Un caïd du ransomware gagne 90 000 dollars par an

Un caïd du ransomware gagne 90 000 dollars par an

Spécialiste du Dark web, Flashpoint a étudié les dessous d'une campagne russe de « ransomware-as-a-service » (RaaS). Son pilote aurait gagné 7 500 dollars par mois en moyenne.

Fournisseur d'analyses des Deep et Dark web, Flashpoint a étudié les dessous d'une campagne de « ransomware-as-a-service » (RaaS) pilotée, selon lui, par des escrocs russes. Le RaaS consiste pour l'auteur du rançongiciel à proposer à d'autres de diffuser des versions personnalisées de son programme pour chiffrer les données et verrouiller les terminaux d'utilisateurs. Les cibles sont appelées à payer en cryptomonnaie pour reprendre le contrôle de leurs données. La rançon est perçue par l'auteur du ransomware qui la partagera ensuite avec les diffuseurs.
C'est ainsi qu'une pointure des ransomwares en Russie aurait mené la campagne RaaS étudiée ces cinq derniers mois par Flashpoint. L'auteur de la campagne, qui ciblait des entreprises occidentales et des particuliers depuis au moins 2012, selon Flashpoint, aurait recruté des diffuseurs du programme ayant pour mission de trouver et infecter des cibles en échange d'un pourcentage sur les profits générés. Les novices étaient également invités à se lancer, sans frais d'entrée, le programme malveillant à diffuser étant accompagné d'instructions détaillées qu'un « écolier » pourrait suivre.

L'appât du gain

Le « patron » russe aurait ainsi recruté 10 à 15 « affiliés » chargés de diffuser le code de son ransomware. Soit en achetant un accès à des ordinateurs infectés, soit en passant par des serveurs insécurisés, ou du spam, ou encore en leurrant des utilisateurs de sites de rencontre et réseaux sociaux. Une fois que le code est installé et s'exécute, son auteur se charge des communications avec les victimes pour obtenir une rançon d'un montant moyen de 300 dollars par clé de déchiffrement et par victime, mais une somme additionnelle peut être exigée avant l'envoi de la clé.
Pour le paiement, la cryptomonnaie Bitcoin a été utilisée. 40 % des fonds ainsi détournés auraient été partagés entre les affiliés et 60 % seraient revenus au pilote de la campagne. Le « boss du ransomware » aurait ainsi empoché 7 500 dollars par mois en moyenne (90 000 dollars par an) et ses affiliés près de 600 dollars par mois chacun. Cela représente près de 30 paiements de rançon par mois.
« Nos résultats contestent la perception commune de cybercriminels hors du commun, éclairés, aisés, inaccessibles, inexposables et inarrêtables », soulignent les auteurs de l'étude. Et « Les montants des revenus du ransomware ne sont pas aussi séduisants et juteux » que l'on pourrait le croire. Il n'empêche, ces montants sont bien supérieurs au salaire moyen russe passé, selon une analyse de la Sberbank citée par RFI, de 1058 dollars par mois en 2012 à 433 dollars par mois en 2016.

crédit photo © frank_peters / Shutterstock.com
Article original de Ariane Beky

Réagissez à cet article

Original de l'article mis en page : Un caïd du ransomware gagne 90 000 dollars par an

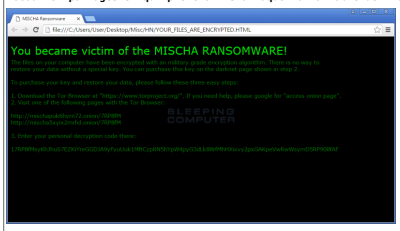
---

Mischa, le ransomware

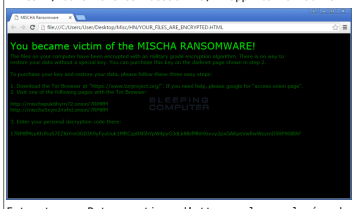
successeur de Petya

Mischa, le ransomware successeur de Petya

Apparu au mois de mars, le ransomware Petya a ouvert une nouvelle voie dans le développement des ransomwares. Il s'agissait du premier cas d'un malware qui allait au-delà du chiffrement des fichiers sur les disques locaux et partagés et qui préférait s'attaquer à la table de fichiers principale



