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.

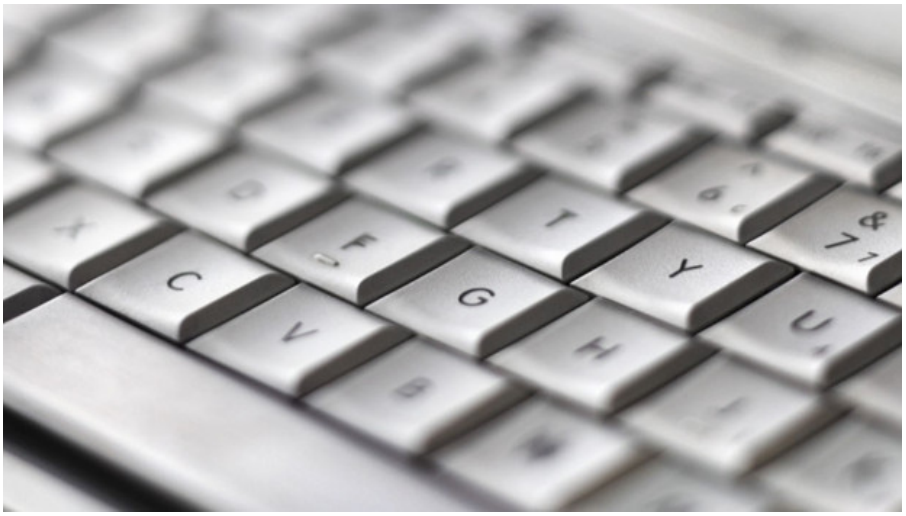
Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

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.

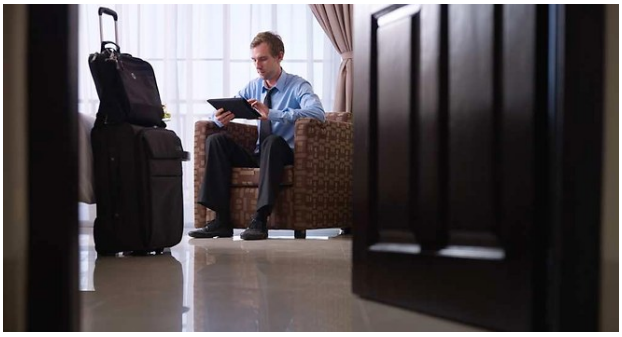
Mais, selon des informations de presse publiées dimanche soir, un pirate informatique est soupçonné d’avoir franchi certaines barrières de sécurité du système gérant les courriels non classifiés. Selon un haut responsable cité par le Washington Post, une « activité inquiétante » a bien été constatée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

---

40 % des employés des grandes entreprises américaines

utilisent leurs matériels personnels, mais…

40 % des employés des grandes entreprises américaines utilisent leurs matériels personnels, mais…

Selon une récente étude réalisée par Gartner, le BYOD (Bring Your Own Device) serait appliqué par 40 % des employés des grandes entreprises aux États-Unis. Mais un point majeur est à préciser : les entreprises sont loin d'être toutes au courant d'un tel usage.

Le BYOD tiré par les employés, non les employeurs

Dans mes précédents papiers publiés ces derniers mois, je suis souvent revenu sur le risque numéro un de ne pas appliquer de politique de BYOD : que les employés utilisent dans le dos de l'entreprise leurs propres appareils, multipliant ainsi les risques de fuites et de sécurité.

Or dans sa dernière étude, si Gartner montre que 40 % des employés des grandes entreprises sont concernés par le BYOD, il faut bien comprendre que seule une partie minoritaire d'entre eux le font sur demande de la société. Plus précisément, nous apprenons qu'un quart des employés concernés le font suite à un besoin express de leur entreprise.

Cela signifie donc que les 75 % restants le font sans qu'il n'y ait de demande particulière. Or seule la moitié des entreprises sont au courant de ces agissements. L'autre moitié de ces 75 % ignore donc totalement ces utilisations. Non seulement cela prouve et confirme que le BYOD aux États-Unis est plus tiré par les employés que par les entreprises elles-mêmes, mais aussi et surtout qu'une partie importante d'entre elles prennent des risques importants du fait de leur manque de politique de BYOD.

