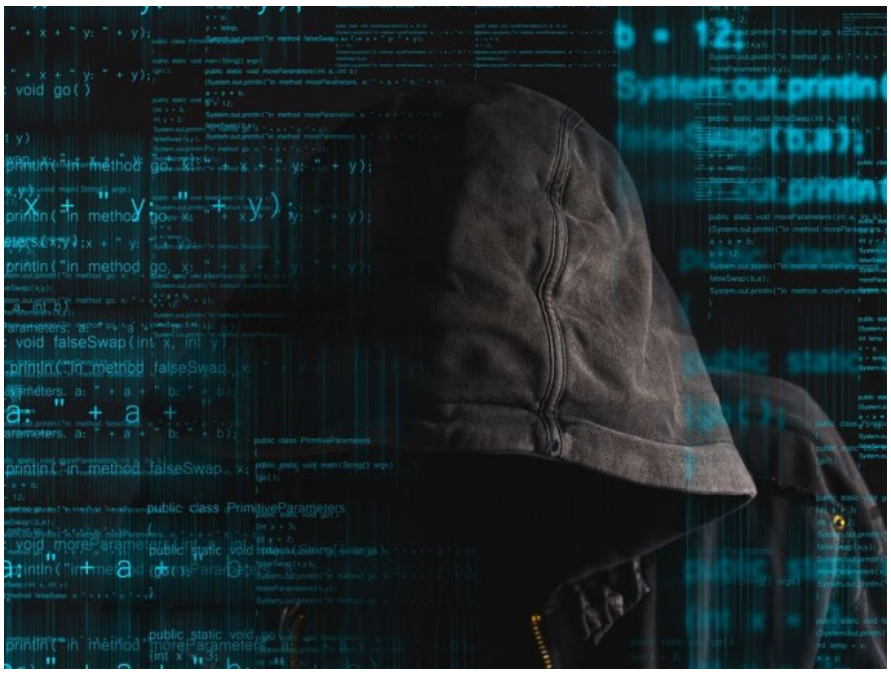
Shadow Brokers, une affaire de Cyberespionnage

	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]

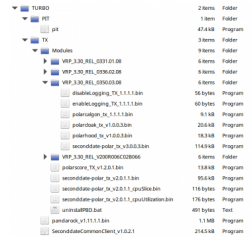
2) Le hacking de la NSA est-il établi ?

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]

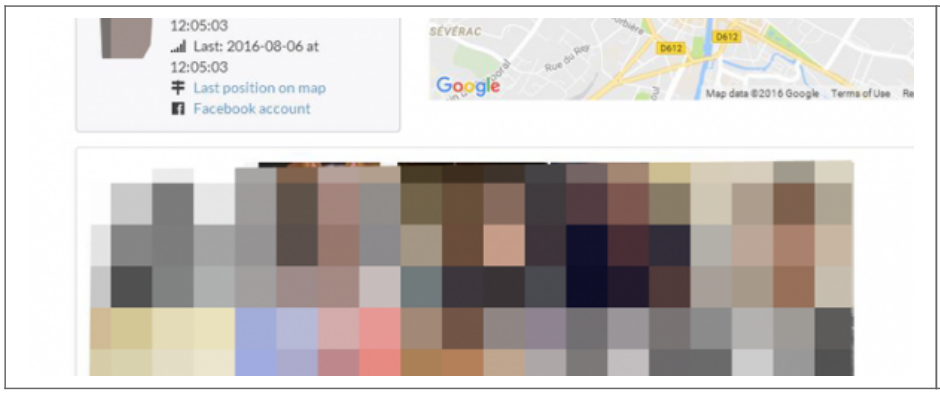
Article original de Reynald Fléchaux

Réagissez à cet article

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

---

Géolocaliser un téléphone mobile en deux clics de souris



Géolocaliser un téléphone mobile en deux clics de souris

Cyber géolocaliser un porteur de téléphone est de plus en plus simple. Un chercheur en informatique montre à ZATAZ.COM comment créer un tracker maison devient simple comme bonjour.

Les téléphones portables, de nos jours, sont de véritables ordinateurs aux capacités de traçage, surveillance et cyber surveillance qui fait froid dans le dos. Regardez, prenons les exemples tels que Facebook et son option « amis à proximité » ou encore PokemonGo et sa capacité de géolocalisation. Du traçage au centimètre. Des technologies de « ciblage » qui deviennent simple à créer et à utiliser. Tristan, informaticien Parisien, vient de contacter ZATAZ pour présenter son cas d'étude : un outil de traçage en temps réel capable de tracer l'itinéraire de ses cibles.

