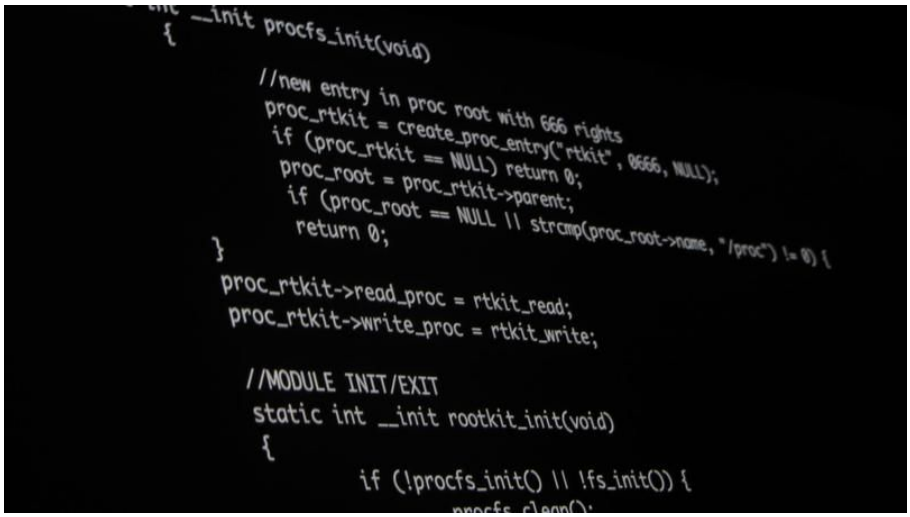
Les américains s’inquiètent de la cyber-sécurité automobile



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

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

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

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

Contactez-nous

Réagissez à cet article

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

---

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.

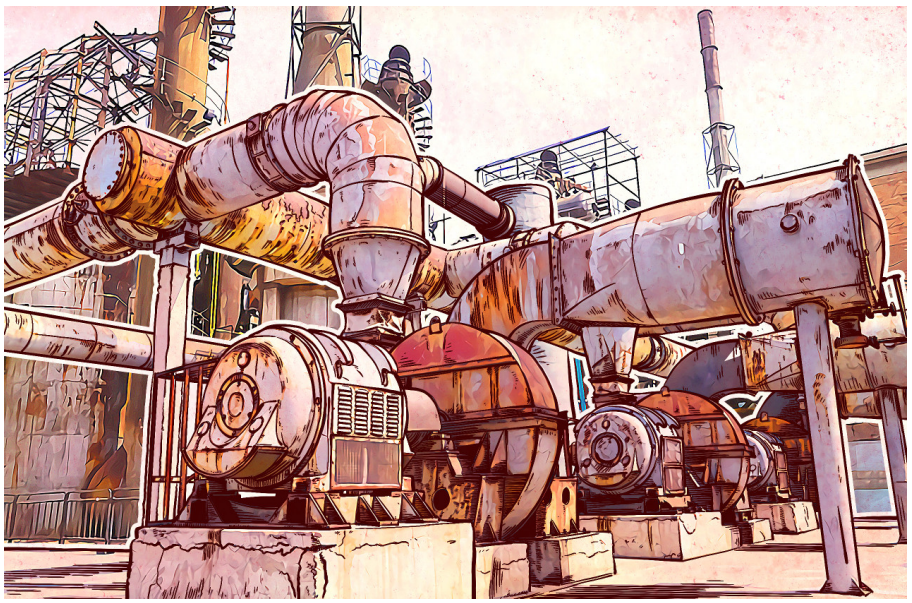
La start-up recommande aux internautes d'utiliser un clavier filaire pour se protéger.

Article original de Ariane Beky

Réagissez à cet article

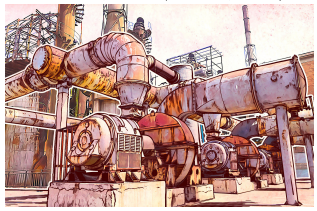
Original de l'article mis en page : Les claviers sans fil, des espions en puissance

Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie ?



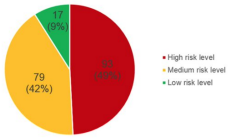
Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie ?

On ne cesse de vous le répéter, il est très important de rester au courant des dernières actualités concernant la cybersécurité et ses menaces. Mieux vaut prévenir que guérir.
Cependant, même ceux qui connaissent tout en matière de cybersécurité, qui utilisent des mots de passe fiables et qui les changent régulièrement, qui reconnaissent des messages d'hameçonnage au premier coup d'œil et qui protègent leurs dispositifs avec une excellente solution de sécurité, même ceux qui font *tout*, ne sont pas totalement à l'abri. Tout simplement parce que nous vivons en société.



Le problème est que nous avons le contrôle sur nos objets personnels, mais pas sur celui des équipements industriels, qui est loin de notre portée.

Vous avez dit cybersécurité ?
Nos experts en cybersécurité ont mené une étude afin de découvrir où nous en sommes concernant la sécurité des systèmes de contrôle industriel.
Shodan, le moteur de recherche pour les dispositifs connectés, nous a montré que 188 019 systèmes industriels dans 170 pays sont accessibles sur Internet. La majorité d'entre eux sont localisés aux Etats-Unis (30,5%) et en Europe, essentiellement en Allemagne (13,9%), Espagne (5,9%) et en France (5,6%).
View image on Twitter



ICS vulnerabilities in 2015 by risk level (CVSS v.2 and CVSS v.3)

Follow
Kaspersky Lab
✔@kaspersky
Industrial #cybersecurity threat landscape https://kas.pr/MY6j #klreport
8:29 PM – 11 Jul 2016
•
•
2020 Retweets
•
99 likes