Ceci étant dit, Petya n'était pas infaillible et les chercheurs ont été rapidement en mesure de créer un outil de restauration de certains des fichiers chiffrés par ce malware. Les individus malintentionnés n'ont pas perdu leur temps et ils ont trouvé le moyen de contourner une autre lacune de Petya : sa dépendance vis-à-vis de la volonté de la victime qui doit octroyer au malware les autorisations d'administrateur pour accéder à la table de fichiers principale (MFT).
Un nouveau programme d'installation de Petya a été détecté la semaine dernière. Celui-ci utilise un scénario de réserve. Si le malware n'obtient pas les autorisations d'administrateur au lancement, c'est un autre ransomware qui sera installé sur la machine infectée, en l'occurrence Mischa.
D'après les explications de Lawrence Abrams, de chez Bleeping Computer, les autorisations d'administrateur indispensables au fonctionnement de Petya figurent dans le manifeste de la version originale. Dans les commentaires envoyés à Threatpost, Lawrence Abrams explique « qu'avant l'exécution du code, Windows affiche la boîte de dialogue UAC qui sollicite ces autorisations. Si le service UAC est désactivé, l'application est exécutée automatiquement avec [les autorisations d'administrateur]. Si l'utilisateur clique sur « No » dans la fenêtre UAC, l'application n'est pas exécutée et, par conséquent, l'installation de Petya n'a pas lieu ».
Pour les exploitants de Petya, ces échecs représentent un gaspillage de ressources d'après Lawrence Abrams. Pour rectifier le tir, ils ont empaqueté un autre ransomware avec le programme d'installation. Il s'agit de Mischa qui sera exécuté si l'option « Petya » n'a pas pu être mise en œuvre.
Le manifeste de la nouvelle version indique que le fonctionnement requiert les données du compte utilisateur. Dans ce cas, Windows autorise le lancement de l'application sans afficher d'avertissement UAC. Comme l'explique Lawrence Abrams, « au lancement du programme d'installation, il sollicite les autorisations d'administrateur conformément à ses paramètres. La boîte de dialogue UAC s'affiche et si l'utilisateur choisit « Yes », ou si UAC est désactivé, l'application obtient les autorisations d'administrateur et installe Petya. Dans le cas contraire, c'est Mischa qui sera installé. Cette méthode est très intelligente ».



Entre temps, Petya continue d'attaquer les employées des services des ressources humaines allemands à l'aide de messages non sollicités qui contiennent des liens vers un fichier malveillant dans le cloud. Au début, les individus malintentionnés utilisaient Dropbox, mais depuis le blocage des liens Dropbox malveillants, ils se sont rabattus sur le service allemand TelekomCloud. Le fichier exécutable se dissimule sous les traits d'un fichier PDF qui serait un prétendu CV d'un candidat à un poste libre. Il contient même une photo.
« Lorsque l'utilisateur télécharge le fichier exécutable, l'icône PDF s'affiche, ce qui laisse penser qu'il s'agit bien d'un CV au format PDF » explique Lawrence Abrams. Toutefois, lorsque ce fichier est ouvert, il tente d'installer Petya. Et si cela ne marche pas, il installe le ransomware Mischa.
Le comportement de Mischa est identique à celui des autres ransomwares standard. Il analyse le disque local à la recherche de fichiers portant certaines extensions. Il chiffre les fichiers à l'aide d'une clé AES et ajoute à leur nom une extension de 4 caractères, par exemple 7GP3. Lawrence Abrams explique que « lorsque Mischa chiffre le fichier, il conserve la clé de chiffrement à la fin du fichier obtenu. Il convient de noter qu'il ne chiffre pas uniquement les fichiers traditionnels dans ce genre d'attaque (PNG, JPG, DOCX, etc.), mais également les fichiers EXE. »
Une fois qu'il a chiffré les fichiers, Mischa exige le versement d'une rançon de 1,93 bitcoins (environ 875 dollars américains) pour le déchiffrement. La somme doit être payée via le site Tor. Il n'existe pas encore d'outil de déchiffrement pour ce ransomware. « Nous conseillons aux victimes de vérifier avant tout la conservation des clichés instantanés à l'aide de Shadow Explorer. Ils pourraient être utile pour restaurer une ancienne version des fichiers chiffrés » conclut Lawrence Abrams.

