Les cyberattaques sont de plus en plus furtives

Les cyberattaques sont de plus en plus furtives

Comment détecter les cyberattaques les plus furtives ? Une priorité au quotidien pour toutes les entreprises. Tomer Weingarten, CEO SentinelOne, nous livre son expertise sur le sujet.

Alors que les cybercriminels – individus, groupements ou Etatiques – utilisent une combinaison de techniques complexes pour échapper à la détection, les cyberattaques deviennent plus intelligentes et furtives. Les techniques traditionnelles de protection reposant sur des signatures statiques – tels que les anti-virus (AV) – ou l'ignorance des vecteurs d'attaques comme les fichiers compromis, ne sont plus adaptés pour faire face au paysage de menaces d'aujourd'hui. Alors comment les entreprises peuvent tenter de se protéger contre les variantes de logiciels malveillants ou des nouveaux exploits, en constante évolution ?

Le poste de travail – incluant une série d'équipements : ordinateurs portables, tablettes, smartphones, serveurs ou même imprimantes – demeure l'une des cibles de choix dans toute attaque. Le poste de travail agit comme une passerelle pour les hackers dans leur intrusion au sein du réseau et une fois qu'un logiciel malveillant a été exécuté sur un poste de travail, les attaquants peuvent se déplacer librement. Ainsi, la détection et la protection doivent se produire sur les terminaux eux-mêmes. Ceci est d'autant plus important à l'ère du BYOD, car les utilisateurs peuvent facilement connecter leurs propres appareils au réseau de l'entreprise. Or, si les utilisateurs se connectent à un dispositif non autorisé ou infecté, le malware peut se déplacer librement au sein du réseau.

Evolution de la menace

Les techniques utilisées par les cybercriminels sont toujours en évolution pour garder une longueur d'avance sur les systèmes de protection et, comme la sophistication des logiciels malveillants se développe également, cela représente de nouveaux challenges pour les entreprises. Dans sa définition, un malware n'a pas changé. **Ce qui est en train de changer, ce sont les techniques d'évasion utilisées par de nouvelles formes de logiciels malveillants dans le but de voler des données précieuses présentent sur les postes de travail.**

Les "binders" sont un excellent exemple : ce sont de petits outils logiciels qui fusionnent deux fichiers .exe différents dans un seul fichier. L'exécution d'un .exe démarre simultanément le second de manière invisible. Ces outils piègent leurs victimes avec l'ouverture d'un fichier connu et qui semble légitime à l'extérieur ; mais qui est en fait malveillant à l'intérieur.

Aujourd'hui, les logiciels malveillants peuvent être conçus pour être « sensibles au contexte » et ont la capacité de détecter s'ils évoluent dans un environnement sandbox physique ou virtualisé. Une fois que ce type de malware détecte un environnement anormal, il échappe activement à la détection en agissant de façon bénigne ou en "dormant" pendant une période de temps définie. À partir de là, le malware tente d'interpréter les mouvements et de déchiffrer, si les actions proviennent d'un être humain ou d'un scanner de code automatisé. Cela permet au malware de contourner facilement les défenses traditionnelles telles que les sandboxes réseau, jusqu'à son exécution.

Reprendre le contrôle

Les attaques étant devenues plus sophistiquées, la protection des postes de travail annonce probablement la fin des anti-virus. Ces derniers reposant effectivement sur une analyse statique qui repère l'empreinte d'un fichier, les attaquants peuvent rapidement adapter des fichiers pour créer quelque chose de complètement nouveau et inconnu ; et ces nouvelles variantes peuvent facilement contourner la solution AV. Il a ainsi été estimé que les anti-virus ne peuvent repérer qu'environ 45 % des cyberattaques – ce qui en fait une solution obsolète face aux défis de la cybersécurité d'aujourd'hui.

Dans ce contexte, **une nouvelle génération de solutions de sécurité du poste de travail est en train d'émerger, telles que les techniques d'analyse comportementale,** afin que les entreprises puissent profiter des avantages des approches innovantes. Cette nouvelle ère de la protection se concentre, en temps réel, sur une approche proactive de la sécurité du poste de travail, réalisée par l'apprentissage automatique (machine learning) et l'automatisation intelligente afin de détecter et de protéger efficacement tous les terminaux contre les attaques les plus perfectionnées. Cette nouvelle génération de protection des postes de travail part du principe qu'elle ne connait rien sur les logiciels malveillants, mais qu'elle observe leur comportement dans le but de repérer les activités considérées comme des anomalies, et mettre en place les étapes de défense pour les dévier complètement.

De plus, **cette nouvelle génération de solutions a des capacités de remédiation pour inverser toutes les modifications apportées par les logiciels malveillants.** Cela signifie que lorsque les fichiers sont modifiés ou supprimés, ou lorsque des modifications sont apportées aux paramètres de configuration ou aux fichiers systèmes, le logiciel a la capacité de restaurer un poste de travail, comme il était, avant l'exécution du malware.

Dans la lutte contre la nouvelle génération de cyberattaques, cette approche plus dynamique et robuste des postes de travail permet aux entreprises de prendre l'avantage face aux cybercriminels.