La statistique est un claque terrible dès lors que cela signifie qu'environ 15 % des employés de toutes les grandes entreprises américaines apportent et utilisent leurs smartphones, leurs tablettes ou leurs PC portables dans le dos de leurs dirigeant. Une donnée catastrophique qui doit donner des sueurs froides à bien des DSI.

On se rappellera d'ailleurs qu'en mai dernier, ce même Gartner indiquait qu'un quart des employés américains utilisant leurs propres appareils avaient dû faire face à des problèmes de sécurité en 2013. Et une partie non négligeable d'entre eux (27 %) l'ont précisé à leur hiérarchie… Un cauchemar en puissance pour les entreprises concernées.

L'ignorance, la pire des situations

Toujours du côté des rappels, deux anciennes études ces derniers mois ont montré que de très nombreuses entreprises n'ont toujours aucune politique de BYOD et que bien peu appliquaient un « Full BYOD ». Si l'on cumule ces informations avec le fait que certains employés confondent BYOD et liberté totale, le résultat ne peut mener qu'à des catastrophes.

« La clé pour disposer d'un appareil sécurisé est de vous assurer qu'il est bien géré » notait fort justement Gartner il y a quelques mois. Or comme je l'ai maintes fois répété, manquer de clarté avec ses employés sur le sujet si épineux des appareils mobiles personnels est un danger gigantesque pour l'entreprise. S'il n'y a pas de politique de BYOD, il faut se montrer ferme. Si une politique est mise place, il ne faut pas semer de doute dans l'esprit des employés et leur préciser les meilleurs comportements à avoir.

Notons enfin qu'il est intéressant d'apprendre que les tablettes tactiles, que ce soit en entreprise ou à la maison, servent avant tout… à jouer. Le jeu passe ainsi juste devant les réseaux sociaux et la lecture d'actualité. « L'importance des jeux sur des tablettes va de paire avec la relativement faible utilisation des appareils à des fins de travail » résume Gartner, qui explique donc que globalement, les entreprises ont un besoin encore assez limité de ce type d'appareils, bien plus utilisé à la maison.

Par Nil Sanyas pour Bring it on

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

Source :
http://www.zdnet.fr/actualites/40-des-employes-des-grandes-entreprises-americaines-utilisent-leurs-materiels-personnels-mais-39809253.htm

---

Outlook Web App ciblé par des

attaques de phishing sophistiquées – Le Monde Informatique

	**Outlook Web App ciblé par des attaques de phishing sophistiquées**

Selon les chercheurs de Trend Micro, un groupe de pirates sévit à l'encontre d'agences militaires, ambassades et d'entreprises liées à la défense nationale et des médias internationaux utilisant Outlook Web App d'Office 365.

Afin de voler les identifiants de messagerie des employés de nombreuses organisations publiques, parapubliques mais également privées, un groupe d'espions a mis en place des techniques de phishing avancées.
Selon des chercheurs de l'entreprise de sécurité Trend Micro, qui ont baptisé cette campagne Operation Pawn Storm dans un document publié la semaine dernière, le groupe à l'origine de ces attaques opèrerait depuis au moins 2007. Au cours de ces années, ils ont utilisé différentes techniques pour atteindre leurs objectifs, notamment des campagnes de phishing pour propager des malwares sous forme de pièces jointes Microsoft Office malveillantes, l'installation de backdoors type SEDNIT ou Sofacy, ou des exploits plus sélectifs pour infecter des sites légitimes.

