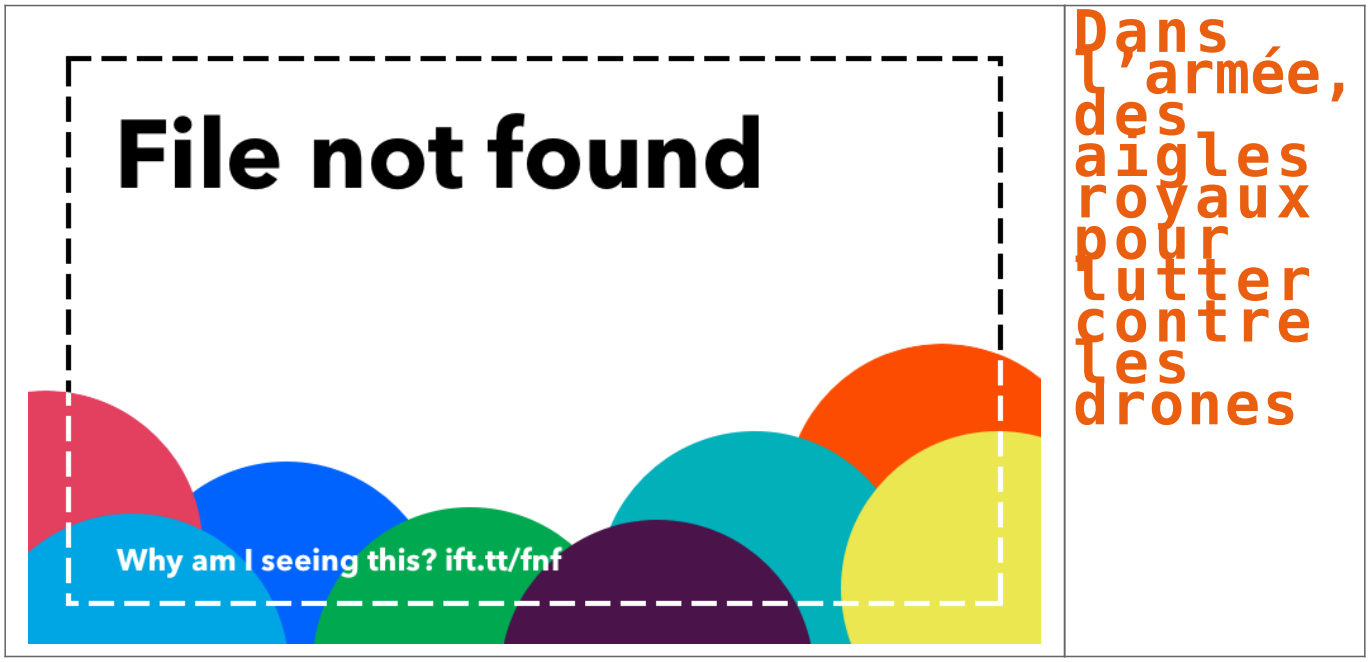
Parapluie, pommeau de douche et diffuseur d’odeurs… Ces objets connectés pour faciliter le quotidien

Parapluie, pommeau de douche et diffuseur d’odeurs… Ces objets connectés pour faciliter le quotidien

Des odeurs pour nous aider à mieux dormir, un parapluie connecté ou encore un pommeau de douche pensé pour responsabiliser son utilisateurs sur sa consommation d’eau……[Lire la suite]

Réagissez à cet article

Dans l'armée, des aigles royaux pour lutter contre les drones



Des soldats d'un nouveau genre… A l'occasion de ses vœux aux Armées, vendredi, François Hollande a pu se glisser dans la peau d'un dresseur d'aigles. Depuis le mois de septembre, ces rapaces sont en effet utilisés par l'Armée de l'Air pour lutter contre les drones.…[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous

assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur sur cette page.

Réagissez à cet article

Agir contre les rançongiciels chiffrants !

Agir contre les rançongiciels chiffrants !

Le CECyF a rejoint en décembre 2016 avec enthousiasme le programme NoMoreRansom. Il regroupe, sous l'égide d'Europol, un certain nombre de partenaires publics et privés œuvrant dans la lutte contre les cryptolockers ou rançongiciels chiffrants.

