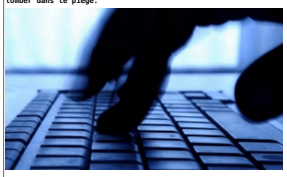
Découvrez le TOP 5 des arnaques informatiques les plus récurrentes au premier trimestre 2016 selon la PLCC

	Découvrez le TOP 5 des arnaques informatiques les plus récurrentes au premier trimestre 2016 selon la PLCC

En Côte d'Ivoire, les préjudices financiers causés par les cybercriminels se chiffrent en milliards. Dans sa stratégie de sensibilisation, la Plateforme de Lutte Contre la Cybercriminalité (PLCC) entreprend d'informer les populations sur les arnaques les plus récurrentes afin de leur permettre de ne pas tomber dans le piège.



Selon les chiffres communiqués par la PLCC, au cours de l'année 2015, le préjudice financier causé par la cybercriminalité a atteint 3 980 833 802 FCFA, contre **5 280 000 FCFA** en 2015. Ce sont **1 409** plaintes qui ont été enregistrées. Elles ont abouti à l'arrestation de **205** individus, dont **159** ont été déférés au parquet. Afin d'informer davantage les populations, la PLCC a sorti les 5 types arnaques qui ont été les plus récurrentes au cours du premier trimestre 2016.

1- La Sextorsion (Enregistrement illégal de communication privée, chantage à la vidéo)

Ce type d'arnaque a occasionné un préjudice de **119 millions de Franc CFA**. Cette technique consiste pour un cybercriminel à se procurer une vidéo intime de sa victime et d'exercer sur elle un harcèlement dont la condition de dénouement est le paiement d'une somme d'argent. Pour y arriver, le cybercriminel s'arrange à établir une relation amicale voire amoureuse avec sa future victime, de manière à gagner son entière confiance. Par la suite, il lui demandera de lui fournir ladite vidéo (en lui demandant d'activer sa caméra au cours d'un échange par exemple), qui deviendra finalement le moyen de pression du cybercriminel.

2 – L'accès frauduleux à un système informatique

Ce type d'arnaque est généralement orienté vers les entreprises. Au premier trimestre 2016, il a causé un préjudice financier de **42.271.426 F CFA**. Elle consiste pour le cybercriminel, à forcer l'accès d'un système informatique pour éventuellement voler des donner, ou causer des dégâts pour porter préjudice.

3 – L'usurpation d'identité (Utilisation frauduleuse d'élément d'identification de personne physique ou morale)

L'usurpation d'identité consiste pour un individu à se faire passer pour une autre. Avec des moyens détournés, le cybercriminel réussi à soutirer des informations sensibles qu'il utilise plus tard pour effectuer des paiements, effectuer des paiements etc. Il peut même aller plus loin en engageant la personne de sa victime, par une signature d'accord par exemple, sans son consentement préalable. Ce sont 37.851.973 Franc CFA de dommages qui ont été causés par ce type d'arnaque sur la même période.

Lire aussi : INTERNET : La sécurité des usagers, dernier soucis des fournisseurs d'accès en Côte d'Ivoire ?

4 – L'arnaque au faux sentiment

Ce type d'arnaque est en net recul, après avoir fait de nombreuses victimes à travers le monde. De plus en plus, les internautes sont plus prudents quoique des victimes continuent de se faire duper. 28.754.746 F CFA, c'est le préjudice causé par ce type d'arnaque au premier trimestre 2016.

5 – La fraude sur le porte-monnaie électronique

Avec l'expansion des services de porte-monnaie électronique via le mobile, ce type d'arnaque a pris de l'ampleur.

Bien ficelée, cette technique pousse la victime donner le contrôle absolu à un cybercriminel sur son compte, sans même le réaliser. Par un simple appel ou SMS, le cybercriminel invite son sa victime à saisir un code USSD, pour bénéficier d'un prétendu bonus. Une fois que la procédure est engagée, la carte SIM de la victime est désactivée, son compte transférée sur une nouvelle carte SIM. Le cybercriminel a alors le contrôle absolu.

Article original de Stéphane Agnini

CREDIT : DR

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

- Expertises techniques (virus, exploits, 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

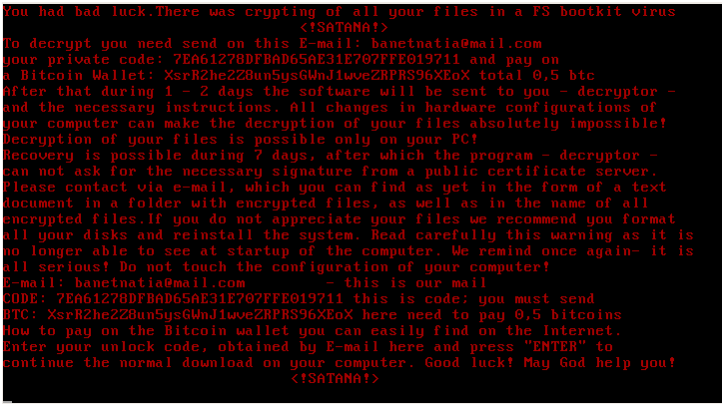
Original de l'article mis en page : Regionale.info CYBERCRIMINALITE : TOP 5 des arnaques les plus récurrentes au premier trimestre 2016 selon la PLCC > Regionale.info