Article du Kaspersky Lab

Réagissez à cet article

Source : *Petya possède un suppléant : Mischa – Securelist*

Forte hausse des applications Android malveillantes

Forte hausse des applications Android malveillantes

Les applications Android malveillantes et les ransomwares dominent le paysage des menaces au 1er trimestre 2016.

La société Proofpoint a publie son Rapport trimestriel sur les menaces, qui analyse les menaces, les tendances et les transformations observées au sein de notre clientèle et sur le marché de la sécurité dans son ensemble au cours des trois derniers mois. Chaque jour, plus d'un milliard de courriels sont analysés, des centaines de millions de publications sur les réseaux sociaux et plus de 150 millions d'échantillons de malwares afin de protéger les utilisateurs, les données et les marques contre les menaces avancées. On apprend, entre autres, que 98 % des applications mobiles malveillantes examinées au 1er trimestre 2016 ont ciblé des appareils Android. Cela demeure vrai en dépit de la découverte médiatisée d'un cheval de Troie pour iOS et de la présence persistante d'applications iOS ou officieuses dangereuses. Les applications Android malveillantes sont de plus en plus nombreuses.

75 % des attaques de phishing véhiculées par des e-mails imposteurs comportent une adresse «répondre à » usurpée afin de faire croire aux destinataires que l'expéditeur est une personne représentant une autorité. Ce type de menaces est de plus en plus mature et spécialisé, et c'est l'un des principaux ciblant les entreprises aujourd'hui, qui leur auraient coûté 2,6 milliards de dollars au cours des deux dernièresannées selon les estimations.

Applications Android malveillantes

Les ransomwares se sont hissés aux premiers rangs des malwares privilégiés par les cybercriminels. Au 1er trimestre, 24 % des attaques par e-mail reposant sur des pièces jointes contenaient le nouveau ransomware Locky. Seul le malware Dridex a été plus fréquent.

L'e-mail reste le principal vecteur de menaces : le volume de messages malveillants a fortement augmenté au 1er trimestre 2016, de 66 % par rapport au 4ème trimestre 2015 et de plus de 800 % comparé au 1er trimestre 2015. Dridex représente 74 % des pièces jointes malveillantes.

Chaque grande marque analysée a augmenté ses publications sur les réseaux sociaux d'au moins 30 %. L'accroissement du volume des contenus générés par les marques et leurs fans va de pair une accentuation des risques. Les entreprises sont constamment confrontées au défi de protéger la réputation de leurs marques et d'empêcher le spam, la pornographie et un langage grossier de polluer leur message.

Les failles de Java et Flash Player continuent de rapporter gros aux cybercriminels. Angler est le kit d'exploitation de vulnérabilités le plus utilisé, représentant 60 % du trafic total imputable à ce type d'outil. Les kits Neutrino et RIG sont également en progression, respectivement de 86 % et 136 %. (ProofPoint)… [Lire la suite]

Article de Damien BANCAL

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Forte hausse des applications Android malveillantes – Data Security BreachData Security Breach*

Un vague massive de spams JavaScript distribue le ransomware Locky

Un vague massive de spams JavaScript distribue le ransomware Locky

---

Les pays européens sont aujourd'hui victimes d'une vague de spams essayant d'exécuter un code JavaScript installant le redoutable ransomware Locky.

Au cours de la semaine écoulée, un grand nombre d'ordinateurs à travers l'Europe – et d'autres endroits dans le monde dont les Etats-Unis et le Canada – ont été touchés par une campagne massive de spams transportant des pièces jointes JavaScript malveillantes qui installent le ransomware Locky. Les pièces jointes sont généralement des fichiers d'archives .zip qui contiennent .js ou fichiers .jse intérieur. Ces fichiers s'exécutent directement sous Windows sans avoir besoin d'applications supplémentaires.

L'éditeur spécialisé dans la sécurité ESET a observé un pic dans les détections de JS / Danger.ScriptAttachment, un téléchargeur malware écrit en JavaScript qui a démarré le 22 mai et a atteint son sommet le 25 mai. JS / Danger.ScriptAttachment permet de télécharger divers programmes malveillants à l'insu des internautes, mais il a récemment été adapté pour distribuer Locky, un programme malveillant répandu qui utilise un chiffrement fort pour crypter les fichiers des utilisateurs. Cependant, il est très rare que des gens envoient des applications légitimes écrites en JavaScript par email. Les utilisateurs devraient éviter d'ouvrir ce type de fichiers.

