Microsoft stocke 200 Mo de données informatiques sous forme d’ADN

	Microsoft stocke 200 Mo de données informatiques sous forme d’ADN

L'université de Washington a collaboré avec Microsoft pour écrire 200 Mo de données informatiques sur un bout d'ADN. Le but est d'optimiser au maximum l'espace de stockage et sa durabilité en allant vers un stockage biologique.

Écrire 200 méga-octets de données informatiques sur de l'ADN de synthèse. C'est la prouesse réalisée par des scientifiques de l'université de Washington en collaboration avec Microsoft. Les informations inscrites sur les molécules contiennent la Déclaration universelle des droits de l'homme en plus de 100 langues, les 100 livres électroniques les plus téléchargés sur la bibliothèque Projet Gutenberg, une partie des bases de données de Crop Trust, un groupe consultatif international pour la recherche agricole et un clip musical du groupe américain Ok Go,
« *Nous utilisons l'ADN comme un espace de stockage de données numériques* », explique le professeur Luis Ceze dans une vidéo. « *La raison pour laquelle nous faisons cela est parce que l'ADN est très dense et que l'on peut mettre énormément d'informations dans un très petit volume* », ajoute-t-il.

LA TOTALITÉ DE L'INTERNET POURRAIT TENIR DANS UNE BOÎTE À CHAUSSURES
Il affirme également que la totalité de l'Internet pourrait tenir dans une boîte à chaussures grâce à ce procédé. L'autre motivation des scientifiques est aussi le fait que l'ADN peut être conservé très longtemps. « *Dans les bonnes conditions, il peut durer des milliers d'années tandis que les technologies de stockages ne tiennent que quelques décennies* ».

L'ADN est fait de différentes séquences de quatre molécules : l'adénine (A), la guanine (G), la cytosine (C) et la thymine (T).Les scientifiques ont réussi à encoder les données qu'ils voulaient stocker sur les quatre molécules de base de l'ADN synthétisé.
En analysant l'ADN, ils peuvent lire les informations et les rétablir à leur état original.
Les 200 Mo de documents sont enregistrés sur un bout d'ADN qui fait la taille de quelques grains de sucre. Celui-ci a été encapsulé pour éviter toute dégradation.
Les capacités de stockage de l'ADN sont énormes. Malheureusement, lire les données dessus prend beaucoup de temps – jusqu'à plusieurs heures. Aussi, ce procédé n'est pas prêt d'être démocratisé, d'autant plus qu'il coûte encore très cher. Mais cela serait apparemment en train de changer. « *La technologie pour lire l'ADN est en train de se développer rapidement et pourrait devenir suffisamment rapide et bon marché pour être commercialisée* », explique Luis Ceze à The Register.
Le scientifique pense que les premiers clients seront probablement les centres de données pour qui l'optimisation de l'espace de stockage est un enjeu permanent.

Article original de Omar Belkaab

Réagissez à cet article

Original de l'article mis en page : Microsoft stocke 200 Mo de données informatiques sous forme d'ADN – Sciences – Numerama

Le chiffrement des smartphones Android incassable ?

Le chiffrement des smartphones Android incassable ?

Un chercheur en sécurité décrit comment faire sauter la protection par chiffrement des données sur les smartphones Android équipés de puces Qualcomm.

Chiffrer l'ensemble de ses données sur un support de stockage est un bon moyen de les protéger en cas de perte ou vol du dit support. Néanmoins, il n'est pas infaillible. Particulièrement sur les smartphones Android équipés de processeurs Qualcomm. C'est ce que démontre le chercheur en sécurité Gal Beniamini. Dans un document très détaillé, il indique comment contourner les systèmes de protection. Et plus particulièrement, *« comment l'exécution du code TrustZone du noyau peut être utilisé pour briser efficacement le schéma de l'Encryption Full Disk d'Android »*, précise le chercheur.

Le Full Disk Encryption (FDE), la technique de chiffrement du disque d'Android, est proposé par Google depuis la version 5.0 de l'OS mobile. Il permet de générer des clés de chiffrement maître et esclave de 128 bits. La clé maître, également appelée DEK (pour Device Encryption Key) est protégée par chiffrement à partir du mot de passe, du code PIN ou du schéma de déverrouillage choisi par l'utilisateur. La DEK est stockée sur le smartphone (ou la tablette) dans un espace non chiffré de l'appareil, le *crypto footer*. Et c'est là que le problème survient. A cause d'une faille dans les processeurs de Qualcomm.

