Darkhotel récupère une faille chez Hacking Team | Le Net Expert Informatique

Le groupe de hackers Darkhotel, spécialisés dans le vol de données ciblant des dirigeants, récupère une faille zero day issue du piratage de Hacking Team pour peaufiner son arsenal.

Selon Kaspersky Lab, laboratoire de recherches en sécurité de l'éditeur, le groupe de hackers Darkhotel, connu pour avoir piraté les réseaux Wifi de luxueux hôtels afin de compromettre les machines de dirigeants d'entreprise, utilise un exploit récupéré lors de l'attaque contre Hacking Team. Rappelons que cette entreprise italienne, spécialisée dans la vente de failles zero day à des gouvernements, a été piratée en juillet. Une opération au cours de laquelle 400 Go de données avaient été dérobés, dont des informations sur des failles jusqu'alors inconnues. Certaines de ces vulnérabilités ont été corrigées en urgence dans le courant de l'été (par Adobe et Microsoft notamment).
Selon Kaspersky, Darkhotel utilise depuis début juillet une vulnérabilité zero day issue de la collection Hacking Team et ciblant Flash Player. L'exploit est hébergé sur un site web compromis (tisone360.com). « N'étant pas connu comme un client de Hacking Team, le groupe Darkhotel semble s'être emparé des fichiers lors de leur divulgation publique », explique l'éditeur russe.

27 antivirus contournés
Les chercheurs de la société estiment que, au cours de ces dernières années, le groupe de hackers a employé une demi-douzaine, voire plus, de ces vulnérabilités visant Adobe Flash Player et a investi largement pour bâtir cet arsenal. Le groupe de hackers a par ailleurs sophistiqué son kit d'infection, en améliorant notamment ses capacités à échapper aux antivirus. L'outil de téléchargement que déploient les hackers afin d'infecter les systèmes de leurs victimes identifie désormais 27 technologies d'antivirus, afin de les contourner.
« De précédentes attaques nous ont appris que Darkhotel espionne les Pdg, senior vice-présidents, directeurs marketing ou commerciaux et de hauts responsables en R&D », rappelle Kurt Baumgartner, chercheur en sécurité au sein des Kaspersky Lab.

Source : http://www.silicon.fr/darkhotel-recupere-faille-hacking-team-123796.html
Par Reynald Fléchaux

Les attaques DRDOS peuvent se propager via les clients BitTorrent | Le Net Expert Informatique

Les attaques DRDOS peuvent se propager via les clients BitTorrent

L'attaque DRDOS (Distributed Reflective Denial of Service) est une variante du DDoS, mais elle est plus puissante et elle peut se propager sur de nombreux protocoles incluant ceux du BitTorrent. Florian Adamsky de la City University London propose un article sur le potentiel nuisible du DRDOS concernant les protocoles BitTorrent.

La plupart connaissent les attaques DDoS, mais le DRDOS est un peu différent. Dans une attaque DDoS, le pirate contrôle un ensemble de machines zombies pour attaquer la cible. Dans une DRDOS, le pirate envoie le trafic à un réseau légitime (appelé le réflecteur) qui transmet ensuite le trafic à la victime. Le trafic qui est envoyé au réflecteur est modifié pour que pour l'adresse IP de la victime soit utilisé plutôt que le paquet d'origine. Et quand le réflecteur respecte les normes habituelles des protocoles internet pour établir la connexion, alors tout le trafic est balancé vers la victime. Et étant donné que cela implique d'envoyer une énorme quantité de trafic vers un réflecteur, les pirates ont trouvé le moyen de l'utiliser pour amplifier le trafic. Les attaques DRDOS peuvent être utilisées vers les protocoles TCP, DNS et NTP. Mais l'article d'Adamsky démontre aussi que le DRDOS peut être exploité avec de nombreux protocoles du BitTorrent.

Les protocoles uTP, MSE, DHT et BTSync sont vulnérables aux attaques DRDOS

Selon Adamsky, les protocoles BitTorrent affectés sont l'uTP (Micro Transport Protocol), le DHT (Distributed Hash Table) et le MSE (Message Stream Encryption). Ces protocoles sont intégrés en natif sur les clients de Torrent BitTorrent, uTorrent et Vuze. De plus, le protocole de synchronisation BTSync, qui est utilisé avec BitTorrent Sync, est également vulnérable. Florian Adamsky a démontré que les tests permettaient d'amplifier le trafic de 50 à 120 fois sur la norme BTSync.

