La sanction de la Cnil contre Optical Center confirmée par le Conseil d’Etat

	La sanction de la Cnil contre Optical Center confirmée par le Conseil d’Etat

Le Conseil d'Etat a validé la sanction pécuniaire de 50 000 € que la Cnil avait prononcé à l'encontre d'Optical Center, le 5 novembre 2015, pour manquement à ses obligations de sécurité et de confidentialité, par une décision du 19 juin 2017. Il a en revanche réformé la délibération de la Cnil sur la mesure de publication, en raison de son absence de limite dans le temps.

Le Conseil d'Etat a, en effet, considéré que la sanction complémentaire infligée à l'opticien était excessive et a jugé que le maintien de la décision de la Cnil non anonymisée sur son site devait être limité à deux ans. Si la publication de la délibération vise à renforcer le caractère dissuasif de la sanction principale en lui assurant une publicité à l'égard du public, elle doit cependant respecter le principe de proportionnalité, rappelle le Conseil d'Etat.

Dans sa délibération du 5 novembre 2015, la formation restreinte de la Cnil avait considéré que la société ne s'était pas mise en conformité sur deux points qu'elle lui reprochait.

• D'abord, elle n'avait pas mis en place les mesures adaptées pour assurer la sécurité et la confidentialité des données des 170 000 comptes utilisateurs sur son site. La Cnil avait constaté que, malgré sa mise en demeure, la zone de saisie de l'identifiant et du mot de passe pour accéder au compte client depuis la page d'accueil n'était pas accessible depuis une page web sécurisée par le protocole https. A noter qu'Optical Center s'était quand même conformé à la demande de la Cnil de *« mettre en œuvre chiffrement du canal de communication et une authentification du site distant lors de l'accès au site web, que ce soit au stade de l'authentification des clients ou au stade du renseignement et de la validation du formulaire de collecte des données aux fins de création du compte ».*

• Par ailleurs, la formation restreinte avait sanctionné la société car le contrat signé avec l'un de ses sous-traitants ne contenait pas de clause précisant les obligations de ce prestataire en matière de protection de la sécurité et de la confidentialité des données des clients.

« Eu égard à la nature, à la gravité et à la persistance des manquements constatés, la formation restreinte la CNIL n'a pas infligé à la société une sanction disproportionnée aux faits de l'espèce en prononçant à son encontre une sanction pécuniaire d'un montant de 50 000 euros. », a jugé le Conseil d'Etat.

Cette sanction particulièrement sévère pour l'autorité de contrôle s'explique en partie, et comme souvent, par le manque de coopération, voire par la résistance de la personne ou de l'organisme épinglé, lors de l'instruction.

Lire la décision

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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Legalis | L’actualité du droit des nouvelles technologies | La sanction de la Cnil contre Optical Center confirmée par le Conseil d’Etat*

Windows 10 S immunisé aux ransomware connus ? Nous l’avons hacké

	Windows 10 S immunisé aux ransomware connus ? Nous l’avons hacké

Microsoft affirme qu' »aucun ransomware connu » ne fonctionne sous Windows 10 S, son système d'exploitation le plus récent et centré sur la sécurité.
Le géant du logiciel a annoncé la version de Windows plus tôt cette année en tant que système d'exploitation phare pour les étudiants de son dernier Surface Laptop. Microsoft a présenté le système d'exploitation comme moins susceptible de céder face aux ransomware en raison de sa configuration verrouillée – au point de ne pouvoir exécuter aucune application hors de sa boutique applicative. Pour obtenir qu'une app soit approuvée, celle-ci doit passer des tests rigoureux garantissant son intégrité. C'est l'une des nombreuses limitations qui aident à protéger le système d'exploitation des logiciels malveillants connus.
Nous avons voulu vérifier si une déclaration aussi audacieuse résistait aux faits.

