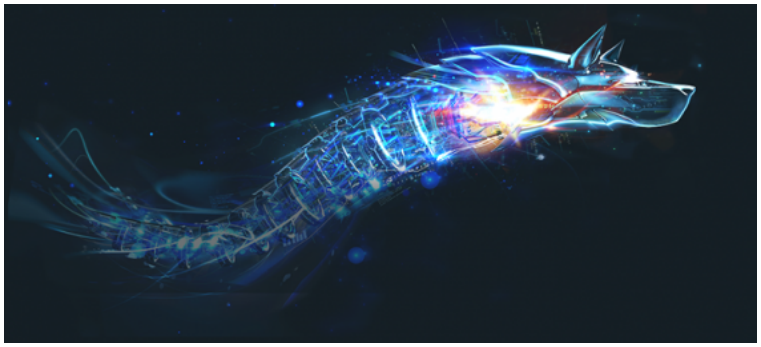
Victime du ransomware Bart ? Bitdefender publie un outil gratuit de déchiffrement

	Victime du ransomware Bart ? Bitdefender publie un outil gratuit de déchiffrement

L'outil proposé par Bitdefender fonctionne avec tous les échantillons connus. Le ransomware Bart, qui chiffre les appareils sans avoir besoin de connexion Internet, a été analysé par les chercheurs des Bitdefender Labs. Les victimes de ce malware peuvent désormais télécharger l'outil gratuit de déchiffrement afin de récupérer leurs données perdues.

Communiqué de presse – Alors que ce ransomware a été détecté en circulation pour la première fois en juillet 2016, Bitdefender est le seul éditeur de solutions de sécurité à proposer un outil de déchiffrement pour toutes les versions de Bart. L'outil de déchiffrement du ransomware Bart permet de déchiffrer les fichiers avec des extensions « .bart.zip », « .bart » et « .perl » et est également téléchargeable sur le site Internet « No More Ransom » depuis le 4 avril 2017.
Cet outil est le fruit d'une collaboration entre Bitdefender, Europol et la police roumaine en soutien à l'initiative « *No More Ransom* » lancée par le Centre européen de lutte contre la cybercriminalité d'Europol.

Le fonctionnement du ransomware Bart
Contrairement à d'autres familles de ransomwares, Bart chiffre les fichiers des victimes sans avoir besoin de recourir à une connexion Internet. Cependant, le processus de déchiffrement nécessite pour sa part une connexion Internet afin d'accéder au serveur de commande et contrôle (C&C) de l'attaquant, de pouvoir transférer des bitcoins et recevoir la clé de déchiffrement.
Alors que les premières versions de Bart se limitaient à un chiffrement plutôt rudimentaire, tel que la création d'archives .zip protégées par mot de passe, les nouvelles versions vont bien au-delà cette méthode.

Voici comment fonctionne Bart :
• Il supprime les points de restauration du système
• Il génère une clé de chiffrement en se basant sur les informations de la machine de la victime
• Il comptabilise tous les fichiers et les chiffre à l'aide de la clé générée
• Il utilise une master key pour chiffrer la clé utilisée pour chiffrer les fichiers (qui devient l'identifiant unique de la victime, l'UID)
• Il affiche l'avis de rançon et redirige vers un site Internet .onion (l'URL contient l'UID de la victime)…[lire la suite]

Réagissez à cet article

Source : *Bitdefender publie un outil gratuit de déchiffrement du ransomware Bart | UnderNews*

Le Wifi de votre téléphone permettra aussi de vous

pister

Le Wifi de votre téléphone permettra aussi de vous pister

Différents projets visent à pister les personnes passant à proximité de capteurs wifi. Ce qui pose notamment la question de l'anonymisation des données.
Marylin Gobert / La Gazette

Beaucoup de villes cherchent aujourd'hui à devenir intelligentes. Elles sont ainsi truffées de capteurs, de compteurs Linky, d'objets connectés, qui permettent de relever et de communiquer les données. Les smart cities sont devenues de véritables pompes à informations. Mais il ne faudrait pas oublier que la data est au service des citoyens. Elle vise à répondre à leurs besoins en améliorant, par exemple, la qualité du service public. Elle ne doit donc être ni intrusive, ni devenir un moyen de contrôle de la vie privée.
D'où l'importance de la protection des données à caractère personnel, définie par l'article 2 de la loi n° 78-17 du 6 janvier 1978 dite « informatique et libertés » comme « toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement ».