---

Satana, un ransomware pire que Petya

Satana, un ransomware pire que Petya

Le nouveau rançomware Satana cumule chiffrement des fichiers et remplacement du secteur d'amorçage du disque.



Une nouvelle génération de ransomware est en train d'émerger. Satana, nom du nouveau malware, combine chiffrement des fichiers et écriture de code sur le secteur d'amorçage du disque, le MBR. Deux techniques inspirées de Petya et Mischa, note Malewarebytes qui constate la croissance du nouvel agent satanique ces dernières semaines.

« *Satana fonctionne en deux modes*, note la société de sécurité sur son blog. *Le premier se comporte comme Petya, un fichier exécutable (sous Windows, NDLR) [et] écrit au début du disque infecté un module de bas niveau, un bootloader avec un noyau personnalisé. Le deuxième mode se comporte comme un ransomware typique et chiffre les fichiers un par un (tout comme Mischa).* » Mais à la différence que les deux modes ne sont pas exploités alternativement mais bien appliqués ensemble, l'un après l'autre, pour s'attaquer à leurs victimes.

Payer ne garantit rien chez Satana

Malwarebytes ne le précise pas mais le mode de propagation de Satana reste probablement classique. A savoir par e-mail (et éventuellement d'un expéditeur en recherche de travail avec des liens vers les fichiers infectieux comme dans le cas de la première version de Petya). Une fois le MBR remplacé, le malware s'attaque au chiffrement des fichiers du disque (et des éventuels volumes reliés à l'ordinateur) et attend patiemment que le système soit redémarré. Quand c'est le cas, un message s'affiche sur l'écran expliquant la démarche à suivre pour récupérer l'accès à son PC, à savoir le paiement d'une rançon de 0,5 bitcoin (plus de 300 euros au cours du jour).

Si l'utilisateur parvient néanmoins à remplacer le MBR par un fichier d'amorçage sain (une manipulation manuelle qui est loin d'être à la portée de tout le monde), il se heurtera aux fichiers chiffrés sur le disque. Lesquels ont été renommés avec, en en-tête du nom, un e-mail aléatoirement choisi parmi ceux de l'équipe des développeurs de Satana, selon l'expert en sécurité (Gricakova@techmail.com, dans l'exemple présenté). Et les méthodes de chiffrement semblent suffisamment avancées pour rendre les fichiers piégés définitivement irrécupérables. D'autant que Malewarebytes pointe un bug pour le moins problématique pour la victime. De par le mécanisme de chiffrement/déchiffrement des fichiers, en cas de déconnexion au serveur de commandes et contrôle (C&C), la clé de décryptage (qui est la même que pour le cryptage) est perdue. Brisant tout espoir de la victime à pouvoir récupérer ses données (sauf à avoir fait préalablement des sauvegardes). « *Même les victimes qui paient peuvent ne pas récupérer leurs fichiers si elles (ou le C&C) sont hors ligne lorsque le chiffrement arrive* », prévient la société de sécurité.

Du code en cours de perfectionnement

Ce n'est pas la seule bizarrerie que remarque le chercheur Hasherezade, auteur du billet. Il constate également que, le ransomware affiche toute la procédure de son déploiement, y compris la progression du chiffrement des fichiers. « *Habituellement les auteurs de logiciels malveillants ne veulent pas laisser le code de débogage dans leur produit final* », écrit le chercheur. Lequel conclut que Satana est probablement encore en cours de développement et contient des failles. « *Le code d'attaque de bas niveau semble inachevée – mais les auteurs montrent un intérêt dans le développement du produit dans ce sens et nous pouvons nous attendre que la prochaine version sera améliorée.* » Une nouvelle génération de rançongiciel est bien en marche.

Article original de Christophe Lagane

Réagissez à cet article

Original de l’article mis en page : Satana, un ransomware pire que Petya

---

Nouvelle forme d’attaque informatique, les crypto-vers

Nouvelle forme d’#attaque informatique, les crypto-vers

Les cybercriminels ont trouvé une nouvelle manière de se faire de l'argent. Cela faisait longtemps qu'ils tentaient de prendre en otage des disques durs, mais les gens sont devenus plus vigilants et n'ouvrent plus n'importe quelle pièce jointe à un mail. Voilà pourquoi les cybercriminels se sont vu contraints d'inventer une nouvelle façon d'installer leur rançongiciel (#ransomware). Leur solution: le ver.

