Le ransomware CryptoWall donne la migraine aux forces de l’ordre

	Le #ransomware CryptoWall donne la migraine aux forces de l’ordre

Bâti sur un labyrinthe de serveurs proxy, ce botnet est, pour l'instant, difficile à neutraliser. Pour se protéger, il faut faire des sauvegardes, mais pas n'importe comment.

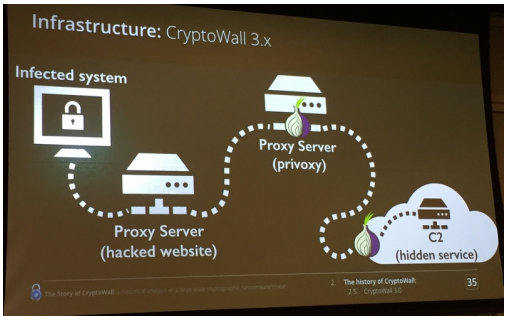
C'est l'un des plus importants « rançongiciels » du moment, et il le sera certainement encore pour un bout de temps. Car les pirates qui se cachent derrière ce néfaste malware ont mis en place un système pour l'instant assez inviolable et diaboliquement efficace. Bienvenue dans l'univers de CryptoWall.

Le chercheur en sécurité Yonathan Klijnsma de la société Fox IT est l'un de ceux qui essayent de pister ses auteurs. Il a profité de la conférence Botconf 2015, qui se déroule actuellement à Paris, pour présenter ses dernières analyses.

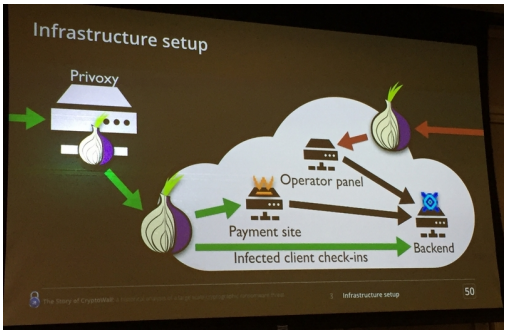
GK — Yonathan Klijnsma

Sur le principe, CryptoWall — qui existe actuellement dans sa version 4.0 — n'a rien d'original. Apparu pour la première fois en novembre 2013, ce code malveillant fonctionne un peu comme son aïeul Cryptolocker. Il infecte les ordinateurs et chiffre les fichiers qui s'y trouvent, ainsi que les noms de ces fichiers. Pour cela, il s'appuie sur les algorithmes AES 256bit et RSA 2048bit. Pour avoir une chance de récupérer ses données, il faut passer à la caisse. Plusieurs moyens de paiement sont acceptés : bitcoin, litecoin, UKash, moneypak, paysafecard, etc.
Ce qui rend ce malware si difficile à terrasser, c'est son infrastructure sous-jacente, composée d'une multitude de serveurs proxy en cascade, des intermédiaires qui servent essentiellement à brouiller les pistes. *« C'est un vrai labyrinthe. On ne sait jamais si la ressource que l'on a détectée est le véritable serveur de commande et contrôle, ou simplement un autre proxy »*, explique Yonathan Klijnsma.

Autre subtilité : le premier niveau de proxy est constitué de serveurs Web piratés. *« Ce sont de vrais sites totalement légitimes. Les propriétaires, évidemment, ne savent pas que leurs serveurs ont été détournés par des pirates. C'est assez malin de leur part, car cela complique le démantèlement du botnet. On ne peut pas simplement tirer le cordon. Il faut contacter chaque administrateur un par un »*, souligne le chercheur en sécurité.



© DR



© DR

Derrière le serveur Web piraté se trouve un autre proxy qui va faire le lien avec le réseau d'anonymisation Tor, dans lequel les pirates ont planqué toute leur infrastructure d'administration : les clés de chiffrement, le paiement, la diffusion de malware, etc. Tous ces « services » sont créés sous la forme de services Tor cachés (Tor Hidden Service). *« Pour les forces de l'ordre, c'est techniquement très difficile d'identifier les serveurs qui se cachent derrière »*, souligne Yonathan Klijnsma.
Pour avoir une chance de démanteler le réseau, il faut donc utiliser des méthodes d'investigation plus classiques, par exemple en infiltrant des forums de discussion. Mais cette méthode prend du temps et n'est pas forcément couronnée de succès.

