# Le pirate Informatique ayant attaqué Sony enfin démasqué ?


Le pirate Informatique ayant attaqué Sony enfin démasqué ?

**Ce serait la première fois qu'un studio d'Hollywood – en l'occurence Sony – soit la victime d'une cyberattaque venue de la Corée du Nord, et pourtant. Selon le site d'informations technologiques Re/code, Pyongyang a mené une attaque informatique pour pirater les bureaux de Sony Pictures à Los Angeles.**

La vengeance est un plat qui se mange froid, même en Corée du Nord. En juin dernier, les autorités de Pyongyang avaient annoncé qu'une réponse sans merci serait adressée à «l'acte de guerre» que constituait la sortie du film «L'interview qui tue!» d'Evan Goldberg, dans laquelle deux agents de la CIA se font passer pour des journalistes afin d'assassiner le dictateur nord-coréen Kim Jong-un.

Les menaces n'avaient pas été prises au sérieux: le film est une comédie avec Seth Rogen dans le rôle principal, et personne ne se doutait que la Corée du Nord puisse réellement prendre la mouche devant ce qui n'est qu'une parodie potache. C'était oublier le caractère absurde de la dictature nord-coréen. De mystérieux «Gardiens de la paix» ont mené une attaque informatique en début de semaine dernière contre le réseau informatique de Sony Pictures – qui distribue le film. Les employés du studio américano-nippon (deux pays ennemis de la Corée du Nord, Ndlr) ont été renvoyés chez eux, mardi avec la consigne de ne pas se connecter au réseau informatique de la société, selon Next web.

**CINQ FILMS PIRATÉS**

Cinq films ont été piratés et puis jetés en pâture sur le Web: «Annie», nouvelle version de la comédie musicale, avec Quvenzhané Wallis et Jamie Foxx, «Mr. Turner» de Mike Leigh, «Still Alice», drame avec Julianne Moore and Alec Baldwin, ou encore «Fury» avec Brad Pitt, déjà sorti en salles. Selon «Variety», les films ont été téléchargés illégalement par plus de 1,2 millions d'utilisateurs… Les pirates auraient pu également volés de nombreuses données personnelles de stars liées à Sony comme Angelina Jolie, Cameron Diaz et Jonah Hill. Pas sûr que cet épisode de guerre cyber se retrouve dans le bonus DVD de «L'interview qui tue!».

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.parismatch.com/Culture/Cinema/Kim-Jong-un-dictateur-susceptible-660458

# Les consommateurs réclament transparence, pertinence et simplicité dans l’utilisation des données en ligne


Les consommateurs réclament transparence, pertinence et simplicité dans l’utilisation des données en ligne

**Les consommateurs se disent prêts à partager leurs données personnelles si c'est fait avec transparence et à condition qu'ils en retirent un intérêt.**
Pour offrir une expérience captivante en ligne, une marque doit savoir quelles sont les attentes des clients et comment les satisfaire. Pour se démarquer de la concurrence, les entreprises ont compris l'importance de nouer une relation d'engagement et d'être en capacité de la traduire rapidement en action. Mais une stratégie basée sur de bonnes idées, sur l'intuition ou même ce qui a fonctionné par le passé ne suffit plus. Les consommateurs d'aujourd'hui sont complexes et exigeants. Ils veulent être compris et traités individuellement mais se montrent intraitables quant à leur sphère privée. Pour attirer et garder leur attention, les entreprises doivent pouvoir se procurer la bonne information au bon moment et de la bonne façon.
Nous avons interrogé 2 000 adultes britanniques pour obtenir leur point de vue dans le débat qui oppose personnalisation et protection de la vie privée. Il ressort de cette étude que les consommateurs acceptent volontiers de partager des données personnelles avec les marques, du moment que cet échange virtuel de bons procédés respecte trois valeurs fondamentales : la transparence, la pertinence et la simplicité.
84 % des 18-34 ans partagent volontiers leurs données personnelles avec les marques en utilisant pour se connecter les identifiants de leur compte sur les réseaux sociaux. Dans ce contexte, voici trois pistes à suivre par les marques pour rassurer les consommateurs et se distinguer de la concurrence en instaurant des relations privilégiées.

**Transparence, des gages de protection de la vie privée des consommateurs**
Les consommateurs rechignent à partager des données personnelles avec les marques de peur que celles-ci en fassent un mauvais usage. Il est important de réaffirmer aux consommateurs l'importance que vous accordez à la confidentialité des données et de leur dire clairement quelle utilisation vous faites de leurs données. Chaque fois que vous avez besoin d'accéder à des données personnelles, énoncez clairement l'utilisation que vous allez en faire et l'intérêt pour vos clients de jouer le jeu.
Les clients interrogés sur ce qui les inciterait à communiquer davantage d'informations les concernant à une entreprise ou une marque ont cité deux conditions majeures : être certains que la société ne partagera pas leurs données avec un tiers et savoir quels usages la société s'engage à faire des informations ainsi collectées. Chaque entreprise devrait se doter d'une politique claire qui réaffirme son approche vis-à-vis du respect de la confidentialité des données. Plutôt que de contraindre vos clients à faire l'effort de comprendre votre approche de la gestion des données, prenez les devants et publiez une déclaration d'engagement brève et formelle. Insistez sur la volonté de votre entreprise de respecter les dernières préconisation en matière de sécurité des données et envoyez un message clair à vos clients et à vos prospects qui souligne le sérieux de votre approche de protection de la confidentialité et de la sécurité des données.
En proposant aux utilisateurs de se connecter à votre site via un tiers, à savoir le compte de leur choix sur les réseaux sociaux (Facebook, Twitter, Google, etc.), vous leur permettez de décider quelles informations ils sont d'accord de partager ou non. Vous les dispensez aussi de devoir se remémorer plusieurs combinaisons d'identifiants et de mots de passe et vous-même n'aurez pas besoin de stocker ces données et les maintenir à jour.

