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

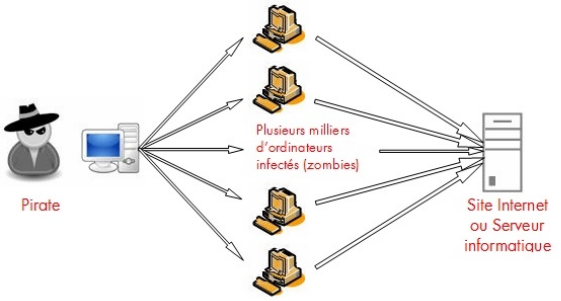
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

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

Dis papa, c'est quoi une attaque DDOS ?

Dis papa, c'est quoi une attaque DDOS ?

L'objectif d'une attaque DDOS, (en déni de service) vise à rendre inaccessible ou inopérant un site Internet. Parmi les attaques les plus fréquemment lancées, ce sont les attaques en déni de service distribué (DDoS : Distributed Denial of Service) qui sont les plus fréquentes.
Ce type d'attaque s'appuie sur un principe simple, celui du nombre qui fait la force : Il suffit de faire en sorte que plusieurs milliers machines sur Internet lancent de façon synchronisée de multiples requêtes vers leur cible.
Les machines lançant ces attaques peuvent le faire soit à l'insu de leur propriétaire (cas d'un « botnet » ou réseau de machines zombies) ou alors le font sur demande explicite et consciente d'une personne (cyber hacktivisme).



Le pirate active à distance tous les zombies (plusieurs milliers) préalablement infectés et leur donne l'ordre de contacter simultanément une cible. Au bout de quelques minutes, cette cible ne peut plus répondre à de nouvelles connexions, elle devient inaccessible.

Saturation des ressources
Dans le deux cas, le résultat est le même : les capacités de traitement du site sont dépassées, celui-ci est inaccessible. La saturation peut concerner tant la bande passante de l'accès réseau, des tables de session d'un firewall, la CPU des serveurs web, …
En fonction du point de saturation, on peut constater un effet boule de neige : Si c'est la bande passante réseau qui est totalement consommée inutilement alors, non seulement le site visée par l'attaque sera bloqué mais tous les autres serveurs de la plateforme seront aussi inaccessibles.

Le trou-noir (« blackholing ») à la rescousse
Le trou-noir est l'une des contre-mesures utilisée communément pour contrer une attaque en DDoS. Le fournisseur d'accès Internet va activer, au sein de son réseau, une règle de routage spécifique afin de détruire tous les flux à destination de l'adresse IP ciblée par l'attaque.
Cela aura pour effet immédiat de bloquer les flux d'attaques en amont de l'accès réseau et donc d'annuler tout effet de saturation. Activer un blackholing ne nécessite aucun équipement spécifique car tout est réalisé via les fonctions de routage de paquets nativement présentes dans les équipements réseau.

Pour se protéger d'une attaque de ce type, plusieurs solutions existent, le blackholing en est une, la plus simple à mettre en oeuvre, mais comme à chaque fois, quand le voleur s'est fait piéger en rentrant par la porte, la prochaine fois il rentrera par la fenêtre ou ailleurs…

Vous avez été victime d'une attaque DDOS ?
Vous souhaitez mettre en oeuvre une protection ?
Profitez de notre expertise et consultez-nous

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

Source : http://www.orange-business.com/fr/blogs/securite/series/les-5-minutes-du-professeur-audenard-episode-3-cleanpipe-bgp-et-gre

---

Les sites Internet de la

Gendarmerie et de la Police attaqués par des Anonymous pour dénoncer les bavures

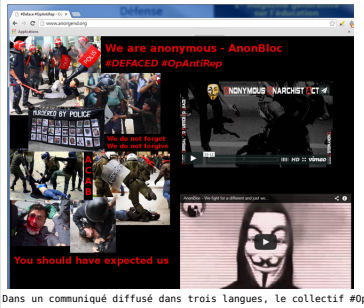
Les sites Internet de la Gendarmerie et de la Police attaqués par des Anonymous pour dénoncer les bavures

Aux manifestations organisées partout en France samedi dernier contre les violences policières se sont jointes des opérations menées en ligne par un collectif affilié à Anonymous. Des bases de données sur des Gendarmes ont été publiées, et des sites ont été piratés.