Pour l'instant, ce cyberracket constitue donc quasiment le crime parfait. Les auteurs sont tellement insouciants qu'ils n'hésitent pas à se moquer ouvertement de leurs victimes, en les félicitant — sur l'un des écrans d'alerte — d'avoir rejoint *« la grande communauté CryptoWall »*.

Un malware d'origine russe ?

Certains éléments techniques semblent indiquer que les auteurs de CryptoWall — ou une partie d'entre eux — se trouvent en Russie. Un mécanisme dans le code évite, en effet, qu'il ne s'installe sur des ordinateurs qui se trouvent en Russie, en Biélorussie, en Ukraine ou au Kazakhstan. Ce type d'exception est typique pour des cybercriminels qui ne souhaitent pas avoir de problèmes avec les forces de l'ordre locales. *« En même temps, on ne peut jamais être sûr à 100 %. Cela pourrait être un faux indice »*, ajoute le chercheur.
En tant qu'utilisateur, pour se prémunir contre un fléau tel que CryptoWall ou consorts, le mieux c'est de faire des sauvegardes régulières de ses fichiers. Mais attention : pas n'importe comment. Il faut éviter les sauvegardes automatiques sur un disque en réseau sur lequel l'ordinateur est connecté en permanence. *« Dans ce cas, le malware ne va pas seulement chiffrer le contenu de l'ordinateur, mais aussi les sauvegardes »*, explique le chercheur. L'idéal, c'est donc de faire des sauvegardes régulières, mais à la main.

Réagissez à cet article
Source : http://www.01net.com/actualites/cryptowall-le-ransomware-qui-donne-la-migraine-aux-forces-de-l-ordre-934345.html
Gilbert KALLENBORN

Attentats : attention au message bidon “On est tous Paris”

Attention au message bidon “On est tous Paris”

Comme après les attentats de janvier, un « hoax » ou « fake » circule à grande vitesse ces dernières heures par SMS, Facebook ou Twitter. Il s'agit d'un message qui dit vouloir prévenir que le mail « On est tous Paris » est dangereux et contient un virus.

En fait, ce message de « prévention » est lui-même potentiellement un virus ou au moins un message bidon qui n'a rien d'officiel.
L'éventuel mail « On est tous Paris » n'existe pas.
Si vous le recevez, soyez vigilants et ne cliquez surtout pas, ne le relayez pas. Il pourrait infecter votre téléphone ou votre ordinateur.
Le voici :

> Vous risquez de recevoir un mail nommé "on est tous Paris" qui est diffusé
> à grande échelle depuis ce WEEK-END.
> Dans ce message une photo de bébé avec un bracelet de naissance où il est
> écrit "on est tous PARIS" vous invitant à cliquer sur la photo.
> Ce message contient un malware (virus) qui permet de prendre le controle à
> distance de votre ordinateur et de récupérer toutes vos données et mots de passe.
> Source : service de cyber criminalité du ministère de la défense.
> Donc, envoyez ce message à vos contacts. C'est urgent et ca va très vite, ca circule depuis dimanche.
> La confirmation de cette info a été diffusée sur EUROPE 1 ce matin.

Ni le service de cybercriminalité du ministère de la défense, ni Europe 1 n'ont diffusé cette pseudo-information. Et les nombreuses fautes d'orthographe et de typographie prouvent facilement que ce message est un « fake ». Ne le diffusez pas !

Depuis vendredi, les rumeurs, fausses infos circulent sur le web. Nous en avons recensé ici :
http://france3-regions.francetvinfo.fr/nord-pas-de-calais/attentats-de-paris-mefiez-vous-des-rumeurs-sur-les-reseaux-sociaux-853751.html

Soyez prudents. Informez sur des sites de confiance et ne relayez pas des images.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, #arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !
Source : http://france3-regions.francetvinfo.fr/nord-pas-de-calais/attentats-attention-au-message-bidon-est-tous-paris-855033.html

Kaspersky Decryptor : un outil pour décrypter les fichiers des ransomware Coinvault et Bitcryptor | Le Net Expert Informatique

Kaspersky Decryptor : un outil pour décrypter les fichiers des ransomware Coinvault et Bitcryptor

L'éditeur d'outils de sécurité a réussi à récupérer toutes les clés de décryptage de deux malwares qui corrompent les fichiers utilisateurs.

Kaspersky Decryptor : un outil pour décrypter les fichiers des ransomware Coinvault et Bitcryptor
Dans la liste des logiciels malveillants les ransomware font partie des plus redoutables pour extorquer de l'argent aux victimes. Kaspersky propose toutefois un outil pour venir à bout de deux d'entre eux tout en offrant la possibilité de décrypter les fichiers corrompus.