Le spécialiste de la sécurité Kaspersky lance donc une mise en garde. Le 'crypto-ver' est « une forme mixte dangereuse de maliciel (malware) et de rançongiciel qui se répand d'elle-même ». Elle peut se propager d'ordinateur à ordinateur, sans spam (pourriel) ou autre infection. Le malware se duplique simplement dans les appareils interconnectés.
Le premier ver, baptisé SamSam, s'est manifesté en avril. Et au cours des dernières semaines, des experts en sécurité ont découvert le ver ZCryptor. Ce dernier se présente sous la forme d'une simple mise à jour d'un programme largement utilisé tel Flash. Une fois en place, le ver commence à se propager, puis il crypte des dizaines d'extensions. Les victimes voient ensuite apparaître leur écran habituel, qui les informe que leurs fichiers ont été pris en otage et qu'ils doivent verser une rançon pour pouvoir y accéder de nouveau.
Les spécialistes des la sécurité n'ont pas encore trouvé une parade contre ZCryptor. Voilà pourquoi Kaspersky prodigue le conseil suivant: soyez sur vos gardes, veillez à disposer d'une bonne protection et effectuez régulièrement des sauvegardes (backups).

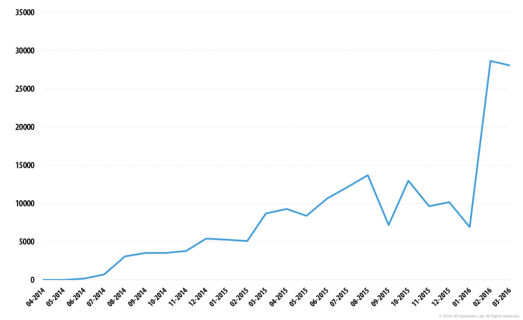
Réagissez à cet article

Original de l'article mis en page : Nouveau: le ver ravisseur – ICT actualité – Data News.be

Evolution des Ransomwares pour appareils mobiles en 2014-2016

Evolution des Ransomwares pour appareils mobiles en 2014-2016

L'activité des ransomwares pour appareils mobiles, qui ne bénéficie pas de la même couverture médiatique que les ransomwares pour PC, a également explosé au cours de la période couverte par le rapport. Et plus particulièrement au cours de la deuxième moitié de celle-ci.



Nombre d'utilisateurs confrontés à des ransomwares pour appareils mobiles au moins une fois au cours de la période comprise entre avril 2014 et mars 2016

D'avril 2014 à mars 2015, les solutions de Kaspersky Lab pour Android ont protégé 35 413 utilisateurs contre des ransomwares pour appareils mobiles. Un an plus tard, ce nombre avait presque quadruplé et atteignait 136 532 utilisateurs. La part des utilisateurs attaqués par des ransomware par rapport aux utilisateurs attaqués par n'importe quel autre type de malware a également augmenté : de 2,04 % pour la période 2014-2015, elle est passée à 4,63 % pour la période 2015-2016. La courbe de croissance est peut-être plus modeste que celle observée pour les ransomwares pour PC, mais son ampleur suffit à confirmer une tendance inquiétante.

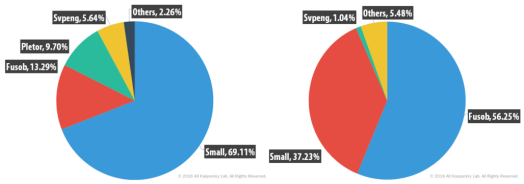
Principaux acteurs dans le milieu des ransomwares pour appareils mobiles

Sur l'ensemble de la période couverte par le rapport, les chercheurs de Kaspersky Lab ont été en mesure d'identifier les quelques familles de ransomwares pour appareils mobiles auxquelles les utilisateurs de nos produits étaient les plus souvent confrontés. En 2014-2015, il s'agissait de : Pletor, Fusob, Svpeng et Small. En 2015-2016, l'activité de Svpeng a enregistré une dégringolade et n'a concerné qu'une part modeste des utilisateurs attaqués.

A un moment donné en 2014-2015, Svpeng, connu à l'origine comme un malware bancaire, a été modifié par ses créateurs afin de pouvoir verrouiller un appareil infecté. Depuis lors, nous avons suivi les deux versions de Svpeng : le malware bancaire et le ransomware. La version ransomware est devenue populaire en 2014-2015 lorsqu'elle a touché 5,64 % des utilisateurs attaqués par un malware quelconque.

La situation a toutefois changé au cours de la deuxième période lorsque le ransomware a chuté vers le bas du Top 30 des menaces. Toutefois, la version malware bancaire de Svpeng a repris du service, ce qui signifie probablement que les créateurs du malware ont simplement perdu leur intérêt dans le développement d'un ransomware et ont décidé de se concentrer sur le malware bancaire.