Article original de iTPro.fr

Réagissez à cet article

Original de l’article mis en page : Détecter les cyberattaques les plus furtives | iTPro.fr

---

L’arnaqueur Chinaper Chinapa roi de l’escroquerie sur Internet enfin arrêté

L’arnaqueur Chinaper Chinapa roi de l’escroquerie sur Internet enfin arrêté

Il se nomme Chinaper Chinapa, un arnaqueur de Côte d'Ivoire qui vient d'être arrêté. Il arnaquait des hommes et des femmes sur Internet.

Les scammeurs, les brouteurs, bref les escrocs qui s'attaquent aux internautes sont légions sur la toile. Ils usent de multiples arnaques pour soutirer de l'argent à leurs victimes. Ils jouent ensuite les « rois » dans leur quartier. Parmi les pièges usités : l'arnaque à l'amour, le wash-wash, la création de billets, le faux mail d'inquiétude d'un proche perdu, la fausse location ou loterie… Pour Chinaper Chinapa, chaussures et portes feuilles magiques en bonus ! Je possède une liste d'une quarantaine d'arnaques possibles mises en place par les brouteurs.

Chinaper Chinapa le chenapant !

L'un des « rois » des brouteurs se nommait Chinape Chinapa. L'amateur de casquettes et baskets « bling-bling » se faisait passer pour un « magicien ». Il affirmait être capable de faire sortir des billets de chaussures, de boite magique. Il avait aussi mis en place des arnaques amoureuses, se faisant passer pour des hommes et des femmes à la recherche de l'âme sœur. Il volait les photos sur Facebook et « chassait », ensuite, sur des sites de rencontres.

J'ai pu croiser cet escroc de Chinaper Chinapa, il y a quelques mois, dans son pays (il se baladait aussi beaucoup au Bénin). Ce « roi » des boites de nuit qui sortait les billets de banque plus vite que 007 son Walther PPK.

Mi juin 2016, l'homme avait été tabassé par des personnes qu'il avait escroquées. Quinze jours plus tard, la police lui mettait la main dessus pour une série d'escroqueries. Arrêté par la police début juillet, détail confirmé par le journal Koaci. Le flambeur s'est retrouvé les menottes aux poignets dans son appartement de Cocody. Il est accusé d'activités cybercriminelles et de multiples escroqueries. Pas évident que sa « magie » fonctionne dans la prison d'Abidjan.

Un ami a besoin de vous

15h, un courrier signé d'un de vos amis arrive dans votre boîte mail. Pas de doute, il s'agit bien de lui. C'est son adresse électronique. Sauf que derrière ce message, il y a de forte chance qu'un brouteur a pris la main sur son webmail. Les courriels « piégés » arrivent toujours avec ce type de contenu « ***Je ne veux pas t'importuner. Tu vas bien j'espère, puis-je te demander un service ?***« . Le brouteur, par ce message, accroche sa cible. En cas de réponse de votre part, l'interlocuteur vous sortira plusieurs possibilités liées à sa missive « ***J'ai perdu ma carte bancaire. Je suis coincé en Afrique, peux-tu m'envoyer de l'argent que je te rembourserai à mon retour*** » ; « ***Je voudrais urgemment recharger ma carte afin de pouvoir régler mes frais de déplacement et assurer mon retour. J'aimerais s'il te plaît, que tu me viennes en aide en m'achetant juste 4 coupons de rechargement PCS MASTER CARD de 250 € puis transmets moi les codes RECH de chaque coupon de rechargement, je te rembourserais dès mon retour***« . Je possède plus d'une centaine de variantes d'excuses.

Bien entendu, ne répondez pas, ne versez encore moins d'argent. Attention, selon les brouteurs, des recherches poussées sur leurs victimes peuvent être mises en place. J'ai dernièrement traité le cas d'un brouteur qui connaissait le lieu de résidence du propriétaire du compte webmail que le voyou utilisait. De quoi faire baisser les craintes des amis contactés.

A noter que le scammeur indiquera toujours un besoin de confidentialité dans sa demande : « ***Je souhaite également que tu gardes ce mail pour toi uniquement. Je ne veux pas inquiéter mon entourage. Y'a t'il un buraliste ou un supermarché non loin de toi ?***« .

Remboursement de l'argent volé

Une autre arnaque de brouteurs est intéressante à expliquer. Elle est baptisée « *remboursement*« . Le voleur écrit aux internautes se plaignant, dans les forums par exemple, d'avoir été escroqués. L'idée de l'arnaque est simple : le voleur indique qu'il a été remboursé grâce à un policier spécialisé dans les brouteurs. Le voyou fournit alors une adresse électronique.