Coinvault et Bitcryptor sont deux malwares de type « ransomware ». Ils prennent place sur l'ordinateur en trompant l'utilisateur puis appliquent un chiffrement sur les fichiers de l'utilisateur qui deviennent inaccessibles sans clé de déverrouillage. Les malfaiteurs proposent de délivrer la clé contre le paiement d'une rançon, d'où le nom ransomware.

Ransomware Coinvault
Depuis plusieurs mois Kaspersky collabore avec les les forces de l'ordre néerlandaises pour récupérer des clés de décryptage. Après avoir récupéré quelques échantillons en début d'année, ils annoncent aujourd'hui que toutes les clés de décryptage, plus de 14000, sont à présent disponibles. Cela permettra aux utilisateurs infectés de se débarasser du logiciel malveillant tout en retrouvant l'accès à leurs fichiers.

Kaspersky Decryptor
La procédure (en anglais https://noransom.kaspersky.com/static/CoinVault-decrypt-howto.pdf) explique la marche à suivre. Le logiciel malveillant est tout d'abord éliminé en utilisant la suite Kaspersky Internet Security (http://www.cnetfrance.fr/telecharger/kaspersky-internet-security-39184140s.htm) puis le logiciel Kaspersky Ransomware Decryptor (https://noransom.kaspersky.com/) déchiffre les fichiers de l'ordinateur grâce à la liste qu'il récupère ou dans un dossier désigné par l'utilisateur.

Tous les logiciels malveillants agissant de cette façon ne sont toutefois pas concernés. Il est donc recommandé pour éviter tout problème de sauvegarder régulièrement ses fichiers personnels sur un support externe tel qu'un disque amovible ou un service de stockage en ligne.

Source :
http://www.cnetfrance.fr/news/kaspersky-decryptor-un-outil-pour-decrypter-les-fichiers-des-ransomware-coinvault-et-bitcryptor-39827670.htm

---

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.


README_FOR_DECRYPT2.txt

```
1  Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048
   generated for this computer.
2
3  To decrypt files you need to obtain the private key.
4
5  The single copy of the private key, which will allow to decrypt the files, located on a secret
   server at the Internet. After that, nobody and never will be able to restore files...
6
7  To obtain the private key and php script for this computer, which will automatically decrypt
   files, you need to pay 1 bitcoin(s) (~420 USD).
8  Without this key, you will never be able to get your original files back.
9
10
11 ____________________________________
12
13 !!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE):
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx !!!!!!!!!!!!!!!!!!!!
14 WEBSITE: https://z54n57pg2el6uze2.onion.to
15
16 INSTRUCTION FOR DECRYPT:
```

Source : Dr.WEB

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

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

Des chercheurs découvrent un navigateur malveillant, il se présente comme une imitation de Chrome afin de tromper les utilisateurs | Le Net Expert Informatique

Des chercheurs découvrent un navigateur malveillant, il se présente comme une imitation de Chrome afin de tromper les utilisateurs

Face à la diversité des outils de détection de malwares, les pirates informatiques n'hésitent pas à faire preuve d'inventivité pour atteindre leurs objectifs. En effet, une société du nom de Claralabsoftware a mis en œuvre un navigateur du nom d'eFast. Ce navigateur est censé améliorer l'expérience de navigation en fournissant des résultats de recherche les plus pertinents, en affichant des réductions et bonnes affaires disponibles sur la toile, et en fournissant des outils de protection contre les phishings et divers malwares. Il est basé sur Chromium, le navigateur open source sur le lequel sont fondés plusieurs autres navigateurs dont Chrome, Opera, Vivaldi, etc.

Les utilisateurs voyant donc les caractéristiques d'eFast pourraient croire à une application dénuée de tout code malveillant, mais tant s'en faut. Selon le rapport de Malwarebytes, l'entreprise de sécurité informatique, lorsque vous installez eFast, ce dernier essaie automatiquement de prendre le contrôle du terminal sur lequel il est installé en cherchant à devenir le navigateur par défaut.

En plus de cette action, eFast s'associe par défaut avec les extensions de fichiers suivantes : gif, htm, html, jpeg, jpg, pdf, png, shtml, webp, xht, xhtml. La même association est effectuée pour les schémas, protocoles, et autres objets URL suivants : ftp, http, https, irc, mailto, mms, news, nntp, sms, smsto, tel, urn, webcal.

