Votre vie privée numérique en danger sur Leakedsource

Votre vie privée numérique en danger sur Leakedsource

Depuis quelques semaines, le site leakedsource engrange des centaines de millions de données volées par des pirates informatiques. Un business juteux qui met en danger des millions d'internautes.

LeakedSource, nouvelle source d'informations pour pirates informatiques ? Souvenez-vous, on vous parlait en juillet, de données volées appartenant à un ancien garde du corps de Vladimir Poutine, le Président Russe, ou encore de Nicolas Sarkozy, ancien Président de la République Française. Son identité, ses données privées, des courriels… Un piratage qui semblait être particulièrement compliqué à orchestrer tant les sources d'informations concernant ce body guard étaient variés. Après enquête, j'ai découvert que si le résultat pouvait être particulièrement préjudiciable pour la cible, la mise en place et l'exécution de cette attaque était aussi simple que « *1 + 1 font 2*« .

Leakedsource, source quasi inépuisable de malveillances

Pour ce garde du corps, mais aussi pour de nombreuses personnalités, le risque est énorme. Tout débute par le piratage de centaines de bases de données de part le monde. Myspace, Adobe, Linkedin, Twitch , Xat , Badoo… ne sont que des exemples parmi d'autres. Je gère, avec le protocole d'alerte ZATAZ, des dizaines de fuites de données par mois concernant des PME et entreprises Françaises. Imaginez donc ce que brassent des sites comme leaked source.

Leakedsource.com, un espace web tenu par des Russes, a pour mission de regrouper les informations volées par des pirates et de permettre de consulter les informations en question. Les administrateurs du portail expliquent que leur service est fait pour s'assurer que les données volées ne vous concernent pas. Sauf que, des données, il y en a des centaines de millions, et vous pourriez bien vous y retrouver, comme Mark Zuckerberg, cofondateur et directeur général de Facebook, piraté en juin 2016 parce que son mot de passe « *DaDaDa* » était accessible dans une base de données piratées et stockées chez Leakedsource.

Vous ne risquez rien ? Vraiment ?

Cela n'arrive qu'aux autres ? Allez donc regarder du côté de vos données. C'est d'ailleurs ce qu'aurait dû faire l'auteur des jeux vidéo Garrysmod et de Rust, Garry Newman. J'ai pu avoir une longue conversation avec l'auteur de divertissements vidéo ludique qui ne s'attendaient pas à découvrir sa vie numérique mise en pâture de la sorte. Il faut dire aussi que plusieurs pirates ont contacté la rédaction de ZATAZ.COM pour se vanter d'avoir mis la main sur ses données Paypal, Amazon, gMail de ce créateur de jeux vidéo britannique. Bref, pour 4 dollars (le prix journalier d'un abonnement Leaked source pour accéder aux données) n'importe quel internaute peut se transformer en vulgaire violeur de vie 2.0. Il suffit de rentrer un mail, un pseudonyme ou encore une adresse IP et Leakedsource cherche dans ses bases de données la moindre concordance. Cerise sur le gâteau, quand le mot de passe est hashé, donc illisible à la première lecture, Leaked source propose la version du précieux sésame déchiffré. « ***Si les personnes [les pirates, NDR) sont malines, elles peuvent faire beaucoup de dégâts avec ce genre d'outil accessible à Monsieur tout le monde*** » me confirme un utilisateur.

Que faire pour éviter ce type de fuite de données ?

Je vais très rapidement être honnête avec vous, si vous mettez vos données en ligne, dites vous qu'elles ne sont plus en sécurité. Et ce n'est pas notre vénérable CNIL qui pourra vous aider. Avec plusieurs centaines de cas de fuite de données que je traite avec le protocole d'alerte de zataz par an, j'ai déjà pu croiser mes propres informations. Je vous parlais plus haut de Leakedsource, j'ai pu y retrouver mon compte Adobe. Pourtant, le géant du logiciel l'avait juré, il était « *secure* » [sécurisé, ndr].