Géolocaliser un téléphone : Souriez, vous êtes pistés

Depuis quelques temps Tristan s'intéresse aux applications proposées dans les mobiles, et plus précisément aux logiciels qui font transiter des informations telles que des positions de latitude et de longitude. Avec un associé, il a lancé Lynx Framework, une entité spécialisée dans la création d'outils de sécurité pour les applications web.
A parti de ses recherches, Tristan a créé un outil de « traque », de quoi géolocaliser un téléphone qui met à jour les dangers de nos mobiles et de leurs capacités à indiquer notre emplacement, mais aussi, nos itinéraires. « ***En analysant les requêtes envoyées par certaines applications je me suis rendu compte qu'il serait possible de récupérer le positionnement de plusieurs personnes en même temps et de les positionner sur une carte de type google map.*** » m'explique le chercheur.

A l'image des sauvegardes de Google Map que je vous indiquais en 2015, l'outil « privé » de Tristan fait pareil, mais en plus discret encore. Via un outil légal et disponible sur Internet, Burp Suite, notre chercheur a analysé les requêtes envoyées par plusieurs logiciels de rencontres disponible dans le Google Play.

Comment cela fonctionne-t-il ?

« *Le tracker prend le contrôle de plusieurs comptes d'application de rencontre et récupère la position des personnes à proximité,* indique-t-il à ZATAZ.COM. *Il ajoute ces informations dans sa base de données et vérifie l'existence des positions pour cette identité. » Si l'application de Tristan retrouve la même personne, mais pas à la même position, il va créer un itinéraire de l'individu via son ancienne position*« . Nous voilà avec la position et le déplacement exacts d'un téléphone, et donc de son propriétaire, à une heure et date données.

Géolocaliser un téléphone : Chérie, tu faisais quoi le 21 juillet, à 12h39, à 1 cm de ta secrétaire ?

Après quelques jours de recherche, Tristan a mis en place une base de données de déplacement dans une ville. Une commune choisie au hasard. Son outil est en place, plusieurs systèmes sont lancés : Une carte avec le positionnement des personnes croisées ; une page plus explicite pour chaque personne avec la date de croisement, son âge… ; une page ou notre chercheur gère ses comptes dans l'application. Bonus de son idée, un système d'itinéraire complet a été créé. Il permet de tracer un « chemin » de déplacement si la personne croisée a déjà été croisée dans le passé, dans un autre lieu. « J'ai positionné un compte au centre de la ville, un autre à l'entrée et le suivant à la sortie, ce qui a données en quelques heures une 50ène de données » confie-t-il « Il est inquiétant de voir autant de données personnelles transitées en clair via ces applications ».

Géolocaliser un téléphone : détournement possible d'un tel « tracker » ?

Vous l'aurez compris, « tracer » son prochain est facilité par ses applications qui ne protègent pas les informations de positionnement des utilisateurs. Il devient possible d'imaginer une plateforme, en local, avec plusieurs comptes positionnés à des endroits différents dans une ville. Bilan, suivre plusieurs individus devient un jeu d'enfant. Si on ajoute à cela les applications de déplacement de type UB, qui communique les données de ses chauffeurs par exemple, ainsi que celles d'autres réseaux sociaux, il devient réellement inquiétant de se dire que positionner une personne et la tracer se fait en quelques secondes. Deux solutions face à ce genre de traçage : jeter votre portable ou, le mieux je pense, forcer les éditeurs d'applications à vérifier la sécurisation des données envoyées, et les chiffrer pour éviter qu'elles finissent en clair et utilisable par tout le monde.
Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Géolocaliser un téléphone mobile en deux clics de souris – ZATAZ

---

15 millions de comptes Telegram d’Iraniens piratés

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Une ancienne faille non corrigée dans Telegram aurait permis de mettre la main sur des millions d'informations d'utilisateurs Iraniens.

Des chercheurs en sécurité informatique ont annoncé à l'agence de presse Reuters que l'application Telegram avait subit une attaque informatique qui a donné l'occasion aux malveillants de mettre la main sur 15 millions de données d'utilisateurs Iraniens.