Les manifestations en hommage à Rémi Fraisse et contre les violences policières qui se sont déroulées samedi dernier dans une vingtaine de villes françaises ont également connu un relais immatériel. Dans le cadre d'une action mondiale « contre les répressions policières » baptisée #OpAntiRep, un collectif de hackers anonymes utilisant la bannière Anonymous a réalisé samedi une série d'actions, en particulier contre les policiers et gendarmes italiens, mais également en France.

Outre d'habituelles attaques DDOS qui ont provoqué l'indisponibilité d'une vingtaine de sites internet, dont celui du syndicat de policiers Alliance http://anorgend.org, le collectif a surtout piraté le forum d'un site internet dédié aux réservistes de la Gendarmerie http://www.reserve-gendarmerie.org, destiné à « faire connaître la réserve et à mettre en relation les réservistes et candidats ». Ils affirment avoir réussi à pirater les noms, adresse e-mail, adresse IP et mot de passe (pour certains déchiffrés) de quelques 2 000 membres inscrits sur ce forum, et fournissent une capture d'écran de la base de données en guise de preuve :

Ce lundi, le site non officiel de la réserve de la Gendarmerie française était toujours fermé, un message expliquant aux visiteurs qu'il était « en maintenance ». Le forum est toutefois accessible, et affiche 1544 membres inscrits à l'heure où ces lignes ont été publiées sur le site source.
D'autres actions ont été menées, notamment contre le site de l'Association nationale des officiers de réserve de la Gendarmerie nationale (Anorgend), qui a été piraté pour en modifier la page d'accueil, désormais toute à la gloire d'Anonymous. Là aussi, une base de données de membres avec des mots de passe chiffrés a été diffusée :

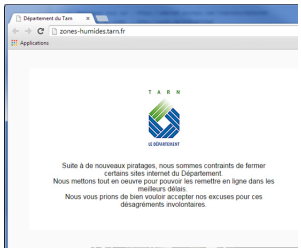


Dans un communiqué diffusé dans trois langues, le collectif #OpAntiRep explique que la journée du 22 novembre avait « pour origine des collectifs – occupants de différentes ZAD (Zones à défendre) – suite au décès par grenade offensive d'un étudiant en écologie lors d'un rassemblement », et affirme que « partout dans le monde, de nombreux camarades ont été tués ou blessés par leurs armes dans des manifestations contre l'oppression de ces gouvernements,sous la pression du monde capitaliste qui veut imposer ses projets de société ». L'appel à manifester partout dans le monde avait été relayé sur un site anarchiste.

« Nous devons informer le peuple par toutes les tactiques possibles », ajoutait le collectif Anonymous pour expliquer le sens de sa mobilisation en ligne. « Nous ne pouvons pas tolérer plus longtemps que le peuple soit mis à genoux par des robots sans âmes. Qui « servent et protègent » des machines, des institutions capitalistes et l'injustice. Nous protégeons le peuple. Nous ripostons ! ».
L'appel d'Anonymous France à agir en ligne le 22 novembre avait été lancé le 11 novembre dernier par une vidéo sur YouTube, vue près de 7000 fois :

D'autres documents ont été obtenus par les pirates, dont le plus sensible est le calendrier prévisionnel de positionnement et de relève des unités de CRS en France, dans le cadre des missions permanentes, jusqu'à la fin de l'année 2014. Le reste est plus anecdotique, avec la grille de rémunérations des CRS en fonction des grades, le règlement intérieur des compagnies, ou encore un manuel détaillé des véhicules de reconnaissance utilisés par les CRS.