La France touchée à 36%

De nombreux pays en Europe ont été touchés. Les taux de détection les plus élevés ont été observés au Luxembourg (67%), en République tchèque (60%), en Autriche (57%), aux Pays-Bas (54%), au Royaume Unie (51%) et en France 36%. Les données de télémétrie de l'éditeur ont également montré des taux de détection importants pour cette menace au Canada et aux États-Unis. Bien que Locky n'a pas de défauts connus qui permettraient aux utilisateurs de déchiffrer leurs fichiers gratuitement, les chercheurs en sécurité de Bitdefender ont développé un outil gratuit qui peut prévenir les infections Locky. L'outil trompe le ransomware en lui indiquant que l'ordinateur est déjà infecté.
L'utilisation de fichiers JavaScript pour distribuer Locky a commencé un peu plus tôt cette année, ce qui a incité Microsoft à publier une alerte à ce sujet en avril dernier.
Article de Lucas Mearian/ IDG NS (adaptation SL)

Réagissez à cet article

Source : *Un vague massive de spams JavaScript distribue le ransomware Locky – Le Monde Informatique*

Augmentation de 30% des demande de rançon informatique en 3 mois

	**Augmentation de 30% des demande de rançon informatique en 3 mois**

Le #ransomware a dépassé les attaques de type APT (menaces persistantes avancées) pour devenir le principal sujet d'actualité du trimestre. 2900 nouvelles variantes de malwares au cours de ces 92 jours.

Selon le rapport de Kaspersky Lab sur les malwares au premier trimestre, les experts de la société ont détecté 2900 nouvelles variantes de malwares au cours de cette période, soit une augmentation de 14 % par rapport au trimestre précédent. 15 000 variantes de ransomware sont ainsi dorénavant recensés.

Un nombre qui va sans cesse croissant.
Pourquoi ? Comme j'ai pu vous en parler, plusieurs kits dédiés aux ransomwares sont commercialisés dans le blackmarket. Autant dire qu'il devient malheureusement très simple de fabriquer son arme de maître chanteur 2.0.
Au premier trimestre 2016, les solutions de sécurité de l'éditeur d'antivirus ont empêché 372 602 attaques de ransomware contre leurs utilisateurs, dont 17 % ciblant les entreprises. Le nombre d'utilisateurs attaqués a augmenté de 30 % par rapport au 4ème trimestre 2015. Un chiffre à prendre avec des pincettes, les ransomwares restant très difficiles à détecter dans leurs premiéres apparitions.

Locky , l'un des ransomwares les plus médiatisés et répandus au 1er trimestre
Le ransomware Locky est apparu, par exemple, dans 114 pays. Celui-ci était toujours actif début mai. Un autre ransomware nommé Petya est intéressant du point de vue technique en raison de sa capacité, non seulement à crypter les données stockées sur un ordinateur, mais aussi à écraser le secteur d'amorce (MBR) du disque dur, ce qui empêche le démarrage du système d'exploitation sur les machines infectées.
Les trois familles de ransomware les plus détectées au 1er trimestre ont été Teslacrypt (58,4 %), CTB-Locker (23,5 %) et Cryptowall (3,4 %). Toutes les trois se propagent principalement par des spams comportant des pièces jointes malveillantes ou des liens vers des pages web infectées. « Une fois le ransomware infiltré dans le système de l'utilisateur, il est pratiquement impossible de s'en débarrasser sans perdre des données personnelles. » confirme Aleks Gostev, expert de sécurité en chef au sein de l'équipe GReAT (Global Research & Analysis Team) de KL.

Une autre raison explique la croissance des attaques de ransomware : les utilisateurs ne s'estiment pas en mesure de combattre cette menace. Les entreprises et les particuliers n'ont pas conscience des contre-mesures technologiques pouvant les aider à prévenir une infection et le verrouillage des fichiers ou des systèmes, et négligent les règles de sécurité informatique de base, une situation dont profitent les cybercriminels entre autres. Bref, trop d'entreprise se contente d'un ou deux logiciels de sécurité, se pensant sécurisées et non concernées. L'éducation du personnel devrait pourtant être la priorité des priorités… [Lire la suite]

Article de Damien BANCAL

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybersécurité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Ransomware: +30% d'attaques en 3 mois – Data Security BreachData Security Breach*

Un hôpital paye la rançon mais n'obtient rien en échange.

