Sony Pictures va piéger les films piratés pour mettre un terme aux fuites

Sony Pictures va piéger les films piratés pour mettre un terme aux fuites

Victime d’un piratage à l’envergure peu commune, Sony Pictures semble être plus que déterminé à mettre un terme à la diffusion de ses fichiers sur le Net. En effet, la filiale du groupe japonais orchestrerait elle-même plusieurs opérations de piratage afin d’empêcher le partage de documents sensibles…

L’information est révélée par le site Re/Code, qui évoque des sources « en connaissance directe du dossier ». Selon celles-ci, Sony Pictures s’appuierait sur les datacenters asiatiques d’Amazon utilisés pour fournir les services cloud du marchand afin de mener une attaque par déni de service sur les sites proposant de télécharger des données issues du récent piratage dont la compagnie a été victime. Et ce ne serait pas tout : le Japonais s’attèlerait également à décourager les curieux en diffusant des copies piégées des fichiers volés.
Rappelons que Sony Pictures a toutes les raisons de chercher à mettre un terme à ces fuites. Outre des films encore inédits, la centaine de To de données volées contenait aussi de nombreux documents personnels d’employés et d’acteurs, des rapports financiers, ou encore des accords confidentiels. Si la diffusion de ces informations a d’ores et déjà occasionné quelques grincements de dents, le Japonais se doit de limiter les dégâts, d’autant que tout ce butin numérique n’est pas encore disponible sur le Web. La méthode, toutefois, peut laisser perplexe.
Cependant, ce n’est pas la première fois qu’un poids lourd des médias combat le feu par le feu. En 2007, plusieurs firmes, dont Sony Pictures mais aussi Universal, EMI, Paramount ou encore Ubisoft avaient été pointées du doigt pour avoir eu recours aux services de MediaDefender, dont les tactiques anti-piratage étaient fort décriées. En effet, ce spécialiste de la défense des intérêts des producteurs de médias pratiquait déjà la diffusion de faux fichiers afin de rendre le piratage franchement laborieux – sans compter qu’il s’était particulièrement illustré par un litige avec The Pirate Bay, qui l’accusait, non sans preuve, d’avoir orchestré une attaque en bonne et due forme contre ses serveurs.

Mais revenons-en à l’affaire qui nous occupe. Pour l’heure, les spécialistes qui se penchent sur le cas de Sony Pictures sont unanimes : il s’agit d’une attaque sophistiquée, qui aurait sans l’ombre d’un doute fonctionné contre une vaste majorité de systèmes. Son origine, toutefois, demeure à confirmer. Bien que les regards se soient d’emblée tournés vers la Corée du Nord, et bien que les pirates aient explicitement demandé l’annulation du film The Interview, qui met en scène l’assassinat de Kim Jong-un par deux journalistes plutôt limités, le régime nie avoir avoir entrepris une quelconque action à l’encontre de Sony Pictures au-delà de ses sommations de renoncer au long-métrage. Une autre piste, de plus, a fait son apparition : une des salves de leaks (fuites) a été orchestrée depuis le très chic hôtel St. Regis, à Bangkok. De quoi s’interroger sur la véritable identité des curieusement vindicatifs Guardians of Peace.

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

Source : http://www.lesnumeriques.com/sony-pictures-mene-attaque-ddos-pour-mettre-terme-fuites-n37601.html
Par Johann Breton

Cyber-sécurité : 10 tendances pour 2015

	Cyber-sécurité : 10 tendances pour 2015

L'année 2014 a été particulièrement chargée pour les professionnels de la sécurité informatique. A quoi s'attendre pour 2015 ? Le point avec Thierry Karsenti, directeur technique Europe de Check Point.

