Déchiffrement des communication numériques (Telegram et autres). Où en est-on ?

Déchiffrement des communication numériques (Telegram et autres). Où en est-on ?

Ce mardi 23 Août, Bernard Cazeneuve se réunissait avec son homologue allemand pour discuter d'une initiative européenne contre le chiffrement des données, afin de lutter contre le terrorisme. Une initiative qui ne fait pas l'unanimité.

Une initiative européenne contre les chiffrements trop forts ?

Face au terrorisme international et sachant que les messageries instantanées visées par le projet de loi sont majoritairement américaines, Bernard Cazeneuve s'en remet à une initiative européenne. L'idée serait d'étendre aux services de messageries et d'appels sur internet, les mêmes règles de sécurité et de confidentialité destinées jusque-là, aux opérateurs télécom. Le ministre a ainsi fermement déclaré vouloir obliger les services en ligne «*non coopératifs*» à «*retirer des contenus illicites ou déchiffrer des messages dans le cadre d'enquêtes judiciaires, que leur siège soit en Europe ou non*».

Conscient de la polémique qui entoure ce projet de loi, le ministre a précisé que l'utilisation des données déchiffrées ne servirait que dans le cadre « *judiciaire* ». Ce qui voudrait dire qu'elles ne seraient pas utilisées par les services secrets, comme le redoutent beaucoup de personnes. Se voulant rassurant, il a insisté « *Il n'a bien sûr, jamais été question de remettre en cause le principe du chiffrement des échanges* ». Le 16 septembre prochain, le projet de loi contre le chiffrement des données sera discuté lors du sommet des chefs d'états européens.

…[lire la suite]

Original de l'article mis en page : Une initiative franco-allemande contre le chiffrement numérique

Révélations sur de petits piratages informatiques entre alliés…

Révélations sur de petits piratages informatiques entre alliés…

C’est une révélation assez rare pour être soulignée, mais elle était passée inaperçue. Bernard Barbier, l’ancien directeur technique de la DGSE, le service de renseignement extérieur français, s’est livré en juin dernier à une longue confession devant les élèves de l’école d’ingénieurs Centrale-Supélec (voir vidéo ci-dessous), comme l’explique Le Monde.

Cet ex-cadre de l’espionnage a notamment confirmé que les Etats-Unis étaient bien responsables de l’attaque informatique de l’Elysée en 2012.

Entre les deux tours de la présidentielle de 2012, des ordinateurs de collaborateurs de Nicolas Sarkozy avaient été infectés à l’Elysée. Jusqu’à présent, les soupçons se portaient bien vers la NSA mais ils n’avaient jamais été confirmés. « Le responsable de la sécurité informatique de l’Elysée était un ancien de ma direction à la DGSE. Il nous a demandé de l’aide. On a vu qu’il y avait un malware », a expliqué Bernard Barbier en juin dernier. « En 2012, nous avions davantage de moyens et de puissance techniques pour travailler sur les métadonnées. J’en suis venu à la conclusion que cela ne pouvait être que les Etats-Unis. »

La France aussi impliquée dans un pirate informatique

Ce cadre de la DGSE a ensuite été envoyé par François Hollande pour s’entretenir avec ses homologues américains. « Ce fut vraiment un grand moment de ma carrière professionnelle », explique-t-il. « On était sûrs que c’était eux. A la fin de la réunion, Keith Alexander (l’ex-directeur de la NSA), n’était pas content. Alors que nous étions dans le bus, il me dit qu’il est déçu, car il pensait que jamais on ne les détecterait. Et il ajoute : ‘Vous êtes quand même bons.’ Les grands alliés, on ne les espionnait pas. Le fait que les Américains cassent cette règle, ça a été un choc. »

Pourtant, au cours de cette conférence, Bernard Barbier a aussi révélé l’implication de la France dans une vaste opération d’espionnage informatique commencée en 2009 qui avait touché notamment l’Espagne, la Grèce ou l’Algérie. Le Canada, lui aussi visé, avait à l’époque soupçonné Paris, mais rien n’avait été confirmé en France. « Les Canadiens ont fait du reverse sur un malware qu’ils avaient détecté. Ils ont retrouvé le programmeur qui avait surnommé son malware Babar et avait signé Titi. Ils en ont conclu qu’il était français. Et effectivement, c’était un Français. »

Article original de Thomas Liabot

Réagissez à cet article

Original de l’article mis en page : Les Etats-Unis étaient bien à l’origine du piratage informatique de l’Elysée en 2012 – leJDD.fr

---

Le logiciel de téléchargement Transmission à nouveau piraté

Le logiciel de téléchargement Transmission à nouveau piraté

Le Net Expert vous avait déjà informé en juillet dernier de cet type d'attaque dont avait été victime la sphère Apple. Apparemment la leçon n'a pas servi. Même méthode, même punition.