Ainsi, sur le site NoMoreRansom vous trouverez des informations sur cette menace, la façon de s'en prémunir et surtout, **dès qu'une solution existe, des liens vers les outils vous permettant de déchiffrer les fichiers compromis** par le cryptolocker dont vous êtes victime…[lire la suite

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : No More Ransom – Agissons contre les rançongiciels chiffrants ! | CECyF

Après les ransomwares, la prochaine menace est le ransomworm

Après les ransomwares, la prochaine menace est le ransomworm

Plusieurs spécialistes de la sécurité informatique sont formels les ransomwares vont évoluer pour s'en prendre au réseau à travers des vers.

Star de l'année 2016 dans le domaine de la sécurité informatique, le ransomware entend bien continuer sa progression et sa malfaisante économie. Pour mémoire, le groupe Symantec Security Response a recensé une moyenne de 4000 attaques quotidiennes en 2016. Aux Etats-Unis, les rançongiciels ont coûté 209 millions de dollars aux entreprises au 1er trimestre 2016, constate le FBI.

Face à ce pactole, les cybercriminels vont redoubler d'ingéniosité prévoit les spécialistes de la sécurité. Interrogé par nos confrères de *MIS-Asia*, Corey Nachreiner, directeur technique de Watchguard Technologies, estime que 2017 va voir « *l'arrivée du premier ransomworm permettant une propagation plus rapide du rançongiciel* ». Imaginer la combinaison d'un Locky avec des vers connus comme CodeRed, SQL Slammer ou le plus récent et encore actif Conficker. « *Après avoir infecté une victime, la charge utile va se copier inlassablement sur chaque ordinateur du réseau local* », indique Corey Nachreiner. Et de pronostiquer « *que vous croyiez ou non à ce scénario, les cybercriminels y pensent déjà* ». Un avis partagé par Nik Poltar, CEO et fondateur d'Exabeam. « *Le ransomware constitue un gros business pour les pirates et le ransomworm peut garantir des revenus récurrents. En clair, il chiffre vos dossiers, vous payez pour les récupérer mais au passage il vous laisse des cadeaux empoisonnés.* »

Une première alerte avec Zcryptor

Et le mal a commencé. Microsoft a découvert au mois de mai dernier, une souche de ransomware baptisé Zcryptor, qui se comporte comme un ver. C'est-à-dire qu'il est capable de se déplacer d'un ordinateur Windows à un autre via des supports externes (clés USB, disque dur externe, etc.) ou des disques réseaux. A l'époque, Michael Jay Villanueva, un chercheur de Trend Micro, soulignait que « *ce ransomware est un des rares à être en mesure de se diffuser par lui-même. Il laisse une copie de lui-même sur les disques amovibles, rendant l'emploi des supports USB risqué* »…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Après les ransomwares, la prochaine menace est le ransomworm

La Russie crée des unités d’élite de pirates informatiques

	La Russie crée des unités d’élite de pirates informatiques

La Russie s'appuie sur les médiaux sociaux pour appeler de jeunes recrues à intégrer des « escadrons scientifiques » capables d'accéder à des systèmes et réseaux, à l'insu des cibles. Accusée par les États-Unis d'avoir influencé l'élection américaine de novembre à travers des opérations de piratage informatique, la Russie a accéléré ses recrutements de pirates bien avant ces évènements, rapporte le *New York Times* en référence à une enquête du site d'information russophone Meduza. En plus de recruter dans les écoles d'ingénieurs, Moscou diffuse depuis plusieurs années des annonces sur les médias sociaux à l'attention d'étudiants et de programmeurs professionnels. Des hackers ayant maille à partir avec la justice sont également ciblés, selon Meduza.

L'une de ces annonces a été publiée sur le réseau social russe Vkontakte. Dans le spot vidéo ci-dessous, on devine un homme diposant d'une arme et d'un ordinateur portable. On peut y lire ce message : *« si tu es diplômé de l'enseignement supérieur, si tu es un spécialiste des technologies, nous t'offrons des opportunités, des équipements techniques de pointe, des capacités de calcul puissantes, du matériel dernier cri, un véritable entraînement au combat »*. Sans oublier le logement tout confort.

Former des « escadrons scientifiques »

Dans une autre annonce citée dans l'enquête, les autorités russes sont à la recherche d'informaticiens ayant des connaissances des *« patchs, vulnérabilités et exploits »*, explique Meduza, le site d'information russophone basé à Riga (Lettonie). La recherche de talents ne s'arrête pas là. Moscou se tournerait également vers des *« hackers ayant des problèmes avec la loi ».* Le gouvernement russe leur proposant une remise de peine en échange de leur engagement au service de la Russie…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Comment la Russie crée des unités d'élite de pirates informatiques

Des sites de piratage bientôt bannis du net par les USA ?