Pour l'année 2014, « nous nous attendions à une augmentation des tentatives d'ingénierie sociale, et l'avons bien constatée. Elles ont conduit à d'importantes fuites de données dans plusieurs enseignes bien connues. Les campagnes de logiciels malveillants ciblées se sont également intensifiées. Les attaques de « RAM scraping » et les attaques de rançonneurs ont fait les gros titres. Le nombre de problèmes de sécurité mobile a également continué d'augmenter, indique Thierry Karsenti. Le hic, ce sont les vulnérabilités massives qui ont été découvertes dans des composants informatiques établis, tels que Heartbleed et BadUSB, qui ont touché des dizaines de millions de sites web et d'appareils dans le monde entier. Personne n'y avait été préparé. 2015 verra-t-il les mêmes cyber-risques ?

1. **Les logiciels malveillants « zéro seconde »**

Plus d'un tiers des entreprises auraient téléchargé au moins un fichier infecté par des logiciels malveillants inconnus au cours de l'année dernière. Les auteurs de logiciels malveillants utilisent de plus en plus des outils spécialisés de masquage, afin que leurs attaques puissent contourner les mécanismes de détection des produits antimalwares et infiltrer les réseaux. Efficaces, les bots continueront d'être une technique d'attaque privilégiée, indique Thierry Karsenti.

2. **La mobilité**

Comme vecteurs d'attaque, les appareils mobiles offrent un accès direct à des actifs plus variés et plus précieux que tout autre moyen d'attaque individuel. « C'est également le maillon faible de la chaîne de sécurité, qui donne aux agresseurs un accès à des informations personnellement identifiables, des mots de passe, la messagerie professionnelle et personnelle, des documents professionnels, et l'accès aux réseaux et aux applications d'entreprise », précise le directeur technique.

3. **Les systèmes de paiement mobile**

Le lancement d'Apple Pay avec l'iPhone 6 est susceptible de relancer l'adoption des systèmes de paiement mobiles par les consommateurs, ainsi que d'autres systèmes de paiement concurrents : "Tous ces systèmes n'ont pas été testés pour résister à de réelles menaces, ce qui pourrait signifier d'importantes chances de succès pour les agresseurs qui trouveront des vulnérabilités à exploiter ».

4. **Les failles dans l'open source**

Qu'il s'agisse de Heartbleed (voir l'interview de Patrick Duboys, fondateur d'Alice and Bob http://www.solutions-logiciels.com/actualites.php?actu=14573) ou de Shellshock (voir l'interview vidéo de Vincent Hinderer, expert en cyber-sécurité au Cert du groupe Lexsi http://www.solutions-logiciels.com/actualites.php?actu=15039), les vulnérabilités critiques des plates-formes open source communément utilisées (Windows, Linux, iOS) sont très prisées par les agresseurs car elles offrent d'énormes possibilités. Logiquement, ces derniers vont donc continuer de rechercher des failles pour essayer de les exploiter.

5. **Les attaques sur les infrastructures critiques**

Les systèmes Scada qui commandent les processus industriels devenant de plus en plus connectés, cela va étendre les vecteurs d'attaque qui ont déjà été exploités par des agents logiciels malveillants connus tels que Stuxnet. Près de 70% des entreprises d'infrastructures critiques interrogées par le Ponemon Institute ont subi des attaques au cours de l'année passée.

6. **Les objets connectés**

L'Internet des objets fournit aux criminels un réseau mieux connecté et plus efficace pour lancer des attaques. Les entreprises doivent se préparer à leur impact.

7. **Les réseaux définis par logiciel (SDN)**

La sécurité n'est pas intégrée au concept SDN, « et doit l'être », affirme Thierry Karsenti qui enchérit : « *Avec son adoption croissante dans les centres de données, nous nous attendons à voir des attaques ciblées qui tentent d'exploiter les contrôleurs centraux SDN pour prendre le contrôle des réseaux et contourner les protections réseau* ».

8. **L'unification des couches de sécurité**

Pour lui, les architectures de sécurité monocouche et les solutions isolées provenant de différents fournisseurs n'offrent plus une protection efficace pour les entreprises. Il affirme que de plus en plus de fournisseurs proposeront des protections unifiées issues de développements, de partenariats et d'acquisitions.

