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

LastPass affecté par une faille critique d’accès à distance

	LastPass affecté par une faille critique d’accès à distance

Le chercheur en sécurité Tavis Ormandy a repéré une faille critique dans LastPass qui permettrait d'établir un accès à distance dans le gestionnaire de mots de passe. Un signalement à LastPass a été effectué, qui prépare un correctif.

Les gestionnaires de mots de passe peuvent se montrer d'une grande aide pour celui qui tient à conserver en un seul endroit une multitude de codes d'accès. Surtout, ils satisfont d'un coup plusieurs exigences en matière de sécurité informatique qui sont parfois contradictoires ou inapplicables au-delà d'un certain seuil.
Regardons un instant ce que l'on demande en règle générale à l'usager : l'utilisation d'un mot de passe unique par service, tout en respectant un strict formalisme qui va de la longueur du mot de passe (x caractères au minimum) à sa complexité (des lettres, des chiffres, des symboles, des majuscules et des minuscules, en mélangeant le tout), en passant par son renouvellement (sait-on jamais).

Bien entendu, il est évidemment tout à fait déconseillé de les noter simplement sur un bout de papier (on n'est jamais trahi que par les siens) ou de les enregistrer dans un fichier sur le PC (qui peut se faire pirater). Or, la seule mémorisation n'est pas une solution d'avenir : au-delà de quelques services, l'utilisateur s'y perdrait. D'où l'intérêt de passer par des gestionnaires de mots de passe.

Mais leur utilité ne doit pas faire oublier le fait que ces programmes sont par essence imparfaits.
Malgré tout le soin qui peut être apporté pendant leur conception, ces logiciels (les plus connus sont Dashlane, 1Password, KeePass et LastPass) peuvent être sensibles à certaines attaques. On l'a vu par exemple avec LastPass, qui est annoncé comme vulnérable au hameçonnage et qui a essuyé une intrusion dans son infrastructure, a priori sans dommage pour les mots de passe eux-mêmes.
Dans ce contexte, des initiatives comme celle lancée par la Commission européenne, qui consiste à organiser un audit du code source de KeePass – qui est un logiciel libre, ce qui facilite grandement les choses – sont à accueillir avec bienveillance. Elles contribuent à un rehaussement général du niveau de fiabilité de ce type de logiciel, à défaut de le rendre invulnérable, ce qui est illusoire.
La contribution d'un chercheur comme Tavis Ormandy est aussi précieuse, même si de prime abord elle provoque légitimement une inquiétude sur le degré de finition de certains logiciels. En effet, l'intéressé indique avoir déniché dès le premier coup d'œil une série de problèmes critiques qui lui ont sauté aux yeux. Il a ajouté avoir fait suivre un rapport complet à LastPass pour qu'il les règle.
La nature des vulnérabilités repérées n'est pas précisée par Tavis Ormandy. Le blog Naked Security, édité par l'éditeur d'antivirus Sophos, écarte pour le moment la piste de la faille 0-Day. Une telle vulnérabilité désigne les brèches n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu. Elles sont les plus dangereuses, car elles sont secrètes et peuvent être exploitées en toute discrétion.
Tout juste sait-on que la vulnérabilité en question permettrait un accès complet à distance. L'on peut imaginer que des détails supplémentaires seront donnés ultérieurement, lorsque LastPass aura fini son intervention. Dans un autre tweet, Tavis Ormandy ajoute qu'il va se pencher dans la foulée sur 1Password et regarder s'il peut repérer des fragilités dans ce gestionnaire.
Dans le cadre d'une divulgation responsable, les spécialistes en sécurité informatique sont en effet invités à signaler d'abord aux sociétés les failles qu'ils repèrent dans les logiciels qu'elles éditent, et cela en toute discrétion. Ce n'est qu'ensuite qu'une diffusion publique peut avoir lieu, une fois les correctifs appliqués, de façon à ce que des personnes mal intentionnées ne puissent pas en profiter.
Tavis Ormandy est une pointure dans le domaine de la sécurité informatique.
Il s'est illustré à diverses reprises en signalant des brèches critiques dans un certain nombre de logiciels, comme Linux, Windows, la plateforme de jeux Uplay conçue par Ubisoft ou encore le shell Bash. Il a aussi épinglé les éditeurs d'antivirus Sophos et Trend Micro. Il travaille depuis quelques années dans l'équipe Project Zero mise sur pied par Google pour traquer les failles 0-Day, qui regroupe quelques personnalités. À tel point qu'elle est présentée comme une dream team.
Article original de Julien Lausson

Réagissez à cet article

Original de l’article mis en page : LastPass affecté par une faille critique d’accès à distance – Tech – Numerama

---

Attention, des antivirus auraient des trous de sécurité !