Des capteurs d'habitudes

La récente loi du 7 octobre 2016 pour une République numérique a encore renforcé ces principes, en affirmant la nécessaire maîtrise de l'individu sur ses données. La Commission nationale de l'informatique et des libertés (Cnil) veille notamment à leur anonymisation.
L'une des tentations actuelles est de mesurer les flux des passants, de cartographier leurs déplacements au moyen de capteurs des signaux wifi de smartphones.
L'exemple du géant de l'affichage publicitaire, JCDecaux, qui voulait placer des boîtiers dans son mobilier publicitaire, sur l'esplanade de La Défense à Paris, afin de capter les téléphones dans un rayon de 25 mètres, illustre cette tendance. Cela lui aurait permis d'estimer la fréquentation de ce quartier parisien.
Situation semblable à Rennes pour lutter contre la désertification du centre-ville. Une association de commerçants a voulu mettre en place des capteurs de signaux wifi. Le but ? Assurer un maillage de cette zone pour connaître les habitudes des consommateurs et en tirer des moyens de dynamiser le quartier…[lire la suite]

Réagissez à cet article

Source : *L'indispensable anonymisation des données personnelles des passants*

Windows 10 : Microsoft dévoile les données personnelles qu'il récolte

Microsoft dévoile les données personnelles que Windows 10 récolte

---

Un cadre haut placé chez Microsoft vient de révéler la publication d'une liste des données personnelles que l'entreprise récolte sur Windows 10. Si Microsoft tente de rassurer sur sa politique de confidentialité et la sécurisation des données, ce nouveau procédé est susceptible de relancer des débats.

Selon le site theverge.com, le chef Windows Terry Myerson explique que **Microsoft publie désormais des informations sur les données collectées** dans le cadre de Windows 10. Ces données sont publiées sur le site TechNet de Microsoft. Dans le cadre de la dernière mise à jour Creators Update et de la nouvelle politique de confidentialité, les contrôles autour des niveaux de collecte sont renforcés.

Les données personnelles : une question de sécurité des utilisateurs

Si Microsoft tente de rassurer sur les contrôles et la sécurisation des données personnelles, il n'en demeure pas moins que ses pratiques posent problème. **Microsoft est soupçonné de suivre ses utilisateurs via des traçeurs** et de ne pas respecter des choix de confidentialité exprimés par les utilisateurs Windows 10. Il y aurait danger pour le droit au respect de la vie privée. Il peut même s'agir d'espionnage.
Toutefois, les autorités de régulation veillent au grain. La France vient d'ordonner à Microsoft de cesser toute traçabilité. L'agence de protection des données de l'Union Européenne ont mis en garde contre les insuffisances des changements apportés par Microsoft Creators Update.

Le débat sur les données personnelles relancé ?

La révélation des données peut constituer une **atteinte du droit à la protection de la vie privée.** Il est tout de même légitime de se poser la question de savoir si les autorités de régulation ne protège pas certains intérêts particuliers ou si leur examen n'est pas dicté par un esprit partisan.
Après tout, Amazon, Facebook et Google sont déjà capables de repérer vos habitudes de consommation, et de vous proposer des produits en lien avec vos acquisitions passées. Même si Google a déjà pu faire l'objet d'une procédure à l'initiative de l'UE, on peut se demander pour quelles raisons, des entreprises comme Amazon, ne pourraient pas subir le même traitement que celui réservé à Google et Microsoft…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Windows 10 : Microsoft dévoile les données personnelles qu'il récolte*

Voyagez aux Etats-Unis et laissez vos données être espionnées

Voyagez aux Etats-Unis et laissez vos données être espionnées

---

L'administration Trump envisage de demander aux voyageurs arrivant aux Etats-Unis l'accès aux données de leur smartphone et à leurs comptes Twitter, Facebook ou LinkedIn. Une sévère menace pour la cybersécurité des entreprises européennes.