Pour rappel, Telegram a été fondé en 2013 par le Russe Pavel Durov. Cet outil de messagerie permet de rendre « illisible » des communications entre personnes autorisées (sauf si groupe publique). Pour cela, les communications sont chiffrées. Dans les options de l'application : chiffrer les messages, auto destruction des textes…

Collin Anderson et Claudio Guarnieri, les deux chercheurs travaillent entre autres pour Amnesty International, ont expliqué que la vulnérabilité est exploitable via son utilisation des SMS. Une faille qui avait pourtant été révélée en 2013 par Karsten Nohl. Selon les deux chercheurs, les utilisateurs Iraniens ont été touchés par une infiltration qui a peut-être permis à des « espions » de mettre la main sur les informations de 15 millions d'utilisateurs de ce pays.

[block id="24761" title="Pied de page HAUT"]

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

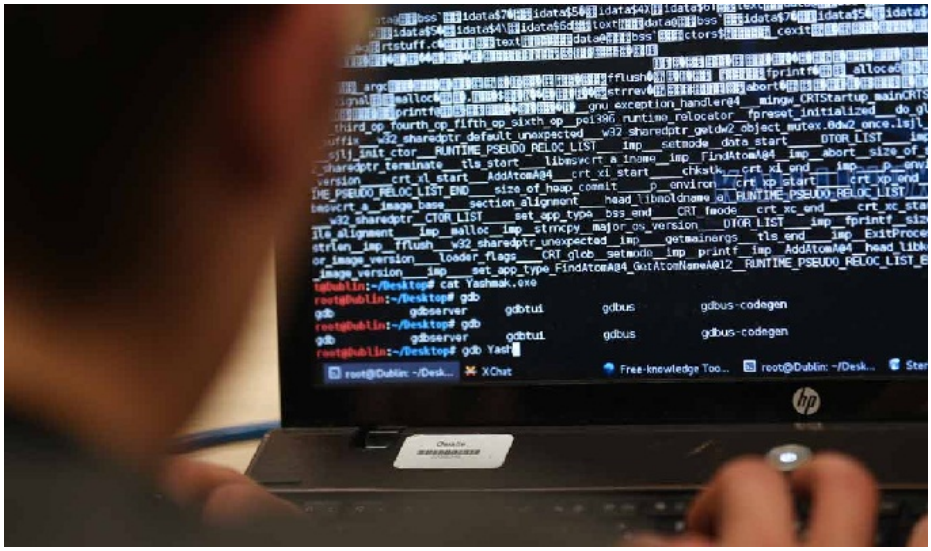
Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Original de l'article mis en page : Piratage de comptes

Telegram : 15 millions d’Iraniens concernés – ZATAZ

Cyberattaques terroristes déjouées au Maroc



Cyberattaques terroristes déjouées au Maroc

Des cyberattaques de sites étatiques planifiées par des individus soupçonnés d'avoir des penchants extrémistes et des relations avec Daech ont été déjouées dans le Royaume du Maroc grâce à une vaste opération antiterroriste qui a abouti à l'arrestation et la garde à vue de 52 personnes.

Selon un communiqué du ministère de l'Intérieur cité par des médias locaux, dont le Matin.ma, ainsi que le quotidien ivoirien Fraternité Matin, cette opération antiterroriste a été menée sous la houlette du parquet général et visait 343 individus.

Outre des projets terroristes ciblant des centres de loisir, des festivals, des établissements sécuritaires du Royaume, des cyberattaques à un niveau de préparation bien avancée devaient être dirigées contre les institutions marocaines. Objectif? Bloquer le fonctionnement des structures étatiques et paralyser l'économie.

D'autres personnes arrêtées par les forces de police marocaine sont soupçonnées de recruter des combattants mineurs via les réseaux sociaux.

Article original de Alselme AKEKO

Réagissez à cet article

Original de l’article mis en page : Terrorisme : des cyberattaques déjouées au Maroc | CIO MAG

Le site Internet des avocats de Mossack Fonseca, encore piraté !

System	Linux portal.mossfon.com 3.8.13-16.2.1.el6uek.x86_64 #1 SMP Thu Nov 7 17:01:44 PST 2013 x86_64
Build Date	Oct 15 2014 12:13:58
Configure Command	'./configure' '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib64' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--with-xpm-dir=/usr' '--enable-gd-native-ttf' '--without-gdbm' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr

Le site Internet des avocats de Mossack Fonseca, encore piraté !

Nous aurions pu penser que l'affaire des fuites de données du Panama Papers et du cabinet d'avocats Mossack Fonseca aurait permis à ces derniers de comprendre ce qu'était la sécurité informatique ! Raté !

Mossack Fonseca, pour rappel, un cabinet d'avocats basé au Panama qui a connu des fuites de données, voilà quelques mois. Des juristes qui cherchent des opportunités économiques aux entreprises, banques, artistes, politiques et sportifs ayant de l'argent à placer… hors de leur juridiction fiscale nationale.

