WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages

WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages

Si les messageries mobiles se renforcent grâce à un dispositif de chiffrement, un hackeur a trouvé le moyen de récupérer l'intégralité des messages en clair.

Avec un chiffrement de bout-en-bout, les messages sont normalement sécurisés. Cela permet d'éviter les attaques de type man-in-the-middle, et par ailleurs, même le prestataire de service n'est pas en mesure de prendre connaissance du contenu de ces échanges. Pourtant, il existe un moyen de contourner ces dispositifs. La société Ability a partagé ses exploits en vidéo avec le magazine Forbes.
Concrètement, la faille se trouve au sein du système de signalisation n° 7 (SS7), un ensemble de protocoles de signalisation téléphonique. C'est le réseau principal permettant de connecter les réseaux téléphoniques entre eux. C'est également lui qui établit des relations entre le téléphone d'un utilisateur et le réseau, par exemple les tonalités d'appel après une numérotation ou de mise en attente ou encore le renvoi vers la messagerie.

Téléchargez WhatsApp Le hackeur fait ainsi croire au SS7 qu'il dispose du même numéro de téléphone que celui de la victime. Il est ensuite en mesure d'installer l'application WhatsApp ou Telegram puis de recevoir le code secret permettant d'authentifier son smartphone.
sécurité security banner gb
Dès lors, le hackeur peut récupérer l'historique des conversations synchronisées et se faire passer pour la victime. De son côté, cette dernière recevra un message l'avertissant que son compte est utilisé autre part. L'application sera donc déconnectée et l'identité de la victime… usurpée.
Puisque le SS7 est un réseau global utilisé par les opérateurs téléphoniques à travers le monde, celui-ci n'appartient vraiment à personne. Cela signifie que la vulnérabilité n'a pas été corrigée et le processus semble pour l'heure compliqué. Autant dire qu'il s'agit d'une porte ouverte pour les agences de renseignement.

Voici la procédure en vidéo :

Article original de Guillaume Belfiore

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 : WhatsApp, Telegram ou Signal peuvent être piratés malgré le chiffrement des messages

---

Skimer, la nouvelle menace pour distributeurs de billets

Skimer, la nouvelle menace pour distributeurs de billets

Skimer, un groupe russophone, force les distributeurs automatiques de billets (DAB) à l'aider à dérober de l'argent. Découvert en 2009, Skimer a été le premier programme malicieux à prendre pour cible les DAB. Sept ans plus tard, les cybercriminels ré-utilisent ce malware. Mais le programme, ainsi que les escrocs, ont évolué ; ils représentent une menace encore plus importante pour les banques et leurs clients partout dans le monde.

Imaginons qu'une banque découvre avoir été victime d'une attaque. Étrangement, aucune somme d'argent n'a été dérobée et rien n'a été modifié dans son système. Les criminels sont partis comme ils sont venus. Serait-ce possible ? Je vous parlais de ce type d'attaque l'année dernière. L'éditeur Gdata m'avait invité en Allemagne pour découvrir l'outil malveillant qui permettait de pirater un distributeur de billets. Aujourd'hui, l'équipe d'experts de Kaspersky Lab a mis au jour le scenario imaginé par les cybercriminels et découvert des traces d'une version améliorée du malware Skimer sur l'un des DAB d'une banque. Il avait été posé là et n'avait pas été activé jusqu'à ce que les criminels lui envoient un contrôle : une façon ingénieuse de couvrir leurs traces.
Le groupe Skimer commence ses opérations en accédant au système du DAB, soit physiquement, soit via le réseau interne de la banque visée. Ensuite, après été installé avec succès dans le système, l'outil Backdoor.Win32.Skimer, infecte le cœur de l'ATM, c'est-à-dire le fichier exécutable en charge des interactions entre la machine et l'infrastructure de la banque, de la gestion des espèces et des cartes bancaires.
Ainsi, les criminels contrôlent complètement les DAB infectés. Mais ils restent prudents et leurs actions témoignent d'une grande habileté. Au lieu d'installer un skimmer (un lecteur de carte frauduleux qui se superpose à celui du DAB) pour siphonner les données des cartes, les criminels transforment le DAB lui-même en skimmer. En infectant les DAB avec Backdoor.Win32.Skimer, ils peuvent retirer tout l'argent disponible dans le distributeur ou récupérer les données des cartes des utilisateurs qui viennent retirer de l'argent, y compris le numéro de compte et le code de carte bancaire des clients de la banque.
Il est impossible pour un individu lambda d'identifier un DAB infecté car aucun signe de le distingue d'un système sain, contrairement à un DAB sur lequel a été posé un skimmer traditionnel qui peut être repéré par un utilisateur averti.