Utiliser une Trustlet

Pour comprendre pourquoi, il faut savoir que Android dispose, comme iOS, de mécanismes de temporisation et de blocage de l'appareil pour interdire les attaques par force brute (essais successifs de saisie des identifiants). Ces mécanismes sont liés au module KeyMaster qui s'exécute dans un environnement séparé de l'OS et considéré comme sécurisé, le Trusted Execution Environment (TEE). Le KeyMaster peut ainsi générer des clés de chiffrement sans les révéler au système d'exploitation. Une fois générées, ces clés sont à leur tour chiffrées et communiquées à l'OS. Quand ce dernier les sollicite, un bloc de données (le Blob, Binary Large OBject, un type de données qui permet l'intégration d'un pilote, souvent propriétaire, dans le code du noyau Linux) est fourni au KeyMaster sous forme d'une clé RSA de 2048 bits.

Mais le KeyMaster dépend de l'implémentation qu'en fait le fabricant sur son matériel. En l'occurrence, Qualcomm exploite bien le KeyMaster dans la TrustZone. Sauf que le TEE fourni par le constructeur, le QSEE (Qualcomm Secure ExecutionEnvironment), autorise des appliquettes (Trustlets) a s'exécuter dans cette zone sécurisée. Et, selon le chercheur, il est possible d'exécuter sa propre Trustlet dans la TrustZone en exploitant potentiellement une vulnérabilité Android. A partir de là, l'attaquant peut obtenir des privilèges administrateur et accéder au Blob qui contient les clés générées. Il ne reste alors plus qu'à lancer une attaque par force brute pour retrouver le code secret de l'utilisateur et disposer ainsi de la clé de déchiffrement du support de stockage.

Une correction difficile

Certes, la manœuvre n'est pas à la portée du premier venu. Et nécessite de disposer du terminal en main. Mais le déchiffrement d'un disque peut visiblement être exécuté par le fabricant des puces. Lequel peut avoir à se plier à une requête judiciaire comme on l'a vu avec Apple dans l'affaire de l'attentat de San Bernardino. Qui plus est, selon Qualcomm, le « bug » n'est pas facile à corriger. La correction demandera probablement une modification de l'architecture des processeurs. Lesquels équipent aujourd'hui une majorité de smartphones Android de la planète.

Néanmoins, le chercheur reste optimiste. *« J'espère qu'en jetant la lumière sur le sujet, cette recherche va motiver les équipementiers et Google à se réunir pour penser à une solution plus robuste pour le FDE*, écrit-il. *[…] Je crois qu'un effort concentré des deux côtés peut aider à rendre la prochaine génération d'appareils Android vraiment « inviolable ». »*

Article original de Christophe Lagane

Original de l'article mis en page : Le chiffrement des smartphones Android n'est pas incassable

---

Alerte : Une Backdoor destinée à voler les identifiants sur Mac OS X

(ESET)

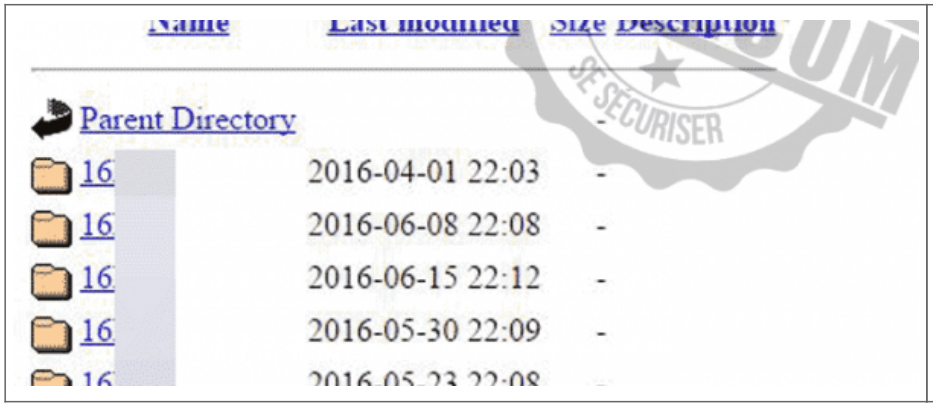
Alerte : Une Backdoor destinée à voler les identifiants sur Mac OS X (ESET)

Le malware Keydnap exfiltre les mots de passe et les clés stockés dans le gestionnaire de mot de passe « KeyChain » de Mac OS X et crée une porte dérobée permanente.