Dès la fin octobre, Anonymous avait réagi à la mort de Rémi Fraisse en affirmant qu'il « ne restera pas les bras croisés », et en annonçant une « Opération Testet » (#OpTestet) pour s'opposer au barrage de Sivens sur la zone humide du Testet. S'en était suivie une série d'actions menées notamment contre le site officiel de la Région du Tarn ou celui de la FNSEA locale :



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

Source : http://www.numerama.com/magazine/31367-opantirep-anonymous-s-attaque-a-la-gendarmerie-francaise.html

---

Les ordinateurs de Sony Pictures piratés, et paralysés

Les ordinateurs de Sony Pictures piratés, et paralysés

Décidement, Sony Pictures est une cible de prédilection pour les pirates. En 2011, c'est le site du studio qui avait été compromis et des données personnelles dérobées. A présent, c'est le réseau informatique qui a fait l'objet d'une intrusion.

Comme le rapporte The Verge, les salariés des différents bureaux de Sony Pictures ont ainsi découvert une image inattendue sur l'écran de leur ordinateur au moment de se connecter à leur session.

Une entreprise paralysée
Une image représentant un squelette écarlate les informait qu'ils avaient été hacké par #GOP. Le message précise que des données sensibles de l'entreprise et ont été dérobées. Les pirates menacent d'ailleurs de les dévoiler sur Internet si leur demande n'est pas satisfaite – une ou des exigences qui ne sont pas précisées.

Les salariés de Sony Pictures étaient hier encore dans l'incapacité d'utiliser les outils informatiques, d'envoyer par exemple un mail ou même de répondre au téléphone – vraisemblablement de la ToIP.
Outre le blocage des ordinateurs de Sony Pictures, ce sont des douzaines de 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.
Une affaire de plus à suivre…

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

Source : http://www.zdnet.fr/actualites/les-ordinateurs-de-sony-pictures-pirates-et-paralyses-39810107.htm

---

Un virus informatique prend pour cible la Russie et l'Arabie Saoudite

Un virus informatique prend pour cible la Russie et l'Arabie Saoudite

Un virus informatique très sophistiqué a lancé une attaque contre des opérateurs télécoms russes et saoudiens, a révélé la compagnie de cyber-sécurité Symantec.

Ce virus, baptisé « Regin », serait au moins aussi redoutable que « Stuxnet », qui avait causé de gros dégâts en 2010 dans le programme nucléaire iranien, retardant sans doute de plusieurs années les travaux des ingénieurs iraniens soupçonnés de mettre au point des armements nucléaires…
Stuxnet avait été développé par les services secrets américains et israéliens, selon des sources concordantes.

Un voleur qui fait disparaître ses traces…
Selon le 'Financial Times', qui cite lundi des sources au sein de Symantec, Regin pourrait lui aussi avoir été mis au point par des services secrets occidentaux, et serait d'une sophistication sans précédent… On ignore encore de quelle manière le virus infecte les systèmes informatiques, mais il s'est jusqu'à présent attaqué à des fournisseurs d'accès à internet en Russie, Arabie Saoudite, au Mexique en Irlande et en Iran.
Son objectif serait de dérober des données confidentielles, et il aurait la capacité de s'adapter à tous types de réseaux. Il serait aussi capable, dans certains cas, de faire disparaître toute trace de son passage une fois son forfait accompli… Regin aurait notamment ciblé les serveurs de messageries gérées par Microsoft, ainsi que les conversations de téléphones mobiles circulant sur de grands réseaux mondiaux.

L'industrie, nouvelle cible des « hackers », selon Kaspersky
Au même moment, Eugene Kaspersky, le directeur général d'une autre firme de sécurité informatique, Kaspersky Labs, a mis en garde contre la multiplication des cyberattaques contre les systèmes de groupes industriels, notamment dans le secteur énergétique (centrales électriques…). Selon lui, l'industrie est devenue la cible privilégiée du crime organisé, avec des attaques qui vont plus loin que les récents vols de données personnelles dont ont été victimes les clients de JP Morgan, Home Depot ou Target aux Etats-Unis. Les hackers ont notamment réussi à éviter que des chargements soient contrôlés dans des ports, ou à voler des stocks de céréales dans une usine ukrainienne en falsifiant les jauges pour qu'elles affichent des poids inférieurs à la réalité, a indiqué M. Kaspersky au 'FT'…

L'an dernier, l'office de police criminelle intergouvernemental Europol avait rendu public le démantèlement d'un réseau de trafiquants de drogue, qui avaient « hacké » les ordinateurs du port belge d'Anvers… Les trafiquants étaient parvenus à déplacer les conteneurs contenant de la drogue pour leur éviter de subir des contrôles douaniers.

