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.

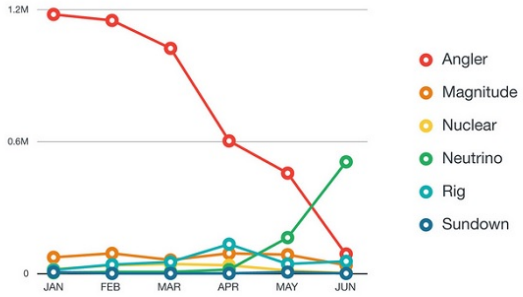


Figure 3: Number of times exploit-kit-hosting URLs were accessed in the first half of 2016

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

---

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

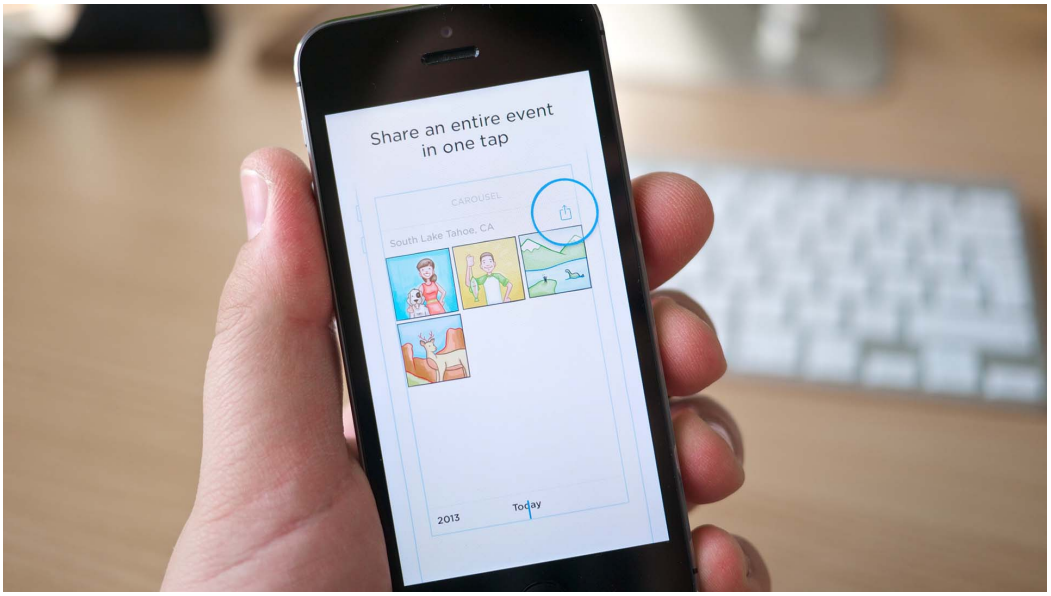
Réagissez à cet article

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.

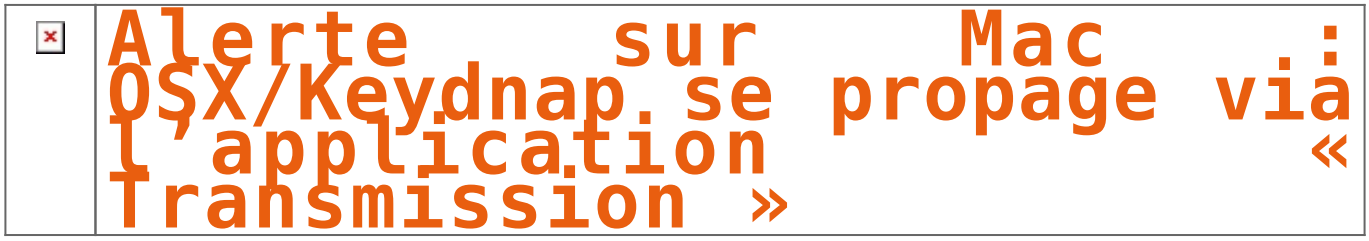
Ce piratage dont la base de données resurgit après plusieurs années est le dernier en date d'une série similaire, qui fait penser qu'il pourrait s'agir du même groupe, ou de mêmes failles ont pu être exploitées à l'époque. Ainsi ces derniers mois on a appris la diffusion de 171 millions de mots de passe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

Alerte sur Mac : OSX/Keydnap se propage via l'application « Transmission »



Le mois dernier, les chercheurs d'ESET ont découvert un malware sur Mac OS X nommé OSX/Keydnap, qui exfiltre les mots de passe et clés stockés dans le gestionnaire de mots de passe « KeyChain » ; et qui crée une porte dérobée permanente.
Au moment de la découverte, notre Malware Researcher Marc-Etienne Léveillé expliquait que « tous les utilisateurs d'OS X doivent rester vigilants car nous ne savons toujours pas comment Keydnap est distribué, ni combien de victimes ont été touchées ».

