Des cybercriminels dérobent 25M$ à des banques russes

	Des cybercriminels dérobent 25M$ à des banques russes

Un groupe de cybercriminels baptisé Anunak a réussi à infiltrer les réseaux informatiques et à détourner les distributeurs automatiques d'institutions bancaires en Russie et dans des pays voisins. Il a également ciblé des terminaux point de vente de revendeurs américains et européens.

Un groupe de cybercriminels très aguerris a volé plus de 25 millions de dollars en piratant l'infrastructure de plusieurs institutions financières russes et de pays de l'ancien bloc soviétique, et en détournant des systèmes de points de vente appartenant à des revendeurs américains et européens. Des chercheurs de l'entreprise russe spécialisée dans la cybercriminalité Group-IB, et de l'entreprise de sécurité néerlandaise Fox-IT, ont baptisé le groupe Anunak, d'après le malware qui a servi de base au set d'outils utilisé par les pirates.
En général, les cybercriminels ciblent les clients des institutions financières, mais le groupe Anunak s'est attaqué directement aux institutions elles-mêmes, s'infiltrant dans leurs réseaux informatiques, jusqu'aux postes de travail et aux serveurs. Grâce à cet accès, le groupe a pu transférer des fonds sur des comptes dont ils avaient le contrôle, réussissant même dans certains cas, à détourner des distributeurs de billets automatiques sur lesquels ils ont pu ensuite retirer frauduleusement de l'argent. « Depuis 2013, ce groupe est parvenu à infiltrer les réseaux de plus de 50 banques russes et de 5 systèmes de paiement, et deux de ces institutions ont été privées de leur licence bancaire », a déclaré l'entreprise de sécurité russe Group-IB dans un rapport publié lundi. « À ce jour, le montant total du vol dépasse le milliard de roubles (environ 25 millions de dollars), la plus grande partie ayant été volée au cours du second semestre de 2014 ».

Un arsenal d'outils au service du piratage
Tout commence par l'infection des ordinateurs des salariés avec des logiciels malveillants, lesquels servent ensuite de point d'accès au réseau interne, aux serveurs et aux comptes de domaine actifs. Et le groupe Anunak ne lésine pas sur les outils : scanners de réseau, keyloggers, logiciels pour cracker les mots de passe, backdoors SSH, programmes de contrôle à distance, avec en plus, la plupart du temps, le framework Metasploit pour tester les failles et réaliser des exploits. Mais, leur principal outil est un cheval de Troie nommé Anunak. Celui-ci est basé sur le malware Carberp, conçu pour dérober des informations d'identification sur les sites de banque en ligne et dont le code source a été rendu public en juin 2013. Les chercheurs de Group-IB pensent que le groupe Anunak comprend sûrement des membres de l'ancien gang Carberp, éclaté en 2013 après des conflits internes.
Les attaquants utilisent plusieurs méthodes pour infecter les ordinateurs avec le Trojan Anunak. Par exemple, le téléchargement de logiciels malveillant quand les ordinateurs se connectent à certains sites (autrement appelé drive-by downloads) via des kits d'exploits (les chercheurs pensent que le groupe a injecté du code malveillant sur le site php.net en 2013 pour attaquer les visiteurs) ; des faux e-mails avec des pièces jointes malveillantes à en-tête de la Banque centrale de la Fédération de Russie ; l'installation d'autres programmes malveillants en utilisant les services de botnets. « Les cybercriminels sont de mèche avec plusieurs propriétaires de botnets pour diffuser massivement leurs programmes malveillants », ont expliqué les chercheurs de Group-IB. « Ils achètent aux propriétaires de botnets des informations sur les adresses IP des ordinateurs sur lesquels il y a déjà des logiciels malveillants contrôlés par le botnet et ils vérifient si les adresses IP appartiennent à des institutions financières ou gouvernementales. Si le malware du botnet se trouve dans les plages d'adresses que le groupe veut cibler, ils paient le propriétaire du réseau de zombies pour qu'il diffuse leur logiciel malveillant ».

Le vol de données de cartes de crédit confirmé
Depuis le début du second trimestre 2014, le groupe Anunak a également ciblé des revendeurs aux États-Unis, en Australie et en Europe, l'objectif étant d'infecter les terminaux points de vente avec leurs logiciels malveillants et de voler des données de cartes de paiement au moment des transactions. « Plus d'une quinzaine de violations potentielles ont été identifiées, dont une douzaine aux États-Unis, et le vol de données de cartes de crédit a été confirmé dans trois de ces cas », ont déclaré les chercheurs dans leur rapport. Le groupe a également compromis les ordinateurs de trois entreprises du secteur des relations publiques et des médias basées aux États-Unis. « Ils cherchaient peut-être des informations qu'ils pouvaient exploiter sur le marché boursier », ont déclaré les chercheurs. « Nous n'avons aucune preuve du piratage de banques en Europe occidentale ou aux États-Unis, mais les attaquants peuvent très bien utiliser les mêmes méthodes pour cibler des banques hors de Russie », ont mis en garde les chercheurs.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-des-cybercriminels-derobent-25m$-a-des-banques-russes-59699.html
Par Jean Elyan

Le site web de l’Internet System Consortium touché par un malware

Le site web de l’Internet System Consortium touché par un malware

Le site web de l’Internet System Consortium, qui édite notamment la solution BIND pour la gestion de DNS, a été victime d’un malware. Les utilisateurs qui ont visité le site web de l’ISC dans les dernières semaines sont invités à scanner leurs machines.