Suivre

ZATAZ.COM Officiel @zataz

Prudence à l'adresse « interpol.police.antiarnaque@gmail(.)com » qui n'est pas celle d' #interpol *! L'escroc cherche des personnes escroquées.*

23:12 – 14 Mai 2015

•

•

1111 Retweets

•

55 j'aime

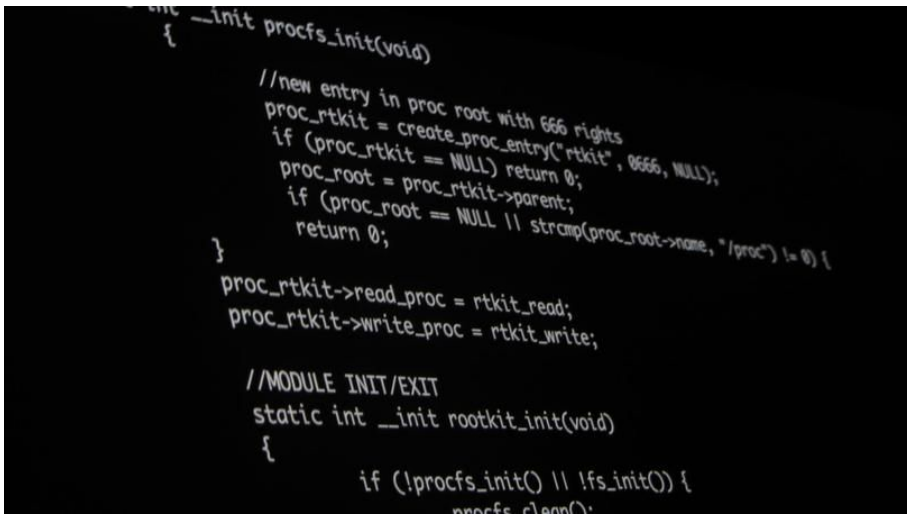
Derrière cette fausse adresse de policier, un autre brouteur. Il va tenter d'escroquer le pigeon déjà pigeonné. Sa mission, se faire envoyer de l'argent via Western Union, MoneyGram. Certains brouteurs sont à la solde de petits commandants locaux qui imposent un quota d'argent à collecter. En 2013, la cyber police de Côté d'Ivoire estimait que les brouteurs avaient pu voler pas moins de ***21 millions d'euros****. N'hésitez pas à me contacter si vous avez croisé la route d'arnaques.*

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Brouteur : Chinaper Chinapa roi de l’escroquerie 2.0 – ZATAZ

Les américains s’inquiètent de la cyber-sécurité automobile



Les américains s’inquiètent de la cyber-sécurité automobile

Après l'attentat de Nice, les questions de cyber-sécurité sont devenues une urgence pour les américains, qui imaginent le scénario catastrophe d'un pirate informatique prenant le contrôle d'un véhicule.

L'attentat terroriste de Nice a ravivé dans le secteur automobile américain les craintes d'un scénario catastrophe où un pirate informatique prend à distance le contrôle d'une voiture pour l'utiliser comme projectile. Cette éventualité, digne d'un scénario hollywoodien, est alimentée par la circulation croissante de voitures semi-autonomes et connectées, équipées de systèmes multimédias embarqués censés les rendre plus sûres et fiables.

Paradoxalement, ces mêmes technologies de pointe en font des cibles privilégiées pour les hackers, selon les sociétés de sécurité informatique américaines Mission Secure Inc (MSi) et Perrone Robotics Inc. Car, selon celles-ci, les pirates informatiques pénètrent via les connexions sans fil, bluetooth et wifi, nécessaires à leur fonctionnement. «La technologie crée beaucoup d'opportunités nouvelles et excitantes pour les consommateurs mais (génère) aussi des défis», opine Mary Barra, la PDG de General Motors (GM). «L'un de ces défis est la problématique sur la cyber-sécurité», a-t-elle insisté vendredi devant un parterre composé de ses pairs, d'officiels et d'experts de l'automobile réunis à Detroit pour évoquer les cyber-attaques.

Le 14 juillet, Mohamed Lahouaiej-Bouhlel, un Tunisien, a foncé au volant d'un camion dans la foule à Nice tuant 84 personnes et blessant plus de 330 personnes.

«Nous connaissons ces terroristes (…) il ne faut pas beaucoup d'imagination pour penser qu'ils vont se servir d'une voiture autonome et la faire foncer dans une foule.»
John Carlin, un ministre-adjoint américain de la Justice.

«Nous connaissons ces terroristes. Ils n'en ont peut-être pas encore les capacités mais s'ils parviennent à convaincre les gens de foncer dans une foule avec un camion, il ne faut pas beaucoup d'imagination pour penser qu'ils vont se servir d'une voiture autonome et la faire foncer dans une foule», redoute John Carlin, un ministre-adjoint américain de la Justice. «Les méchants emploient de plus en plus de moyens sophistiqués», souscrit David Johnson, un des responsables du FBI chargé des cybercrimes et des menaces sur internet.