Pletor, le malware considéré comme le premier exemple de ransomware et prétendument créé par les auteurs du tristement célèbre trojan bancaire Acecard, a connu une situation similaire. Au cours de la période 2014-2015, il a touché une part considérable des utilisateurs mobiles attaqués par des ransomwares mais en 2015-2016, il ne figurait plus dans le haut du classement et laissait le « marché » à seulement trois grandes familles de ransomwares.



Répartition de la part d'utilisateurs attaqués entre les familles de ransomwares pour appareils mobiles les plus actives en 2014-2015 (gauche) comparée à celle de 2015-2016 (droite).

Parmi les autres phénomènes importants observés au cours des 24 mois couverts par le rapport, on ne peut ignorer la concurrence entre deux grandes familles de ransomwares : Small et Fusob. En 2014-2015, c'est la famille Small qui dominait, du moins en termes de parts d'utilisateurs attaqués. Elle était signalée par 69,11 % de l'ensemble des utilisateurs qui avaient été confrontés au moins une fois à des ransomwares pour appareils mobiles. Mais un an plus tard, c'est la famille Fusob qui prenait la tête avec 56,25 % des utilisateurs. Toutefois, la famille Small se maintenait en 2e position avec 37,23 % des utilisateurs attaqués. Il est probable que les malwares Svpeng, Pletor, Small et Fusob seront vendus par leurs auteurs à d'autres cybercriminels ou qu'ils seront propagés via des réseaux d'affiliés. Les quatre familles ont subi de nombreuses modifications. Cependant, Small et Fusob semblent avoir été les plus modifiés, comme on peut le voir clairement dans les statistiques.

A la différence du phénomène des ransomwares pour PC qui est déjà largement couvert par les chercheurs de différentes sociétés, dont Kaspersky Lab, les ransomwares pour appareils mobiles n'ont pas encore fait l'objet d'une analyse en profondeur. Afin de remédier à cette situation, nous proposons une brève description des ransomwares les plus répandus et les plus dangereux à compter d'avril 2016

Pour en savoir plus sur l'évolution de la menace des ransomwares, lisez le rapport complet accessible via.

Article original de Kaspersky Lab

Réagissez à cet article

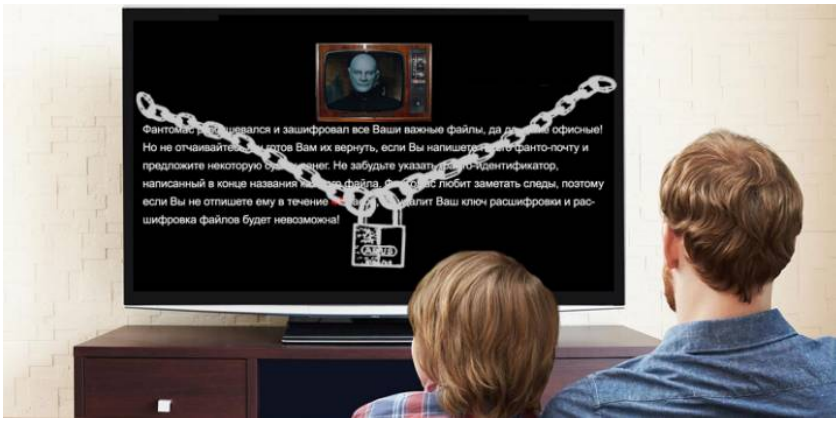
Original de l’article mis en page : Rapport KSN : ransomwares pour appareils mobiles en 2014-2016 – Securelist

---

Les Smart TV, nouvelle cible des ransomwares ?

Les Smart TV, nouvelle cible des ransomwares ?

Si les ransomwares sont chaque jour plus nombreux à venir « pourrir » le quotidien des particuliers comme des entreprises, voilà que ces derniers ne s'en prennent plus seulement aux ordinateurs et aux smartphones. En effet, Frantic Locker s'attaque également aux Smart TV.



Frantic Locker, le rançongiciel qui bloque les Smart TV

Alors que les ransomwares font de nombreuses victimes, le spécialiste de la sécurité informatique Trend Micro révèle que le rançongiciel Frantic Locker s'en prend désormais aux Smart TV.

Présent sur le marché depuis avril 2015, il n'a cessé d'évoluer et un grand nombre de variantes différentes ont développées lui permettant de s'ouvrir à de nouveaux horizons.

Ainsi, dernièrement, Frantic Locker, aussi connu sous le nom FLocker, est diffusé via des campagnes de spam par SMS ou bien par un site web préalablement piégé. Bien évidemment, l'objectif des cybercriminels est toujours le même : faire télécharger des applications malveillantes par l'intermédiaire de clics sur des liens frauduleux.