Attention, des antivirus auraient des trous de sécurité !

Des chercheurs israéliens ont découvert une vulnérabilité dans plusieurs antivirus. D'autres failles seront présentées à la Black Hat.
Où l'on reparle de ces produits antivirus qui abritent des failles permettant de contourner les mécanismes de défense de Windows… En septembre 2015, l'expert en sécurité informatique Tavis Ormandy, qui travaille au sein de l'équipe Google Project Zero, avait publié une étude à ce sujet.
Deux de ses confrères – en l'occurrence, Tomer Bitton et Udi Yavo, de la start-up israélienne enSilo, spécialisée dans la détection des attaques en temps réel – avaient approfondi la problématique.
Dans leur rapport, ils pointaient du doigt trois éditeurs (AVG, Kaspersky, McAfee), tout en suggérant que d'autres logiciels étaient probablement concernés par la vulnérabilité qu'ils avaient découverte.
La vulnérabilité en question permet, sans nécessiter de privilèges de niveau administrateur, d'exécuter du code malveillant en déjouant des technologies de type ASLR (distribution aléatoire de l'espace d'adressage) ou DEP (prévention de l'exécution des données).
Pour faire la jonction avec chacun des processus associés à une application (par exemple, plusieurs onglets dans un navigateur Web), l'antivirus leur alloue une zone mémoire avec des permissions en lecture, écriture et exécution (RWX).
Problème : dans de nombreux cas, cette zone est toujours à la même adresse. Un tiers parvenu à prendre le contrôle d'un programme et de son pointeur d'instructions peut donc facilement copier son code malveillant dans ladite zone… et l'exécuter.

Detours de Microsoft sur la sellette

La conférence Black Hat USA 2016, qui aura lieu du 30 juillet au 4 août à Las Vegas, sera, pour Tomer Bitton et Udi Yavo, l'occasion de faire le point sur l'avancée de leurs travaux.
À première vue, il y a des choses à dire : une demi-douzaine de failles ont été dénichées dans plus d'une quinzaine de produits. Mais ce sont potentiellement des milliers de logiciels qui sont affectés. Tout du moins tous ceux qui s'appuient sur la bibliothèque Microsoft Detours, destinée notamment à intercepter des fonctions d'applications et de processus, puis à en réécrire le code pour des fonctions cibles.
Les principaux antivirus exploitent cette technique dite de « hooking » pour détecter des comportements malveillants, entre autres au niveau des fonctions d'allocation de la mémoire (VirtualAlloc, VirtualProtect…). L'essentiel des programmes « intrusifs », comme ceux qui analysent les performances du système, en font aussi usage, dixit ITespresso.
Malheureusement, l'implantation des mécanismes d'injection de code depuis le noyau n'est pas toujours bien effectuée – que ce soit par import de tables, fonctions asynchrones ou modification du point d'entrée de la fonction cible.
enSilo a mis à disposition un outil baptisé AVulnerabilityChecker pour permettre à chacun de vérifier s'il existe, sur son système Windows, une application potentiellement vulnérable… et plus particulièrement un antivirus.
Article original de Silicon

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 : Des trous de sécurité dans les antivirus

---

Vous utilisez des objets connectés? Gare à vos données

Vous utilisez des objets connectés? Gare à vos données

Une étude publiée par l'entreprise de cybersécurité AV-Test montre que la plupart des objets connectés testés, destinés à surveiller sa forme, sont susceptibles d'être piratés.

Ils mesurent toutes les performances. Seulement voilà: d'après une étude publiée par l'entreprise de cybersécurité AV-Test le 18 juillet 2016, les objets connectés utilisés pour surveiller sa forme ne sont pas sécurisés. Pire encore, ils présentent des failles de sécurité pouvant permettre à des pirates informatiques d'accéder à leurs données et de les manipuler.

Des appareils utilisés par les assureurs

Pour en arriver à cette conclusion, AV-Test a examiné sept appareils utilisant Android, le système d'exploitation mobile de Google, et repéré des vulnérabilités similaires à celles qu'elle avait déjà identifiées il y a un an. Beaucoup d'appareils manquent de connexions sécurisées ou de protection contre les accès non autorisés. Les fabricants « ne font souvent pas assez attention à l'aspect de la sécurité », indique l'étude.

Elle fait pourtant valoir qu'il faudrait prendre davantage au sérieux la sécurité de ces appareils dont l'usage s'élargit, certaines assureurs santé commençant même à les utiliser pour fixer leurs tarifs ou proposer des remises.