Pour la deuxième fois en moins de six mois, la version Mac du logiciel Transmission a été corrompue, a révélé mardi 30 août l'entreprise de sécurité informatique Eset. Ce client BitTorrent gratuit, qui permet de télécharger des fichiers (vidéo, sons…) est l'un des plus utilisés.
Cette fois l'éditeur propose une procédure à suivre si vous avez été piégé en téléchargeant la version 2.92 du logiciel entre le 28 et le 29 août. Si vous avez un doute, n'hésitez pas à suivre cette procédure.
Comme l'explique l'équipe de Transmission sur son site, des pirates se sont introduits dans ses serveurs et ont remplacé le logiciel par une version modifiée contenant un *malware* baptisé « OSX/Keydnap ». Ce logiciel malveillant permet, selon Eset, de dérober des mots de passe et d'installer une porte dérobée sur les ordinateurs touchés, permettant d'y avoir accès en permanence.

Un précédent avec un logiciel de racket

Tous les utilisateurs de Transmission ne sont pas concernés : seules les personnes ayant téléchargé la version 2.92 du logiciel entre le 28 et le 29 août risquent d'avoir par la même occasion installé le malware sur leur ordinateur. Ni Eset, ni Transmission n'ont précisé combien de personnes cela représentait. L'équipe du logiciel souligne toutefois que les mises à jour automatiques ne comprenaient pas ce malware.
Transmission dit avoir « *immédiatement* » supprimé la version piratée de son serveur après avoir découvert son existence, « *soit moins de vingt-quatre heures après que le fichier a été mis en ligne* ». Son site a publiéune marche à suivre pour les personnes ayant téléchargé le logiciel corrompu.
En mars, Transmission avait été victime du même type de piratage : le logiciel avait été remplacé sur le site par un *ransomware*, un logiciel de racket qui verrouille l'accès aux fichiers de sa victime et exige de l'argent en échange du déblocage de l'ordinateur.
Source : Le Monde

Réagissez à cet article

Original de l’article mis en page : Le logiciel de téléchargement Transmission à nouveau piraté

Alerte : Un canular sur Facebook qui diffuse de fausses informations terroristes

Alerte : Un canular sur Facebook qui diffuse de fausses informations terroristes

---

Les chercheurs ESET ont découvert une arnaque qui cible les utilisateurs de Facebook. D'abord répandu en République Tchèque et en Slovaquie, elle pourrait se propager dans d'autres pays

Les utilisateurs de Facebook en République Tchèque et en Slovaquie font face à une vague de fausses informations sur une attaque meurtrière à Prague. Quand l'utilisateur clique sur le canular, il est redirigé vers une page Internet de phishing qui essaye de le tromper en l'incitant à partager ses identifiants Facebook.

« D'après ce que nous savons à propos de cette campagne, l'attaque pourrait se propager dans plusieurs autres pays » met en garde Lukáš Štefanko, Malware Researcher chez ESET.

Cette prétendue attaque terroriste est facile à discréditer car la photo publiée ne ressemble pas à Prague, ni à aucune autre ville d'Europe. Malgré cela, l'arnaque se diffuse rapidement. « Les utilisateurs de Facebook partagent fréquemment des histoires sans les avoir lues. Les campagnes d'arnaques, si elles font appel à l'émotion, réussissent étonnamment bien à cause de notre empathie naturelle » commente Lukáš Štefanko.

Peu après le lancement de la campagne, Facebook a commencé à stopper les pages de phishing utilisées dans cette campagne. Les solutions de sécurité ESET sont conçues pour bloquer les pages Internet de phishing liées à ce type d'escroquerie ainsi que d'autres domaines enregistrés par cette même personne.

« Au cours des dernières semaines, il y a eu 84 domaines enregistrés par la même personne. La plupart d'entre eux possède une fonction de phishing, tandis que d'autres pourraient être utilisées à l'avenir lors d'une attaque à plus grande échelle » ajoute Lukáš Štefanko.

Voici les recommandations des experts ESET pour ceux qui pensent avoir été escroqué en partageant leurs identifiants Facebook :

– Changez votre mot de passe Facebook et utilisez les deux facteurs d'authentification fournis par Facebook

– Si vous avez utilisé le même mot de passe pour plusieurs services, changez-le partout – et mettez un terme à cette pratique très dangereuse.