Les attaques DRDOS sur les protocoles BitTorrent sont indétectables par les pare-feu

Mais la mauvaise nouvelle ne s'arrête pas là. En plus d'amplifier considérablement l'attaque, le DRDOS sur BitTorrent ne peut pas être détecté avec des pare-feu standard à cause de l'utilisation de ports dynamiques et du chiffrement pendant les échanges de données sur ces protocoles. Pour contrer ce type d'attaque, il faudrait utiliser une solution telle que DPI (Deep Packet Inspection) qui est trop coûteuse pour la majorité des infrastructures. BitTorrent a corrigé certains de ces problèmes avec sa version en bêta, mais Vuze et BitTorrent travaillent encore pour colmater les brèches qui permettent d'exploiter le DRDOS.

Source : http://actualite.housseniawriting.com/technologie/2015/08/16/les-attaques-drdos-peuvent-se-propager-via-les-clients-bittorrent/7227/
Par Houssen Moshinaly

L’Afrique menacée par la cybercriminalité | Le Net Expert Informatique

L’Afrique menacée par la cybercriminalité

L'Afrique est à la traîne en matière de législation sur la cyber-sécurité, un vide juridique qui constitue un véritable danger pour le continent, où, non seulement, il engendre d'énormes pertes économiques, mais porte atteinte à la souveraineté des pays du continent, en mettant les données personnelles des Etats et des citoyens à la merci des firmes internationales du numérique.

L'Afrique n'a aucune maîtrise de la chaine numérique. Par conséquent, elle se retrouve dans un système de colonisation et de dépendance numérique, fait observer le Pr Olivier Sagna, Secrétaire Général de l'observatoire sur les systèmes d'information, les réseaux et les inforoutes au Sénégal (OSIRIS).
Sagna regrette le fait que « l'Afrique ne possède pas de point d'échange internet, tous les messages échangés passent par un point de transit, qui en fonction des accords et des coûts de droits de communications internationaux, coûte des millions de dollars » aux pays du continent noir.
Selon le Directeur associé de Performances Group au Sénégal, Mouhamed Tidiane Seck, plus de 17 millions de victimes dans le monde ont fait les frais de la cybercriminalité, entre 2012 et 2013. Soit une augmentation de 87% de cas malveillants, occasionnant des conséquences économiques évaluées à trois milliards de dollars de perte bancaire.
L'Afrique du Sud, est l'un des rares pays du continent, grâce à la force de ses lobbys, à avoir mis en place une politique de protection des données personnelles à l'endroit des firmes internationales du numérique.
Concernant l'aspect juridique sur la protection des données personnelles, le Dr Mouhamadou Lo, Président de la Commission de protection des Données Personnelles (CDP) refuse de parler de « désert juridique » en Afrique. « En Afrique, en plus de l'Afrique du Sud, il existe deux textes au niveau de la région Ouest africaine », a indiqué Dr Mouhamadou Lo.
Sur cette dynamique, il faut souligner que la Convention de l'Union Africaine sur la Cyber-sécurité et la protection des données à caractère personnel a été adoptée à Malabo en 2014. « Voter une loi est un premier pas, mais il faut la mise en place d'une commission opérationnelle », a-t-il conclu.

Source : http://www.lemagazinedumanager.com/11300-senegal-la-cybercriminalite-une-menace-pour-lafrique.html

On peut voler des identifiants Active Directory depuis Internet via SMB | Le Net Expert Informatique

On peut voler des identifiants Active Directory depuis Internet via SMB

Deux chercheurs ont montré sur la conférence Black Hat 2015 qu'une attaque via le protocole de partage de fichiers SMB connue pour s'effectuer au sein d'un réseau local peut en fait servir à attaquer des serveurs Windows hébergés dans le cloud.