92% (172 982) des systèmes de contrôle industriel (SCI) détectés sont vulnérables. Lamentablement, 87% ont un niveau de risque moyen de bugs et 7% connaissent des problèmes critiques.
Ces cinq dernières années, les experts ont méticuleusement examiné de tels systèmes et y ont découvert de nombreuses failles de sécurité. Durant ce laps de temps, le nombre de vulnérabilités dans les composants SCI a multiplié par dix.
Parmi les systèmes que nos experts ont analysés, 91,6% ont utilisé des protocoles non sécurisés, en donnant l'opportunité aux cybercriminels d'intercepter ou de modifier les données utilisant des attaques de l'homme du milieu.
Egalement, 7,2% (environ 13 700) des systèmes appartiennent à de grandes compagnies aéronautiques, des transports et de l'énergie, pétrolières et gazières, métallurgiques, de l'industrie alimentaire, de la construction et autres secteurs primordiaux.
View image on Twitter

Follow
Kaspersky Lab
✔@kaspersky
Maritime industry is easy meat for cyber criminals – http://ow.ly/Nio2a
12:25 AM – 23 May 2015
•
•
3232 Retweets
•
1313 likes

En d'autres termes, des hackers qualifiés peuvent influencer n'importe quel secteur économique. Leurs victimes (les entreprises piratées) porteraient préjudice à des milliers ou millions de personnes en leur fournissant de l'eau contaminée ou de la nourriture immangeable, ou en leur coupant le chauffage en plein hiver.

Qu'est-ce que cela implique pour nous tous ?
Les possibles effets et conclusions dépendent des entreprises que les cybercriminels visent, et quel SCI elles utilisent.
Nous avons connaissance de quelques exemples de piratages industriels. En décembre 2015, la moitié des maisons de la ville ukrainienne Ivano-Frankivsk s'étaient retrouvées sans électricité à cause du piratage d'un générateur électrique. La même année avait également eu lieu une attaque de l'entreprise Kemuri Water.
Comme si cela ne suffisait pas, l'**aéroport Frédéric Chopin de Varsovie** avait aussi été la cible d'une attaque. Et un an plus tôt, des hackers avaient perturbé l'opération d'un haut-fourneau dans une aciérie en Allemagne.
Follow
Kaspersky Lab
✔@kaspersky
Black Hat and DEF CON: Hacking a chemical plant –https://kas.pr/RT61
9:35 PM – 19 Aug 2015

Black Hat and DEF CON: Hacking a chemical plant
Since there's nothing unhackable in this world, why should chemical plants should be the exception?
blog.kaspersky.com
•
•
1313 Retweets
•
1010 likes

Globalement, la sécurité des systèmes de contrôle industriel laisse encore à désirer. Kaspersky Lab a émis à plusieurs reprises des mises en garde concernant ces risques, mais d'éternels insatisfaits trouvent en général la parade : informez-nous de cas *réels* où ces vulnérabilités ont*vraiment* été exploitées. Malheureusement, on peut désormais le faire.

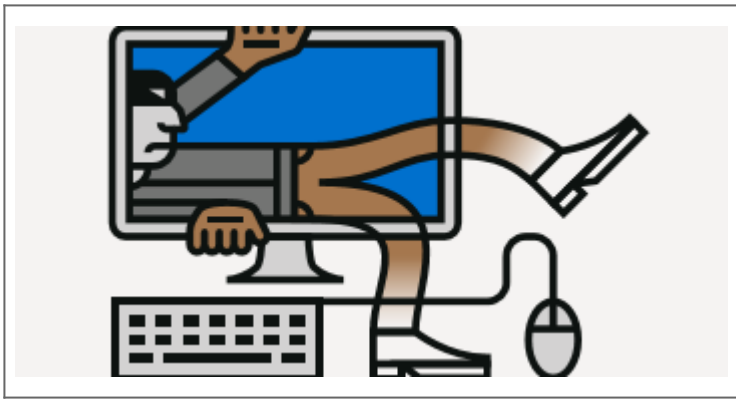
Bien évidemment, une personne seule ne peut pas faire grand-chose pour résoudre un problème systémique. Un équipement industriel ne peut pas être changé du jour au lendemain ou même en l'espace d'une année. Toutefois, et comme nous l'avons déjà dit, la défense la plus importante en matière de cybersécurité est de rester informés. Plus de personnes sont au courant du problème, et plus il y a de chances pour que les infrastructures industrielles soient à l'abri d'attaques néfastes.
Article original de John Snow

Réagissez à cet article

Original de l’article mis en page : Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

---

77 % des entreprises totalement impuissantes face à des Cyberattaques



77 % des entreprises totalement impuissantes face à des Cyberattaques

---

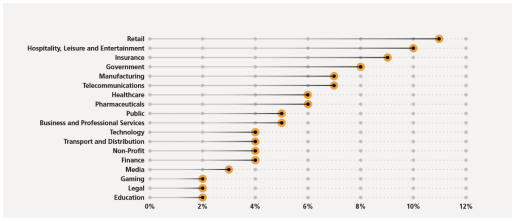
Pénurie de compétences et manque d'investissements : les entreprises sont non seulement vulnérables aux attaques, mais aussi impuissantes pour les résoudre seules. Décryptant les tendances de ces trois dernières années dans le monde, un rapport de NTT Com Security souligne le peu de progrès réalisés dans ce domaine, et note même un recul….

Le GTIR (« Global Threat Intelligence Report ») analyse une énorme masse de données issues de 24 centres d'opérations de sécurité (SOC), sept centres R&D, 3 500 milliards de logs et 6,2 milliards d'attaques. Ces résultats sont donc particulièrement intéressants pour suivre l'état des menaces dans le monde. Son édition 2016, qui décrypte les tendances de ces trois dernières années souligne le peu de progrès réalisés par les entreprises dans leur lutte contre les menaces, et note même une légère hausse du nombre d'entre elles mal préparées qui s'élève à 77 %. Face à des attaques d'envergure, elles doivent le plus souvent solliciter une intervention extérieure. Seules 23 % des organisations seraient donc en mesure de se défendre efficacement contre des incidents de sécurité majeurs.