Mais là où le rançongiciel étonne, c'est qu'il ne bloque pas que les ordinateurs et les smartphones tournant sous Android. En effet, les cybercriminels ont fait des Smart TV leurs nouvelles victimes. Autrement dit, de nombreux téléspectateurs peuvent désormais vivre la mauvaise expérience de voir leur télévision laisser apparaître un message informant qu'une rançon de 200 dollars (en cartes-cadeaux iTunes) était nécessaire pour débloquer leur appareil.

Si tel n'est pas le cas, l'écran restera figé.

Un type d'attaque qui épargne encore certains pays

Depuis son lancement au printemps 2015, le rançongiciel Frantic Locker n'a cessé de se propager au point de cibler un nombre croissant de terminaux.

Concernant les Smart TV, toutes sont potentiellement vulnérables au ransomware FLocker mais selon Trend Micro, il s'autodétruirait en s'installant sur les Smart TV localisées dans plusieurs pays de l'Est de l'Europe comme la Russie, l'Ukraine, la Biélorussie, la Géorgie, la Bulgarie, l'Arménie, l'Azerbaïdjan, le Kazakhstan ou encore la Hongrie.

Article original de Jérôme DAJOUX

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

Original de l’article mis en page : Les Smart TV, nouvelle cible des ransomwares ?

Les utilitaires de déchiffrement fonctionnent contre toutes les versions de TeslaCrypt

	Les utilitaires de déchiffrement fonctionnent contre toutes les versions de TeslaCrypt

---

Il y a un mois environ, la clé principale de TeslaCrypt a été divulguée, ce qui a mis un terme à cette escroquerie qui marchait bien jusque là. Au cours de cette période, plusieurs utilitaires de déchiffrement capables de récupérer les fichiers endommagés par TeslaCrypt ont été créés.

Ainsi, Kaspersky Lab a actualisé son utilitaire Rakhni en y ajoutant un utilitaire de déchiffrement pour Bitman (TeslaCrypt) version 3 et 4. La semaine dernière, Cisco a réalisé une mise à jour similaire. Son outil est désormais capable de récupérer les fichiers chiffrés par l'ensemble des 4 versions existantes de ce ransomware.
D'après Earl Carter, analyste en chef chez Cisco Talos, la clé principale publiée le 19 mai était utilisée pour récupérer les fichiers chiffrés par TeslaCrypt version 3 et 4. Il ajoute : « Nous ne savons pas si cette clé principale fonctionne pour les versions antérieures. La version 2 était défectueuse et elle a pu être facilement déchiffrée et nous dispositons de l'utilitaire de déchiffrement pour la version originale. L'utilisateur devait d'abord identifier la version du ransomware qui l'avait infecté avant de pouvoir choisir l'utilitaire de déchiffrement adéquat. Nous avons actualisé l'utilitaire d'origine afin qu'il puisse s'occuper de toutes les versions existantes. »
Pour l'instant, les raisons qui ont poussé les opérateurs de TeslaCrypt à mettre un terme à leur projet sont inconnues. Les attaques de ransomwares contre des entreprises ou des particuliers ne faiblissent pas. D'après les estimations du FBI, au cours du premier trimestre seulement, les auteurs de ces attaques ont empoché plus de 200 millions de dollars américains sous la forme de rançons payées. D'ici la fin de l'année, ce chiffre pourrait atteindre 1 milliard. Ceci étant, TeslaCrypt, en tant qu'acteur sur ce marché juteux, n'était pas parfait. Il affichait des défauts qui avaient permis aux chercheurs, presque dès le début, de trouver dans le code les clés de déchiffrement et de créer des outils pour venir en aide aux victimes.
Le jeu du chat et de la souris pouvait commencer : les individus malintentionnés ont renforcé le chiffrement tandis que les chercheurs ont réalisé des analyses plus en profondeur pour trouver l'antidote. « Certains ransomwares utilisent le chiffrement symétrique et dans ce cas, il est possible de trouver la clé sur l'ordinateur et de déchiffrer les fichiers » explique Earl Carter. « D'autres privilégient l'infrastructure PKI et dans ce cas, il est plus difficile de récupérer les fichiers, principalement parce que la clé n'est pas enregistrée sur l'ordinateur infecté. »
Dès qu'un utilitaire de déchiffrement a été réalisé pour une des versions, d'autres chercheurs commencent également à fournir des efforts dans ce sens. Il est tout à fait possible que cela soit la raison pour laquelle les opérateurs de TeslaCrypt ont tué le projet.
« Les ransomwares sont très rentables et tout le monde veut sa part » signale Earl Carter. « Dans la mesure où toutes les versions [de TeslaCrypt] avaient été déchiffrées, on pourrait croire qu'elles n'étaient pas aussi rentables que le souhaitaient les opérateurs. Ceci n'est qu'une hypothèse car nous ne disposons pas des preuves concrètes. Mais à première vue, on dirait bien que c'est cela qui s'est passé. Le malware était toujours déchiffré, les revenus récoltés ne correspondaient pas aux attentes et à la fin, ils ont décidé de faire une croix sur le projet.
La clé principale de TeslaCrypt a été publiée sur le forum d'assistance technique du ransomware après qu'un chercheur de l'ESET avait repéré des indices qui laissaient entendre que le projet allait être abandonné et il a demandé la clé aux auteurs. TeslaCrypt pourrait être remplacé par CryptXXX qui, d'après BleepingComputer, est déjà diffusé via des kits d'exploitation répandus. Certaines sociétés spécialisées dans la sécurité de l'information, comme Kaspersky Lab, surveillent attentivement le développement de CryptXXX et ont même créé des outils de déchiffrement pour ses premières versions.
Le système de chiffrement adopté par TeslaCrypt était actualisé fréquemment afin que les chercheurs ne puissent pas le déchiffrer. Au début de cette année, ce malware se propageait via des redirections WordPress et Joomla ainsi que via le kit d'exploitation Nuclear. Au mois d'avril, des chercheurs de chez Endgame ont découvert deux nouveaux échantillons du ransomware dotés d'outils d'obfuscation et de dissimulation supplémentaires ainsi que d'une liste d'extensions plus longue. A ce moment, TeslaCrypt se propageait déjà via des campagnes de spam.
« Les kits d'exploitation ont commencé à charger des ransomwares au lieu d'enregistreurs de frappe ou de malware de fraude au clic ». L'association du kit d'exploitation et de la publicité malveillant a considérablement simplifié la tâche des attaquants » résume Earl Carter.
Article original de Securelsti