Lors de la conférence Black Hat 2015 (Las Vegas, du 1er au 6 août), deux chercheurs ont montré qu'une technique d'attaque via le protocole de partage de fichiers SMB que l'on croyait ne fonctionner que sur les réseaux locaux peut en fait être exécutée sur Internet. Avec cette attaque, dite de relais SMB, un ordinateur Windows appartenant à un domaine Active Directory laisse apparaître les informations d'identification de l'utilisateur quand celui-ci consulte une page web, un courriel dans Outlook ou regarde une vidéo dans Windows Media Player. L'attaquant peut ensuite détourner ces identifiants pour s'authentifier au nom de l'utilisateur sur des serveurs Windows où il dispose d'un compte, y compris ceux hébergés dans le cloud.
Dans un réseau Active Directory, les ordinateurs Windows retournent automatiquement leurs informations d'identification pour accéder aux différents services de partage de fichiers à distance, aux serveurs de messagerie Microsoft Exchange ou aux outils de collaboration SharePoint. Ces informations d'authentification – en l'occurrence le nom de l'ordinateur, le nom de l'utilisateur, tous deux en texte clair, et un hash cryptographique dérivé du mot de passe de l'utilisateur – sont envoyées à l'aide du protocole d'authentification NTLMv2. En 2001, des chercheurs en sécurité avaient déjà mis au point une attaque dite par relais SMB : en se positionnant entre un ordinateur Windows et un serveur, les attaquants pouvaient intercepter les informations d'identification, puis les relayer vers le serveur et s'authentifier à la place de l'utilisateur légitime. Mais à l'époque, tout le monde pensait que l'attaque ne fonctionnait qu'en local.

Authentification configurée par défaut dans IE
Sauf que, dans Internet Explorer, l'authentification de l'utilisateur est configurée par défaut avec l'option « ouverture de session automatique réservée à la zone intranet ». Or, les chercheurs en sécurité Jonathan Brossard et Hormazd Billimoria, ont constaté que cette option était ignorée et qu'il était possible de duper le navigateur pour que celui-ci laisse fuiter vers Internet les informations Active Directory de l'utilisateur – c'est à dire son nom et la séquence de code cryptographique basée sur son mot de passe – pour les transmettre à un serveur SMB distant contrôlé par les pirates. Les chercheurs ont pu suivre le trajet d'un fichier DLL propre à Windows, utilisé aussi bien par Internet Explorer que par de nombreuses applications pouvant accéder aux URL, comme Microsoft Outlook, Windows Media Player ou d'autres programmes tiers. « Quand l'application veut accéder à une URL, le fichier DLL vérifie les informations d'authentification dans le registre, mais tout en les ignorant », ont expliqué les chercheurs pendant leur présentation.

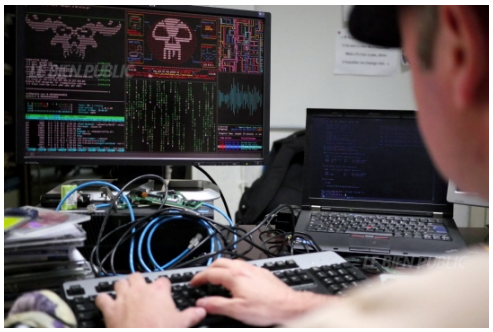
Toutes les versions actuelles de Windows et d'Internet Explorer (ou encore supportées) sont concernées par le problème. « C'est la première attaque à distance capable de compromettre potentiellement Windows 10 et le nouveau navigateur Microsoft Edge », a alerté Jonathan Brossard. « Nous sommes au courant de ce problème et nous enquêtons à ce sujet », a déclaré jeudi un représentant de Microsoft par courriel.

Plusieurs scénarios possibles
« Une fois que les attaquants ont mis la main sur les informations d'identification de l'utilisateur, ils peuvent les utiliser de différentes façons », a précisé Jonathan Brossard. Un premier scénario consisterait à monter une attaque par relais SMB pour s'authentifier à la place de la victime sur des serveurs hébergés hors du réseau local en utilisant une fonctionnalité appelée « NTLM over http », ajoutée pour étendre le périmètre des réseaux dans les environnements cloud. Les pirates pourraient notamment accéder à un shell distant sur le serveur qu'ils utiliseraient ensuite pour installer des logiciels malveillants ou exécuter des programmes exploitant des failles. Si le serveur distant est un serveur Exchange, les attaquants pourraient télécharger toute la boîte aux lettres de l'utilisateur.