Tellement « *secure* » qu'un de mes mails, et le mot de passe attenant, sont disponible dans ce big data du malveillant. Autant dire que l'adresse mail et le mot de passe en question ont été détruits et ne seront plus utilisés.

Que faire donc ? D'abord, un compte mail par service. Je sais, c'est long est fastidieux. Mais je pense qu'il va être beaucoup plus long et fastidieux pour Garry Newman de revalider l'ensemble de ses comptes « infiltrés », car il utilisait la même adresse électronique pour ses accès Paypal, Amazon…

Ensuite, ne mettez pas le même mot de passe pour l'ensemble de vos services en ligne. On a beau le répéter, cesser de vous croire plus malin que les 010101 qui nous régissent. Mark Zuckerberg et son « *DaDaDa* » lui ont coûté son Twitter et son Pinterest. Pour Garry, plus grave encore, son compte Amazon et Paypal, avec des données sensibles [adresses postales, données bancaires…] qui ne devraient pas être disponibles à la planètes web. Donc, oui, c'est fastidieux, mais un mot de passe par compte est une obligation.

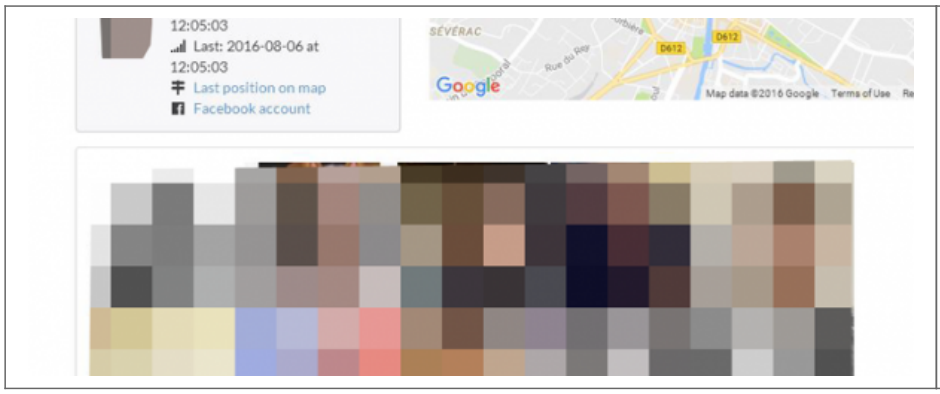
Pour finir, en ce qui concerne l'IP, n'hésitez plus à utiliser un VPN. L'outil permet de cacher votre véritable adresse de connexion, en plus de chiffrer vos informations transitant sur la toile. Je vous invite à regarder du côté de nos partenaires et amis de chez **NoLimitVPN** ou encore HMA! pour blinder vos connexions PC, Mac et mobiles.

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : ZATAZ Leakedsource, le site qui met en danger votre vie privée – ZATAZ

Géolocaliser un téléphone mobile en deux clics de souris



Géolocaliser un téléphone mobile en deux clics de souris

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

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

Géolocaliser un téléphone : Souriez, vous êtes pistés

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

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

Comment cela fonctionne-t-il ?

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

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

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

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

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

Réagissez à cet article

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

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.