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

Source :
http://www.boursier.com/actualites/economie/un-virus-informatique-prend-pour-cible-la-russie-et-l-arabie-saoudite-26186.html

Une ville victime de Cyberattaques. Ottawa ciblée, Toronto menacée

Une ville victime de Cyberattaques. Ottawa ciblée,

«Anonymous» attaque le site de la Ville d'Ottawa
Un pirate informatique qui dit faire partie du groupe Anonymous a menacé dimanche de cibler les sites web appartenant à la Ville et à la police de Toronto.

Cette menace en ligne provient d'un présumé pirate appelé Aerith. Il s'agit du même internaute qui aurait paralysé le site internet de la Ville d'Ottawa, vendredi soir. La page en question affichait alors une image d'une banane dansante et un message menaçant envers un policier d'Ottawa.

Aerith a également revendiqué les problèmes informatiques ayant paralysé ce week-end le site web de la police d'Ottawa. De samedi soir jusqu'à tôt dimanche matin, le site ottawapolice.ca était complètement hors service.
«Notre équipe d'enquête travaille aux côtés de nos experts en technologie de l'information afin d'identifier la source des problèmes techniques qui ont eu lieu la nuit dernière, a indiqué dimanche le chef de la police d'Ottawa, Charles Bordeleau. Notre réseau reste sécurisé», a-t-il assuré.
Le porte-parole de la Ville de Toronto Jackie DeSouza a indiqué que la Ville était au courant de ce qui était arrivé à Ottawa. Les fonctionnaires «demeurent très vigilants» et surveillent toute activité suspecte sur le site toronto.ca, a-t-il assuré.
Le compte Twitter de Aerith – qui indiquait, probablement à tort, avoir été fondé en Turquie – a été suspendu depuis les possibles cyberattaques.
Le groupe Anonymous s'en prendrait ainsi à la Ville d'Ottawa pour défendre la cause d'un adolescent de Barrhaven, en banlieue de la capitale nationale. Ce dernier fait face à 60 chefs d'accusation pour avoir fait de faux appels rapportant des menaces à la bombe, des prises d'otages ou des fusillades, tout en imitant la voix d'une autre personne, généralement un rival de la communauté de jeu en ligne.
Les attaques informatiques revendiquées par «Anonymous» seraient en lien avec une nouvelle preuve qui n'aurait pas été retenue par les enquêteurs et qui démontrerait que l'adolescent de Barrhaven n'est pas responsable des méfaits, mais qu'il s'agit plutôt d'un homme du New Jersey. La police de Toronto aurait déposé quelques-unes des 60 accusations.

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

Source : http://fr.canoe.ca/techno/nouvelles/archives/2014/11/20141123-175629.html

Quand chaque minute compte

	**Quand chaque minute compte..**

McAfee, filiale d'Intel Security, publie aujourd'hui un nouveau rapport, « Prévention des menaces : chaque minute compte ! », qui évalue la capacité des entreprises à détecter et à détourner les attaques ciblées.