**Pertinence, l'importance de la personnalisation**
Dans un monde où les consommateurs sont confrontés à des centaines de messages de marketing par jour, la clé est de leur délivrer des annonces pertinentes et de leur faire vivre des expériences qui leur parlent. Mais pour que ces expériences reflètent les attentes et les souhaits des consommateurs d'une façon authentique et respectueuse, les entreprises ont besoin des données des personnes concernées (first-party data). Les techniques de ciblage traditionnelles, comme les cookies de traçage, relèvent d'un jeu de devinette : ce que vous apprendrez dépend des pièces du parcours de navigation que vous allez pouvoir associer. Ces techniques ne permettent pas de dépeindre le profil complet de l'utilisateur.

Les informations les plus importantes restent de côté : les loisirs, les centres d'intérêts, les marques préférées et les relations. Et si plusieurs utilisateurs se partagent le même appareil, ces données sont encore plus diluées.

De plus, les cookies ne permettent pas de faire un suivi de l'activité sur terminaux mobiles. Maintenant qu'ils sont sensibilisés à la question de la protection de leur confidentialité, de plus en plus d'utilisateurs se protègent au moyen de logiciels qui bloquent les publicités (ad blockers) et d'applications anti-tracking, au détriment des marketers qui ont recours à ces méthodes. Ceux-ci obtiennent les données du consommateur directement qui donne son accord pour recevoir des informations par e-mail, en s'abonnant à un service, ou en se connectant via un réseau social, etc. Selon les prévisions mondiales de Bloomberg, deux milliards de personnes posséderont un smartphone en 2015.

Les entreprises doivent se familiariser avec ce nouveau paysage multicanal, veiller à soigner leur présence sur les canaux les plus stratégiques et apprendre à lisser leur image de marque et la cohérence de l'expérience qu'elles proposent, du PC fixe au terminal mobile au point de vente. Dans cette démarche d'engagement des clients sur les différents canaux, la compagnie aérienne KLM Royal Dutch Airlines a développé le programme Meet & Seat auquel les voyageurs acceptent de se connecter pour partager les infos de leurs profils Facebook ou LinkedIn avec les autres passagers.
Tous ceux qui le souhaitent ont ainsi accès aux profils sociaux des autres utilisateurs du service et peuvent choisir à côté de qui ils veulent voyager.

**Simplicité, le confort pratique avant tout**
Dès que vous invitez des utilisateurs à s'identifier, il faut que la procédure soit pratique et transparente. Notre étude montre que 59,4 % des adultes britanniques se connectent à leurs sites préférés via leur profil sur des réseaux sociaux pour gagner du temps et éviter d'en perdre à devoir remplir des formulaires.
Et plus ces consommateurs utiliseront des terminaux mobiles, plus ils chercheront à éviter les processus d'authentification longs et alambiqués pour s'inscrire et se connecter à des sites Web et à des applications. Ceux d'entre vous qui se sont arraché les cheveux à se remémorer leur mot de passe d'accès à un site se reconnaissent probablement dans les 62 % de consommateurs qui ont quitté un site Web faute d'avoir pu retrouver leur identifiant et/ou mot de passe.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.journaldunet.com/ebusiness/expert/59273/utilisation-des-donnees-en-ligne–les-consommateurs-reclament-transparence–pertinence-et-simplicite.shtml par Patrick Sayler – Directeur Général, GIGYA

---

# Sony : plusieurs films

# piratés avant même leur sortie dans les salles


## Sony : plusieurs films piratés avant même leur sortie dans les salles

**Victime d'une attaque informatique d'envergure, Sony Pictures a vu ses activités tourner au ralenti la semaine dernière. Dimanche, des hackers publiaient plusieurs copies des grosses productions à venir sur la toile, compromettant le lancement de plusieurs films.**