Les États-Unis ont toujours pris très au sérieux les menaces de la cybercriminalité, que ce soit à l'égard de l'économie du pays ou bien à l'égard de la sécurité nationale.

L'Oncle Sam ne lésine pas sur les moyens pour traquer sans relâche les présumés pirates informatiques. Tout récemment, le gouvernement américain a rendu publique la liste regroupant des sites considérés comme ayant des liens à des affaires de piratage.
Au fil des années, de nouvelles méthodes de piratage, plus sophistiquées les unes que les autres, apparaissent. Alors, *aux grands maux les grands remèdes* ! Des trackers notoires sont depuis des années dans le collimateur des États-Unis. C'est le cas, parmi tant d'autres, de ***The Pirate Bay*** **ou** ***ExtraTorrent***. La Maison Blanche, selon des sources plausibles, inclut également dans sa liste de sites à abattre certains hébergeurs de fichiers. Parmi les noms cités figurent notamment *Rapidgator,* mais aussi *Uploaded*. Mais ces plateformes sont déjà connues, ou du moins, soupçonnées d'être mêlées à des activités d'espionnage. Ce qui est surprenant dans cette affaire, c'est surtout le fait que les États-Unis se penchent aussi sérieusement sur des sites de ripping tels que YouTube-MP3.

Jusqu'à preuve du contraire, les sites européens ne sont pas dans le collimateur des États-Unis

C'est en tout cas ce que laissent entendre des pistes sérieuses qui se penchent sur la cybercriminalité. Ce serait vraiment sidérant de la part du gouvernement américain puisqu'il n'y a pas un seul pays européen où **les sites pirates ne pullulent pas.** En France, pour des raisons qu'on ne connaît pas, Zone-Téléchargement ne figure pas dans la liste noire des États-Unis. À noter tout de même que cette plateforme fait partie des plus gros acteurs du marché français.
Un grand nombre de sites de streaming sont **également dans le viseur de la Maison Blanche.** C'est le cas notamment de *Putlocker*, *Primewire* ou encore *123movies…* Comme pour la drogue, une grande partie des moyens financiers déployés par le gouvernement américain est destinée à la répression.
.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Les États-Unis révèlent les noms des sites de piratage qu'ils souhaitent bannir du net – MeilleurActu

Des spécialistes du vote électronique assurent qu’« Il est facile de pirater l’élection américaine »

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Des spécialistes du vote électronique assurent qu’« Il est facile de pirater l’élection américaine »				

Deux chercheurs de l'université du Michigan ont participé aux recomptages dans certains Etats après le scrutin de novembre.

L'élection présidentielle américaine de novembre a-t-elle été piratée ? Depuis l'intrusion de hackers dans les serveurs du Parti démocrate, la question taraude les Etats-Unis. Sans aller aussi loin, le président Barack Obama a dénoncé des *« cyberactivités qui avaient pour but d'influencer l'élection »*. Sur cette base, il a fait déclarer, jeudi 29 décembre « persona non grata », aux Etats-Unis, trente-cinq diplomates de l'ambassade de Russie à Washington et du consulat à San Francisco.

Pour leur part, après avoir participé aux opérations de recomptage des voix qui ont eu lieu dans certains Etats dans les semaines suivant le scrutin, Alex Halderman et Matt Bernhard, chercheurs de l'université du Michigan, spécialistes du vote électronique, en sont arrivés à la conclusion que l'élection n'a probablement pas été piratée. Mais que celle de 2020 pourrait bien l'être. C'est ce qu'ils ont expliqué lors du Chaos Computer Congress, grand-messe des hackers, qui se tient du 27 au 30 décembre à Hambourg, en Allemagne.

« Nous savions que des attaques sans précédent avaient été lancées pour interférer dans l'élection. Nous savions aussi qu'il était possible pour un attaquant de changer suffisamment de votes dans les machines à voter pour changer le résultat du scrutin », rappelle M. Halderman. Mais *« le recomptage a conforté l'idée que l'élection a été fiable »,* déclare M. Bernhard.

« Il est plus facile de pirater l'élection présidentielle américaine que je ne le pensais », reconnaît toutefois M. Halderman, qui avertit : *« Même si l'élection de 2016 n'a pas été piratée, l'élection de 2020 pourrait bien l'être. Nous faisons face à de plus en plus d'attaquants étatiques. Nous avons besoin de défenses efficaces pour les empêcher de mettre à mal le cœur de notre démocratie. »*

Quels contrôles sur d'éventuels piratages ?