Ce dernier révèle également le Top 8 des indicateurs d'attaques les plus critiques et examine les meilleures pratiques proactives en matière de réponse aux incidents. Il illustre combien les entreprises sont plus efficaces lorsqu'elles effectuent des analyses des attaques subtiles en temps réel en prenant en compte plusieurs variables mais surtout dès lors qu'elles ont intégré et priorisé le temps de détection et les menaces intelligentes dans leur évaluation des risques.
Conjointement au rapport, une étude menée par Evalueserve, révèle que la majorité des entreprises interrogées manquent de confiance en leur capacité à détecter les attaques ciblées dans un temps opportun. Même les entreprises les mieux préparées à gérer les attaques ciblées passent beaucoup trop de temps à enquêter sur des événements, contribuant à un sentiment d'urgence, plutôt qu'à se concentrer pro-activement à la détection et à l'atténuation des menaces.
Le rapport met en évidence le fait qu'en France :
• Seulement 26 % des entreprises sont confiantes dans leur capacité à détecter une attaque en quelques minutes, et 29 % ont déclaré que cela pouvait leur prendre des jours, des semaines, voire des mois avant qu'elles ne remarquent un comportement suspect.
• 71 % des DSI interrogés ont indiqué que les attaques ciblées sont une préoccupation majeure pour leur entreprise.
• 54 % des entreprises ont enquêté sur plus de 10 attaques l'an dernier.
• 95 % de celles qui sont capables de détecter les attaques en quelques minutes possèdent une solution de gestion des évènements et des informations de sécurité (SIEM).
• Plus de la moitié des entreprises interrogées (61 %) ont indiqué qu'elles sont équipées des outils et des technologies nécessaires pour fournir une réponse rapide aux attaques. Cependant, les indicateurs critiques ne sont généralement pas isolés de la masse des alertes générées et provoquent une charge de travail supplémentaire aux équipes qui doivent passer au crible toutes les données des menaces.
« Pour garder la main sur les attaquants il faut relever le défi du temps dans la détection », déclare David Grout, Directeur Europe du Sud de McAfee, filiale d'Intel Security. « En simplifiant, grâce à une analyse intelligente et en temps réel, le travail frénétique de filtrage d'un large volume d'alertes et d'indicateurs d'attaques vous pourrez plus efficacement appréhender des événements pertinents et prendre des mesures pour contenir et détourner les attaques plus rapidement. »
Compte tenu de l'importance de l'identification des indicateurs critiques, le rapport de McAfee Intel Security a révélé le Top 8 des indicateurs d'attaque les plus courants.
Parmi ceux-ci, cinq reflètent le suivi des événements à travers le temps écoulé et montrent l'importance de la corrélation contextuelle :
1. Des hôtes internes communiquent vers des destinations inconnues ou mal connues ou vers un pays étranger où il n'y a pas d'affaire en cours.
2. Des hôtes internes communiquent vers des hôtes externes qui utilisent des ports non standards ou en inéquation avec le protocole/port, tels que l'envoi d'interpréteurs de commandes (SSH) plutôt que du trafic HTTP sur le port 80, qui est le port Web par défaut.
3. Des accès publiques ou en zone démilitarisée (DMZ) communiquant vers des hôtes internes. Cela permet de brûler les étapes de l'extérieur vers l'intérieur et en arrière-plan, permet l'exfiltration de données et l'accès à distance à des actifs. Il neutralise la valeur de la DMZ.
4. Détection de logiciels malveillants en heures Off. Ces alertes qui peuvent se produire en dehors des heures standards d'ouverture de l'entreprise (la nuit ou le week-end) et qui pourraient signaler un hôte compromis.
5. Scans de réseau par les hôtes internes communiquant avec plusieurs hôtes dans un court laps de temps, qui pourrait révéler une attaque se déplaçant latéralement au sein du réseau. Les défenses du périmètre réseau, tels que pare-feu et IPS, sont rarement configurées pour surveiller le trafic sur le réseau interne (mais pourrait l'être).
6. Plusieurs événements alarmants à partir d'un seul hôte ou à répétition sur une période de 24 heures sur plusieurs machines dans le même sous-réseau, tels que les échecs d'authentification.
7. Après avoir été nettoyé, un système est réinfecté par des logiciels malveillants dans les cinq minutes qui suivent – les réinfections répétées signalent la présence d'un rootkit ou d'une compromission persistante.
8. Un compte utilisateur tente de se connecter à de multiples ressources en quelques minutes à partir de ou vers différentes régions – signe que les informations d'identification de l'utilisateur ont été volées ou que l'utilisateur a des intentions suspectes.
« Un jour, nous avons remarqué qu'un poste de travail subissait des demandes d'authentification du contrôleur de domaine à deux heures du matin. Cela pouvait bien sur être tout à fait normal, mais il se pouvait aussi que cela soit un signe d'alerte malveillante », commente Lance Wright, directeur principal de l'information de sécurité et de conformité à Volusion, un fournisseur de solutions de commerce contributeur de l'élaboration du rapport. *« Suite à cet incident, nous avons créé une règle pour nous alerter si un poste de travail avait plus de cinq demandes d'authentification en dehors des heures ouvrables pour nous aider à identifier le début de l'attaque, avant que les données ne soient compromises. »*