Denis JACOPINI vous recommande les outils de protection suivants :

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 : Boîte de réception – denis.jacopini@gmail.com – Gmail

L’un des outils préférés des cybercriminels mis à mal par un coup de filet ?

L’un des outils préférés des cybercriminels mis à mal par un coup de filet ?

Karspersky publie aujourd'hui sur son blog un compte rendu d'une enquête des autorités russes à laquelle ils ont collaboré. Celle-ci a permis l'arrestation en juin d'un groupe de 50 cybercriminels, baptisés Lurk, qui opéraient notamment l'Angler exploit kit.

L'Angler Exploit Kit connaissait ces dernières années une popularité redoublée. Ce couteau suisse du cybercriminel était une plateforme utilisée pour infecter les machines de victimes : en l'installant sur un serveur et en amenant la cible à se connecter à ce serveur via un navigateur par exemple, le cybercriminel pouvait avoir recours à tout un éventail d'exploits fournis par les créateurs du kit pour tenter d'infecter la machine de la victime.

Simple à utiliser, évolutif et souvent à jour avec les derniers exploits et dernières vulnérabilités découvertes, l'Angler Exploit Kit dominait naturellement le marché. Mais en juin 2016, l'utilisation de cet outil par les cybercriminels a soudainement chuté sans véritable explication.

De nombreux observateurs avaient néanmoins fait le lien entre l'arrestation d'un groupe de 50 cybercriminels par les autorités russes et la soudaine disparition de l'Angler Kit. Dans une longue note de blog, Ruslan Stoyanov, dirigeant de l'unité investigation chez Kaspersky confirme cette théorie et détaille les 5 années passées sur la piste de ce groupe de cybercriminels de haute volée qui avaient été baptisés « Lurk ».

Le nom du groupe Lurk vient du premier malware repéré par Kaspersky en 2011. Celui-ci se présentait sous la forme d'un malware bancaire sophistiqué, qui visait principalement les logiciels bancaires afin de procéder à des virements frauduleux en direction des cybercriminels. Swift a connu plusieurs versions et évolutions, allant parfois jusqu'à fonctionner entièrement in memory pour éviter la détection.

Le malware Lurk se présentait comme un logiciel modulaire, pouvant embarquer plusieurs modules capables de réaliser des actions différentes, mais toujours orientées vers le vol de données bancaires et l'émission de virements frauduleux depuis les machines infectées.

Une petite PME sans histoire

« Avec le temps, nous avons réalisé que nous étions face à un groupe d'au moins 15 personnes. (…) Cette équipe était en mesure de mettre en place le cycle complet de développement d'un malware : à la fois sa conception, mais aussi la diffusion et la monétisation, à l'instar d'une petite entreprise de développement logiciel » explique Ruslan Stoyanov. Et le groupe Lurk avait également un autre atout de taille dans sa poche : exploitant leur renommée parmi les cybercriminels russophones, ils avaient commencé à louer les services de leur plateforme d'exploit, baptisée Angler Kit.

Cet exploit kit était à l'origine utilisé pour diffuser le malware bancaire Lurk, mais face aux mesures de sécurisation mises en place par de nombreuses banques, les revenus déclinants du groupe les ont forcés à diversifier leur activité. Les premières détections d'Angler Kit remontent à 2013, mais ce kit vendu en Saas par les cybercriminels du groupe Lurk a rapidement gagné en popularité.

Les créateurs du Blackhole kit ont été arrêtés en 2013, ce qui a laissé au nouveau programme du groupe Lurk un boulevard pour devenir le nouvel exploit kit préféré des cybercriminels. Dès le mois de mai 2015, celui-ci dominait largement le marché. Angler Kit pouvait être loué par d'autre groupe de cybercriminels qui s'en servaient pour diffuser différents types de malwares allant du ransomware au traditionnel trojan bancaire.

