Les réseaux SDN ouverts à tous les vents (mauvais)

Les réseaux SDN ouverts à tous les vents (mauvais)

Des scientifiques italiens démontrent une vulnérabilité de sécurité propre au fonctionnement intrinsèque des réseaux SDN. Inquiétant alors que les déploiements ont déjà démarré…

Et si l'un des principes de base du fonctionnement des SDN masquait une inquiétante faille de sécurité ? Les contrôleurs des Software Defined Networks, pilotés de manière logicielle, configurent le réseau en attribuant de nouvelles règles de traitement des flux aux switches. Et c'est ce fonctionnement même qui poserait problème.

C'est du moins le résultat des travaux de trois chercheurs italiens, Mauro Conti (de l'université de Padoue), Fabio De Gaspari et Luigi V. Mancini (tous deux de l'université de Sapienza). *« Nous pensons que des aspects importants de la sécurité des SDN restent encore inexplorés »*, notent-ils dans leur rapport. Pour en convaincre la communauté, ils ont mis au point une nouvelle forme d'attaque, baptisée Know Your Enemy (KYE), au moyen de laquelle un attaquant peut recueillir des informations vitales sur la configuration du réseau.

Moisson d'informations de configuration

A travers leurs travaux, ils entendent démontrer comment un attaquant peut recueillir des informations sur la configuration des outils de sécurité du réseau (dont les seuils de détection d'attaque par scan), sa politique de qualité de service ou encore sa virtualisation. Et d'ajouter qu'une seule table de routage d'un commutateur peut fournir ces informations tout en servant de canal d'attaque. Cerise sur le gâteau : *« nous montrons qu'un attaquant peut effectuer une attaque KYE dans un mode furtif, à savoir sans risquer d'être détecté »*, expliquent-*ils*.

Selon les universitaires, un attaquant pourrait se connecter aux ports d'écoute passive qu'intègrent la plupart des commutateurs pour le débogage à distance afin de récupérer le plan de routage (notamment avec la commande 'dpctl' sur les HP Procurve qu'ils ont utilisés au cours de leurs travaux), en déduire des informations sur la table de routage, espionner le contrôle du trafic en cas d'absence de protection de ce dernier (par chiffrement TLS ou usage de certificats d'authentification), exploiter les vulnérabilités connues dans les systèmes d'exploitation des switches pour introduire une backdoor, ou encore extraire la table de routage ou le contenu de la mémoire du commutateur pour la copier vers un support externe au réseau.

Obscurcir pour limiter les risques

Autant d'informations qui permettent une attaque ou un espionnage plus massif ou plus ciblé du SI dans l'absolu. Les conclusions des chercheurs italiens sont d'autant plus inquiétantes que, en apportant une flexibilité optimale de gestion des réseaux, les technologies SDN sont de plus en plus adoptées par les opérateurs et grandes entreprises. Le rapport insiste bien sur le fait que ces possibilités d'espionnage ne sont pas liées aux systèmes matériels présents sur le réseau, mais bien à son fonctionnement intrinsèque.

Pour limiter les risques d'attaque, les scientifiques détaillent une contremesure basée sur un « *obscurcissement* » des flux entrants. *« S'il était possible d'empêcher l'attachant de comprendre quel flux est responsable de l'application des règles de routage, l'attaque KYE serait irréalisable »*, indiquent-ils. Ce qu'ils ont réussi à faire en exploitant la possibilité de modification du transit des flux dont dispose un switch OpenFlow. Et les chercheurs de rappeler que les risques décrit dans leur travail ne touchent que les réseaux SDN, les structures « traditionnelles » étant par défaut épargnées. Ce qui ne les empêche pas d'avoir leurs propres soucis de sécurité.

Article original de Christophe Lagane

Réagissez à cet article

Original de l'article mis en page : Sécurité : les réseaux SDN ouverts à tous les vents (mauvais) | Silicon

Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence ?

Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence ?

Alors que le tribunal en première instance avait jugé que les éléments n'étaient pas réunis pour justifier une telle procédure extra-judiciaire, le Conseil d'État a autorisé la police à exploiter des données informatiques saisies à Roubaix chez un suspect ayant fait l'objet d'une perquisition administrative.

À la suite de l'attentat de Nice, le gouvernement a réintégré en juillet dernier dans le dispositif de l'état d'urgence la possibilité pour la police de procéder à la saisie de matériels ou données informatiques présentes ou accessibles sur les lieux d'une perquisition administrative. Mais conformément aux préconisations du Conseil constitutionnel, il l'a fait en assortissant cette entorse à la vie privée et au droit de propriété d'un certain nombre de garanties minimales.
En particulier, il est désormais précisé que de tels matériels et données ne peuvent être saisis que « *si la perquisition révèle l'existence d'éléments, notamment informatiques, relatifs à la menace* » que représenterait la personne visée. Par ailleurs, les policiers ne peuvent rien faire des données saisies sans l'autorisation d'un juge des référés d'un tribunal administratif, qui a 48 heures pour donner son aval.

Or Nextinpact rapporte que le ministère de l'intérieur a dû faire appel d'une décision défavorable du tribunal administratif de Roubaix, pour avoir le droit d'exploiter les données saisies chez un suspect. Sur place, la perquisition et la fouille des données informatiques accessibles n'avait apporté strictement aucun élément matériel permettant d'étayer une éventuelle infraction pénale du justiciable. Le juge de première instance en avait donc déduit qu'il ne pouvait pas autoriser l'exploitation des données injustement saisies.
Ce faisant, le juge restait dans l'esprit de l'avis du Conseil constitutionnel, qui s'opposait aux saisies et exploitations de données « *alors même qu'aucune infraction n'est constatée* ».
L'INTÉRESSÉ A INDIQUÉ COMMUNIQUER AVEC EUX AU MOYEN DE SON TÉLÉPHONE PORTABLE, EN USANT NOTAMMENT DE MESSAGERIES INSTANTANÉES OU CRYPTÉES

Mais le Conseil d'État, lui, en reste à une lecture plus littérale de ce que le gouvernement a écrit dans la nouvelle loi, qui n'a pas été soumise au Conseil constitutionnel. Celle-ci ne demande pas qu'une infraction soit constatée, mais uniquement que la perquisition « révèle l'existence d'éléments », matériels ou non, relatifs à la menace. C'est beaucoup plus vague.

