Nouvelle menace DDoS : Portmapper | Le Net Expert Informatique

Nouvelle menace DDoS : Portmapper

La société Level 3 vient de révéler une nouvelle possibilité d'attaque en DDoS via Portmapper.

Depuis quelques temps, les attaques de type DDoS sont en recrudescence. Et la société Level 3 vient de dévoiler un nouveau vecteur d'attaques : Portmapper.
Durant l'année dernière, certaines attaques ont atteint des débits de plusieurs centaines de gigabits par seconde, entraînant l'effondrement de sites. Jusqu'à maintenant, les principaux vecteurs d'attaques étaient les services basés sur UDD , tout particulièrement DNS, NTP et SSDP. Ces services sont utilisés à la fois pour masquer l'origine de l'attaque et amplifier la bande passante. Toutefois, les administrateurs réseaux ont depuis réussi à mettre en échec ces types d'attaques.

Service d'annuaires pour RPC
C'est pour cette raison que c'est désormais le mécanisme Portmapper qui est exploité. Portmapper est également appelé rpcbind, portmap ou RPC Portmapper. II s'agit d'un mécanisme avec lequel les services RPC (Remote Procedure Call) s'entregistrent pour permettre des appels via l'internet. Comme le souligne Level 3, on peut considérer Portmapper comme un service d'annuaires pour RPC.
Lorsqu'un client cherche à trouver le service approprié, le Portmapper est sollicité pour l'assister. Et la taille de la réponse renvoyée par Portmapper dépend les services RPC qui opèrent sur l'hôte. Dans ces conditions, il est relativement facile de masquer une attaque DDoS par ce biais car les réponses Portmapper n'ont pas une taille fixe.
Le document de Level 3 est accessible à cette adresse :
http://blog.level3.com/security/a-new-ddos-reflection-attack-portmapper-an-early-warning-to-the-industry
Les experts de l'entreprise recommandent quelques méthodes pour contrer cette menace, en particulier la désactivation des services de ce type qui ne sont pas indispensables.

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

Source : http://www.mag-securs.com/news/articletype/articleview/articleid/34705/nouvelle-menace-ddos-portmapper.aspx
Par Raphaël Stencher

Kaspersky trompe ses client avec de faux virus ? | Le Net Expert Informatique

	**Kaspersky trompe ses client avec de faux virus ?**

Deux ex-employés de l'éditeur accusent Kaspersky d'avoir inondé ses concurrents de fichiers spécialement conçus pour tromper leur algorithme de détection de malwares. Et créer de faux positifs chez les utilisateurs.

Selon Reuters, Kaspersky a tenté de faire passer des fichiers bénins pour malicieux afin de tromper les capacités de détection de ses concurrents sur le marché des antivirus. Ces affirmations, très graves pour l'éditeur russe, se basent sur les déclarations à nos confrères de deux ex-employés de la société basée à Moscou, aujourd'hui parmi les leaders mondiaux des logiciels de sécurité.
Cette duperie, qui aurait démarré il y a plus de dix ans – avec un pic entre 2009 et 2013 -, ciblait notamment les antivirus de Microsoft, AVG ou Avast et visait à les inciter à effacer des fichiers importants sur les PC de leurs utilisateurs. Les deux sources de nos confrères, qui demeurent anonymes, affirment que des chercheurs ont été affectés à ces sabotages pendant des semaines ou des mois, avec pour tâche principale la rétro-ingénierie des technologies de détection des concurrents ciblés. Une étape indispensable à la mise au point de faux positifs.

Intoxiquer la concurrence
Reuters assure que, dans certains cas, la décision a été prise par Eugene Kaspersky en personne (en photo ci-dessus), le fondateur de l'éditeur russe souhaitant se venger de concurrents qui, selon lui, se contentaient d'imiter sa technologie. La société a démenti ces pratiques, assurant « n'avoir jamais mené de campagne secrète pour tromper des concurrents avec de faux positifs (des fichiers bénins identifiés comme malwares, NDLR) ».
En 2010, Kaspersky s'était plaint de l'exploitation que ses concurrents faisaient de ces travaux. A l'appui de sa démonstration, l'éditeur avait créé 10 fichiers sans risque et les avaient déclarés comme malicieux à VirusTotal, l'outil de partage d'informations sur les menaces de Google. Une semaine et demi plus tard, 14 fournisseurs d'outils de sécurité estimaient ces fichiers dangereux, suivant aveuglément les conclusions de la société russe, selon Kaspersky.
D'après les deux sources de Reuters, Kaspersky ne se serait pas arrêté à cette opération de communication. La société injectait ainsi du code malicieux dans des fichiers fréquemment rencontrés sur les PC puis les signalait anonymement à VirusTotal dans l'espoir de voir les antivirus concurrents assimiler ces fichiers essentiels au fonctionnement d'un PC à des malwares.