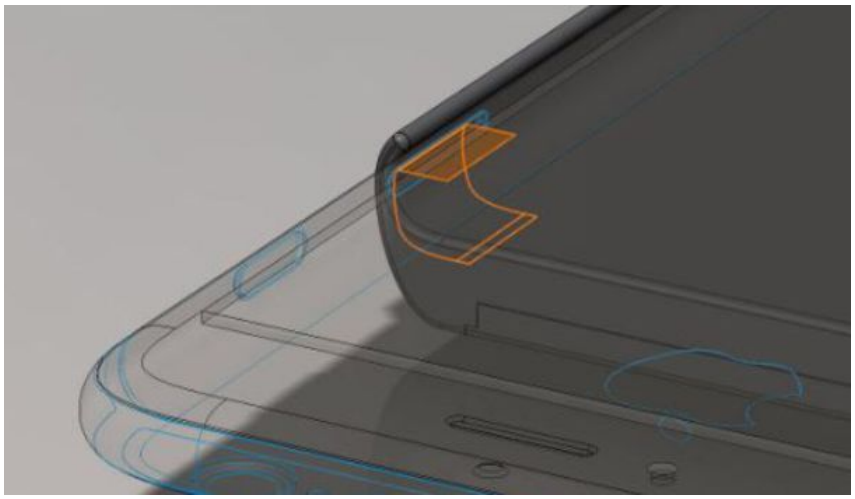
Article original de Reynald Fléchaux

Réagissez à cet article

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

---

Snowden conçoit une coque d’iPhone anti-espionnage – L’Express L’Expansion



Snowden conçoit une coque d’iPhone anti-espionnage

Cette coque a pour objectif de protéger les données de nos smartphones. Un premier prototype sera rendu public d'ici un an.

Edward Snowden continue son combat contre la surveillance. L'ancien analyste de la NSA et lanceur d'alerte, qui a levé le voile sur les pratiques d'écoute massive à travers le monde, travaille à la réalisation d'une nouvelle coque d'iPhone. Son atout: elle est capable de protéger les données du téléphone qu'elle abrite.

Pour ce projet, Edward Snowden s'est associé au hacker Andrew « Bunnie » Huang. Dans un rapport, les deux hommes précisent que le mode avion est loin d'être efficace contre le piratage. « Croire au mode avion d'un téléphone hacké équivaut à laisser une personne ivre juger de sa capacité à conduire », indiquent-ils.

Contrôler les signaux envoyés à l'iPhone

Le système, encore au stade d'étude, a été présenté à l'occasion d'une conférence le 21 juillet. L'objet est un périphérique sous logiciel libre qui se pose à l'emplacement de la carte SIM. Il permet ensuite de contrôler les signaux électriques envoyés aux antennes internes du téléphone et donc de savoir si le téléphone partage des informations avec des tiers, sans que vous en soyez conscients.

Une alerte est envoyée dès lors qu'une transmission anormale est détectée.
Mashable explique que « lorsque le mode avion est activé et que les connexions réseaux sont supposées être désactivées, une alerte est envoyée dès lors qu'une transmission anormale est détectée ». L'anomalie repérée, le périphérique peut même éteindre le téléphone immédiatement.

Journaliste, activiste et lanceur d'alerte

L'outil, dont le premier prototype devrait être rendu public d'ici un an, a été pensé pour venir en aide aux journalistes, activistes et lanceurs d'alerte « pour détecter quand leurs smartphones sont surveillés et trahissent leurs localisations ».

Le programme d'espionnage américain de la NSA, révélé par Edward Snowden a, permis la collecte de données personnelles de millions de citoyens, ainsi que des institutions et chefs d'Etats étrangers. Ces révélations ont montré que ces collectes dépassaient le cadre de la lutte nécessaire contre le terrorisme ou contre les autres risques géopolitiques.

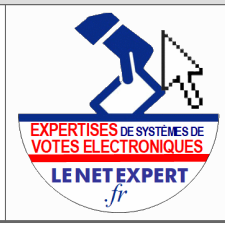
Article original de l'express

Réagissez à cet article

Original de l’article mis en page : Snowden conçoit une coque d’iPhone anti-espionnage – L’Express L’Expansion

---

15 millions de comptes Telegram d’Iraniens piratés



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"]

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

Telegram : 15 millions d’Iraniens concernés – ZATAZ

Ma vie disséquée à travers mes données personnelles

	Ma vie disséquée à travers mes données personnelles

---

Original de l’article mis en page : Ma vie disséquée à travers mes données personnelles

---

L’ANSSI alerte sur les risques liés à Pokémon Go

L’ANSSI alerte sur les risques liés à Pokémon Go

Face au phénomène Pokémon Go, l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'information) a publié un bulletin de sécurité sur l'installation et l'usage de cette application.