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

Original de l'article mis en page : Les utilitaires de déchiffrement fonctionnent contre toutes les versions de TeslaCrypt — Securelist

---

QRCodes : pièges à internaute ? — ZATAZ

QRCodes : pièges à internaute ? — ZATAZ

Détection du premier cas d'email frauduleux utilisant des QRCodes. Le Flashcode, une porte d'entrée à pirate qu'il ne faut pas négliger.

On retrouve ces QRcodes, baptisés aussi Flashcode, dans les journaux, la publicité… Il est possible de naviguer vers un site internet ; mettre l'adresse d'un site en marque-page ; faire un paiement direct via son cellulaire (Europe et Asie principalement) ; ajouter une carte de visite virtuelle (vCard, MeCard) dans les contacts, ou un événement (iCalendar) dans l'agenda électronique ; déclencher un appel vers un numéro de téléphone ; envoyer un SMS ; montrer un point géographique sur Google Maps ou Bing Maps ; coder un texte libre. SnapChat, par exemple, propose un QR Code maison pour suivre un utilisateur. Bref, toutes les possibilités sont ouvertes avec un QRcode. Il suffit de présenter l'image à votre smartphone, et à l'application dédiée, pour lancer la commande proposée par le QR Code. A première vue, un pirate a eu l'idée de fusionner QR Code et hameçonnage.

Fusionner QR Code et hameçonnage

Le hameçonnage, baptisé aussi Phishing/Filoutage, est une technique qui ne devrait plus être étrangère aux internautes. Pour rappel, cette attaque informatique utilise le Social Engineering dont l'objectif est la collecte des identifiants de connexion (mail, login, mot de passe, adresse IP…). Dans l'attaque annoncée il y a quelques jours par la société Vade retro, le cybercriminel a présenté son mail comme une image usurpée à un opérateur national et proposant au destinataire un remboursement consécutif à une facture payée. Le QR Code conduisait à un site présentant une page falsifiée qui incitait la victime à renseigner son identifiant et mot de passe légitime chez l'opérateur usurpé, puis présentait un message d'erreur.

L'illustration flagrante des cyber-risques pour tous

Comme le rappel Maitre Antoine Chéron, avocat spécialisé en propriété intellectuelle et NTIC aujourd'hui, presque tout le monde a une adresse électronique personnelle ou du moins professionnelle. C'est en effet devenu un mode de communication indispensable non seulement pour travailler mais également pour consommer toutes sortes de biens et services. Destinées aux particuliers, les messageries électroniques ne sont pas toujours sécurisées. Avec l'usage en masse de l'internet, et la dématérialisation des richesses, ce sont de précieux biens tels que nos données personnelles, « l'or noir du 21ème siècle », qui sont aujourd'hui convoités par les personnes mal intentionnées.