Or la haute juridiction administrative note dans son ordonnance (.pdf) que « l'intéressé a déclaré au cours de la perquisition être resté en contact avec quatre amis de Roubaix, qu'il a nommément désignés, partis en Syrie et en Irak pour y mener le djihad », et qu'il « a indiqué communiquer avec eux au moyen de son téléphone portable, en usant notamment de messageries instantanées ou cryptées ». Ces déclarations sont donc en elles-mêmes des éléments relatifs à la menace que pourrait représenter l'individu, qui justifient d'autoriser l'exploitation des données saisies.

UNE OBLIGATION DE RESTITUTION SOUS 15 JOURS

Cette affaire fera certainement redire aux avocats qu'il est toujours primordial de garder le silence, mais il faut noter que le suspect semble pleinement coopératif, et qu'il a accepté que ses données soient inspectées. Il a peut-être préféré que son innocence soit ainsi vérifiée, plutôt que sa présomption d'innocence reste, dans l'esprit des services de renseignement, une présomption de culpabilité.
Selon le PV de perquisition, la police avait procédé à la saisie d' « un ordinateur de marque ACER et de son chargeur, d'un téléphone portable de marque Apple et de son chargeur, d'une clef USB rouge de marque Emtec d'une capacité de 16 Gb, d'une clé USB noire de marque Verbatim d'une capacité de 16 Gb, d'une carte SD de marque Viking d'une capacité de 512 Mb et d'une carte SD de marque Sandisk d'une capacité de 8 Gb ».
Selon les termes de la loi, l'ensemble de ces matériels doivent être retournés à leur propriétaire dans les 15 jours suivant l'autorisation (délivrée ici par ordonnance du 23 août), sans prorogation motivée ou découverte d'éléments probants. Les données non pertinentes devront être détruites sous un délai de 3 mois.
Article original de Guillaume Champeau

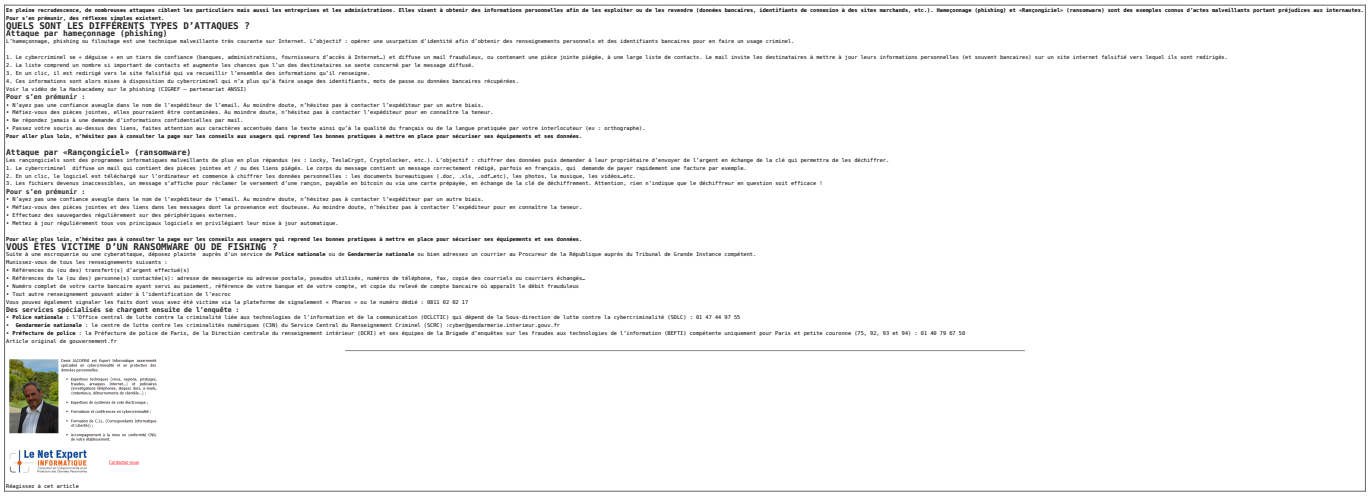
Réagissez à cet article

Original de l’article mis en page : Pourquoi le Conseil d’État autorise une exploitation de données saisies via l’état d’urgence – Politique – Numerama

---

Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?

Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?



En pleine recrudescence, de nombreuses attaques ciblent les particuliers mais aussi les entreprises et les administrations. Elles visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants de connexion à des sites marchands, etc.). Hameçonnage (phishing) et «Rançongiciel» (ransomware) sont des exemples connus d'actes malveillants portant préjudices aux internautes.
Pour s'en prémunir, des réflexes simples existent.
QUELS SONT LES DIFFERENTS TYPES D'ATTAQUES ?
Attaque par hameçonnage (phishing)
L'hameçonnage, phishing ou filoutage est une technique malveillante très courante sur Internet. L'objectif : opérer une usurpation d'identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel.