A l'été 2015, deux chercheurs américains en informatique ont démontré qu'il était facile de prendre le contrôle d'une voiture «connectée». Charlie Miller et Chris Valase étaient parvenus à pirater à distance la Jeep Cherokee d'un journaliste du site spécialisé Wired. Ils avaient ainsi pu allumer la radio, fait fonctionner les essuie-glaces et, surtout, couper le moteur. Ils étaient aussi parvenus à désactiver les freins. Les «menaces évoluent», avance Titus Melnyk chargé de la sécurité chez Fiat Chrysler Automobiles (FCA), qui vient de lancer un programme visant à encourager les hackers à informer le groupe des failles liées à la cyber-sécurité de ses voitures. Le constructeur des Jeep promet une prime pouvant aller jusqu'à 1.500 dollars par alerte. «On ne sait jamais. Cela peut être la base d'une attaque», défend M. Melnyk insistant sur le fait que ce programme est «très sérieux».

En 2015, le constructeur de véhicules électriques de luxe Tesla – dont les deux modèles commercialisés (Model S et Model X) sont équipés d'un système d'aide à la conduite leur permettant d'effectuer seuls certaines manoeuvres comme le freinage en urgence – avait été l'un des premiers à lancer un tel plan. Tesla, qui a construit sa réputation sur l'innovation, n'avait pas le choix: deux chercheurs avaient révélé qu'ils pouvaient couper à distance le moteur d'une berline Model S en piratant le système multimédia. GM, qui dit recevoir et résoudre plusieurs alertes liées à de possibles cyber-attaques par jour, gère un programme sur les vulnérabilités de ses voitures sur le site hackerone.com.

Les nouvelles technologies embarquées exposent également les conducteurs à un vol potentiel de leurs données personnelles quand ils connectent leur téléphone intelligent.

Article original de lefigaro.fr

Réagissez à cet article

Original de l’article mis en page : Les américains s’inquiètent de la cyber-sécurité automobile

---

Orange corrige un sérieux problème de sécurité dans l’une de ses boutiques en ligne

Orange corrige un sérieux problème de sécurité dans l’une de ses boutiques en ligne

---

Alterte ! Plusieurs problèmes découverts dans le site orangeboutique.fr. L'un d'eux aurait pu permettre d'injecter un document piégé directement dans une boutique Orange.
Imaginez, vous visitiez le site orangeboutique.fr [espace fermé depuis le 19/07/16] et téléchargiez ce que vous pensiez être un document officiel de l'opérateur téléphonique Français. Un PDF vous proposant les dernières réductions et promotions. Sauf que dans ce fichier Adobe, un code malveillant orchestrant le téléchargement d'un logiciel espion dans votre ordinateur.
De la science-fiction ? Malheureusement, non ! Le protocole d'alerte de ZATAZ a permis la correction de plusieurs problèmes dans le site orangeboutique.fr. Parmi les « bugs » que je peux vous révéler aujourd'hui, la possibilité d'injecter dans l'espace 2.0 n'importe quel fichier à partir d'une page dédiée non verrouillée.
L'équipe sécurité d'Orange a très rapidement pris en main et corrigé le problème dès la réception du Protocole d'Alerte. D'autres failles et fuites concernées ce même site, avec par exemple l'accès à des documents internes. Des fichiers non sensibles [pas de données clients], sauf dans les mains de la concurrence pouvant ainsi découvrir les actions commerciales à venir dans les agences physiques Orange (Tarifs, produits, cibles clientèles…). Des accès sans aucune restriction, ni mot de passe. Le site a été fermé le 19 juillet 2016.
Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Orange corrige un sérieux problème dans l'une de ses boutiques en ligne – ZATAZ

L’Internet des objets, ce piège de cristal

	L’Internet des objets, ce piège de cristal

Encore une fois, l'actualité technologique nous démontre que l'Internet des objets est un problème de sécurité de masse en devenir.

Vous le savez sans doute si vous suivez mes articles, je suis un tantinet sceptique quant à la montée de l'Internet des objets, soit le mariage entre l'Internet et les objets du quotidien. Non pas que je doute des possibilités offertes par les systèmes qui émergeront de cette tendance, bien au contraire. Ce sont plutôt les problèmes de sécurité qu'ils engendreront qui me laissent quelque peu pantois.

Imaginez les grands titres : «Incapables de regarder le Canadien de Montréal à cause d'un maliciel». Je vous jure, là, les gens vont débarquer dans les rues.

Lorsqu'on prend du recul et qu'on regarde ce qui se passe, nous sommes littéralement en train de nous créer notre propre piège de cristal : c'est bien beau et reluisant à l'extérieur, mais un gros problème se cache à l'intérieur. Nous sommes en train de devenir dépendants de systèmes extrêmement poreux. Or, je ne serais pas surpris de voir que bon nombre d'objets connectés que l'on considère comme des «acquis» finissent par tomber en otage aux mains d'un Hans Gruber en puissance qui décide tout simplement de nous faire cracher le cash pour retrouver le contrôle desdits objets.
Ça semble peut-être bien théorique en ce moment, mais la journée où des voitures, des frigos, des systèmes de chauffages, ou des téléviseurs cesseront de fonctionner pour la simple et bonne raison qu'ils seront tombés entre les griffes d'un quelconque cryptorançongiciel remâché, ça risque de déranger pas mal de monde, et pire, en inquiéter encore plus. Imaginez les grands titres dans les tabloïds : «Incapables de regarder le Canadien de Montréal à cause d'un maliciel». Je vous jure, là, les gens vont débarquer dans les rues.