Cette fois-ci, la côte d'alerte est clairement franchie. Dans ses colonnes, le *Wall Street Journal* évoque un projet de l'administration Trump qui pourrait forcer les visiteurs arrivant aux Etats-Unis à communiquer aux autorités les contacts et contenus présents sur leur téléphone mobile ainsi que les mots de passe de leurs comptes de réseaux sociaux, permettant d'accéder aux messages privés envoyés sur ces canaux. Un projet qui ne serait pas limité aux pays soumis aux règles de sécurité les plus strictes – et dont les ressortissants doivent obtenir un visa -, mais concernerait aussi les pays considérés comme des alliés des États-Unis, dont la France.
Rappelons que, pour se rendre de façon temporaire sur le sol américain, pour affaires ou en tant que touriste, les Français doivent déjà solliciter une autorisation électronique (Esta), valable 2 ans. En février, le ministre de l'Intérieur américain (Homeland Security) avait déjà évoqué, lors d'une audition devant le Sénat, le fait que les voyageurs étrangers (notamment issus des 6 pays blacklistés par un décret de l'administration Trump) venant aux États-Unis seraient tenus de fournir leurs mots de passe sur les médias sociaux aux autorités d'immigration avant de rentrer sur le territoire américain.

La peur de l'espionnage économique

Selon le *Wall Street Journal,* cette mesure serait donc étendue à d'autres pays et aussi aux contacts téléphoniques. « *S'il existe un doute sur les intentions d'une personne venant aux États-Unis, elle devrait avoir à prouver la légitimité de ses motivations, vraiment et véritablement jusqu'à ce que cela nous satisfasse* », a expliqué le conseiller principal du Homeland Security, Gene Hamilton, cité par le quotidien économique.
Si la question ne manquera pas de soulever de vifs débats sur le sol américain et entre les États-Unis et ses partenaires et si une procédure de la sorte pose également quelques questions pratiques assez épineuses, la perspective risque d'échauder de nombreuses entreprises européennes. Car, les activités des services de renseignement US associent sans vergogne antiterrorisme et espionnage économique au profit des entreprises américaines. Une porosité d'ailleurs assumée, comme l'ont montré de nombreux documents dévoilés par Edward Snowden ou *Wikileaks* et révélant les activités de la NSA en matière d'espionnage économique. Les activités de cette nature ne sont d'ailleurs pas limitées à la seule agence de Fort Meade, mais s'étendent à toute la communauté du renseignement aux Etats-Unis.
Au passage, les mesures envisagées par l'administration Trump signeraient probablement l'arrêt de mort du Privacy Shield, l'accord transatlantique sur les transferts de données qui succède au Safe Harbor. Pour mémoire, ce dernier érige comme credo le fait que les données des citoyens européens exportées aux Etats-Unis bénéficient de la même protection que celle que leur accorde le droit européen. En février, les CNIL européennes s'étaient déjà inquiétées des conséquences possibles du décret sur l'immigration du Président Trump sur cet accord…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *L'entrée aux Etats-Unis conditionnée par les données des smartphones ?*

Ce vibromasseur connecté muni d’une caméra est vraiment trop facile à hacker

Ce vibromasseur connecté muni d’une caméra est vraiment trop facile à hacker

Oui, évidemment on se demande bien qui voudrait hacker ce type d'objet, pour visionner ce type d'images. Mais ainsi va le monde : le Wi-fi de ce vibromasseur connecté se pirate en deux clics.

On ne le dira jamais assez, mais une connexion WiFi est une porte d'entrée royale pour n'importe quel hacker. Même fermée, elle est très simple à pirater. Ensuite, le pirate peut avoir accès à l'ensemble des données du trafic internet de l'objet connecté.

Photos, identifiants, mots de passe pour un téléphone, mais aussi flux *streaming* pour ce vibromasseur connecté. S'il vient à être piraté, c'est une tout autre intimité qui peut être violée.

Vibromasseur avec hot spot WiFi

Le vibromasseur Svakom Siime Eye (disponible au prix de 249 dollars) dispose du WiFi et d'une caméra intégrée pour procéder à des *livestreams*. Les chercheurs en sécurité de Pen Test Partners ont découvert que l'interface de l'objet connecté était très simple à hacker pour toute personne se trouvant à portée de la connexion WiFi (et pourvu d'un minimum de connaissance en la matière, cela s'entend).
Un piratage d'autant plus facilité que le mot de passe par défaut de ce point d'accès WiFi est « 88888888 », soit 8 fois le chiffre 8.