Un zombie dormant
Les retraits directs depuis un DAB ne peuvent pas passer inaperçu alors qu'un malware peut tranquillement siphonner des données pendant une longue période. C'est pourquoi le groupe Skimer n'agit pas immédiatement et couvre ses traces avec beaucoup de prudence. Leur malware peut opérer pendant plusieurs mois sans entreprendre la moindre action.
Pour le réveiller, les criminels doivent insérer une carte spécifique, qui contient certaines entrées sur sa bande magnétique. Après lecture de ces entrées, Skimer peut exécuter la commande codée en dur ou requérir des commandes via le menu spécial activé par la carte. L'interface graphique de Skimer n'apparaît sur l'écran qu'une fois la carte éjectée et si les criminels ont composé la bonne clé de session, de la bonne façon, sur le pavé numérique en moins de 60 secondes.
À l'aide du menu, les criminels peuvent activer 21 commandes différentes, comme distribuer de l'argent (40 billets d'une cassette spécifique), collecter les données des cartes insérées, activer l'auto-suppression, effectuer une mise à jour (depuis le code du malware mis à jour embarqué sur la puce de la carte), etc. D'autre part, lors de la collecte des données de cartes bancaires, Skimer peut sauvegarder les fichiers dumps et les codes PIN sur la puce de la même carte, ou il peut imprimer les données de cartes collectées sur des tickets générés par le DAB.
Dans la plupart des cas, les criminels choisissent d'attendre pour collecter les données volées afin de créer des copies de ces cartes ultérieurement. Ils utilisent ces copies dans des DAB non infectés pour retirer de l'argent sur les comptes clients sans être inquiétés. De cette manière, ils s'assurent que les DAB infectés ne seront pas découverts. Et ils récupèrent de l'argent simplement.

Des voleurs expérimentés
Skimer a été largement répandu entre 2010 et 2013. À son arrivée correspond une augmentation drastique du nombre d'attaques sur des distributeurs automatiques de billets, avec jusqu'à neuf différentes familles de malwares identifiées par Kaspersky Lab. Cela inclut la famille Tyupkin, découverte en mars 2014, qui est devenue la plus populaire et la plus répandue. Cependant, il semblerait maintenant que Backdoor.Win32.Skimer soit de retour. Kaspersky Lab identifie 49 modifications de ce malware, dont 37 ciblent les DAB émanant de l'un des plus importants fabricants. La version la plus récente a été découverte en mai 2016.
En observant les échantillons partagés avec VirusTotal, on note que les DAB infectés sont répartis sur une large zone géographique. Les 20 derniers échantillons de la famille Skimer ont été téléchargés depuis plus de 10 régions à travers le monde : Émirats Arabes Unis, France, États-Unis, Russie, Macao, Chine, Philippines, Espagne, Allemagne, Géorgie, Pologne, Brésil, République Tchèque… [Lire la suite]
Remarquable article de Damien Bancal

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

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

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

Contactez-nous

Réagissez à cet article

Source : *Skimer, la nouvelle menace pour distributeurs de billets – Data Security BreachData Security Breach*

L’État crée encore un nouveau fichier secret de données personnelles

L’État crée encore un nouveau fichier secret de données personnelles

---

Le gouvernement a fait connaître vendredi la création d'un fichier de données personnelles utilisé pour les services de renseignement intitulé « #BCR-DNRED », dont le contenu et la portée sont confidentiels. Il s'agit d'un fichier permettant les enquêtes contre la fraude douanière, orienté vers les crimes graves.