Die Harder

*Le pire dans tout ça, c'est qu'on est véritablement devant une chronique de mort annoncée. Déjà, on a constaté que certains objets connectés pouvaient être massivement piratés par toutes sortes de moyens. Il y a quelques mois de cela, on découvrait par exemple que des ampoules et des serrures connectées **pouvaient être ciblées et exploitées par des pirates informatiques malintentionnés**. On imagine déjà le potentiel de ce genre de vulnérabilités pour la sécurité résidentielle. Pourtant, on en est qu'aux débuts en ce qui concerne les problèmes dans les systèmes de sécurité.*

*(Photo : **Frédéric Bisson**)*

*Tout récemment, on a d'ailleurs vécu le comble de l'ironie dans les systèmes de sécurité alors que pas moins de 25 000 caméras de surveillance ont fait partie **d'un réseau de botnets lançant des attaques par déni de services**. Grosso modo, des pirates informatiques ont été en mesure de pirater des caméras de surveillance mal sécurisées, de les fédérer dans un réseau sous un serveur de commandement et de contrôle et de les réutiliser pour commettre des attaques informatiques ultérieures. C'est-y pas beau ça!?*

*Pourtant, on avait déjà eu des signes avant-coureurs de ce genre d'attaques. Des réseaux de botnetsconstruits avec des caméras de surveillance avaient déjà **été découverts dans des analyses précédentes**. Des analyses qui démontraient par ailleurs que ces objets connectés étaient passablement poreux.*
*Et on est loin d'être sortis du bois, je vous en passe un papier. Non seulement il existe **des moteurs de recherche permettant de trouver les objets connectés** présents sur Internet, mais en plus, on a des petits génies informatiques qui se mettent à les **géolocaliser en utilisant des drones**. Donc, si vous aviez espoir que ça ralentirait quelque peu, détrompez-vous.*

*Pourtant, je ne suis pas le seul qui a des problèmes de sommeil par rapport à cette situation. En 2014, Europol prédisait **qu'un meurtre mené par Internet allait probablement se produire dans les prochains mois**. Bon, moi je n'irais pas jusqu'à faire une prédiction temporelle, mais c'est clair que, tôt ou tard, un truc du genre va finir par arriver. Je ne suis pas certain que ce sera un événement intentionnel, mais considérant la vitesse à laquelle on intègre des objets connectés dans le réseau de la santé, ce n'est qu'une question de temps avant que quelqu'un meurt suite à un incident informatique.*

Marche ou crève

Bon, j'ai beau couiner et geindre, c'est bien dommage, mais on ne changera pas pour autant les avancées technologiques. Le néo-luddisme ne sert strictement à rien dans ce cas; il faudra à terme que l'industrie atteigne un niveau de maturité suffisant pour construire les objets connectés avec une architecture centrée sur la sécurité. En attendant, on est dû pour quelques coups fumants de piratage et de prises d'otages numériques.
En fait, la vraie question que l'on doit se poser est celle du «retour sur investissement». Dans le cas du secteur de la santé par exemple. Oui, c'est clair que des gens finiront par mourir dus à des problèmes liés à l'informatique. Cependant, il faut aussi considérer l'autre côté de la médaille, c'est-à-dire combien de personnes ont été sauvées par ces mêmes systèmes informatiques.
Il en va de même avec les gestes que posent John McClane dans la série Die Hard. Oui, il finit par causer beaucoup de dommages et par tuer beaucoup de monde au cours de ses aventures, mais il sauve également la vie de centaines de victimes innocentes.

Yippee Ki-Yay Mother$&@%!*
Article original de Benoît Gagnon

Réagissez à cet article

Original de l’article mis en page : L’Internet des objets, ce piège de cristal | Branchez-vous

---

Attention, faille découverte dans les réseaux mobiles GSM et 4G LTE !

Attention, faille découverte dans les réseaux mobiles GSM et 4G LTE !

Un audit de sécurité a trouvé une faille critique dans un compilateur de code utilisé par plusieurs logiciels propres aux réseaux mobiles GSM et 4G LTE

Plusieurs logiciels pour la gestion et l'interconnexion des réseaux mobiles du monde entier GSM et LTE (4G) sont vulnérables à une faille permettant une exécution de code à distance où un attaquant peut donc prendre le contrôle d'un équipement réseau. Le CERT-US a déjà lancé un avertissement sur cette vulnérabilité.

Classée sous le nom CVE-2016-5080, cette faille a été découverte lors d'un audit de sécurité d'Objective Systems, un éditeur américain qui commercialise asn1C, un compilateur de code servant à créer les applications de gestion et d'interconnexion des réseaux mobiles. Asn.1 (Abstract Syntax Notation One) est une norme internationale qui décrit les structures de données et les protocoles de transfert utilisés dans le domaine des télécommunications. Asn1c est une application qui récupère les instructions, les opérations et les structures des données pour le convertir en C, C++, C# ou en Java. Cette transformation peut ensuite être intégrée dans des applications fonctionnant sur des réseaux mobiles GSM ou LTE.