1. Le cybercriminel se « déguise » en un tiers de confiance (banques, administrations, fournisseurs d'accès à Internet…) et diffuse un mail frauduleux, ou contenant une pièce jointe piégée, à une large liste de contacts. Le mail invite les destinataires à mettre à jour leurs informations personnelles (et souvent bancaires) sur un site internet falsifié vers lequel ils sont redirigés.
2. La liste comprend un nombre si important de contacts et augmente les chances que l'un des destinataires se sente concerné par le message diffusé.
3. En un clic, il est redirigé vers le site falsifié qui va recueillir l'ensemble des informations qu'il renseigne.
4. Ces informations sont alors mises à disposition du cybercriminel qui n'a plus qu'à faire usage des identifiants, mots de passe ou données bancaires récupérées.
Voir la vidéo de la Mackacademy sur le phishing (CIGREF – partenariat ANSSI)
Pour s'en prémunir :
• N'ayez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
• Méfiez-vous des pièces jointes, elles pourraient être contaminées. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
• Ne répondez jamais à une demande d'informations confidentielles par mail.
• Passez votre souris au-dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français ou de la langue pratiquée par votre interlocuteur (ex : orthographe).
Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.

Attaque par «Rançongiciel» (ransomware)
Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus (ex : Locky, TeslaCrypt, Cryptolocker, etc.). L'objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.
1. Le cybercriminel diffuse un mail qui contient des pièces jointes et / ou des liens piégés. Le corps du message contient un message correctement rédigé, parfois en français, qui demande de payer rapidement une facture par exemple.
2. En un clic, le logiciel est téléchargé sur l'ordinateur et commence à chiffrer les données personnelles : les documents bureautiques (.doc, .xls, .odf…etc), les photos, la musique, les vidéos…etc.
3. Les fichiers devenus inaccessibles, un message s'affiche pour réclamer le versement d'une rançon, payable en bitcoin ou via une carte prépayée, en échange de la clé de déchiffrement. Attention, rien n'indique que le déchiffreur en question soit efficace !
Pour s'en prémunir :
• N'ayez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
• Méfiez-vous des pièces jointes et des liens dans les messages dont la provenance est douteuse. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
• Effectuez des sauvegardes régulièrement sur des périphériques externes.
• Mettez à jour régulièrement tous vos principaux logiciels en privilégiant leur mise à jour automatique.

Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.
VOUS ÊTES VICTIME D'UN RANSOMWARE OU DE FISHING ?
Suite à une escroquerie ou une cyberattaque, déposez plainte auprès d'un service de Police nationale ou de Gendarmerie nationale ou bien adressez un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.
Munissez-vous de tous les renseignements suivants :
• Références du (ou des) transfert(s) d'argent effectué(s)
• Références de la (ou des) personne(s) contactée(s): adresse de messagerie ou adresse postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels ou courriers échangés…
• Numéro complet de votre carte bancaire ayant servi au paiement, référence de votre banque et de votre compte, et copie du relevé de compte bancaire où apparaît le débit frauduleux
• Tout autre renseignement pouvant aider à l'identification de l'escroc
Vous pouvez également signaler les faits dont vous avez été victime via la plateforme de signalement « Pharos » ou le numéro dédié : 0811 02 02 17
Des services spécialisés se chargent ensuite de l'enquête :
• Police nationale : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui dépend de la Sous-direction de lutte contre la cybercriminalité (SDLC) : 01 47 44 97 55
• Gendarmerie nationale : le centre de lutte contre les criminalités numériques (C3N) du Service Central du Renseignement Criminel (SCRC) :cyber@gendarmerie.interieur.gouv.fr
• Préfecture de police : la Préfecture de police de Paris, de la Direction centrale du renseignement intérieur (DCRI) et ses équipes de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) compétente uniquement pour Paris et petite couronne (75, 92, 93 et 94) : 01 40 79 67 50
Article original de gouvernement.fr

Denis JACOPINI est Expert informatique assermenté spécialisé en cybercriminalité et protection des données personnelles.
• Expertises techniques (virus, spyware, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…);
• Expertises de systèmes de vote électronique ;
• Formations et conférences en cybercriminalité ;
• Formation de C.I.L. (Correspondants Informatique et Libertés) ;
• Accompagnement à la mise en conformité CNIL de votre établissement.
Le Net Expert INFORMATIQUE
Contactez nous
Réagissez à cet article

Original de l'article mis en page : Cybercriminalité | Gouvernement.fr

---

Alerte : Twitter pour Android infecté par un Cheval de Troie

Alerte : Twitter pour Android infecté par un Cheval de Troie

ESET découvre le premier botnet sous Android qui contrôle Twitter

Les chercheurs ESET ont découvert une porte dérobée sous Android qui contient un Cheval de Troie et qui est contrôlée par des tweets. Détecté par ESET comme étant Android/Twitoor, **il s'agit de la première application malveillante utilisant Twitter** au lieu d'une commande et d'un contrôle traditionnel de serveur (C&C).
Après son lancement, le Cheval de Troie cache sa présence sur le système et vérifie le compte Twitter défini par intervalle régulier pour les commandes. Sur la base des commandes reçues, il peut soit télécharger des applications malveillantes, soit basculer le serveur C&C d'un compte Twitter à un autre.
« L'utilisation de Twitter pour contrôler un botnet est une étape innovante pour une plateforme Android », explique Lukáš Štefanko, malware researcher chez ESET et qui a découvert cette application malicieuse.
Selon Lukáš Štefanko, les canaux de communication basés sur des réseaux sociaux sont difficiles à découvrir et impossible à bloquer entièrement – alors qu'il est extrêmement facile pour les escrocs de rediriger les communications vers un autre compte de façon simultanée.

Twitter a d'abord été utilisé pour contrôler les botnets de Windows en 2009. « En ce qui concerne l'espace Android, ce moyen de dissimulation est resté inexploité jusqu'à présent. Cependant, nous pouvons nous attendre à l'avenir à ce que les cybercriminels essayent de faire usage des statuts de Facebook ou de déployer leurs attaques sur LinkedIn et autres réseaux sociaux » , prévoit Lukáš Štefanko.
Android/Twitoor est actif depuis juillet 2016.Il ne peut pas être trouvé sur l'un des app store officiels d'Android (selon Lukáš Štefanko) mais il est probable qu'il se propage par SMS ou via des URL malveillantes. Il prend l'apparence d'une application mobile pour adulte ou d'une application MMS mais sans fonctionnalité. Plusieurs versions de services bancaires mobiles infectés par un malware ont été téléchargées. Cependant, les opérateurs de botnet peuvent commencer à distribuer d'autres logiciels malveillants à tout moment, y compris des ransomwares selon Lukáš Štefanko.