Le site web de l’Internet System Consortium a été temporairement mis hors ligne suite à la découverte d’une attaque ayant pu affecter les visiteurs du site. Une page statique est actuellement en ligne avec des indications nécessaires pour les utilisateurs de BIND, le serveur DNS proposé par l’ISC. L’attaque subie par le consortium n’a pas affecté les programmes publiés par l’ISC dont le code source est hébergé sur un serveur différent du site web. Selon The Register, qui a contacté un membre de l’Internet System Consortium, l’attaque n’était pas ciblée et n’a touché que le site web, qui avait recours au CMS WordPress. Une attaque automatisée « inhérente aux CMS de ce type » ajoute Dan Mahoney, responsable de la sécurité de l’ISC.
L’attaque a permis aux attaquants de rediriger certains internautes vers une page distribuant un malware windows, le Angler Exploit Kit. Celui ci est connu depuis quelques temps et exploite plusieurs failles dans Flash, Internet Explorer et SilverLight pour ensuite exécuter du code malveillant sur la machine ciblée. La finalité du malware reste encore peu connue, mais mieux vaut prévenir que guérir. Pour l’instant, l’ISC n’a pas encore signalé d’utilisateur infecté par leur site mais a préféré mettre le site hors ligne en attendant de résoudre le problème.
Plus de peur que de mal donc, mais l’ISC fait partie des sociétés vitales pour Internet : le consortium développe et maintient le code de BIND, le serveur DNS le plus largement utilisé aujourd’hui sur le réseau et héberge l’un des 13 serveurs racine du DNS. Si ces derniers ne sont pas affectés par l’attaque, les internautes et administrateurs systèmes qui ont visité le site wordpress de l’ISC avant le 22 décembre ont en revanche de quoi s’inquiéter.

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

Source : http://www.zdnet.fr/actualites/le-site-web-de-l-internet-system-consortium-touche-par-un-malware-39812011.htm
Par Louis Adam

Sony adopte de nouvelle règles de sécurité – PS4, PS3, PS Vita News – Play3-Live

	**Sony adopte de nouvelle règles de sécurité**

Comme nous avons pu le voir depuis quelques jours, ni Sony, ni Microsoft ne sont à l'abri d'action malveillante de la part d'un certains groupe d'individus mal intentionné. Suite aux différents hacks dont il fut victime récemment, Sony se rend compte qu'une protection en ligne appropriée est nécessaire pour garder les clients et les parties prenantes heureuses, ils sont donc dans l'optique d'une embauche d'un nouveau directeur du management d'ingénierie en vulnérabilité pour prévenir d'autres incidents.

L'offre d'emploi stipule que le candidat retenu sera responsable de ce qui suit:
• Unifier et améliorer l'architecture de sécurité mondiale du groupe, inclure une stratégie de gestion de la vulnérabilité cohérente englobant toutes les sociétés du groupe Sony
• Servir en tant qu'expert technique référent en matière de sécurité et conseiller pour les initiatives prioritaires de sécurité
• Gérer les équipes d'ingénieurs et développeurs hautement qualifiés, conduire et orienter la pensée, le développement de carrière, le mentorat et les conseils techniques
• Superviser l'élaboration de systèmes de gestion de la vulnérabilité, des initiatives, intégration et l'assistance d'évaluation technique
• Diriger des équipes et coordonner les efforts ou initiatives concernant les tests de pénétration, le système et la gestion de la vulnérabilité de l'application, l'évaluation globale des risques techniques, et les opérations de chasse
• Développer et affiner des normes techniques de sécurité de l'information, des directives et de la formation
• Soutenir la coordination des activités de planification budgétaire de l'entreprise liées à des outils d'information et de services de sécurité, afin d'inclure le leadership des activités de planification d'entreprise de milieu de gamme
• Appuyer la gestion, la planification et l'exécution du budget de l'ingénierie de la sécurité mondiale
• Assembler et entraîner divers ensembles de l'information et des intervenants experts sécurité dans la formulation des exigences de sécurité de l'information unifiée et des normes d'architecture pour la plupart des projets et contrats du groupe
• Servir en tant qu'expert en la matière fournissant des services consultatifs intra-entreprise liés à la stratégie de l'architecture de sécurité et de mise en œuvre de la technologie
Vous l'aurez compris, Sony semble apprendre de ses erreurs et chercher une pointure dans le domaine de la sécurité afin de ne plus être victime des soucis rencontrés il y a quelques heures encore.