« La veille en temps-réel, la bonne intelligence et les solutions de gestion des évènements et des informations de sécurité (SIEM), permettent de minimiser le temps de détection, d'éviter de manière proactive les violations fondées sur la contextualisation des indicateurs lors de l'analyse et d'apporter des réponses en matière d'action automatisés », précise David Grout *« Grâce aux solutions qui permettent d'accélérer la capacité de détection, de réaction et d'apprentissage sur les attaques, les entreprises peuvent grandement changer leur posture de sécurité et passer de 'traquées' à 'traqueuses'. »*

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.itrnews.com/articles/152073/chaque-minute-compte.html

---

Airbus Helicopters a-t-il été victime d'un piratage informatique américain?

Airbus Helicopters a-t-il été victime d'un piratage informatique américain?

Selon des sources concordantes, Airbus Helicopters a été victime d'une attaque informatique. Le constructeur a de « fortes suspicions » d'une attaque venant des États-Unis.

C'est peut-être une affaire d'État. Certes ce qui s'est passé chez Airbus Helicopters n'est pas réellement surprenant mais si l'enquête des autorités françaises en cours confirme les « fortes suspicions » du constructeur de Marignane, selon des sources concordantes, elle mettrait une nouvelle fois en lumière les pratiques détestables d'espionnage des États-Unis à l'égard de leurs alliés malgré toutes les conséquences néfastes sur le plan diplomatique de l'affaire Snowden. Ce qui est sûr, selon ces mêmes sources, c'est que Airbus Helicopters a bien été victime d'une attaque informatique, dont l'ampleur reste encore à déterminer.
Le constructeur de Marignane s'est récemment aperçu d'une intrusion ou d'une tentative d'intrusion dans ses réseaux de communications. Alerté par Airbus Helicopters, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), l'autorité nationale en matière de sécurité et de défense des systèmes d'information, a lancé une enquête pour savoir si les intrusions ont réussi et, si c'est le cas, pour déterminer l'ampleur des dommages. Contacté par La Tribune, Airbus Helicopters affirme qu' »aucune information classifiée » n'a été dérobée. Mais, selon des sources concordantes interrogées par La Tribune, le constructeur nourrit de « fortes suspicions » vis-à-vis des États-Unis. « Mais nous n'avons pas encore d'éléments pour le démontrer », explique-t-on chez le constructeur à La Tribune.

En jeu, un important appel d 'offre en Pologne
Pourquoi les États-Unis ? Selon ces mêmes sources, le constructeur suspecte s'être fait « piraté » dans le cadre de l'appel d'offres international lancé par la Pologne, qui veut acheter 70 hélicoptères de transport pour un montant estimé à 2,5 milliards d'euros environ. Les trois compétiteurs – l'italien AgustaWestland (AW149), Airbus Helicopters (Caracal ou EC725) et l'américain Sikorsky (S-70) attendent une décision de Varsovie fin 2014, voire début 2015. Les candidats ont jusqu'au 28 novembre pour déposer leurs offres. Jusqu'ici la compétition entre Airbus Helicopters et Sikorsky était très, très chaude.
Depuis plusieurs jours, Sikorsky joue d'ailleurs un drôle de jeu en Pologne. Les Américains veulent vendre des hélicoptères dont les performances ne correspondent pas au cahier de charge établi par Varsovie. Ce sont des appareils d'ancienne génération qu'ils ont en stock. Le ministère polonais de la Défense a répliqué fin octobre sur un ton extrêmement ferme à un courrier du président du consortium Sikorsky Aircraft Corporation (SAC) Mick Maurer, en affirmant que c'est à lui qu'appartient de « définir les besoins des forces armées et non au soumissionnaire de lui indiquer ce qu'il a à vendre ».

