurité 2014 :
Il ne faut négliger aucune menace, aussi minime soit-elle. Les pirates utilisent des méthodes simples pour déjouer la sécurité des entreprises et causer d'importants dégâts.
Les RAM scrapers, ces malware installés sur les terminaux de points de vente, sont presque devenus monnaie courante en 2014. Plusieurs cibles notables ont perdu des millions de données clients au profit des malfaiteurs tout au long de l'année.
De nouvelles attaques ont démontré qu'aucune application n'était invulnérable face à des pirates qui se diversifient.
La banque en ligne et mobile a connu ses plus importants défis de sécurité en 2014, notamment une sérieuse remise en question de l'authentification à deux facteurs comme garant de la sécurité des opérations sensibles.
Les ransomware ont gagné en puissance et en sophistication. Ils se sont étendus à de nouvelles régions du monde et à de nouvelles cibles. Ils vont désormais jusqu'à chiffrer les fichiers sur les systèmes infectés pour s'assurer du paiement de la rançon.

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

Source : http://www.globalsecuritymag.fr/Trend-Micro-dresse-le-bilan-de-l,20150309,51375.html

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

---

Une victime des pirates informatique guidée en ligne pour payer la rançon

Une victime des pirates informatique guidée en ligne pour payer la rançon

Témoignage d'un client :
L'informaticien Robert Hyppolite a dû payer une rançon aux pirates de SynoLocker… qui lui ont offert une assistance en ligne.

«Imaginez une entreprise de conseil juridique qui perd tous ses documents: mémoires, pièces, scans.
C'est un énorme coup dur. Sans les pièces, il y a de quoi perdre un procès!» Robert Hyppolite travaille depuis trente ans dans l'informatique à Genève. Il a notamment fondé l'entreprise Infologo, rachetée par VTX. Depuis 2007, il propose à ses clients le produit Synology, un système d'exploitation pour les serveurs de stockage en réseau. Des pirates ont élaboré un virus baptisé «SynoLocker TM» (sic) qui exploite la faille de sécurité de certaines anciennes versions du système. La police genevoise prend connaissance de cinq à dix nouveaux cas chaque semaine. Sur les trente clients de Robert Hyppolite équipés de Synology, deux ont été infectés et leurs sauvegardes ont également été atteintes. L'informaticien a dû payer une rançon en urgence dans la nuit de mardi à mercredi: l'un des deux clients touchés demandait une solution immédiate.

«La première difficulté était qu'il fallait payer en bitcoins, explique-il. On ne peut pas en acheter du jour au lendemain: il faut ouvrir un compte, donner son identité, faire un virement… Pour gagner du temps, je suis allé au distributeur de bitcoins des Pâquis (lire: Le bitcoin gagne l'économie réelle à Genève). La somme exigée par les pirates est de 0,6 bitcoin, ce qui correspondait à 650 francs, mais le cours est très fluctuant et dépend des pays et des plates-formes. »

Contre paiement de la rançon, un code permet normalement de décrypter les données et de retrouver ses fichiers. Sauf que l'aventure ne s'est pas arrêtée là. «Le virus chiffre les fichiers avec une clé réputée inviolable (2048 bits), ce qui les rend inutilisable. Ils restent normalement visibles avec leur nom correct. Mais le système de cette entreprise n'a pas réagi comme les autres et a été entièrement corrompu.» Conséquence: il a fallu réinstaller le système d'exploitation Synology, puis… réinstaller le virus, pour pouvoir permettre le décryptage des fichiers au moyen du code.