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

Source : http://www.play3-live.com/news/sony-adopte-de-nouvelle-reegles-de-seecuritees-70376

DDoS du PSN – Nous avons discuté avec un membre de Lizard Squad

	DDoS du PSN – Nous avons discuté avec un membre de Lizard Squad

Après trois jours de coupure, de connexion impossible et d'erreur de maintenance, le PSN semble, ce matin, plutôt accessible pour la plupart des joueurs autant sur PS4 que PS3 et PS Vita. Hier, dans la soirée, un membre de Lizard Squad a souhaité rentrer en contact avec nous, pour nous proposer quelques informations. Nous avons donc pu discuter par message écrit avec @AironeHD, qui nous en dit plus sur les causes du DDoS du PSN de Sony, et la durée souhaitée des coupures de ce même PSN.

Lizard Squad veut montrer l'incompétence de Sony

Ce qui ressort de notre interview avec l'un des contributeurs français de Lizard Squad est que le groupe de hackeur ne souhaite pas faire de mal aux joueurs. Non, la motivation est de prouver que Sony est incompétent dans sa gestion du PSN : « Nous ne sommes pas méchants nous voulons simplement « troller » ces chefs incompétents, incapables de protéger des serveurs alors qu'ils ont les moyens financiers pour le faire. » Nous apprenons également au cours de l'interview que le souhait premier de Lizard Squad n'est pas de pirater les comptes PSN et Xbox Live pour récupérer des données personnelles et bancaires, mais simplement de bloquer les serveurs online.

Lorsque nous avons demandé à AironeHD quel était le motif des attaques, celui-ci nous a répondu : « Montrer tout simplement aux chefs de Sony (avant, Microsoft également, mais plus maintenant) que leurs systèmes de sécurité sont faibles. Et que tout le monde (informaticien assez doué) peut rentrer dans leurs systèmes. Et que l'on soit connus pour nos actes. »

Le PSN sera perturbé tant que Sony ignorera Lizard Squad

Nous avons ensuite demandé à AironeHD combien de temps allait durer les coupures régulières du PSN. La réponse est claire et non équivoque : « C'est une durée indéterminée, impossible de vous dire pour l'instant. On ne compte pas lâcher. Les chefs de Sony essayent de nous ignorer. Alors nous continuons. » Enfin, nous avons tenté de savoir pourquoi le Xbox Live était moins perturbé que le PSN. Le membre de Lizard Squad déclare vaguement que les attaques échoueraient assez souvent, et qu'il était donc plus compliqué de mettre à terre le Xbox Live que le PSN. Pour les indisponibilités des serveurs EA et Activision (FIFA et Call of Duty: Advanced Warfare), les actes de Lizard Squad sont simplement du « troll » selon AironeHD.

N.B – Cette interview avec un membre présumé de Lizard Squad en France est à but uniquement informative. Tout comme les autres membres du groupe de hackeur sur Twitter, nous ne pouvons pas prouver l'implication de AironeHD dans les attaques DDoS du PSN via des pièces justificatives. Ces déclarations ne sont donc pas des preuves, mais un bon aperçu de ce que souhaite vraiment faire Lizard Squad. Merci de votre compréhension.

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

Source : http://playerone.tv/news/v/6352/ddos-du-psn-nous-avons-discut%C3%A9-avec-un-membre-de-lizard-squad.html

---

La Corée du Nord totalement coupée d'Internet

La Corée du Nord totalement coupée d'Internet

Quelques jours après que les Etats-Unis ont accusé le régime nord-coréen d'être à l'origine du piratage informatique de Sony Pictures, plusieurs analystes rapportent, lundi 22 décembre, que les connexions Internet en Corée du Nord sont très mal en point, le résultat d'une possible cyberattaque.

Selon la société américaine Dyn Research, spécialisée dans la cybersécurité, les connexions Internet entre la Corée du Nord et le reste du monde ne fonctionnent plus. Doug Madory, chargé des questions internet, explique à l'AFP :
« En général, on détecte de courtes interruptions, mais jamais de problèmes continus de connexion. Je ne serais pas surpris qu'ils soient en train d'encaisser une attaque à l'heure actuelle. »
Interrogée par le New York Times, CloudFlare, une compagnie similaire installée à San Francisco, rapporte que le peu de connexions qui existent en Corée du Nord – officiellement, il y a 1 024 adresses IP selon le régime – sont « cramées ». Ils n'écartent pas un problème technique majeur de routeurs pour expliquer la disparition subite de ces connexions, mais comme le souligne Doug Madory, cette coupure « dure depuis plusieurs heures, et empire au lieu de s'améliorer ».

« PARMI NOS RÉPONSES, CERTAINES SERONT VISIBLES, D'AUTRES PAS »
Le président américain Barack Obama a promis une réponse « proportionnée » à la cyberattaque, la plus grave jamais survenue aux Etats-Unis, sans toutefois en préciser la nature. Lors d'une interview à CNN, dimanche, il a dit qu'il « ne pense pas que cela ait été un acte de guerre [mais] un acte de cyber-vandalisme qui a été très coûteux ».
Au département d'Etat, la porte-parole adjointe, Marie Harf, a dit ne pas être en mesure de pouvoir commenter les informations sur une coupure de l'accès à Internet en Corée du Nord. L'administration Obama « examine une série d'options » pour répondre à la cyberattaque, a-t-elle poursuivi. « Parmi nos réponses, certaines seront visibles, d'autres pas », avait-elle poursuivi.
Comme le souligne le New York Times, si « l'attaque était d'origine américaine, ce que les Etats-Unis ne reconnaîtront probablement jamais, ce serait une tentative inédite des Etats-Unis d'attaquer les connexions Internet d'un pays souverain. Jusqu'ici, la plupart des opérations menées par les Etats-Unis se sont résumées à du cyberespionnage pour collecter des informations ou des communications de personnes soupçonnées de terrorisme ».
Pour le département d'Etat américain, le gouvernement nord-coréen « a une longue histoire en matière de dénégations de responsabilité » et il devrait admettre sa responsabilité, ce que Pyongyang dément fermement. Il propose une enquête conjointe avec les Etats-Unis, assure être en mesure de prouver son innocence et met en garde contre les « graves conséquences » qu'aurait la poursuite des accusations à son encontre.