Un hôpital paye la rançon mais n'obtient rien en échange

Certains groupes de pirates qui exploitent des ransomwares pour faire fortune sans effort n'ont ni morale ni parole, si l'on en croit la prise en otage de données d'un hôpital, qui a payé pour rien la rançon demandée.

Les maître-chanteurs sont aussi parfois de véritables escrocs, et ça n'est jamais une bonne idée de céder à leurs exigences. Après la messagerie chiffrée Protonmail qui avait payé une rançon et avait malgré tout continué à subir des attaques DDOS massives, c'est un hôpital américain qui l'apprend à ses dépens.

Ainsi Network World rapporte que le Kansas Heart Hospital à Wichita a accepté de payer une rançon après que des pirates ont réussi à infecter son système informatique avec un ransomware, qui chiffre les données stockées avec une clé que seul le ravisseur connaît. Ce n'est pas le premier hôpital à être visé et à céder ainsi à un chantage informatisé, mais c'est la première fois que les pirates ne respectent pas leur part du marché. Pire, ils en demandent plus.

PAYER ENCORE POUR DÉBLOQUER UN PEU PLUS

L'attaque avait eu lieu la semaine dernière, et avait rendu des fichiers de l'hôpital inaccessibles, sans possibilité de recourir à des archives. Pour les débloquer, il fallait payer de l'argent en utilisant un service anonymisé, sur Tor, avec un compte en bitcoins intraçable. Étant donnée l'importance des données, les administrateurs de l'établissement ont accepté de payer une somme indéterminée, relativement faible. Mais plutôt que de déchiffrer les données, les pirates n'en ont libéré qu'une petite partie, et exigé davantage d'argent pour déchiffrer le reste.

L'hôpital a alors refusé. « Ce n'était plus une manœuvre sage ou une stratégie », s'est justifiée la direction, qui a mis en place un plan B pour limiter les effets de l'attaque. Selon le Kansas Heart Hospital, aucun patient n'a eu à subir d'effets négatifs en raison de l'indisponibilité de certaines données… [Lire la suite]

Réagissez à cet article

Source : *Ransomware : un hôpital paye la rançon mais n'obtient*

rien en échange – Business – Numerama

Auteur : Guillaume Champeau

Victime du ransomware TelsaCrypt ? Voici finalement la clé de déchiffrement

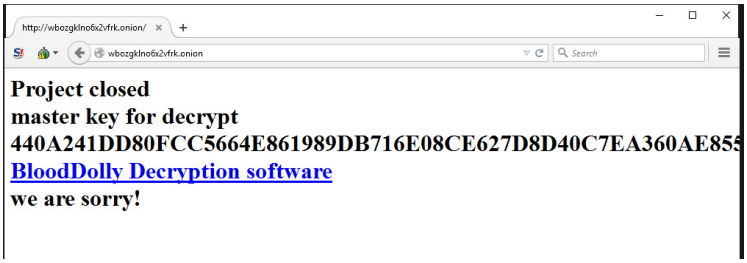
Victime du ransomware TelsaCrypt ? Voici finalement la clé de déchiffrement

---

Les auteurs du ransomware TeslaCrypt ont décidé de réparer leurs méfaits en fournissant gracieusement la clé qui permet aux victimes du logiciel d'extorsion de reprendre le contrôle sur leurs données.

Les maître-chanteurs des temps modernes auraient-ils aussi parfois une conscience, qui se réveille tardivement ? Depuis de nombreux mois, des groupes de délinquants anonymes inondaient des systèmes informatiques d'un ransomware basé sur le framework TeslaCrypt, à l'action hélas désormais bien connue. La victime se retrouvait avec tous ses fichiers et documents personnels chiffrés sur son disque dur, et le seul moyen de les déchiffrer pour y avoir de nouveau accès était de payer une rançon, en suivant les instructions affichées à l'écran. Mais l'auteur (ou les auteurs ?) de TeslaCrypt a décidé de faire amende honorable.