Le retail le plus touché par les incidents

Après des années passées en tête des secteurs les plus touchés dans les précédents rapports GTIR, la finance cède sa place à la grande distribution qui enregistre 22 % des interventions sur incidents (contre 12 % l'année passée) de NTT Com Security. La grande distribution a été particulièrement exposée aux attaques de spear phishing. Parce qu'elles brassent d'importants volumes de données personnelles, dont des informations bancaires, les organisations de ce secteur constituent une cible particulièrement attractive, et ce au point d'enregistrer le plus fort taux d'attaques par client. Le secteur financier a représenté 18 % des interventions.

En 2015, le groupe NTT a également noté une augmentation des attaques à l'encontre du secteur de l'hôtellerie, des loisirs et du divertissement. Tout comme la grande distribution, ce secteur draine aussi de gros volumes d'informations personnelles, y compris des données de cartes bancaires. De même, le niveau relativement élevé des transactions dans le milieu (hôtels, stations touristiques…) suscitent la convoitise des attaquants. Avec sa palette de programmes de fidélité, l'hôtellerie est une vraie mine d'informations personnelles. Plusieurs violations de sécurité ont d'ailleurs défrayé la chronique en 2015 : Hilton, Starwood ou encore Hyatt.



Les attaques par secteur – 2015

Hausse de 17 % des menaces internes

A quels types d'incidents NTT Com Security a-t-il été confronté ? Les violations de sécurité ont représenté 28 % des interventions en 2015, contre 16 % en 2014. Un grand nombre d'incidents concernaient des vols de données et de propriété intellectuelle. Les menaces internes ont connu de leur côté une véritable envolée, passant de seulement 2 % en 2014 à 19 % en 2015. Elles résultent le plus souvent d'une utilisation abusive des données et ressources informatiques par des salariés ou prestataires externes.

En 2015, 17 % des interventions de NTT Com Security se sont produites sur des attaques par spear phishing, alors qu'elles représentaient moins de 2 % auparavant. Basées sur des tactiques sophistiquées d'ingénierie sociale, comme l'utilisation de fausses factures, ces attaques visaient principalement des dirigeants et autres personnels de la fonction comptabilité-finance.

Enfin, le GTIR 2016 a enregistré un recul des attaques DDoS par rapport aux années précédentes. Elles ont reculé de 39 % par rapport à 2014. Le rapport attribue cette baisse aux investissements réalisés dans les outils et services de défense contre ce type d'agression.

A noter cependant une augmentation des cas d'extorsion, où les victimes d'acquittent d'une rançon pour lever les menaces ou stopper une DDos en cours.

Top 10 External Vulnerabilities	
Outdated PHP Version	8%
Cross-Site Scripting (CSS/XSS)	7%
Outdated Apache Web Server	7%
SSL/TLS Information Disclosure	6%
Web Clear Text Username/Password	5%
Weak SSL/TLS Ciphers/Certificate	5%
Outdated Apache Tomcat Server	4%
Weak/No HTTPS cache policy	4%
Cookie without HTTPOnly attribute set	3%
SSL Certificate Signed using Weak Hashing Algorithm	3%

Top 10 Internal Vulnerabilities	
Outdated Java Version	51%
Outdated Adobe Flash Player	11%
Outdated Adobe Reader and Acrobat	5%
Outdated Microsoft Windows	3%
Outdated Microsoft Internet Explorer	3%
Outdated Mozilla Firefox	2%
Outdated Microsoft Office	1%
Outdated Linux Kernel	1%
Outdated Novell Client	1%
Outdated OpenSSH Version	1%

Top 10 des vulnérabilités internes et externes – 2015. Parmi l'ensemble des vulnérabilités externes identifiées, le top 10 compte pour 52 % des cas recensés. Les 48 % restants étaient composés de milliers de vulnérabilités. Parmi l'ensemble des vulnérabilités internes identifiées, le top 10 compte pour 78 % des cas recensés. Ces 10 vulnérabilités internes étaient directement liées à la présence d'applications obsolètes sur les systèmes visés.

Le rapport ici

Article original de Juliette Paoli

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

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Cyberattaques : 77 % des entreprises totalement impuissantes | Solutions Numériques

Trois histoires vrais de vies inquiétées par du piratage informatique ciblé

Trois histoires vrais de vies inquiétées par du piratage informatique ciblé

L'expérience le prouve : même les vieux habitués d'Internet n'arrivent pas toujours à se protéger des piratages ciblés. Étant donné que notre vie quotidienne devient de plus en plus connectée à Internet et à d'autres réseaux, la sécurité en ligne s'est convertie comme un besoin impératif.

La plupart d'entre nous ont un email, un compte sur les réseaux sociaux et une banque en ligne. On commande sur le web, et utilisons notre mobile pour nous connecter à Internet (par exemple, dans les solutions de l'authentification à deux facteurs) et pour d'autres choses tout aussi importantes. Malheureusement, aucun de ces systèmes n'est 100% sûr.
Plus nous interagissons en ligne et plus nous devenons les cibles de hackers sournois. Les spécialistes en sécurité appellent ce phénomène « la surface d'attaque ». Plus la surface est grande et plus l'attaque est facile à réaliser. Si vous jetez un coup d'œil à ces trois histoires qui ont eu lieu ces trois dernières années, vous comprendrez parfaitement le fonctionnement de cette attaque.