Dans ses dernières attaques de phishing, le groupe a utilisé une technique particulièrement intéressante, ciblant les organisations qui utilisent Outlook Web App (OWA), une composante du service Office 365 proposé par Microsoft. Pour chaque attaque, le groupe a créé deux faux domaines : un premier, qui reproduit un site Web tiers connu des victimes – par exemple le site d'une conférence dans un secteur de l'industrie qui les intéresse – et un second, similaire au domaine utilisé pour le déploiement d'Outlook Web App par l'organisation visée. Les attaquants ont ensuite créé des courriels contenant un lien vers le faux site tiers sur lequel ils hébergeaient un code JavaScript non malveillant dont le but était double : ouvrir le site légitime dans un nouvel onglet et rediriger l'onglet déjà ouvert du navigateur Outlook Web App vers une page de phishing. « Le code JavaScript faisait croire aux victimes que leur session OWA était close, et la page malveillante leur demandait de se reconnecter en tapant à nouveau leurs identifiants », ont écrit les chercheurs de Trend Micro dans leur document.
« Les attaquants ont réussi à rediriger les victimes vers de fausses pages Outlook Web App en agissant sur les propriétés d'ouverture des pages de leurs navigateurs ».

Une technique de phishing multi-navigateurs
Selon les chercheurs, cette technique n'exploite aucune vulnérabilité et fonctionne avec tous les navigateurs courants dont Internet Explorer, Mozilla Firefox, Google Chrome et Safari d'Apple. Cependant, il faut deux conditions pour que ce mode opératoire fonctionne : « Les victimes doivent utiliser OWA et ils doivent cliquer sur les liens intégrés au volet de prévisualisation OWA », ont-ils expliqué. L'attaque est redoutable parce que l'onglet du navigateur ne permet pas aux victimes de voir que leur session OWA est illégitime et ils ont peu de chance de se rendre compte que l'URL a été usurpée avant de rentrer leurs identifiants. « De plus, les attaquants ont pris soin d'utiliser des noms de domaine très similaires à ceux choisis par les organisations ciblées pour leurs pages de log in OWA, et dans certains cas, ils ont même acheté des certificats SSL légitimes, de sorte que les navigateurs des victimes affichent aussi les indicateurs de connexion sécurisée HTTPS pour les sites de phishing », ont encore ajouté les chercheurs de Trend Micro.

Parmi les personnes visées, on trouve des employés de l'entreprise militaire privée américaine Academi, anciennement connue sous le nom de Blackwater ; l'Organisation pour la sécurité et la coopération en Europe (OSCE) ; le Département d'État des États-Unis ; le fournisseur du gouvernement américain Science Applications International Corporation (SAIC) ; une société multinationale basée en Allemagne ; l'ambassade du Vatican en Irak ; des médias de radiodiffusions de plusieurs pays ; les ministères de la Défense de la France et de la Hongrie ; des responsables militaires pakistanais ; des employés du gouvernement polonais et des attachés militaires de différents pays. Parmi les appâts utilisés par les assaillants, les chercheurs ont identifié des événements et des conférences bien-connus pour lesquels les victimes pouvaient avoir un intérêt.
« Mais, ce n'est pas tout : les assaillants ont combiné leur tactique de phishing à diverses attaques éprouvées afin de compromettre les systèmes et entrer dans les réseaux pour y voler des données », ont déclaré les chercheurs de Trend Micro.
« Les variantes de SEDNIT utilisées ont été semble-t-il très efficaces car elles ont permis aux pirates de voler des informations sensibles sur les ordinateurs des victimes en évitant de se faire repérer ».

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

Source :
http://www.lemondeinformatique.fr/actualites/lire-outlook-web-app-cible-par-des-attaques-de-phishing-sophistiquees-59081.html

---

Un grand pas vers la détection des fraudes nommé

ArgyleDB

Un grand pas vers la détection des fraudes nommé ArgyleDB

L'éditeur Argyle Data a lancé sa solution de détection des fraudes reposant sur le SGBD Accumulo créé par la NSA ainsi que sur le moteur de requêtes SQL distribué Presto développé par Facebook.