Plusieurs fuites de données avaient été révélées en mars 2016, visant les clients de cette entreprise d'Amérique Centrale. Je vous expliquais comment, en quelques clics de souris et l'ami Google, j'avais pu accéder à plusieurs dizaines de milliers de CV, sauvegardés dans le portail web de « Monseca », comme du vulgaire papier. La presse Internationale, via les Panama Papers avaient diffusé des centaines d'informations sur des « VIP » ayant tenté de cacher à l'administration fiscale l'argent qu'ils possédaient.

Six mois plus tard, nous aurions pu penser que ces « professionnels » avaient pris quelques cours, du moins d'éducation numérique, pour protéger leurs sites Internet. Raté ! D'abord le noyau Linux qui fait tourner leur serveur. Un pirate Russe leur a stipulé, sur Twitter, qu'il datait toujours de 2013. Autant dire qu'il s'est empressé de lancer une petite attaque, histoire de réveiller ses interlocuteurs. Une autre fuite, cette fois avec le fichier phpinfo.php, accessible d'un clic de souris, offrant a qui sait le lire, des données pouvant être exploitées à des fins malveillantes.

A noter que de nouvelles révélations sont annoncées dans cette affaire du Panama Papers. Du blanchiment d'argent et du détournement concernant des hommes d'affaires, en Afrique !

Article original de Damien Bancal

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

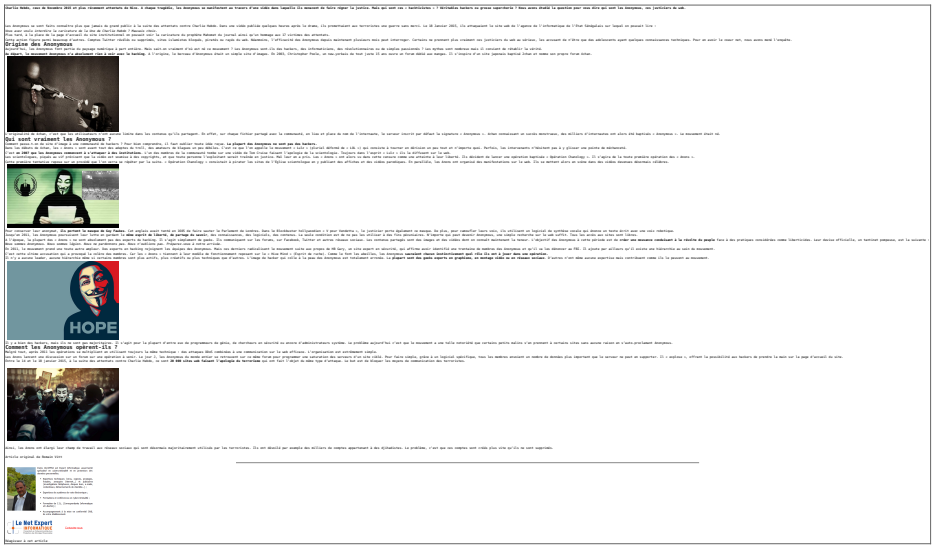
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : ZATAZ Fuites de données : le site des avocats de Mossack Fonseca, encore ! – ZATAZ

Qui sont vraiment les Anonymous, ces justiciers du web ?

Qui sont vraiment les Anonymous, ces justiciers du web ?



Original de l’article mis en page : Anonymous : qui sont vraiment ces justiciers du web ?

#PokemonGo hacké en moins de 2h…

#PokemonGo hacké en moins de 2h…

Suricate Concept, un GIE (Groupement d'Intérêt Economique) spécialisé dans la cyber-sécurité, a publié un rapport de 10 pages sur des failles de sécurité majeures identifiées dans le nouveau phénomène de société « Pokemon Go », après avoir réussi à pirater le jeu en un temps record.

L'étude intitulée « Comment on a hacké Pokemon Go en moins de 2h… » explique en détails comment l'équipe d'experts en cyber-sécurité s'est penché par hasard sur l'application et a rapidement identifié des failles qui permettaient aux joueurs de gagner des niveaux sans efforts en manipulant le programme.

Monir Morouche, à la tête du département cyber-sécurité et Président du GIE Suricate Concept a déclaré : « Chez Suricate Concept, tous les jours nous nous battons pour rendre le web un endroit plus sur et pour protéger les données et la vie privée des utilisateurs ainsi que les ressources en ligne de nos clients. Lorsque l'on a découvert Pokemon Go, complètement par hasard, on voulait savoir si le programme avait été suffisamment sécurisé par ses développeurs et si nous serions capable de trouver des failles dans l'application « .