Le gouvernement a fait publier vendredi au Journal Officiel un décret n° 2016-725 du 1er juin 2016 qui ajoute un 13e fichier à la liste des fichiers confidentiels de données personnelles mis en œuvre par l'État, « *intéressant la sûreté de l'Etat, la défense ou la sécurité publique* ».
Comme le veut la règle, on ne sait strictement rien de ce fichier si ce n'est qu'il est baptisé « BCR-DNRED » et sera utilisé par les « *services du ministère des finances et des comptes publics (administration des douanes et droits indirects) traitant de la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la prolifération des armes de destruction massive* ».
L'acronyme BCR-DNRED est sans aucun doute une référence à la Direction nationale du renseignement et des enquêtes douanières (DNRED), rattachée à Bercy. Considérée comme un service de renseignement, elle est chargée notamment de collecter des informations sur les les grands trafics de contrebande, et de lutter contre les flux financiers clandestins.

UN FICHIER CONTRE LE TRAFIC

JORF n°0128 du 3 juin 2016
texte n° 87

Délibération n° 2016-010 du 21 janvier 2016 portant avis sur un projet de décret portant création au profit de la direction nationale du renseignement et des enquêtes douanières d'un traitement automatisé de données à caractère personnel dénommé « BCR-DNRED »

NOR: CNIX1614799X
ELI: Non disponible

Avis favorable avec réserve.

L'avis « favorable avec réserve » de la Cnil.

On imagine donc que le fichier BCR-DNRED s'inscrit dans une politique de croisement d'informations concernant de possibles trafics internationaux illicites de biens ou d'argent qui transitent par la France, avec une orientation plus spécifique vers la recherche de financements de crimes graves.
La Cnil, qui n'a pas le droit de publier son avis, a émis un avis « favorable avec réserve », ce qui veut dire qu'elle a estimé qu'au moins sur certains points, le fichier projeté n'était pas conforme à la loi de 1978 sur la protection des données personnelles. Elle avait déjà émis des réserves non publiées concernant les deux derniers fichiers créés par l'État, le fichier CAR relatif au suivi des prisonniers créé en novembre 2015, et le Fichier de traitement des Signalés pour la Prévention et la Radicalisation à caractère Terroriste (FSPRT) modifié quelques jours plus tôt.

Article original de Guillaume Champeau

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

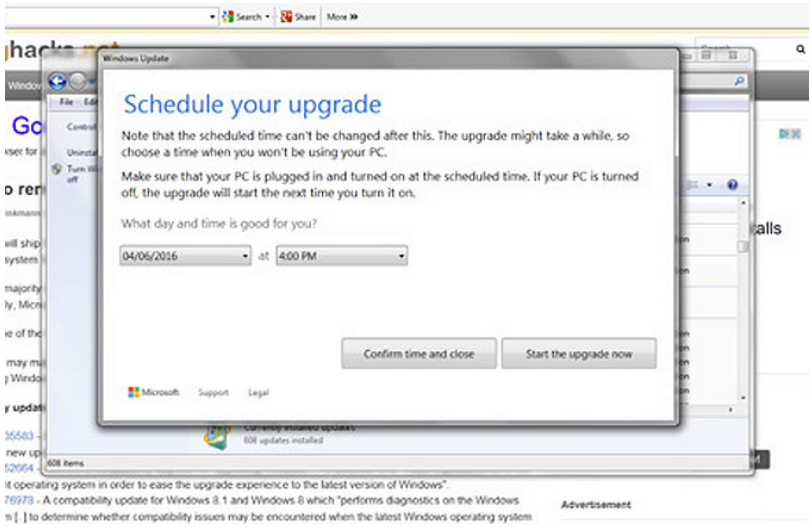
Réagissez à cet article

Original de l'article mis en page : L'État crée encore un nouveau fichier secret de données personnelles — Politique — Numerama

Microsoft supprimerait carrément la possibilité de refuser Windows 10

Microsoft supprimerait carrément la possibilité de refuser Windows 10

Selon une capture d'écran diffusée par The Register, Microsoft changerait à nouveau de méthode pour imposer la mise à jour vers Windows 10. Cette fois littéralement.