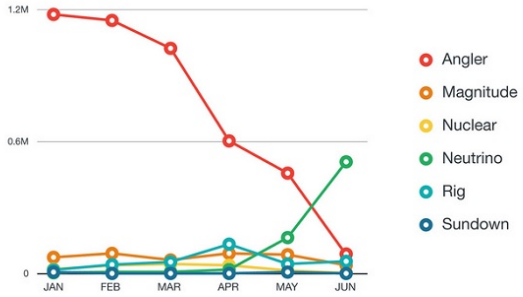


Figure 3: Number of times exploit-kit-hosting URLs were accessed in the first half of 2016

Mais le 7 juin, les autorités russes sont parvenues à arrêter les cybercriminels cachés derrière ce système. Kaspersky explique avoir collaboré avec les autorités afin de mener cette investigation, notamment via de l'échange d'informations compilées par la société sur le groupe. Un processus qui semble avoir été long et difficile, mais qui aura finalement porté ses fruits : l'Angler Kit est hors service et peut maintenant laisser la place… au nouvel exploit kit à la mode.

Selon les données récentes compilées par la société Trend Micro, l'exploit kit Neutrino aurait maintenant le vent en poupe et profiterait le plus de la retraite anticipée de son concurrent. Un de coffré, dix de retrouvés ?

Article original de Louis Adam

Réagissez à cet article

Original de l’article mis en page : L’un des outils préférés des cybercriminels mis à mal par un coup de filet ? – ZDNet

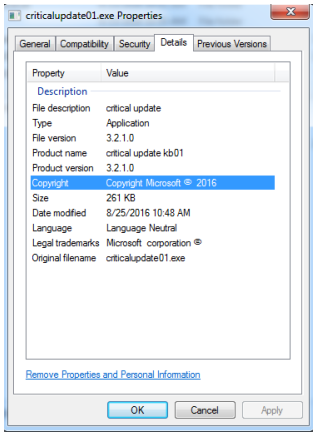
---

Alerte : Fantom, un nouveau ransomware qui sévit sous Windows 10

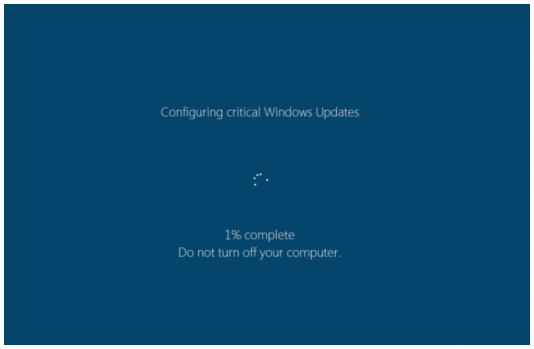
Alerte : Fantom, un nouveau ransomware qui sévit sous Windows 10

Windows 10 lance automatiquement ses mises à jour, ainsi que tous les utilisateurs que ça importunent le savent. Une bonne opportunité pour les cybercriminels de sévir tranquillement.

C'est ainsi qu'un nouveau ransomware a été découvert par un analyste de chez AVG Technologies.
Un premier exécutable maquille ses propriétés afin de faire croire qu'il provient de Microsoft et qu'il s'agit d'une mise à jour critique.



Une fois ce malware installé, il en télécharge un autre dans le répertoire AppDataLocalTemp, sous le nom WindowsUpdate.exe. Puis il l'exécute.
Pour l'utilisateur, c'est une mise à jour qui s'est déclenchée, tant l'écran de cette seconde partie du malware est bien faite, avec les polices de Microsoft bien imitées.



L'utilisateur n'est pas surpris de voir que son disque dur tourne, tourne… Une 'expérience utilisateur' qu'il doit régulièrement supporter…
Sauf que là, le disque tourne parce que le malware en crypte toutes les données. Le méfait accomplit, un autre écran apparaît, moins habituel, avec une invitation à contacter les cybercriminels par mail, pour finalement devoir payer une rançon afin de récupérer les données.
Utilisateurs de Windows 10, la prochaine fois que vous verrez un écran de mise à jour, croisez les doigts !

Article original de fredericmazue

Denis JACOPINI vous recommande le logiciel de sécurité suivant :

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 : Fantom : un nouveau ransomware qui sévit sous Windows 10 | Programmez!

Caméras IP installées par des incompétents ? Une aubaine pour les pirates

Caméras IP installées par des incompétents ? Une aubaine pour les pirates

---

Le piratage des caméras de vidéo surveillance, un jeu d'enfant pour les plus dégourdis du web. Sauf que ces pirates n'ont rien de génie, ils profitent uniquement de la fainéantise des utilisateurs.

Le piratage des caméras de vidéo surveillance n'est pas nouveau. Je vous parlais déjà de ces infiltrations de webcams en 2000. En novembre 2015, par exemple, je revenais sur un fichier contenant des centaines de webcams non sécurisées vendues dans le blackmarket ou encore de ce bébé réveillé par des hurlements d'un idiot du village ayant pris la main sur le baby phone de la famille.