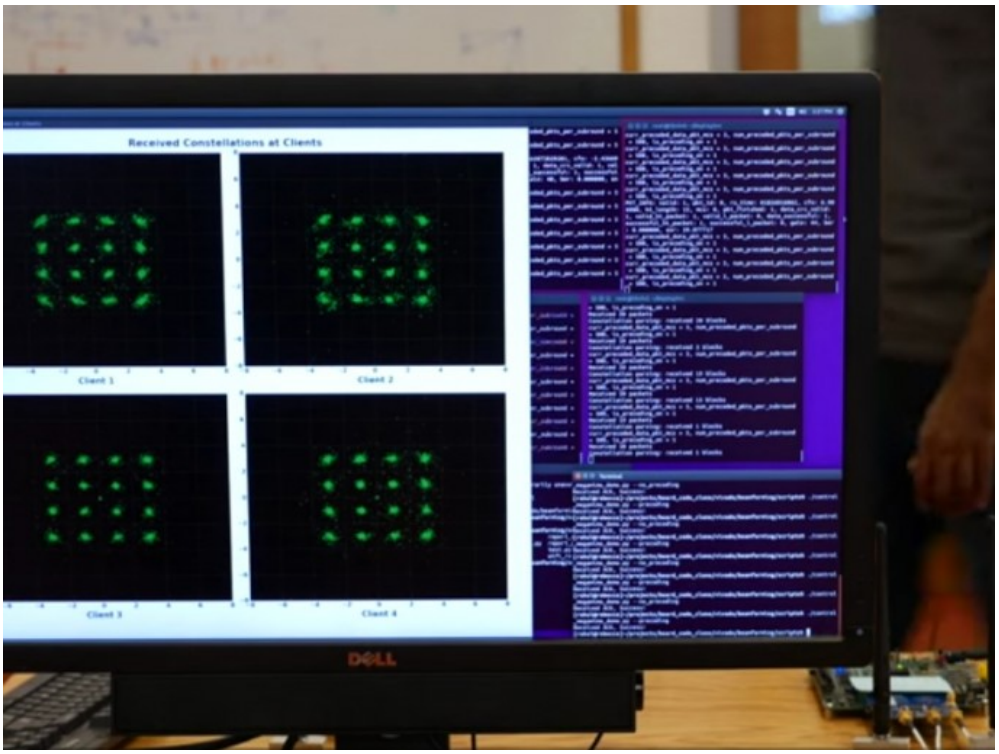
Twitoor est le parfait exemple de l'innovation des cybercriminels pour leur business. Les utilisateurs d'Internet devraient continuer à protéger leurs activités avec de bonnes solutions de sécurité valables pour les ordinateurs et les appareils mobiles », conclut Lukáš Štefanko.
Source : ESET

Pour protéger vos équipements, nous recommandons l'application suivante :

Réagissez à cet article

La vitesse de votre Wi-Fi

sera bientôt multipliée par 3



La vitesse de votre Wi-Fi sera bientôt multipliée par 3

Des chercheurs du MIT ont mis au point un système qui coordonne différents points d'accès Wifi environnants pour palier la congestion du trafic.

Des chercheurs du CSAIL (Computer Science and Artificial Intelligence Lab au Massachussetts Institute of Technology) ont développé une technique qui améliore grandement les performances du Wifi et des communications sans fil plus généralement.

Ezzeldin Hamed, Hariharan Rahul, Mohammed Abdelghany et Dina Katabi présentent leurs travaux dans le cadre du ACM SIGCOMM 16 (Association for Computing Machinery's Special Interest Group on Data Communications), qui se tient au Brésil (à Florianópolis) jusqu'au 26 août. Ils entendent palier les risques de congestion qui peuvent survenir dans un réseau sans fil traditionnel quand deux points d'accès rapprochés émettant à la même fréquence risquent de causer des interférences.

Aujourd'hui, la solution pour éviter ces interférences consiste à traiter les requêtes les unes après les autres, ce qui restreint inévitablement l'envoi des données (même si, à haute fréquence de traitement, cela ne se perçoit pas tant que le point d'accès n'est pas saturé de connexions). Un peu comme si les supermarchés n'étaient équipés que d'une seule caisse obligeant les consommateurs à d'interminables queues pour payer leurs achats (même si la caissière est super rapide…). Les scientifiques du MIT ont donc envisagé une autre approche visant à coordonner de multiples points d'accès sans fil à la même fréquence sans créer d'interférences.

Utiliser efficacement le spectre disponible

« Dans le monde sans fil d'aujourd'hui, vous ne pouvez pas résoudre le problème de la contraction du spectre en multipliant les émetteurs, car ils continueront d'interférer les uns avec les autres, explique Ezzeldin Hamed, selon des propos repris par le site de news du MIT. *La réponse tient dans une coordination de tous les points d'accès afin d'utiliser efficacement le spectre disponible. »* Et cette réponse se traduit par la mise au point du **dispositif MegaMIMO 2.0**, un boîtier de la taille d'un routeur traditionnel qui embarque processeur, système de traitement radio temps réel, émetteur-récepteur et, surtout, algorithmes maison.