Les chercheurs ESET se sont penchés sur OSX/Keydnap, un cheval de Troie qui vole les mots de passe et les clés stockées dans le gestionnaire de mot de passe « keychain », en créant une porte dérobée permanente.
Bien que la façon dont les victimes se trouvent exposées à cette menace ne soit pas très clair, nous pensons qu'elle pourrait se propager via des pièces jointes contenues dans les spams, des téléchargements à partir de sites non sécurisés ou d'autres vecteurs.
Le code malveillant Keydnap est distribué sous forme de fichier .zip avec le fichier exécutable imitant l'icône Finder habituellement appliqué aux fichiers texte ou JPEG. Cela augmente la probabilité que le destinataire double-clique sur le fichier. Une fois démarré, une fenêtre de terminal s'ouvre et la charge utile malveillante est exécutée.
À ce stade, la porte dérobée est configurée et le malware débute la collecte et l'exfiltration des informations de base figurant sur la machine Mac attaqué. À la demande de son serveur C&C, Keydnap peut obtenir les privilèges administratifs en ouvrant la fenêtre dédiée d'OS X.
Si la victime saisit ses identifiants, la porte dérobée fonctionne alors comme un root, avec le contenu exfiltré du porte-clés de la victime.
Bien qu'il existe des mécanismes de sécurité multiples en place au sein d'OS X pour réduire l'impact des logiciels malveillants, il est possible de tromper l'utilisateur.
Tous les utilisateurs d'OS X doivent rester vigilants car nous ne savons toujours pas comment Keydnap est distribué, ni combien de victimes ont été touchées », rapporte Marc-Etienne M. Léveillé, Malware Researcher chez ESET.
Des détails supplémentaires sur Keydnap peuvent être trouvés dans notre article technique disponible sur WeLiveSecurity.com.

Réagissez à cet article
Source : ESET

Fuite de données colmatée pour l'Université de Bordeaux



Fuite de données colmatée pour l'Université de Bordeaux

Un problème informatique à l'université de Bordeaux donnait accès à plus de 15 000 dossiers d'étudiants. La CNIL est intervenue à la suite du protocole d'alerte de ZATAZ pour faire colmater une fuite de données que personne n'avait vue.

Tout a débuté voilà quelques semaines. Benjamin postule sur la plateforme APOFLUX de l'Université de Bordeaux. Rapidement, APOFLUX permet de déposer ses vœux pour rejoindre un cursus, une formation. Comme l'indique le site, APOFLUX est un outil de dépôt de vœux « ***Il ne s'agit en aucun cas de votre inscription administrative définitive à l'Université de Bordeaux***« . Bref, un espace ou les étudiants déposent des dizaines d'informations allant du simple au très sensible. « ***En cherchant une information sur mon dossier,*** m'expliquait alors Benjamin, ***je me suis rendu compte d'un – truc – plutôt moche***« . Et je trouve que le terme moche est très poli. Via un espace web non protégé baptisé « Dépôt », n'importe quel internaute avait accès à l'ensemble des dossiers des étudiants postulants. Chaque espace de stockage offrait à la lecture des curieux, de maladroits de la souris ou de violeurs d'intimité numérique, les relevés de notes, lettres de motivations, CV… ainsi qu'à l'ensemble des candidatures passées par APOFLUX. Le lien avait beau être en HTTPS, le S voulant dire que les connexions entre l'internaute et le serveur était chiffré, cela ne protégeait pas pour autant les informations sauvegardées.

Fuite de données colmatée, étudiant dans le silence

J'ai saisi la CNIL, qui au passage est d'une efficacité redoutable dès que je leur communique une alerte. Le problème a été colmaté en quelques heures. Pour le moment, l'université n'a pas contacté les étudiants concernés par cette fuite d'information. Espérons qu'aucun malveillant ne soit passé par là avant l'alerte de ZATAZ. Impossible de savoir depuis quand ces « portes ouvertes » étaient accessibles sur la toile.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Fuite de données colmatée pour l'Université de Bordeaux – ZATAZ

Le portable de Manuel Valls a-t-il été piraté par Israël ?