1. Comment détourner un compte : faut-il le pirater ou simplement passer un coup de fil ?

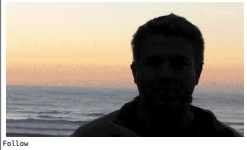
Un des outils les plus puissants utilisés par les hackers est le « piratage humain » ou l'ingénierie sociale. Le 26 février dernier, le rédacteur en chef de Fusion Kevin Roose, a voulu vérifier s'il était aussi puissant qu'il n'y paraissait. Jessica Clark, ingénieure sociale spécialisée en piratage informatique et l'expert en sécurité Dan Tentler ont tout deux accepté ce défi.
Jessica avait parié qu'elle pouvait pirater la boîte mail de Kévin rien qu'avec un email, et sans grande difficulté elle y est arrivé. Tout d'abord, l'équipe de Jessica a dressé un profil de 13 pages qui définissait quel genre d'homme il était, ses goûts, etc, provenant de données collectées de diverses sources publiques.
Après avoir préparé le terrain, Jessica a piraté le numéro mobile de Kévin et appelé sa compagnie de téléphone. Pour rendre la situation encore plus réelle, elle ajouta un fond sonore d'un bébé en train de pleurer.
Jessica se présenta comme étant la femme de Roose. L'excuse inventée par cette dernière fut qu'elle et son « mari » devaient faire un prêt, mais qu'elle avait oublié l'email qu'ils utilisaient en commun, en se faisant passer pour une mère de famille désespérée et fragile. Accompagnée des cris du bébé, Jessica ne mit pas longtemps à convaincre le service technique de réinitialiser le mot de passe du mail et ainsi d'y avoir pleinement accès.
Dan Tentler a accompli cette tâche avec l'aide de l'hameçonnage. Tout d'abord, il avait remarqué que Kevin possédait un blog sur Squarespace et lui envoya un faux email officiel depuis la plateforme, dans lequel les administrateurs de Squarespace demandaient aux utilisateurs de mettre à jour le certificat SSL (Secure Sockets Layer) pour des questions de « sécurité », permettant ainsi à Tentler d'accéder à l'ordinateur de Kévin. Dan créa de nombreux faux pop-up demandant à Roose des informations bien spécifiques et le tour était joué.
Tentler réussit à obtenir l'accès à ses données bancaires, son email, ses identifiants sur les sites web, ainsi que ses données de cartes de crédit, son numéro de sécurité sociale. De l'écran de son ordinateur, il capturait des photos toutes les deux minutes et ce pendant 48h.
View image on Twitter

Follow

Kaspersky Lab
@kaspersky
What is phishing and why should you care? Find outhttps://kas.pr/6bpe #iteducation #itsec
8:05 PM – 11 Dec 2015
•
•
1717 Retweets
•
77 likes

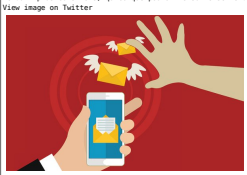
2. Comment détourner de l'argent à un ingénieur informatique en moins d'une nuit

Au printemps 2015, le développeur de logiciels Partap Davis a perdu 3000$. Durant une nuit, en seulement quelques heures, un hacker inconnu a obtenu l'accès de ses comptes mail, son numéro de téléphone et son Twitter. Le coupable a contourné habilement le système de l'authentification à deux facteurs et littéralement vidé le portefeuille des bitcoins de Partap. Comme vous devez sans doute l'imaginer, Davis a passé une mauvaise journée le lendemain.
Il est important de noter que Partap est une pointure concernant l'usage d'Internet : il choisit toujours des mots de passe fiables et ne clique jamais sur des liens malveillants. Son email est protégé avec le système d'authentification à deux facteurs de Google, ce qui veut dire que lorsqu'il se connecte depuis un nouvel ordinateur, il doit taper les six numéros envoyés sur son mobile.



Follow

The Verge
@verge
Anatomy of a hack: a step-by-step account of an overnight digital heist http://www.theverge.com/a/anatomy-of-a-hack …
4:02 PM – 4 Mar 2015
•
•
6969 Retweets
•
7171 likes
Davis gardait ses économies sur trois portefeuilles Bitcoin, protégés par un autre service d'authentification à deux facteurs, conçu par l'application mobile Authy. Même si Davis utilisait toutes ces mesures de sécurité prévoyantes, ça ne l'a pas empêché de se faire pirater.
Suite à cet incident, Davis était très en colère et a passé plusieurs semaines à la recherche du coupable. Il a également contacté et mobilisé des journalistes de The Verge pour l'enquête. Tous ensemble, ils sont parvenus à trouver comment le piratage avait été exécuté. Davis utilisait comme mail principal l'adresse suivante : Patrap@mail. Tous les mails furent envoyés à une adresse Gmail plus difficile à mémoriser (étant donné que Patrap@gmail était déjà utilisé).
Pendant plusieurs mois, quiconque pouvait ensuite se rendre sur la page Hackforum et acheter un script spécial afin d'obtenir les mots de passe qui se trouvaient dans la boite mail. Apparemment, le script était utilisé pour contourner l'authentification à deux facteurs et changer le mot de passe de Davis.
View image on Twitter



Follow

Kaspersky Lab
@kaspersky
Unfortunately two-factor authentication can't save you from#banking Trojans https://kas.pr/S4jV #mobile
4:40 PM – 11 Mar 2016
•
•
2828 Retweets
•
1515 likes
Ensuite, l'hacker a fait une demande de nouveau mot de passe depuis le compte de Davis et demandé au service client de transférer les appels entrants à un numéro de Long Beach (ville en Californie). Une fois le mail de confirmation reçu, le service technique a donné le contrôle des appels à l'hacker. Avec une telle technique, il n'était pas bien difficile de contourner l'authentification à deux facteurs de Google et avoir accès au compte Gmail de Davis.
Pour surmonter cet obstacle, l'hacker a tout simplement réinitialisé l'application sur son téléphone en utilisant une adresse mail.com et une nouvelle confirmation de code, envoyée de nouveau via un appel vocal. Une fois que l'hacker mit la main sur toutes les mesures de sécurité, il changea les mots de passe des portefeuilles Bitcoin de Davis, en utilisant Authy et l'adresse email .com afin de lui détourner de l'argent.
L'argent des deux autres comptes est resté intact, l'un des services interdisant le retrait des fonds 48h après le changement du mot de passe, et l'autre demandant une copie du permis de conduire de Davis, que l'hacker n'avait pas en sa possession.