Victime de plusieurs attaques informatiques la semaine passée, l'intranet de Sony Pictures est tombé peu après que la sécurité de l'un des serveurs de la firme ait été compromise. Les hackers, qui ont pénétré dans le système, ont menacé Sony Pictures de diffuser les dernières superproductions de Sony sur la toile si le distributeur ne répondait pas aux exigences des pirates, lesquelles n'ont pas été dévoilées publiquement.
Dimanche, le groupe de pirates menait ses menaces à exécution en diffusant plusieurs copies de films récents ou à venir comme Fury, Annie, Mr. Turner ou encore Still Alice, en version DVD.
En quelques heures, Fury, le dernier film de Brad Pitt, était déjà le second film le plus téléchargé sur Pirate Bay.
La diffusion de ces copies DVD de films pas encore sortis ou tout juste disponibles dans les salles est une grande première sur la toile. Si plusieurs films ont déjà fait les frais d'une diffusion à grande échelle avant leur sortie, comme The Expendables 3 ou X-Men, c'est la première fois que tout le catalogue de films d'un distributeur est diffusé simultanément. Un fiasco qui pourrait bien sûr affecter les résultats de Sony Pictures au cours des prochains mois mais aussi pousser les distributeurs à investir davantage dans la sécurité informatique.
Le distributeur, qui a très peu communiqué sur le piratage de son intranet, a réagi à la diffusion de son catalogue de films sur Pirate Bay en évoquant un "crime". Elle a également indiqué travailler avec les forces de l'ordre pour retrouver les auteurs des attaques.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://geeko.lesoir.be/2014/12/01/sony-plusieurs-films-pirates-avant-meme-leur-sortie-dans-les-salles/

# Detekt : l’outil Anti-Espions d’Amnesty International, Digitale Gesellschaft, l’Electronic Frontier Foundation et Privacy International…


Detekt : l’outil Anti-Espions d’Amnesty International…

**Amnesty International, Digitale Gesellschaft, l'Electronic Frontier Foundation et Privacy International, ont lancé un outil anti-espion : Detekt.**

Ce billet a été rédigé par Marek Marczynski, responsable à Amnesty International du programme sur les transferts d'équipements ou de compétences dans les domaines militaire, de sécurité ou de police.

**Imaginez que vous n'êtes jamais seul**
Quelqu'un regarde par-dessus votre épaule, enregistre toute activité sur votre ordinateur, lit et écoute vos conversations privées sur Skype, allume le microphone et la caméra de votre téléphone portable pour vous surveiller, vous et vos collègues, sans même que vous vous en rendiez compte.
Pour des milliers de défenseurs des droits humains et de journalistes qui, aux quatre coins de la planète, s'efforcent de dévoiler des atteintes aux droits humains et des injustices choquantes, nul besoin de l'imaginer.
Ils sont victimes d'une nouvelle forme sophistiquée de surveillance illégale. Certains gouvernements utilisent déjà des technologies de pointe pour installer des espions virtuels dans leurs bureaux et leurs salons.
La plupart des personnes ciblées ne savent même pas qu'elles sont espionnées, jusqu'à ce qu'on leur montre des copies de courriels et de vidéos où elles apparaissent, avec leurs collègues. Ces documents ont été extraits subrepticement de leurs propres ordinateurs portables. Ces « preuves » refont souvent surface lorsque les militants sont passés à tabac dans des cellules sordides, sanctionnés pour leur travail légitime ou contraints d' »avouer » des crimes qu'ils n'ont pas commis.

**Le militant des droits humains et blogueur Ahmed Mansoor est l'un d'entre eux.**
Ressortissant des Émirats arabes unis, il a été relâché en 2011. Il avait été incarcéré parce qu'il avait signé une pétition en faveur de la démocratie et animait un forum de discussion en ligne, que le gouvernement avait bloqué un an auparavant sous prétexte qu'il hébergeait des commentaires critiques envers les autorités. Après sa libération, Ahmed Mansoor a découvert que ses déplacements étaient parfois surveillés et a été agressé physiquement à deux reprises. Il s'est plus tard rendu compte que son ordinateur avait été infecté par des logiciels espions qui permettaient aux autorités de surveiller chacun de ses mouvements. Sa messagerie et son compte Twitter étaient également piratés.
Ce type de logiciels espions sophistiqués est l'arme idéale contre les défenseurs des droits humains. Ils sont de plus en plus utilisés dans le monde, même dans des États qui proclament défendre les libertés fondamentales.
Ces logiciels sont développés et produits dans des pays comme le Royaume-Uni, l'Allemagne et l'Italie, pour être ensuite vendus à des gouvernements du monde entier, sans qu'aucune réglementation ne garantisse qu'ils ne serviront pas à faciliter des atteintes aux droits humains.

**« Cette nouvelle forme de surveillance semble tout droit sortie de 1984 de George Orwell, et elle rencontre un vif succès. Auparavant, les gouvernements interceptaient des communications ; aujourd'hui, ils peuvent entrer dans les systèmes et tout surveiller comme s'ils se trouvaient dans la pièce** », a déclaré Marek Marczynski, responsable à Amnesty International du programme sur les transferts d'équipements ou de compétences dans les domaines militaire, de sécurité ou de police.

Et même si l'Union européenne s'est récemment engagée à adopter des réglementations sur le commerce des équipements de surveillance, cette technologie dangereuse se développe à un rythme effréné.