Lorsque ces extensions sont associées par défaut à eFast, pour toute tentative d'ouverture de fichier, d'appel d'un protocole ou toute action utilisant les objets listés plus haut, c'est le navigateur eFast qui exécutera l'action souhaitée.

En plus de cela, eFast redirigeraient les internautes vers des pages publicitaires ou d'autres pages web qui pourraient héberger des malwares. En outre, PCrisk rapporte qu'eFast est un aspirateur de données de navigation. Ces informations une fois collectées pourraient être partagées avec d'autres personnes et utilisées à mauvais escient afin de gâcher la vie d'un internaute.

Selon PCrisk, ce programme pourrait s'installer lors de l'installation de certains programmes. En effet, les développeurs pourraient cacher l'option d'installation de ce programme dans les paramètres personnalisés. C'est pourquoi il est recommandé de ne pas installer les applications en utilisant les paramètres de recommandation, mais plutôt les paramètres personnalisés.

Une des choses à ne pas négliger par ailleurs est que lors de l'installation d'eFast, celui-ci se charge de supprimer les raccourcis de Chrome sur le bureau et la barre des tâches et installe par la même occasion des raccourcis de YouTube, Amazon, Facebook, Wikipedia et Hotmail sur le bureau. Il faut noter qu'il est très similaire à Chrome aussi dans la présentation générale que dans les couleurs de l'icône.

Enfin, nous précisons qu'en voulant nous rendre sur le site de l'éditeur clara-labs afin d'effectuer des recherches supplémentaires, Chrome nous a envoyé une alerte afin de signaler que le site que nous voulons ouvrir contient des programmes dangereux. Ce n'est donc pas uniquement le produit de l'entreprise qui est étiqueté comme dangereux, mais même le site l'est également.

Source :
http://www.developpez.com/actu/91354/Des-chercheurs-decouvrent-un-navigateur-malveillant-base-sur-Chromium-il-se-presente-comme-une-imitation-de-Chrome-afin-de-tromper-les-utilisateurs/
par Olivier Famien

Découverte d’un malware sous Linux derrière un important botnet | Le Net Expert Informatique

Découverte d’un malware sous Linux derrière un important botnet

Réputé plus sûr que Windows, Linux connaît aussi son lot d’attaques, et en connaîtra de plus en plus avec l’augmentation des objets connectés reposant sur une distribution Linux. En témoigne un nouveau malware découvert principalement en Asie, qui forme un botnet capable d’orchestrer des attaques DDOS très puissantes, jusqu’à plus de 150 Gbps.

La firme Akamai a révélé lundi la découverte d’un botnet qui serait capable d’organiser une attaque DDoS de plus de 150 Gbps, formé grâce à un malware qui cible les ordinateurs et serveurs sous Linux. Baptisé XOR DDoS, l’armée de zombies rassemblés par des chevaux de Troie se compose également de nombreux appareils connectés dont la couche logicielle repose souvent sur des systèmes Linux non mis à jour, soit que le service après-vente n’est pas assuré, soit que les utilisateurs n’aient pas le réflexe de mettre à jour le firmware d’un appareil qui semble fonctionner correctement.

Selon Akamai, le malware d’origine asiatique se répandrait grâce aux services SSH d’appareils mal sécurisés tels que de routeurs, qui peuvent être attaqués par force brute (tenter des milliers de mots de passe jusqu’à tomber sur le bon). Chaque accès gagné sur une machine permet de gagner un nouveau relais vers de nouveaux serveurs, et ainsi de suite.

Le botnet XOR DDoS aurait déjà été utilisé de très nombreuses fois (une vingtaine d’attaques par jour dont 90 % vers l’Asie), avec des degrés divers de puissance, allant de flots de données de 2 Gbps à plus de 150 Gbps. Les cibles prioritaires seraient le secteur du jeu d’argent, suivi par les institutions éducatives. Une orientation qui peut être le fait des créateurs du botnet, ou des clients qui louent ses services pour attaquer une URL ou une adresse IP en payant à l’heure et à la puissance d’attaque voulue.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.numerama.com/magazine/34342-decouverte-d-un-malware-sous-linux-derriere-un-important-botnet.html
par Guillaume Champeau

Des applications malveillantes dans l’App Store | Le Net Expert Informatique

Des pirates ont trouvé le moyen de faire entrer des applications malveillantes dans la boutiques d'Apple. Ils ont pour cela convaincu des développeurs d'utiliser une version modifiée de Xcode, introduisant ainsi des malwares sur l'App Store.