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

Source : http://www.lemonde.fr/pixels/article/2014/12/22/coupure-massive-de-l-acces-a-internet-en-coree-du-nord_4545129_4408996.html

---

Des plans de réacteurs

nucléaires ont été piratés

Des plans de réacteurs nucléaires ont été piratés

Des documents internes de Korea Hydro & Nuclear Power Co. (KHNP), notamment des plans de réacteurs nucléaires sud-coréens, ont été dérobés et publiés de nouveau vers 1h30 ce dimanche sur Internet, pour la quatrième fois depuis le 15 décembre.

Un internaute, qui serait à l'origine de ces vols de données, a publié sur le réseau social Twitter des documents internes concernant le Réacteur 2 de la centrale de Kori, le Réacteur 1 de la centrale de Wolsong et le manuel informatique utilisé dans les centrales nucléaires du pays.
Le soi-disant «président du groupe antinucléaire à Hawaï» a demandé d'arrêter le fonctionnement des premier et troisième réacteurs à Kori et le deuxième à Wolsong à partir du jour de Noël, en menaçant d'effectuer une deuxième série de «destructions» si les réacteurs ne sont pas arrêtés.
KHNP a indiqué hier que la publication de ces documents qui ne contiennent pas d'informations confidentielles n'affectera pas la sécurité des centrales nucléaires dans un communiqué de presse. La société a néanmoins dit qu'elle effectuerait un exercice de simulation général contre l'éventualité d'une cyberattaque en vue de renforcer ses contre-mesures.
Le ministère du Commerce, de l'Industrie et de l'Energie Yoon Sang-jick a présidé lui aussi une réunion extraordinaire pour vérifier la cybersécurité hier matin suite à la fuite des documents internes en convoquant des chefs d'entreprises publiques spécialisées dans la production d'électricité et d'énergies, dont Korea Electric Power Corp. (KEPCO).

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

Source : http://french.yonhapnews.co.kr/national/2014/12/21/0300000000AFR20141221000200884.HTML

Le régulateur mondial

d’internet victime d’une attaque informatique

Le régulateur mondial d’internet victime d’une attaque informatique

Le régulateur mondial d’internet, l’Icann, a annoncé que des pirates informatiques avaient réussi à pénétrer dans ses ordinateurs.

Une attaque par « hameçonnage » a en effet visé l’agence américaine et plusieurs de ses employés ont reçu des courriels destinés à ressembler à ceux envoyés par un de leurs collègues avec une adresse se terminant en « icann.org », selon le blog de l’Icann.

« Plusieurs employés ont vu leurs références dérobées », a précisé l’agence.
L’attaque a, semble-t-il, commencé en novembre. Typiquement, les attaques par hameçonnage sont destinées à duper les gens en les conduisant à cliquer sur des pages factices où ils rentrent leurs adresses et mots de passe, qui sont ainsi récupérés par les pirates informatiques.
Cette ruse a permis aux hackers de récupérer les adresses et mots de passe de plusieurs employés de l’Icann. Ils ont donc pu s’introduire plus avant au sein du système informatique de l’organisation.
Ils ont ainsi pu pénétrer dans des serveurs sécurisés où ils ont récupéré des dossiers sur des noms de domaines, des adresses et des mots de passe d’utilisateurs, a encore indiqué l’Icann.
Le blog et l’annuaire n’ont pas été trafiqués, a encore noté l’Icann sans préciser qui pourrait être à l’origine de l’attaque.
L’Icann, dont la mission est d’attribuer les noms de domaines des sites internet, devrait quitter le giron américain en fin d’année prochaine. Washington a en effet annoncé en mars qu’il pourrait ne pas renouveler son contrat avec la société basée à Los Angeles si un système de contrôle indépendant est en place pour assurer la fiabilité du système d’attribution des adresses.

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

Source : http://www.7sur7.be/7s7/fr/4134/Internet/article/detail/2156470/2014/12/18/Le-regulateur-mondial-d-internet-victime-d-une-attaque-informatique.dhtml

---

Une attaque informatique endommage une usine métallurgique allemande

Une attaque informatique endommage une usine métallurgique allemande

Un rapport allemand publié jeudi a révélé une attaque informatique inédite contre une usine métallurgique. Le piratage a provoqué d'importants dégâts matériels sur un haut fourneau.