Un piratage enfantin

N'importe quelle personne à proximité du signal peut accéder au flux vidéo. Pire, en poussant leur investigation un peu plus loin, ces chercheurs sont parvenus à accéder au serveur web et à la racine de l'appareil pour configurer une connexion à distance.

Les utilisatrices qui voudraient partager ces instants intimes avec leur partenaire, pourraient se retrouver à faire de même avec leur voisin de palier. Une perspective peu réjouissante.
Le fondateur de Pen Test, Ken Munro, explique qu'il a tenté de contacter la compagnie pendant des mois avant de rendre publique ces informations.
Ce n'est pas la première fois que ce type d'objet connecté est mis au ban : le mois dernier, la société canadienne Standard Innovation a été condamnée à verser 3 millions de dollars à ses clientes pour avoir omis de mentionner qu'elle collectait leurs données personnelles via leur vibromasseur connecté et l'application dédiée.
Auteur : Elodie

Réagissez à cet article

Source : *Ce vibromasseur connecté muni d'une caméra est vraiment trop facile à hacker*

Alerte : Sérieuse faille WiFi. Mettez à jour vos iPhones avec la IOS 10.3.1

Alerte : Sérieuse faille WiFi. Mettez à jour vos iPhones avec la IOS 10.3.1

La mise à jour 10.3.1 du système d'exploitation mobile iOS corrige une vulnérabilité permettant d'exécuter du code à distance sur les puces WiFi de Broadcom dans les iPhone, iPad et iPod. Le fabricant de puces a pu obtenir une grâce d'une dizaine de jours avant divulgation de l'exploit par l'équipe sécurité de Google, Project Zero.

L'iPhone 7 est concerné par la faille WiFi et éligible pour la mise à jour iOS 10.3.1. (crédit : Susie Ochs)

Si vous n'avez pas mis à jour iOS pour vos terminaux mobiles Apple depuis longtemps, voici une bonne occasion de le faire. Apple a en effet lancé la version 10.3.1 de son système d'exploitation pour iPhone, iPad et iPod pour corriger une vulnérabilité permettant à un attaquant d'exécuter du code malveillant distant sur les puces WiFi Broadcom de ces terminaux. Cette vulnérabilité touche la fonction d'authentification dans le protocole 802.11r permettant aux terminaux de se connecter de façon sécurisée entre plusieurs stations de base sans fil d'un même domaine. Les hackers peuvent exploiter cette faille pour exécuter du code au sein même du firmware de la puce WiFi s'ils se trouvent à portée du réseau sans fil des terminaux visés.
Il s'agit là d'une vulnérabilité parmi d'autres trouvées par le chercheur Gal Benjamini de l'équipe de sécurité de Google, Project Zero, dans le firmware des puces Broadcom WiFi. Certaines d'entre elles concernent également les terminaux Android et ont été patchées dans le cadre du bulletin de sécurité Android d'avril. La mise à jour iOS 10.3.1, lancée lundi, est quelque peu inhabituelle car elle vient une semaine à peine après la 10.3 qui apportait pourtant un lot de correctifs touchant différents composants. L'explication pour ce court intervalle entre ces deux mises à jour est à voir du côté du délai pratiqué par Google Project Zero pour dévoiler au public les exploits de failles…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Apple colmate une sérieuse faille WiFi dans iOS – Le Monde Informatique*

Alerte : Les revendeurs informatiques de Tech Data France ciblés par un site Internet Frauduleux

Alerte : Les revendeurs informatiques de Tech Data France ciblés par un site Internet Frauduleux

---

Chers revendeurs informatiques, attention à la nouvelle arnaque. Les intentions des pirates ne sont pas encore connues, mais les intentions sont forcément malveillantes.