Pour minimiser les risques d'infection des terminaux mobiles, les éditeurs de plateformes recommandent (ou imposent) l'utilisation de leurs boutiques d'applications officielles. Il est malgré tout possible d'éviter les mécanismes de contrôle mis en place par exemple par Google et Apple.

Et Apple vient d'ailleurs d'en faire les frais. La firme a confirmé officiellement à Reuters avoir dû retirer plusieurs apps de l'App Store suite à la découverte d'une faille de sécurité. Des pirates ont trouvé une solution pour échapper à la vigilance de l'éditeur.

Xcode corrompu pour pénétrer l'App Store

Pour concevoir des applications pour iOS et OS X, les développeurs ont recours aux outils de développement d'Apple regroupés au sein du logiciel Xcode. Les pirates ont ainsi mis au point une version modifiée de Xcode, diffusée ensuite auprès de développeurs d'apps. Les applis réutilisant cet outil se transformaient dès lors en malwares.

Présenté sous la dénomination XcodeGhost, ce malware a pu faire son entrée sur l'App Store. Plusieurs applications populaires ont été compromises par cette méthode dont la messagerie WeChat, CamCard ou le concurrent chinois d'Uber, Didi Chuxing.

WeChat a précisé dans un billet de blog que seule la version de son appli antérieure au 10 septembre était affectée par la faille de sécurité. Une nouvelle version a depuis été diffusée pour remédier au problème.

« Nous travaillons avec les développeurs afin de garantir qu'ils utilisent la version authentique de Xcode pour redévelopper leurs apps » déclare un porte-parole d'Apple auprès de Reuters. Le malware XcodeGhost est présenté par la société de sécurité Palo Alto Networks comme particulièrement nuisible et dangereux.

L'éditeur de sécurité précise également que la version compromise de Xcode a été identifiée sur un serveur en Chine. Et si elle a été utilisée par les développeurs, c'est probablement car elle s'avérait plus rapide à télécharger que le logiciel officiel hébergé chez Apple.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source : http://www.zdnet.fr/actualites/apple-contraint-de-supprimer-des-apps-malveillantes-de-l-app-store-39825174.htm

Un nouveau Virus vise les iPhones et l’iPads | Le Net Expert Informatique

	Un nouveau Virus vise les iPhones et l’iPads

Cette nouvelle #famille de virus, baptisée « #KeyRaider« , s'attaque à des iPhone et iPad débloqués pour y installer des applications non approuvées par Apple.

« Nous pensons que c'est le plus grand vol connu de comptes Apple causé par un virus », indique la société de sécurité informatique américaine Palo Alto Networks.©CAROLINE SEIDEL

Des chercheurs en sécurité informatique affirment avoir identifié une nouvelle famille de virus, baptisée « KeyRaider », qui s'attaque à des iPhone et iPad débloqués pour pouvoir y installer des applications non approuvées par Apple. « Nous pensons que c'est le plus grand vol connu de comptes Apple causé par un virus », indique la société de sécurité informatique américaine Palo Alto Networks sur son site internet, où elle résume les résultats d'une enquête réalisée avec WeipTech, un groupe technique amateur réunissant des fans d'Apple en Chine.

« KeyRaider a ainsi déjà réussi à voler plus de 225 000 comptes Apple valides » avec leurs mots de passe, qui ont été retrouvés stockés sur un serveur, ainsi que « des milliers de certificats, clés privées et tickets d'achats », précise Palo Alto Networks. Le virus fonctionne en interceptant les communications de l'appareil avec iTunes, la boutique de musique en ligne d'Apple. Il vole et partage des informations d'achats à l'intérieur d'applications et désactive la fonction de déblocage locale ou à distance de l'iPhone ou de l'iPad.

Dix-huit pays touchés

Certaines des victimes ont constaté des achats anormaux, d'autres ont vu leur appareil bloqué par des pirates qui leur ont demandé une rançon, indique encore la société de sécurité informatique. KeyRaider s'attaque aux appareils utilisant iOS, le système d'exploitation mobile d'Apple, qui ont été débloqués et est distribué en Chine par l'intermédiaire de Cydia, une application non officielle pour iOS donnant accès à des applications non validées par Apple.

Palo Alto Research estime au total que des consommateurs de 18 pays ont été touchés, dont la Chine mais aussi la France, la Russie, le Japon, le Royaume-Uni, les États-Unis, le Canada, l'Allemagne, l'Australie, Israël, l'Italie, l'Espagne, Singapour et la Corée du Sud.