9. **Les protections en mode SaaS**

Thierry Karsenti prévoit « une utilisation croissante des solutions de sécurité sous forme de services pour fournir visibilité, contrôle, prévention des menaces et protection des données ». Cette augmentation se fera parallèlement à l'utilisation croissante des services de sécurité externalisés dans le Cloud public.

10. **L'évolution des analyses grâce au Big Data**

Le Big Data va apporter d'énormes possibilités à l'analyse des menaces pour identifier de nouveaux schémas d'attaque, selon l'éditeur. Les fournisseurs intégreront de plus en plus ces capacités analytiques à leurs solutions, et les entreprises devront également investir dans leurs propres systèmes d'analyse pour prendre les bonnes décisions en fonction du contexte et des menaces pesant sur leur activité. Le partage collaboratif de renseignements sur les menaces continuera de se développer, pour proposer des protections à jour qui répondent aux besoins spécifiques des utilisateurs finaux. Le directeur technique de Check Point ajoute que ces possibilités alimenteront à leur tour des solutions de sécurité unifiées capables de fournir automatiquement une protection contre les nouvelles menaces émergentes pour renforcer la sécurité des entreprises.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…
Source : http://www.solutions-logiciels.com/actualites.php?actu=15189&titre=Cyber-securite-10-tendances-pour-2015 Par Juliette Paoli

Sony victime de hackers organisés et obstinés

Sony victime de hackers organisés et obstinés

Outre une société de sécurité mandatée par Sony, le FBI enquête lui aussi sur l'attaque informatique qui a visé récemment une filiale du groupe japonais, Sony Pictures. Et de premiers éléments ont été présentés par les enquêteurs au Sénat américain.

Ainsi comme les experts en sécurité de Mandiant, le FBI estime que l'attaque était inhabituelle et complexe à prévenir. Seules quelques entreprises auraient eu la capacité de bloquer la réalisation d'une telle attaque, estime l'agence fédérale.

Une attaque efficace sur 90% des entreprises

« Le malware qui a été utilisé aurait passé 90% des protections Internet qui sont déployées à l'heure actuelle dans le secteur privé et aurait probablement constitué un défi y compris pour un gouvernement fédéral » a déclaré le directeur adjoint de la division cybersécurité du FBI, Joe Demarest.

A l'occasion de cette audition devant un comité du Sénat, ce dernier a également précisé, selon The Hill, que l'attaqué était organisée et que son niveau de sophistication était extrêmement élevé. Quant à l'identité des auteurs, le FBI estime ne pas pouvoir la déterminer à ce stade, faute de preuves suffisantes.

Des liens avec la Corée du Nord ont été évoqués depuis le début de l'affaire, mais non confirmés. Les autorités du pays ont depuis démenti être à l'origine de cette cyberattaque, après avoir entretenu le flou au départ.

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

Source : http://www.zdnet.fr/actualites/sony-victime-de-hackers-organises-et-obstines-39811145.htm

ESET s’engage auprès de Facebook pour protéger les utilisateurs des cyber-menaces

	ESET s’engage auprès de Facebook pour protéger les utilisateurs des cyber-menaces

ESET protège tous les utilisateurs Facebook contre le piratage.
ESET rejoint l'initiative Anti-malware lancé par Facebook et offre « ESET Online Scanner » à tous les utilisateurs de Facebook. Cette solution permet d'identifier les posts provenant non pas des utilisateurs mais de logiciels malveillants. Ces posts sont alors retirés en toute sécurité. ESET Online Scanner pour Facebook est disponible depuis le 03 décembre 2014 et pour tous les utilisateurs de Facebook.

« Notre but est d'offrir à nos utilisateurs la meilleure technologie afin d'améliorer l'utilisation de nos services et de protéger au mieux leurs appareils connectés. ESET Online Scanner va de manière significative diminuer le nombre de clics sur des liens malicieux, effectués des milliards de fois chaque jour sur Facebook » explique Chetan Gowda, Web developer chez Facebook.