Le portable de Manuel Valls a-t-il été piraté par Israël ?

Lors de son déplacement en Israël, une délégation de Matignon a laissé ses portables sans surveillance pendant une réception officielle. Et a relevé des anomalies de fonctionnement sur certains terminaux ensuite, assure l'Express.

Manuel Valls s'est-il fait pirater son smartphone lors de son déplacement en Israël, fin mai dernier ? C'est la question que posent nos confrères de l'Express. Lors de son déplacement qui avait pour ambition de relancer le processus de paix avec la Palestine, le Premier ministre, qui se présente volontiers comme « l'ami d'Israël » et la délégation l'accompagnant ont été priés de laisser leurs téléphones portables à l'accueil avant d'être reçu en haut lieu. Demande à laquelle ils auraient accédé, laissant leurs terminaux sans surveillance pendant l'entretien.
Problème : quand ils ont récupéré leurs terminaux pourtant sécurisés, certains présentaient des « anomalies », selon l'Express. Des dysfonctionnements qui peuvent laisser suspecter une tentative d'intrusion de la part des services secrets israéliens. L'Express ne précise pas le ou les modèles des terminaux concernés par ces tentatives d'espionnage supposées.

Pas d'espionnage entre alliés. Sans blague ?
Depuis, les téléphones en question ont été remis à l'Agence nationale de la sécurité des systèmes d'information (Anssi), qui mène l'enquête. Interrogée par nos confrères, celle-ci s'est toutefois refusée à tout commentaire. De son côté, Matignon reconnaît qu'un terminal est bien tombé en panne durant la visite du Premier ministre en Israël. Et indique à nos confrères qu'un allié n'espionne jamais ses amis. Défense de rire.
Rappelons que, pour les échanges les plus sensibles, les officiels français disposent de terminaux Teorem, fournis par Thales et habilités confidentiel-défense. Ceux-ci se révèlent toutefois peu pratiques d'usage, si bien que les ministres utilisent souvent des smartphones du commerce, durcis avec des technologies de sécurité complémentaires. Récemment, l'Elysée s'est ainsi équipé de smartphones Hoox, conçus par Bull. Ces machines, des smartphones Android bénéficiant d'une surcouche logicielle de sécurisation, sont vouées aux échanges de type « diffusion restreinte », un niveau de classification de l'information moins exigeant que le confidentiel-défense.
Article original de Reynald Fleychaux

Réagissez à cet article

Original de l’article mis en page : Le portable de Manuel Valls a-t-il été piraté par Israël ?

Un nouveau malware s’attaque aux Mac

Un nouveau malware s’attaque aux Mac

BitDefender a découvert Backdoor.MAC.Eleanor, un malware qui permet aux attaquants de prendre le contrôle des machines Apple sous Mac OS et de les piloter à travers le réseau d'anonymisation Tor.

Selon l'éditeur de sécurité, Eleanor est distribué sous forme d'un logiciel que l'on peut télécharger depuis des sites web légitimes dédiés à l'univers Apple. Une fois installé, l'agent malveillant affiche une interface de conversion de fichiers par drag&drop, service supposément légitime qui, en toute opacité, installe des composants sur le système. A partir de là, l'attaquant peut prendre le contrôle complet de la machine, y compris capturer des images depuis la webcam du portable. Comme Eleanor n'est pas certifiée Apple, les utilisateurs sous El Capitan, la dernière version d'OS X verront s'afficher un message d'alerte de sécurité lors de l'installation de l'application infectieuse. Une barrière qui permettra d'éviter le pire.
Article original de Silicon

Réagissez à cet article

Original de l’article mis en page : Télégrammes :Darktrace; Google; e-Privacy; backdoor Mac

---

Quelques chiffres sur les risques du WiFi public

Quelques chiffres sur les risques du WiFi public

Aéroports, hôtels, cafés… Le WiFi public est très utilisé, mais pas sans risque. 30 % des managers ont fait les frais d'un acte cybercriminel lors d'un voyage à l'étranger, selon Kaspersky Lab.