Un porte-parole d'Apple a souligné dans un courriel que « le problème ne touche que ceux qui non seulement ont débloqué leurs appareils (pour permettre des utilisations non utilisées par le fabricant, NDLR) mais ont aussi téléchargé le virus depuis des sources non fiables ».

« L'iOS est conçu pour être fiable et sûr à partir du moment où on allume l'appareil. Pour protéger nos utilisateurs des virus, nous surveillons le contenu de l'App Store et nous assurons que toutes les applications dans l'App Store adhèrent aux lignes directrices fixées pour nos développeurs », a-t-il rappelé. Il a toutefois assuré qu'Apple avait pris « des mesures pour protéger ceux affectés par le problème en aidant les propriétaires à réinitialiser leurs comptes (en ligne) iCloud avec un nouveau mot de passe ».

Lire la suite….

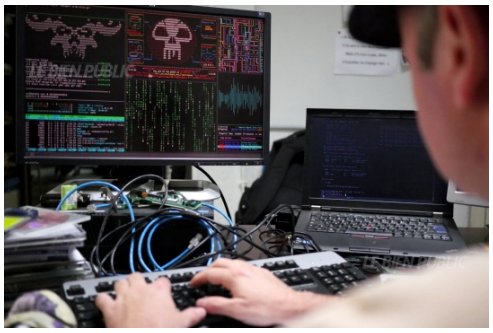
Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.lepoint.fr/high-tech-internet/piratage-informatique-l-iphone-et-l-ipad-vises-par-un-nouveau-virus-02-09-2015-1961181_47.php

---

Alerte à partager : Vigilance face au logiciel malveillant Didrex | Le Net Expert

Informatique



Alerte à partager : Vigilance face au logiciel malveillant Didrex

Vols d'identifiants et d'informations personnelles, transferts de fonds non autorisés… devant la multiplication du nombre d'ordinateurs infectés par le logiciel malveillant Dridex, la gendarmerie nationale lance une mise en garde à tous les utilisateurs d'Internet et distille quelques conseils pour se prémunir de la menace.

Depuis le début du mois de juin 2015, la France fait face à une campagne massive de dissémination de logiciel malveillant (malware) par le biais de courriers électroniques non sollicités (Spam). Ce logiciel connu sous le nom de «Dridex» a pour vocation d'infecter les postes informatiques utilisant le système d'exploitation Microsoft Windows (toutes versions allant de Windows XP à Windows 8.1). Actuellement, 28 000 postes sont infectés en France.

Un mail trompeur sous forme de facture
Le but de ce logiciel est de prendre le contrôle de la machine à des fins crapuleuses. En effet, après avoir été infecté, le poste informatique compromis va servir, à la fois, à la collecte de données personnelles (numéro de compte, identifiants et mot de passe de connexion, numéro de carte bancaire, historique de navigation, etc.) ainsi qu'à la réalisation de manœuvres frauduleuses (transfert d'argent, connexion à des sites Internet, envoi de message, relais mandataire, etc.) et ce, à l'insu du légitime propriétaire de la machine. La victime, particulier ou entreprise, est destinataire d'un message électronique contenant une pièce jointe, le plus souvent, un document au format Microsoft Word/Excel, voire dans certains cas, au format portable Document File (.pdf). Cette pièce jointe est souvent intitulée «Invoice» ou «facture» et l'objet du message est souvent en lien avec un paiement ou une facture.

Tous vos codes et données collectés
L'ouverture de cette pièce jointe entraîne, lorsque l'activation des macros est autorisée, le téléchargement d'un logiciel malveillant qui va permettre la prise de contrôle à distance de la machine. Par la suite, lorsque la victime se connecte au site de sa banque en ligne, le malware, va récupérer toutes les informations intéressantes (identifiant, mot de passe, nom, prénom, numéro de téléphone, numéro de compte, numéro de carte bancaire, solde du compte, etc.). Muni de l'ensemble de ces données, l'escroc va alors réaliser des transferts de fonds depuis le compte de la victime vers celui d'une tierce personne pouvant se trouver en France, mais plus généralement à l'étranger.

