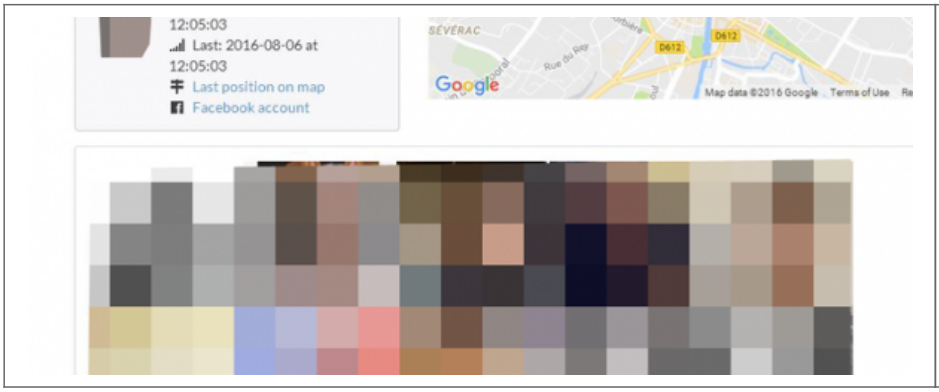
Géolocaliser un téléphone mobile en deux clics de souris



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

Découvrez la faille qui ouvre toutes les Volkswagen sans clef

Découvrez la faille qui ouvre toutes les Volkswagen sans clef

---

Tous les véhicules vendus par Volkswagen depuis environ 20 ans peuvent être ouverts sans clef. Et la technique mise au point par des chercheurs de l'université de Birmingham fonctionne aussi avec d'autres constructeurs.

Nul doute que Volkswagen aurait préféré ne pas revoir de sitôt Flavio D. Garcia. Travaillant à l'université de Birmingham, cet ingénieur en informatique présente, lors de la conférence Usenix qui se tient du 10 au 12 août à Austin (Texas), les conclusions d'une étude (« Lock it and still lose it ») sur les télécommandes permettant l'ouverture des voitures de tourisme.

Des conclusions peu flatteuses pour le groupe automobile allemand : la quasi-totalité des véhicules qu'il a vendus ces 20 dernières années, près de 100 millions pour la seule période allant de 2002 à 2015, peuvent être déverrouillés sans clés… et sans plip, du nom de cette fameuse télécommande aujourd'hui livrée en standard avec la plupart des voitures de tourisme.

Flavio D. Garcia étudie depuis plusieurs années les vulnérabilités associées aux systèmes de commande à distance dans l'univers automobile. En 2012, il avait constaté, avec plusieurs collègues, que les récepteurs RFID Magamos Crypto, adoptés par de nombreuses marques de luxe, pouvaient être détournés non seulement pour ouvrir et fermer les portes, mais aussi pour faire démarrer le moteur, le tout sans disposer des clés.

Contacté par ses soins en mai 2013, Volkswagen avait déposé plainte, arguant qu'une publication de ces recherches exposerait ses véhicules à un risque accru de vol. La Haute Cour du Royaume-Uni lui avait accordé une injonction, retardant d'autant la publication, finalement effectuée il y un an et sous une forme très restreinte : une seule phrase, dans les annexes de la conférence Usenix, comme le souligne *Bloomberg*.

Arduino pour intercepter les données

Cette fois-ci, Flavio D. Garcia s'est épargné les considérations juridiques. Avec deux associés de l'université de Birmingham et la firme allemande Kasper & Oswald, il aborde deux vulnérabilités distinctes ; l'une concernant Volkswagen et l'autre applicable à une longue liste de constructeurs.

Point commun entre ces failles : elles sont fondées sur l'interception des données transmises par les télécommandes, qui fonctionnent sur les bandes de fréquence à 433 ou 868 MHz en Europe et 315 MHz en Amérique du Nord – à l'exception de quelques anciens systèmes basés sur la technologie infrarouge.