Spécialiste des solutions de sécurité informatique, Kaspersky Lab publie les résultats d'une enquête réalisée par l'agence Toluna auprès de 11 850 salariés, cadres et dirigeants dans 23 pays, sur leur utilisation de terminaux et Internet à l'étranger. Tous ont voyagé à l'international l'an dernier, à titre professionnel ou personnel. Premier constat : 82 % ont utilisé des services WiFi gratuits, mais non sécurisés (aucune authentification n'étant nécessaire pour établir une connexion réseau), depuis un aéroport, un hôtel, un café… Or, 18 % des répondants, et 30 % des managers, ont fait les frais d'un acte cybercriminel (malware, vol de données, usurpation d'identité…) lorsqu'ils étaient à l'étranger.

Droit ou devoir de déconnexion ?

« Les businessmen assument que leurs terminaux professionnels sont plus sûrs du fait de la sécurité intégrée », a souligné l'équipe de Kaspersky Lab dans un billet de blog. Et si cela n'est pas le cas, ils considèrent que ce n'est pas leur problème. Ainsi *« un répondant sur quatre (et plus de la moitié des managers) pense qu'il est de la responsabilité de l'organisation, plutôt que de celle de la personne, de protéger les données. En effet, à leurs yeux, si les employeurs envoient du personnel à l'étranger, ils doivent accepter tous les risques de sécurité qui vont avec »*.

Si des données sont perdues ou volées durant leur voyage, la plupart des managers seraient prêts à blâmer leur département informatique. Et ce pour ne pas avoir recommandé l'utilisation de moyens de protection comme un réseau privé virtuel (VPN), des connexions SSL ou encore la désactivation du partage de fichiers lors d'une connexion WiFi… Quant au droit à la déconnexion, lorsqu'il existe, il se pratique peu. Pour 59 % des dirigeants et 45 % des managers *« intermédiaires »*, il y une attente de connexion quasi continue de la part de leur employeur.

Article original de Ariane Beky,

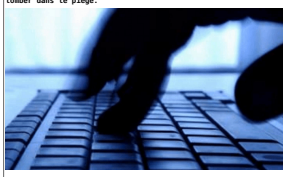
Réagissez à cet article

Original de l'article mis en page : Les voyageurs d'affaires ignorent les risques du WiFi public

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

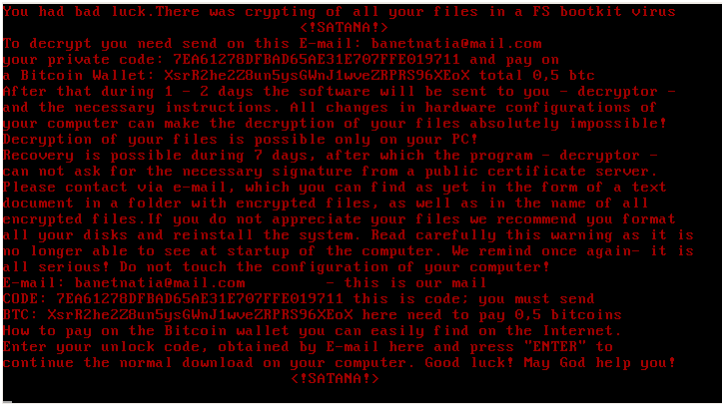
Original de l'article mis en page : Regionale.info CYBERCRIMINALITE : TOP 5 des arnaques les plus récurrentes au premier trimestre 2016 selon la PLCC > Regionale.info

---

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.