Un autre scénario impliquerait de casser la séquence de code cryptographique et de l'utiliser pour accéder à un serveur Remote Desktop Protocol. Des pirates peuvent y arriver en utilisant des plates-formes spécialisées ou des services donnant accès à une grosse puissance de calcul. Un mot de passe de huit caractères ou moins peut être craqué en deux jours environ. « Et, déchiffrer toute une liste de hashs volés ne serait pas plus long, puisque le processus teste toutes les combinaisons à la fois », a ajouté le chercheur. Des identifiants Windows volés via Internet seraient également utiles à des attaquants qui ont déjà réussi à se faufiler dans un réseau local, mais ne disposent pas des privilèges d'administration. En envoyant un simple message électronique à l'administrateur légitime, ils pourraient récupérer ses identifiants dans Outlook et utiliser le hash volé pour mener une attaque par relais SMB contre les serveurs connectés au réseau local.

Source : http://www.lemondeinformatique.fr/actualites/lire-black-hat-2015-on-peut-voler-des-identifiants-active-directory-depuis-internet-via-smb-62000.html
Par Jean Elyan et IDG News Service

Alerte à partager : Vigilance face au logiciel malveillant Didrex | Le Net Expert Informatique

	Alerte à partager : Vigilance face au logiciel malveillant Didrex

Vols d'identifiants et d'informations personnelles, transferts de fonds non autorisés… devant la multiplication du nombre d'ordinateurs infectés par le logiciel malveillant Dridex, la gendarmerie nationale lance une mise en garde à tous les utilisateurs d'Internet et distille quelques conseils pour se prémunir de la menace.

Depuis le début du mois de juin 2015, la France fait face à une campagne massive de dissémination de logiciel malveillant (malware) par le biais de courriers électroniques non sollicités (Spam). Ce logiciel connu sous le nom de «Dridex» a pour vocation d'infecter les postes informatiques utilisant le système d'exploitation Microsoft Windows (toutes versions allant de Windows XP à Windows 8.1). Actuellement, 28 000 postes sont infectés en France.

Un mail trompeur sous forme de facture
Le but de ce logiciel est de prendre le contrôle de la machine à des fins crapuleuses. En effet, après avoir été infecté, le poste informatique compromis va servir, à la fois, à la collecte de données personnelles (numéro de compte, identifiants et mot de passe de connexion, numéro de carte bancaire, historique de navigation, etc.) ainsi qu'à la réalisation de manœuvres frauduleuses (transfert d'argent, connexion à des sites Internet, envoi de message, relais mandataire, etc.) et ce, à l'insu du légitime propriétaire de la machine. La victime, particulier ou entreprise, est destinataire d'un message électronique contenant une pièce jointe, le plus souvent, un document au format Microsoft Word/Excel, voire dans certains cas, au format portable Document File (.pdf). Cette pièce jointe est souvent intitulée «Invoice» ou «facture» et l'objet du message est souvent en lien avec un paiement ou une facture.

Tous vos codes et données collectés
L'ouverture de cette pièce jointe entraîne, lorsque l'activation des macros est autorisée, le téléchargement d'un logiciel malveillant qui va permettre la prise de contrôle à distance de la machine. Par la suite, lorsque la victime se connecte au site de sa banque en ligne, le malware, va récupérer toutes les informations intéressantes (identifiant, mot de passe, nom, prénom, numéro de téléphone, numéro de compte, numéro de carte bancaire, solde du compte, etc.). Muni de l'ensemble de ces données, l'escroc va alors réaliser des transferts de fonds depuis le compte de la victime vers celui d'une tierce personne pouvant se trouver en France, mais plus généralement à l'étranger.