Le module d'interception, sur base Arduino.

Pour intercepter les données envoyées par les télécommandes, les chercheurs ont fabriqué un module radio à partir d'une carte Arduino. Et se sont aperçus que, de manière générale, le niveau de protection des données dépendait de l'âge des véhicules. Sur des modèles du début des années 2000, il arrive qu'aucune méthode de cryptographie ne soit appliquée : un code unique est envoyé à chaque appui sur le(s) bouton(s) d'ouverture et de fermeture des portes. Sur des voitures plus récentes, des paramètres ont été ajoutés. Notamment un compteur incrémenté à chaque pression, permettant d'éviter qu'une commande soit exécutée deux fois.

Clonage des clefs

Mais, dans tous les cas, il est possible de déterminer la structure des paquets de données, d'autant plus que ceux-ci sont souvent transmis à plusieurs reprises, sans doute pour s'assurer que la communication aboutisse dans les environnements difficiles sujets à des interférences.

Une télécommande Volkswagen de nouvelle génération.

L'équipe de Flavio D. Garcia a identifié pas moins de 7 schémas de transmission. Parfois, le signal varie en amplitude ; d'autres fois, en fréquence. La quantité de données change elle aussi, au même titre que les algorithmes de chiffrement. Mais dans tous les cas, la sécurité peut être déjouée et la clé, clonée.

Cette opération de clonage ne peut toutefois se faire qu'une fois obtenue la clé logée dans le récepteur RFID de la voiture. Pour cela, les chercheurs en ont extrait le *firmware*. Et ont alors fait une sacrée découverte : cette « clé maîtresse » est la même sur des dizaines de millions de véhicules du groupe Volkswagen.

Mais aussi Nissan, Dacia, et Renault…

Sur la liste – non exhaustive – des modèles considérés comme vulnérables figurent les Audi A1, Q3, R8, S3 et TT, les Skoda City Go, Roomster, Fabia 1 et 2, Octavia, SuperB et Yeti, les Seat Alhambra, Altea, Arosa, Cordoba, Ibiza, Leon, MII et Toledo… ainsi que les Volkswagen Amarok, (New) Beetle, Bora, Caddy, Crafter, e-Up, Eos, Fox, Golf 4, 5 et 6, Golf Plus, Jetta, Lupo, Passat, Polo, T4, T5, Scirocco, Sharan, Tiguan, Touran et Up.

Dans le prolongement de ces conclusions, Flavio D. Garcia et consorts se sont intéressés aux circuits intégrés PCF7946 et PCF7947, que le fabricant de semi-conducteurs NXP fournit à de nombreux constructeurs automobiles, détaillent nos confrères de *ITespresso*.

Avec le même mode opératoire, ils sont ainsi parvenus à pirater une Fiat Punto, un Citroën Jumper, un Dacia Duster, une Renault Modus ou encore un Nissan Qashqai. Il leur a toutefois fallu ici pousser l'expérimentation plus loin, en interceptant plusieurs codes (4 à 8, d'après le rapport, car ces codes changent à chaque pression sur la télécommande) et en utilisant un ordinateur pour déchiffrer certaines données. En l'occurrence, une partie des 28 bits du compteur.

Une étape indispensable : sur un grand nombre de véhicules, la télécommande se bloque si ledit compteur, censé augmenter d'une unité à chaque appui, n'est pas synchronisé avec celui du récepteur RFID.

Des vols bien réels

Le déchiffrement prend moins de 10 minutes en exploitant les failles de HiTag2, un algorithme de cryptographie lancé il y a près de 20 ans et associé aux circuits intégrés PCF7946/7947. Pour intercepter plus rapidement le nombre de codes requis, les chercheurs ont bloqué la transmission des signaux afin que les utilisateurs ciblés pressent à nouveau le bouton de leur télécommande.