Le site britannique The Register publie ainsi la capture d'écran réalisée par un lecteur, qui montre qu'en lieu et place de la popup, Windows 7 lui a affiché une fenêtre qui impose de programmer une mise à jour vers Windows 10, avec un réglage de la date et de l'heure de l'opération. Il y a deux boutons sur la fenêtre ; le premier qui permet de confirmer la date et l'heure saisis ; le deuxième qui permet de demander une mise à jour immédiate.
Il n'y a aucun autre bouton pour refuser la mise à jour, ni de bouton « X » pour fermer la fenêtre (ce que Microsoft prenait de toute façon pour un accord).

COMMENT FAIRE ?

Les utilisateurs qui souhaitent refuser la mise à jour pourront toujours mettre une date de programmation très lointaine. Notez qu'au pire, en cas de mise à jour involontaire, il est possible de revenir vers Windows 7 ou Windows 8 en refusant d'accepter les conditions d'utilisation de Windows 10, présentées lors du premier lancement du système d'exploitation.
Le refus entraîne en effet une annulation de l'installation de Windows 10 puisque, même s'il peut forcer l'installation des fichiers du système, Microsoft ne peut pas encore obliger l'utilisateur à accepter son contrat.
La mise à jour vers Windows 10 reste gratuite jusqu'au 29 juillet 2016. Il faudra ensuite payer une licence. Notez que si vous avez déjà effectué la mise à jour et que vous devez réinstaller votre système, la gratuité de Windows 10 ne vaudra que si vous réinstallez l'OS sur le même ordinateur, reconnu par ses principaux composants. En cas de changement de carte mère ou de processeur par exemple, il devrait être imposé d'acheter la licence de Windows 10, auquel vous vous serez habitué…
Auteur : Guillaume Champeau

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 : Microsoft supprimerait carrément la possibilité de refuser Windows 10 – Tech – Numerama

---

Les pays arabes mutualisent leurs forces pour faire face à la cybercriminalité

Les pays arabes mutualisent leurs forces pour faire face à la cybercriminalité

Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.

La rencontre qui devrait être clôturée vendredi dernier vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité.

(CIO Mag) – Un atelier sur la sécurité informatique réunit les pays arabes depuis lundi dernier à Tunis. La rencontre qui devrait être clôturée ce vendredi vise à évaluer la prédisposition des Etats concernés à faire face aux attaques informatiques d'après le président du Centre arabe régional de la cybersécurité cité par le webmanagercenter.com.

Le directeur général de l'agence tunisienne de sécurité informatique, lui, indique que Tunis a pris très tôt des initiatives pour lutter contre la cybercriminalité. Mohamed Naoufel Frikha, repris par nos confrères, rappelle qu'un travail important a été réalisé depuis 1999 avec la création du premier centre en Afrique, le troisième dans le monde arabe.

Le rendez-vous de Tunis entend amener les pays arabes à créer des centres de cyber-alerte. Leur nombre est très insuffisant dans l'espace arabophone puisque seuls dix pays en disposent. Des représentants de treize Etats prennent part aux échanges.

Article de Ousmane Gueye

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 : Cybercriminalité: les pays

arabes mutualisent leurs forces pour faire face au phénomène | CIO MAG

L’Écosse veut désactiver les téléphones utilisés en prison

L’Écosse veut désactiver les téléphones utilisés en prison

L'Écosse a trouvé possiblement une solution radicale pour lutter contre la présence des téléphones portables dans les prisons : elle veut tout simplement pouvoir faire désactiver la carte SIM en cause dans les mains des opérateurs.