Une usine métallurgique allemande a subi une cyberattaque qui a provoqué des dégâts matériels conséquents, a révélé jeudi la publication d'un rapport gouvernemental allemand, cité par le site ITworld.
Les pirates ont pris le contrôle du réseau de l'usine après avoir obtenu les informations nécessaires à l'aide de techniques sophistiquées d'ingénierie sociale.
L'attaque a provoqué la défaillance de plusieurs composants qui ont empêché l'arrêt contrôlé d'un haut fourneau, endommageant l'infrastructure.

« Techniques très avancées »
Selon le rapport – qui ne donne ni le nom de l'usine, ni la date de l'attaque – les hackers disposaient de capacités techniques « très avancées » et ont démontré maîtriser également les processus de production et de contrôle industriels.
ITworld souligne que des intrusions à l'origine de tels dégâts restent rares, citant le ver Stuxnet qui avait visé les capacités de recherches nucléaires iraniennes, détruisant près de 1000 centrifugeuses.

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

Source : http://www.rts.ch/info/sciences-tech/reperages-web/6399258-une-attaque-informatique-endommage-une-usine-metallurgique-allemande.html

---

Cryptolocker : quand un virus prend vos données en otage contre rançon

Cryptolocker : quand un virus prend vos données en otage contre rançon

Depuis quelques jours, une campagne d'attaque utilisant CryptoLocker (logiciel malveillant de type cheval de Troie) semblerait être en cours. La société d'antivirus Trend Micro a été alertée par de nombreux appels et messages de la part de ses clients et partenaires. Loïc Guézo, évangéliste Sécurité de l'Information pour l'Europe du Sud chez Trend Micro et administrateur du Clusif, livre quelques pistes pour lutter contre ce ransomeware (logiciel malveillant prenant les données personnelles de l'utilisateur en otage) particulièrement nuisible.

Vous cliquez sur le lien d'un e-mail reçu. Le fond d'écran change. Une fenêtre s'ouvre. Un avis apparaît, vous informant que vos fichiers importants sont cryptés. Vous tentez de cliquer ailleurs. Impossible de quitter la fenêtre. L'écran est verrouillé. Un cauchemar nommé « Cryptolocker ».
Ce « ransomware » (ou rançongiciel) est un logiciel malveillant qui piège l'ordinateur de ses victimes et prend en otage leurs données personnelles. Il est précisé que le chiffrage des données du disque par le logiciel malveillant les rend inutilisables jusqu'au versement de la rançon demandée. Le pirate promet de fournir la clé capable de déchiffrer les données en échange d'une somme de quelques centaines d'euros, à régler en ligne via Paypal ou un virement en bitcoins. Le tout avec un compteur de temps bien visible, qui signifie que la décision doit être prise rapidement.
Bien sûr une clé unique est utilisée pour chaque machine piégée. Si la rançon demandée n'est pas versée dans le temps imparti, la clé de chiffrement ne sera pas communiquée et les données chiffrées définitivement perdues. Et si la rançon est payée, rien ne garantit pour autant la suite des opérations…
Ce scénario digne d'un thriller a fait son apparition fin 2013 et revient en force depuis quelques semaines. S'il est encore trop tôt pour connaître précisément le nombre de systèmes infectés par le programme malveillant, Le Monde Informatique du 6 janvier 2014 rapporte que Cryptolocker 2.0 aurait infecté 200 à 300 000 PC et qu'environ 0,4 % des victimes ont probablement payé la rançon réclamée, même si payer ne garantit absolument pas le déblocage du système.
Ce banditisme virtuel est basé sur un chantage avec comme otage les données de la victime. Il a été jugé suffisamment grave pour que des policiers, spécialement formés, enquêtent pour retrouver ces malfaiteurs du Net et les poursuivent. Des unités spéciales américaines et européennes ont, par exemple, travaillé ensemble et uni leurs efforts pour démanteler le 2 juin dernier le réseau criminel GameOver Zeus qui, entre autres, pouvait distribuer Cryptolocker.

L'INGÉNIERIE SOCIALE, VECTEUR DE L'INFECTION
Les malfaiteurs s'appuient sur des techniques d'ingénierie sociale. Ils procèdent à l'envoi initial de leurres sous forme de vagues d'e-mails ciblés. D'où l'importance de vérifier la légitimité de chaque message. Il convient de toujours faire preuve d'une extrême prudence lorsque nous ouvrons la pièce jointe à un message électronique dont la source nous est inconnue.
Ce sont principalement aujourd'hui les utilisateurs de PC qui sont visés (des versions visant les mobiles apparaissent déjà). Mais le point de départ est bien le geste de l'utilisateur lui-même, piégé par un message avec pièce jointe. L'hameçon psychologique est celui de l'inquiétude naturelle, de la surprise ou de l'intérêt du destinataire du message. Il peut s'agir de faux courriers paraissant provenir d'un organisme social, d'une banque, d'une assurance, d'e-commerçants, de logisticiens ou de transporteurs, etc. La pièce jointe est censée être un document lié à un litige, une facture impayée, un avis de livraison en suspens, un remboursement sur trop-perçu…
L'éducation et la vigilance des utilisateurs isolés sont donc indispensables. Sur un réseau d'entreprise, l'information d'alerte doit être donnée et pourra plus facilement être souvent répétée : « n'ouvrez pas les mails de provenance inconnue sans vérification, ne cliquez jamais sur un lien si vous avez le moindre doute », etc.