La principale limitation de la méthode imaginée par les chercheurs réside dans la portée des télécommandes. Généralement quelques dizaines de mètres. Il faut donc impérativement se trouver dans ce périmètre. Dès lors, il est possible d'envisager d'autres scénarios d'attaque. Par exemple, une sorte de DDoS à partir du système de blocage de la télécommande.

Ces recherches permettent de mettre le doigt sur un phénomène en pleine explosion : aux États-Unis, les forces de l'ordre constatent de plus en plus de vols de voitures sans effraction. Les images de vidéosurveillance révèlent souvent l'utilisation d'un simple boîtier électronique. Ce mois-ci, une trentaine de Jeep ont ainsi été volées dans le Texas avec un simple ordinateur.

Article original de Silicon

Original de l'article mis en page : Sécurité : toutes les Volkswagen peuvent être ouvertes sans clef

---

« AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d'Ivoire à l'honneur au Maroc, du 21 au 24 septembre 2016

« AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d'Ivoire à l'honneur au Maroc, du 21 au 24 septembre 2016

Le Sénégal et la Côte d'Ivoire, qui compte parmi les pays d'Afrique subsaharienne à avoir engagé des projets de gouvernance électronique, seront à l'honneur au Maroc lors de la première édition du Salon de l'innovation et de la transformation digitale en Afrique, « AITEX – AFRICA IT EXPO », qui aura lieu du 21 au 24 septembre 2016 à Casablanca.

Dans un communiqué transmis à notre Rédaction, la **Fédération marocaine des technologies de l'information, des télécommunications et de l'Offshoring (APEBI),** chef d'orchestre de l'AFRICA IT EXPO, explique le choix du Sénégal et de la Côte d'Ivoire par le souci d'établir une connexion sud-sud des ressources du continent. Un défi majeur que le Royaume chérifien veut relever en commençant par ces deux pays qui sont la locomotive économique de la sous-région ouest-africaine. La Côte d'Ivoire connaît une forte croissance économique qui se situe entre 7 et 8 % par an. Une performance portée en partie par un secteur privé qui fait de la transformation numérique, un vecteur de compétitivité. Le Sénégal, deuxième économie de l'Afrique de l'Ouest francophone derrière la Côte d'Ivoire, est plébiscitée pour les efforts fournis dans le domaine du digital. Là où l'Afrique a atteint un taux de pénétration moyen autour de 100%, le Sénégal lui signe un taux de 113,66% en mars 2016. En choisissant ces deux pays, le Maroc veut leur apporter son « soutien pour conforter leur leadership régional et aussi pour accélérer leur transformation numérique ».

Le communiqué :
« Salon des Technologies de l'Information « AITEX – AFRICA IT EXPO » – 21 – 24 septembre 2016 à Casablanca
Le 1er salon de l'innovation et de la transformation digitale du continent met à l'honneur le Sénégal et la Côte d'Ivoire

La Fédération marocaine des technologies, de l'information, des télécommunications et de l'Offshoring (APEBI) organise la 1ère édition du Salon des Technologies de l'Information « AITEX – AFRICA IT EXPO », qui aura lieu du 21 au 24 septembre 2016 à la foire internationale de Casablanca. « AITEX – AFRICA IT EXPO » est la première plateforme de l'innovation et de la transformation digitale en Afrique, qui va réunir 150 exposants – tous issus des entreprises référencées dans le domaine -, 200 donneurs d'ordre, mais aussi des experts et des utilisateurs venus d'Afrique, du Moyen Orient et d'Europe. Pour cette édition, l'APEBI met à l'honneur le Sénégal et la Côte d'Ivoire, deux pays amis avec lesquels le Royaume entretient des relations de longue date, qui constituent un modèle de coopération exemplaire, et qui jouent par ailleurs un rôle de locomotive en Afrique de l'Ouest dans le domaine des TIC.