Pratiques connues
Reuters affirme par ailleurs que Microsoft, AVG et Avast lui ont confirmé que des tiers non identifiés avaient tenté d'introduire de faux positifs dans leur mécanisme de détection au cours des dernières années. Dennis Batchelder, qui dirige la recherche antimalware de Microsoft, a ainsi expliqué à Reuters avoir identifié, à partir de mars 2013, des fichiers altérés afin de paraître malicieux. Et d'affirmer que ses équipes ont isolé des centaines, voire des milliers de cas de la sorte. Sans toutefois faire un quelconque lien avec Kaspersky. Plus largement, aucun concurrent du Russe n'a émis de commentaire sur l'implication éventuelle de la société moscovite.

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

Source : http://www.silicon.fr/kaspersky-accuse-infecte-concurrents-faux-virus-124122.html#LJcrRvhoptort4dm.99

La France, 1ère cible des attaques DDoS de botnet en Europe | Le Net Expert Informatique

La France, 1ère cible des attaques DDoS de botnet en Europe

Kaspersky Lab nous apprend qu'au 2ème trimestre, la France était la 1ère cible des attaques DDoS de botnet en Europe.

En effet, les trois quarts des ressources attaquées au cours du deuxième trimestre 2015 par des botnets se situent dans 10 pays seulement (source : Kaspersky DDoS Intelligence). En tête du classement, on trouve les Etats-Unis et la Chine qui enregistrent un grand nombre d'attaques en raison du faible coût d'hébergement de ces pays. Cependant, le nombre croissant de pays affectés par ce type d'attaque prouvent qu'aucun territoire n'est sécurisé face aux attaques DDoS.
Dans ce Top 10, la France figure en 6ème position, mais est aussi le premier pays européen avec 2,8% des attaques (en hausse par rapport au 1er trimestre), devant la Croatie (8ème avec 1,4% des attaques) et l'Allemagne (9ème avec 1% des attaques).
« Les techniques d'ingénierie sociale, l'apparition de nouveaux types d'appareils avec accès internet, les failles logicielles et la sous-estimation de l'importance d'une protection anti-malware ont contribué à la diffusion des botnets et à l'augmentation du nombre d'attaques DDoS, explique Evgeny Vigovsky, Directeur de Kaspersky DDoS Protection, chez Kaspersky Lab. Par conséquent, des entreprises complètement différentes peuvent être ciblées indépendamment de leur location, de leur taille ou de leur type d'activité. La liste des victimes protégées des attaques DDoS par Kaspersky Lab au second trimestre 2015 incluait des organisations gouvernementales, des institutions financières, des médias de masse et même des institutions éducatives ».
Kaspersky Lab a d'ailleurs noté une forte augmentation du nombre d'attaques au cours de la première semaine de mai, le pic d'attaques par jour (1960) ayant été enregistré le 7 mai.
Sur le plan technique, les cybercriminels impliqués dans ce type d'attaques investissent de plus en plus dans la création de botnets de produits réseaux comme les routeurs et les modems DSL. Ce qui préfigure certainement d'une augmentation du nombre d'attaques DDoS utilisant des botnets à l'avenir.

Source : http://www.infodsi.com/articles/157658/france-1ere-cible-attaques-ddos-botnet-europe.html

La foudre frappe des serveurs Google rendant des données momentatnément inaccessibles | Le Net Expert Informatique

La foudre frappe des serveurs Google rendant des données momentatnément inaccessibles

A la suite d'un orage en Belgique, des serveurs appartenant à Google ont été privés de courant avec pour conséquence l'inaccessibilité de certaines données personnelles.