En tant que revendeur informatique, il est fort probable que vous commandiez votre matériel destiné à la revente ou non chez les principaux et parmis les plus anciens grossistes et importateurs Français : Ingram ou Techdata.
Une récente communication de Techdata, qui nous a été remontée par un précieux partenaire Parisien, nous informe que Techdata vient de lancer l'alerte suivante auprès de ses clients :

Cher client,
Il a été porté à notre connaissance que certains Clients de TECH DATA ont reçu des emails comportant un lien internet vers un site web frauduleux leur demandant :
– de s'inscrire à une conférence dans laquelle TECH DATA et d'autres distributeurs participeraient,
– de fournir des informations type login et mot de passe de TECH DATA ainsi que d'autres informations sensibles.
Le site Web apparaît comme indiqué ci-dessous :

Veuillez noter que ce site web n'est d'aucune façon associé à TECH DATA. La sécurité de nos partenaires est une priorité pour TECH DATA et nous n'autorisons aucun tiers à collecter les identifiants de connexion de nos clients.
Aussi, actuellement nous œuvrons avec les autorités compétentes pour la fermeture de ce site frauduleux.
A ce jour, à notre connaissance les clients européens ne semblent pas affectés, ce site frauduleux visant les clients américains principalement.
Cependant, nous comptons sur votre vigilance et vous remercions de nous informer dans le cas où vous recevriez des emails contenant des liens vers ce site internet ou similaires en vous adressant à l'adresse suivante : itsecurity@techdata.com
Nous attirons votre attention sur la sophistication et l'augmentation de la cybercriminalité (phishing), dès lors restez vigilants.
Nous vous remercions de votre attention et collaboration.
Tech Data Europe

Comme vous pouvez le remarquer, à l'instar de KPMG pourtant spécialisé en audit et conseil dans de nombreux domaines dont la sécurité informatique, pourtant victime d'une arnaque au Président leur ayant coûté plusieurs millions d'Euros (7,6) en 2014, les professionnels de l'informatique sont aussi la cible des pirates.
Nous espérons que, même si la plupart n'ont pas assisté à nos conférences de sensibilisation à la Cybercriminalité, ils sauront à quoi ressemble le loup pour ne pas le laisser rentrer dans la bergerie.

Denis JACOPINI

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *E-mailing Tech Data France*

Samsung Galaxy S8 ou S8+ : Une première faille de

sécurité dénichée

Samsung Galaxy S8 ou S8+ : Une première faille de sécurité dénichée

La semaine dernière, le géant Sud-Coréen Samsung dévoilait ses nouveaux Smartphones Galaxy S8 et S8+. Un enjeu important pour le constructeur qui souhaite retrouver une image de marque suite à ses déboires avec les batteries explosives de son Note 7. Mais alors que les nouveaux modèles S8 et S8+ ne sont pas encore commercialisés, une première faille vient d'être décelée, le système de reconnaissance faciale peut être en effet trompé par une simple photo.

Galaxy S8 : Le système de reconnaissance faciale déjoué par une simple photo

Quelques jours seulement après sa présentation officielle, le Samsung Galaxy S8 est déjà sous le feu des critiques. En effet, une vidéo mise en ligne le 29 mars par la chaîne iDeviceHelp montre un utilisateur déverrouiller un **Samsung Galaxy S8** à l'aide d'une simple photo. Le système de **reconnaissance faciale** censé être un procédé sécurisé montre donc déjà sa première faille !

Avec ses deux nouveaux modèles, le constructeur Samsung avait pourtant misé sur la sécurité avec la présence **d'un système de reconnaissance d'iris**, un lecteur d'empreintes digitales situé désormais au dos de l'appareil ainsi que la reconnaissance faciale, une manière rapide et aisée de déverrouiller le Galaxy S8 ou S8+…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur
: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Samsung Galaxy S8 ou S8+ : Une première faille de*

Bug Butter : la plateforme collaborative de mise en relation entre pirates et forces de l’ordre

Bug Butter : la plateforme collaborative de mise en relation entre pirates et forces de l’ordre

La plateforme Bug Butter met en relation pirates et membres des forces de l'ordre autour d'une place de marché d'informations sensibles.