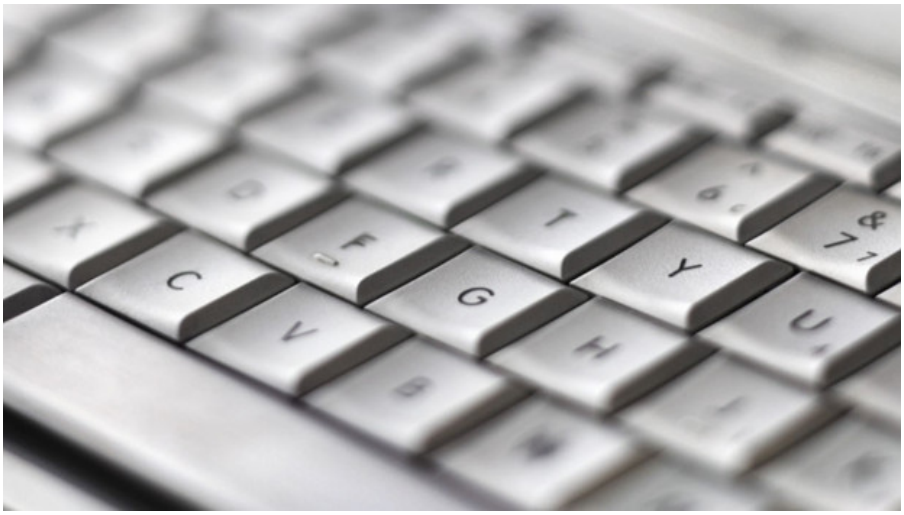
Que va faire Sikorsky ?
« Les exigences concernant l'hélicoptère multitâche étaient connues depuis mai dernier et la société SAC dispose d'appareils qui y répondent », a relevé le ministère polonais, avant de noter que « les autres candidats ont annoncé qu'ils présenteraient des offres correspondant aux exigences de l'Inspection de l'Armement ». Le ministère « ne prévoit pas d'annuler l'appel d'offres ou d'en modifier les termes au détriment de la Pologne », a assuré Varsovie, laissant entendre que tel était le sens de la lettre de Sikorsky. Il « reste ouvert à un dialogue équitable avec tous les candidats, mais ne cède pas aux pressions de contractants potentiels concernant les termes de la commande ».
Du coup, le 30 octobre, Sikorsky Aircraft a annoncé qu'elle ne participerait pas à l'appel d'offres pour la fourniture de 70 hélicoptères à la Pologne si les termes n'en sont pas modifiés. Le constructeur a précisé qu'il ne présenterait pas de proposition avec son partenaire polonais PZL Mielec car il lui semble impossible de livrer ses hélicoptères Black Hawk dans les conditions définies par l'appel d'offres. Dans un communiqué, le ministère polonais de la Défense a qualifié cette attitude de tactique de négociation, ce qu'a démenti Sikorsky. Le ministère a confirmé qu'il n'envisageait pas de modifier les termes de l'appel d'offres.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/20141113trib0392bd0ed/airbus-helicopters-a-t-il-ete-victime-d-un-piratage-informatique-americain.html

---

Cyberattaque contre le département d'Etat américain



Cyberattaque contre le département d'Etat américain

Après des attaques contre le réseau informatique de la Maison Blanche le mois dernier et celui de la Poste américaine il y a quelques jours, ce serait désormais le département d'Etat américain qui aurait été victime de piratage.

Le département d'Etat américain a dû déconnecter ce week-end son réseau informatique non confidentiel après des soupçons de piratage, ont rapporté les médias américains. Vendredi, le département d'Etat avait invoqué une opération de maintenance de routine sur son principal réseau non confidentiel, affectant le trafic de courriels et l'accès aux sites internet publics.

Mais, selon des informations de presse publiées dimanche soir, un pirate informatique est soupçonné d'avoir franchi certaines barrières de sécurité du système gérant les courriels non classifiés. Selon un haut responsable cité par le Washington Post, une « activité inquiétante » a bien été constatée mais aucun des systèmes confidentiels n'a été touché.

Série de cyberattaques contre les organismes publics

Si elle se confirme, cette attaque informatique contre le département d'Etat serait la dernière d'une série de cyberattaques visant les organismes publics américains. La semaine dernière, la Poste américaine (USPS) avait annoncé que des pirates informatiques avaient volé des informations sur leurs employés et sans doute sur certains clients.