Alerte Spoiler : il n'en est rien.
Le premier jour de la semaine dernière, nous avons mis la main sur le nouveau Surface Laptop, le premier terminal de son genre à exécuter Windows 10 S. Nous l'avons démarré, avons finalisé le processus d'installation, créé un compte hors ligne et installé un nombre incalculable de correctifs de sécurité – comme tout autre utilisateur ordinaire (j'espère).
Et c'est à ce moment-là que nous avons posé à Matthew Hickey, un chercheur en sécurité et cofondateur de l'entreprise de cybersécurité Hacker House, une question assez simple : un ransomware s'installera-t-il sur ce système d'exploitation. Il lui a fallu un peu plus de trois heures pour briser les différentes couches de sécurité du système d'exploitation, mais il y est parvenu.

« Je suis sincèrement surpris que ce soit aussi facile » a-t-il déclaré lors d'un appel téléphonique après son attaque. « Lorsque j'ai pris connaissance de la marque et du marketing du nouveau système d'exploitation, j'ai pensé qu'ils l'avaient encore améliorée. J'aurais voulu plus de restrictions sur les tentatives d'exécution de processus privilégiés au lieu d'un processus aussi court. »…[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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Windows 10 S immunisé aux ransomware connus ? Nous l'avons hacké – ZDNet*

Voilà la prochaine cyberattaque

	Voilà la prochaine cyberattaque

Après WannaCry et ses 200.000 demandes de rançon, une nouvelle cyberarme cible les réseaux électriques. Où sont les failles? Nos industries sont-elles parées? Enquête exclusive.

À lui seul, son nom file déjà des frissons. Baptisé “Industroyer” (contraction des termes anglais “industrial” et “destroyer”), un nouveau virus vient d’être identifié par des chercheurs en sécurité informatique. Il s’agit d’un puissant logiciel malveillant, voire une cyberarme de destruction massive. Ce virus industriel cible en effet le secteur de l’énergie. “C’est même la menace la plus puissante pour les systèmes de contrôle industriels depuis Stuxnet!”, enchérit le spécialiste slovaque en cybersécurité ESET, codécouvreur de cette nouvelle menace avec l’américain Dragos.
Pour rappel, le ver informatique Stuxnet, attribué aux services secrets américains et israéliens, a saboté une centrale nucléaire iranienne en 2010, provoquant même des explosions. Une première mondiale dans l’histoire du piratage informatique, qui aurait pu se solder selon les experts russes par un accident pire que celui de Tchernobyl. Le potentiel de cette super-mine numérique? D’après ces chercheurs européens et américains, Industroyer serait déjà responsable du piratage du réseau ukrainien en décembre 2016, qui avait privé une partie de Kiev d’électricité pendant plus d’une heure. “Ce nouveau virus peut être immédiatement adapté pour attaquer des réseaux en Europe et dans une partie du Moyen-Orient et de l’Asie”, avertit encore l’expert US. Cette cyberarme peut-elle dès lors frapper la Belgique, pays fortement nucléarisé et très densément électrifié? Se couvrant derrière le secret-défense, aucun opérateur belge ne se risque à y répondre…[lire la suite]

Bref commentaire de Denis JACOPINI :
Les années nous ont donné raison, nous les lanceurs d’alertes qui sensibilisons les décideurs et les élus depuis des années en tirant la sonnette d’alarme pour anticiper les risques. Chaque jour qui passe nous donne raison nous comptons les victimes de la cybercriminalité par milliers.
Le cybercrime peut prendre de nombreuses apparences, mais les décideurs et les élus, pénalement responsables aussi bien des fuites de données que de la perte des données doivent prendre les devants. Fort de nos années d’expérience dans ce domaine, nous organisons, en collaboration avec les CCI, les clubs d’entreprises et les centres de formations des sessions de sensibilisation aux risques informatiques et à la mise en conformité de vos données personnelles.
Contactez-nous

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 d’expertises, d’audits, de formations et de sensibilisation 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

Source : *Voilà la prochaine cyberattaque | Moustique.be*

---

198 millions de données personnelles d’Américains ont été exposées

	198 millions de données personnelles d’Américains ont été exposées

---

Un chercheur en cybersécurité a découvert, le 12 juin, 1 téraoctet d'informations issues de fichiers électoraux ou d'analyses de données, librement accessibles en ligne. Derrière la faille, une société qui compte le Parti républicain parmi ses clients.