Ce qui débuta comme un challenge interne au détour d'une pause de travail devint rapidement la base pour une étude plus poussée lorsque l'équipe réalise comment ils parvenaient facilement à manipuler le programme, générant ainsi des gains de niveaux et de ressources rapides pour un joueur à qui il faudrait normalement plusieurs semaines d'efforts pour y parvenir.

« Au sein de l'équipe, nous sommes toujours en train de nous challenger les uns les autres lorsque que quelque chose de nouveau dans l'univers du web ou des nouvelles technologies apparait. Pokemon Go était un sujet d'étude rêvé, du fait qu'il était présent partout dans l'actualité. Nous ne pouvions pas passer à côté. Dans toutes les démonstrations de hacking que nous conduisons, l'objectif premier est de sensibiliser les utilisateurs aux risques encourus et les éduquer sur comment être un utilisateur du web responsable », poursuit Monir Morouche.

L'étude publiée par Suricate Concept inclut une analyse technique de la façon dont l'équipe a procédé au hack en contournant les systèmes de sécurité existant du jeu, sans pour autant dévoiler tous les détails, qui « seront mis à disposition des développeurs de Pokemon Go sur demande » a indiqué Monir Morouche. Cela afin de que ces derniers ne soient pas utilisés à mauvais escient par des joueurs ou hackers mal intentionnés. Il ne s'agit pas du premier coup d'essai de la team Suricate Concept qui régulièrement au travers de démonstrations choc met en avant des failles de sécurité dans des services en ligne, ou objets connectés utilisés quotidiennement par le public. On peut par exemple citer parmi leurs récents travaux le hacking du moteur de recherche Google ou celui des cartes de paiement sans contact.

Suricate Concept a également annoncé il y a quelques mois lors du dernier Forum International de la Cyber-sécurité avoir réussi à hacker un objet médical connecté , un pace-maker, afin d'en prendre le contrôle complet. La démonstration a été dévoilée dans une vidéo avec un scénario d'inspiration hollywoodienne intitulée « The hacking dead » , en rapport avec la série à succès The Walking Dead.

Article original de

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 : Lille, 28 Juillet 2016 – Communiqué de presse: « Comment on a hacké PokemonGo en moins de 2h… » | Farouk JEBALI | LinkedIn

---

Piratage de 1,6 million de comptes Clash of King

Piratage de 1,6 million de comptes Clash of King

Pour ne pas avoir corrigé une faille vieille de 3 ans, le jeu Clash of King se retrouve avec 1,6 million de comptes de joueurs dans la nature.

vBulletin, un framework (un outil Internet NDR) de forum très utilisé sur le réseau des réseau a subi à plusieurs reprises des failles de sécurité. Des « bugs » que s'empressent d'utiliser les pirates informatique. La dernière campagne malveillante officielle visant ce forum concerne la société Elex qui produit le jeu sur mobile « Clash of Kings ». Ce jeu est utilisé par des millions de joueurs sur les plateformes mobiles. Ces joueurs s'enregistrent sur le forum afin d'échanger avec d'autres utilisateurs.
Le pirate a profité d'une faille vBulletin connue pourtant depuis 2013. Comme le rappel Matthieu Dierick, de chez F5 Networks, les failles ne sont pas nouvelles et l'ANSSI avait déjà alerté les autorités au sujet de vBulletin. Bref, si vous ne patchez pas, il ne faut pas pleurer ! vBulletin n'est pas responsable du fait que les entreprises ne programment pas leur mise à jour.
Pour détecter si un serveur est vulnérable, il suffit de lancer une requête HTTP sur une liste de serveurs et d'attendre un code retour. Voici un exemple de requête utilisée pour détecter la vulnérabilité d'un serveur : *http://[l'url du site]/ajax/api/hook/decodeArguments?arguments=O:12: »vB_dB_Result »:2{s:5: »*db »;O:11: »vB_Database »:1:{s:9: »functions »;a:1{s:11: »free_result »;s:6: »assert »;}}s:12: »*recordset »;s:20: »print_r(md5(92829)) »;}*.
Si le code retour contenait le hash 92829, alors l'espace numérique est vulnérable. C'est l'action qu'a orchestré le pirate de Clash of King. C'est la recherche qu'aurait du faire les équipes de Clash of King pour se protéger et sécuriser les utilisateurs.
Nous ne connaissons pas encore la vulnérabilité exploitée mais lors des dernières campagnes de piratage sur vBulletin, les pirates ont réussi à envoyer leur SHELL (Outil installé dans le serveur qui permet au pirate d'être maître de l'espace infiltré, NDR) sur le serveur et a exécuter des requêtes SQL en mode « root ». Pour cela, ils passaient par des fonctions PHP, par exemple la fonction system() qui permet l'exécution de commande shell.