COMMENT SE DÉFENDRE ET PRÉVENIR LE BLOCAGE ?
Il existe plusieurs moyens pour gérer cette menace, tant pour les particuliers que pour les entreprises. Il a été largement démontré que la sécurité basée sur les signatures a atteint ses limites, mais il existe cependant d'autres solutions avec des fonctions d'alerte plus évoluées. Ce sont par exemple des solutions basées sur les éléments environnementaux (comme la réputation d'adresses IP, les noms de domaine…). Un service de réputation va en particulier permettre de bloquer l'accès à certaines adresses IP correspondant à des C&C de botnets, empêchant tout simplement le Cryptolocker de s'initialiser et donc de chiffrer la cible !
Revoir la politique de sécurité des pièces jointes est urgent pour de nombreuses entreprises. L'adoption des bonnes pratiques permettra d'éviter une contamination très rapide.
Posons-nous les bonnes questions pour contrer Cryptolocker. Est-ce que l'entreprise dispose bien d'une politique de blocage des pièces jointes aux messages, empêchant par exemple le déclenchement d'un fichier exécutable ? Peut-on analyser « en amont » le comportement des pièces jointes ? Utilise-t-on un service avancé de réputation ? Surveille-t-on le comportement des pièces jointes sur la durée? A-t-on simplement le moyen de contrôler que la solution de sécurité reste activée ? Ces quelques premières précautions permettront d'éviter les catastrophes, en particulier pour les PME.
Il faut bien sûr toujours être sur ses gardes, ne pas négliger de mettre à jour les logiciels de sécurité installés et vérifier que le navigateur utilise la réputation de sites Web avant de cliquer sur un lien ou bien utiliser un service gratuit comme Trend Micro Site Safety Center.
Quant aux grandes entreprises, qu'elles se préparent à recevoir des attaques type Cryptolocker mais désormais ciblées. Et bien sûr, toujours communiquer en interne sur les risques, et communiquer, c'est répéter…

LES SYSTÈMES INFORMATIQUES DOIVENT ÊTRE PRÉPARÉS POUR RÉSISTER
On ne soulignera jamais assez que la formation des utilisateurs, la mise à jour régulière des logiciels et de bonnes pratiques d'utilisation de l'ordinateur individuel restent le socle de défense contre Cryptolocker ou toutes les nouvelles menaces similaires. Il est désormais nécessaire d'introduire des outils d'analyses plus complets (vision en temps réel de la menace ou exécution en environnement contrôlé – sandboxing – par exemple).
Si les cybercriminels perfectionnent chaque jour leurs logiciels malveillants qui deviennent ainsi de plus en plus sophistiqués, alors les systèmes informatiques doivent également être préparés pour résister mais surtout être cyber-résilients face à ces attaques. Cette lutte doit être globale pour non seulement réduire le taux de l'infection, mais également briser la chaîne de transmission des logiciels malveillants par une stratégie de défense en profondeur, y compris lors de son déroulement.
L'autre aspect fondamental reste la lutte policière et judiciaire contre ces nouvelles formes de criminalité dont les dernières semaines ont montré l'ampleur et le dynamisme.

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

Source : http://www.usine-digitale.fr/article/cryptolocker-quand-un-virus-prend-vos-donnees-en-otage-contre-rancon.N302748
par Loïc Guézo, Evangéliste Sécurité de l'Information pour l'Europe du Sud chez Trend Micro & Administrateur du Clusif

---

Ce que révèlent les milliers de documents confidentiels volés à Sony Pictures

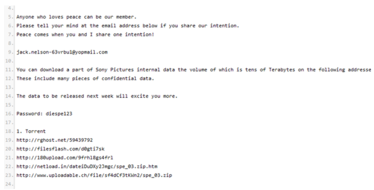
Ce que révèlent les milliers de documents confidentiels volés à Sony Pictures

Des centaines de gigaoctets de fichiers ont déjà été diffusés par des pirates. Une situation catastrophique pour le géant du divertissement hollywoodien.

Imaginez que toutes les données – ou presque – qui transitent sur votre ordinateur de travail, stockées sur les disques durs et serveurs de votre entreprise, soient compilées et rendues accessibles à tous. Voilà la situation devant laquelle se retrouvent actuellement les employés et la direction de Sony Pictures Entertainment, après l'attaque informatique de grande ampleur subie le 24 novembre. Depuis, des milliers de gigaoctets de fichiers confidentiels du géant du divertissement hollywoodien, producteur et diffuseur de nombreux films, sont dispersés sur le Web.