**Detekt**
En réaction au nombre croissant de militants arrêtés arbitrairement et interrogés avec violence sur la base d'informations soutirées illégalement, des experts en technologie se sont mis à jouer « au chat et à la souris » pour combattre la surveillance ciblant des personnes qui exercent leur droit à la liberté d'expression et d'association. Certains de ces experts se sont associés avec Amnesty International, Digitale Gesellschaft, l'Electronic Frontier Foundation et Privacy International, afin de lancer un nouvel outil.
Detekt est un logiciel simple qui permet d'effectuer une analyse sur un ordinateur fonctionnant avec le système d'exploitation Microsoft Windows pour y trouver la trace de logiciels espions et alerter ses utilisateurs afin qu'ils puissent agir.

Selon Claudio Guarnieri, l'un des cerveaux qui a développé cet outil, Detekt répond à une demande d'aide croissante de la part des militants depuis 2012.

« Nous avons commencé à faire des recherches sur les pays qui commercialisent des équipements de surveillance et avons découvert qu'une société allemande en vendait aux autorités de Bahreïn, qui les avaient utilisés contre les manifestants durant le soulèvement [depuis février 2011]. Tout est parti de là, et cela nous a emmenés vers des pays comme le Maroc, la Tunisie, l'Éthiopie et quelques autres, qui s'en sont eux aussi servis », a déclaré Claudio Guarnieri.

« Tant de pays utilisent désormais ces technologies, qu'il serait plus simple de se pencher sur les autres. Si vous prenez une carte et placez un point rouge sur chaque pays concerné, cela fait froid dans le dos: Bahreïn, le Maroc, les Émirats arabes unis, Oman, l'Éthiopie, le Soudan, l'Ouzbékistan, le Kazakhstan, l'Azerbaïdjan, l'Indonésie, la Malaisie, l'Australie, l'Inde, le Mexique, Panama, le Royaume-Uni et l'Allemagne, entre autres. »

La Coalition contre l'exportation illégale de technologies de surveillance, dont Amnesty International est membre, estime que le commerce mondial des technologies de surveillance représente 4 milliards d'euros par an, et qu'il est en expansion.

FinFisher compte parmi les entreprises qui développent ce type de logiciels espions. Cette société allemande qui a appartenu à l'entreprise britannique Gamma International a conçu le logiciel espion FinSpy, grâce auquel il est possible d'effectuer un suivi des conversations sur Skype, d'extraire des fichiers de disques durs, d'enregistrer toute utilisation du microphone ainsi que les courriels, et même de prendre des captures d'écran et des photos en utilisant la caméra de l'appareil.
Selon des recherches menées par Citizen Lab et des informations rendues publiques par Wikileaks, FinSpy a permis d'espionner des militants et des avocats défenseurs des droits humains à Bahreïn – dont certains vivaient au Royaume-Uni.
C'est le cas de Saeed Al Shehabi, militant politique bahreïnite actuellement installé au Royaume-Uni. En juillet 2014, Privacy International a publié des informations indiquant que Gamma International avait vendu des services de logiciels aux autorités bahreïnites.

**« Nous savions que les autorités surveillaient les militants à Bahreïn, mais nous ne pensions pas qu'il leur était possible de le faire ici, au Royaume-Uni. J'ai peur, parce qu'on ne sait jamais quelles informations ils ont recueillis, ni comment ils vont les déformer et s'en servir. Je ne me sens pas du tout en sécurité. Detekt me semble un outil très utile, et inestimable pour des militants comme moi** », a déclaré Saeed.

**Sécurité et droits humains**
Les organisations qui dénoncent la surveillance ciblée illégale sont fréquemment accusées de développer des outils susceptibles d'entraver l'action légitime du gouvernement contre le crime organisé.

Toutefois, les experts comme Claudio Guarnieri s'accordent à dire que le problème est l'absence quasi totale de contrôle, de cadres juridiques et de lignes directrices quant à l'utilisation de ces technologies intrusives.

**« La transparence n'est pas de mise pour savoir qui s'en sert et dans quelles circonstances. La seule chose que nous savons, c'est que ces technologies servent souvent à entraver le travail des militants et des journalistes. Nous souhaitons lancer un débat pour tenter de comprendre comment cela fonctionne, car tout se déroule dans le plus grand secret. Il faut plus de transparence sur les implications légales, morales et politiques de l'emploi de ces technologies** », a déclaré Claudio Guarnieri.

Nous espérons que Detekt apportera un sentiment de sécurité aux défenseurs des droits humains, aux journalistes, aux avocats et aux militants, et qu'il permettra d'ouvrir le débat sur la nécessité de réglementer le développement, la vente et l'utilisation des technologies de surveillance.

« Ce marché échappe à tout contrôle. Il faut des réglementations légales solides pour qu'il soit en phase avec les normes relatives aux droits humains. Les conséquences négatives et les dangers du recours non réglementé à ces technologies puissantes sont énormes et celles-ci doivent être contrôlées », a déclaré Marek Marczynski.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.huffingtonpost.fr/genevieve-garrigos/detekt-un-nouveau-logiciel-dans-le-jeu-du-chat-et-de-la-souris-contre-big-brother_b_6235750.html
par Geneviève Garrigos Présidente Amnesty International France

---

# CryptoPHP – Plus de 23 000 serveurs web infectés

CryptoPHP – Plus de 23 000 serveurs web infectés

**La propagation du backdoor CryptoPHP se fait par les plug-ins et les thèmes piratés pour les CMS WordPress, Joomla et Drupal.**

Plus de 23 000 serveurs web ont été infectés par un backdoor baptisé CryptoPHP qui est arrivé avec les thèmes et les plug-ins piratés pour des systèmes de gestion de contenu très populaires, à savoir WordPress, Joomla et Drupal. CryptoPHP est un script malveillant qui permet des attaques à distance avec la possibilité d'exécuter du code délictueux sur des serveurs web et d'injecter du contenu inapproprié sur des sites web.