Argyle Data a annoncé le lancement d'ArgyleDB, sa solution de surveillance et de détection des fraudes en temps réel taillé pour les environnements Hadoop et à forte volumétrie de données. La société indique avoir conçu son offre sur la base du système de gestion de base de données Accumulo, initialement développé par la NSA avant d'être récupéré en 2011 par la fondation Apache, mais également de Presto, la technologie Open Source utilisée par Facebook pour permettre d'analyser les données en utilisant des requêtes SQL et d'automatiser les futures requêtes sur les données en direct.
Argyle Data indique par ailleurs que sa solution supporte un ensemble d'algorithmes permettant de détecter une activité frauduleuse, à une échelle pétaflopique, en une quinzaine de minutes seulement contre 24 heures ou plus habituellement. L'année dernière, Argyle Data avait annoncé travailler sur une gamme de produits utilisant le machine learning sur une pile Hadoop afin de créer des applications capables d'ingérer des données et de les analyser en temps réale pour réduire la fenêtre de détection des fraudes et d'intrusion de plusieurs heures ou jours à quelques secondes.

Une levée de fonds de 4,5 millions de dollars
Parallèlement à ce lancement, Argyle Data a annoncé un nouveau tour de table financier qui lui a permis de lever 4,5 millions de dollars, portant à 21 millions de dollars le montant total des fonds levés depuis sa création en 2009. L'équipe de direction est également étoffée avec l'arrivée de Arshak Navruzyan, Ian Howells, Padraig Stapleton et Volkmar Scharf-Katz Navruzyan qui ont tous un solide vécu en matière d'analytique et de machine learning.

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

Source :
http://www.lemondeinformatique.fr/actualites/lire-argyledb-la-detection-des-fraudes-avec-des-technologies-de-facebook-et-la-nsa-59068.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

---

Les cybercriminels utilisent aussi les Sous-domaines abandonnés

Les cybercriminels utilisent aussi les Sous-domaines abandonnés

Si la plupart des hackeurs tentent de contourner les mesures de sécurité mises en place sur les serveurs d'une entreprise, il est parfois plus simple de scruter l'architecture d'un site au global et les sous-domaines, notamment.

Spécialisée dans la sécurité, la société Detectify, propose un outil de scan en mode SaaS et annonce avoir mené une enquête concernant la vulnérabilité des sous-domaines. Ces derniers seraient largement laissés à l'abandon et constitueraient un vecteur d'attaques.
Un prestataire de services proposant de créer des comptes utilisateur en leur attribuant un sous-domaine peut lui-même créer son propre sous-domaine pour lancer un service ou une campagne promotionnelle pendant quelques semaines, voire quelques années. Par la suite, à la fin de cette campagne ou à la fermeture du service en question, Detectify explique que le prestataire n'efface pas systématiquement la redirection du sous-domaine pointant vers le service ou la campagne. Or, un internaute peut donc se créer un compte chez ce prestataire de service puis obtenir ce même sous-domaine et orchestrer une attaque de phishing, par exemple.
Cette manipulation est possible lorsque la société en question ne procède pas à la validation du détenteur de chaque sous-domaine. Et il en existerait un certain nombre parmi lesquels nous retrouvons Heroku, Github, Bitbucket, Squarespace, Shopify, Desk, Teamwork, Unbounce, Helpjuice, HelpScout, Pingdom, Tictail, Campaign Monitor, CargoCollective, StatusPage.io ou encore Tumblr.
« Nous avons également identifié 200 organisations qui s'en trouvent affectées. Dans beaucoup de cas, nous parlons de société listées au NASDAQ ou figurant dans le top 100 d'Alexa », ajoute Detectify.
Pour vérifier si une personne est bien le propriétaire d'un domaine ou d'un sous-domaine, quelques sociétés, comme Google demandent de transférer un ficher HTML via FTP ou d'ajouter une CNAME particulière dans le panneau de contrôle du nom de domaine.

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

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-735061-domaine-abandonnes-vecteur-attaques-hackeurs.html?&xvc_mode=M&xvc_campaign=NL_ClubicPro_New_25/10/2014&partner=-&xvc_position=717264607&xvc_misc=-&crmID=639453874_717264607&sstat_url=http%3A%2F%2Fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-735061-domaine-abandonnes-vecteur-attaques-hackeurs.html

---

Après JP Morgan, 9 autres banques auraient été piratées

Après JP Morgan, 9 autres banques auraient été piratées

Le groupe responsable du piratage de JP Morgan cet été aurait mené des attaques sur 9 autres établissements financiers. Comme la loi américaine n'oblige pas les banques à communiquer sur ce genre d'incident, l'ampleur exacte de la fuite potentielle de données reste inconnue.