Ces derniers génèrent un signal qui permet à de multiples émetteurs indépendants de transmettre des données sur la même ressource hertzienne à plusieurs points d'accès indépendants sans interférer les uns avec les autres grâce à une synchronisation de leur phase d'ondes. Autrement dit, une sorte de réseau MIMO distribué que nombre d'ingénieurs tenaient jusqu'à présent pour difficile à mettre au point. Mais l'équipe du CSAIL a fait une démonstration de l'efficacité du MegaMIMO 2.0, via une simulation de quatre ordinateurs portables en mouvement dans une salle de réunion. Il en ressort une augmentation des débits de 330 % par rapport à un système Wifi traditionnel (et même par rapport à leurs premiers travaux, MegaMIMO, présentés en 2012 et dans lesquels l'utilisateur devait fournir manuellement les informations sur les différentes fréquences). Sans oublier un doublement de la portée du signal. MegaMIMO permet même d'adapter le signal en fonction des obstacles environnants (par exemple lorsque quelqu'un se positionne entre l'émetteur et le récepteur).

Applicable aux réseaux mobiles

Les chercheurs entendent poursuivre leurs travaux pour parvenir à coordonner des dizaines de routeurs sans fil afin de gérer toutes ces ressources comme une seule, ce qui devrait encore démultiplier les performances. Mais le système vise avant tout à palier les risques de congestion du réseau alors que ses usages progressent beaucoup plus vite que la disponibilité des ressources hertziennes.

Dans l'absolu, le MegaMIMO pourrait en effet parfaitement s'appliquer aux réseaux cellulaires. Et permettrait d'assurer des services mobiles de qualité dans les endroits particulièrement fréquentés, comme les stades lors des événements sportifs, les gares les jours de grève ou lors d'incidents de circulation des transports, etc. En attendant, les campus et grandes entreprises pourraient être les premiers à adopter le MegaMIMO pour fournir des accès Wifi efficaces… si le système est commercialisé un jour.

Original de l'article mis en page : MegaMIMO 2.0, le système qui multiplie par 3 les performances du Wi-Fi

Un vendeur d’armes du Black Market jugé

Un vendeur d’armes du Black Market jugé

Le vendeur d'armes Gun Runner arrêté et jugé. Il revendait dans le black market pistolets et armes de guerre.

Je vous ai souvent parlé de ce vendeur d'armes du black market baptisé GunRunner. Ce commerçant du dark web commercialisait Glocks, Uzi et pistolet Walthers, celui de James Bond, comme un boulanger vend des petits pains. Arrêté et jugé en juin dernier, Michael Andrew Ryan, a été traqué par l'ATF, l'agence en charge du contrôle des armes et explosifs sur le sol de l'Oncle Sam.

Gun Runner a oublié que l'ATF possédait un service de renseignement plutôt costaud et des bases de données qui feraient pâlir les amateurs de Big Data. Bilan, même si Michael Andrew Ryan limait les numéros de série, l'ATF a pu remonter au vendeur et à l'historique de ses produits vendues dans le black market. Il vendait son arsenal via son domicile du Kansas. Il revendait ses armes dans plusieurs boutiques, dont le shop Reloaded. Il a plaidé coupable. Il risque tout de même une peine maximale de 10 ans de prison et jusqu'à 250 000 $ d'amende.

Ryan connaitra son sort le 12 Septembre. Je doute qu'il passe Noël chez lui avec les matériels et les munitions qu'il a pu vendre : Beretta 9 mm, Taurus .38, Uzi, …

En novembre 2015, je vous parlais d'un autre vendeur de 48 ans qui a proposé 32 armes dans le dark web à des Suédois et Australiens. Selon une étude réalisée par un professeur de l'Université Carnegie Mellon, la vente illégale d'armes à feu représenterait moins de 3% des négociations dans les boutiques du Dark Web. Il faut dire aussi qu'avec les centaines de boutiques fourguant des milliers de drogues, le chiffre ne veut pas dire grand-chose.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : ZATAZ Black market : un vendeur d'armes jugé – ZATAZ

Pokémon Go, le nouveau jeu favori des spammeurs

Pokémon Go, le nouveau jeu favori des spammeurs

La distribution de malwares à travers Pokémon Go est aujourd'hui supplantée par des campagnes de spam par SMS.
Pokémon Go, le jeu star de l'été qui fait exploser les revenus de son concepteur Niantic et des stores d'applications (il aurait généré plus de 200 millions de dollars en un mois avec 100 millions de téléchargements), est une aubaine pour les pirates. Lesquels n'hésitent pas à profiter de la popularité du jeu de réalité augmentée pour multiplier les tentatives d'arnaques.

Captures du SMS et du site vers lequel renvoie le lien.

AdaptiveMobile, société spécialisée dans la sécurité mobile, relève aujourd'hui une campagne de spam par SMS invitant les destinataires à se rendre sur un faux site baptisé Pokemonpromo.xxx. La campagne semble se concentrer pour l'heure sur les joueurs d'Amérique du Nord. *« Il s'agit d'un site de phishing sophistiqué qui imite fidèlement le vrai site Pokémon GO. Il prétend fournir à l'utilisateur des fonctionnalités supplémentaires au jeu s'il référence 10 de ses amis (susceptibles d'être à leur tour spammés) »*, indique AdaptiveMobile dans un billet de blog daté du 17 août. Le site, signalé pour ses activités de phishing, n'est plus actif aujourd'hui.