QRCodes : carrés aux angles dangereux

Les QRcodes envahissent le web et nos vies. Déjà, dès 2012, je vous informais d'une attaque découverte dans le métro parisien. Preuve que les pirates se penchaient sur la manipulation des QRcode depuis longtemps. J'ai pu rencontrer un chercheur « underground » qui s'est penché sur le sujet. Nous l'appellerons DBTJ. Il se spécialise dans la recherche de procédés détournés pour QRcode. « ***Avec mes collègues,*** explique-t-il à ZATAZ.COM, ***nous avons testés plusieurs cas, qui, hélas, se sont avérés efficaces.*** » Dans les cas de Qrcodes malveillants que j'ai pu constater : naviguer vers un site internet et se retrouver face à un code raquetteur (Ransomware) : mettre l'adresse d'un site en marque-page (Shell) ; ajouter une carte de visite virtuelle (vCard, MeCard) dans les contacts, ou un événement (iCalendar) dans l'agenda électronique, lancer un DDoS… bilan, derrière cette possibilité se cachait un vol de données et une mise en place d'usurpation d'identité.
J'ai pu constater aussi des QR Code capable de déclencher un appel vers un numéro de téléphone ou envoyer un SMS. « Nous avons réfléchis aux méthodes d'infections les plus débiles aux plus élaborés, s'amuse mon interlocuteur. Envoyer le QRcode depuis votre téléphone ; la fonctionne SMS dans SET pourrait être intéressante et ne laissera pas de traces ; utiliser le QRcode sur de faux sites, ou encore des sites vulnérables XSS (via un iframe) ; fausses publicités ; remplacer les QRcode aperçus sur des affiches. »
Ce dernier cas a été remarqué par ZATAZ.COM. Il suffit de coller un autre Flashcode, malveillant cette fois, en lieu et place de l'original sur une affiche, dans un arrêt de bus par exemple. Effet malheureusement garanti. « Dans le cadre de la démonstration, nous avons infecté exactement 1.341 personnes d'une banlieue de Saint-Denis, et cela en seulement 14 heures, souligne le témoin de ZATAZ.COM. Avec une technique de SE (Social Engineering) d'une simplicité redoutable, nous avons fait des publicités contenant notre QRcode pour un jeu mobile gratuit que nous avons ensuite imprimé en plusieurs exemplaires et diffuser dans les lieux publics (gare/train – centre-ville). » ZATAZ.COM peut confirmer qu'après le test, les « pentesteurs » du QRcode ont effacé l'intégralité des informations collectées.
Bref, voilà de quoi regarder ces petits carrés noirs et blancs d'un œil nouveau … et plus suspicieux. Pour se protéger, des logiciels comme GData QRCode permettent de palier ce type d'intrusion. A utiliser sans modération.

Article original 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

Original de l'article mis en page : QRCodes : pièges à internaute ? – ZATAZ

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

Alerte nouveau ransomware : Le Javascript RAA est diffusé par spams

Le ransomware RAA se propage à grande vitesse en Russie par le biais de campagnes de spams. Il prend la forme d'une pièce jointe en Javascript.

RAA, un ransomware entièrement écrit en Javascript

Si la plupart des logiciels malveillants qui ciblent des machines Windows est écrite en C++, voilà que RAA surprend puisque lui est intégralement écrit en Javascript, un langage destiné principalement à être interprété par les navigateurs web.

Pour les cybercriminels, le choix de ce langage n'est pas dû au hasard étant donné qu'ils tentent d'infecter les machines à distance via la diffusion de spams. Toutefois, tout utilisateur doit normalement agir avec méfiance avec les pièces jointes, d'autant plus si celles-ci sont dans un format Javascript. En effet, ce format doit inciter les utilisateurs à mettre le mail dans leur corbeille et surtout à ne pas ouvrir la pièce jointe.

Si tel est le cas, RAA peut faire des ravages puisqu'il est conçu pour chiffrer les documents disposant des extensions .doc, .xls, .rtf, .pdf, .dbf, .jpg, .dwg, .cdr, .psd, .cd, .mdb, .png, .lcd, .zip, .rar et .csv comme le révèlent nos confrères du Monde Informatique.

Autant dire donc que le téléchargement de la pièce jointe n'est pas sans conséquences.

Pas de vaccin disponible pour déchiffrer les contenus

S'il existe parfois des vaccins contre les ransomwares, RAA n'a pas encore le sien si bien qu'une fois vos fichiers chiffrés, vous n'aurez aucune autre alternative que payer la rançon si vous voulez débloquer de nouveau l'accès à vos documents.

Pour l'heure, ce rançongiciel se propage principalement en Russie puisqu'il semble que c'est depuis ce pays qu'opèrent les cybercriminels. Toutefois, il y a fort à parier que la diffusion de RAA va s'étendre dans les prochains mois et qu'une version « internationale » du rançongiciel sera développée par ces spécialistes du genre.

Article original de Fabrice Dupuis

Réagissez à cet article

Original de l’article mis en page : RAA : un nouveau ransomware diffusé par spams

---

La France dans le Top 10 du piratage informatique

La France dans le Top 10 du piratage informatique

NATIC Magazine vous fait une synthèse de l'actualité tournant autour des problématiques de cybersociété: Hacking, Sécurité, Codes malveillants, Piratage, Vie privée numérique, Protocole d'alerte, Alerte propagande, Web Tv, etc.