JP Morgan serait loin d'être la seule banque à avoir été attaquée par ce groupe de pirates. Il s'agirait en réalité d'une vague d'intrusions, dont l'ampleur exacte reste inconnue.

Elle aurait permis aux assaillants « d'infiltrer environ 9 autres établissements financiers », explique le New York Times en s'appuyant sur des sources proches de l'enquête.

De nombreux points à éclaircir
Peu de détails ont été révélés par les canaux officiels. D'ailleurs, le journal américain n'a pas pu obtenir les noms des établissements infiltrés et ignore toujours ce à quoi les pirates ont pu accéder.
JP Morgan, seule banque à avoir communiqué sur le sujet, affirme que les responsables n'ont pu accéder qu'aux noms des clients et à d'autres informations non-financières. Le personnel chargé de la sécurité de la banque aurait repéré l'attaque avant que les assaillants n'accèdent aux données sensibles. Ceci étant dit, l'intrusion n'aurait pas été entièrement arrêtée avant la mi-août alors qu'elle avait débuté en juillet.
Pour ce qui est de l'identité des pirates, les autorités en charge de l'enquête pencheraient pour un groupe opérant depuis la Russie. Ils auraient une « vague connexion » avec des membres du gouvernement de Moscou.
Les motivations des pirates restent, elles aussi, inconnues. Cependant, ces attaques pourraient avoir été menées en représailles aux sanctions visant la Russie dans le cadre de la crise ukrainienne, présument les services de renseignement américains.

Une brèche dans les systèmes mais aussi dans la loi ?
Outre l'aspect sécuritaire, l'attaque met en évidence une potentielle lacune dans la loi américaine. On apprend aujourd'hui que l'incident a bien plus d'ampleur qu'il n'y parait. Peut être qu'une meilleure information aurait permis de limiter l'intrusion ou d'aider à faire avancer l'enquête. Seulement, les banques en ligne ne sont pas obligées de communiquer sur les événements ayant pu compromettre les données des clients à moins qu'ils leur aient fait perdre de l'argent.

Dans certains Etats américains, les banques peuvent attendre jusqu'à un mois avant d'informer les autorités et les clients de ce type d'incident. La loi californienne, par exemple, impose simplement un délai « raisonnable », une définition sujette à interprétations. Il est alors difficile, dans un tel contexte, de lutter efficacement contre ce type de piratage.

La France n'est pas mieux lotie : les banques ne sont pas tenues d'informer les clients lors d'une fuite de données. Pour l'instant, seuls les fournisseurs d'accès et opérateurs ont l'obligation de notifier la CNIL ou les clients. Cependant, le régulateur français et ses équivalents européens cherchent à étendre ces exigences à l'ensemble des services en ligne.

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

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-731231-jp-morgan-9-banques-attaquees-pirates.html

---

500 000 PC infectés à cause d'une faille Windows XP

500 000 PC infectés à cause d'une faille Windows XP

Selon les chercheurs en sécurité de Proofpoint, 52% des PC infectés par le botnet Qbot font tourner Windows XP. Exploitant une faille de Windows XP mais également de Seven et Vista, un groupe de cybercriminels russe a réussi à activer le botnet Qbot fort 500 000 PC zombies, essentiellement localisés aux Etats-Unis. Son objectif : Aspirer les identifiants bancaires des utilisateurs de ces PC corrompus.

Des pirates russes à l'origine du botnet Qbot ont construit une impressionnante armée de 500 000 PC zombies en exploitant des failles non corrigées dans des ordinateurs tournant sous Windows XP mais également Windows 7 et Vista. Des PC localisés principalement aux Etats-Unis, a fait savoir la société Proofpoint. Ces derniers temps, les hackers russes ont fait monter la pression avec des incursions sérieuses telle que l'attaque qui a visé la banque américaine JPMorgan Chase. Avec ce botnet, baptisé Qbot, les chercheurs de Proofpoint ont fait ressortir que le groupe qui est à l'origine de sa création l'a élaboré de façon méticuleuse à travers le temps, sans faire de vague, au point de rester sous les radars des sociétés de sécurité et donc de ne pas avoir attiré leur attention.