Les tribunaux de shérif d'Écosse (ou «Sheriff courts») auront bientôt la compétence de contraindre les opérateurs télécoms à déconnecter les téléphones portables non autorisés dont on détecterait une utilisation en prison. Concrètement, le tribunal ordonnera à l'opérateur de réseaux de désactiver ou déconnecter un téléphone mobile et/ou une carte SIM. C'est le sens d'un texte qui vient d'être notifié à Bruxelles, cette disposition imposant une restriction normative dans un État membre.

Accéder aux réseaux sociaux, intimider les témoins

« *Des détenus ont utilisé des téléphones portables non autorisés pour accéder aux réseaux sociaux, intimider des témoins et poursuivre et contrôler leurs activités criminelles depuis les institutions pénitentiaires,* expliquent les autorités écossaises en appui de leur texte. *Ils représentent par conséquent une menace notable pour la sécurité et le bon fonctionnement des établissements pénitentiaires.* »

Le hic est qu'actuellement, « *il est extrêmement difficile de trouver à l'intérieur d'institutions pénitentiaires des cartes SIM en raison de leur taille. Si c'est moins le cas pour les téléphones portables, ces détenus qui ont pris possession de téléphones portables seront prêts à faire l'impossible pour empêcher la détection desdits téléphones, notamment par des menaces et l'intimidation d'autres personnes.* »

En France, le projet de loi sur la réforme pénale

Le texte pourra entrer en vigueur dans trois mois, une fois achevé le round de la notification bruxelloise. En France, si les pouvoirs du juge profitent théoriquement d'une large latitude pour ordonner ce type de mesure, dans le projet de loi sur la réforme pénale, la réaction du législateur gagne plusieurs crans au-dessus par rapport aux textes antérieurs.

D'un, le pénitentiaire va devenir un service du renseignement. De deux, les autorités, qu'elles soient judiciaires ou administratives et sans qu'on sache très bien où se placera la frontière de leurs compétences, pourront installer une ribambelle de dispositifs techniques pour détecter des communications, et notamment des IMSI catchers. De là, elles seront en capacité d'effectuer des interceptions de sécurité pour prendre connaissance des correspondances échangées avec l'extérieur, etc… [Lire la suite]

Marc Rees auteur de cet article

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

Source : *L'Écosse veut désactiver les téléphones utilisés en prison – Next INpact*

Et si charger la batterie de

son smartphone via un port USB était dangereux ?

	**Et si charger la batterie de son smartphone via un port USB était dangereux ?**

On s'est tous probablement retrouvés un jour ou l'autre dans une situation où il nous restait peu de batterie sur notre téléphone et que nous n'avions pas de chargeur à portée de main. Le pire, c'est ce que ça nous est arrivé au moment même où on en avait le plus besoin, comme attendre un appel important, un message ou un e-mail, etc.

Il parait donc tout à fait normal de chercher une source d'électricité à proximité lors d'une telle situation, par exemple utiliser un port USB. Mais est-ce bien sûr ? Non, en réalité cela peut s'avérer dangereux. Via une connexion USB, n'importe qui peut s'emparer de vos fichiers, infecter votre smartphone d'un virus ou même le rendre inutilisable.

Chevaucher la foudre

Avant d'aborder le problème des hackers, il est important de préciser que toute les sources d'électricité ne sont pas forcément bonnes pour votre téléphone. Il existe beaucoup de plaintes sur Internet, principalement d'utilisateurs tentant de charger leur téléphone dernier cri en les connectant à des adaptateurs ou des chargeurs d'occasion (ou non originaux). Dans certains cas, les téléphones ont été rendus inutilisables. Dans certains cas encore plus étranges, des personnes prenant leur téléphone alors qu'ils étaient en charge ont été sérieusement blessées ou même tuées.