M. Halderman, qui tente depuis des années de rendre le vote électronique plus fiable, a été convié, un peu plus d'une semaine après l'élection, à participer à une conférence téléphonique avec l'équipe de campagne de Hillary Clinton. Lors de cette discussion, à laquelle participait John Podesta, le directeur de campagne de M^me^ Clinton, plusieurs universitaires ont tenté de convaincre les vaincus de demander un recomptage des voix.

« De manière choquante, même dans ces circonstances, aucun Etat n'allait vérifier les traces en papier du scrutin électronique pour savoir si piratage il y avait », raconte M. Halderman, aux yeux de qui seule cette comparaison entre votes décomptés électroniquement et traces papier de ces votes pouvait permettre de s'assurer des résultats.

Mais l'équipe de campagne de la candidate démocrate est plus que réticente. Comme le temps presse — la loi fédérale impose aux Etats de finaliser leurs résultats le 13 décembre — l'un des collègues de M. Halderman suggère une alternative : demander à la candidate du Parti écologiste, Jill Stein (elle a obtenu un peu plus de 1 % des voix au niveau national), de requérir un recomptage dans certains Etats où le résultat a été très serré.

Où des contrôles ont-ils été réalisés ?

Les chercheurs et les équipes de M^me^ Clinton identifient trois Etats où un recomptage pourrait être intéressant : le Wisconsin, le Michigan et la Pennsylvanie. Ces trois Etats du nord du pays, où M^me^ Clinton était censée l'emporter, ont été arrachés par M. Trump. Ils comptent pour 46 grands électeurs, soit davantage que l'écart qui sépare les deux candidats dans le collège électoral. M. Trump a conquis ces Etats avec moins de 0,8 point d'avance, soit moins de 78 000 votes en tout. Autrement dit, si ces trois Etats avaient basculé du côté de M^me^ Clinton, cette dernière l'aurait emporté.

Les avocats de M. Trump ayant multiplié les recours, aucun recomptage total ne sera finalement réalisé dans aucun de ces trois Etats. En Pennsylvanie, il n'a jamais vraiment commencé. Au Michigan, il aura duré trois jours. Cette comparaison entre résultats et traces écrites a tout de même permis, selon M. Halderman et M. Bernhard, d'écarter le spectre d'une fraude généralisée. Aucune preuve de trucage n'a été découverte…[lire la suite]

Réagissez à cet article

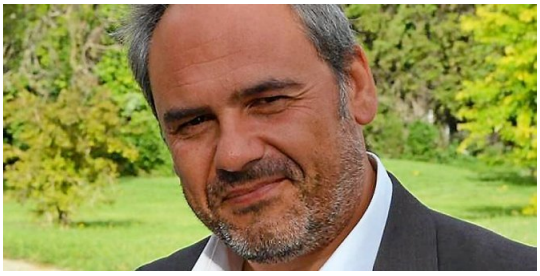
A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles
3 points à retenir pour vos élections par Vote électronique
Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique
Modalités de recours au vote électronique pour les Entreprises
L'Expert Informatique obligatoire pour valider les systèmes de vote électronique
Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise



Vos expertises seront réalisées par **Denis JACOPINI** :
• Expert en Informatique **assermenté et indépendant** ;
• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;
• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;
• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;
• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Original de l’article mis en page : « Il est facile de pirater l’élection américaine », assurent des spécialistes du vote électronique

---

Le réseau électrique américain pénétré par des pirates Russes

Le réseau électrique américain pénétré par des pirates Russes

---

Washington – Des pirates informatiques russes sont parvenus à pénétrer le réseau électrique américain via un fournisseur du Vermont, une cyberattaque sans conséquence sur les opérations de cette entreprise mais qui a pu révéler une « vulnérabilité », rapporte vendredi le Washington Post.