Multiplication des campagnes de spam

Mais ce n'est pas le seul dans le genre. Une autre campagne de phishing par SMS propose par exemple 14 500 Pokecoins (la monnaie virtuelle du jeu utilisée pour des achats internes) pour 100 points collectés et pointe vers d'autres sites de spam (dédiés ou non au jeu de Niantic) depuis une URL raccourcie. Citons par exemple Pokemon.vifppoints.xxxx ou Pokemon Generator… Autant de sites qui cherchent à leurrer l'utilisateur en l'invitant à fournir ses identifiants de connexion. Des sites promus par SMS comme depuis les réseaux sociaux et autres forums dédiés à Pokémon Go, précise le fournisseur de solutions de protection pour mobiles.
Autant de campagnes malveillantes qui ne se tariront pas avant que la popularité du jeu ne commence à décliner, estime AdaptiveMobile. D'ici là, les utilisateurs sont invités à redoubler de prudence, surtout s'ils reçoivent un message (SMS ou autre) accompagné d'un lien vers un site web. *« Méfiez-vous des messages SMS non sollicités que vous recevez et qui mentionnent l'application »*, rappelle l'entreprise dans son billet.
Les campagnes de spam ne sont pas les seuls dangers qui guettent les joueurs de Pokémon Go. Mi juillet, les cybercriminels profitaient de l'absence du jeu dans les stores de certains marchés, dont la France, pour distribuer le fichier .APK de la version Android de l'application. Fichier évidemment compromis par le malware DroidJack (ou SandroRAT) qui ouvrait grandes les portes du système infecté aux attaquants. Plus récemment, début août, l'Anssi (Agence nationale de la sécurité des systèmes d'information) y allait de son grain de sel en alertant sur les risques liés à Pokémon Go. De quoi nous gâcher l'envie de jouer…
Article original de Christophe Lagane

Réagissez à cet article

Original de l'article mis en page : Pokémon Go, le nouveau jeu favori des spammeurs

Comment être payé pour lancer des attaques informatiques de type DDoS

Comment être payé pour lancer des attaques informatiques de type DDoS

Déjà que lancer des DDoS était accessible au premier idiot du village, voilà que maintenant, il pourrait être possible de les payer pour leurs attaques.

Le DDoS, une plaie du web qui a pour mission de bloquer un serveur à coups de connexions de masse. Un Déni Distribué de Service, c'est un peu comme déverser des poubelles devant l'entrée d'une maison, plus personne ne peut rentrer, plus personne ne peut en sortir. Deux chercheurs américains viennent de rajouter une couche dans ce petit monde fou-fou des DDoSeurs : payer les lanceurs d'attaques.

Eric Wustrow de l'Université du Colorado et Benjamin VanderSloot de l'Université du Michigan se sont lancés dans la création d'une crypto-monnaie, comme le bitcoin, qui pourrait rémunérer les lanceurs de DDoS. Ils ont baptisé leur « idée » : DDoSCoin. Sa mission, récompenser les participants à des dénis de service distribués (DDoS). Cette « monnaie » ne fonctionne que lorsque l'ordinateur de la cible a le TLS activé (Security Layer Transport), un protocole de chiffrement pour les communications Internet sécurisée.

Créer une monnaie qui permet aux « mineurs » de prouver leur participation à un DDoS vers un serveur web ciblé peut paraitre bizarre. Les deux étudiants cherchent des méthodes pour contrer et remonter ce type d'attaque.

Article original de Damien Bancal

Vous comprendrez que le titre de cet article n'a pas pour but de vous inciter à utiliser cette technique, mais plutôt de vous faire découvrir qu'elle existe pour l'anticiper.

Denis Jacopini

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

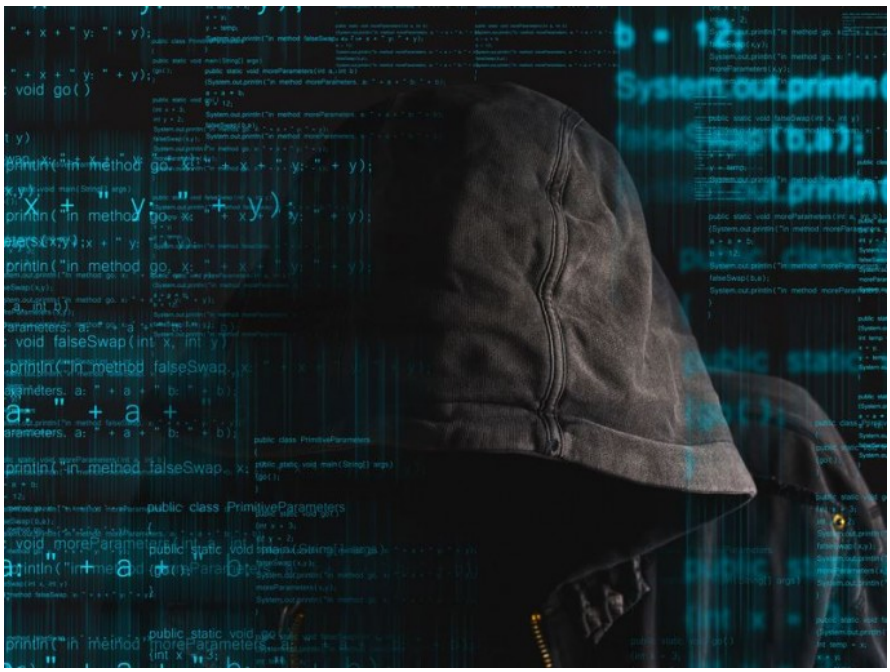
Réagissez à cet article

Original de l'article mis en page : Être payé pour lancer des DDoS – Data Security BreachData Security Breach

---

Shadow Brokers, une affaire

de Cyberespionnage



Shadow Brokers, une affaire de Cyberespionnage

Tour d'horizon des conséquences d'une affaire de cyber-espionnage au retentissement international alors que les fichiers mis en ligne par les mystérieux Shadow Brokers, et probablement dérobés à la NSA, commencent à livrer leurs secrets.

1) Pourquoi un tel intérêt pour les Shadow Brokers ?

Lundi 15 août, un groupe de hackers appelé Shadow Brokers a annoncé avoir piraté des systèmes informatiques utilisés par Equation, une organisation réputée proche de la NSA. A l'appui de ses affirmations, ce groupe jusqu'alors inconnu a posté deux archives sur des sites de partage. La première, en libre accès, renferme 300 Mo de données, où se mêlent des outils et des techniques pour infiltrer des systèmes…. [lire la suite]

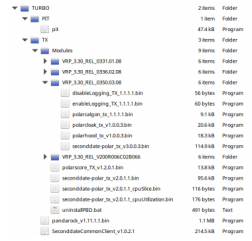
2) Le hacking de la NSA est-il établi ?