3. La menace rôde sur nos vies

Comme l'a écrit le journal Fusion en octobre 2015, la vie de la famille Straters s'est retrouvée anéantie à cause d'une pizza. Il y a plusieurs années, des cafés et restaurants locaux se sont installés sur leur arrière-cour, les envahissant de pizzas, tartes et toute sorte de nourriture.
Peu de temps après, des camions de remorquage ont déboulé munis de grandes quantités de sable et de gravier, tout un chantier s'était installé sans aucune autorisation au préalable. Malheureusement, il ne s'agissait que de la partie visible de l'iceberg comparé au cauchemar des trois années suivantes.
Follow

Techmeme @Techmeme
How the Strater family endured 3 years of online harassment, hacked accounts, and swatting http://fusion.net/story/212802/haunted-by-hackers-a-suburban-familys-digital-ghost-story/ …http://www.techmeme.com/151025/p4##a151025p4 …
6:36 PM – 25 Oct 2015

Haunted by hackers: A suburban family's digital ghost story
A suburban Illinois family has had their lives ruined by hackers.
fusion.net
•
•
88 Retweets
•
66 likes
Paul Strater, ingénieur du son pour une chaine de télé locale et sa femme, Amy Strater, ancienne directrice générale d'un hôpital, ont été tout deux victimes d'un hacker inconnu ou de tout un groupe. Il s'avérait que leur fils Blair était en contact avec un groupe de cybercriminels. Les autorités ont reçu des menaces de bombe signées du nom du couple. Les hackers ont utilisé le compte d'Amy pour publier une attaque planifiée dans une école primaire, dans lequel figurait ce commentaire « Je tirerai sur votre école ». La police faisait des visites régulières à leur domicile, n'améliorant en rien les relations du couple avec leur voisinage, qui à force se demandait ce qu'il se passait.
Les hackers ont même réussi à pirater le compte officiel de Tesla Motors et posté un message qui encourageait les fans de la page à appeler les Strater, en échange de gagner une voiture Tesla. Les Strater « croulaient sous les appels téléphoniques », environ cinq par minute, provenant des « admirateurs » de Tesla, désireux de gagner la voiture. Un jour, un homme s'est même présenté au domicile des Strater en demandant aux propriétaires d'ouvrir leur garage, prétendant qu'ils cachaient la Tesla à l'intérieur.
Follow

r00t @rootworx
Again, There is no free car, I did not hack Elon Musk or Tesla's Twitter account. A Finnish child is having fun at your (and my) expense.
12:51 AM – 26 Apr 2015
•
•
1414 Retweets
•
1818 likes
Paul tenta de démanteler le groupe d'hackers en changeant tous les mots de passe de ses comptes et en donnant l'ordre aux patrons des restaurants locaux de ne rien dévoiler sur leur adresse. Il contacta également le Département de Police d'Oswego en leur demandant de vérifier à l'avance si une urgence était bien réelle, avant d'envoyer des renforts. En conséquence de tous ces problèmes, Paul et Amy finirent par divorcer.
Les attaques ont continué par la suite. Les réseaux sociaux d'Amy ont été piratés et utilisés pour publier toute une série de revendications racistes, ce qui a causé la perte de son emploi. Elle fut licenciée malgré avoir dit à ses supérieurs qu'elle et sa famille étaient les victimes de hackers et que leur vie s'était transformée en un véritable cauchemar.
Amy réussit à temps à reprendre le contrôle de son LinkedIn et à supprimer son compte Twitter. Malheureusement, elle était incapable de retrouver un travail dans sa branche à cause de ce qui s'était passé. Elle fut contrainte de travailler chez Uber pour arrondir ses fins de mois, mais disposait de ressources insuffisantes pour payer son loyer.
« Avant, lorsqu'on tapait son nom sur Google, on pouvait voir ses nombreux articles scientifiques et son travail admirable » a déclaré son fils Blair au journal Fusion. « Désormais, on ne voit plus que des hackers, hackers, hackers ».
De nombreuses personnes ont critiqué Blair Strater pour avoir été impliqué lui-même dans de nombreux réseaux de cybercriminels, où il n'arrivait pas à se faire d'amis. Dans le cas précis de la famille Strater, les parents de Blair ont payé pour les « crimes » de leur fils, alors qu'eux n'avaient absolument rien à voir avec les hackers.
Article original de Kate Kochetkova

Denis JACOPINI ne peut que vous recommander d'être prudent.
Si vous désirez être sensibilisé aux risques d'arnaques et de piratages afin d'en être protégés, n'hésitez pas à nous contacter, nous pouvons animer conférences, formations auprès des équipes dirigeantes et opérationnelles.
La sécurité informatique et la sécurité de vos données est plus devenu une affaire de Qualité (QSE) plutôt qu'un problème traité par des informaticiens.
Vous souhaitez être aidé ? Contactez-nous

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

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

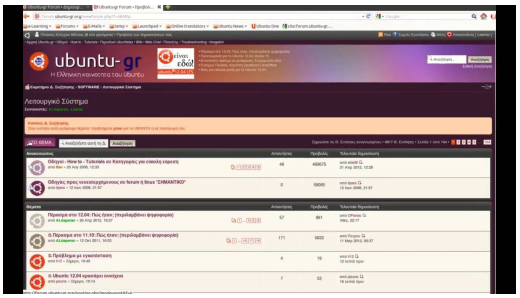
Le Net Expert INFORMATIQUE
Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Comment pirater, détourner de l’argent et rendre la vie de quelqu’un impossible sur Internet : trois histoires inquiétantes de piratages ciblés. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Deux millions de données d’utilisateurs Ubuntu dérobées



Deux millions de données d’utilisateurs Ubuntu dérobées

Le forum de la distribution Ubuntu a été victime d'une grave attaque informatique. Deux millions d'utilisateurs se sont fait voler leurs données.