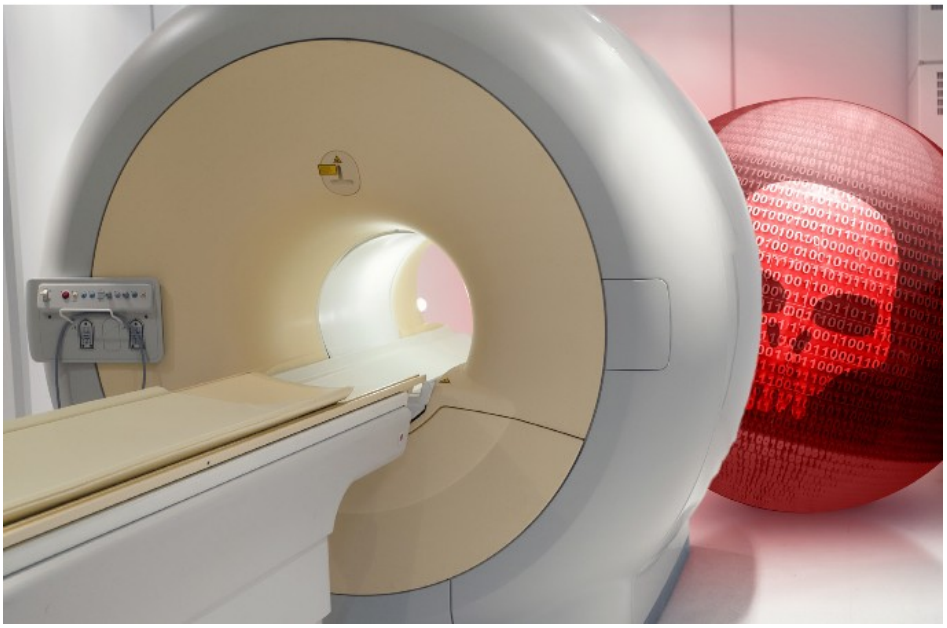
Article original de Christophe Lagane

Réagissez à cet article

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

---

Risques d’infection dans le médical des Objets Connectés



Risques d’infection dans le médical des Objets Connectés

La faible sécurité des équipements de santé connectés entraîne la résurgence des vieux virus comme Conficker.

Un des problèmes de la montée en puissance de l'Internet des objets ? La sécurité.
Spécialistes, constructeurs, éditeurs répètent à longueur de conférences qu'il faut absolument que l'IoT soit « secure by design ». Entendez par là que les capteurs, le protocole de communication, la plateforme de traitement de l'information, l'architecture soient sécurisés dès leur conception.
Oui mais voilà, c'est sans compter sur le fameux héritage technique. Le monde de la santé rentre typiquement dans ce cadre et tout particulièrement les outils médicaux connectés. On pense ici aux IRM, scanners, radios, ou pompes à insuline. Ces équipements sont de plus en plus ciblés par les cyberattaquants, car ils sont moins bien protégés que des PC ou des serveurs.
Conséquence de cette faible sécurité, les vieux virus se rappellent aux bons souvenirs des administrateurs et des RSSI. Un rapport de la société de sécurité TrapX Labs, disséquant une attaque baptisée MEDJACK.2, montre que les attaques utilisent des malwares comme networm32.kido.ib ou le ver Conficker en complément de menaces plus sophistiquées. Moshe Ben Simon, co-fondateur de TrapX, résume bien ce paradoxe : « *un loup intelligent déguisé avec des vieux habits de mouton* ».

Mise en place de backdoors

Premier constat, les équipements médicaux connectés à Internet fonctionnent avec des versions de Windows non corrigées allant de XP (qui n'est plus supporté par Microsoft) aux versions 7 et 8. Des cibles de choix pour les anciens virus. « *Ces vieux virus sont utilisés avec des malwares (en l'occurrence MEDJACK.2) plus élaborés pour installer des backdoors dans l'établissement de santé et ensuite mener une campagne par exfiltration de données, voire se transformer en #ransomware* », souligne le rapport.
Les échantillons de Conficker que les experts de la société de sécurité ont analysé, montrent que le ver a été modifié pour avoir une meilleure capacité à se déplacer dans un réseau. Pire, son évolution fait qu'il est devenu indétectable pour les équipements médicaux. Dans son enquête auprès de 3 hôpitaux, TrapX relève qu'aucune alerte n'a été remontée par les établissements sur la présence de Conficker. A son apogée en 2009, Conficker avait infecté entre 9 et 15 millions d'ordinateurs. Il avait, comme capacité, de casser les mots de passe, d'enrôler les PC dans des botnets, etc. La version actuelle est diffusée par phishing envoyé aux personnels de l'hôpital.

Les données patients : la ruée vers l'or

L'objectif de ces attaques : obtenir les dossiers patients. Des informations très demandées sur le Dark Web et affichant une forte valeur marchande au marché noir. « *Les cybercriminels peuvent voler l'identité d'un patient pour se faire rembourser par les assurances des traitements coûteux et, en plus, revendre ces traitements au marché noir* ». TrapX estime qu'un dossier médical se monnaye entre 10 et 20 dollars sur le marché, contre 5 dollars pour une information financière. En début de semaine, on apprenait le vol de 9,3 millions de données de santé de citoyens américains. Le calcul est vite fait…
Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Sécurité : Conficker revient infecter l’IoT médical