

Et si Gmail vous protégeait contre les expéditeurs potentiellement malveillants ?

 <p>Denis JACOPINI vous informe LCI</p>	<p>Et si Gmail vous protégeait contre les expéditeurs potentiellement malveillants ?</p>
--	--

Gmail renforce ses outils de filtrage contre les expéditeurs non authentifiés et les liens vers des sites frauduleux ou indésirables.

Google ajoute de nouvelles fonctionnalités à Gmail pour protéger toujours plus ses utilisateurs des dangers du Net. Dans les prochaines semaines, le webmail se verra doté d'un système alertant son utilisateur quand il reçoit un e-mail en provenance d'un expéditeur non authentifié. Un point d'interrogation s'affichera alors en lieu et place de l'image correspondant au profil de l'expéditeur, à côté de son nom (voir l'image ci-dessous), indique le service de mise à jour des applications de l'entreprise de Mountain View.



Une façon d'inviter le destinataire à la plus grande prudence face à un e-mail douteux, surtout si le message contient des pièces jointes. Même si tous les expéditeurs non authentifiés ne sont pas nécessairement des pourvoyeurs de spam ou d'autres contenus à caractères frauduleux. « *Il peut arriver que l'authentification ne fonctionne pas lorsqu'une organisation envoie des messages à de grands groupes d'utilisateurs, via des listes de diffusion, par exemple* », rappelle Google dans l'aide de Gmail.

Pour authentifier les expéditeurs, Google s'appuie sur les protocoles SPF et DKIM. Le premier (Sender Policy Framework) se charge de vérifier le nom de domaine de l'expéditeur d'un courriel. Ce protocole est normalisé dans la RFC 7208 dans l'objectif de réduire les envois de spams. Le second, DomainKeys Identified Mail, permet à l'expéditeur de signer électroniquement son message afin de garantir à la fois l'authenticité du domaine ainsi que l'intégrité du contenu.

Deuxième niveau d'alerte

Au cas où un expéditeur mal intentionné aurait réussi à contourner (ou exploiter) ces normes d'authentification, Gmail s'enrichit d'un deuxième niveau de protection. Lorsque l'utilisateur cliquera sur un lien considéré comme frauduleux (pointant vers un site de phishing, pourvoyeur de malwares, voire de logiciels indésirables), il sera averti par le système des risques qu'il encourt à poursuivre sa navigation. Une fonction héritée du Safe Browsing, un système lancé en 2006 chargé de référencer les sites frauduleux, et qui équipe le navigateur Chrome mais aussi Firefox et Safari (via une API).



Signalons que Safe Browsing est en évolution constante, notamment grâce à la participation des internautes. Le mois dernier, Google a annoncé renforcer cette protection. « *Dans les prochaines semaines, ces améliorations de détection deviendront plus visibles dans Chrome : les utilisateurs verront plus d'avertissements que jamais sur les logiciels indésirables* », indiquait alors l'éditeur.

Article original de Christophe Lagane



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.

Original de l'article mis en page : Gmail va pointer les expéditeurs potentiellement malveillants

Découvrez à quoi ressemble une plateforme de cyberespionnage avancée

 **Découvrez à quoi ressemble une plateforme de cyberespionnage avancée**

Kaspersky détaille le fonctionnement d'une plateforme avancée de cyberespionnage, baptisée Projet Sauron. Un outil remarquablement sophistiqué et probablement aux mains d'un Etat.

Kaspersky détaille le fonctionnement d'une plateforme avancée de cyberespionnage, baptisée Projet Sauron. Un outil remarquablement sophistiqué et probablement aux mains d'un Etat.

Symantec et Kaspersky mettent au jour ce qu'ils présentent comme un nouvel acteur du cyberespionnage, probablement soutenu par un Etat étant donné le niveau de sophistication atteint et les investissements requis (plusieurs millions de dollars, selon les chercheurs de l'éditeur russe). Kaspersky explique que la découverte de ce qu'il a baptisé le Projet Sauron, un nom que les assaillants emploient dans leurs fichiers de configuration, remonte à septembre 2015, suite à la détection de trafic réseau anormal au sein d'une organisation gouvernementale, via un de ses produits. Selon le Russe, la menace, qui cible les environnements Windows, est active depuis au moins juin 2011. Symantec, de son côté, a baptisé la nouvelle menace du nom de Strider. Chez l'éditeur américain également, la détection provient d'anomalies remontées par un de ses produits, travaillant par analyse comportementale.