En 2014, je vous révélais la création d'un site Internet Russe qui référencent plusieurs dizaines de milliers de webcams. Bref, un business juteux pour les commerçants du voyeurisme et autres vendeurs de données sensibles (La boutique est-elle vide ? Le hangar stocke en ce moment des téléphones portables ; la banque vient d'être livrée en billets frais…).

Je te soupçonne de taper dans la caisse ! (Boutique de la Ville de Rai)

La sécurité des caméras sur IP est souvent mise à la mal comme j'ai pu le montrer dans ZATAZWeb.tv de mars 2014. Il ne devrait pas être si facile, normalement, de regarder dans la chambre d'un étranger, et encore moins dans des centaines de chambres filmées par ces caméras de vidéo surveillance. Pourtant, cela reste possible comme je vais vous l'expliquer plus bas.

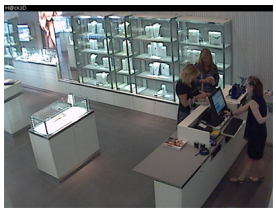
Montrez moi votre contrat, que je vous renseigne. (Boutique du 92)

Failles et mots de passe facilitent le piratage des caméras de vidéo de surveillance

Pour accéder à une caméra de vidéo surveillance rien de plus facile. D'abord avoir l'IP de la cible. Un détail pour les adeptes du social engineering. Autant dire que cette adresse n'est à communiquer à personne. Lisez le mode d'emploi de votre caméra. Chercher les options de sécurité proposées. Soyons honnête, plus votre webcam IP aura d'option, plus elle sera coûteuse. Mais la réflexion vaut, je pense, la sécurité de ce que vous souhaitez protéger. Ensuite, le malveillant va rechercher la marque de votre matériel. Pour cela, rien de plus simple une fois encore. La page d'accès à l'administration de votre matériel parle.

Mais tu vas le changer ce password… c'est marqué en GRAS ! (Hôtel du 77)

Un conseil, faites de manière à ce qu'elle ne soit pas lisible : un Htaccess par exemple, ou modifier le logo et toutes marques de reconnaissance pour le malveillant. Ensuite, le mot de passe. Trop de webcam IP, de caméras de vidéo surveillance gardent le mot de passe usine. Je vous laisse imaginer la facilité déconcertante que de retrouver ce sésame dans les notices et listes disponibles sur la toile. Un *admin:admin ; root:root et autre admin:0000* sont légions. Des clés qui se changent. Vous le faites bien quand vous perdez les clés de votre maison, faites le sur Internet. Enfin, les failles. Assurez-vous que votre cerbère ne soit pas référencé comme étant un outil « *open bar*« . Pour cela, un petit coup de Google ou ne soyez pas timide, posez la question !



La bijouterie est vide ! Le matériel, la caisse, le coffre sont repérés. Autant d'informations qui faciliteront l'action d'un malveillant. Vous aurez remarqué le petit « H@ck3D » en haut à gauche qui ne semble perturber personne !

Branleurs, voleurs, mateurs… même combat

Dans mon exemple, le pirate possède donc dorénavant l'IP, l'accès à la page d'administration de votre webcam IP, sa marque, vous n'avez pas changé le mot de passe usine et si c'est le cas, il vient de rechercher sur la toile les failles et accès « *pasvraimentprévudanslemodedemploi*« . Dernier exemple en date que ZATAZ a pu constater, l'alerte au sujet de la société AXIS. Un logiciel pirate, baptisé « *Hack AXIS* » permettait (permet toujours pour les caméras non mises à jour, NDR) d'accéder à la racine des périphériques sans avoir besoin de connaitre le mot de passe ; changer le mot de passe du matériel ; contrôler la caméra et, dans ce cas, lancer des attaques via la caméra transformée en Zombie/botnet. La caméra prise en main de la sorte par un pirate au fait de la faille, même mise à jour ensuite, restait dans le sac à malveillance de l'intrus. Une attaque d'autant plus gênante que l'exploit a été diffusé, en juillet 2016.

Bref, voilà donc le pirate avec une nouvelle source d'information à votre sujet. Imaginez, le serveur et l'IP l'oriente sur votre situation numérique ; la caméra, et les informations qu'elle peut transporter, fournissent au malveillant les yeux qu'il n'avait pas. En France, c'est une liste de plusieurs milliers de webcams accessibles qui trainent sur la toile, que ce soit dans le blackmarket ou sur des sites offrant de regarder à travers ces « yeux » non sécurisés.