Le rapport annuel de Symantec sur le piratage informatique est une fois encore percutant. Selon le géant mondial de la cybersécurité, la France fait partie des 10 pays les plus concernés par les attaques informatiques. En 9ème position mondiale, le pays subit plus de 10 millions de tentatives avérées par an, en forte hausse d'une année sur l'autre.
Selon la version 2016 du rapport, les brevets technologiques et les trésors de propriété intellectuelle des grands groupes français attirent les meilleurs pirates mondiaux. Lancées par des concurrents, des activistes ou même des états, ces attaques visent également des PME ou même des particuliers ce qui est plus étonnant. Ces derniers sont très vulnérables notamment lorsqu'ils utilisent les réseaux sociaux. On observe en particulier une percée remarquable de l'utilisation des ransomwares ou rançongiciels – en hausse de 260% en France en 2015. Le phénomène prend de l'ampleur.
Dans le rapport de Symantec version 2016, le Top 3 des pays victimes de piratage en 2015 est constitué de la Chine, des Etats-Unis et de l'Inde.
Article original

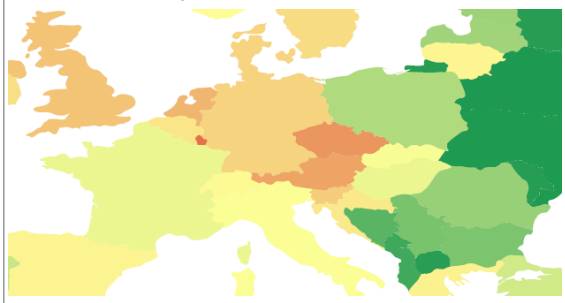
Réagissez à cet article

Original de l’article mis en page : La France dans le Top 10 du piratage

ESET, seul éditeur à obtenir 100% de protection contre la nouvelle vague du ransomware Locky qui contamine l’Europe

ESET, seul éditeur à obtenir 100% de protection contre la nouvelle vague du ransomware Locky qui contamine l’Europe

Les rapports de détection réalisés par ESET montrent une augmentation importante de la prolifération du malware JS/Danger.ScriptAttachement dans plusieurs pays européens. Les pays les plus touchés sont le Luxembourg (67 %), la République tchèque (60%), l'Autriche (57%), les Pays-Bas (54%) et le Royaume-Uni (51%).



ESET, seul éditeur à obtenir 100% de protection contre la nouvelle vague du ransomware Locky qui contamine l'Europe Les rapports de détection réalisés par ESET montrent une augmentation importante de la prolifération du malware JS/Danger.ScriptAttachement dans plusieurs pays européens. Les pays les plus touchés sont le Luxembourg (67 %), la République tchèque (60%), l'Autriche (57%), les Pays-Bas (54%) et le Royaume-Uni (51%).

ESET considère les ransomwares comme l'une des menaces informatiques les plus dangereuses à l'heure actuelle. Par conséquent, nous recommandons aux particuliers et aux entreprises de garder leurs ordinateurs et leurs logiciels à jour, d'utiliser un logiciel de sécurité fiable et de sauvegarder régulièrement leurs données importantes.

«Les utilisateurs d'ESET sont protégés contre cette menace. Nos solutions sont capables de bloquer le téléchargement et l'exécution en force par les différentes familles de ransomwares», commente Ondrej Kubovič, ESET IT Security Specialist.
En effet, lors du test réalisé par SE Labs qui compare 8 solutions de protection anti-malware, ESET Smart Security 9 remporte la première place avec 100% de réussite dans toutes les catégories.
«Chez ESET, nous nous engageons dans notre travail pour faire des produits qui protègent des millions d'utilisateurs à travers le monde. Nous apprécions de voir que les tests réalisés par SE Labs valident l'approche multicouches que nous construisons depuis plus de 20 ans.», a déclaré Palo Luka, Chief Technology Officer chez ESET.
ESET Smart Security 9 se distingue comme le seul produit ayant bloqué toutes les menaces. «ESET Smart Security contrôle parfaitement les attaques ciblées et les menaces Internet, ce qui est un excellent résultat. Il est rare d'obtenir 100% de réussite dans les tests de détection de menaces en temps réel, pour un produit sans compromis qui offre une protection complète et qui contrôle également des applications et des sites Web dits légitimes sans commettre une seule erreur», explique Simon Edwards, SE Labs' founder and Director.

Pour en savoir plus ces produits, rendez-vous sur http://www.eset.com/fr/
Article original de Benoit Grunemwald

Réagissez à cet article

Original de l'article mis en page : Locky se propage en Europe