L'éditeur de logiciels de sécurité ESET avait en effet remarqué que les créateurs de TeslaCrypt avaient choisi de mettre fin à leur projet maléfique. Prenant leur audace à deux mains, les ingénieurs du groupe ont donc contacté les créateurs de TeslaCrypt en passant par le service d'assistance intégré au ransomware, et leur ont demandé s'ils accepteraient de publier la « master key » qui permettrait à toutes les victimes de déchiffrer leurs fichiers sans payer un centime.
À leur propre surprise, les pirates ont accepté. La clé est désormais visible sur le site du groupe (accessible uniquement en passant par Tor).



« *Nous sommes désolés* », peut-on lire sur ce site, qui donne également le lien vers un outil de déchiffrement mis au point par BloodDolly, présenté par BleepingComputer comme un « expert de TeslaCrypt ». Il avait déjà proposé un outil gratuit pour déchiffrer les fichiers bloqués par TeslaCrypt 1.0, mais la communication de la clé maître permet désormais à l'outil de déchiffrer y compris TeslaCrypt 3.0 et TeslaCrypt 4.0. ESET a également publié son propre outil gratuit.
L'histoire ne dit pas pourquoi les auteurs du ransomware ont été pris de remords… [Lire la suite]

Réagissez à cet article

Source : *Les auteurs du ransomware TelsaCrypt s'excusent et offrent la clé – Tech – Numerama*

Prise d'otage numérique par Rançongiciels, la nouvelle arme fatale des cyberpirates

Prise d'otage numérique par Rançongiciels, la nouvelle arme fatale des cyberpirates

---

Les prises d'otages numériques, avec demande de rançon, se multiplient. Payer est souvent la seule solution

Locky, Cryptolocker, Synolocker, Cryptowall, TeslaCrypt, Petya… Si vous n'êtes pas un spécialiste de la sécurité informatique, ces noms barbares ne vous disent probablement rien. Et pourtant, ils représentent la nouvelle menace qui pèse sur vos ordinateurs. Depuis quelques années, en effet, un nouveau type de logiciel malveillant a le vent en poupe: les rançongiciels – un néologisme 2.0 dérivé du mot «ransomware» dans la langue de Shakespeare. Ces virus prennent, à distance, le contrôle de PC, tablettes ou smartphones et bloquent l'ensemble de leurs données. Pour les récupérer, les propriétaires légitimes sont sommés de payer une rançon dans un délai très court, dans une monnaie virtuelle et non traçable comme les bitcoins.
Selon une étude d'Intel Security-McAffe, datant de mars 2016, ce type d'attaque a augmenté de 26% au dernier trimestre 2015, par rapport à l'année précédente.

Les PME ne sont pas préparées

«Les demandes de rançons après un piratage sont en plein essor dans le monde et en Suisse, résume Ilia Kolochenko, CEO et fondateur de l'entreprise genevoise High-Tech Bridge, spécialisée dans la sécurité informatique. C'est devenu une véritable industrie.»
De fait, les exemples se multiplient – proches de nous. En avril 2016 par exemple, Ralph Eberhard, patron de la gérance Immogeste basée à Genève, témoigne dans le journal *Le Temps* avoir dû payer 1800 francs à des hackers. Le même mois, un peu plus loin d'ici, dans le Béarn, le PDG d'une entreprise raconte peu ou prou la même histoire, dans le journal *La République des Pyrénées*.
En effet, à chaque fois le scénario est identique. Un matin, en allumant leurs ordinateurs, les salariés voient s'afficher sur leur moniteur un message martial, généralement rouge sur fond noir, qui dit en substance: «Tous les fichiers de votre disque dur ont été cryptés. Pour les déchiffrer et les récupérer, vous devez nous payer.» La plupart du temps, les montants exigés ne s'avèrent pas dissuasifs: de quelques centaines de francs pour des particuliers à quelques milliers pour les PME. Mais parfois les sommes demandées sont astronomiques. En février 2016, un ransomware a infecté un hôpital de Los Angeles, bloquant l'ensemble des données médicales des patients. Pour remettre le système d'information d'aplomb, les pirates ont réclamé 9000 bitcoins, soit l'équivalent de 3,6 millions de dollars!
«Auparavant, les hackers s'attaquaient à de grosses entreprises, afin de toucher le jackpot, rappelle Ilia Kolochenko. Aujourd'hui, ils se recentrent sur les PME et les particuliers, parce qu'ils ont compris que même si les sommes obtenues sont moindres, l'activité se révèle moins risquée et plus facile. Si vous attaquez une grande banque, vous devez d'abord déjouer une sécurité informatique de premier plan. Et si vous y parvenez, vous pouvez être certain qu'elle ne vous lâchera jamais. Elle vous traquera pendant des années s'il le faut. A l'inverse, les particuliers et les PME ne sont absolument pas préparés à ce type d'attaque et en plus ne disposent pas des moyens nécessaires pour retrouver les auteurs.» Selon un rapport de Symantec publié en avril 2016, 57% de ces attaques ciblent des entreprises de moins de 250 salariés.
Mais comment ces logiciels malveillants se diffusent-ils? «Ces chevaux de Troie accèdent à l'ordinateur par le biais de courriels infectés ou de sites Internet piratés», explique la centrale Melani. Concrètement, «les hackers possèdent des robots informatiques, les botnets, qui scrollent l'ensemble des pages Internet – un peu comme Google – à la recherche de failles connues, explique Ilia Kolochenko. Lorsqu'une vulnérabilité est découverte, le virus s'installe et attend sa victime, en affichant par exemple un nouveau lien. Lorsque quelqu'un clique sur ce dernier, le virus passe sur son ordinateur et crypte l'ensemble des données.»