Noms, prénoms, dates de naissance, adresses postales et mail, numéros de téléphone, affiliations politiques et origines ethniques autodéclarées : autant de données personnelles qu'accumulent les (très bavards) fichiers électoraux américains. Et dont les deux grands partis, et les entreprises spécialisées dans le *big data* ou le pilotage de campagne électorale, font leur miel. Or le 12 juin, Chris Vickery, chercheur pour l'entreprise de cybersécurité Upguard, a découvert qu'une telle base de données concernant 198 millions d'électeurs, soit près de 99% des inscrits, était librement accessible en ligne, sans identifiant ni mot de passe, dans un espace de stockage loué à Amazon… Aux informations issues des fichiers électoraux s'ajoutaient en outre des éléments «prospectifs» issus d'analyses de données : la religion supposée, mais aussi la probabilité d'avoir voté Obama en 2012, ou d'adhérer à la politique *«America First»*de Donald Trump…[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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Les données personnelles de 198 millions d'Américains ont été exposées – Libération*

Les entreprises du CAC 40 sont la cible de

cyberattaques

	Les entreprises du CAC 40 sont la cible de cyberattaques

Renault n’est pas la seule entreprise dans le viseur des cyberterroristes. Les champions de la défense et les géants de la Bourse peaufinent leur bouclier.
par Guerric PONCET

« En 2016, de gros industriels ont été touchés et des géants du CAC 40 ont pris conscience qu’ils pouvaient disparaître du jour au lendemain à cause d’une cyberattaque », nous confie Guillaume Poupard, directeur général de l’Agence nationale de la sécurité des systèmes d’information (Anssi). « Je veux dire que, si leur piratage était dévoilé, ils étaient *OPAbles* le lendemain », précise-t-il. En effet, la révélation d’une telle attaque ferait immédiatement chuter le cours de la Bourse…
Nos champions de la cybersécurité, Airbus, Thales, Capgemini et Orange en tête, sont sollicités de toutes parts par les comités exécutifs. Mais leurs tarifs sont souvent hors de portée des PME : dans le cyber, la défense coûte cent fois le prix de l’attaque. Et, quand bien même, le budget ne fait pas tout : JP Morgan, Yahoo !, Adobe, Visa ou encore Sony ont beau avoir alloué des centaines de millions de dollars à leur sécurité informatique, ils ont tous vécu des intrusions gravissimes. « Il est impossible de créer un cyberbouclier infaillible », tranche Guillaume Poupard, pour qui il faut avoir « une bonne gouvernance avant même de parler technique ». « Jusqu’à présent, nous avons stoppé les attaques majeures qui nous visaient, mais, si l’une d’elles réussissait, ce serait une catastrophe, avec des conséquences sur la souveraineté économique de la France et, très rapidement, sur la sécurité des populations », nous glisse, sous le couvert de l’anonymat, le responsable de la sécurité informatique d’une entreprise classée « opérateur d’importance vitale » (OIV).
Des exercices de crise sont régulièrement menés pour anticiper et limiter les dégâts que créerait assurément une cyberattaque chez un OIV – panne générale dans la production électrique, paralysie des transports, implosion des télécoms… Des agents de l’Anssi jouent aux hackers, tentent de déjouer les systèmes de sécurité… et y parviennent : « La dernière fois, ils ont pris le contrôle d’une partie de notre système assez facilement, ils auraient pu créer des accidents graves », reconnaît, lui aussi en toute discrétion, le responsable informatique d’un autre OIV. Nous voilà rassurés…[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 d’expertises, d’audits, de formations et de sensibilisation 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

Source : *Cyberguerre : le CAC 40 dans le viseur – Le Point*

« La plupart des crypto virus viennent de Russie et d’Ukraine»

	« La plupart des crypto virus viennent de Russie et d’Ukraine»

Lors du salon Viva Technology, qui se déroulait à Paris du 15 au 17 juin, Ondrej Vlcek, directeur technique de la société Avast, l'un des antivirus les plus populaires du monde, animait une conférence sur «le commerce des malwares». Alors qu'une nouvelle attaque d'un logiciel malveillant appelé WannaCry a touché la planète en mai dernier, comment se prémunir d'une telle menace à l'avenir? Quelles sont les bonnes pratiques à adopter pour minimiser les risques?