Comment se prémunir de Didrex
-> Observez une grande vigilance vis-à-vis de la messagerie électronique et ayez un esprit critique sur l'origine des messages qui vous parviennent
– Supprimez tous les e-mails suspects prospectifs (spam) reçus dans la boîte de messagerie, surtout s'ils contiennent des pièces jointes.
– N'ouvrez surtout pas les documents en pièce jointe contenus dans un spam; il suffit de les supprimer.
– Si vous avez des suspicions sur un courriel prétendant provenir d'organisations légitimes (banques, administrations, sites de ventes, etc…), il vaut mieux avant, vérifier auprès de ces organisations en question, la véracité de l'envoi du message et l'authenticité de la pièce jointe.
– Installez une solution antimalware qui protège également des spams. En premier lieu, cela devrait du moins réduire ou au mieux éliminer le risque d'ouvrir accidentellement un de ces pourriels et pièces jointes malveillantes
– Désactivez les macros exécutables automatiquement dans Microsoft Word et Excel
– S'il y a soupçon d'infection, changez immédiatement le mot de passe d'accès au compte bancaire en ligne, pour ce faire veuillez contacter rapidement votre établissement bancaire et l'alerter d'un risque potentiel de fraude. DRIDEX étant capable de dérober d'autres types d'identifiants de connexion, il est vivement recommandé pour tous autres accès à des services en ligne, de modifier les « logins et mots de passe ». ATTENTION : faites ceci en utilisant un autre moyen de connexion que l'ordinateur suspecté d'infection
– Procédez à la même mesure concernant tous autres comptes de services internet dont vous êtes titulaires (fournisseur d'accès internet, vente en ligne, réseaux sociaux, etc…). Dridex vole aussi ce genre d'information
– Surveillez l'activité de vos comptes bancaires et vérifiez la légitimité de vos transactions.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.bienpublic.com/actualite/2015/08/06/la-gendarmerie-appelle-a-la-vigilance-face-a-didrex

---

Une faille de sécurité de Hacking Team a été utilisée par un important groupe de pirates | Le Net Expert Informatique

Une faille de sécurité de Hacking Team a été utilisée par un important groupe de pirates

Des groupes de pirates informatiques ont utilisé, peu après leur publication, le contenu des fichiers volés à l'entreprise Hacking Team pour se livrer à des tentatives de piratage, révèle l'entreprise de sécurité Kaspersky. Selon Kaspersky, le groupe « Darkhotel », notamment, a utilisé des vulnérabilités qui avaient été employées par Hacking Team, une entreprise spécialisée dans la vente de logiciels de surveillance.

« Darkhotel » s'est notamment signalé par le passé pour avoir utilisé des méthodes élaborées pour placer des logiciels espions – par exemple en prenant le contrôle des réseaux wifi utilisés dans de grands hôtels. Parmi ses cibles figurent des dirigeants de très grandes entreprises, dans la chimie, les cosmétiques ou la pharmacie, des militaires et des responsables d'ONG, dans plusieurs pays d'Europe, d'Asie et d'Afrique, toujours selon Kaspersky. Des cibles et un niveau de sophistication qui laissent supposer à Kaspersky qu'il s'agit d'un groupe étatique ou soutenu par un Etat.
Hacking Team, société italienne à la réputation sulfureuse, est spécialisée dans la vente de logiciels espions et de dispositifs de surveillance électronique. L'intégralité des données de l'entreprise a été publiée en ligne après un piratage, y compris le contenu des messageries de la société. Des associations et des élus européens ont demandé l'ouverture d'une enquête sur les pratiques commerciales de la société, soupçonnée d'avoir notamment vendu des logiciels au Soudan, et une réforme de la législation sur l'exportation de ces technologies.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemonde.fr/pixels/article/2015/08/10/une-faille-de-securite-de-hacking-team-a-ete-utilisee-par-un-important-groupe-de-pirates_4719735_4408996.html

---

Démonstrations de piratages au salon de «hackers» de Las Vegas | Le Net Expert Informatique

Démonstrations de piratages au salon de «hackers» de Las Vegas

Des pirates informatiques ont fait aussi bien que la bande de George Clooney dans Ocean's eleven en arrivant samedi, lors d'un salon à Las Vegas, à ouvrir un coffre-fort et à tromper la vigilance des caméras de surveillance sans être repérés.