Trois appareils avec des risques de piratages importants

Dans le détail, les appareils affichent des niveaux de sécurité variés. Selon l'étude, le risque le plus élevé est présenté par les appareils de Runtastic, Striiv et Xiaomi, où AV-Test relève 7 à 8 vulnérabilités potentielles sur un total de dix. AV-Test indique notamment que « ces appareils peuvent être suivis à la trace plutôt facilement » et qu'ils utilisent des systèmes d'identification et de protection contre les accès non autorisés incohérents ou inexistants, ou encore que leur programme n'est pas assez protégé pour garantir la sécurité des données collectées.

« Pire que tout, Xiaomi stocke toutes les données de manière non cryptée sur le smartphone », s'inquiète l'étude. Les appareils les plus sûrs, avec 2 à 3 risques potentiels pour la sécurité, sont la montre Pebble Time, le bracelet Band 2 de Microsoft et le moniteur d'activité et de sommeil Basis Peak.

L'Apple Watch tire son épingle du jeu

La montre connectée Apple Watch, évaluée selon des critères différents car elle utilise un autre système d'exploitation, a pour sa part, selon les chercheurs d'AV-Test, une « note de sécurité élevée », malgré des « vulnérabilités théoriques ».

L'Apple Watch est « presque impossible à suivre à la trace », mais dévoile certaines caractéristiques d'identification quand elle est en mode avion alors que ça « ne devrait pas être le cas », détaillent-ils. L'appareil « utilise essentiellement des connexions cryptées qui ont des sécurités supplémentaires », mais ses mises à jour se font par une connexion non cryptée, notent-ils aussi.

D'après le cabinet de recherche IDC, plus de 75 millions d'appareils connectés « fitness » ont été vendus en 2015 dans le monde, et le niveau devrait franchir la barre des 100 millions cette année.

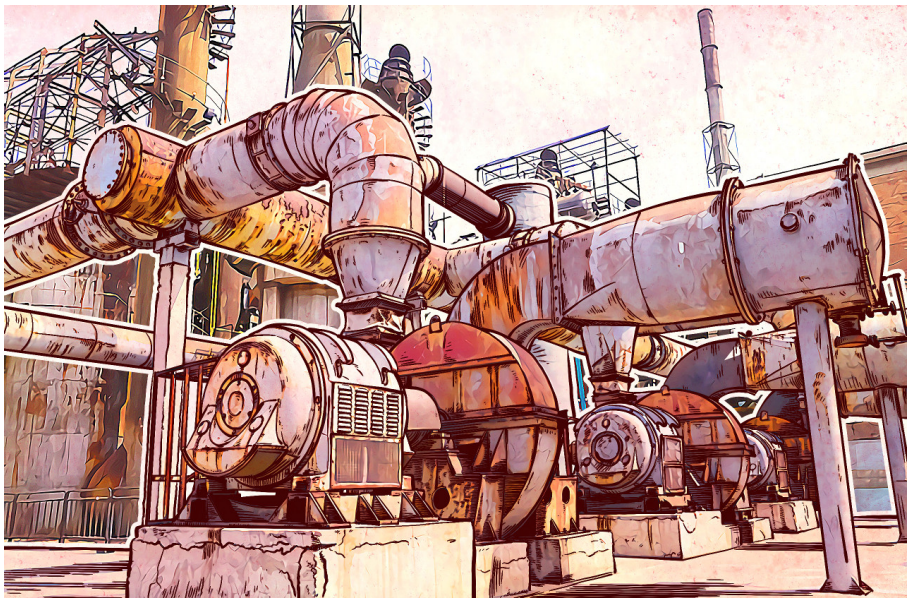
Article original de Stephen Lam

Réagissez à cet article

Original de l’article mis en page : Vous utilisez des objets connectés? Gare à vos données – L’Express L’Expansion

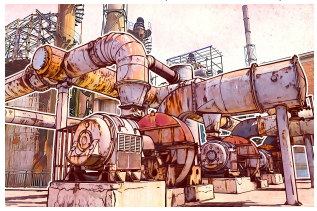
---

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



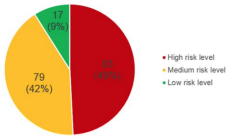
Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie ?

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.

Double authentification et numéros premium, attention au hold-up !

Double authentification et numéros premium, attention au hold-up !

Un chercheur a subtilisé de l'argent à Instagram, Google et Microsoft en appelant des numéros surtaxés via les systèmes de double authentification.