Auteur : Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Vidéo surveillance : Vous n’en avez pas marre d’être des idiots du 2.0 – ZATAZ

Les pirates informatiques recrutent des complices chez les opérateurs télécoms

Les pirates informatiques recrutent des complices chez les opérateurs télécoms

---

Un rapport de Kaspersky détaille les nombreuses menaces qui ciblent les opérateurs de télécommunications, réparties en deux catégories : celles qui les ciblent directement (DDoS, campagnes APT, failles sur des équipements, ingénierie sociale…) et celles qui visent les abonnés à leurs services. Parmi les premières, le recrutement de complicités internes, sous la menace ou par appât du gain, progressent, même si elles restent l'exception.

Les opérateurs de télécommunications constituent une cible de choix pour les cyberattaques. Ils gèrent des infrastructures de réseau complexes utilisées pour les communications téléphoniques et la transmission de données et stockent de grandes quantités d'informations sensibles. Dans ce secteur, les incidents de sécurité ont augmenté de 45% en 2015 par rapport à 2014, selon PwC. Dans un rapport intitulé « Threat intelligence report for the telecommunications industry » publié cette semaine par Kaspersky, l'éditeur de logiciels de sécurité détaille les 4 principales menaces qui visent les opérateurs de télécommunications et fournisseurs d'accès Internet (FAI) : les attaques en déni de service distribué (en hausse), l'exploitation de failles dans leur réseau et les terminaux clients, la compromission d'abonnés (par ingénierie sociale, phishing ou malware) et, enfin, le recrutement de personnes capables d'aider les cyber-criminels en interne, au sein même des entreprises attaquées.

Lorsque les attaques passent par des collaborateurs contactés par les cybercriminels, il est difficile d'anticiper ces risques car les motivations sont diverses : appât du gain, collaborateur mécontent, coercition ou tout simplement négligence. Certains de ces relais internes agissent de façon volontaire, d'autres y sont forcés par la menace ou le chantage. Chez les opérateurs de télécoms, on demande principalement à ces « insiders » de fournir un accès aux données, tandis que chez les fournisseurs d'accès Internet (FAI), on les utilise en appui à des attaques contre le réseau ou des actions de type man-in-the-middle (MITM). Même si le recours à des collaborateurs indélicats reste rare, cette menace progresse, selon Kaspersky, et ses conséquences peuvent être extrêmement critiques car elle peut ouvrir une voie directe vers les données ayant le plus de valeur. Le chantage est l'un des vecteurs de recrutement le plus efficace. A ce sujet, le spécialiste en technologies de sécurité remet en mémoire l'intrusion sur le site de rencontres extra-conjugales Ashley Madison, l'été dernier. Celle-ci a permis le vol de données personnelles que les attaquants ont pu confronter à d'autres informations publiquement accessibles pour déterminer où les personnes travaillaient et les compromettre.

Même des pirates inexpérimentés peuvent mener des attaques DDoS

D'une façon générale, Kaspersky répartit en deux catégories l'ensemble des menaces visant les opérateurs télécoms à tous les niveaux : d'une part, celles qui les ciblent directement (DDoS, campagnes APT, failles sur des équipements, contrôles d'accès mal configurés, recrutement de complicités internes, ingénierie sociale, accès aux données), d'autre part celles qui visent les abonnés à leurs services, c'est-à-dire les clients des opérateurs mobiles et des FAI. Les attaques en déni de service distribué ne doivent pas être sous-estimées, rappelle Kaspersky, car elles peuvent être un signe précurseur d'une deuxième attaque, plus préjudiciable. Elles peuvent aussi servir à affecter un abonné professionnel clé, ou encore à ouvrir la voie à une attaque par ransomware à grande échelle. Le 1er cas a été illustré par l'intrusion subie en 2015 par Talk Talk, l'opérateur de télécoms britannique, résultant dans le vol d'1,2 millions d'informations clients (noms, emails, dates de naissance, données financières…). L'enquête a montré que les pirates avaient dissimulé leurs activités derrière l'écran de fumée d'une attaque DDoS. L'un des éléments préoccupants de ces menaces, c'est que même des attaquants inexpérimentés peuvent les organiser de façon relativement efficace, rappelle Kaspersky.