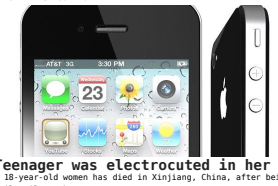
Follow

Daily Mail Online

@MailOnline

Teen dies after being electrocuted in her sleep while charging her iPhone http://dailym.ai/1o7Eia5

2:10 PM – 31 Jul 2014



Teenager was electrocuted in her sleep while charging her iPhone

A 18-year-old women has died in Xinjiang, China, after being electrocuted in her sleep while charging her iPhone 4s. It is not known if she was using an authentic Apple phone charger.

dailymail.co.uk

•

•

140140 Retweets

•

2424 likes

Malheureusement, il s'agit plus que de simples accidents. Par exemple, l'année dernière un appareil a été baptisé à juste titre : le tueur USB. Il contenait un impressionnant ensemble de condensateurs hébergés dans une carte mémoire flash USB, qui déchargeait 220 V dans le port USB auquel il était connecté. Une telle décharge pourrait dans le meilleur des cas détruire le port USB et dans le pire sans doute la carte mère de tout l'ordinateur. Nous doutons que vous souhaitiez tester la durabilité de votre téléphone de cette façon.

Montrez-moi vos fichiers

Deuxièmement, les ports USB n'ont pas été conçus uniquement pour la charge, mais aussi pour transférer des données. Les téléphones consommant le plus de données sont ceux conçus sur la plateforme Android 4 *x* et les versions antérieures, ils se connectent sur le mode MTP (Media Transfer Protocol) par défaut, exposant tous les fichiers de l'appareil.

En moyenne, il faut plus d'une centaine de kilo octets de données rien que pour le système hôte des fichiers et dossiers du téléphone. Pour vous donner une idée, il s'agit de la taille d'une copie de l'e-book d'*Alice au pays des merveilles*.

Bloquer votre téléphone vous éviterait de courir un tel risque mais honnêtement seriez-vous prêt à vous passer de votre téléphone pendant qu'il est en charge ? Et à toujours le débrancher du port USB lorsque vous recevez un message par exemple ?

A présent, jetons un coup d'œil de plus près aux données qui sont transmises du port USB même lorsque le mobile est en mode (bloqué) » charge seule « . La taille de ces données varie, dépendant de la plateforme du mobile et du système d'exploitation de l'hôte. Mais dans tous les cas, il s'agit plus que d'une » simple charge « . Comme nous l'avons découvert, ces données incluent le nom du mobile, le nom du fournisseur et le numéro de série.

Accès complet et au-delà

Vous devez sûrement penser que vous ne voyez pas où est le problème, seulement il y en a un, puisque nous avons trouvé en cherchant des informations accessibles au public qu'un fournisseur en particulier autorise beaucoup plus que ce qui est spécifié par le système.

Comment est-ce possible ?

Cela est rendu possible via un ancien système de commandes appelées commandes AT. Ces dernières ont été développées il y a quelques dizaines d'années afin de permettre les communications des modems et ordinateurs. Plus tard, elles ont été intégrées au standard du GSM et désormais sont toujours utilisées sur les smartphones.

Pour vous donner une idée de l'usage des commandes AT, laissez-moi vous donner quelques exemples que nous avons été en mesure de découvrir à la surface d'Internet : elles permettent à un hacker d'obtenir votre numéro de téléphone et de télécharger les contacts enregistrés dans la carte SIM. Ces commandes permettent d'établir un appel à n'importe quel numéro, et ce à vos frais, bien entendu. Et si vous êtes en roaming, de tels appels inattendus peuvent vite faire grimper la facture. Dépendant du vendeur, le mode du roaming peut faciliter l'accès à un hacker d'installer n'importe quel type d'applications, y compris malveillantes.

Tout ce qu'on vient de mentionner est possible, même si votre smartphone est bloqué !