La version dédiée d'ESET Online Scanner pour Facebook, a été conçue pour détecter et nettoyer les ordinateurs infectés des utilisateurs de Facebook. « ESET est heureux d'offrir ses services aux utilisateurs de Facebook du monde entier. ESET est reconnu pour sa légèreté et sa qualité de détection, ces deux atouts se retrouvent dans cette version pour Facebook, gratuitement.», annonce Ignacio Sbampato, Directeur Commercial et Marketing chez ESET HQ.

Votre ordinateur a besoin d'être nettoyéSuppression des logiciels malveillants Un fonctionnement simple et ciblé
Lorsqu'un utilisateur se connecte à son compte, Facebook cherche des comportements malicieux – comme l'envoi de spams ou de liens infectés provenant d'amis Facebook. Si ce type d'activité est détecté, Facebook invite l'utilisateur à utiliser ESET Online Scanner. L'analyse s'effectue directement sur Facebook, gratuitement et en tâche de fond.

L'utilisation du scanner est sans impact sur le système de l'utilisateur, de sorte qu'il peut continuer à utiliser son appareil sans gêne. Une fois l'analyse terminée, l'utilisateur reçoit une notification de la part de Facebook; un compte rendu du scan est aussi disponible. Le nettoyage commence une fois l'analyse terminée si des malwares ont été détectés.

Ce service pour Facebook est basé sur une solution gratuite ESET Online Scanner protégeant des millions d'internautes. Sur plus de 44 millions de scans, ESET Online Scanner a détecté avec succès des malwares dans presque la moitié des analyses.

ESET est un outil de protection et de désinfection que je conseille personnellement.
Vous avez envie de découvrir et de tester gratuitement ce logiciel de protection (ESET NOD32 ou ESET SMART SECURITY, je peux vous communiquer une licence sur simple demande.
Denis JACOPINI

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

Source : https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14a2e1044c5865c4

Le PSN inaccessible suite à une attaque de Lizard Squad

Le PSN inaccessible suite à une attaque de Lizard Squad

Depuis quelques heures, le PlayStation Network de Sony est inaccessible pour de nombreux utilisateurs. Il s'agirait visiblement d'une nouvelle attaque DDOS, revendiquée par le groupe Lizard Squad.

Les problèmes touchent principalement l'Amérique du Nord, mais d'autres joueurs dans le monde ont remarqué quelques soucis depuis le milieu de la nuit.
PlayStation a rapidement tenu informé ses joueurs via Twitter, sans toutefois donner trop d'informations.
On ne sait donc pas vraiment quand seront réglés ces soucis, mais on sait au moins que les équipes de Sony travaillent à régler le problème, et c'est déjà une bonne nouvelle.
Le groupe Lizard Squad a revendiqué cette attaque, et c'est donc visiblement le serveur d'authentification de Sony qui est visé (comme l'indique ce tweet https://twitter.com/LizardPatrol/status/541751366297743360), perturbant ainsi grandement le PSN.
Espérons que tout rentrera dans l'ordre rapidement, puisque ces problèmes répétés risquent fortement d'agacer les joueurs.

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

Source : http://www.gameblog.fr/news/47390-le-psn-inaccessible-suite-a-une-attaque-de-lizard-squad

SONY : Connexion impossible au PSN

SONY : Connexion impossible au PSN

Déjà responsable de la paralysie des serveurs du Xbox Live sur Xbox One et Xbox 360 dernièrement, le groupe de hacker Lizard Squad semble de nouveau être en train de complètement faire disjoncter le PSN, causant des messages de connexion impossible sur PS4, PS3 et PS Vita en ce lundi 8 décembre 2014. En effet, les joueurs se plaignent un peu partout de ne plus pouvoir jouer en ligne sur leur console PlayStation, et de ne plus avoir accès au PSN.