Ondrej Vlcek : C'est le nom d'une catégorie de malwares («logiciels malveillants») qui réclament une rançon. Généralement, une fois qu'un rançongiciel est installé, le hacker s'empare du disque dur des victimes avec tous leurs fichiers personnels et demande de l'argent pour rendre les fichiers – sans quoi il les supprime. Une fois que l'ordinateur est infecté, le rançongiciel commence à chiffrer les fichiers, c'est-à-dire à les transformer afin qu'ils ne soient plus lisibles et que l'on ait besoin d'un mot de passe ou d'une clé de chiffrement pour y avoir accès. Il existe aujourd'hui de nouvelles variantes : en plus de crypter le disque dur, le rançongiciel peut aussi menacer l'utilisateur de faire fuiter les fichiers volés sur tout l'Internet.

Les vieux virus étaient beaucoup moins agressifs : ils détournaient votre ordinateur et l'utilisaient simplement pour envoyer des spams ou vous obliger à cliquer sur des pubs afin de générer de l'argent. Ils pouvaient aussi détourner votre ordinateur pour vous espionner et connaître vos mots de passe et identifiants. Là, une fois que la machine est infectée, vos fichiers personnels sont immédiatement modifiés et l'on vous réclame tout de suite de l'argent pour y accéder.

WannaCry est particulièrement inquiétant, car c'est un rançongiciel « auto-répliquant ». Qu'est-ce que cela signifie ?

Normalement, la plupart des logiciels malveillants aujourd'hui nécessitent l'action de l'homme : vous devez cliquer sur un lien, ouvrir une pièce jointe associée à un message électronique ou faire quelque autre exécution manuelle. Ici, tout est entièrement automatisé, c'est-à-dire que si vous avez un ordinateur vulnérable ou pas à jour, WannaCry peut l'infecter sans avoir besoin d'aucune interaction humaine, sans même que vous soyez devant votre ordinateur.

Quelles conséquences cela peut-il avoir sur l'ampleur de WannaCry ?

Cela rend sa propagation beaucoup plus rapide, car le fait de devoir cliquer sur un lien peut prendre des jours ou des semaines. Concernant WannaCry, le monde entier a été infecté en deux heures, le logiciel passant d'un ordinateur à l'autre.

Savons-nous aujourd'hui d'où viennent tous ces logiciels malveillants ? Et quelles sommes d'argent sont impliquées dans ces attaques ?

Pour ce qui concerne les rançongiciels, la plupart viennent de Russie et d'Ukraine (concernant WannaCry, la piste nord-coréenne semble la plus probable, ndlr). Nous avons des indications qui nous laissent penser que la majorité des rançongiciels aujourd'hui sont déployés de façon à ce qu'ils n'affectent pas les personnes vivant en Russie. La raison est qu'il existe en Russie une loi qui rend la création de rançongiciels illégale lorsqu'ils peuvent avoir un impact sur des citoyens russes, mais techniquement légale, d'une certaine manière, lorsqu'ils infectent des gens hors de Russie. L'année dernière, une estimation publiée par le FBI chiffrait le coût de ces cyberattaques à plus d'un milliard de dollars. Cette année, ce montant va probablement doubler et monter à plus de deux milliards de dollars.

Peut-on neutraliser ce type de logiciels malveillants ?

Il y a deux enjeux. Le premier, c'est la prévention. Très important : utiliser un système d'exploitation à jour afin de ne pas être trop vulnérable. Il faut aussi installer un logiciel antivirus de qualité. Enfin, il vaut mieux faire des sauvegardes régulièrement, car vous pouvez ainsi récupérer vos fichiers en cas d'attaque. Je fais des sauvegardes tous les jours et je recommande à tout le monde de faire de même.

La majorité des sauvegardes se font automatiquement, mais il faut être prudent sur ce point parce que, si le rançongiciel est installé sur l'ordinateur depuis un certain temps – un jour ou deux – la sauvegarde peut aussi enregistrer les fichiers infectés qui écraseront les anciennes versions saines.