Jusqu'à environ 800.000 personnes rémunérées par la Poste américaine, y compris les sous-traitants, pourraient être concernées par ce piratage, selon un porte-parole de l'entreprise publique. Les pirates se seraient aussi introduits dans le système de paiement des bureaux de poste et en ligne, ce qui impliquerait aussi des clients, selon l'USPS. Le FBI a annoncé l'ouverture d'une enquête.

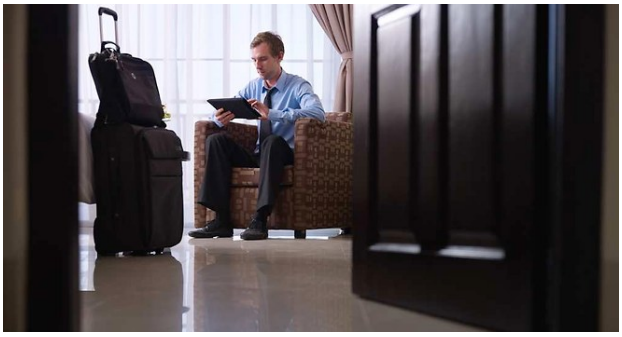
Le mois dernier, la Maison Blanche avait elle aussi fait état d'une « intrusion » dans son réseau informatique non confidentiel. Selon le Washington Post, des hackers russes sont soupçonnés d'en être à l'origine.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :

http://lci.tf1.fr/monde/amerique/le-departement-d-etat-americain-victime-d-une-cyber-attaque-8519395.html

Nouvelle vague d’attaques cybercriminelles : le « Dark hotel »



Nouvelle vague d’attaques cybercriminelles : le « Dark hotel »

« Dark hotel » : ces hackers qui exploitent les réseaux Wi-fi des hôtels de luxe.
Des hackers ont pris pour cible des directeurs généraux et autres cadres dirigeants d’entreprises lorsqu’ils voyagent à l’étranger. Un phénomène qui durerait depuis quatre ans.
Nom de code « Dark Hotel ». Ce nouvel acteur dans le monde du cyberespionnage sévit depuis au moins quatre ans, révèle la société de sécurité russe Kaspersky Lab. **Ses cibles appartiennent à l’élite économique internationale : directeurs généraux, vice-présidents, directeurs des ventes et marketing de grosses entreprises américaines et asiatiques**. Pour les piéger et leur dérober des données sensibles, ces hackers mettent à profit les réseaux Wi-fi des hôtels de luxe dans lesquels ils voyagent.

Ces hackers sans visage ont un mot d’ordre : ne jamais frapper deux fois la même cible. Leur mode opératoire ? Un faux logiciel, de type Adore Reader ou Google Toolbar, que le visiteur est invité à télécharger après s’être connecté au réseau Wi-fi de son hôtel. Un cheval de Troie permet ensuite au hacker de recueillir des données privées, y compris les mots de passe sur Firefox, Chrome, Internet Explorer ainsi que les identifiants sur Gmail, Yahoo,Facebook et Twitter.

Les victimes se font ainsi voler des données qui relèvent du domaine de la propriété intellectuelle des entreprises qui les emploient. Après l’opération, toute trace est effacée du réseau de l’hôtel, le hacker retournant dans l’ombre. Une « précision chirurgicale », souligne Kaspersky Lab.

Selon l’unité de recherche de la société russe, une empreinte laissée par les hackers suggère que les cybercriminels parlent coréen. Le plus haut volume d’activité a été détecté entre août 2010 et 2013. 90 % des cyberattaques étaient localisées au Japon, Taïwan, en Chine, en Russie et en Corée du Sud. Depuis 2008, elles se comptent par milliers. Kaspersky Lab n’est, pour l’heure, pas parvenu à tracer ces hackers.

A partager sans modération

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lesechos.fr/tech-medias/hightech/0203938482430-dark-hotel-ces-hackers-qui-exploitent-les-reseaux-wi-fi-des-hotels-de-luxe-1064496.php
Aurélie Abadie