Selon Proofpoint, 75% des 500 000 PC infectés par le botnet Qbot sont situés aux Etats-Unis, sachant que parmi eux, 52% font tourner Windows XP, 39% Windows 7 et 7% Windows Vista. En Grande-Bretagne, la proportion de PC infectés est bien moindre, 15 000 postes environ. « Avec 500 000 clients infectés volant les identifiants des comptes bancaires en ligne des utilisateurs, le groupe de cybercriminels a le potentiel pour réaliser des bénéfices vertigineux », ont indiqué les chercheurs de la société de conseil en sécurité. Mais le botnet Qbot ne s'attaque pas seulement aux comptes bancaires, il compromet également les sites WordPress, soit en infectant le site lui-même ou bien en injectant des contenus corrompus dans leurs newsletters.
Article de Dominique Filippone

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

Source :
http://www.lemondeinformatique.fr/actualites/lire-500-000-pc-infectes-a-cause-d-une-faille-windows-xp-58878.html

---

Un nouveau malware vise les Mac, 17.000 machines

affectées ?

Un nouveau malware vise les Mac, 17.000 machines affectées ?

Selon la firme russe Dr.Web un malware visant spécifiquement les possesseurs de Mac serait actuellement actif, affectant plus de 17.000 machines à travers le monde. Pas une première, mais ce malware possède quelques spécificités amusantes.

Pas la peine de se mentir, les produits Apple eux aussi sont parfois victimes de malwares. En 2011, le Trojan Flashback avait ainsi infecté des centaines de milliers d'ordinateurs Apple. Le malware détecté par Dr Web est en revanche bien moins diffusé : 17.000 utilisateurs seulement seraient infectés.
Ce malware se range sous la catégorie des Botnets, infectant l'ordinateur de l'utilisateur afin de permettre à l'attaquant de l'exploiter pour d'autres fonctions à l'insu de son utilisateur. Le malware a été baptisé, un peu rapidement, iWorm par Doctor Web, bien que le mode exact de propagation du virus reste encore peu clair.
La particularité qui a retenu l'attention des chercheurs, c'est la façon dont les ordinateurs infectés récupèrent les adresses IP des serveurs de command&control. Les machines du botnet vont ainsi chercher sur Reddit les adresses de leurs centre de command&control : celles-ci sont postées à intervalles régulier dans la section commentaire d'un sujet destiné à recenser des serveurs Minecraft via un compte tenu par les individus responsables de la propagation du malware.

Reddit est innocent !
Reddit n'a rien à se reprocher, le site n'a pas été altéré ou son utilisation n'a pas été techniquement détournée, mais cette approche originale mérite d'être notée. Comme le relève le chercheur Graham Cluley, même en supprimant le compte utilisé pour router vers ces adresses IP, cela n'empêcherait pas les pirates de recréer un compte et de continuer leur activité.
Comme souvent néanmoins, il convient de rester prudent avec les alertes lancées par les firmes spécialisées dans la vente d'antivirus. Dr.Web annonce ainsi 17.000 ordinateurs infectés à travers le monde, mais ne précise pas du tout quel mode de diffusion a été choisi pour propager le malware. Selon des sources anonymes, le principal mode d'infection se ferait via le téléchargement de logiciels Adobe et Microsoft piratés sur les plateformes de partage en P2P.
De la même manière, peu d'informations sont disponibles pour ceux qui souhaitent se prémunir de ce malware, si ce n'est la solution vendue par Dr.Web… Mais selon MacRumors, l'outil de protection maison proposé par Apple à ses clients Xprotect, a été mis à jour pour détecter et empêcher la propagation de cette menace.
Attention Livo !

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

Source :
http://www.zdnet.fr/actualites/un-nouveau-malware-vise-les-mac-17000-machines-affectees-39807339.htm
Par Louis Adam | Lundi 06 Octobre 2014