Devant l'ampleur du phénomène (près de 100 millions de téléchargements), l'application Pokémon Go pose quelques problèmes de sécurité. L'ANSSI (en quelque sorte le Gardien de la sécurité des Systèmes d'Information des Organisme d'Importance Vitale, des Organes et Entreprise de l'état Français selon Denis JACOPINI expert Informatique assermenté spécialisé en cybercriminalité) ne pouvait pas rester sourde à cette question et vient de publier via le CERT-FR un bulletin de sécurité dédié aux « *cyber-risques liés à l'installation et l'usage de l'application Pokémon Go* ».

Applications malveillantes et collectes de données

Dans ce bulletin, il est rappelé qu'avec le succès, de nombreuses fausses applications se sont créées. Le CERT-FR en a recensé 215 au 15 juillet 2016. Elles sont surtout présentes dans les pays où le jeu n'est pas présent. Il recommande donc de ne pas télécharger cette application sur des sites tiers, et de n'installer que les versions originales disponibles sur Google Play ou l'Apple Store. Nous nous étions fait l'écho de la disponibilité d'APK Pokémon Go pour Android qui contenait des malwares. Le bulletin constate aussi que Niantic a résolu le problème de permission qui exigeait un accès complet au profil Google de l'utilisateur.

Sur les données personnelles, l'ANSSI observe comme beaucoup d'autres organisations que Pokémon Go collecte en permanence de nombreuses données personnelles. Informations d'identité liées à un compte Google, position du joueur par GPS, etc. L'UFC-Que Choisir avait récemment alerté sur cette question de la collecte des données. La semaine dernière la CNIL a publié un document concernant « jeux sur votre smartphone, quand c'est gratuit… » où elle constatait que ce type d'application était très gourmande en données. L'ANSSI préconise la désactivation du mode « réalité augmentée » lors de la phase de capture d'un Pokémon.

BYOD et Pokémon Go, le pouvoir de dire non

L'ANSSI répond sur le lien qu'il peut y avoir entre le BYOD (Bring Your Own Device), c'est-à-dire l'utilisation de son terminal personnel dans un cadre professionnel et Pokémon Go. Le CERT-FR constate qu'il est « *tentant d'utiliser un ordiphone professionnel pour augmenter les chances de capturer un Ronflex (un Pokémon rare à trouver)* ». Surtout quand la demande émane d'un VIP et qu'il est souvent difficile de refuser. Eh bien comme Patrick Pailloux (prédécesseur de Guillaume Poupard à la tête de l'ANSSI) l'avait dit en son temps, il faut avoir le pouvoir de dire non à l'installation de ce type d'application dans un environnement professionnel.

Toujours dans le cadre du travail, l'agence déconseille l'usage de l'application dans des lieux où le geo-tagging du joueur pourrait avoir des conséquences (lieu de travail, sites sensibles).

Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : L’ANSSI alerte sur les risques liés à Pokémon Go

---

L’application Telegram a aussi sa faille

L’application Telegram a aussi sa faille

Un chercheur a trouvé une faille de sécurité sur la version Mac de Telegram. L'éditeur minimise l'importance de cette vulnérabilité.

Une grave affaire prise à la légère ou, au contraire, beaucoup de bruit pour rien ? Les avis sont partagés à propos de la faille de sécurité découverte sur **Telegram** par le dénommé Kirill Firsov.
Ce chercheur russe s'est aperçu que la version Mac du service sécurisé de messagerie enregistrait, dans les journaux système (*syslog*), chaque message collé dans le champ de discussion depuis le presse-papiers. Le 23 juillet, il avait, sur Twitter, interpellé Pavel Durov, cofondateur du service avec son frère Nikolai.
S'est ensuivi un échange de tweets à l'issue duquel le bug a été résolu… sans qu'on puisse mesurer quelle était sa réelle ampleur. L'explication entre les deux hommes s'est effectivement terminée sur un « Imagine que la police saisisse ton ordinateur portable et qu'elle retrouve trace de tes messages 'secrets' dans syslog » lancé par Kirill Firsov.