Le second enjeu apparaît lorsque l'infection s'est produite : que peut-on faire ? En fait, quasiment la moitié des rançongiciels peuvent être supprimés et décryptés sans payer la rançon, car le chiffrement n'est pas bien installé, et possède des failles. Nous ou d'autres entreprises spécialisées dans la cybersécurité sommes capables d'accéder à l'algorithme de chiffrement et de décrypter les fichiers. Mais s'il est installé correctement, il n'y a aucune chance. Avec les ordinateurs d'aujourd'hui, décrypter les fichiers prendrait des centaines d'années.

Mon conseil : si vous êtes attaqué et qu'il n'y a pas de moyen de décrypter le disque dur aujourd'hui, ne supprimez pas vos fichiers infectés pour autant si vous en avez vraiment besoin. Bien que l'outil de décryptage pour ce rançongiciel en particulier ne soit pas disponible pour le moment, il peut l'être dans six mois, un mois ou même une semaine…[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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Cybercriminalité: «La plupart des rançongiciels viennent de Russie et d'Ukraine» – Technologies – RFI*

Al Jazeera (Qatar) victime d'une cyberattaque au travers de sa télévision nationale

Al Jazeera (Qatar) victime d'une cyberattaque au travers de sa télévision nationale

Trois jours après la mise en place de sanctions sur le Qatar et un mois après le hacking de l'agence de presse nationale, le groupe Al Jazeera ainsi que la chaîne nationale qatarie ont été frappés par une vague de cyberattaques.
« Sur les dernières semaines, nous avons connu une cyberactivité grandissante contre les propriétés web et réseaux sociaux d'Al Jazeera. Aujourd'hui, nous avons remarqué une augmentation significative des tentatives cyber visant nos utilisateurs et systèmes.
Nos équipes travaillent assidûment à garantir que tous nos utilisateurs sont protégés et que tous nos systèmes opèrent normalement.
Nous continuons à être vigilants dans notre défense de nos utilisateurs, réseaux et systèmes ».

Article original
Jeudi 8 juin à 18h43 heure française, le compte Twitter d'Al Jazeera English a publié que le groupe essuyait une cyberattaque généralisée. *« Les sites webs et plateformes numériques d'Al Jazeera Media Network subissent des tentatives systématiques et continues de piratage. Ces tentatives gagnent en intensité et prennent des formes variées. Cependant, les plateformes n'ont pas été compromises »*, affirme ainsi Al Jazeera sur son site à 19h13.
BREAKING : AL JAZEERA MEDIA NETWORK UNDER CYBER ATTACK ON ALL SYSTEMS, WEBSITES & SOCIAL MEDIA PLATFORMS. MORE SOON : HTTPS://T.CO/9O3IHGGVJDPIC.TWITTER.COM/ZLBBEPTDF6
— AL JAZEERA ENGLISH (@AJENGLISH) JUNE 8, 2017
[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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Qatar : Al Jazeera et la télévision nationale ont essuyé une cyberattaque – Politique – Numerama*

Instagram détourné pour espionner des membres de gouvernements

	Instagram détourné pour espionner des membres de gouvernements

Turla, le groupe de cyberespionnage qui cible des représentants de gouvernements et des diplomates, lance une nouvelle attaque en se servant d'Instagram®. En février 2017, Forcepoint® a publié une liste de sites Internet récemment compromis.

Les cybercriminels utilisent **la technique d'attaque de trou d'eau**, qui vise à rediriger les victimes ayant cliqué sur un site compromis vers leurs serveurs C&C. Les chercheurs ESET® ont repéré **une extension de Firefox® qui utilise une URL bit.ly pour renvoyer vers les serveurs C&C. Le chemin de l'URL est diffusé via des commentaires d'une publication Instagram.** Dans l'échantillon analysé par ESET, l'un des commentaires s'affiche sur une photo du compte officiel de Britney Spears.

© https://www.instagram.com/p/BO8gU41A45g/

Pour obtenir l'URL bit.ly, l'extension scrute les commentaires de chaque photo et pour chaque commentaire en calcule un hash. Si la valeur de hash correspond à un code de déclenchement, l'extension exécute une opération pour convertir le commentaire en URL.