« Un code associé à l'opération de piratage informatique baptisée Grizzly Steppe par l'administration Obama a été détecté à l'intérieur du système d'un fournisseur d'électricité du Vermont », écrit le quotidien sur son site Internet, sans indiquer de date.
Se référant à des responsables américains non identifiés, il souligne que ce si code *« n'a pas été activement utilisé pour perturber les opérations du fournisseur* […] *la pénétration du réseau électrique national est importante parce qu'elle représente une vulnérabilité potentiellement grave ».*
Les autorités américaines ignorent à ce stade quelles étaient les intentions des Russes, poursuit le *Washington Post*, supputant qu'ils pourraient avoir tenté de porter atteinte aux activités du fournisseur –non identifié par les sources du journal– ou qu'il pourrait simplement s'agir d'un test de faisabilité.
Selon le journal, le Vermont compte deux importants fournisseurs d'électricité : Green Mountain Power et Burlington Electric.
Les pirates russes auraient envoyé des emails pour piéger les destinataires, leur faisant révéler leurs mots de passe.
En décembre 2015, 80 000 habitants de l'ouest de l'Ukraine avaient été plongés plusieurs heures dans le noir à la suite d'une cyberattaque d'une ampleur inédite. Les Russes avaient été désignés comme en étant les auteurs, ce qu'ils avaient nié…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Des pirates russes ont pénétré le réseau électrique américain | Le Devoir

Alerte : Un hack par MMS bloque l’application Messages de votre iPhone

	Alerte : Un hack par MMS bloque l’application Messages de votre iPhone

Un nouveau hack iPhone permet de bousiller à distance l'application Messages, qui permet d'envoyer et de recevoir les textos et MMS. Il s'agit d'un fichier .vcf (une fiche contact) corrompue, qui semble complètement faire flipper votre application Message, qui freeze, avant devenir complètement inutilisable. Même un redémarrage de l'iPhone ne vient pas à bout du problème qui touche tous les iPhone sous toutes les versions d'iOS 9 et d'iOS 10, y compris les versions bêta.

Dans la vidéo Youtube que vous pouvez voir en fin d'article, @Vicedes3 montre un nouveau hack à distance des iPhone assez embarrassant. En fait, l'ouverture d'une fiche contact viciée envoyée par MMS suffit à rendre l'application Messages, vitale pour envoyer et recevoir des messages, complètement inutilisable. Le redémarrage du terminal, voire même un hard reset n'y feront rien.
Nous vous recommandons donc de ne pas vous amuser à l'essayer sur votre iDevice. Pour que vous compreniez ce qui se passe, ce fichier .vcf est en fait extrêmement lourd, et excède des limites de taille qu'Apple a tout simplement omis de définir. Du coup, ce fail devrait être relativement simple à corriger. Apparemment, toutes les versions d'iOS 9 et 10, même les bêtas les plus récentes sont concernées par ce problème.
Personne n'ayant eu auparavant l'idée d'exploiter la taille des fiches contact, la faille serait ainsi tout simplement passée inaperçue pendant tout ce temps. La seule manière de réellement se protéger, c'est de ne surtout pas ouvrir les fiches contact reçues depuis des sources autres que vos contacts de confiance. Ce n'est pas en soit un virus, donc si vous le recevez, c'est que quelqu'un vous fait une mauvaise blague…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : iPhone : ce nouveau hack par MMS bousille votre application Messages

Ça y est, les ransomwares qui désactivent les téléviseurs connectés arrivent !

Ça y est, les ransomwares qui désactivent les téléviseurs connectés arrivent !

L'infection d'un téléviseur LG par un malware, racontée sur Twitter par un ingénieur informatique, rappelle la vulnérabilité des téléviseurs connectés face à ces logiciels malveillants. Et la difficulté de s'en débarrasser.

Les réserves des experts en sécurité informatique au sujet des téléviseurs connectés fonctionnant avec Android, qui seraient vulnérables aux mêmes malwares que ceux diffusés sur les smartphones, remontent à loin. L'incident raconté par Darren Cauthon prouve que ces craintes étaient justifiées.

À Noël, cet ingénieur informatique a découvert que le téléviseur connecté LG de l'un de ses proches était victime d'un ransomware que l'on trouve plus communément sur smartphone. Ce dernier est connu sous le nom de Cyber.Police, FLocker, Frantic Locker ou encore Dogspectus.

Le téléviseur aurait été infecté par une application de streaming. À la moitié du film, l'appareil s'est arrêté pour finalement rester bloqué sur la page d'accueil du ransomware. L'ingénieur ne sait néanmoins pas si l'application venait du PlayStore ou d'un tiers. Ce qui pourrait, dans le cas d'une application de piratage, expliquer que le ransomware se soit introduit si facilement sur le téléviseur.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : Un ransomware désactive un

téléviseur connecté LG — Tech — Numerama