Suite à leur première découverte, les équipes de Kaspersky racontent avoir isolé un étrange exécutable chargé en mémoire sur le serveur du contrôleur de domaine d'une organisation infectée. Une librairie enregistrée comme un filtre de mots de passe Windows, fonction utilisée par les administrateurs pour obliger les utilisateurs à respecter les règles de sécurité ; et surtout un module ayant accès à des informations sensibles, comme les mots de passe desdits administrateurs. « *La backdoor passive de Projet Sauron démarre chaque fois qu'un domaine, un utilisateur local ou un administrateur se connecte ou change son mot de passe, et elle récupère alors rapidement les mots de passe en clair* », écrit Kaspersky.

Cibler les communications chiffrées

Au fil de son enquête, l'éditeur russe a pu mieux cerner les contours de cette menace jusqu'alors inconnue. Pour le spécialiste de la sécurité informatique, Projet Sauron masque une organisation à la pointe en matière de cyber-espionnage, une organisation à la tête d'une plate-forme modulaire de piratage, « *conçue pour orchestrer des campagnes de long terme via des mécanismes de persistance furtifs couplés à de multiples méthodes d'exfiltration d'information* ». Certaines d'entre elles étant peu communes. La plate-forme recourt notamment au protocole DNS pour exfiltrer des données. Tous les modules ou protocoles réseau de Sauron emploient par ailleurs des algorithmes de cryptage forts, comme RC4, RC5, RC6 ou AES.

D'autres éléments témoignent de la sophistication de cette menace et de son intérêt pour des informations hautement confidentielles. Comme l'utilisation de codes fonctionnant uniquement en mémoire, ce qui rend leur détection plus complexe. Une technique déjà exploitée par Duqu, une menace déjà mise au jour par Kaspersky et à l'œuvre... sur ses propres systèmes ! Le Russe explique encore que Projet Sauron s'intéresse tout particulièrement aux logiciels de chiffrement de ses cibles, tentant de dérober des clefs, des fichiers de configuration et les adresses IP des serveurs gérant les clefs. Autre détail révélateur de la volonté de Sauron de pénétrer les organisations les mieux protégées : la capacité, sur des réseaux isolés d'Internet (employés dans les domaines les plus sensibles), à exfiltrer des données sur des supports de stockage USB spécialement reconfigurés pour abriter une zone invisible du système d'exploitation hôte, zone dans laquelle vont être stockées des données à exfiltrer.

Si Kaspersky admet ne pas connaître le vecteur d'infection qu'utilisent les assaillants pour compromettre un premier système, il explique que Sauron détourne les scripts des administrateurs système de sa cible pour déployer ses malwares sur le réseau de sa victime. Des scripts normalement dédiés au déploiement de logiciels légitimes... De quoi faciliter les déplacements latéraux des assaillants une fois un premier système compromis.

Disparition des indicateurs de compromission

Pour Kaspersky, Projet Sauron a par ailleurs appris des erreurs d'autres acteurs similaires (comme Duqu, Flame, Equation ou Regin), évitant par exemple d'utiliser les mêmes artefacts d'une cible à l'autre. « *Ce qui réduit leur valeur comme indicateurs de compromission pour les futures victimes* », relève l'éditeur. Kaspersky estime que plus de 50 types différents de plug-ins peuvent venir se connecter sur la plate-forme de cyber-espionnage de Projet Sauron. « *Presque tous les implants cœur de Projet Sauron sont uniques, possèdent des tailles et des noms de fichiers différents et sont bâties individuellement pour chaque cible* », écrit Kaspersky. Bref, pour l'éditeur, les assaillants ont intégré les méthodes des chercheurs en sécurité, qui traquent des schémas ou comportements identiques d'une cible à l'autre afin d'identifier de nouvelles menaces. « *Sans ces schémas, l'opération sera plus difficile à mettre au jour* », résume la société russe.

Cette dernière dit avoir identifié 30 organisations attaquées. « *Mais nous sommes sûrs qu'il ne s'agit là que du minuscule sommet de l'iceberg.* » Les organisations attaquées sont situées en Russie, en Iran et au Rwanda. Et opèrent dans des secteurs sensibles : gouvernement, recherche scientifique, armée, opérateurs télécoms, finance. S'y ajouteraient des cibles situées dans les pays italophones, selon Kaspersky, qui relève que la plate-forme de Sauron a été configurée pour cibler des organisations utilisant cette langue. De son côté, Symantec explique avoir identifié la menace chez 4 organisations ou individus en Russie, au sein d'une compagnie aérienne chinoise, dans une organisation suédoise et dans les murs d'une ambassade située en Belgique.