Un mécanisme bien rodé

Les pirates, réfugiés derrière l'acronyme #GOP (pour Guardian of Peace), avaient au départ évoqué onze terabytes de documents (11 000 gigaoctets) subtilisés lors de leur attaque. Ils parlent maintenant de « dizaines de térabytes » de données – une centaine, disent les médias américains. Qu'un tel volume de données ait effectivement été volé semble de plus en plus probable.
Les documents internes de Sony Pictures publiés (fichiers Excel, Word, Powerpoint, PDF, etc.) se comptent déjà par centaines de milliers et en dizaine de gigaoctets, selon un décompte fiable établi par l'entreprise spécialisée en sécurité informatique Risk Based Security.
Le processus de diffusion est toujours le même. Des liens permettant de télécharger des fichiers RAR ou ZIP volumineux, par des sites de téléchargement direct ou grâce à des fichiers torrent, apparaissent sur l'éditeur de texte en ligne Pastebin, qui assure un certain anonymat à leurs auteurs. Les hackers envoient ensuite le lien du document Pastebin par e-mails à leurs contacts, soit n'importe qui ayant signifié son intérêt pour les documents Sony Pictures en écrivant aux adresses anonymes et temporaires que les membre de GOP diffusent régulièrement (journalistes, sympathisants des hackers, entreprises de sécurité informatique, enquêteurs, concurrents…).


Anyone who loves peace can be our member.
Please tell your mind at the email address below if you share our intention.
Peace comes when you and I share one intention!

jack.nelson-63vrbu1@yopmail.com

You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresse
These include many pieces of confidential data.

The data to be released next week will excite you more.

Password: diespe123

1. Torrent
http://rghost.net/59439792
http://filesflash.com/d0gti7sk
http://180upload.com/9frhl8gs4frl
http://netload.in/dateiDuDXy2Jmgc/spe_03.zip.htm
http://www.uploadable.ch/file/sf4dCf3tKWn2/spe_03.zip

Extrait d'un message donnant accès aux fichiers volés à Sony Pictures Entertainment. | Pastebin

Les données sont ensuite accessibles pendant quelques heures, avant la désactivation des liens de téléchargement par les hébergeurs et la suppression du document Pastebin – vraisemblablement sur requête des autorités ou de représentants légaux de Sony. Entre le 24 novembre et le 10 décembre, six « livraisons » de ce type ont eu lieu. Les pirates, maniant le sens du teasing, en promettent à chaque fois davantage : « les données que nous publierons la semaine prochaine vous exciteront encore plus », annonçait par exemple un document Pastebin publié le 5 décembre.

Un chantage pécuniaire ?

Les textes diffusés par les hackers qui accompagnent la publication de ces fichiers n'en disent en revanche que peu sur les motivations réelles justifiant cette fuite massive et organisée. La piste de la Corée du Nord, qui agirait en représailles au film The Interview parodiant le régime de Kim Jong-un, est accréditée par des similarités constatées entre l'attaque du 24 novembre et celle subie par la Corée du Sud en 2013. Mais l'un des cadres du FBI, officiellement chargé de l'enquête, a confié le 9 décembre qu'il n'était pour l'instant pas possible d'en attribuer la responsabilité à Pyongyang.
Dans un document publié le même jour, les membres proclamés des GOP demandent bien à Sony d'« arrêter immédiatement de diffuser un film sur le terrorisme qui peut mettre fin à la paix régionale et causer une guerre », sans nommer le film en question, et reprenant une rhétorique déjà servie auparavant à The Verge. Mais ils signalent également avoir « formulé une demande claire à l'équipe dirigeante de Sony », encore une fois sans préciser laquelle :

« Ils ont refusé de l'accepter. On dirait que vous pensez que tout se passera bien, si vous trouvez les attaquants et ne réagissez pas à notre demande. Nous vous avertissons à nouveau. Répondez à ce que nous vous demandons si vous voulez nous échapper. »

De quoi donner du crédit à l'hypothèse d'une tentative d'extorsion de fonds de la part des hackers de « Guardian of Peace ». Ce motif a d'ailleurs été clairement exposé dans un e-mail envoyé aux dirigeants de Sony Pictures quelques jours avant l'attaque : « Nous avons de quoi causer beaucoup de tort à Sony Pictures. (…) Nous voulons une compensation monétaire. Payez, ou Sony Pictures sera frappé dans son ensemble. »

La diffusion au compte-gouttes des documents confidentiels constituerait, dans ce contexte, un moyen de pression supplémentaire pour obtenir cette « compensation », de nature à alimenter un feuilleton médiatique dévastateur pour Sony Pictures. Les médias du monde entier ont ainsi repris :

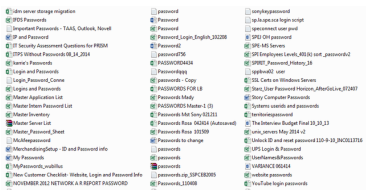
Les données privées de célébrités

Des adresses postales, des numéros de téléphone, des adresses électroniques, ou encore le numéro de sécurité sociale de Sylvester Stallone, contenus dans les documents liés aux films et séries de Sony Pictures ont été rendus publics. Parmi ces informations, on trouve les pseudonymes utilisés par Tom Hanks, Natalie Portman ou encore Ice Cube pour conserver un peu de tranquillité (lors d'une réservation d'hôtel par exemple).
Ont également été publiés une cote de popularité des acteurs pays par pays, ou encore les sommes d'argent perçues par Seth Rogen et James Franco pour le film The Interview. Le premier aurait reçu 8,4 millions de dollars pour avoir coréalisé et interprété l'un des rôles principaux, le second 6,5 millions : des divulgations auxquelles ils ont réagi avec humour.