Les équipes ESET viennent de découvrir que le malware OSX/Keydnap se distribue via une version compilée de l'application BitTorrent.

Une réponse instantanée de l'équipe de transmission

Suite à l'alerte donnée par ESET, l'équipe de transmission a supprimé le fichier malveillant de leur serveur Web et a lancé une enquête pour identifier le problème. Au moment de la diffusion de la première alerte, il était impossible de préciser depuis combien de temps le fichier malveillant a été mis à disposition en téléchargement.

Selon les informations de la signature, l'application a été signée le 28 août 2016, mais ne se serait répandue que le lendemain. Ainsi, les équipes ESET conseillent aux personnes qui ont téléchargé la transmission V2.92 entre le 28 et le 29 août 2016 de vérifier si leur système est compromis en testant la présence de l'un des fichiers ou répertoires suivant :

- /Applications/Transmission.app/Contents/Resources/-License.rtf
- /Volumes/Transmission/Transmission.app/Contents/-Resources/License.rtf
- $HOME/Library/Application Support/com.apple.iCloud.sync.-daemon/icloudsyncd
- $HOME/Library/Application Support/com.apple.iCloud.sync.-daemon/process.id
- $HOME/Library/LaunchAgents/com.apple.iCloud.sync.daemon.-plist
- /Library/Application Support/com.apple.iCloud.sync.-daemon/
- $HOME/Library/LaunchAgents/com.geticloud.icloud.photo.-plist

Si l'un d'eux est présent, cela signifie que l'application malveillante de « transmission » a été exécutée et que le malware Keydnap est probablement en cours d'exécution. Notez également que l'image malicieuse du disque se nomme Transmission 2.92.dmg tandis que l'original se nomme Transmission–2.92.dmg (trait d'union).

Article original de ESET

Pour protéger votre Mac, Denis JACOPINI recommande l'application suivante :

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

Des systèmes biométriques piratés à partir de vos photos Facebook

Des systèmes biométriques piratés à partir de vos photos Facebook

Des chercheurs découvrent comment pirater des systèmes biométriques grâce à Facebook. Les photographies sauvegardées dans les pages de Facebook peuvent permettre de vous espionner.

De nombreuses entreprises de haute technologie considèrent le système de reconnaissance faciale comme l'une des méthodes fiables pour être reconnu par votre ordinateur. J'utilise moi-même la reconnaissance biométrique digitale, rétinienne et du visage pour certaines de mes machines. C'est clairement un des moyens simples et fiables de vérification d'une identité. Cependant, des chercheurs prouvent que la biométrie peut se contourner, dans certains cas, avec une photo, de la colle…

Une nouvelle découverte vient de mettre à mal, cette fois, la reconnaissance faciale mise en place par Facebook. Comme je pouvais vous en parler en 2014, Facebook met en place une reconnaissance faciale que des commerçants Américains ont pu tester avec succès. Des chercheurs ont découvert que cette prouesse technologique n'est pas encore parfaite et sujette au piratage. Des pirates peuvent utiliser votre profil Facebook, et les photos sauvegarder.

Systèmes biométriques

Des étudiants de l'Université de Caroline du Nord ont expliqué lors de la conférence d'Usenix, à Austin, avoir découvert une nouvelle technique particulièrement exaspérante pour intercepter l'intégralité d'un visage, via Facebook. Le rendu 3D et certaines « lumières » peuvent permettre de cartographier votre visage en deux clics de souris. Les chercheurs ont présenté un système qui créé des modèles 3D du visage via les photos trouvées sur Facebook. Leur modèle 3D va réussir ensuite à tromper quatre systèmes de reconnaissance faciale… sur 5 testés : KeyLemon, Mobius, TrueKey, BioID, et 1D.

Pour leur étude, 20 cobayes volontaires ont participé à l'expérience. Leurs photos sont tirées d'espaces publiques comme Facebook, mais aussi LinkedIn et Google+. La modélisation des visages à partir de 27 images différentes va permettre de créer des modèles en 3D, avec des animations faciales : bouches, yeux… Les chercheurs ont reconstruit les visages via les bouts trouvés sur les différentes photographies.