Il y a peu de temps, Lizard Squad avait annoncé une campagne visant à complètement mettre à terre les services online de Microsoft et Sony le jour de Noël 2014, et est déjà responsable de plusieurs épisodes de paralysie du PSN et du Xbox Live ces dernières semaines. Prendre en otage le PSN aujourd'hui même, alors que Sony est en pleine PlayStation Experience est-il un message d'avertissement aux deux constructeurs ? Difficile à dire, d'autant que rien n'est jamais demandé en retour. C'est alors les joueurs qui se retrouvent pénalisés avec des connexions impossible au PSN et Xbox Live. Cependant, dans l'ombre, Anonymous souhaite ne pas en rester là, et menace à son tour Lizard Squad dans une vidéo postée sur internet il y a deux jours, disponible ci-dessous.
Bien entendu, il est toujours assez délicat d'accorder de la légitimité aux nouvelles vidéos d'Anonymous, tant ce groupe est volatile, et peut être représenté par n'importe qui. Vont-ils essayer de voler dans les plumes d'un Lizard Squad qui multiplie les actions pour mettre à terre les services online de la PS4 et de la Xbox One régulièrement ? De son côté, Sony avoue être en ce moment même au travail pour rétablir les connexions à son PSN. Nous vous tiendrons bien entendu au courant de la situation, dans notre colonne d'actualité jeux vidéo, comme toujours.

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

Source : http://playerone.tv/news/v/6234/connexion-impossible-au-psn-lizard-squad-ddos-encore-les-services-playstation.html

---

Live streaming illégal : Le revers de la médaille

Live streaming illégal : Le revers de la médaille

Si depuis l'aube d'Internet, les sites pornographiques constituent le vecteur principal de propagation de virus sur la toile, les sites illégaux de live streaming représentent une concurrence de taille. Selon l'étude de l'AISP, alors que 97 % des sites de streaming illégaux sont infectés par des malwares (logiciels malveillants), faisant de cette pratique la voie d'infection la plus courante sur Internet, les plateformes illégales de live streaming représentent une grande partie des ces infections. Au point de devenir une véritable porte ouverte à la fraude et au vol de données.

Le streaming vidéo, qui constitue aujourd'hui 91 % du trafic Internet mondial, est depuis quelque temps déjà ancré dans le paysage virtuel mondial. Son pendant « en direct », le live streaming, est quant à lui entré dans les mœurs il y a peu. Développées en 2008 par des entreprises comme Youtube ou Google, les technologies permettant le visionnage et le partage de vidéos en direct sur Internet ont plus ou moins stagné depuis. Il faudra attendre la Coupe du monde de football 2014 au Brésil pour démocratiser la pratique dans le monde entier, mais surtout pour voir un véritable marché noir du live streaming se développer en parallèle. Du 12 juin au 13 juillet dernier, plus de 20 millions de personnes à travers le monde ont regardé les matches de la Coupe du monde en live streaming sur des sites illégaux.

Une question d'informations

Leur gratuité, si elle a permis à ces sites de se démocratiser, est aussi la cause principale de l'émergence des pirates dénoncée par l'AISP. Comme n'importe quelle marchandise ou service, un site peut être gratuit soit parce qu'il bénéficie de subventions ou de dons – une hypothèse peu probable pour les sites illégaux de live streaming – soit parce qu'il a minoré ses investissements dans son développement, le plus souvent au détriment de sa sécurité.

Faire sauter les pare-feu des sites illégaux de live streaming est ainsi bien souvent un jeu d'enfants pour pirates et hackers. Toujours selon ce rapport de l'AISP, certains d'entre eux vont même jusqu'à créer et développer leurs propres sites de live streaming illégal, infectés et porteurs de chevaux de Troie dès leurs créations, afin d'augmenter leurs chances d'attraper un internaute dans leur toile. Ainsi, alors que 160 000 nouveaux malwares sont créés par jour, les sites illégaux de live streaming ont envahi les moteurs de recherche et représentent une pierre de plus à l'édifice de menaces que constitue Internet aujourd'hui.