Selon le cabinet de sécurité néerlandais Fox-IT, qui a publié un rapport sur cette menace la semaine dernière, la porte dérobée est principalement utilisée pour l'optimisation de BHSEO (Black hat search engine optimization), une opération qui consiste à injecter des mots-clés et des pages indélicates sur les sites compromis afin de détourner les recherches effectuées par les moteurs traditionnels et pousser du contenu malveillant le plus haut possible dans les résultats de recherche.

**Un backdoor profitant de la culture pirate des webmasters**

Contrairement à la plupart des backdoors s'attaquant aux sites web, CryptoPHP ne s'installe pas en exploitant les vulnérabilités. Les hackers distribuent simplement des versions piratées des plug-ins et thèmes commerciaux pour Joomla, WordPress et Drupal et attendent simplement que les webmasters les téléchargent et les installent sur leurs propres sites web. Ces plug-ins et thèmes pirates intègrent le backdoor CryptoPHP. Les serveurs web infectés par CryptoPHP agissent comme un réseau de zombies. Ils se connectent à des serveurs de commande et de contrôle exploités par les hackers en utilisant un canal de communication chiffré et attendent les instructions.

Avec l'aide du Centre national de la cybersécurité du gouvernement néerlandais et d'organisations de lutte contre la cybercriminalité (Fondation Shadowserver, Abuse.ch et Spamhaus), Fox-IT a pris le contrôle des domaines de commande et de contrôle de CryptoPHP envoyant des instructions aux serveurs infectés pour recueillir des statistiques. Une opération connue sous le terme « sinkholing ».

**Plus de 1000 sites web infectés en France**

« Au total, 23 693 adresses IP uniques étaient reliés aux centres de contrôle », ont indiqué dans un billet de blog les chercheurs de Fox-IT. Cependant, le nombre de sites concernés est probablement plus élevé, parce que certaines de ces adresses IP correspondent à des serveurs d'hébergement web partagé qui ont plus d'un site infecté. Les cinq premiers pays infectés par CryptoPHP étaient les États-Unis (8657 adresses IP), l'Allemagne (2877 adresses IP), la France (1 231 adresses IP), les Pays-Bas (1008 adresses IP) et la Turquie (749 adresses IP).

Depuis la publication du rapport de Fox-IT sur CryptoPHP la semaine dernière, les hackers ont fermé les sites qui ont poussé les plug-ins et thèmes piratés pour en créer de nouveaux. Ils ont également introduit une nouvelle version de leur backdoor, peut-être dans une tentative d'échapper à la détection.

Les chercheurs Fox-IT ont publié deux scripts Python sur GitHub que les webmasters peuvent utiliser pour scanner leurs serveurs et leurs sites web à la recherche de CryptoPHP. Ils ont également fourni des instructions pour le supprimer sur leur blog, tout en notant que finalement il est préférable de complètement réinstaller son CMS afin de repartir sur une base saine.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-plus-de-23-000-serveurs-web-infectes-par-cryptophp-59420.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter
Le rapport : https://foxitsecurity.files.wordpress.com/2014/11/cryptophp-whitepaper-foxsrt-v4.pdf
Article de Peter Sayer, IDG NS (adaptation Serge Leblal)

---

# Les e-commerçants ciblés par les attaques des cybercriminels


Les e-commerçants ciblés par les attaques des cybercriminels

**Selon un rapport d'Imperva réalisé en octobre 2014, les e-commerçants sont les plus souvent ciblés par les cyber-attaques. Les attaques seraient plus nombreuses, mais également plus longues. 48 % des attaques cibleraient directement des applications web des e-commerçants, mais les institutions financières sont également concernées.**

**Les données des e-commerçants visées par les hackers**
Les chiffres sont issus du rapport Web Application Attack Report (WAAR), réalisé par l'Application Defense Center (ADC) d'Imperva. Selon l'équipe du spécialiste de la sécurité informatique, près d'une attaque sur deux cible les e-commerçants, et notamment leurs applications web. 40 % des attaques par injection SQL et 64 % des campagnes de trafic http malveillant concernent les sites de commerce en ligne.