Peu d'acteurs concernés par la faille ?

Objective Systems précise que la vulnérabilité se trouve dans la compilation du code ASN.1 vers C et C++. La faille consiste en un débordement de la mémoire tampon ouvrant la porte aux attaquants pour exécuter du code sur les systèmes compromis, à distance et sans avoir besoin d'authentification sur le périphérique. L'éditeur a corrigé son logiciel et continue à vérifier la compilation vers C# et Java.

La question est de savoir qui est touché par cette faille. Le Cert américain a lancé son avertissement auprès de 34 opérateurs mobiles et équipementiers. Peu ont répondu à cet appel, Qualcomm a indiqué dans qu'il intégrait ce code dans ses produits cellulaires, mais que la faille n'est pas exploitable. Malgré cet optimisme, la société américaine a diffusé le patch d'Objective Systems sur ses solutions. D'autres entreprises comme HPE ou Honeywell ont précisé qu'elles n'étaient pas concernées.

Objective Systems revendique une base client comprenant plusieurs grands noms des réseaux mobiles comme Alcatel-Lucent, AT&T, BT, Cisco, Deutsche Telekom, etc. Le problème est qu'à la différence d'un terminal mobile, il est plus difficile de patcher les équipements télécoms.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Une faille découverte dans les réseaux mobiles GSM et 4G LTE

Les claviers sans fil pourraient aussi servir à espionner !

Les claviers sans fil pourraient aussi servir à espionner !

Avec un simple dongle USB, une antenne et quelques lignes de code, un pirate peut capter toutes les frappes d'un clavier sans fil, selon la start-up Bastille.

Après les souris (MouseJack), les claviers sans fil… Avec une simple antenne et un dongle USB, plus quelques lignes de code écrites en Python, un pirate peut enregistrer *« toutes »* les frappes réalisées par l'utilisateur d'un clavier sans fil bon marché ou générer ses propres frappes, selon la start-up américaine Bastille. Et ce dans un rayon de plusieurs dizaines de mètres autour de la cible.

Claviers sans fil vulnérables

« Lorsque nous achetons un clavier sans fil, nous nous attendons à ce que le fabricant ait conçu et intégré la sécurité nécessaire au coeur du produit », a déclaré Marc Newlin, ingénieur et chercheur chez Bastille. *« Nous avons testé les claviers de 12 fabricants et nous avons constaté, malheureusement, que 8 d'entre eux (soit les deux tiers) sont vulnérables à une attaque [que l'on nomme] KeySniffer »*.

Ces claviers sans fil utilisent le plus souvent des protocoles radio propriétaires peu testés et non sécurisés pour se connecter à un PC, à la différence du standard de communication Bluetooth. Ils sont d'autant plus faciles à détecter car leur signal est toujours actif… Les fabricants concernés (dont HP, Toshiba et Kensington) ont tous été alertés. Selon Bastille, la plupart, voire tous les claviers exposés à KeySniffer ne peuvent pas être mis à jour et devront être remplacés.

Absence de chiffrement

En 2010 déjà, les développeurs de Dreamlab Technologies ont exposé une faille dans un clavier sans fil Microsoft. Le *« renifleur »* et programme Open Source KeyKeriki a capté le signal et déchiffrer les données transmises à un ordinateur… Mais la découverte de Bastille, KeySniffer, est différente. Elle montre que des fabricants produisent et vendent encore des claviers *wireless* sans chiffrement.

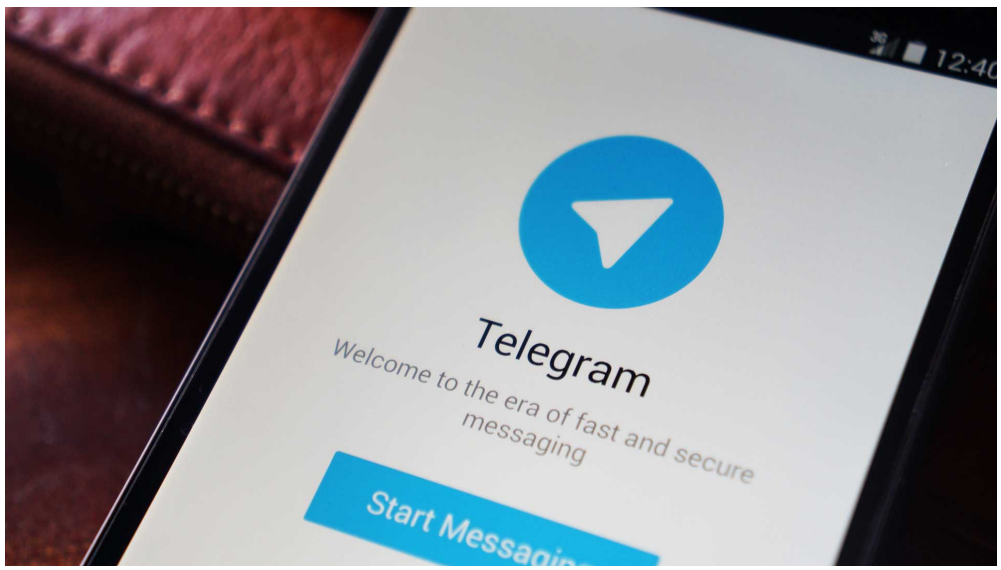
La start-up recommande aux internautes d'utiliser un clavier filaire pour se protéger.