Difficile évidemment de déterminer d'où émane l'attaque. Kaspersky estime qu'il s'agit même là d'un problème « *insoluble* », étant donné la capacité des assaillants à multiplier les écrans de fumée afin de brouiller les pistes. L'éditeur russe relève toutefois un détail intéressant : l'emploi de termes renvoyant aux manuels Unix et notamment de 'Cruft' (désignant un élément superflu du logiciel), utilisé par les spécialistes de BSD. Pour Kaspersky, cette bizarrerie pourrait indiquer la présence, dans les équipes du Projet Sauron, de développeurs 'old school' ayant effectué leurs premières armes au sein de ces environnements. A moins qu'il ne s'agisse là que d'un écran de fumée de plus.

Article original de Reynald Fléchoux



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.

Les logiciels indésirables sont 3 fois plus répandus que les malwares



Les logiciels indésirables sont 3 fois plus répandus que les malwares

Google génère 60 millions d'alertes aux logiciels indésirables chaque semaine. Les injecteurs de publicités et autres scarewares se cachent, le plus souvent, dans les offres groupées de logiciels.

Disponible pour Google Chrome, Mozilla Firefox et Apple Safari, la fonction Navigation sécurisée de Google analyse des milliards d'URL. Chaque semaine, elle génère plus de 60 millions d'alertes aux logiciels indésirables, selon Google. C'est trois fois plus que le nombre d'avertissements concernant des programmes malveillants (malwares), tels que les virus, les vers et les chevaux de Troie.

Paiement à l'installation (PPI)

La plupart des alertes aux logiciels non sollicités apparaissent lorsque les utilisateurs téléchargent involontairement un pack de logiciels (*software bundles*) bardé d'applications additionnelles. Ce modèle peut rapporter au diffuseur jusqu'à 1,50 dollar par installation effective (*pay-per-install*, PPI).

Outre la cible (les internautes), de nombreux acteurs sont impliqués : annonceurs, réseaux d'affiliation, développeurs, éditeurs et distributeurs des logiciels. Toutes les offres groupées de logiciels ne cachent pas une tentative d'installation de programmes non sollicités. Mais il suffit d'un acteur peu scrupuleux dans la chaîne de distribution pour inverser la tendance.

Injecteurs de publicités

Une étude menée par des chercheurs de Google, de NYU et de l'ICSI de Berkeley, montre que les réseaux PPI fleurissent (une cinquantaine a été analysée). Quatre des réseaux les plus étendus distribuaient régulièrement des injecteurs de publicités, des détournateurs de navigateur et des roges ou scarewares. Ces derniers sont de faux logiciels de sécurité. Ils prennent la forme de fenêtres d'alerte et prétendent que les fichiers du système utilisé par l'internaute sont infectés..

Par ailleurs, 59 % des offres des réseaux d'affiliation PPI ont été signalées comme étant indésirables par au moins un antivirus. Pour détecter la présence de ces antivirus, les programmes indésirables vont le plus souvent marquer d'une empreinte (*fingerprinting*) la machine de l'utilisateur. Ils ont aussi recours à d'autres techniques pour contourner les mesures de protection.

Autorégulation

« Ces packs de logiciels sont promus à travers de fausses mises à jour, des contenus bidons et du détournement de marques », explique Google dans un billet de blog. « Ces techniques sont ouvertement présentées sur des forums souterrains comme des moyens destinés à tromper les utilisateurs pour qu'ils téléchargent involontairement des logiciels et acceptent les termes d'installation proposés ».

« Ce modèle décentralisé incite les annonceurs à se concentrer uniquement sur la monétisation, et les éditeurs à maximiser la conversion sans tenir compte de l'expérience utilisateur final », regrettent les chercheurs de Google Kurt Thomas et Juan Elices Crespo.

L'industrie travaille à l'encadrement de ces pratiques. C'est l'objectif affiché de la Clean Software Alliance, regroupement d'acteurs de la distribution de logiciels et d'éditeurs d'antivirus. Impliqué, Google détaillera ses plans cette semaine lors du USENIX Security Symposium d'Austin, Texas.

Article original de Ariane Beky



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Logiciels indésirables : 3 fois plus répandus que les malwares

Ransomware : trois cyber criminels sur quatre prêts à négocier la rançon

Denis JACOPINI



vous informe

Trois cyber
criminels sur
quatre prêts à
négocier la
rançon

Les auteurs de ransomware (logiciels rançonneurs) ne sont pas complètement fermés au dialogue.