Des équipements vulnérables et des malwares difficiles à éliminer

Les vulnérabilités existant dans les équipements réseaux, les femtocells (éléments de base des réseaux cellulaires) et les routeurs des consommateurs ou des entreprises fournissent aussi de nouveaux canaux d'attaques, de même que les logiciels exploitant des failles dans les smartphones Android. Ces intrusions mettent en œuvre des malwares difficiles à éliminer. En dépit des nombreux vols de données perpétrés au cours des 12 derniers mois, les attaques se poursuivent, exploitant souvent des failles non corrigées ou nouvellement découvertes. En 2015, par exemple, le groupe Linker Squad s'est introduit chez Orange en Espagne à travers un site web vulnérable à une injection SQL et a volé 10 millions de coordonnées sur les clients et les salariés. Par ailleurs, dans de nombreux cas, les équipements utilisés par les opérateurs présentent des interfaces de configuration auxquelles on accède librement à travers http, SSH, FTP ou telnet et si le pare-feu n'est pas configuré correctement, ils constituent une cible facile pour des accès non autorisés, explique encore Kaspersky.

En résumé, les menaces visant les opérateurs de télécommunications existent à de nombreux niveaux – matériel, logiciel, humain – et les attaques peuvent venir de différentes directions. Les opérateurs doivent donc « regarder la sécurité comme un processus englobant tout à la fois la prédiction, la prévention, la détection, la réponse et l'enquête », conclut Kaspersky.

Article de Maryse Gros

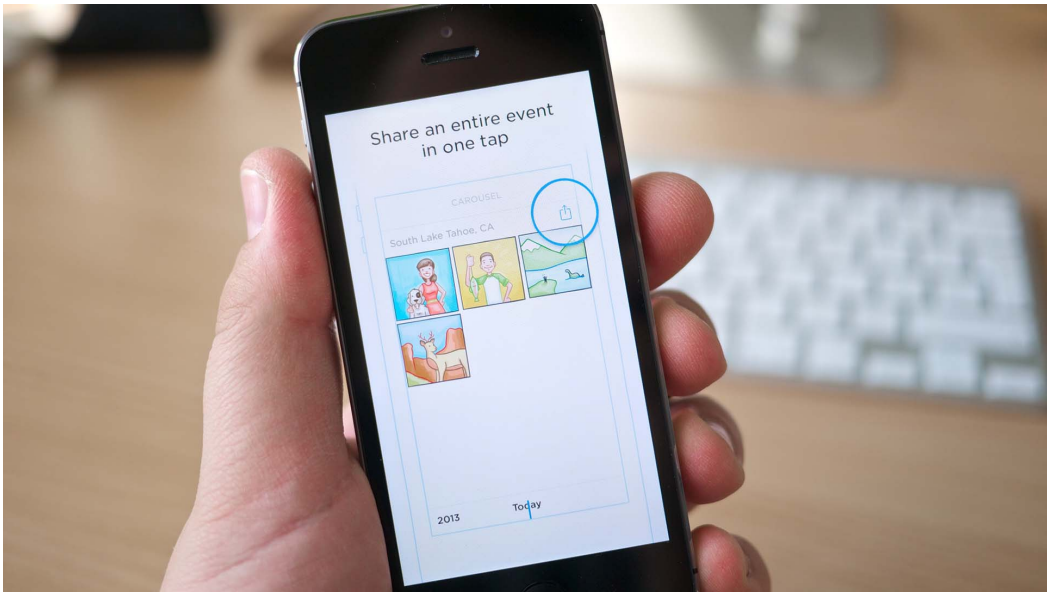
Réagissez à cet article

Original de l'article mis en page : Les pirates recrutent des complices chez les opérateurs télécoms – Le Monde Informatique

---

68 millions de comptes

Dropbox piratés



68 millions de comptes Dropbox piratés

Quatre ans avoir avoir été victime d'un piratage et avoir su qu'il avait donné accès à une liste d'adresses e-mail, Dropbox a décidé il y a quelques jours de réinitialiser les mots de passe. Mais ce n'est qu'aujourd'hui que l'on en découvre l'ampleur.

La semaine dernière, Dropbox annonçait la réinitialisation de mots de passe d'utilisateurs inscrits depuis au moins 2012, en expliquant avoir été informé du fait qu'une base de données piratée à l'époque circulait, dans laquelle des adresses e-mails et des mots de passe hashés figurent. Dropbox avait prévenu dès 2012 qu'il avait été victime d'un tel piratage dû au vol d'un mot de passe d'un employé, et que les adresses e-mails obtenues avaient été utilisées pour envoyer des spams.