Bien entendu, ni la célèbre agence américaine ni le groupe de hackers Equation, réputé proche de celle-ci, n'a confirmé que les outils mis en ligne par les Shadow Brokers provenaient bien de leurs serveurs. Mais plusieurs éléments concordants établissent un lien direct entre les fichiers mis en ligne par les Shadow Brokers et le couple NSA/Equation. D'abord, c'est l'éditeur russe Kaspersky qui remarque que plus de 300 fichiers présents dans la première archive utilisent une implémentation des algorithmes de chiffrement RC5 et RC6 identique à celle utilisée par le groupe Equation. « *La probabilité que tout ceci (l'archive mise en ligne, NDLR) soit un faux ou ait été conçu par rétro-ingénierie est extrêmement faible* », écrivent les chercheurs de Kaspersky dans un billet de blog. [lire la suite]

3) Que dit cette affaire du groupe Equation ?

Le nom de ce groupe, choisi en raison de sa prédilection pour les techniques de chiffrement de haut vol, a été donné début 2015 par Kaspersky à un groupe de hackers, que l'éditeur russe décrivait alors comme le plus techniquement doué qu'il ait jamais identifié. La société parlait alors « *d'une menace qui dépasse tout ce qui est connu en termes de complexité et de sophistication des techniques employées, une menace active depuis au moins deux décennies* ». Equation exploitait depuis 2008 des failles zero day qui ne seront mises à jour que plus tard, à l'occasion du piratage du nucléaire iranien par Stuxnet. [lire la suite]

4) Que renferme l'archive des Shadow Brokers ?



Plusieurs chercheurs en sécurité se sont déjà penchés sur le cyber-arsenal mis à disposition par les Shadow Brokers (lire notamment l'analyse de Mustafa Al-Bassam ou la synthèse réalisée par *Softpedia*). On y trouve des *exploits*, autrement dit des codes d'exploitation permettant de prendre le contrôle ou d'espionner des pare-feu ou passerelles VPN fournis par de grands constructeurs comme Cisco, Juniper ou Fortinet. Des constructeurs qui ont déjà reconnu que les outils mis en ligne menaçaient bien certains de leurs matériels. Mais, dans tous les cas, il s'agit de générations anciennes de machines. Les appliances Cisco Pix, ciblées par plusieurs outils, ne sont par exemple plus supportées par le constructeur depuis 2009. [lire la suite]

5) L'archive a-t-elle livrée tous ses secrets ?

Et il y a aussi les outils dont la vocation ne se limite pas à cibler une gamme de machines en particulier. *The Intercept* explique ainsi que des éléments d'une architecture exploitée par la NSA pour mettre en place des attaques de type Man-in-the-Middle, autorisant l'interception de requêtes Web, figurent dans l'archive des Shadow Brokers.Sans risque de se tromper, la réponse est non. « *Comme il y a 300 Mo de code, de documentations, de binaires, personne n'a publié d'analyse complète* », remarquent Hervé Schauer et Christophe Renard.[lire la suite]

6) Quels sont les risques pour les entreprises ?

Voir de tels outils mis à la disposition de cybercriminels est évidemment inquiétant. « *On est ici face à des outils d'attaque de haut niveau, mis librement à disposition sur le Web*, explique Gérôme Billois. *Les entreprises doivent donc être très attentives, effectuer l'inventaire des matériels exposés sur leur parc et apporter les modifications nécessaires pour protéger leurs infrastructures. Heureusement, les exploits mis au jour sont assez anciens et ciblent donc du matériel âgé. Mais certaines machines peuvent toujours être en exploitation.* » Au fur et à mesure que les codes de l'archive des Shadow Brokers seront décortiqués, des correctifs et des indicateurs de compromission vont être publiés. Ce qui permettra aux RSSI de contrer la menace. C'est donc plutôt une course de fond qui s'engage. [lire la suite]

7) Qui a fait le coup ?

La liste des suspects s'est très vite limitée à quelques noms. Très rapidement, Nicolas Weaver, de l'université de Berkeley, pointe la Chine, soupçonnée de nombreux actes de cyber-espionnage contre les intérêts américains, et la Russie. Une seconde hypothèse que défend lui aussi Edward Snowden, précisément réfugié en Russie après avoir été à l'origine de la plus importante fuite de données de l'histoire de la NSA. [lire la suite]

8) Un second lanceur d'alertes à la NSA ?

Car une autre hypothèse a également de nombreux partisans : celle de l'implication d'un 'insider', un nouveau lanceur d'alerte à la NSA. Plusieurs éléments viennent étayer cette hypothèse. Primo, l'archive en question renferme différentes versions d'un même outil, des manuels d'utilisation ou des fichiers à vocation interne. Ce qui cadre mal avec l'hypothèse d'un serveur d'attaque, ou d'un serveur de pré-production, qui aurait été compromis par un assaillant externe. [lire la suite]

9) Quelles sont les conséquences possibles ?

D'ores et déjà, la fuite a dû déclencher un branle-bas de combat au sein de la NSA, qui doit chercher l'origine de cette encombrante archive et, surtout, comment mettre fin aux révélations successives sur ses activités offensives. L'agence devra également s'assurer qu'elle n'exploite plus les codes révélés au public pour ses opérations actuelles. Car, très rapidement, les outils de sécurité seront en mesure de détecter les signatures des outils révélés par les Shadow Brokers.[lire la suite]

10) Qu'en pense Bernard Cazeneuve ?