La plupart des services web proposent pour la double authentification l'envoi de code via un SMS. Mais l'utilisateur peut aussi choisir de recevoir un appel et un robot dicte à haute voix le code. Un chercheur en sécurité, Arne Swinnen a montré que les différents services testés ne vérifient pas les numéros appelés. Il a donc réussi à rattacher ses différents comptes, Instagram, Office 365 ou Google à des numéros surtaxés.
Pour Instagram, le chercheur constate qu'une fois le SMS envoyé avec le code à 6 chiffres, le service attend 30 secondes avant d'émettre un appel téléphonique depuis la Californie pour transmettre ce code. Arne Swinnen a acheté un numéro surtaxé localisé au Royaume-Uni à 0,06 livre la minute. Il a automatisé les appels vers son numéro et a obtenu 1 livre sterling au bout d'un peu plus de 17 minutes. Un pirate pourrait alors subtiliser 48 livres par jour, 1440 livres par mois et 17 280 livres par an. Avec un peu de travail, il pourrait même multiplier ses gains par 100 en gérant 100 comptes Instagram sur un numéro surtaxé. Soit une fraude évaluée à 1,728 million de livres sterling.

Google plus difficile mais pas impossible

Pour Google, l'exercice a été plus compliqué, car la firme américaine ne bascule pas automatiquement sur un appel lors du processus d'authentification sur mobile. Il s'agit d'une option qui a ses limites. En entrant un numéro premium, il était bloqué après plusieurs tentatives sans entrer le code fourni. D'où l'idée par Arne Swinnen de passer par un serveur SIP et un client SIP (comme un centre d'appel). Le numéro de téléphone fourni a été accepté par Google en lui ouvrant la voie à 10 appels par heure sans avoir besoin de rentrer le code (ce qui l'a un peu étonné). Pour automatiser le processus, il a écrit des scripts qui lui ont permis de récolter son premier euro au bout de deux heures et de 17 appels. Soit 12 euros par jour, 360 euros par mois et 4320 euros par an. Une opération qui peut être centuplée en liant 100 comptes Google à ce numéro.

Microsoft piégé par le zéro

Dernier exemple, la validation de compte Office 365. Microsoft autorise des numéros premium, mais les bloque au bout de 7 essais invalides. Mais le chercheur a trouvé des moyens de contourner cette limitation. Elles sont au nombre de deux. La première réside dans l'apposition du 0 devant le numéro de téléphone qui revalide ce numéro et permet donc un rappel. Arne Swinnen a poussé le vice à placer 18 fois le 0 devant le numéro et cela fonctionnait encore. L'autre moyen pour contourner les blocages est de rajouter de manière aléatoire jusqu'à 4 chiffres. Un savant calcul donne par numéro premium un retour sur investissement de 668 882 euros.

Récompenses et reconnaissance

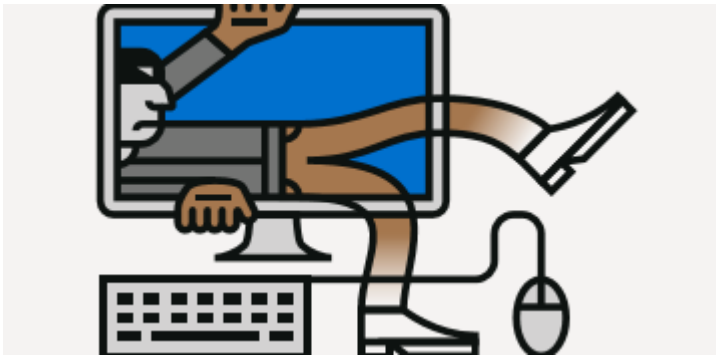
Chaque démonstration a été envoyée aux différentes sociétés pour prendre les mesures nécessaires et réparer les erreurs. Microsoft a intégré ces découvertes au sein de son programme de Bug Bounty en allouant au chercheur une prime de 500 dollars. Une prime de 2000 dollars a été également donnée par Facebook dans le cadre de son programme de recherches de bugs. Cette récompense a été doublée, car le chercheur en a fait don à une œuvre caritative. Quand à Google, il remercie Arne Swinnen non pas en espèces sonnantes et trébuchantes, mais par une reconnaissance en le plaçant dans son Hall of Fame (à la 85ème position).
Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Double authentification et numéros premium, attention au hold-up !

---

77 % des entreprises totalement impuissantes face à des Cyberattaques



77 % des entreprises totalement impuissantes face à des Cyberattaques

---

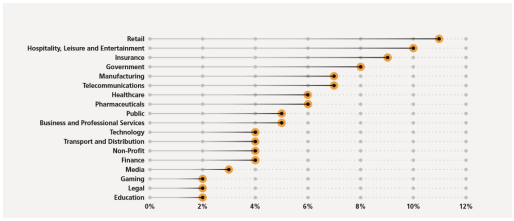
Pénurie de compétences et manque d'investissements : les entreprises sont non seulement vulnérables aux attaques, mais aussi impuissantes pour les résoudre seules. Décryptant les tendances de ces trois dernières années dans le monde, un rapport de NTT Com Security souligne le peu de progrès réalisés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