Le butin du pirate est plus qu'impressionnant. Noms, mots de passe, adresse mails et IP, les données de deux millions d'utilisateurs du forum d'Ubuntu se sont envolées. La nouvelle a été annoncée jeudi dans un communiqué par Canonical l'éditeur d'Ubuntu. *« A 20h33 UTC le 14 Juillet 2016, Canonical et l'équipe ont été informés par un membre du Conseil Ubuntu que quelqu'un prétendait avoir une copie de la base de données des forums. Après enquête initiale, nous avons été en mesure de confirmer qu'il y avait bien eu une exposition des données et nous avons fermé les forums par mesure de précaution. »*

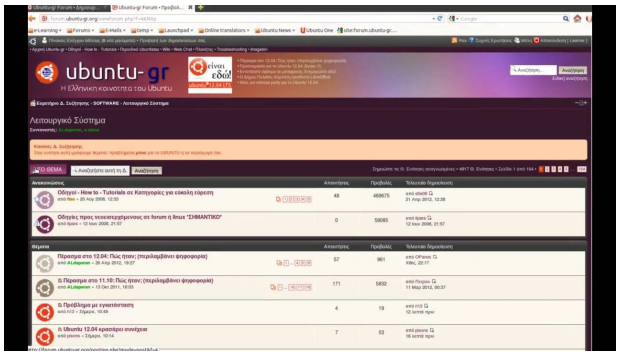
Une attaque par injection SQL

Une enquête plus poussée a révélé que la méthode employée est une injection SQL. Le pirate a pu injecter des requêtes SQL formatées dans la base de données des forums pour ensuite télécharger les datas.

Cependant, le communiqué précise que le hacker n'a pas pu accéder aux mots de passe utilisateur valides ni au référentiel de code Ubuntu ou au mécanisme de mise à jour. Moins certain, le rapport précise que normalement les services Canonical ou Ubuntu en sortent indemnes, comme certains forums.

Tout est plus ou moins rentré dans l'ordre

Des mesures correctives ont été prises et les forums restaurés. Les mots de passe du système et de la base de données ont été réinitialisés et ModSecurity, une Web Application Firewall vient renforcer le dispositif de sécurité. Selon Canonical, ça va mieux, même si après ce genre de vol il est légitime de penser que le mal est fait.



Article original de Victor Miget

Réagissez à cet article

Original de l'article mis en page : Ubuntu : les données de

deux millions d’utilisateurs dérobées

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Locky, TeslaCrypt, Cryptolocker, Cryptowall… Depuis plusieurs mois, les rançongiciels (« ransomware »), ces virus informatiques qui rendent illisibles les données d'un utilisateur puis lui réclament une somme d'argent afin de les déverrouiller, sont une préoccupation croissante des autorités. Le commissaire François-Xavier Masson, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, une unité de la police spécialisée dans la criminalité informatique, explique au Monde les dangers de cette menace.