La réalité a fini par dépasser la fiction. Eric Van Albert et Zach Banks, deux chercheurs en informatique, ont fait dans la vraie vie ce que Hollywood a déjà accompli à moult reprises. Ils ont détourné le flux vidéo de caméras de sécurité pour injecter à la place leurs propres images et ainsi tromper la vigilance des surveillants en leur faisant croire que tout était normal. En général, au cinéma, c'est là que les cambrioleurs en profitent pour amasser leur butin et s'enfuir ni vu ni connu. Dans les faits, il ne s'agit que d'une simple démonstration, réalisée à l'occasion de la Def Conf, un célèbre salon de «hackers» à Las Vegas.
«Nous avons mis sur pied notre dispositif en restant le plus fidèle possible à ce qui se fait dans les films», a déclaré Eric Van Albert. «Nous voulions voir à quel point ce type d'attaque était plausible», a-t-il ajouté. Lui et son acolyte ont dépensé environ 500 dollars pour fabriquer l'outil qui permet de pénétrer le câble reliant les caméras aux écrans des gardiens. Le flux est ensuite passé à la moulinette d'un programme informatique qui restitue des images inoffensives.

Ouvrir un coffre-fort avec une clef USB
Les deux chercheurs pourraient s'associer avec Daniel Petro et Oscar Salazar de Bishop Fox, une entreprise de sécurité informatique qui a réussi à ouvrir un coffre-fort avec une clé USB. Le coffre n'était pas une boîte en métal épais «toute bête» mais était équipé pour compter les billets et créditer les comptes de dépositaires par internet. Les deux hommes ont indiqué qu'ils avaient choisi la prise USB parce qu'elle leur permettait d'utiliser un ordinateur plus puissant pour ouvrir le coffre. Mais Daniel Petro a souligné que, de toute façon, il fallait accéder physiquement au coffre pour pouvoir en retirer l'argent.
Pour éviter que ce scénario hollywoodien ne se répète, les deux hommes ont prévenu la compagnie qui fabrique les coffres-forts, et qui a déjà trouvé une parade à ce type d'attaque.

Source : http://www.lefigaro.fr/secteur/high-tech/2015/08/09/32001-20150809ARTFIG00158-des-hackers-s-inspirent-de-hollywood-pour-piller-des-coffres-forts.php

---

Le Pentagone visé par une cyber-attaque russe ! | Le Net Expert Informatique

Le Pentagone visé par une cyber-attaque russe !

Aux alentours du 25 juillet, des pirates informatiques russes ont lancé « une cyber-attaque sophistiquée » contre un système de courriels non confidentiels de l'état-major interarmées au Pentagone, selon des responsables américains ayant requis l'anonymat et cités par la chaîne NBC. Aucune fuite d'informations secrètes n'aurait eu lieu.

Le système informatique du Pentagone est débranché depuis une quinzaine de jours, l'attaque ayant visé 4 000 civils et militaires qui travaillent pour l'état-major interarmées, précise NBC.
Le Pentagone confirme avoir mis le système hors-circuit pour mener une enquête approfondie.
« Par principe et pour des raisons de sécurité opérationnelle, nous ne commentons pas les cyber-incidents ou attaques contre nos réseaux », a indiqué la lieutenant-colonel Valérie Henderson, l'une des porte-paroles du Pentagone dans un courriel.
Selon NBC, l'attaque était automatisée et a réussi, en moins d'une minute, à amasser et à rediffuser les informations collectées sur Internet. La cyber-attaque a été coordonnée par le biais de comptes cryptés et par les réseaux sociaux, d'après ces responsables américains anonymes. Le gouvernement russe n'a pas été directement accusé d'être à l'origine de l'attaque. Mais au regard de sa sophistication, l'attaque aurait été menée par des gens travaillant pour le compte d'une agence gouvernementale, précise NBC.
Ce n'est pas la première fois que des « hackers russes » mythiques sont accusés d'attaques contre les sites de médias et d'institutions occidentales. Fin avril dernier, le porte-parole du Kremlin, Dmitri Peskov, commentait les rapports sur les attaques de « pirates informatiques russes » contre les réseaux informatiques américains et estimait qu'accuser Moscou de tous les maux « était devenu une sorte de sport ».

Source : http://www.partiantisioniste.com/actualites/le-pentagone-vise-par-une-cyber-attaque-russe-2492.html

Les e-mails de hauts gradés de l’armée américaine piratés | Le Net Expert Informatique

	Economie – Les e-mails de hauts gradés de l’armée américaine piratés

Le système de messagerie utilisé par 4 000 hauts gradés de l'armée américaine a été compromis fin juillet par des pirates informatiques et fermé par le Pentagone, selon les médias américains. L'enquête privilégie la piste russe.