La sandbox pour limiter les dégâts

Pour Pavel Durov, la vulnérabilité, repérée sur les versions 2.16 et 2.17 de Telegram, n'est pas aussi importante qu'elle en a l'air : n'est concerné que le texte collé depuis le presse-papiers… auquel toutes les autres applications Mac ont accès.
Sans nier cet état de fait, Kirill Firsov avait pointé du doigt le fait que les messages font l'objet d'une journalisation. Ce à quoi Pavel Durov avait répondu qu'avec le mécanisme dit de « bac à sable » (*sandbox*), les applications téléchargées sur l'App Store d'OS X – à l'image de Telegram – ne peuvent qu'écrire dans *syslog* ; pas y accéder en lecture (voir, à ce propos, la documentation d'Apple).
Bilan pour celui qui a financé Telegram via son fonds Digital Fortress, corriger la faille revient juste à éliminer une redondance : le fait que toutes les applications peuvent accéder au contenu du presse-papiers.

Le service qui monte

L'histoire de Telegram est particulière. Ses fondateurs s'étaient installés à Berlin après avoir, sur fond de lutte d'influence politique avec l'entourage de Vladimir Poutine, perdu le contrôle du réseau social vKontakte, qu'ils avaient créé en Russie.
Utilisé à l'origine par les seules équipes de vKontakte, Telegram avait basculé, en 2013, dans une exploitation ouverte au grand public.
En insistant sur la dimension de confidentialité des échanges, le service a dépassé, fin février, les 100 millions d'utilisateurs actifs par mois, souligne ITespresso.
Une ascension qui n'a pas laissé la concurrence indifférente. Illustration chez WhatsApp, qui avait décidé, fin 2015, de bloquer, sur Android, les liens vers l'application Telegram diffusés par ses utilisateurs.
Le service, qui exploite un protocole de chiffrement maison (MTProto), a aussi été mis en lumière pour des considérations plus sombres : selon Trend Micro, 34 % des organisations terroristes l'utilisent comme point de contact.
Article original de Silicon

Réagissez à cet article

Original de l’article mis en page : Sécurité : Telegram, une vulnérabilité qui prête à discussion

---

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.

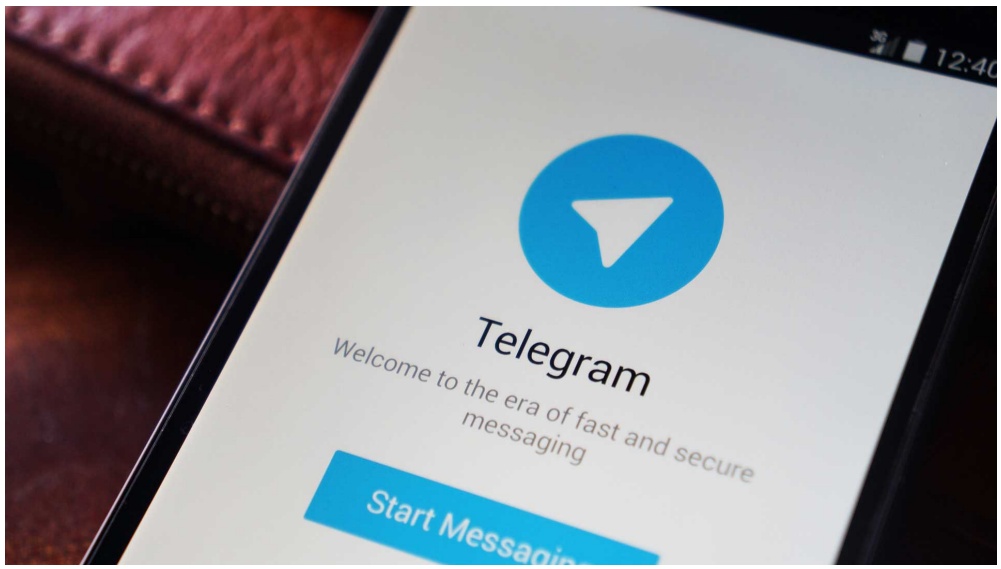
Article original de iTPro.fr

Réagissez à cet article

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

---

Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ? – Politique – Numerama



Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ?

