Et si Gmail vous protégeait contre les expéditeurs potentiellement malveillants ?

Et si Gmail vous protégeait contre les expéditeurs potentiellement malveillants ?

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 malintentionné 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

Réagissez à cet article

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

---

Découvez à quoi ressemble une plateforme de cyberespionnage avancée

Découvez 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 État 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 bâtis 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 Fléchaux

Réagissez à cet article

Original de l’article mis en page : Projet Sauron : anatomie d’une plateforme de cyberespionnage avancée

---

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 détourneurs de navigateur et des rogues 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

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

	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.

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 : 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

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

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

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

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

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

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

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

Les meilleurs conseils pour choisir vos mots de passe

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

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

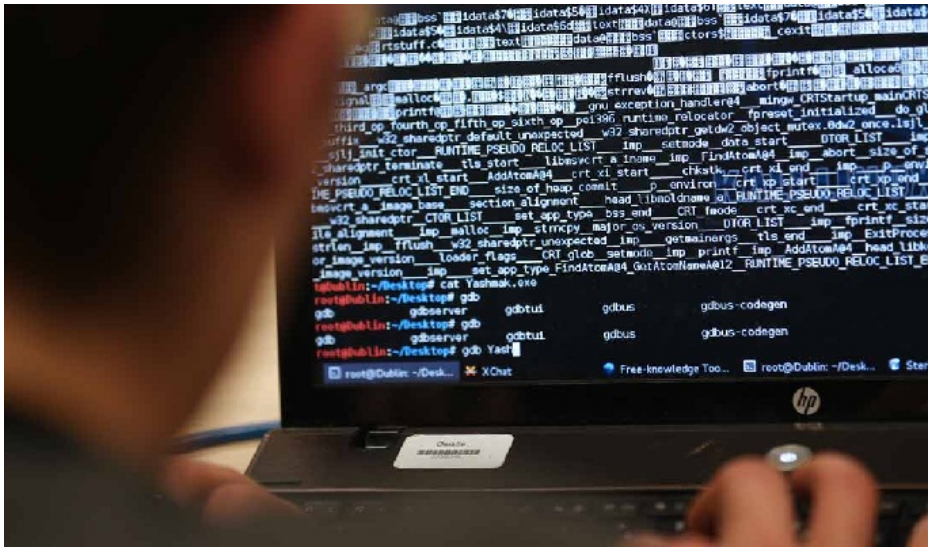
Attaques informatiques : comment les repérer ?

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

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

Telegram : 15 millions d’Iraniens concernés – ZATAZ

Cyberattaques terroristes déjouées au Maroc



Cyberattaques terroristes déjouées au Maroc

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

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

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

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

Article original de Alselme AKEKO

Réagissez à cet article

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

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

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

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

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

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

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

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

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

Article original de Damien Bancal

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

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

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

Contactez-nous

Réagissez à cet article

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

---

150 Go de données médicales volées seraient dans la nature !

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 enregistements 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

Réagissez à cet article

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

Attention, Cheval de troie dans une Application sur Google Play découverte par Eset

Attention, Cheval de troie dans une Application sur Google Play découverte par Eset

Avant même la sortie sous Android de Prisma, une application populaire de retouche photos, Google Play Store s'était retrouvé inondé de fausses applications.

Les chercheurs d'ESET ont découvert de fausses applications imitant Prisma, dont plusieurs Chevaux de Troie dangereux. Dès l'avertissement d'ESET, le service sécurité de Google Play a retiré toutes les fausses applications du store officiel d'Android. Ces dernières auront tout de même atteint plus d'1,5 millions de téléchargements.
Prisma est un éditeur de photos unique publié par les laboratoires de Prisma. D'abord développé pour iOS, cette application a remporté d'excellents résultats de la part des utilisateurs d'iTunes et de l'App Store d'Apple. Les utilisateurs d'Android étaient à leurs tours impatients de la découvrir sur le Google Play (disponible depuis le 24 juillet 2016).
« La plupart des fausses applications de Prisma disponibles sur Google Play ne disposent pas d'une fonction retouche photo. A l'inverse, elles affichent uniquement des annonces, avertissements ou de faux sondages pour tromper l'utilisateur qui fournit des informations personnelles le concernant ; ou encore pour le faire souscrire à de faux services type SMS onéreux », commente Lukáš Štefanko, Malware Researcher chez ESET.
La plus dangereuse des fausses applications imitant Prisma et trouvée dans le Google Play est un Cheval de Troie téléchargeur détecté par ESET comme Android/TrojanDownloader.Agent.GY. Des informations sur les périphériques sont envoyées au serveur C&C, ce qui lui permet de télécharger sur demande des modules supplémentaires et de les exécuter afin de voler des données sensibles telles que le numéro de téléphone, l'opérateur, le pays, la langue etc.
A cause de ses capacités de téléchargement, la famille des malwares type Android/TrojanDownloader.-Agent.GY pose de sérieux risques pour les plus de 10.000 utilisateurs Android qui ont installé cette application dangereuse avant d'être retiré du Google Play Store.

Pour se protéger, Denis JACOPINI recommande l'application suivante :

Article original de Eset

Réagissez à cet article

Les cyberattaques sont de plus en plus furtives

Les cyberattaques sont de plus en plus furtives

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

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

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

Evolution de la menace

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

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

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

Reprendre le contrôle

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

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

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

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

Article original de iTPro.fr

Réagissez à cet article

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