D'après l'équipe ADC, le système de gestion de contenu WordPress est également souvent visé par les attaques. Pour Imperva, l'audience des sites est un critère de choix pour les hackers : « quand une application web ou une plateforme devient populaire, les hackers savent que le retour sur investissement d'une attaque sur ces supports sera intéressant pour eux, ils passent donc plus de temps à les explorer, soit pour voler des données soit pour utiliser les systèmes comme bots », estime le rapport WAAR.
Selon l'enquête d'Imperva, les sites de commerce en ligne sont attaqués deux fois plus souvent que des sites plus classiques. Les attaques durent aussi plus longtemps : près de deux fois plus longtemps qu'en 2013.
« Les e-commerçants doivent prendre ces menaces de cyber-attaque très au sérieux », soutient Amichai Schulman, directeur de la technologique pour Imperva, qui évoquent le verrouillage des bases de données et leur cryptage.
En France, la Fevad (Fédération du e-commerce et de la vente à distance) et Médiamétrie estiment que les consommateurs vont se tourner en masse vers les achats en ligne pour Noël 2014. 68% des internautes envisagent un achat sur internet d'ici la fin de l'année.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.commentcamarche.net/news/5865731-les-e-commercants-cibles-par-les-attaques-des-cybercriminels

---

# Tom's Guide victime d'une attaque de l'armée électronique syrienne


# Tom’s Guide victime d’une attaque de l’armée électronique syrienne

**En début d’après-midi, Tom’s Guide et de nombreux sites d’information ont été victimes d’une attaque informatique de la part de l’armée syrienne électronique. Des magazines tels que « The Independent » et « The Telegraph », en Grande Bretagne, le Chicago Tribune aux Etats-Unis ou encore le site de la ligue nationale de hockey (NHL.com) ont été simultanément touchés par cette attaque.**

Sur ces sites, comme sur tomsguide.fr, le procédé de l’armée électronique syrienne est le même. Celle-ci aurait réussi à exploiter une faille du CDN de Gigya. Il s’agit d’un réseau de diffusion de contenus, notamment sociaux, qui est utilisé par plusieurs sites médias dans le monde, dont tomsguide.fr. Dès lors qu’elle a réussi à s’attaquer à Gigya, l’armée électronique syrienne a pu injecter une redirection dans le code distribué par ce service.

**Des hackers proches de Bachar el-Assad**

C’est la raison pour laquelle, une partie de des lecteurs de tomsguide.fr a vu s’afficher un message revendiquant le piratage du site et un lien affichant le drapeau du groupe de hackers. L’armée électronique syrienne est un groupe de pirates informatiques proche du régime de Bachar el-Assad. Né en 2011 en début de la guerre civile syrienne, il s’emploie à perturber le fonctionnement de médias occidentaux qu’il juge hostiles au régime syrien.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.tomsguide.fr/actualite/piratage-armee-syrienne,45695.html

# CyberArk publie un rapport sur les nouvelles tendances en matière d’attaques ciblées avancées – Global Security Mag Online

| | |
|---|---|
|  | CyberArk publie un rapport sur les nouvelles tendances en matière d’attaques ciblées avancées – Global Security Mag Online |

**CyberArk annonce la publication d'un nouveau rapport qui détaille les tendances actuelles des cyberattaques ciblées avancées, lesquelles ont communément adopté comme signature clé l'exploitation malveillante des comptes à privilèges.**

L'étude intitulée « Privileged Account Exploits Shift the Front Lines of Security » apporte une expertise sur les récentes tendances des attaques ciblées, à partir de l'expérience de terrain des analystes les plus réputés au monde en matière de menaces informatiques et de résolution des attaques de sécurité les plus dévastatrices. Les participants à cette analyse incluent :

· Groupe de renseignements de sécurité et de recherche Cisco Talos
· Service de consultance financière Deloitte LLP – Equipe de recherche informatique
· Deloitte & Touche LLP – Services en matière de risques informatiques
· Mandiant, une entreprise FireEye
· RSA, Division Sécurité d'EMC
· L'équipe RISK de Verizon

« Cette coalition rassemble certains des analystes des menaces informatiques les plus brillants, expérimentés et réputés au monde. C'est en comparant et en comprenant les points communs de nos recherches respectives que nous avons pu dresser un aperçu approfondi des modes de fonctionnement des attaques ciblées, explique Udi Mokady, PDG de CyberArk. Cette étude nous a permis de découvrir que presque chaque attaque avancée implique une exploitation de comptes à hauts pouvoirs, raison principale pour laquelle elles sont si difficiles à déceler et à stopper. Ces comptes permettent en effet aux assaillants d'accéder à des réseaux et bases de données sécurisés, d'effacer toute trace d'infraction, d'éviter toute détection et de créer des portes de sortie rendant leur éviction des réseaux quasi impossible. La sécurisation des comptes à privilèges est devenue la nouvelle priorité des systèmes de défense dans la bataille que les entreprises mènent actuellement face à la cybercriminalité. »

Les comptes à privilèges, qui se composent notamment des identifiants utilisés pour l'administration informatique des mots de passe par défaut et codés en dur ainsi que de backdoors d'applications, offrent aux pirates informatiques un véritable laissez-passer qui leur permet de se rendre où ils le souhaitent et de traverser le réseau sans le moindre obstacle. Ces comptes permettent également aux hackers d'effacer leurs traces et de soutirer des données en tous genres. Et dès que ceux-ci parviennent à obtenir un accès privilégié aux systèmes et applications critiques, il est extrêmement difficile de les arrêter et d'atténuer les risques de perte de données et de préjudice commercial.