La toile est en effet souvent pointée du doigt comme la source de dangers toujours plus nombreux et variés. Des accusations parfois exagérées qui ne doivent pas faire oublier la responsabilité de l'internaute. Pour Anton Korobkov-Zemlianski, un membre de la commission de la science et des innovations de la Chambre publique de Russie, également expert en médias, Internet « présente moins de dangers que d'autres objets que nous utilisons. Les voitures causent la mort de beaucoup plus de monde qu'Internet (…) Beaucoup commencent à voir dans Internet une panacée appelée à simplifier leur vie. Le web ne simplifie pas notre vie, il crée des conditions nouvelles et exige que les gens changent et évoluent ».

Une réglementation comme le Code de la route est cependant impossible à mettre en place sur la toile, l'anonymat étant à la portée de tous sur Internet. La diffusion de l'information et la responsabilisation des usages apparaissent alors comme la plus fiable des solutions. Et tandis qu'il suffit d'ajuster son comportement aux risques et aux menaces d'Internet, « il vaut mieux prévenir que guérir » n'a jamais été aussi adapté.

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

Source : http://www.generation-nt.com/live-streaming-illegal-donnees-actualite-1909470.html
par Julien Hatier

Après le piratage, les employés de Sony reçoivent un email de menaces – L'Express avec L'Expansion

Après le piratage, les employés de Sony reçoivent un email de menaces – L'Express avec L'Expansion

Une semaine après s'être fait pirater, la société Sony Pictures a indiqué que ses employés avaient reçu un email de menaces d'un groupe de pirates informatiques. Le FBI enquête sur le dossier.

Les attaques viennent de toutes parts. Des employés de Sony Pictures, qui a fait l'objet la semaine dernière d'une attaque informatique massive, ont reçu un email de menaces qui se dit être du groupe de pirates informatique GOP (« Guardians of Peace ») a indiqué un porte-parole de la société américaine.
Il assure par ailleurs être « au courant du problème et travailler avec les forces de l'ordre ». Le FBI, la police fédérale américaine, enquête sur le dossier.

Les familles des employés aussi menacées
L'attaque informatique, qui s'est traduite par le vol de données personnelles d'employés de Sony, dont leurs adresses, dates de naissance et numéro de sécurité sociale, et la mise en ligne illégalement de cinq films du studio, a touché quelque 47 000 personnes, selon des experts informatiques.

L'email adressé aux employés est reproduit par Variety. Il ordonne à son destinataire d'envoyer son nom à une adresse email « si vous ne voulez pas faire l'objet de représailles ». « Si vous ne le faites pas, non seulement vous mais votre famille serez en danger », précise le message.

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

Source : http://lexpansion.lexpress.fr/high-tech/apres-le-piratage-les-employes-de-sony-recoivent-un-email-de-menaces_1629800.html

L’attaque informatique de Sony Pictures a touché 47.000 personnes

L’attaque informatique de Sony Pictures a touché 47.000 personnes

Les pirates informatiques responsables de la cyberattaque géante de Sony Pictures ont dévoilé des informations confidentielles de 47.000 individus dont des personnalités, ont affirmé vendredi des experts en sécurité informatique.

Les noms, adresses, numéros de sécurité sociale et dates de naissance ont ainsi été dérobés, autant d’informations permettant des usurpations d’identité, selon la société Identity Finder.
« Le plus inquiétant est le nombre très élevés de copies des numéros de sécurité sociale retrouvés dans les dossiers que nous avons analysés », a fait remarquer le président de cette société, Todd Feinman.
Il a précisé que ces numéros apparaissaient dans plus de 400 documents différents, « offrant aux pirates la possibilité de causer davantage de dégâts ». Selon lui, quelques 15.000 personnes, actuels ou anciens employés de Sony, ont eu leur numéro de sécurité sociale dérobé.
Sony Pictures a confirmé cette semaine avoir été victime d’un vol « très important de données confidentielles » fin novembre. En plus de ces informations confidentielles, cinq films, y compris des films pas encore sortis, avaient été piratés.