Article original de Damien Bancal

Réagissez à cet article

Original de l'article mis en page : Pirater des systèmes biométriques à partir de vos photos Facebook — Data Security BreachData Security Breach

Filtre anti espion sur les prochains ordinateurs portables Hewlett-Packard

Filtre anti espion sur les prochains ordinateurs portables Hewlett-Packard

Le géant de l'informatique Hewlett-Packard s'associe avec 3M pour préinstaller sur ses prochains ordinateurs portables professionnels un filtre anti espion.

Quoi de plus courant que de croiser à la terrasse d'un café, dans le train ou dans un aéroport ces fiers commerciaux pressés de travailler, même dans un lieu non sécurisé. Autant dire que collecter des données privées, sensibles, en regardant juste l'écran de ces professionnels du « c'est quoi la sécurité informatique ? » est un jeu d'enfant.

Hewlett-Packard (HP), en partenariat avec 3M, se prépare à commercialiser des ordinateurs portables (Elitebook 1040 et Elitebook 840) dont les écrans seront équipés d'un filtre anti voyeur. Un filtre intégré directement dans la machine. Plus besoin d'utiliser une protection extérieure.

Une sécurité supplémentaire pour les utilisateurs, et un argument de vente loin d'être négligeable pour le constructeur. Selon Mike Nash, ancien chef de la division de sécurité de Microsoft et actuellement vice-président de Hewlett-Packard, il est possible de croiser, partout, des utilisateurs d'ordinateurs portables sans aucune protection écran. Bilan, les informations affichés à l'écran peuvent être lues, filmées, photographiées.

Le filtre pourra être activé et désactivé à loisir.

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : Filtre anti espion sur les prochains Hewlett-Packard – Data Security BreachData Security Breach

---

Devez-vous changer votre mot de passe DropBox ?

	Devez-vous changer votre mot de passe DropBox ?

On vous demande de créer un nouveau mot de passe sur dropbox.com. Pourquoi et que devez-vous faire ?
L'entité propose de faire des sauvegardes de ses fichiers dans le Cloud, le fameux nuage. Bref, des disques durs hors de chez vous, hors de votre entreprise, sur lesquels vous déposez vos données afin d'y accéder partout dans le monde, et peu importe le support : Ordinateur, smartphone…
Depuis quelques heures, une vague de courriels aux couleurs de DropBox vous indique « ***On me demande de créer un nouveau mot de passe sur dropbox.com. Pourquoi et que dois-je faire ?***« , si les plus paranoïaques ont jeté la missive de peur d'être nez-à-nez avec un phishing, je me suis penché sur le sujet, histoire de m'assurer que l'alerte valait la peine d'être lancée. Je vais être rapide avec le sujet, oui, il s'agit bien d'un courriel officiel de la firme US.

Lors de votre prochaine visite sur dropbox.com, vous serez peut-être invité à créer un nouveau mot de passe. Une modification « ***à titre préventif à certains utilisateurs*** » souligne Dropbox. Les utilisateurs concernés répondent aux critères suivants : ils ont créé un compte Dropbox avant mi-2012 et ils n'ont pas modifié leur mot de passe depuis mi-2012. Vous commencez à comprendre le problème ? Comme je vous le révélais la semaine dernière, des espaces web comme Leakedsource, le site qui met en danger votre vie privée, sont capable de fournir aux pirates une aide précieuse. Comment ? En diffusant les informations collectées dans des bases de données piratées.

Que dois-je faire ?
Si, quand vous accédez à dropbox.com, vous êtes invité à créer un nouveau mot de passe, suivez les instructions sur la page qui s'affiche. Une procédure de modification des mots de passe qui n'a rien d'un hasard. Les équipes en charge de la sécurité de DropBox effectuent une veille permanente des nouvelles menaces pour leurs utilisateurs. Et comme vous l'a révélé ZATAZ, Leaked Source et compagnie fournissent à qui va payer les logins et mots de passe d'utilisateurs qui utilisent toujours le même sésame d'accès, peu importe les sites utilisés. Bref, des clients Adobe, Linkedin … ont peut-être exploité le même mot de passe pour DropBox.
Bilan, les pirates peuvent se servir comme ce fût le cas, par exemple, pour ma révélation concernant le créateur des jeux Vidéo Rush et GarryMod ou encore de ce garde du corps de Poutine et Nicolas Sarkozy. Les informaticiens de Dropbox ont identifié « ***d'anciennes informations d'identification Dropbox (combinaisons d'adresses e-mail et de mots de passe chiffrés) qui auraient été dérobées en 2012. Nos recherches donnent à penser que ces informations d'identification sont liées à un incident de sécurité que nous avions signalé à cette époque***. » termine DropBox.
A titre de précaution, Dropbox demande à l'ensemble de ses utilisateurs qui n'ont pas modifié leur mot de passe depuis mi-2012 de le faire lors de leur prochaine connexion.
Article original de Damien Bancal