Les pirates répondent en ligne
Comment installer soi-même un virus? L'informaticien fait une curieuse découverte: «Sur le site Internet des ravisseurs, on trouve un onglet «support»… avec un chat en direct. Ils m'ont répondu très poliment: «Cher Monsieur, nous avons pris note de votre problème…» J'avais l'impression de parler à l'assistance en ligne d'une compagnie officielle! Une heure après, ils m'envoyaient une marche à suivre: il fallait entrer manuellement des instructions en ligne de commande. Tout a fonctionné sauf la dernière opération. A nouveau, le support informatique des pirates m'a répondu: leur dernière instruction contenait une erreur. J'ai ensuite pu entrer le code et tout est revenu à la normale.»
Une sauvegarde sur un serveur ou un disque dur séparé aurait permis de récupérer les données sans être rançonné. «Je préconise toujours cette mesure, mais dès qu'il faut s'équiper, il n'y a plus personne, regrette l'informaticien. Les clients pensent qu'on veut leur vendre des produits ou services inutiles, sauf ceux qui ont déjà vécu un sinistre…»
L'entreprise Synology souffrira-t-elle du virus SynoLocker? «Oui, mais ce sera vite oublié, estime Robert Hyppolite. J'ai vécu la mise à jour de l'antivirus Avast qui rendait les machines inutilisables… Pendant une année, leurs ventes ont baissé. Depuis, ils se sont rattrapés.» L'informaticien devra encore résoudre le problème du second client pris en otage. L'occasion, peut-être, d'une nouvelle discussion avec des ravisseurs informatiques très organisés et qui semblent prendre soin de leurs «clients».
Note: en cas d'infection avec SynoLocker, la police recommande de ne pas s'acquitter de la rançon et de réinitialiser les disques durs. Dans une note publiée ce jeudi, la Confédération émet des recommandations contre SynoLocker et conseille un outil de décryptage gratuit contre un virus au fonctionnement semblable, Cryptolocker.
Lire la suite…
Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.tdg.ch/high-tech/hard-software/Des-pirates-informatiques-guident-leurs-victimes-en-ligne/story/19256356

Un logiciel d’extorsion (ransomware) utilise un simple fichier batch

Un logiciel d’extorsion (ransomware) utilise un simple fichier batch
Informatique

Des chercheurs de Symantec ont récemment identifié une menace d’extorsion qui fonctionne avec un script et une ligne de commande en utilisant le programme de chiffrement Open Source GnuPG.

Pour extorquer de l’argent aux utilisateurs, des pirates ont mis au point un nouveau programme capable de chiffrer les fichiers sur l’ordinateur cible. Ce nouveau type de malware indique que les attaquants n’ont plus besoin de compétences pointues en programmation pour créer de dangereux programmes d’extorsion (ransomware) très efficaces, surtout quand les technologies de chiffrement avancé sont accessibles gratuitement. Des chercheurs du fournisseur d’antivirus Symantec sont récemment tombés sur un logiciel malveillant de ce type, d’origine russe, dont le composant principal se limite à un simple fichier batch, c’est à dire un script avec une ligne de commande. Cette stratégie de développement permet à l’attaquant de contrôler et de mettre facilement à jour le malware, explique dans un billet le chercheur Kazumasa Itabashi.

Le fichier batch télécharge une clef publique RSA en 1024 bits depuis un serveur et l’importe dans GnuPG, un programme de chiffrement gratuit qui fonctionne également par ligne de

commande. GnuPG est une implémentation Open Source de la norme de chiffrement OpenPGP. Il est utilisé pour chiffrer les fichiers de la victime avec la clé téléchargée. « Si l'utilisateur veut déchiffrer les fichiers concernés, ils a besoin de récupérer la clé privée de l'auteur du malware », indique le chercheur.

Une rançon de 150 € pour déchiffrer ses propres données

Dans le chiffrement à clé publique sur lequel est basé OpenPGP, les utilisateurs génèrent une paire de clés associées, l'une rendue publique et l'autre qui reste privée. Le contenu chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante. La nouvelle menace représentée par le ransomware que Symantec appelle Trojan.Ransomcrypt.L chiffre les fichiers avec les extensions suivantes: .xls, .xlsx, .doc, .docx, .pdf, .jpg, .cd, .jpeg, .1cd, .rar, .mdb et .zip. Les victimes sont invitées à payer une rançon de 150 € pour récupérer la clef privée.

Ce qui distingue le Trojan.Ransomcrypt.L des autres malwares ne tient pas à l'usage du chiffrement à clé publique – d'autres menaces adoptent la même technique – mais à sa simplicité et au fait que l'auteur a choisi d'utiliser un programme de chiffrement légal et Open Source, au lieu de créer sa propre mise en oeuvre, ce que font souvent les auteurs de malwares.

Les chercheurs prévoient une augmentation des menaces

Il existe certains programmes d'extorsion complexes avec des fonctionnalités avancées, développés essentiellement pour être vendus à d'autres cybercriminels qui n'ont pas les compétences nécessaires. Mais Trojan.Ransomcrypt.L montre qu'il est devenu possible de développer ce type de logiciels malveillants à peu de frais et sans connaissance de programmation avancée. Si bien que les chercheurs de Symantec s'attendent à une augmentation du nombre de menaces de ce type dans l'avenir.

Article de Jean Elyan avec IDG News Service

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.lemondeinformatique.fr/actualites/lire-un-logiciel-d-extorsion-utilise-un-simple-fichier-batch-58248.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter