Le nombre d'incidents de sécurité informatique a augmenté de 48% en 2014 !

Le nombre d'incidents de sécurité informatique a augmenté de 48% en 2014 !

D'après l'enquête The Global State of Information Security Survey, le nombre d'incidents de sécurité informatique dans le monde a augmenté de 48 % cette année.

C'est à l'instigation de PwC, CIO et CSO que le sondage The Global State of Information Security Survey a été réalisé auprès 9700 chefs de direction et gestionnaires en finances, en informatique et en sécurité informatique dans le monde, 35% en Amérique du Nord, 34% en Europe, 14% de l'Asie-Pacifique, 13% d'Amérique du Sud et 4% du Moyen-Orient et d'Afrique.

Publiés ce jeudi, les résultats sont que le nombre d'incidents de sécurité informatique à l'échelle internationale a augmenté de 48% en 2014 pour atteindre près de 43 millions d'incidents, soit un peu plus de 117 000 attaques par jour.

Alors que ce chiffre donne déjà des frissons, il est estimé que plus de 70% des incidents informatiques ne sont pas détectés en raison des méthodes de plus en plus sophistiquées qui sont utilisées par leurs auteurs.
Ce constat a vraiment de quoi inquiété vu qu'il est estimé que le coût global de la cybercriminalité cette année dépasse les 23 milliards de dollars, et cela uniquement pour les incidents détectés. Le coût global réel des atteintes à la sécurité informatique est « impossible à établir » selon les auteurs de l'enquête. En soulignant qu'il est particulièrement difficile de chiffrer la valeur de certains types d'informations, par exemple la propriété intellectuelle et les secrets commerciaux.
L'enquête révèle par ailleurs qu'un tiers des incidents sont imputables aux employés, un autre tiers aux ex-employés et un quart aux pirates informatiques. Les attaques des États, le crime organisé et de la concurrence font partie des incidents les moins fréquents.

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

Source : http://www.linformatique.org/le-nombre-dincidents-de-securite-informatique-augmente-de-48-en-2014/

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 piratés 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)

La police judiciaire découvre une escroquerie à la carte bancaire inédite

La police judiciaire découvre une escroquerie à la carte bancaire inédite

L'office anti cyber-criminalité de la police judiciaire a annoncé vendredi avoir démantelé un réseau d'une quinzaine d'escrocs à la carte bancaire utilisant une méthode nouvelle. Ils auraient fait plus d'une centaine de victimes.

Ils pensaient avoir trouvé un système imparable pour s'enrichir à distance. Mais malgré leur inventivité et après avoir fait des centaines de victimes en France, une quinzaine d'escrocs à la carte bancaire ont été interpellés par l'office anti cyber-criminalité de la direction centrale de la police judiciaire (DCPJ).

Des escrocs créatifs… et bricoleurs

Les cyber-escrocs qui comptaient dans leurs rangs des petits commerçants, n'avaient pourtant rien laissé au hasard mais surtout, ils avaient innové.

Leur méthode consistait à fabriquer eux-même des « TPE » (les terminaux de paiements électriques que l'on trouve dans la plupart des magasins) permettant d'enregistrer le code de la victime ainsi que les données associées à sa carte bancaire. Ces informations en main, les escrocs débitaient les cartes depuis l'étranger, échappant à tous les filtres habituels.

Les victimes elles, ne se doutaient de rien. Au terme de la transaction sur le « TPE » frauduleux elles recevaient même le reçu habituel leur garantissant que leur carte avait bien été débité du montant indiqué sur l'appareil.

« Eviter l'effet « boule de neige » »

« Nous avons enquêté pendant un an il fallait agir avant que cette méthode ne fasse « boule de neige » en France » a affirmé Valérie Maldonado, directrice de l'office anti cyber-criminalité de la PJ (**OCLCTIC**).

Reste maintenant à retrouver les victimes. Leur nombre pourrait dépasser la centaine. Quant au préjudice total il reste lui aussi à déterminer mais pourrait atteindre des centaines de milliers d'euros.

Des escroqueries qui se multiplient

La fraude à la carte bancaire n'a cessée de progresser ces dernières années en France, selon un rapport de l'Observatoire national de la délinquance et des réponses pénales (ONDRP). Entre 2010 et 2012, le volume de ces fraudes a augmenté de 44%. En 2012, on estimait le préjudice total à plus de 450 millions d'euros. Dans plus des deux tiers des cas, les victimes ne sont débitées qu'une seule fois pour un montant moyen de 900 euros. On estime que le nombre d'escroqueries à la carte bancaire augmente deux plus vite que le nombre de cartes mises en circulation.

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

Source : http://www.franceinfo.fr/actu/justice/article/la-police-judiciaire-decouvre-une-escroquerie-la-carte-bancaire-inedite-609719

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

Les collégiens de plus en plus victimes de cyberviolences

Les collégiens de plus en plus victimes de cyberviolences

Selon une enquête de l'Éducation nationale dévoilée par RTL jeudi, 18% des élèves de collège déclarent avoir été insultés, humiliés ou victimes d'actions dévalorisantes par le biais de leur téléphone portable ou de leur ordinateur en 2013.

Souvent utiles, les outils numériques comme les téléphones portables, les tablettes ou les ordinateurs peuvent aussi se retourner contre leurs utilisateurs. Au grand dam parfois des plus jeunes, plus vulnérables face à ces nouvelles technologies. Commentaires désobligeants, insultes, photos publiées à leur insu… Depuis deux ans, la cyberviolence se développe dans des proportions inquiétantes dans les collèges.
18% des collégiens déclarent ainsi avoir été insultés, humiliés ou victimes d'actions dévalorisantes en 2013 par le biais des nouvelles technologies, selon une enquête de l'Éducation nationale dévoilée par RTL jeudi.
Parmi eux, 5% affirment avoir subi cette violence de façon répétée et être sujet au «cyberharcèlement». En comparaison, en 2011, seuls 9% des élèves de collège déclaraient avoir été insultés ou humiliés par textos ou internet. Mais à l'époque, l'enquête ne se basait pas sur les mêmes critères qu'aujourd'hui puisque les photos, agressions et «happy slapping» (agressions filmées, ndlr) n'étaient pas pris en compte.

La direction de l'évaluation, de la prospective et de la performance (Depp), la branche statistique du ministère de l'Éducation nationale qui est à l'origine de ce rapport alarmant, a constaté que ce phénomène touchait davantage les élèves de troisième et plus particulièrement les filles. Il n'est par ailleurs pas plus répandu dans les établissements difficiles qu'ailleurs.

Les enseignants aussi victimes de cyberharcèlement
Autre donnée statistique: les élèves victimes de cyberviolence sont en général plus touchés que leurs camarades par d'autres types d'agressions. Un collégien sur trois déclare ainsi avoir subi des coups en plus d'attaques sur la toile, contre un sur sept qui ne déclare pas de cyberviolence. Selon la note de la Depp, «les élèves touchés par la cyberviolence sont aussi deux à trois fois plus nombreux à avoir été épiés dans les toilettes». Ce nouveau type de violence reste toutefois difficile à quantifier, les jeunes victimes ayant souvent du mal à en parler. Si elles se laissent aller à des confidences, c'est le plus souvent en-dehors de leur établissement, à un ami ou un parent. Mais elles sont encore plus d'un tiers à ne pas réussir à en parler.

À une moindre échelle, les enseignants sont eux aussi parfois victimes de cyberharcèlement. Si le phénomène n'est pas nouveau et qu'il reste marginal au regard des autres formes de violences dont sont victimes les professeurs, il n'en reste pas moins en hausse. Les «préjudices informatiques» représentent 3,7 % des dossiers traités par les Autonomes de solidarité laïques (ASL) – qui assurent depuis plus de 110 ans la défense des personnels de l'enseignement public et privé laïque – et la Maif, bien loin derrière les agressions verbales, qui prédominent (75 %). Mais ces chiffres ne prennent en compte que les dossiers déclarés, selon l'assureur Maif, qui évoquait en avril auprès du Figaro une «omerta» autour du cyberharcèlement.

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

Source : http://www.lefigaro.fr/actualite-france/2014/11/27/01016-20141127ARTFIG00086-education-les-collegiens-de-plus-en-plus-victimes-de-cyberviolences.php

---

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

---

La collaboration

transfrontalière, clé de la lutte contre la cybercriminalité

La collaboration transfrontalière, clé de la lutte contre la cybercriminalité

Europol vient d'annoncer l'interpellation d'une quinzaine d'individus, dont six français, suspectés d'avoir utilisé des chevaux de Troie pour perpétrer différents types de cyber-attaque. L'opération, pilotée par la France, a été réalisée en collaboration avec différents pays européens.

L'office de police intergouvernemental Europol, les forces de l'ordre françaises ainsi que six autres pays (Royaume-Uni, Estonie, Roumanie, Lettonie, Italie et Norvège) ont œuvré conjointement pour mettre la main sur quinze hackers. Jean-Pierre Carlin, directeur Europe du sud de LogRhythm, éditeur américain de logiciels de sécurité informatique basé dans le Colorado (Etats-Unis) et dont le siège social en France se trouve à Neuilly-sur-Seine (92), se félicite de cette collaboration transfrontalière. « Cette arrestation montre que nous sommes en train de rattraper notre retard sur les pirates informatiques, affirme-t-il. Nous disposons de davantage d'outils pour détecter l'origine des attaques et nous sommes capables de les tracer. Partager l'intelligence au-delà des frontières est la clé absolue. »

Coopération inégale

Car, jusqu'à présent, les forces de l'ordre détectaient les malware et les chevaux de Troie sans remonter à la source. Les hackers bénéficiaient donc d'un anonymat total. « Puis, la collaboration entre les pays s'est peu à peu tissée, ajoute Jean-Pierre Carlin. Mais tous les Etats ne coopèrent pas de la même façon. Les pays européens adhérents d'Europol travaillent main dans la main, mais pour les Etats-Unis et les états asiatiques, la donne est différente. »

Cependant, des opérations comme celles-ci ne peuvent être un succès que si les bonnes informations sont mises à disposition. Les organisations ont un rôle à jouer, celui d'assurer leur propre protection. « Toutes les entreprises doivent garantir la surveillance de la moindre activité sur leur réseau en temps réel, précise le directeur Europe du sud de LogRhythm. Avec une visibilité accrue, les comportements anormaux sont identifiés immédiatement et les informations collectées sont partagées avec les autorités pour arrêter les criminels. C'est la fonction de notre produit d'analyse LogRhythm Security Analytics. »

Caroline Albenois

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

Source : http://www.info.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-1e13ba8f63fad9bbf651b6e811431989.htm

---

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…

Source : http://www.developpez.com/actu/77586/Sony-Pictures-victime-d-une-attaque-informatique-les-pirates-ont-publie-certaines-donnees-sensibles-apres-un-chantage/