Ces conclusions se basent sur une récente expérience détaillée dans le rapport F-Secure Evaluating the Customer Journey of Crypto-Ransomware and the Paradox Behind It (« Évaluation de l'expérience utilisateurs des victimes de logiciels rançonneurs, récit d'un paradoxe »). Cette étude a pour but d'évaluer « l'expérience utilisateur » de cinq logiciels rançonneurs actuels, dès lors que s'affiche le message réclamant la rançon. Elle retrace les différentes interactions ayant lieu avec les pirates.

Plusieurs conclusions émergent de ce rapport. Tout d'abord, les interfaces utilisateur de logiciels rançonneurs les plus professionnelles ne sont pas nécessairement celles qui offrent le « suivi » le plus adapté.

Les pirates utilisant ransomware sont souvent disposés à négocier le prix de la rançon. Pour trois des quatre logiciels rançonneurs, ils se sont montrés prêts à négocier : la rançon a été revue à la baisse, de 29% en moyenne. Les dates limites, quant à elles, ne sont pas nécessairement gravées dans le marbre. 100% des groupes contactés ont accordé un report de la date limite. L'un des groupes a déclaré qu'une entreprise avait fait appel à lui pour hacker une autre entreprise.

Le rapport souligne également le paradoxe des logiciels rançonneurs : « *D'un côté, les auteurs sont des criminels sans scrupules, mais de l'autre, ils doivent établir un degré relatif de confiance avec la victime et être prêts à offrir certains niveaux de « services » pour que cette dernière effectue finalement le paiement* ». Les groupes utilisant des ransomware fonctionnent sur le modèle des entreprises : ils possèdent un site internet, une FAQ (Frequently Asked Questions – Foire aux questions), des « essais gratuits » pour le déchiffrement de fichiers et même un chat d'assistance.

« *Nous lisons chaque jour des histoires au sujet de logiciels rançonneurs... Dernièrement, le mot 'épidémie' a été employé pour faire état de l'ampleur des attaques* », explique Sean Sullivan, Security Advisor chez F-Secure. « *Nous avons voulu proposer une approche différente face à ces attaques en masse, et également rappeler aux particuliers et aux entreprises ce qu'il est possible de faire pour se protéger de ce type de menaces. Avant même d'être victime d'une attaque, il faut adopter plusieurs réflexes-clés : la mise à jour des logiciels, l'utilisation d'un bon logiciel de cyber protection, la vigilance face aux e-mails suspects et surtout, des sauvegardes régulières* ».

Article original de [itrmanager](#)



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.

Original de l'article mis en page : Ransomware : trois cyber criminels sur quatre prêts à négocier la rançon

15 millions de comptes Telegram d'Iraniens piratés

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

 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LENETEXPERT .fr	 RGPD CYBER LE NET EXPERT MISES EN CONFORMITE	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
--	--	---	--	---	---



15 millions de comptes Telegram d'Iraniens piratés

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"]

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



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 site Internet des avocats de Mossack Fonseca, encore piraté !



The screenshot shows a PHP configuration page with the following details:

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	<pre>./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-gdjpeg' '--with-gdgif' '--with-gdjpeg' '--with-gdjpeg-dir=/usr'</pre>

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 à 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.

150 Go de données médicales volées seraient dans la nature !



Un pirate (ou un groupe) aurait mis en ligne 150 Go de données médicales d'un réseau de cliniques d'urologie américain, contenant des données précises sur le suivi de patients. Une tendance de plus en plus répandue outre-Atlantique.

Les données médicales semblent prisées des pirates. Un (groupe de) pirate(s), nommé Pravvy Sector, aurait ainsi mis en ligne 150 Go de données médicales d'un réseau de cliniques d'urologie de l'Ohio, rapportait hier Motherboard. Le contenu trouvé concernerait à la fois les cliniques elles-mêmes (avec des données sur ses ressources humaines) et les patients, avec des indications précises sur leur suivi médical, leur traitement ou encore leurs informations d'assurance.

Motherboard a contacté trois patients présents dans le fichier identifié, dont deux ont pu confirmer que les informations publiées étaient exactes pour eux. L'origine des données, qui semblent bien venir du réseau de cliniques lui-même, n'a pas pu être confirmée. Contactée par le site américain, l'organisation n'a pas encore répondu à ses demandes de commentaires.

Bien avant cette publication, Pravvy Sector aurait été en quête de reconnaissance, contactant directement certains médias avec les contenus de « fuites » précédentes. Mais le plus important est la tendance que deviennent les incidents liés aux données médicales. Comme le relève The Verge, 49 intrusions affectant plus de 500 personnes ont été signalées dans le secteur médical, depuis le début de l'année.