Selon La Voix du Nord, au moins l'un des deux auteurs de l'attentat de l'église de Saint-Étienne-du-Rouvray utilisait régulièrement la messagerie chiffrée Telegram pour communiquer avec des islamistes, et aurait posté un message une heure avant l'attentat.

Il faut s'attendre à voir très vite renaître le débat sur le chiffrement et l'obligation qui pourrait être faite aux fournisseurs de messageries électroniques de laisser les services de Renseignement accéder aux communications. La Voix du Nord affirme qu'Adel Kermiche, l'un des deux coauteurs de la tuerie de l'église de Saint-Étienne-du-Rouvray, près de Rouen, utilisait la messagerie chiffrée Telegram, à des fins djihadistes. Il aurait envoyé un message sur un canal de discussion une heure avant l'attaque.
« Selon nos informations, Adel Kermiche avait ouvert sur Telegram une « private channel » (haqq-wad-dalil), une chaîne lui permettant de s'adresser à une audience ultra-sélectionnée. Il avait choisi pour nom de code Abu Jayyed al-Hanafi et la photo de Abou Bakr al-Baghdadi, chef suprême de l'État islamique, comme représentation », écrit le quotidien régional.

TÉLÉCHARGER (SIC) CE QUI VA VENIR ET PARTAGER LE EN MASSE ! ! ! !
Selon les membres arabophones de la rédaction de Numerama, haqq-wad-dalil signifierait quelque chose comme « preuve de la vérité » ou « guide de la vérité ».
La Voix du Nord ajoute que « le terroriste correspondait depuis des mois via ce canal avec près de 200 personnes, dont une dizaine de Nordistes », qui étaient d'abord approchés par Facebook. Le matin de l'attentat, le 26 juillet 2016 à 8h30, il aurait envoyé sur ce salon un message qui disait : « Télécharger (sic) ce qui va venir et partager le en masse ! ! ! ! ».
Le quotidien ne dit rien d'un éventuel document qui aurait pu être mis en partage par la suite, ce qui ne laisse la voie qu'à des spéculations. Peut-être Kermiche avait-il prévu de filmer son acte odieux, ou des revendications, et espérait trouver des relais à sa diffusion à travers ses contacts sur Telegram.
Si cette information se confirme ce serait, à notre connaissance, la première fois qu'un lien direct est effectué entre un attentat terroriste en France et l'utilisation de messageries chiffrées.

COMMENT SURVEILLER TELEGRAM ?
La Voix du Nord ne dit pas par quel biais le message aurait été découvert. Il est possible que les enquêteurs aient trouvé ce message en accédant à l'historique Telegram du terroriste, depuis son téléphone mobile qui n'aurait pas été bloqué. Le plus probable est toutefois que l'information provienne d'un autre utilisateur du salon haqq-wad-dalil, puisque le quotidien cite le témoignage de l'un d'entre eux, qui explique que les échanges pouvaient y être « écrits ou oraux mais toujours détruits rapidement ».
Il est connu depuis de très nombreux mois que Telegram, qui dispose de plus de 100 millions d'utilisateurs à travers le monde, est aussi utilisé par des djihadistes qui recherchent la sécurité d'une messagerie chiffrée.
Après avoir refusé d'opérer la moindre censure, en tout en continuant à livrer la moindre information personnelle sur ses utilisateurs, Pavel Durov a fini par décider en novembre 2015 de fermer des salons de discussion liés à l'État islamique, pour mettre fin aux accusations de complicité passive. Il avait appelé les internautes à les signaler pour permettre leur fermeture.
Théoriquement, les canaux de discussion peuvent être infiltrés par les agents des services de renseignement. Reste qu'en l'absence de communication d'informations sur les utilisateurs, il peut être difficile de remonter jusqu'à l'auteur d'un message présentant une menace particulièrement élevée.
Article original de Guillaume Champeau

Original de l'article mis en page : Attentat dans une église : la messagerie chiffrée Telegram utilisée par un terroriste ? — Politique — Numerama