Mot de passe hashé ? la belle affaire !
Les données volées concernent les identifiants avec mot de passe hashé, l'adresse mail, l'adresse IP et les tokens liés aux réseaux sociaux. Par hashé, comprenez que le mot de passe ne se lit plus directement (ZATAZ se transforme en hashé md5 par *79e35664717c21b96225d8d6ed4f0b16*). Les utilisateurs du forum doivent donc changer leur mot de passe même si ceux-ci étaient rendus illisibles au niveau de la base de données. Le hash MD5 ne sertb à rien si un mot de passe trop simple a été enregistré. Reprenons mon exemple avec *79e35664717c21b96225d8d6ed4f0b16*. Allez sur le site crackstation.net et rentrez *79e35664717c21b96225d8d6ed4f0b16*. En quelques millièmes de secondes, le mot de passe hashé n'est plus illisible. Pour une meilleure sécurité, dirigez-vous plutôt vers bcrypt !
« ***Toute infrastructure de données doit être protégée par des mécanismes d'analyse de niveau 7 tels que les Firewall Applicatifs ou Web Application Firewall.*** Indique Matthieu Dierick (Il commercialise ce genre d'outil, NDR). ***Cela peut empêcher un pirate de lancer des commandes sur un serveur même si celui-ci est concerné par une faille de sécurité***« . La politique de WAF empêche l'exécution de scripts, de commandes shell et de commandes PHP non autorisées.
En attendant, les 1,6 millions de clients impactés de Clash of King sont invités à changer leur mot de passe… surtout si ce dernier est aussi utilisé sur d'autres espaces web !

0Day vBulletin dans la nature ?
A noter que la société Trillian a alerté ses utilisateurs de l'utilisation d'un 0day vBulletin qui a touché l'un de ses services. La société ne sait pas vraiement quand a eu lieu l'attaque [on parle de décembre 2015, NDR] mais a fermé le site et le serveur contenant les forums impactés par la fuite de données. Dans les informations prises en main par le pirate : les données du blog de la société [sous WordPress] et « une poignée d'autres bases de données marketing qui contenait les noms d'utilisateurs Trillian et leurs adresses mail ». Les mots de passe étaient, eux aussi, en Md5. Le plus inquiétant à mon sens est que Trillian indique que les données « volées » étaient âgées de 3 à … 14 ans !
Article original de

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 : ZATAZ Piratage de 1,6 million de comptes Clash of King – ZATAZ

Les cyberattaques sont de plus en plus furtives

Les cyberattaques sont de plus en plus furtives

Comment détecter les cyberattaques les plus furtives ? Une priorité au quotidien pour toutes les entreprises. Tomer Weingarten, CEO SentinelOne, nous livre son expertise sur le sujet.

Alors que les cybercriminels – individus, groupements ou Etatiques – utilisent une combinaison de techniques complexes pour échapper à la détection, les cyberattaques deviennent plus intelligentes et furtives. Les techniques traditionnelles de protection reposant sur des signatures statiques – tels que les anti-virus (AV) – ou l'ignorance des vecteurs d'attaques comme les fichiers compromis, ne sont plus adaptés pour faire face au paysage de menaces d'aujourd'hui. Alors comment les entreprises peuvent tenter de se protéger contre les variantes de logiciels malveillants ou des nouveaux exploits, en constante évolution ?

Le poste de travail – incluant une série d'équipements : ordinateurs portables, tablettes, smartphones, serveurs ou même imprimantes – demeure l'une des cibles de choix dans toute attaque. Le poste de travail agit comme une passerelle pour les hackers dans leur intrusion au sein du réseau et une fois qu'un logiciel malveillant a été exécuté sur un poste de travail, les attaquants peuvent se déplacer librement. Ainsi, la détection et la protection doivent se produire sur les terminaux eux-mêmes. Ceci est d'autant plus important à l'ère du BYOD, car les utilisateurs peuvent facilement connecter leurs propres appareils au réseau de l'entreprise. Or, si les utilisateurs se connectent à un dispositif non autorisé ou infecté, le malware peut se déplacer librement au sein du réseau.