Passée la boutade, le ministre de l'Intérieur français, qui entend prendre la tête d'une initiative internationale permettant d'encadrer le chiffrement, a devant les yeux une autre illustration des limites que pointent de nombreux spécialistes, y compris le Conseil national du numérique (CNNum).Après l'affaire Juniper (le constructeur avait employé un algorithme de chiffrement affaibli par la NSA, qui avait été détourné par un acteur inconnu), les révélations des Shadow Brokers illustrent une fois encore le caractère spécifique des armes cyber.[lire la suite]

Article original de Reynald Fléchaux

Réagissez à cet article

Original de l’article mis en page : Cyberespionnage : 10 questions pour comprendre l’affaire Shadow Brokers

---

Votre vie privée numérique en danger sur Leakedsource

Votre vie privée numérique en danger sur Leakedsource

Depuis quelques semaines, le site leakedsource engrange des centaines de millions de données volées par des pirates informatiques. Un business juteux qui met en danger des millions d'internautes.

LeakedSource, nouvelle source d'informations pour pirates informatiques ? Souvenez-vous, on vous parlait en juillet, de données volées appartenant à un ancien garde du corps de Vladimir Poutine, le Président Russe, ou encore de Nicolas Sarkozy, ancien Président de la République Française. Son identité, ses données privées, des courriels… Un piratage qui semblait être particulièrement compliqué à orchestrer tant les sources d'informations concernant ce body guard étaient variés. Après enquête, j'ai découvert que si le résultat pouvait être particulièrement préjudiciable pour la cible, la mise en place et l'exécution de cette attaque était aussi simple que « *1 + 1 font 2*« .

Leakedsource, source quasi inépuisable de malveillances

Pour ce garde du corps, mais aussi pour de nombreuses personnalités, le risque est énorme. Tout débute par le piratage de centaines de bases de données de part le monde. Myspace, Adobe, Linkedin, Twitch , Xat , Badoo… ne sont que des exemples parmi d'autres. Je gère, avec le protocole d'alerte ZATAZ, des dizaines de fuites de données par mois concernant des PME et entreprises Françaises. Imaginez donc ce que brassent des sites comme leaked source.

Leakedsource.com, un espace web tenu par des Russes, a pour mission de regrouper les informations volées par des pirates et de permettre de consulter les informations en question. Les administrateurs du portail expliquent que leur service est fait pour s'assurer que les données volées ne vous concernent pas. Sauf que, des données, il y en a des centaines de millions, et vous pourriez bien vous y retrouver, comme Mark Zuckerberg, cofondateur et directeur général de Facebook, piraté en juin 2016 parce que son mot de passe « *DaDaDa* » était accessible dans une base de données piratées et stockées chez Leakedsource.

Vous ne risquez rien ? Vraiment ?

Cela n'arrive qu'aux autres ? Allez donc regarder du côté de vos données. C'est d'ailleurs ce qu'aurait dû faire l'auteur des jeux vidéo Garrysmod et de Rust, Garry Newman. J'ai pu avoir une longue conversation avec l'auteur de divertissements vidéo ludique qui ne s'attendaient pas à découvrir sa vie numérique mise en pâture de la sorte. Il faut dire aussi que plusieurs pirates ont contacté la rédaction de ZATAZ.COM pour se vanter d'avoir mis la main sur ses données Paypal, Amazon, gMail de ce créateur de jeux vidéo britannique. Bref, pour 4 dollars (le prix journalier d'un abonnement Leaked source pour accéder aux données) n'importe quel internaute peut se transformer en vulgaire violeur de vie 2.0. Il suffit de rentrer un mail, un pseudonyme ou encore une adresse IP et Leakedsource cherche dans ses bases de données la moindre concordance. Cerise sur le gâteau, quand le mot de passe est hashé, donc illisible à la première lecture, Leaked source propose la version du précieux sésame déchiffré. « ***Si les personnes [les pirates, NDR) sont malines, elles peuvent faire beaucoup de dégâts avec ce genre d'outil accessible à Monsieur tout le monde*** » me confirme un utilisateur.

Que faire pour éviter ce type de fuite de données ?

Je vais très rapidement être honnête avec vous, si vous mettez vos données en ligne, dites vous qu'elles ne sont plus en sécurité. Et ce n'est pas notre vénérable CNIL qui pourra vous aider. Avec plusieurs centaines de cas de fuite de données que je traite avec le protocole d'alerte de zataz par an, j'ai déjà pu croiser mes propres informations. Je vous parlais plus haut de Leakedsource, j'ai pu y retrouver mon compte Adobe. Pourtant, le géant du logiciel l'avait juré, il était « *secure* » [sécurisé, ndr].

Tellement « *secure* » qu'un de mes mails, et le mot de passe attenant, sont disponible dans ce big data du malveillant. Autant dire que l'adresse mail et le mot de passe en question ont été détruits et ne seront plus utilisés.

Que faire donc ? D'abord, un compte mail par service. Je sais, c'est long est fastidieux. Mais je pense qu'il va être beaucoup plus long et fastidieux pour Garry Newman de revalider l'ensemble de ses comptes « infiltrés », car il utilisait la même adresse électronique pour ses accès Paypal, Amazon…

Ensuite, ne mettez pas le même mot de passe pour l'ensemble de vos services en ligne. On a beau le répéter, cesser de vous croire plus malin que les 010101 qui nous régissent. Mark Zuckerberg et son « *DaDaDa* » lui ont coûté son Twitter et son Pinterest. Pour Garry, plus grave encore, son compte Amazon et Paypal, avec des données sensibles [adresses postales, données bancaires…] qui ne devraient pas être disponibles à la planètes web. Donc, oui, c'est fastidieux, mais un mot de passe par compte est une obligation.

Pour finir, en ce qui concerne l'IP, n'hésitez plus à utiliser un VPN. L'outil permet de cacher votre véritable adresse de connexion, en plus de chiffrer vos informations transitant sur la toile. Je vous invite à regarder du côté de nos partenaires et amis de chez **NoLimitVPN** ou encore HMA! pour blinder vos connexions PC, Mac et mobiles.

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Leakedsource, le site qui met en danger votre vie privée – ZATAZ