**Parmi les principales découvertes du rapport :**
· Chaque secteur et chaque entreprise est aujourd'hui une cible : Les pirates informatiques ont élargi leur champ d'action et **ciblent aujourd'hui les entreprises de toutes tailles**, dans tous les secteurs confondus. Chaque attaque a souvent une cible bien déterminée, et les **pirates visent fréquemment leurs partenaires et fournisseurs**. Les analystes en sécurité ont étudié des attaques visant des cibles non-traditionnelles, telles que des **sociétés de transport par camion** et de nombreux autres prestataires de services professionnels (**conseillers en gestion, auditeurs, avocats spécialisés dans les contentieux, etc.**), lesquelles constituent une étape clé dans le processus d'attaque d'un partenaire commercial.
· La résistance de périmètre est futile : Les pirates parviendront tout de même à s'introduire dans le périmètre de sécurité, et les employés constitueront le point d'infection le plus probable. L'attaque par hameçonnage est la technique la plus répandue et ne fait que gagner en sophistication, ce qui a rendu les connexions des employés beaucoup plus simples à infiltrer que les réseaux ou autres logiciels.
· Les pirates restent cachés pendant plusieurs mois ou années : Lors de leur détection, la plupart des attaques étaient en cours depuis au moins 200 jours. Les attaques financières sont quant à elles décelables plus rapidement, en règle générale en moins de 30 jours. Les assaillants peuvent dissimuler leurs traces par le biais des comptes à privilèges, en supprimant l'historique des connexions ainsi que les autres preuves.
· Les pirates convoitent les accès à hauts pouvoirs : Dans presque chaque cyberattaque ciblée, des comptes à privilèges ont été piratés. D'après leurs recherches, les analystes de la sécurité déclarent qu'entre 80 et 100% des incidents de sécurité les plus graves avaient pour « signature » une exploitation malveillante de comptes à hauts pouvoirs au cours de leur processus d'attaque.

· Les menaces liées aux comptes à privilèges largement sous-estimées : Les risques et les failles de sécurité que présentent les comptes à privilèges sont bien plus importants que les entreprises ne le réalisent. Les sociétés sous-estiment grandement le nombre de comptes à hauts pouvoirs qu'elles possèdent et ignorent quels systèmes les hébergent. Les recherches de CyberArk ont démontré que les organisations comptent aujourd'hui au minimum trois à quatre fois plus de comptes à privilèges que d'employés.

· Les cyberattaques contre les comptes à privilèges sont de plus en plus sophistiquées : Les analystes de la sécurité ont recensé plusieurs types d'infractions au niveau des comptes à hauts pouvoirs, qui vont de l'attaque répétée des comptes de service à la violation des appareils embarqués de l' « Internet des objets », en passant par la création d'identités multiples dans Microsoft Active Directory afin d'assurer la redondance des points d'accès et des portes dérobées.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.globalsecuritymag.fr/CyberArk-publie-un-rapport-sur-les,20141120,48898.html
par CyberArk

# Un logiciel malveillant caché dans le chargeur d’une cigarette électronique

Un logiciel malveillant caché dans le chargeur d’une cigarette électronique

**Selon des experts interrogés par The Guardian, si le véhicule de l’attaque est inédit, l »anecdote » en elle-même n’a rien de surprenante : les différents supports USB sont fréquemment à l’origine de virus informatiques.**

Décidément, on ne peut plus se fier à rien de nos jours ! The Guardian rapporte l’histoire d’un cadre d’une grande entreprise qui s’est fait piéger par un logiciel malveillant codé dans son chargeur de cigarette électronique. »L’ordinateur d’un des cadres était infecté par un logiciel malveillant dont la source ne pouvait être déterminée. Le système était à jour, avait un antivirus et disposait de tous les dispositifs anti-malwares. […] Au final, après avoir cherché du côté de tous les moyens d’infection traditionnels, le service informatique a cherché d’autres possibilités. Ils ont demandé au cadre: « Y a-t-il des changements dans votre vie récemment? » Et le cadre a répondu: « oui, j’ai arrêté de fumer il y a deux semaines et me suis mis à la cigarette électronique », témoigne un membre du personnel informatique de l’entreprise en question sur le site Reddit.

Selon des experts interrogés par The Guardian, si le véhicule de l’attaque est inédit, l »anecdote » en elle-même n’a rien de surprenante : les différents supports USB sont fréquemment à l’origine de virus informatiques. Les clefs USB sont d’ailleurs plus difficiles à pirater que les périphériques USB. Pour Pierre-Yves Bonnetain, consultant sécurité informatique interrogé par France Info, il faudrait remonter l’ensemble de la chaîne de production des cigarettes électroniques pour en savoir plus. »La chaîne de fabrication est relativement complexe. A un moment ou à un autre, quelque part dans la chaîne, il est parfaitement possible qu’un des ces soust-traitants approvisionnent des composants qui ont déjà été frabriqués en étant malveillants », explique-t-il.