L'affiche de « The Interview ». | Sony Pictures

Les données privées des salariés et partenaires de Sony Pictures

Numéros de téléphone, CV, photos d'identité, montants de salaires, demandes d'augmentation, e-mails, planning de vacances, factures médicales… Autant d'éléments propres à la vie interne d'une structure qui emploie près de 7 000 personnes aux Etats-Unis, et qui a collaboré avec de très nombreuses personnes ces dernières années – stagiaires, prestataires ou partenaires directs au sein d'entreprises rachetées par Sony, comme Columbia Pictures. Ces détails apparaissent notamment dans un dossier intitulé « Ressources humaines », et se trouvent aussi dans des documents de travail liés aux tournages de films et de séries Sony.
Encore plus grave, de très nombreux mots de passe utilisés par les employés pour se connecter à tous types de services (propres à Sony Pictures, mais aussi ailleurs sur Internet) font partie des publications. Comme le note cruellement Gizmodo, ils étaient stockés sur les disques durs de Sony Pictures dans des fichiers Word et Excel sans protection, et dans un dossier appelé « Mot de passe ».



Les mots de passes de Sony Pictures. | Risk Biaised Security

De quoi pousser d'anciens employés à réfléchir à une plainte collective, arguant du manque flagrant de sécurité du réseau de l'entreprise. « Il y a des raisons de penser qu'il y a eu une grosse négligence de la part de [Sony Pictures]. Nous nous inquiétons tous concernant notre vie privée, et nos familles », a déclaré l'un d'entre eux à Fox News, après avoir vu diffuser son passeport, son visa, son numéro de sécurité sociale et ses contrats passés avec l'entreprise.
Des avocats californiens incitent également les salariés actuels à se lancer dans de telles procédures. Particulièrement exposés, ils se sont vus en plus directement menacés dans un e-mail leur étant adressé. « Tout le monde panique, et personne ne sait quoi faire », a témoigné l'un d'eux sur le site Fusion, décrivant une hostilité grandissante au sein de Sony Pictures à l'encontre du service informatique. Le FBI, chargé de l'enquête, devrait faire le point devant les employés sur le comportement à adopter face à cette situation le 12 décembre.
Les dirigeants de Sony Pictures ne sont pas épargnés. L'un des premiers documents diffusés par le site d'information Fusion dresse le détail des rémunérations des 17 salariés les mieux payés, à commencer par le dirigeant Michael Lynton (3 millions de dollars par an) – une seule femme dans ce palmarès. Parmi les fichiers publiés figurent des sauvegardes de plusieurs mois de conversations par courriels (professionnels et personnels) issues des messageries Outlook de cadres de l'entreprise : Amy Pascal, vice-présidente de Sony Pictures, Steve Mosko, à la tête de Sony Television, ou encore Leah Weill, conseiller juridique en chef.

Des révélations sur les films et les séries Sony

Dans son ensemble, cette masse de données fourmille d'informations sur la manière dont Sony Pictures gère son catalogue, ses productions et ses projets. Finances de l'entreprise, projets marketing, bilans comptables liés aux séries diffusées à la télévision américaine, rétrospectives annuelles, bases de contacts, documents préparatoires pour des négociations… Ces milliers de fichiers bruts s'accompagnent de visées stratégiques, comme en témoignent les points de vue exprimés par des employés (s'énervant par exemple contre l'omniprésence d'Adam Sandler à l'écran).
Dans ces documents se nichent ainsi, fatalement, des informations propres aux films et aux séries télévisées estampillées Sony. On y apprend par exemple comment les dirigeants de Sony Pictures ont fait modifier la fin du film The Interview (attention spoiler !), et négocié avec Marvel, qui souhaitait que Spiderman apparaisse dans le prochain Captain America. Plus problématique, des scripts inédits d'épisodes de séries, et même de films devant sortir en 2015, ont été repérés.
Plusieurs médias, comme le Wall Street Journal, ont également extrait diverses phrases chocs des e-mails échangés ces dernières années par la vice-présidente Amy Pascal avec le tout-Hollywood (réalisateurs, agents, stars, etc.). On y trouve quelques commentaires désobligeants sur des acteurs : Angelina Jolie et son « ego devastateur » en prennent pour leur grade. Ou encore, une chronique détaillée des négociations et conversations, parfois brutes de décoffrage, entourant le biopic sur Steve Jobs sur lequel Sony travaille depuis trois ans (notamment sur les choix de casting du scénariste Aaron Sorkin, qui avait songé à Tom Cruise pour incarner le fondateur d'Apple).

En savoir plus sur http://www.lemonde.fr/pixels/article/2014/12/11/ce-que-revelent-les-milliers-de-documents-confidentiels-voles-a-sony-pictures_4537271_4408996.html#Ox8W3PwS6l8JJu0T.99
Par Michaël Szadkowski journaliste à Pixels

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

Source : http://www.lemonde.fr/pixels/article/2014/12/11/ce-que-revelent-les-milliers-de-documents-confidentiels-voles-a-sony-pictures_4537271_4408996.html
par Par Michaël Szadkowski