Aujourd'hui, la transformation digitale est devenue un enjeu majeur pour les sociétés, une mutation indispensable pour les entreprises et l'économie. A l'ère du numérique, cette transformation constitue un avantage fort pour nos sociétés, qui crée de la valeur… L'évolution très rapide des TIC -Technologies de l'Information et de la Communication- a profondément façonné le changement de nos modes de vie. Face à la généralisation des TIC dans les pays industrialisés, l'intégration de ces compétences (mais surtout leur maîtrise et leur exploitation) est un enjeu stratégique, sociétal, culturel et technologique en Afrique.
Le continent, qui poursuit son processus de mondialisation et sa dynamique d'émergence doit se « mettre à niveau » pour améliorer l'efficience de son économie et « booster » sa compétitivité locale et internationale. Grâce à une approche bien encadrée, qui va intégrer tous les paramètres, les enjeux et aussi les risques induits, la transformation digitale est sans conteste un levier de croissance économique et de compétitivité, créateur de valeur ajoutée.
La Fédération marocaine des technologies, de l'information, des télécommunications et de l'Offshoring (APEBI), est un acteur régional stratégique en Afrique car elle regroupe des entreprises qui jouent un rôle clé dans l'économie et qui sont des références dans leur domaine.
Pendant trois jours, l'APEBI va être le catalyseur d'une dynamique nouvelle, qui va accélérer le développement du numérique dans le continent.

AITEX – AFRICA IT EXPO : Première plateforme de l'innovation et de la transformation digitale d'Afrique
Cette édition sera marquée par une forte présence d'experts de haut niveau, des opérateurs nationaux et internationaux reconnus, tous réunis autour d'un programme ambitieux qui a pour vocation d'être la première plateforme de l'innovation et de la transformation digitale en Afrique.
Organisé avec le soutien institutionnel de Maroc Export, le salon « AITEX – AFRICA IT EXPO » va accueillir principalement des distributeurs, des fournisseurs de technologie, des intégrateurs de solutions, éditeurs, opérateurs télécoms, ISP, ASP, délocalisation de fonctions de gestion, TMA, help desk conseil, offshoring, mobility, big data, Cloud, réseaux, e-Commerce… Vitrine de l'offre numérique et des dernières évolutions digitales, « AITEX – AFRICA IT EXPO » est une *plateforme* unique de rencontres, d'échanges et d'opportunités d'affaires.
Véritable révélateur des nouvelles tendances, le Salon «AITEX – AFRICA IT EXPO » est une occasion unique de rencontrer et d'échanger sur les problématiques quotidiennes des entrepreneurs, collectivités et de trouver les réponses appropriées grâce au concours de spécialistes, eux-mêmes engagés dans les processus de développement des économies émergentes et de la coopération sud-sud.
Placé sous le thème, «Transformation Digitale : Levier de développement en Afrique», le salon offre une nouvelle occasion de conscientiser et sensibiliser nos sociétés sur la formidable opportunité offerte par les technologies numériques pour accélérer le développement du continent. Des rencontres sont organisées au cours de ces trois journées pour débattre des problématiques actuelles et des enjeux sociétaux de ces mutations afin d'adopter les meilleures pratiques et ainsi anticiper les défis auxquels les entreprises et économies africaines sont confrontées.
«AITEX – AFRICA IT EXPO » va promouvoir les relations d'affaires et la mise en réseau des différents acteurs économiques du continent, à travers des coopérations sud-sud, nord-sud et public-privé.