Après les plates-formes de Bug Bounty, qui visent à mettre en relation des experts en cybersécurité avec des entreprises, une nouvelle étape vient d'être franchie dans la « *plateformisation* » des relations humaines : en partenariat avec l'ANSSI, la société OPFOR Intelligence ouvre aujourd'hui Bug Butter, la première plateforme de mise en relation entre pirates et membres des forces de l'ordre.
Bug Butter a pour ambition de fluidifier le processus d'enquête tout en permettant aux pirates de mieux gérer leur capital informationnel et leur image. La plateforme a également pour objectif de pallier le manque de moyen des services d'enquêtes, en offrant à ces derniers un outil simple et transparent capable d'optimiser le taux de résolution des affaires pour un budget donné.
La plateforme se compose de trois parties essentielles : des profils de cybercriminels, des profils de cyber-enquêteurs et, au centre, une place de marché unique en son genre.
Concrètement, Bug Butter permet aux cybercriminels de s'enregistrer sur une plateforme conçue à l'image de LinkedIn : compétences techniques, exploits réalisés, mentors, affiliations récentes avec des groupes de cybercriminels en vue, ils peuvent créer un profil complet et moderne afin d'offrir une vision complète de leurs activités.
Toutefois, et contrairement aux plateformes sociales que l'on connaît actuellement, ce profil reste pour l'essentiel privé : seul le pseudo du pirate est visible par défaut. C'est ensuite au criminel de décider quelles informations il souhaite rendre visibles, à quel prix, et -surtout- à qui.
Car outre les pirates, la plateforme est ouverte aux membres des forces de l'ordre. Ces derniers peuvent eux aussi créer leur profil de manière similaire. Nationalité, unité de rattachement, centres d'intérêt (fraude aux outils de paiement, recel, harcèlement, moeurs, renseignement…), outils maîtrisés (EnCase, i2 Analyze, Palantir…) là aussi tout est fait pour que chaque investigateur puisse donner une vision à 360° de son activité et valoriser son image…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Bug Butter : la plateforme collaborative de mise en*

relation entre pirates et forces de l’ordre

Hackers stole $800,000 from ATMs using Fileless Malware

	Hackers stole $800,000 from ATMs using Fileless Malware

---

Hackers targeted at least 8 ATMs in Russia and stole $800,000 in a single night, but the method used by the intruders remained a complete mystery with CCTV footage just showing a lone culprit walking up to the ATM and collecting cash without even touching the machine.

Even the affected banks could not find any trace of malware on its ATMs or backend network or any sign of an intrusion.

The only clue the unnamed bank's specialists found from the ATM's hard drive was – two files containing malware logs.

The log files included the two process strings containing the phrases: « Take the Money Bitch! » and « Dispense Success. »

This small clue was enough for the researchers from the Russian security firm Kaspersky, who have been investigating the ATM heists, to find malware samples related to the ATM attack.

In February, Kaspersky Labs reported that attackers managed to hit over 140 enterprises, including banks, telecoms, and government organizations, in the US, Europe and elsewhere with the 'Fileless malware,' but provided few details about the attacks.

According to the researchers, the attacks against banks were carried out using a Fileless malware that resides solely in the memory (RAM) of the infected ATMs, rather than on the hard drive.

Now during the Kaspersky Security Analyst Summit in St. Maarten on Monday, security researchers Sergey Golovanov and Igor Soumenkov delved into the ATM hacks that targeted two Russian banks, describing how the attackers used the fileless malware to gain a strong foothold into bank's systems and cash out, ThreatPost reports.

Mysterious ATM Hack Uncovered by Researchers

Dubbed **ATMitch**, the malware – previously spotted in the wild in Kazakhstan and Russia – is remotely installed and executed on ATMs via its remote administration module, which gives hackers the ability to form an SSH tunnel, deploy the malware, and then sending the command to the ATM to dispense cash.

Since Fileless malware uses the existing legitimate tools on a machine so that no malware gets installed on the system, the ATM treats the malicious code as legitimate software, allowing remote operators to send the command at the time when their associates are present on the infected ATM to pick up the money.

This ATM theft takes just a few seconds to be completed without the operator physically going near the machine. Once the ATM has been emptied, the operator 'signs off,' leaving a very little trace, if any, of the malware.

However, this remote attack is possible only if an attacker tunnels in through the bank's back-end network, a process which required far more sophisticated network intrusion skills…[lire la suite]

Réagissez à cet article

Source : *Hackers stole $800,000 from ATMs using Fileless Malware*