Article original de Ariane Beky

Réagissez à cet article

Original de l'article mis en page : Les claviers sans fil, des espions en puissance

Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ? – Politique – Numerama



Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ?

Selon La Voix du Nord, au moins l'un des deux auteurs de l'attentat de l'église de Saint-Étienne-du-Rouvray utilisait régulièrement la messagerie chiffrée Telegram pour communiquer avec des islamistes, et aurait posté un message une heure avant l'attentat.

Il faut s'attendre à voir très vite renaître le débat sur le chiffrement et l'obligation qui pourrait être faite aux fournisseurs de messageries électroniques de laisser les services de Renseignement accéder aux communications. La Voix du Nord affirme qu'Adel Kermiche, l'un des deux coauteurs de la tuerie de l'église de Saint-Étienne-du-Rouvray, près de Rouen, utilisait la messagerie chiffrée Telegram, à des fins djihadistes. Il aurait envoyé un message sur un canal de discussion une heure avant l'attaque.
« Selon nos informations, Adel Kermiche avait ouvert sur Telegram une « private channel » (haqq-wad-dalil), une chaîne lui permettant de s'adresser à une audience ultra-sélectionnée. Il avait choisi pour nom de code Abu Jayyed al-Hanafi et la photo de Abou Bakr al-Baghdadi, chef suprême de l'État islamique, comme représentation », écrit le quotidien régional.

TÉLÉCHARGER (SIC) CE QUI VA VENIR ET PARTAGER LE EN MASSE ! ! ! !
Selon les membres arabophones de la rédaction de Numerama, haqq-wad-dalil signifierait quelque chose comme « preuve de la vérité » ou « guide de la vérité ».
La Voix du Nord ajoute que « le terroriste correspondait depuis des mois via ce canal avec près de 200 personnes, dont une dizaine de Nordistes », qui étaient d'abord approchés par Facebook. Le matin de l'attentat, le 26 juillet 2016 à 8h30, il aurait envoyé sur ce salon un message qui disait : « Télécharger (sic) ce qui va venir et partager le en masse ! ! ! ! ».
Le quotidien ne dit rien d'un éventuel document qui aurait pu être mis en partage par la suite, ce qui ne laisse la voie qu'à des spéculations. Peut-être Kermiche avait-il prévu de filmer son acte odieux, ou des revendications, et espérait trouver des relais à sa diffusion à travers ses contacts sur Telegram.
Si cette information se confirme ce serait, à notre connaissance, la première fois qu'un lien direct est effectué entre un attentat terroriste en France et l'utilisation de messageries chiffrées.

COMMENT SURVEILLER TELEGRAM ?
La Voix du Nord ne dit pas par quel biais le message aurait été découvert. Il est possible que les enquêteurs aient trouvé ce message en accédant à l'historique Telegram du terroriste, depuis son téléphone mobile qui n'aurait pas été bloqué. Le plus probable est toutefois que l'information provienne d'un autre utilisateur du salon haqq-wad-dalil, puisque le quotidien cite le témoignage de l'un d'entre eux, qui explique que les échanges pouvaient y être « écrits ou oraux mais toujours détruits rapidement ».
Il est connu depuis de très nombreux mois que Telegram, qui dispose de plus de 100 millions d'utilisateurs à travers le monde, est aussi utilisé par des djihadistes qui recherchent la sécurité d'une messagerie chiffrée.
Après avoir refusé d'opérer la moindre censure, en tout en continuant à livrer la moindre information personnelle sur ses utilisateurs, Pavel Durov a fini par décider en novembre 2015 de fermer des salons de discussion liés à l'État islamique, pour mettre fin aux accusations de complicité passive. Il avait appelé les internautes à les signaler pour permettre leur fermeture.
Théoriquement, les canaux de discussion peuvent être infiltrés par les agents des services de renseignement. Reste qu'en l'absence de communication d'informations sur les utilisateurs, il peut être difficile de remonter jusqu'à l'auteur d'un message présentant une menace particulièrement élevée.
Article original de Guillaume Champeau

Original de l'article mis en page : Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ? — Politique — Numerama

---

Connaissez-vous le réseau plus anonyme et rapide que Tor ?

Connaissez-vous le réseau plus anonyme et rapide que Tor ?

Le Massachusetts Institute of technology (MIT), aux États-Unis, et l'École polytechnique fédérale de Lausanne (EPFL), en Suisse, annoncent la création d'un nouveau réseau anonyme sur Internet, baptisé Riffle, encore plus rapide et sécurisé que Tor, la référence en la matière.