La foudre peut frapper deux fois au même endroit, la preuve un bâtiment situé en Belgique a reçu jeudi dernier quatre éclairs en l'espace d'un orage. Celui-ci, un data-center abrite des centaines de serveurs appartenant à Google. A l'intérieur de ceux-ci étaient stockées les données personnelles de nombreux utilisateurs et lorsque la foudre a frappé, le courant a sauté.
La BBC relate que cet aléa météorologique a eu quelques conséquences pour certains utilisateurs du service de stockage en ligne Google Drive. Leurs données ont en effet été momentanément inaccessibles.
Contacté par MyTf1news, le géant de l'Internet a réagi. « C'est une quantité infinitésimal qui a été affectée » a expliqué un responsable avant de poursuivre : « Aucune donnée n'a été perdue grâce à un système de sauvegarde décentralisé ». Dans les faits, il existait une copie des données affectées par la coupure de courant dans un autre data-center ailleurs sur la planète. Les documents des utilisateurs ont donc étaient inaccessibles juste le temps que ce système prenne le relai.
Les bâtiments de ce type sont généralement très bien protégés contre la foudre mais la répétition de ce phénomène n'avait apparemment pas été anticipée. Interrogé par la BBC, Justin Gale, un responsable d'Orion, une entreprise britannique spécialisée dans la protection des infrastructures contre la foudre revient sur le phénomène. L'éclair n'a pas besoin de frapper la structure en elle-même explique-t-il avant de préciser : « Un câble à un kilomètre peut être touché et le choc peut remonter jusqu'au data-center et tout faire disjoncter » détaille-t-il.
Dans un communiqué publié en ligne, Google relativise l'incident. Selon l'entreprise « moins de 0,000001% » de la surface des disques durs alloués à la zone géographique est concernée. La compagnie a néanmoins fait savoir qu'elle avait l'intention de renforcer ses protections contre les coupures de courant pour assurer la sécurité des données stockées sous sa responsabilité.

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

Source : http://lci.tf1.fr/high-tech/des-serveurs-de-google-frappes-par-la-foudre-des-donnees-personnelles-8646545.html
Illustration. Un éclair / Crédits : Comstock/Thinkstock

Cyber-attaque de pompe à morphine : mise en garde de

la FDA | Le Net Expert Informatique

Cyber-attaque de pompe à morphine : mise en garde de la FDA

La FDA met en garde contre les risques de prise de contrôle à distance des pompes à morphine ou PCA (de type PCA analgésie autocontrôlée par le patient) de type Symbiq Infusion System (produites par la marque Hospira). Ces pompes sont généralement prescrites dans le cadre de soins de suite ou d'hospitalisations à domicile.

Elles sont reliées sans fil aux systèmes de communication de l'hôpital pour transmettre des données sur les doses utilisées quotidiennement. Ces informations sont utilisées par les médecins pour adapter les protocoles de soins.

Un cyber-spécialiste démontre la possibilité d'attaques

C'est la deuxième fois en 4 mois que les pompes de ce fabricant font l'objet de cyber attaques, les premiers modèles impliqués étaient les LifeCare PCA3 et PCA 5 qui permettent de délivrer différents types de médicaments ou de traitements intraveineux.

Hospira a annoncé avoir cessé de produire les pompes en question ainsi que les Symbiq Infusion Systemet la FDA met en garde les établissements et les professionnels en les incitant à ne plus utiliser ces dispositifs.

Le département de la sécurité américain s'est saisi du dossier en raison des risques associé à ces cyber attaques (surdoses, ou sous dosage).

C'est un cyber spécialiste – Billy Rios [2] – qui a le premier soulevé cette question sur son blog et expliquant qu'il avait pu modifier les paramètres des pompes à distance sans disposer des codes spécifiques à chaque machines qui sont théoriquement indispensables pour modifier les doses.

Aucun cas de cyber attaque n'a été rapporté en utilisation thérapeutique aux Etats-Unis jusqu'à présent.

Une utilisation contrôlée en France – en théorie

En France, les pompes de type PCA sont utilisées dans les hôpitaux, en hospitalisation à domicile (dans un contexte de lien ville-hôpital), dans les services de soins palliatifs et dans certains centres de soins de suites/maisons de retraite médicalisés.

Elles servent à la prise en charges des douleurs chroniques de l'adulte, essentiellement d'origine cancéreuses et en soins palliatifs. Les principales marques de pompes à morphine de type PCA sont marque Vygon, Baxter, Gelstar, CADD Legacy et Rytmic Plus.

Les pompes à PCA électroniques ne doivent – en théorie – être manipulées que par le personnel médical (médecin ou IDE). Chaque marque diffuse avec le matériel un manuel d'utilisation pour les soignants et des codes permettant de modifier les paramètres ou changer les piles. Mais depuis quelques années, on peut trouver sur Internet des copies de ces manuels, ce qui pourrait permettre aux utilisateurs qui auraient récupéré les codes de façon illicite de modifier les paramètres dans un but de mésusage.