Faut-il payer la rançon ou pas?

Face à cette situation, la centrale Melani recommande de «ne pas céder à l'extorsion car, en payant la rançon, vous participez au financement de l'activité des criminels et leur permettez d'améliorer l'efficacité de leurs prochaines attaques. De plus, il n'existe aucune garantie que les criminels respecteront leur engagement et vous enverront réellement la clé vous permettant de récupérer vos données.»
En pratique, les choses s'avèrent plus compliquées, notamment pour les PME qui, privées de leurs fichiers clients, voient toute leur activité bloquée. «Si vous êtes infectés, il n'existe pas 3000 solutions, reconnaît Ilia Kolochenko. La première consiste à faire des recherches sur Internet, afin de savoir s'il existe déjà une clef de décryptage contre le rançongiciel. Malheureusement, c'est rarement le cas. La seconde, c'est payer. Si vous vous adressez à une entreprise comme la nôtre, nous finirons par remonter jusqu'au coupable et nous parviendrons peut-être à récupérer vos données. Mais cela va prendre beaucoup de temps. Même si cela peut paraître immoral, c'est moins coûteux pour une PME de régler la rançon que de lancer des investigations.» (TDG)
_ [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises Techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.L.I. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité (CNIL) de votre établissement.

Le Net Expert INFORMATIQUE
Contactez-nous

Réagissez à cet article

Source : *Sécurité informatique: Rançongiciels, la nouvelle arme fatale des cyberpirates – News High-Tech: Hard-/Software – tdg.ch*

Jigsaw, un rançongiciel avec compte à rebours destructeur

Jigsaw, un rançongiciel avec compte à rebours destructeur

Une heure… C'est le délai que laisse à sa victime le rançongiciel Jigsaw pour verser sa rançon. Passé ce délai, il commence à détruire les fichiers de l'ordinateur en accélérant son rythme toutes les heures. Des experts en sécurité ont trouvé le moyen de s'en débarrasser. Pour l'instant.

Apparemment, le versement d'une rançon en bitcoins ne suffit plus à certaines cyber-fripouilles, auteurs de ransomwares, pour fournir à leurs victimes la clé qui leur permettra de déchiffrer les fichiers de leur ordinateur. Il s'en trouve maintenant pour exiger des utilisateurs attaqués qu'ils s'en acquittent en moins d'une heure. Un nouveau programme dénommé Jigsaw chiffre les fichiers et commence à les détruire petit à petit jusqu'à ce que le malheureux utilisateur verse l'équivalent de 150 dollars en monnaie virtuelle Bitcoin. Après une heure, le ransomware détruit l'un après l'autre les fichiers, puis, après chaque cycle de 60 minutes, augmente le nombre de fichiers supprimés. Si aucun paiement n'est effectué dans un délai de 72 heures, tous les fichiers restants disparaissent. « Essayez de tenter quelque chose d'amusant et l'ordinateur appliquera certaines mesures de sécurité pour détruire vos fichiers », prévient un message du pirate accompagnée du masque du personnage de tueur Jigsaw, de la série de films d'horreur Saw.

Et ce n'est pas une menace en l'air.