Combien y a-t-il d'attaques par rançongiciel en France ?
On ne le sait pas avec précision, nous n'avons pas fait d'étude précise à ce sujet. Statistiquement, le rançongiciel ne correspond pas à une infraction pénale précise et il recoupe parfois l'intrusion dans un système automatisé de traitement de données. Il faudrait affiner le cadre car nous avons besoin de connaître l'état de la menace.
Avez-vous quand même une idée de l'évolution du phénomène ?
L'extorsion numérique est clairement à la hausse, c'est la grande tendance en termes de cybercriminalité depuis 2013. Tout le monde est ciblé : les particuliers, les entreprises, même l'Etat. Les attaques gagnent en sophistication et en intensité. Il y a aussi une industrialisation et une professionnalisation. La criminalité informatique est une criminalité de masse : d'un simple clic on peut atteindre des millions de machines. Désormais, il n'y a plus besoin de vous mettre un couteau sous la gorge ou de kidnapper vos enfants, on s'en prend à vos données.
Les victimes ont-elles le réflexe de porter plainte ?
Certaines victimes paient sans porter plainte. Ce calcul est fait par les entreprises qui estiment que c'est plus pratique de payer la rançon – dont le montant n'est pas toujours très élevé, de l'ordre de quelques bitcoins ou dizaines de bitcoins – et qu'en portant plainte, elles terniront leur image et ne récupéreront pas nécessairement leurs données. Elles pensent aussi que payer la rançon coûtera moins cher que de payer une entreprise pour nettoyer leurs réseaux informatiques et installer des protections plus solides. C'est une vision de court terme. Nous recommandons de ne pas payer la rançon afin de ne pas alimenter le système. Si l'on arrête de payer les rançons, les criminels y réfléchiront à deux fois. C'est la même doctrine qu'en matière de criminalité organisée.
Qu'est-ce qui pousse à porter plainte ?
Chaque cas est unique mais généralement, c'est parce que c'est la politique de l'entreprise ou parce que le montant de la rançon est trop élevé.
Qui sont les victimes ?
Il s'agit beaucoup de petites et moyennes entreprises, par exemple des cabinets de notaires, d'avocats, d'architectes, qui ont des failles dans leur système informatique, qui n'ont pas fait les investissements nécessaires ou ne connaissent pas forcément le sujet. Les cybercriminels vont toujours profiter des systèmes informatiques vulnérables.
Quel est votre rôle dans la lutte contre les rançongiciels ?
La première mission, c'est bien sûr l'enquête. Mais nous avons aussi un rôle de prévention : on dit que la sécurité a un coût mais celui-ci est toujours inférieur à celui d'une réparation après un piratage. Enfin, de plus en plus, nous offrons des solutions de remédiation : nous proposons des synergies avec des entreprises privées, des éditeurs antivirus. On développe des partenariats avec ceux qui sont capables de développer des solutions. Si on peut désinfecter les machines nous-mêmes, on le propose, mais une fois que c'est chiffré, cela devient très compliqué : je n'ai pas d'exemple de rançongiciel qu'on ait réussi à déverrouiller.
Quel rapport entretenez-vous avec les entreprises ?
On ne peut pas faire l'économie de partenariats avec le secteur privé. Nous pourrions développer nos propres logiciels mais ce serait trop long et coûteux. Il y a des entreprises qui ont des compétences et la volonté d'aider les services de police.
Parvenez-vous, dans vos enquêtes, à identifier les responsables ?
On se heurte très rapidement à la difficulté de remonter vers l'origine de l'attaque. Les rançongiciels sont développés par des gens dont c'est le métier, et leur activité dépasse les frontières. On a des idées pour les attaques les plus abouties, ça vient plutôt des pays de l'Est. Mais pas tous.
Parvenez-vous à collaborer avec vos homologues à l'étranger ?
Oui, c'est tout l'intérêt d'être un office central, nous sommes le point de contact avec nos confrères internationaux. Il y a beaucoup de réunions thématiques, sous l'égide de l'Office européen de police (Europol), des pays qui mettent en commun leurs éléments et décrivent l'état d'avancement de leurs enquêtes. C'est indispensable de mettre en commun, de combiner, d'échanger des informations. Il peut y avoir des équipes d'enquête communes, même si ça ne nous est pas encore arrivé sur le rançongiciel.
De plus en plus d'enquêteurs se penchent sur le bitcoin – dont l'historique des transactions est public – comme outil d'enquête. Est-ce aussi le cas chez vous ?
C'est une chose sur laquelle on travaille et qui nous intéresse beaucoup. S'il y a paiement en bitcoin, il peut y avoir la possibilité de remonter jusqu'aux auteurs. C'est aussi pour cela que l'on demande aux gens de porter plainte même lorsqu'ils ont payé.
Article original de Martin Untersinger

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

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

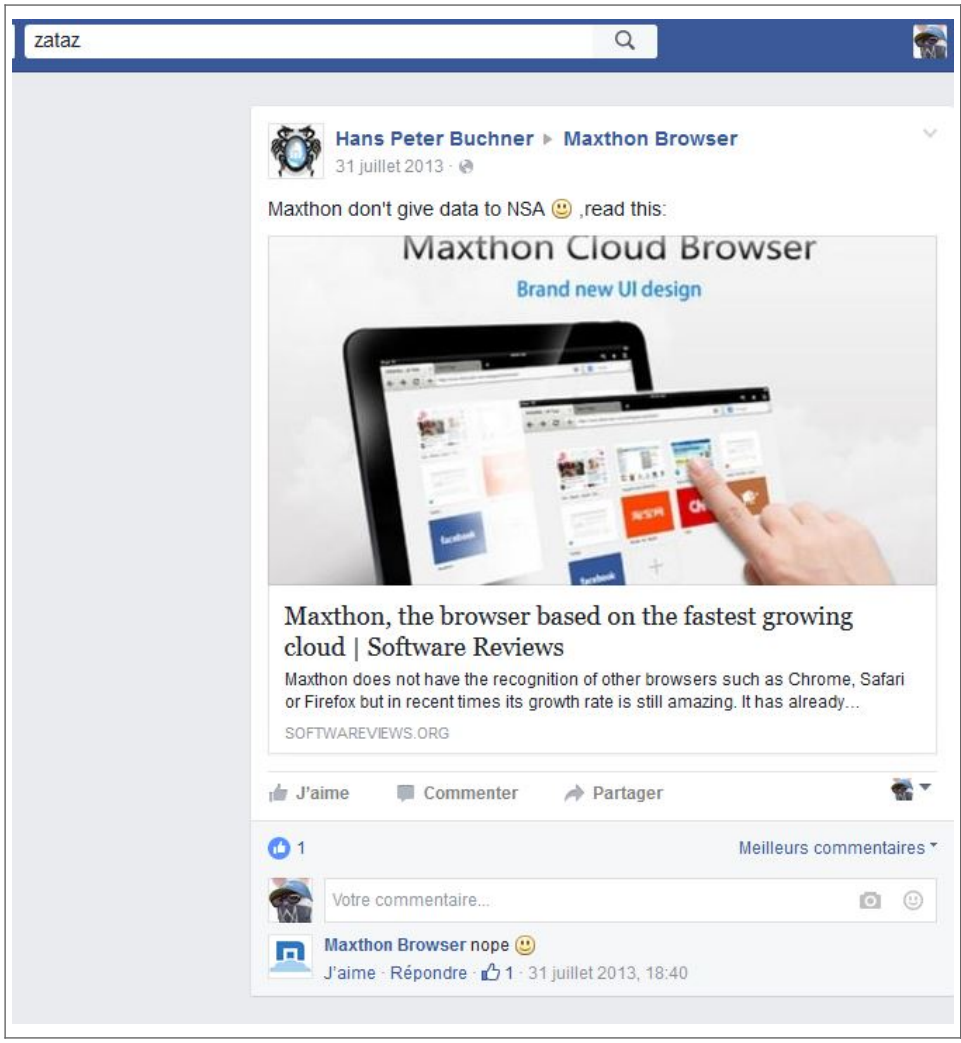
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

Attention, le navigateur Maxhton espionne ses utilisateurs !