En août, deux chercheurs allemands, Karsten Nohl et Jakob Lell, ont réalisé une expérience pour montrer comment il est possible de transformer le code qui permet de faire fonctionner le périphérique USB pour installer un virus sur l’ordinateur. La faille, nommée Bad USB, permettait de mémoriser n’importe quelle saisie sur votre clavier : mots de passe, numéros de carte bancaire… Et à l’heure actuelle, il existe malheureusement très peu de solutions pour se protéger de ce type de virus. Morale de l’histoire : évitez d’acheter des contrefaçons qui circulent sur le net !

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.atlantico.fr/atlantico-light/cyber-piratage-logiciel-malveillant-cache-dans-chargeur-cigarette-electronique-1874188.html

# Sony Pictures victime d’une attaque informatique, les pirates ont publié certaines données sensibles après un chantage

| | |
|---|---|
|  | Sony Pictures victime d’une attaque informatique, les pirates ont publié certaines données sensibles après un chantage |

**Les employés de la filiale du groupe japonais Sony Pictures Entertainment basée à Los Angeles ont eu une surprise des plus désagréables ce lundi 24 novembre 2014. En allumant leurs ordinateurs, une image représentant un squelette avec comme titre en rouge « Hacked By #GOP » (Gardians of Peace) apparaissait sur leurs écrans. Par la suite, les pirates passaient leur message : « nous vous avons déjà prévenu, et ceci n'est que le commencement. Nous continuerons jusqu'à ce que nos exigences soient satisfaites .» En cas de refus d'obtempérer, les pirates menacent de dévoiler à la face du monde des documents obtenus.**

Depuis l'expiration de ce délai le 24 novembre 2014 à 23h GMT, plusieurs archives ont été publiées sur divers sites. Même si la plupart des liens ne fonctionnent pas, il est toujours possible de récupérer, sur Thammasatpress, un fichier au format zip de 207 Mo qui contient trois fichiers intitulés LIST1, LIST2 et « Readme ». Ce dernier se présente sous le format texte et contient des adresses électroniques. Pour les deux autres, ils semblent regrouper des documents financiers ainsi que des codes sources et des bases de données. Une analyse avec la commande GREP, dont le rôle est de rechercher un mot dans un fichier et d'afficher les lignes dans lesquelles ce mot a été trouvé, permet d'identifier des clés de chiffrement, mais aussi ce qui ressemble à des documents d'identité relatifs à certaines stars hollywoodiennes à l'instar d'Angelina Jolie.

La société n'était pas joignable pour commenter ces informations, mais un communiqué adressé au Hollywood Reporter indique que « Sony Pictures Entertainment a connu une perturbation de son réseau, et nous travaillons d'arrache-pied pour la résoudre ». Une source a confirmé « qu'un seul serveur a été compromis et l'attaque s'est propagée à partir de là ». Les employés ont été invités à rentrer chez eux après l'attaque : « nous allons tous travailler de la maison. Nous ne pouvons même pas aller sur internet » a déclaré un employé sous le couvert de l'anonymat. Ce dernier a confirmé que le département informatique de l'entreprise a demandé aux employés d'éteindre leurs ordinateurs et de désactiver le WiFi de leurs appareils mobiles, mais également qu'un message adressé aux employés a précisé que la résolution de cet incident pourrait prendre jusqu'à trois semaines.

Outre le blocage des ordinateurs de Sony Pictures, ce sont de nombreux comptes Twitter de Sony qui ont été provisoirement piratés afin de tweeter le même message sur le réseau social. L'entreprise a depuis repris le contrôle de ces comptes Twitter.

Cependant, le magazine spécialisé The Verge avance avoir reçu un courriel de la part des hackers responsables de cette attaque qui dit « nous voulons l'égalité [sic]. Sony ne le veut pas. C'est une bataille ascendante ». D'ailleurs un tweet cinglant de la part de GOP a été adressé à Michael Lynton, le PDG de Sony Entertainments, sur le compte de Starship Trooper's où lui et le reste du staff ont été traités de « criminels ».

Selon The Verge, les pirates ont affirmé avoir réussi à infiltrer la société en travaillant « avec d'autres employés ayant des intérêts similaires » parce que « Sony ne verrouille pas ses portes, physiquement, ». Pour The Verge, cela peut impliquer que les pirates ont réussi à pénétrer les serveurs de l'entreprise avec l'aide de personnes ayant accès aux serveurs internes de Sony.
Sony Pictures quant à lui a choisi de rester sobre dans sa communication en se contentant de dire que « nous enquêtons sur un incident informatique ».

En août dernier, les pirates ont affirmé être venus à bout de PlayStation Network via une attaque par déni de service qui a inondé le système de données réseau erronées. Toutefois, l'entreprise a tenu à rassurer les utilisateurs en affirmant qu'aucune des données personnelles des 53 millions d'utilisateurs de la plateforme PlayStation Network n'a été compromise suite à l'incident daté du 24 août. D'ailleurs, les ingénieurs ont pu à nouveau rendre l'accès disponible dès le lendemain. En 2011, une brèche dans la sécurité de la même plateforme exposait les identifiants (noms d'utilisateur et mots de passe) des utilisateurs.
Source : bloomberg, the verge

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

S o u r c e :
http://www.developpez.com/actu/77586/Sony-Pictures-victime-d-une-attaque-informatique-les-pirates-ont-publie-certaines-donnees-sensibles-apres-un-chantage/