Evolution de la menace

Les techniques utilisées par les cybercriminels sont toujours en évolution pour garder une longueur d'avance sur les systèmes de protection et, comme la sophistication des logiciels malveillants se développe également, cela représente de nouveaux challenges pour les entreprises. Dans sa définition, un malware n'a pas changé. **Ce qui est en train de changer, ce sont les techniques d'évasion utilisées par de nouvelles formes de logiciels malveillants dans le but de voler des données précieuses présentent sur les postes de travail.**

Les "binders" sont un excellent exemple : ce sont de petits outils logiciels qui fusionnent deux fichiers .exe différents dans un seul fichier. L'exécution d'un .exe démarre simultanément le second de manière invisible. Ces outils piègent leurs victimes avec l'ouverture d'un fichier connu et qui semble légitime à l'extérieur ; mais qui est en fait malveillant à l'intérieur.

Aujourd'hui, les logiciels malveillants peuvent être conçus pour être « sensibles au contexte » et ont la capacité de détecter s'ils évoluent dans un environnement sandbox physique ou virtualisé. Une fois que ce type de malware détecte un environnement anormal, il échappe activement à la détection en agissant de façon bénigne ou en "dormant" pendant une période de temps définie. À partir de là, le malware tente d'interpréter les mouvements et de déchiffrer, si les actions proviennent d'un être humain ou d'un scanner de code automatisé. Cela permet au malware de contourner facilement les défenses traditionnelles telles que les sandboxes réseau, jusqu'à son exécution.

Reprendre le contrôle

Les attaques étant devenues plus sophistiquées, la protection des postes de travail annonce probablement la fin des anti-virus. Ces derniers reposant effectivement sur une analyse statique qui repère l'empreinte d'un fichier, les attaquants peuvent rapidement adapter des fichiers pour créer quelque chose de complètement nouveau et inconnu ; et ces nouvelles variantes peuvent facilement contourner la solution AV. Il a ainsi été estimé que les anti-virus ne peuvent repérer qu'environ 45 % des cyberattaques – ce qui en fait une solution obsolète face aux défis de la cybersécurité d'aujourd'hui.

Dans ce contexte, **une nouvelle génération de solutions de sécurité du poste de travail est en train d'émerger, telles que les techniques d'analyse comportementale,** afin que les entreprises puissent profiter des avantages des approches innovantes. Cette nouvelle ère de la protection se concentre, en temps réel, sur une approche proactive de la sécurité du poste de travail, réalisée par l'apprentissage automatique (machine learning) et l'automatisation intelligente afin de détecter et de protéger efficacement tous les terminaux contre les attaques les plus perfectionnées. Cette nouvelle génération de protection des postes de travail part du principe qu'elle ne connait rien sur les logiciels malveillants, mais qu'elle observe leur comportement dans le but de repérer les activités considérées comme des anomalies, et mettre en place les étapes de défense pour les dévier complètement.

De plus, **cette nouvelle génération de solutions a des capacités de remédiation pour inverser toutes les modifications apportées par les logiciels malveillants.** Cela signifie que lorsque les fichiers sont modifiés ou supprimés, ou lorsque des modifications sont apportées aux paramètres de configuration ou aux fichiers systèmes, le logiciel a la capacité de restaurer un poste de travail, comme il était, avant l'exécution du malware.

Dans la lutte contre la nouvelle génération de cyberattaques, cette approche plus dynamique et robuste des postes de travail permet aux entreprises de prendre l'avantage face aux cybercriminels.

Article original de iTPro.fr

Réagissez à cet article

Original de l’article mis en page : Détecter les cyberattaques les plus furtives | iTPro.fr

---

L’arnaqueur Chinaper Chinapa roi de l’escroquerie sur Internet enfin arrêté

L’arnaqueur Chinaper Chinapa roi de l’escroquerie sur Internet enfin arrêté

Il se nomme Chinaper Chinapa, un arnaqueur de Côte d'Ivoire qui vient d'être arrêté. Il arnaquait des hommes et des femmes sur Internet.

Les scammeurs, les brouteurs, bref les escrocs qui s'attaquent aux internautes sont légions sur la toile. Ils usent de multiples arnaques pour soutirer de l'argent à leurs victimes. Ils jouent ensuite les « rois » dans leur quartier. Parmi les pièges usités : l'arnaque à l'amour, le wash-wash, la création de billets, le faux mail d'inquiétude d'un proche perdu, la fausse location ou loterie… Pour Chinaper Chinapa, chaussures et portes feuilles magiques en bonus ! Je possède une liste d'une quarantaine d'arnaques possibles mises en place par les brouteurs.