Comment se prémunir de Didrex
-> Observez une grande vigilance vis-à-vis de la messagerie électronique et ayez un esprit critique sur l'origine des messages qui vous parviennent
– Supprimez tous les e-mails suspects prospectifs (spam) reçus dans la boîte de messagerie, surtout s'ils contiennent des pièces jointes.
– N'ouvrez surtout pas les documents en pièce jointe contenus dans un spam; il suffit de les supprimer.
– Si vous avez des suspicions sur un courriel prétendant provenir d'organisations légitimes (banques, administrations, sites de ventes, etc…), il vaut mieux avant, vérifier auprès de ces organisations en question, la véracité de l'envoi du message et l'authenticité de la pièce jointe.
– Installez une solution antimalware qui protège également des spams. En premier lieu, cela devrait du moins réduire ou au mieux éliminer le risque d'ouvrir accidentellement un de ces pourriels et pièces jointes malveillantes
– Désactivez les macros exécutables automatiquement dans Microsoft Word et Excel
– S'il y a soupçon d'infection, changez immédiatement le mot de passe d'accès au compte bancaire en ligne, pour ce faire veuillez contacter rapidement votre établissement bancaire et l'alerter d'un risque potentiel de fraude. DRIDEX étant capable de dérober d'autres types d'identifiants de connexion, il est vivement recommandé pour tous autres accès à des services en ligne, de modifier les « logins et mots de passe ». ATTENTION : faites ceci en utilisant un autre moyen de connexion que l'ordinateur suspecté d'infection
– Procédez à la même mesure concernant tous autres comptes de services internet dont vous êtes titulaires (fournisseur d'accès internet, vente en ligne, réseaux sociaux, etc…). Dridex vole aussi ce genre d'information
– Surveillez l'activité de vos comptes bancaires et vérifiez la légitimité de vos transactions.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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 sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.bienpublic.com/actualite/2015/08/06/la-gendarmerie-appelle-a-la-vigilance-face-a-didrex

---

Alerte à partager : Une faille sur Android à corriger d'urgence | Le Net Expert Informatique

Alerte à partager : Une faille sur Android à corriger d'urgence

Si votre fournisseur de smartphone ou de tablette ne patche pas Stagefright de lui même, ce malware basé sur l'envoi de MMS peut être vraiment effrayant. Mais vous pouvez vous en protéger en respectant quelques étapes.

Franchement, la plupart des gens qui reçoivent les logiciels malveillants recherchent les ennuis. Ils ouvrent un fichier suspect envoyé par une personne qu'ils ne connaissent pas, vont sur un site Internet mal famé, voire téléchargent le dernier film ou jeu à la mode sur BitTorrent. Mais Stagefright, c'est différent. Ce logiciel malveillant basée sur une faille de sécurité se déclenche en recevant un MMS sur un appareil Android non patchées. Et bang, vous êtes piraté.
Stagefright peut attaquer tout smartphone Android, tablette, ou un autre dispositif fonctionnant sous Android 2.2 ou supérieur. Des approximativement quelque 1 milliard de gadgets Android présents sur le marché, Stagefright pourrait, en théorie, toucher 95% d'entre eux. Joshua J. Drake, le vice-président de Zimperium zLabs qui a découvert Stagefright prétend qu'il est parmi les « pires vulnérabilités Android découvertes à ce jour ».
Car la partie vraiment sournoise est qu'il n'est pas nécessaire de consulter le MMS pour être infecté. Si vous utilisez l'application Hangouts de Google , vous êtes infectés sans même consulter cette application de messagerie si l'on vous fait parvenir ce message.

Un malware pas comme les autres
Tout ce que l'attaquant a besoin de faire est d'envoyer ce paquet empoisonné à votre numéro de téléphone. Il allume alors votre appareil, et l'attaque commence. Cela peut arriver si vite que le temps que votre téléphone vous avertisse qu'un message est arrivé, vous avez déjà été piraté. Si par ailleurs vous utilisez l'application native de messagerie proposée avec Android, vous devez ouvrir le MMS, mais pas nécessairement déclencher la vidéo, pour être infecté.
Ce détournement de la sécurité d'Android fonctionne en profitant de la bibliothèque Stagefright incluse dans Android. Ce moteur de lecture multimedia est fourni avec des codecs basés sur des logiciels pour lire plusieurs formats de médias populaires. La faille de sécurité semble provenir du fait que pour réduire la latence de l'affichage vidéo Stagefright traite automatiquement la vidéo avant même que vous ne vouliez la regarder. Joshua J. Drake va révéler les détails de du fonctionnement de Stagefright au Black Hat début Août.