« L'utilisation par Turla des réseaux sociaux pour récupérer les adresses C&C ne facilite pas la tâche aux chercheurs en cybersécurité. Il est difficile de distinguer le trafic malveillant du trafic légitime sur les réseaux sociaux, » explique Jean-Ian Boutin, Senior Malware Researcher chez ESET. Par ailleurs, c**ette technique offre plus de souplesse aux pirates :** « comme l'information nécessaire pour obtenir l'URL du serveur C&C n'est autre qu'un commentaire sur les réseaux sociaux, **le cybercriminel a la possibilité de le modifier ou de l'effacer** à tout moment, » poursuit Jean-Ian Boutin.

Pour éviter d'être infecté par une attaque de trou d'eau de ce type, les chercheurs ESET recommandent de :

• mettre à jour les navigateurs et les plugins des navigateurs
• éviter de télécharger ou d'installer des extensions venant de sources non vérifiées
• utiliser une solution de sécurité (à jour) capable de détecter les sites Internet compromis

Seuls 17 clics ont été enregistrés sur ce lien en février lorsque le commentaire a été posté. Le nombre étant relativement faible, ESET suppose qu'il s'agit d'un test pour une attaque de plus grande envergure.

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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *ESET*

Mettez à jour votre téléphone sous Android. 101 failles dont 27 critiques à corriger

	Mettez à jour votre téléphone sous Android. 101 failles dont 27 critiques à corriger

Plus d'une centaine de vulnérabilités sont retirées d'Android. Dont de nombreuses liées aux puces de l'américain Qualcomm.

Google vient de publier le bulletin de sécurité de juin concernant le système d'exploitation mobile **Android** (en moutures 4.4, 5.0, 5.1, 6.0, 7.0 et 7.1).
Au menu, la correction de **101** failles de sécurité, dont **27** sont considérées comme critiques. Ces dernières permettent potentiellement la prise de contrôle du téléphone par une application malveillante.
La plupart de ces failles critiques touchent le code livré par **Qualcomm** pour ses puces. Le concepteur américain de SoC ARM montre ici sa capacité à proposer un bon « service après-vente » logiciel. Avec une amélioration constante des pilotes et applicatifs liés à ses offres.

Mise à jour au bon vouloir des constructeurs

Bien évidemment, il est vivement conseillé d'installer cette mise à jour d'Android rapidement. À condition bien entendu que votre constructeur de smartphone la relaie. Pas de souci à attendre du côté des terminaux mobiles distribués par Google. Les **Nexus** 5X, 6, 6P, 9, Player, ainsi que les **Pixel**, C et XL ont en effet déjà eu droit à cet update…[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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Google corrige 101 failles d'Android, dont 27 critiques*

Devrons nous déconnecter nos

objets connectés pour les protéger ?

Devrons nous déconnecter nos objets connectés pour les protéger ?

Bien évidemment non, certaines astuces très simples permettent de se protéger facilement et de limiter l'intrusion d'un hacker au sein de son entreprise ou son domicile.
Premièrement, en 2017, plus de 8,4 milliards d'objets sont connectés à internet. A moins qu'un hacker ait vraiment une dent contre vous, si votre objet est un minimum sécurisé, sachez qu'il ne perdra pas de temps à vous viser vous particulièrement.
Donc pour éviter toutes tentation, pensez à changer le mot de passe par défaut imposé par le fabricant (exemple : admin : admin). Faites le choix d'un mot de passe long, et rendez le aussi complexe et incohérent que possible. Pour les identifiants, favorisez les pseudonymes et évitez d'indiquer votre vrai nom. Avec cette simple manœuvre, il deviendra très difficile et surtout très long pour une personne mal attentionnée de prendre possession de vos objets connectés. La plupart des personnes hackers et le scandale qui éclate sur le sujet des objets connectés est principalement lié à ce simple oubli de la part des utilisateurs et des installateurs.
Pensez également aux mises à jour si elles vous sont proposées car elle sont importantes et contrairement à ce que la plupart des gens pensent, elles ne sont pas justes là pour ajouter de nouvelles fonctionnalités, mais principalement pour s'actualiser sur les nouvelles menaces existantes.
Alors même si c'est long et contraignant, pensez à vous mettre à jour …

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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Objets connectés et la sécurité, comment se protéger ?*