Les conseils de Denis JACOPINI
Comme tout e-mail reçu, la prudence est de rigueur. Avant de valider l'authenticité d'un e-mail envoyé par une firme telle que Dropbox, nous avons dû analyser l'entête de l'e-mail reçu et comparer les données techniques de celles répertoriées dans les bases de données connues.
J'imagine que vous n'aurez pas le courage d'apprendre à le faire vous même ni que vous trouverez l'intérêt de consacrer du temps pour ça.
Comme chaque mise à jour demandée par un éditeur ou un constructeur, comme tout changement de mot de passe recommandé par une firme, nous vous conseillons de le faire en allant directement sur le site concerné.
Dans le cas de « Dropbox », nous vous recommandons de rechercher « dropbox.com » dans google ou de taper « dropbox.com » dans votre barre d'adresse et de vous identifier. Vous serez ainsi sur le site officiel et en sécurité pour réaliser la procédure demandée.

Attention
Vous ne serez en sécurité que si votre ordinateur n'est pas déjà infecté. En effet, taper un nouveau mot de passe si votre ordinateur est déjà infecté par un programme espion revient à communiquer au voleur une copie de vos nouvelles clés. Taper l'ancien mot de passe revient aussi à donner au voleur la clé permettant peut-être d'ouvrir d'autres portes !!!

Besoin de conseils ? de formation ?, contactez 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 : ZATAZ Changez votre mot de passe DropBox – ZATAZ

Peur d’être surveillés ? mettez à jour votre iPhone

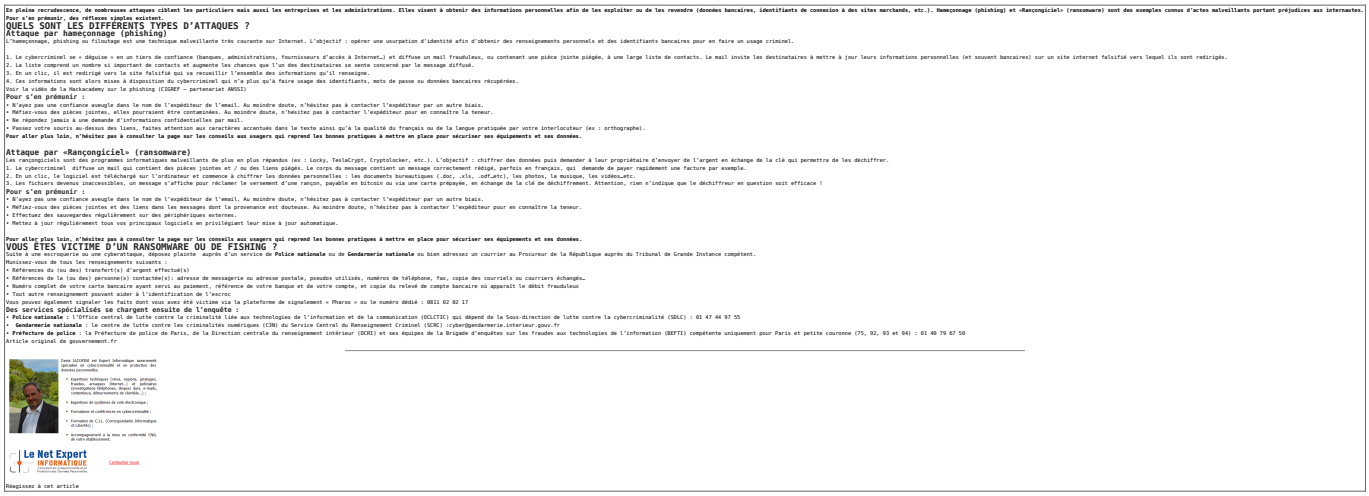
Peur d’être surveillés ? mettez à jour votre iPhone

Original de l’article mis en page : Trois failles zero day d’iOS servaient à espionner des dissidents

---

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 :

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