Chinaper Chinapa le chenapant !

L'un des « rois » des brouteurs se nommait Chinape Chinapa. L'amateur de casquettes et baskets « bling-bling » se faisait passer pour un « magicien ». Il affirmait être capable de faire sortir des billets de chaussures, de boite magique. Il avait aussi mis en place des arnaques amoureuses, se faisant passer pour des hommes et des femmes à la recherche de l'âme sœur. Il volait les photos sur Facebook et « chassait », ensuite, sur des sites de rencontres.

J'ai pu croiser cet escroc de Chinaper Chinapa, il y a quelques mois, dans son pays (il se baladait aussi beaucoup au Bénin). Ce « roi » des boites de nuit qui sortait les billets de banque plus vite que 007 son Walther PPK.

Mi juin 2016, l'homme avait été tabassé par des personnes qu'il avait escroquées. Quinze jours plus tard, la police lui mettait la main dessus pour une série d'escroqueries. Arrêté par la police début juillet, détail confirmé par le journal Koaci. Le flambeur s'est retrouvé les menottes aux poignets dans son appartement de Cocody. Il est accusé d'activités cybercriminelles et de multiples escroqueries. Pas évident que sa « magie » fonctionne dans la prison d'Abidjan.

Un ami a besoin de vous

15h, un courrier signé d'un de vos amis arrive dans votre boîte mail. Pas de doute, il s'agit bien de lui. C'est son adresse électronique. Sauf que derrière ce message, il y a de forte chance qu'un brouteur a pris la main sur son webmail. Les courriels « piégés » arrivent toujours avec ce type de contenu « ***Je ne veux pas t'importuner. Tu vas bien j'espère, puis-je te demander un service ?***« . Le brouteur, par ce message, accroche sa cible. En cas de réponse de votre part, l'interlocuteur vous sortira plusieurs possibilités liées à sa missive « ***J'ai perdu ma carte bancaire. Je suis coincé en Afrique, peux-tu m'envoyer de l'argent que je te rembourserai à mon retour*** » ; « ***Je voudrais urgemment recharger ma carte afin de pouvoir régler mes frais de déplacement et assurer mon retour. J'aimerais s'il te plaît, que tu me viennes en aide en m'achetant juste 4 coupons de rechargement PCS MASTER CARD de 250 € puis transmets moi les codes RECH de chaque coupon de rechargement, je te rembourserais dès mon retour***« . Je possède plus d'une centaine de variantes d'excuses.

Bien entendu, ne répondez pas, ne versez encore moins d'argent. Attention, selon les brouteurs, des recherches poussées sur leurs victimes peuvent être mises en place. J'ai dernièrement traité le cas d'un brouteur qui connaissait le lieu de résidence du propriétaire du compte webmail que le voyou utilisait. De quoi faire baisser les craintes des amis contactés.

A noter que le scammeur indiquera toujours un besoin de confidentialité dans sa demande : « ***Je souhaite également que tu gardes ce mail pour toi uniquement. Je ne veux pas inquiéter mon entourage. Y'a t'il un buraliste ou un supermarché non loin de toi ?***« .

Remboursement de l'argent volé

Une autre arnaque de brouteurs est intéressante à expliquer. Elle est baptisée « *remboursement*« . Le voleur écrit aux internautes se plaignant, dans les forums par exemple, d'avoir été escroqués. L'idée de l'arnaque est simple : le voleur indique qu'il a été remboursé grâce à un policier spécialisé dans les brouteurs. Le voyou fournit alors une adresse électronique.

Suivre

ZATAZ.COM Officiel @zataz

Prudence à l'adresse « interpol.police.antiarnaque@gmail(.)com » qui n'est pas celle d' #interpol *! L'escroc cherche des personnes escroquées.*

23:12 – 14 Mai 2015

•

•

1111 Retweets

•

55 j'aime

Derrière cette fausse adresse de policier, un autre brouteur. Il va tenter d'escroquer le pigeon déjà pigeonné. Sa mission, se faire envoyer de l'argent via Western Union, MoneyGram. Certains brouteurs sont à la solde de petits commandants locaux qui imposent un quota d'argent à collecter. En 2013, la cyber police de Côté d'Ivoire estimait que les brouteurs avaient pu voler pas moins de ***21 millions d'euros****. N'hésitez pas à me contacter si vous avez croisé la route d'arnaques.*

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Brouteur : Chinaper Chinapa roi de l’escroquerie 2.0 – ZATAZ