A l'image de Tor, le plus célèbre des réseaux de ce type, Riffle permet de surfer et de communiquer en théorie en parfait anonymat en s'appuyant sur le protocole de chiffrement "en oignon". Cela signifie qu'il est composé d'une multitude de couches de routeurs, autant de "noeuds" par lesquels transitent les flux d'informations sur le réseau, garantissant ainsi l'anonymat de ses utilisateurs. Les données personnelles de l'internaute (adresse IP, pays) ne peuvent ainsi plus être localisées par les sites visités. Cette alternative serait toutefois selon ses créateurs bien plus sécurisée et fiable que Tor et consorts.
Selon le MIT, l'avantage de Riffle repose sur ses serveurs, capables de permuter l'ordre de réception des messages rendant l'analyse du trafic encore plus complexe et favorisant donc l'anonymat des utilisateurs. Si, par exemple, les messages provenant d'expéditeurs Alice, Bob et Carol atteignent le premier serveur dans l'ordre A, B, C, ils peuvent être renvoyés dans un ordre complètement différent au serveur suivant, et ainsi de suite. Les utilisateurs du réseau deviennent alors en théorie parfaitement impossibles à identifier.
Dernier point non négligeable, Riffle proposerait une meilleure bande passante, garantissant une navigation plus fluide et des échanges de fichiers accélérés.
Cette annonce intervient alors que la sécurité de Tor a récemment été mise à mal par des chercheurs de la Northeastern University de Boston (États-Unis) qui a découvert plus d'une centaine de "nœuds-espions", en réalité des serveurs, capables d'identifier des services cachés et éventuellement de les pirater.
Davantage de détails sur Riffle, toujours en phase de développement, seront communiqués lors de sa présentation officielle à la conférence Privacy Enhancing Technologies Symposium (PETS), qui se déroulera du 19 au 22 Juillet à Darmstadt (Allemagne).
Article original de Etienne Froment

Réagissez à cet article

Original de l'article mis en page : Riffle, le nouveau réseau garanti plus anonyme et rapide que Tor | geeko

Privacy Shield : 1 an de sursis donné par les CNIL européennes

Privacy Shield : 1 an de sursis donné par les CNIL européennes

Les CNIL européennes ne sont pas satisfaites du Privacy Shield, mais prennent date en 2017 pour s'inviter dans la révision de l'accord.

Le verdict était attendu. Les CNIL européennes du groupe de l'article 29 (G29) ont rendu leur décision définitive sur le Privacy Shield. Cet accord encadre le transfert des données entre les Etats-Unis et l'Union européenne Il est le successeur du Safe Harbor, invalidé par la Cour de Justice de l'Union européenne. Dans un communiqué de presse, le G29 souligne ses réserves sur le Privacy Shield. Il considère néanmoins que l'accord a été voté et il donne rendez-vous au 1 an de l'accord lors de sa révision pour un examen plus approfondi de certaines dispositions.

En avril dernier, le groupe avait émis différentes critiques sur le Privacy Shield. Il avait souligné *« un manque de clarté général »*, une *« complexité »*, et parfois une *« incohérence »*, des documents et annexes qui composent le Privacy Shield. C'est notamment le cas pour les voies de recours que pourront emprunter les citoyens européens contestant l'exploitation de leurs données outre-Atlantique, indique le groupe dans son avis consultatif.

Quant à l'accès des agences de renseignement aux données transférées dans le cadre du Privacy Shield (volet sécurité nationale), il soulève de *« fortes préoccupations »*. Le risque d'une collecte *« massive et indiscriminée »* des données par un État n'est pas écarté. Le groupe s'inquiète aussi du statut et de l'indépendance du médiateur (*« ombudsman »*) vers lequel les citoyens européens pourront se tourner.

Un an de sursis et une mise en garde

Certaines réserves ont été prises en compte, note le G29, mais « cependant un certain nombre de préoccupations demeurent ». Au premier rang desquels, le risque toujours bien réel d'une surveillance de masse par le gouvernement américain. Il évoque le rôle du médiateur et la révision annuelle de l'accord.

Les CNIL européennes comptent beaucoup sur cette révision annuelle prévue en juillet 2017. Elles profiteront de cette occasion « *pour non seulement évaluer si les questions en suspens ont été résolues, mais aussi si les garanties prévues par le Privacy Shield entre les Etats-Unis et l'UE sont réalisées et efficaces* ». Et de prévenir, que « *tous les membres de l'équipe en charge de cette révision doivent avoir accès à toutes les informations nécessaires à l'accomplissement de leur examen y compris des éléments favorisant leur propre évaluation sur la proportionnalité et la nécessité de la collecte et l'accès aux données par les pouvoirs publics* ». Une mise en garde contre les risques d'être éconduits dans un an.

Pendant ce temps-là, le Privacy Shield pourrait être contesté par des citoyens européens, comme cela a été le cas avec Max Schrems pour le Safe Harbor. Lors d'une récente discussion dans le cadre de Cloud Confidence, le jeune avocat avais émis l'hypothèse d'une nouvelle action en justice contre le Privacy Shield.

Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Privacy Shield : les CNIL européennes accordent 1 an de sursis