Source : http://www.medscape.fr/voirarticle/3601689
Par Dr Isabelle Catala avec Robert Lowes

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

Votre iPhone est débridé ? Alors vous l’avez rendu vulnérable | Le Net Expert Informatique

	Votre iPhone est débridé ?Alors vous l’avez rendu vulnérable

Quand la firme d'espionnage Hacking Team s'est faite détroussée de 400 gigaoctets de documents internes compromettants sur ses activités, ces derniers ont révélé des failles importantes dans les téléphones iPhone qui ont subi un débridage par leur propriétaire.

Débrider son iPhone le rendrait vulnérable aux intrusions.

La firme d'espionnage Hacking Team en Italie s'est fait prendre, le moins qu'on puisse dire, les «culottes baissées».

Imaginez une société privée, qui vend ses services aux plus offrants – généralement des gouvernements -, développe des procédés informatiques pour infiltrer et dérober à l'aide de logiciels espions et autres chevaux de Troie les ordinateurs de sociétés ou de gouvernements amis comme ennemis.

Et bien Hacking Team s'est fait littéralement détrousser de 400 Go de documents par un petit groupe de pirates qui les a mis en ligne. On y a appris beaucoup de choses, dont que les iPhone débridés par leur propriétaire les rendaient vulnérables aux intrusions.

Hacking Team dispose de moyens pour percer tout type de systèmes d'exploitation; Windows, Mac OS, Linux et les systèmes mobiles comme iOS, Android, Symbian et même BlackBerry.

Si l'espionnage de haute voltige ne concerne véritablement que les services de renseignements des gouvernements, il est intéressant de constater que les utilisateurs d'iPhone – c'est-à-dire vous et moi – deviennent potentiellement des cibles quand les appareils tournant sous iOS sont débridés (jailbreakés) par leurs utilisateurs.

À QUOI SERT DE DÉBRIDER SON IPHONE?

Le débridage permet de passer outre les verrouillages imposés par Apple pour ses téléphones iPhone. Ainsi, il devient possible d'installer des extensions non approuvées et accéder à toutes les fonctions du système.

À chaque mise à jour du système iOS (iOS 8.1, 8.2, 8.3), Apple colmate les brèches découvertes, mais les spécialistes du débridage trouvent toujours un moyen de contourner les parades.

En soi, débrider son appareil mobile n'est pas illégal, mais la manœuvre lui fait perdre sa garantie, auquel cas le propriétaire doit auparavant remettre en état son iPhone pour le faire réparer.

OUPS, DÉBRIDER OUVRE DES «PORTES» DU IPHONE

Dans le grand déballage de documents de Hacking Team, on apprend que les iPhone et iPad modifiés par débridage (tous deux roulent le même système iOS) devenaient vulnérables aux intrusions par ceux qui employaient les outils d'Hacking Team.

Pour environ 72 000 $, Hacking Team vendait au client un module de surveillance (snooping module) capable d'infiltrer les iPhone. Seul préalable, les appareils iOS devaient être débridés.

Note aux petits malins du bidouillage, votre iPhone «maison» a peut-être les portes grandes ouvertes, quel bel accueil pour les intrus!

Apple a depuis peu un argument de poids pour décourager la pratique du débridage. La société fait d'ailleurs tout en son possible pour empêcher les développeurs d'applications de sortir des limites permises d'iOS afin de protéger l'intégrité de son système mobile.

Plus encore, un iPhone débridé et infecté permet non seulement d'accéder à son contenu, mais de pénétrer les informations contenues dans l'ordinateur qui sert à sa synchronisation.

Avec tous les fichiers et applications «illégitimes» qui circulent librement sur les réseaux louches, l'idée de les croire tous «sains» et sans danger n'est que pur délire.

Pour terminer, les activités d'Hacking Team ciblent essentiellement les appareils de quelques individus en raison de leurs activités politiques, par exemple, les chances que vous soyez visé sont pratiquement nulles. Mais la leçon à retenir ici demeure que les protections qu'impose Apple à ses produits sont justifiées.

Quant à la pratique du débridage, elle vient de perdre des points.

Source : http://fr.canoe.ca/techno/materiel/mobiles/apple/archives/2015/08/20150806-120618.html

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

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