Le malware est tout sauf inactif. Selon certains experts du forum de support technique BleepingComputer.com, ce rançongiciel détruit un millier de programmes à chaque fois que l'ordinateur redémarre ou que son processus est relancé. Dans un billet, Lawrence Abrams, fondateur du site, constate que c'est la première fois que l'on voit ce type de menaces propagées par le biais d'une infection par ransomware. La bonne nouvelle, pour l'instant, c'est que les experts ont élaboré une méthode pour déchiffrer les fichiers affectés par Jigsaw sans avoir à payer la rançon.

Inactiver Jigsaw puis déchiffrer les fichiers à l'aide d'un utilitaire

La première chose à faire, c'est d'ouvrir le gestionnaire de tâches de Windows et de terminer tous les processus appelés firefox.exe ou drpbx.exe qui ont été créés par le ransomware, indique Lawrence Abrams. Puis, il faut lancer l'utilitaire Windows MSConfig et supprimer l'entrée de démarrage pointant vers %UserProfile%AppDataRoamingFrfxfirefox.exe. Cela arrêtera le processus de destruction des fichiers et empêchera le malware de se relancer au redémarrage du système. Les utilisateurs pourront alors télécharger l'utilitaire Jigsaw Decrypter hébergé par BleepingComputer.com afin de déchiffrer leurs fichiers. Lorsque ce sera fait, il est hautement recommandé de télécharger un logiciel anti-malware à jour et de lancer un scan complet de son ordinateur pour désinstaller entièrement le ransomware.
En novembre, un précédent programme d'attaque dénommé Chimera menaçait de diffuser les fichiers des utilisateurs sur Internet. Toutefois, rien n'a prouvé qu'il était en mesure de le faire. Par comparaison, Jigsaw met ses menaces à exécution et révèle une évolution inquiétante sur ce terrain. Si les experts en sécurité ont trouvé un moyen de déchiffrer les fichiers cette fois, rien ne garantit qu'ils pourront le faire avec les prochaines versions. Les pourvoyeurs de ransomware sont généralement prompts à corriger leurs erreurs… [Lire la suite]

Pour info, en plus des technologies indispensables comme l'**anti-phishing** (pour **se protéger des e-mails de phishing**) et l'**anti-malware** (pour **se protéger des malwares cachés dans des e-mails ou des sites internet infectés**) qui protègent les clients contre les menaces d'Internet, ESET Smart Security 9 contient une toute nouvelle protection des transactions bancaires. Cette fonction met à disposition l'ouverture d'un navigateur sécurisé pour veiller à ce que toutes les transactions financières en ligne soient effectuées en toute sécurité. L'utilisateur peut également paramétrer lui-même tous les sites bancaires de paiement en ligne qu'il consulte le plus fréquemment.

Réagissez à cet article

Alerte à partager ! Attaques ransomwares aux couleurs d’Orange indétectable

	Alerte à partager ! Attaques ransomwares aux couleurs d’Orange indétectable par les anti-virus

Les attaques ransomwares ne baissent pas. Après avoir usurpé des avocats, des comptables, des PME, des mairies, FREE, voici le courriel piégé aux couleurs d'Orange. Ne cliquez surtout pas sur la pièce jointe.

Le courriel s'invite dans votre boites à mails avec comme objet : « ***Votre demande d'assistance*** » ; « ***Votre assistance Orange*** » ; « ***Votre assistance Orance Business***« . La missive pirate indique qu'une anomalie lors d'un prélèvement oblige le lecteur internaute à lire le fichier joint, un PDF piégé baptisé « ***Montant du mois*** » ou encore « ***Montant de la facture***« . Un piège qui, heureusement, est plutôt mal réalisé pour les internautes avertis. Il peut, cependant, piéger les plus curieux. La cible étant clairement les entreprises, une secrétaire, un comptable ou un responsable n'ayant pas vraiment le temps de lire autrement qu'en « Z » sera tenté de cliquer.

Au moment de l'analyse des fichiers, aucun antivirus n'avait la signature de la bestiole en mémoire. **A noter qu'un antivirus, face à ce genre d'attaque ne peut pas grand chose. Chaque mail et fichier joint portent en eux une signature (identification) unique et différente…** [Lire la suite]

Réagissez à cet article

Source : *ZATAZ Attaques ransomwares aux couleurs d’Orange – ZATAZ*