Attention, le navigateur Maxhton espionne ses utilisateurs !

Le navigateur Maxhton ne serait rien d'autre qu'un outil d'espionnage à la solde de la Chine ?

Des experts en sécurité informatiques de l'entreprise polonaise Exatel viennent de révéler la découverte de faits troublant visant le navigateur *Maxhton*. Ce butineur web recueille des informations sensibles appartenant à ses utilisateurs. Des informations qui sont ensuite envoyées à un serveur basé en Chine. Les chercheurs avertissent que les données récoltées pourraient être très précieuses pour des malveillants.

Les données des utilisateurs de Maxhton envoyées en Chine !
Et pour cause ! Les ingénieurs de *Fidelis Cybersecurity* et *Exatel* ont découvert que Maxthon communiquait régulièrement un fichier nommé ueipdata.zip. Le dossier compressé est envoyé en Chine, sur un serveur basé à Beijing, via HTTP. Une analyse plus poussée a révélé que ueipdata.zip contient un fichier crypté nommé dat.txt. Dat.txt stocke des données sur le système d'exploitation, le CPU, le statut ad blocker, l'URL utilisé dans la page d'accueil, les sites web visités par l'utilisateur (y compris les recherches en ligne), et les applications installées et leur numéro de version.
En 2013, après la révélation du cyber espionnage de masse de la NSA, Maxhton se vantait de mettre l'accent sur la vie privée, la sécurité, et l'utilisation d'un cryptage fort pour protéger ses utilisateurs. (Merci à I.Poireau)
Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Le navigateur Maxhton espionne ses utilisateurs – ZATAZ

Un concessionnaire Lamborghini de Mulhouse piraté

Un concessionnaire Lamborghini de Mulhouse piraté

Le vol de données peut souvent cacher des arnaques et attaques informatiques plus vicieuses encore. Exemple avec le piratage d'un concessionnaire de Lamborghini de l'Est de la France.

Derrière un piratage informatique, 99 fois sur 100, se cache le vol des données que le malveillant à pu rencontrer dans son infiltration. Des données qui se retrouvent, dans l'heure, quand ce n'est pas dans les minutes qui suivent la pénétration du site dans des forums et autres boutiques dédiés à l'achat et revente d'informations subtilisées.Un concessionnaire de Lamborghini, à Mulhouse, vient d'en faire les frais.

Une fois les contenus dérobés exploités (phishing, escroqueries…) le pirate s'en débarrasse en les diffusant sur la toile. C'est ce qui vient d'arriver à un concessionnaire automobile de l'Est de la France. Ici, nous ne parlons pas de la voiture de monsieur et madame tout le monde, mais de Lamborghini.

Prend son site web par dessus la jambe et finir piraté !

Le concessionnaire se retrouve avec l'ensemble des pousses bouton de la planète aux fesses. De petits pirates en mal de reconnaissance qui profitent d'une idiote injection SQL aussi grosse que l'ego surdimensionné de ces « piratins ». Bilan, le premier pirate a vidé le site, revendu/exploité les données. Il a ensuite tout balancé sur la toile. Les « suiveurs » se sont jetés sur la faille et les données. J'ai pu constater des identifiants de connexion (logins, mots de passe) ou encore des adresses électroniques lâchées en pâture. Des courriels internes (webmaster, responsables du site…).

Article original de Damien Bancal

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

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : ZATAZ Un concessionnaire Lamborghini de Mulhouse piraté – ZATAZ

Eleanor, nouvelle menace sur la planète Mac

Eleanor, nouvelle menace sur la planète Mac

Alors que beaucoup d'utilisateurs de Mac se montrent parfois négligents en matière de sécurité, les équipes de BitDefender ont détecté un nouveau backdoor baptisé Eleanor qui ciblent les Mac et qui peut causer d'importants dégâts sur les machines. En effet, il offre la possibilité aux pirates de prendre le contrôle d'une machine à distance.

Le backdoor Eleanor à l'assaut des Mac

Comme souvent, c'est l'éditeur BitDefender qui a identifié la nouvelle menace qui pèse sur les Mac. Eh oui, même si les dangers sont généralement moindres sur Mac que sur PC, voilà que ceux qui ont choisi les ordinateurs d'Apple doivent se montrer vigilants.

En effet, dès lors que ce backdoor silencieux est parvenu à infecter une machine, il a la capacité de permettre à un attaquant de prendre le contrôle du Mac à distance. Ainsi, les hackers peuvent s'en servir pour voler des données présentes sur la machine piratée, télécharger des applis frauduleuses ou même pour détourner la webcam, une pratique de plus en plus courante.

Reste que l'infection du Mac ne se produit pas toute seule et qu'elle est l'une des conséquences du téléchargement de l'application malveillante Easy Doc Converter. En effet, lors du démarrage d'OS X, cette appli va installer sur le Mac trois composantes : un service Tor, un service web capable de faire tourner PHP et un logiciel dédié. Autrement dit le matériel indispensable pour que s'installe, sur Mac, un backdoor silencieux comme Eleanor.

L'intégralité des Mac concernée par Eleanor ?

Si BitDefender a tenu à alerter sur sa découverte, il semblerait tout de même que tous les Mac ne soient pas tous concernés par cette menace.

En effet, parce que le logiciel Easy Doc Converter n'est pas signé numériquement avec un certificat approuvé par Apple, les risques d'infection sont réduits. D'ailleurs, la marque à la pomme a tenu à le préciser en rappelant que tous les Mac dotés de la protection Gatekeeper n'avaient rien à craindre.

Article original de Jérôme DAJOUX

Réagissez à cet article

Original de l’article mis en page : Eleanor, nouvelle menace sur la planète Mac