Le Sénégal et la Côte d'Ivoire à l'honneur
Le défi numérique en Afrique passe inéluctablement par la connexion des ressources du continent. Un aspect *que l'APEBI a compris et intégré dans l'organisation de ce salon, c'est pourquoi la fédération a décidé de mettre à l'honneur, pour sa première édition, le Sénégal et la Côte d'Ivoire.* Ces deux pays, représentant deux premières puissances économiques de l'Afrique de l'ouest francophone engagés dans une dynamique de croissance depuis plusieurs années, ont à cœur de poursuivent respectivement leurs ambitions numériques.
La Côte d'Ivoire connaît une forte croissance économique qui se situe entre 7 et 8 % par an et le développement du numérique est devenu un enjeu majeur, créateur de richesses. Le numérique constitue un potentiel énorme, présent dans tous les esprits, aussi bien du côté du gouvernement que des dirigeants d'entreprise. Selon une étude publiée par le cabinet Deloitte en mai 2016, seulement 36 % des entreprises estiment avoir atteint la maturité numérique.
Le Sénégal, quatrième économie de la sous-région ouest africaine après le Nigéria, la Côte d'Ivoire et le Ghana, et deuxième économie en Afrique de l'Ouest francophone derrière la Côte d'Ivoire s'est largement distingué dans l'évolution de l'économie numérique, premier levier de la transformation digitale. Là où l'Afrique a atteint un taux de pénétration moyen autour de 100%, le Sénégal lui signe un taux de 113,66% en mars 2016.
Le *Sénégal et la Côte d'Ivoire font partie des premiers pays africains à initier des* projets de gouvernance électronique (e-Gouv). Ils ont réalisé au fil des années des progrès importants dans les domaines tels l'économie numérique, la monétique, le courrier hybride, ou encore le taux de connectivité internet, etc.) Néanmoins, les disparités qui existent entre les différents pays du continent peuvent être réduites si un effort de coopération est accompli.
En mettant en avant ces deux pays amis, qui constituent un modèle important d'exemplarité sur le continent africain (et en particulier de ses voisins ouest-africains), le Maroc apporte son soutien pour conforter leur leadership régional et aussi pour accélérer leur transformation numérique. »
Article original de Cio-Mag

Original de l'article mis en page : « AITEX – AFRICA IT EXPO » : le Sénégal et la Côte d'Ivoire à l'honneur au Maroc, du 21 au 24 septembre 2016 | CIO MAG

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

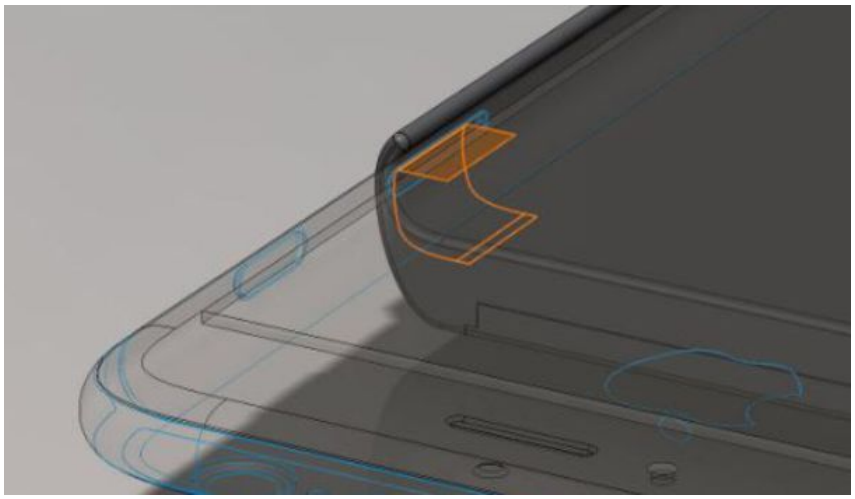
Contactez-nous

Réagissez à cet article

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

---

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

---

Usages et attentes des Français à l’égard du digital en matière d’information sur leur santé

6

Usages et attentes des Français à l’égard du digital en matière d’information sur leur santé

Dans un monde de santé de plus en plus connecté et digitalisé, 4 français sur 10 restent insatisfaits des informations santé qu'ils trouvent sur internet. A la veille du lancement par le laboratoire pharmaceutique MSD d'une nouvelle plateforme digitale d'information médicale, le groupe et Ipsos se sont intéressés aux usages et attentes des Français à l'égard des informations médicales trouvées sur internet.

Article original de Ipsos

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 : Usages et attentes des Français à l’égard du digital en matière d’information sur leur santé

---

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