Google a été réactif…
Zimperium à informé Google du problème en Avril. Selon Drake, « Google a agi promptement et appliqué les correctifs à des branches de code interne sous 48 heures ». Une porte-parole de Google mentionne dans une réponse par e-mail : « Nous avons déjà répondu rapidement (…) en envoyant le correctif pour tous les appareils Android à nos partenaires ».

Elle ajoute :
La sécurité est renforcée dans Android : les applications Android sont exécutées dans ce que nous appelons une « sandbox d'application ». De la même manière qu'un bac à sable empêche le sable de sortir, chaque application est installée dans une « sandbox » virtuelle pour l'empêcher d'accéder à autre chose qu'à ses propres composants, ce qui signifie que même si un utilisateur devait installer accidentellement un morceau de malware, il lui est interdit d'accéder à d'autres parties du dispositif.
L'ouverture de l'écosystème améliore la sécurité et rend Android plus puissant. Comme Android est open source, tout le monde peut l'examiner pour comprendre comment il fonctionne et d'identifier les risques potentiels de sécurité. Toute personne peut mener des recherches et faire des contributions pour améliorer la sécurité d'Android.
Google encourage la recherche en matière de sécurité : le programme de récompenses de sécurité Android, lancé en 2015, et le programme Google Patch Rewards, lancé en 2014, récompensent les contributions de chercheurs en sécurité qui investissent leur temps et leurs efforts à aider à rendre les applications plus sûres.
Alors, avec toutes ces précautions, pourquoi une telle agitation? Oui, il s'agit d'une faille de sécurité particulièrement vicieuse, mais le correctif est là… n'est ce pas ?

…mais pas les fabricants
Euh, et bien en fait Android a un autre problème de sécurité bien plus important. À l'exception des appareils Nexus, Google fournit les correctifs de code source, mais ce sont les fabricants de smartphones et les opérateurs qui doivent les faire parvenir aux utilisateurs qui mettent à jour le firmware. Et au 27 Juillet aucun des principaux acteurs de l'écosystème Android n'a annoncé de plan pour fournir le patch. Pour des appareils anciens, les patches pourraient ne jamais être livrés.

Zimperium affirme que le Blackphone de SilentCircle est protégé contre cette attaque depuis la version 1.1.7 de PrivatOS. Firefox de Mozilla a également inclus un correctif pour ce problème depuis la version 38. Et bien sûr Zimperium propose sa propre protection contre les attaques Stagefright avec sa plate-forme de défense de la menace mobile, zIPS.

Voici comment se débrouiller sans patch
Mais ce que Zimperium ne mentionne pas, c'est qu'Android a déjà une excellente façon de bloquer la plupart des attaques de Stagefrights : bloquer tous les messages texte provenant d'expéditeurs inconnus.

Pour paramétrer cela avec Android Kitkat, la version la plus populaire d'Android, ouvrez l'application 'Messenger' et appuyez sur le menu dans le coin supérieur droit de l'écran (les trois points verticaux), puis appuyez sur 'Paramètres'. Une fois là, sélectionnez Bloquer les expéditeurs inconnus, et c'est tout.

Sur Lollipop, où Hangouts est l'application de messagerie par défaut, il n'y a aucun moyen par défaut de bloquer les expéditeurs inconnus. Vous pouvez toutefois sous 'Paramètres' aller aux 'messages multimédia' et désactivez 'Récupérer automatiquement les messages multimédias'.

Avec Lollipop et d'autres versions d'Android, je recommande de vous tourner vers des applications de blocage de SMS tierces. Pour Android 2.3 à 4.3, j'apprécie 'Blocage des Appels et SMS'. Si vous utilisez KitKat ou les versions au dessus, où une seule application de SMS peut être active au même moment, j'apprécie Postman, alias TEXT BLOCKER. Ce programme fonctionne en conjonction avec votre application préférée de textos pour bloquer les expéditeurs inconnus.

Rien de tout cela n'est parfait. Un ami peut toujours être infecté et propager des programmes malveillants. Mais c'est un bon début. La solution de court terme adviendra quand les fabricants et les opérateurs se magneront enfin le train et pousseront le correctif vers leurs clients. Mais compte tenu de leur historique, je ne vais pas attendre et je vais bloquer les MMS. La solution à long terme arrivera quand les entreprises qui utilisent Android commenceront à travailler avec Google pour fournir des correctifs de sécurité le plus rapidement possible, et tout le temps.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/stagefright-a-quel-point-les-utilisateurs-d-android-doivent-ils-etre-inquiets-39823010.htm
Par Steven J. Vaughan-Nichols