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

Source : http://www.jeanmarcmorandini.com/article-329895-l-attaque-informatique-de-sony-pictures-a-touche-47000-personnes.html

---

Seules 100 personnes sont responsables de la

cybercriminalité dans le monde

Seules 100 personnes sont responsables de la cybercriminalité dans le monde

Selon le Centre de lutte contre la Cybercriminalité d'Europol, il n'y aurait qu'une centaine de personnes responsables de la cybercriminalité dans le monde.

Ce chiffre reflète effectivement la réalité de l'industrialisation de la cybercriminalité d'aujourd'hui, à laquelle sont confronté les entreprises, les Etats et les individus. Ainsi, seul un tout petit nombre de programmes permettant d'exploiter des failles logicielles connues (exploits) et d'outils en matière de cybercriminalité sont très largement exploités par les réseaux cybercriminels professionnels dans le monde entier.
Le dernier rapport semestriel sur la sécurité de Cisco a d'ailleurs mis en évidence le fait que le nombre de kits d'exploits a chuté de 87% depuis que le créateur présumé de Blackhole a été arrêté en 2013. Cela montre à quel point ce kit a largement été utilisé par la communauté cybercriminelle.

Nous savons également que les réseaux de cybercriminels sont si bien organisés qu'ils achètent désormais « clef en main » les kits d'exploits et logiciels qu'ils utilisent pour mener à bien leurs activités. La plupart du temps, ces logiciels sont même fournis avec des manuels d'utilisation et un support technique 24/7. Ensuite, les cybercriminels utilisent Internet pour mettre en place un « réseau de distribution » dans le monde entier et diffuser leurs attaques, que ce soit physiquement ou en ligne, via des réseaux de botnets.
Selon Europol, ces kits et ces malwares sont si sophistiqués qu'avec très peu d'effort ils peuvent être réutilisés maintes fois et adaptés aux cibles des cybercriminels.
Mais si ces outils sont si fréquemment et si largement répandus, pourquoi les entreprises ne parviennent-elles pas à prévenir les attaques de leurs réseaux et leurs PC?
Ceci est en partie dû au fait que les cybercriminels ont une longueur d'avance sur les responsables de la sécurité en trouvant de nouvelles variantes à leurs kits d'exploit alors que les experts en sécurité cherchent le moyen de les bloquer. Cette « course à l'armement » ne cessera jamais et nous savons même que de nombreux réseaux de cybercriminels vont jusqu'à acheter les solutions de sécurité pour tester leurs exploits afin de voir si ces dernières parviennent à les arrêter. Et, si tel est le cas, ils développent une nouvelle version de l'exploit pour la communauté cybercriminelle.
Ce que les professionnels de la cybersécurité ont bien compris depuis longtemps, c'est que les hackers sont très motivés, bien équipés et très qualifiés pour s'enrichir grâce à leurs activités illégales.
Les entreprises doivent ainsi s'assurer que leur sécurité est à jour et dispose des toutes dernières signatures, protections et solutions disponibles. Car, tandis que de nombreuses attaques sont destinées à une entreprise en particulier (attaque ciblée) , nous savons que beaucoup d'entre elles sont moins ciblées mais réussissent grâce à un manque de patching ou de mise à jour des signatures, des protections ou des solutions dont sont équipées les entreprises.
Aussi, les entreprises doivent s'assurer que leurs solutions de sécurité ne prennent pas seulement en compte uniquement la défense des postes de travail, mais qu'elles soient également capables de détecter les activités malicieuses potentielles sur l'ensemble de leur réseau – où les menaces peuvent apparaître. Il est fort probable que votre entreprise soit attaquée un jour, mais plus vite vous le saurez et vous agirez, plus vite vous pourrez déterminer l'ampleur des dommages sur votre business et sur la réputation de votre entreprise.

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

Source : http://www.huffingtonpost.fr/christophe-jolly/seules-100-personnes-responsable-cybercriminalite-mondiale_b_6248606.html