En juin, une autre fuite présumée concernait 655 000 enregistrements médicaux, via plusieurs organismes. Si l'ensemble des données n'a pas pu être authentifié, un échantillon l'avait été à l'époque par Motherboard. Contrairement à la publication de Pravvy Sector, les informations étaient cette fois vendues sur un site spécialisé.

Article original de Guénaël Pépin



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.



[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : États-Unis : 150 Go de données médicales seraient dans la nature

Attention à l'application « Rio Olympics 2016 »



**Avec l'approche des jeux Olympiques de Rio, le téléchargement d'applications thématiques va battre son plein. Gare aux applications dangereuses !
Rio Olympics 2016 Keyboard, un clavier publicitaire dangereux !**

La société Lookout Mobile Security vient d'alerter ZATAZ de certains problèmes de confidentialité et des enjeux rencontrés par les utilisateurs et les entreprises avec l'application Rio Olympics 2016 Keyboard. Une APP disponible en version iOS et Android.

L'application officielle de l'entreprise américaine NBC Universal Media, Rio 2016 Olympics Keyboard est en apparence une simple extension de clavier pour les personnes qui suivent les jeux Olympiques. Cependant, il a identifié que cette application était capable de compiler plus d'information qu'initialement prévu par son développeur, exposant ainsi la confidentialité des données des amateurs des JO de RIO et possiblement des entreprises pour lesquelles ils travaillent.

Finalement, l'équipe de recherche a informé NBCUniversal des enjeux de confidentialité identifiés dans les versions Android et iOS de l'application officielle Rio 2016 Keyboard. NBCUniversal a réagi rapidement pour résoudre les problèmes identifiés et s'assurer que les versions disponibles seraient sécurisées avant l'ouverture des Jeux Olympiques d'été de Rio. Si vous avez téléchargé l'application, effacez là. A vous de décider, ensuite, si vous installez la nouvelle version.



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : ZATAZ L'appli Rio Olympics 2016 Keyboard dangereuse – ZATAZ

Les conséquences inattendues des changements trop fréquents de mots de passe

 Les conséquences inattendues
des changements trop
fréquents de mots de passe

Il est préférable d'opter pour des mots de passe robustes, plutôt que d'imposer des changements fréquents, réaffirme la responsable des technologies de la FTC.

Fraîchement nommée chef des technologies de la Federal Trade Commission (FTC), Lorrie Cranor (également professeur à l'université Carnegie Mellon), avait été surprise par un tweet officiel mis en ligne en janvier. Le régulateur américain du commerce préconisait alors un changement fréquent de mots de passe. La spécialiste s'y est opposée. Depuis, elle fait évoluer la politique interne sur le sujet.

« *Je suis allée voir les personnes en charge des médias sociaux et leur ai demandé pourquoi [la FTC dit à tout le monde de changer de mots de passe]* », a commenté Cranor lors de la conférence *Passwords* de BSidesLV 2016, dont Ars Technica s'est fait l'écho. « *Elles m'ont répondu ceci : 'C'est probablement un bon conseil, car à la FTC nous changeons nos mots de passe tous les 60 jours'* ».

Lorrie Cranor s'est alors entretenue avec le #DSI et le RSSI de la FTC. Elle a souligné, rapport d'experts à l'appui, que les changements fréquents n'améliorent pas la sécurité, mais encouragent au contraire l'utilisation de mots de passe plus susceptibles d'être découverts et détournés.

Un modèle, des mots de passe

Lorsque des utilisateurs doivent changer de mots de passe tous les 90 jours, par exemple, ils ont tendance à utiliser un même modèle. C'est ce qui ressort d'une étude publiée en 2010 par des chercheurs de l'université de Caroline du Nord (UNC) à Chapel Hill.

« *Les utilisateurs prennent leurs anciens mots de passe, puis ils les changent légèrement [d'une lettre, d'un chiffre ou d'un symbole] pour obtenir un nouveau mot de passe* », a expliqué Cranor. Or la capacité de ces mots de passe à résister aux attaques par force brute est faible. 17 % des mots de passe testés par les chercheurs de l'UNC auraient ainsi été découverts en moins de cinq tentatives.

Il est donc préférable, selon eux, d'utiliser des mots de passe forts, plutôt que d'en changer souvent. La double authentification est également recommandée, notamment pour les applications sensibles.

Article original de Ariane Béky



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.

de mots de passe nuisent à la sécurité