DROPBOX A MIS QUATRE ANS À RÉAGIR

Rien ne permet de penser que des mots de passe ont pu être déchiffrés. En revanche si vous utilisez le même mot de passe sur Dropbox que sur d'autres services en ligne, et si ces services ont eux-aussi été piratés, il est possible d'accéder à votre Dropbox en utilisant le mot de passe obtenu ailleurs. En 2012, le service en ligne avait d'ailleurs indiqué que des accès frauduleux avaient été faits par cette méthode, neutralisée lorsque l'on active la validation en deux étapes.

Dès lors, on ne comprend pas pourquoi Dropbox a attendu quatre ans (!) avant de réinitialiser les mots de passe.

Ce piratage dont la base de données resurgit après plusieurs années est le dernier en date d'une série similaire, qui fait penser qu'il pourrait s'agir du même groupe, ou de mêmes failles ont pu être exploitées à l'époque. Ainsi ces derniers mois on a appris la diffusion de 171 millions de mots de passe VK (le Facebook russe),427 millions de comptes Myspace,167 millions de mots de passe LinkedIn ou encore 32 millions de mots de passe Twitter.

Article original de Guillaume Champeau

Réagissez à cet article

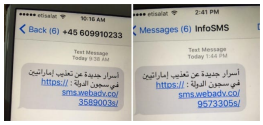
Original de l'article mis en page : Une base de 68 millions de comptes Dropbox circule chez les pirates — Tech — Numerama

Le malware Pegasus exploite 3 failles 0 day sur iPhone

	Le malware Pegasus exploite 3 failles 0 day sur iPhone

Les trois failles corrigées par Apple dans iOS 9.3.5 (ainsi que dans la dernière bêta d'iOS 10 livrée, contre toute attente, vendredi dernier) sont redoutables. Elles ont été exploitées par NSO Group, une société israélienne dont le fonds de commerce n'est autre que l'espionnage de journalistes et de militants. Le site Motherboard raconte la découverte de l'affaire qui relève du thriller…

Ce 10 août, Ahmed Mansoor, un militant des droits de l'homme dans les Émirats Arabes Unis, reçoit sur son iPhone un message lui proposant d'en savoir plus sur de «*nouveaux secrets sur la torture dans les prisons d'État* ». Un lien accompagnait ce message, qu'il s'est bien gardé de lancer.



Les deux messages reçus par Mansoor — Cliquer pour agrandir

À la place, il a contacté un chercheur du Citizen Lab, un organisme de défense des droits numériques rattaché à l'université de Toronto. Aidé par Lookout, un spécialiste de la sécurité mobile, ils ont pu mettre au jour un mécanisme très élaboré de surveillance par iPhone interposé.
Si Mansoor avait touché le lien, il aurait provoqué le jailbreak de son iPhone et donné à NSO Group le plein contrôle de son smartphone. « *Un des logiciels de cyberespionnage parmi les plus sophistiqués que nous ayons jamais vus* », expliquent les chercheurs.
NSO Group vient d'apparaitre sur les radars, mais cette entreprise très discrète (aucune présence sur internet) opère depuis 2010. Le malware qu'elle a mis au point, baptisé Pegasus, permet d'infecter un iPhone, d'intercepter et de voler les données et les communications. Une arme redoutable, qualifiée de « *fantôme* » par NSO pendant une de ses rares interventions publiques en 2013. Cette société vend Pegasus au plus offrant, notamment des gouvernements peu regardants sur les droits de l'homme.

Les données volées par Pegasus — Cliquer pour agrandir
NSO a visiblement pu pénétrer par effraction dans des iPhone depuis le modèle 5. Son malware est programmé avec des réglages qui remontent jusqu'à iOS 7.
Ces trois failles *zero day*, baptisées Trident par les chercheurs, ont été communiquées à Apple il y a dix jours. « *Nous avons été mis au courant de cette vulnérabilité et nous l'avons immédiatement corrigée avec iOS 9.3.5* », explique un porte-parole du constructeur. « *iOS reste toutefois le système d'exploitation mobile grand public le plus sécurisé disponible* », rassure Dan Guido, patron de la société de sécurité informatique Trail Of Bits, qui travaille souvent avec la Pomme.
Il indique toutefois qu'il reste à améliorer le système de détection des vulnérabilités. Apple a annoncé début août un programme de chasse (rémunérée) aux failles.
Article original de Mickaël Bazoge

Réagissez à cet article

Original de l'article mis en page : Cyberspionnage : derrière les failles Trident d'iOS, le redoutable malware Pegasus | iGeneration