Comme un air de Guerre froide. Des « officiels » du Pentagone ont affirmé, jeudi 6 août, à la chaîne américaine NBC, que des pirates informatiques russes avaient réussi à s'introduire dans le système de messagerie informatique utilisé par 4 000 militaires et civils travaillant au Comité des chefs d'état-major interarmées.
La découverte de cette opération de cyberespionnage, lancée aux alentours du 27 juillet, a amené les autorités militaires à fermer entièrement le système de messagerie informatique utilisé par ces hauts gradés. Il ne sera remis à disposition du personnel qu'à la fin de l'enquête.

Cyber Guerre froide ?
Cette attaque est d'autant plus dommageable pour le Pentagone que ce n'est pas la première fois que des cyberespions s'engouffrent dans une faille du système de protection informatique des plus hautes sphères de l'État. Le président américain Barack Obama et le Département d'État (ministère américain des Affaires étrangères) ont ainsi déjà été pris pour cible ces quatre derniers mois.
Ces précédentes opérations avaient été attribuées par plusieurs entreprises de sécurité informatique à un même groupe : Cozy Bear. Leurs membres seraient russes, estiment la société Kaspersky qui leur a consacré plusieurs rapports.
Interrogé par le quotidien britannique « The Guardian », Dmitri Alperovitch, le fondateur de la firme de sécurité informatique CrowdStrike, a noté une recrudescence des attaques informatiques russes visant des cibles américaines depuis l'instauration des sanctions économiques imposées depuis plus d'un an à la Russie par les États-Unis et ses alliés.

Pas de vol d'informations classifiées
Mais même si l'attaque contre le Pentagone est bien le fait de pirates russes, rien n'indique qu'ils ont agi sur ordre du Kremlin. Il peut s'agir de hackers « patriotes », souligne le site « Daily Beast », ou d'un groupe indépendant de pirates informatiques recruté par n'importe quel autre pays ou organisé pour espionner à sa place.
Ils ont à chaque fois utilisé la même technique : un e-mail piégé envoyé à des employés du service visé qui installe un virus dès que l'un d'eux clique sur un lien contenu dans le message. Des similitudes dans les messages et des traces laissées par les pirates sur les ordinateurs indiquent qu'ils ont utilisé les mêmes « armes » (comme un même type de virus personnalisé) pour commettre leur forfait.
Lors de l'attaque contre les hauts gradés du Pentagone, aucune information classifiée, qui ne s'échange que sur une messagerie spécifique, n'aurait été dérobée par ces pirates informatiques, ont affirmé ces sources à plusieurs médias américains. Reste que des échanges, comportant peut-être des informations personnelles sur les membres du premier cercle de l'armée américaine, ont été volés.

Source : http://www.france24.com/fr/20150807-emails-militaires-hauts-grades-armee-americaine-piratage-hacking-russie-pentagone
Par Sébastian SEIBT

La SNCB victime d’un piratage | Le Net Expert Informatique

La SNCB victime d’un piratage

Les systèmes de paiement électroniques de la société ferroviaire sont la cible d'une attaque informatique depuis plusieurs heures.

Les systèmes de paiement électroniques de la SNCB sont la cible d'une attaque informatique depuis plusieurs heures. « Il s'agit d'une attaque d'origine externe dont les premiers signes ont été détectés mercredi soir, confirme la porte-parole, Nathalie Pierard. Nous travaillons avec les services de sécurité informatique du Fédéral pour protéger nos serveurs.» Ce sont les systèmes de paiement électroniques qui sont touchés, tant aux guichets qu'aux automates ou sur le mobile.
« Par période, les services sont fortement ralentis, poursuit Nathalie Pierard. À d'autres, ils sont inaccessibles. On a connu une accalmie vers midi puis les ralentissements ont repris en milieu d'après-midi. »

Pas de surfacturation à bord
Suite à ce piratage dont l'origine est toujours indéterminée, la SNCB a décidé de ne pas faire payer la surfacturation de sept euros pour les billets achetés dans le train.

Source : http://www.lesoir.be/956193/article/economie/2015-08-06/sncb-victime-d-un-piratage