En résumé, ne vous fiez pas aux apparences d'un port USB car il pourrait bien » cacher des choses « . Il s'agit d'un système qui collecte les données des appareils auxquels il est connecté, peu importe les raisons. C'est une source d'énergie bancale, tel un puissant condensateur ou un ordinateur qui installe une porte dérobée sur votre appareil. Une chose que vous ignorez jusqu'à ce que vous le branchiez.

Article de Alexey Komarov

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

Source : *Les dangers de charger la batterie de son smartphone via un port USB – Kaspersky Daily – | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.*

L'adoption de l'analyse comportementale appelée à

s’étendre

L’adoption de l’analyse comportementale appelée à s’étendre

Selon Gartner, les entreprises se tournent de plus en plus vers l'analyse comportementale pour améliorer la détection des incidents et renforcer l'efficacité de leurs SOC. De quoi pousser à une inéluctable consolidation du marché.

L'analyse comportementale – des utilisateurs comme des flux réseau ou des entités connectées à l'infrastructure – a fait une entrée remarquée sur le marché de la sécurité l'an passé. Mais selon Gartner, les solutions isolées actuellement proposées vont être rapidement appelées à s'intégrer, au point d'encourager à une consolidation des acteurs.

Dans une note d'analyse, Avivah Litan et Eric Ahlm résument la situation : « les besoins des acheteurs pour détecter les brèches de tout type vont pousser à la consolidation des systèmes de détection basés sur le comportement, tels que les systèmes d'analyse du comportement des utilisateurs et des entités (UEBA), de détection et de réponse sur les points de terminaison (EDR), et d'analyse du trafic réseau (NTA) ».

Des catégories bien distinctes

Dans la première catégorie, le cabinet mentionne par exemple Securonix, LightCyber, Exabeam et Gurucul. Le premier étant notamment utilisé par HP au sein du système de gestion des informations et des événements de sécurité (SIEM) ArcSight. Pour l'EDR, il prend pour exemples Hexis et Ziften, mais pourrait également évoquer SentinelOne, notamment. En matière de NTA, le cabinet fait référence à SS8 et Niara, mais il faut également compter avec Vectra Networks ou encore Darktrace, entre autres.

Mais voilà, comme le relèvent les deux analystes, les acheteurs de solutions de sécurité ne veulent pas seulement détecter les brèches, « mais aussi y répondre rapidement et efficacement ». S'il le fallait, l'édition 2016 de RSA Conference a fait la démonstration de cette tendance. Ce besoin doit conduire à une « collision du marché entre systèmes de détection basés sur le comportement et systèmes d'orchestration et de réaction ». Et cela parce que ni UEBA, ni EDR, ni NTA ne semble en mesure d'apporter, seul, une réponse complète aux besoins des entreprises.

Des capacités différentes

Ainsi, Avivah Litan et Eric Ahlm soulignent que la première catégorie est efficace pour identifier des compromissions de comptes utilisateurs ou des acteurs internes malveillants, mais peut montrer ses limites dans la détection des incidents impliquant des logiciels malveillants. De son côté, « l'EDR peut être efficace pour trouver les comportements mauvais sur un hôte et identifier les objets malicieux », mais plus faible lorsqu'il s'agit de mettre le doigt sur une menace interne. Enfin, les outils de NTA « peuvent être capables de trouver les conséquences de deux types d'événements, mais n'ont pas les données relatives aux utilisateurs ou aux hôtes nécessaires pour confirmer l'incident ».

Analyse comportementale : la clé de la sécurité ?

D'autres outils peuvent venir en outre compléter l'édifice, qu'il s'agisse des SIEM ou des systèmes de gestion du renseignement sur les menaces comme ceux d'Anomali, de ThreatConnect ou encore de ThreatQuotient. Au final, pour les analystes de Gartner, le marché s'avère « bruyant, chaotique et encombré », pollué notamment par des discours marketing qui s'articulent « autour des mêmes thèmes clés tels que analytique, machine learning, automatisation, et autres termes similaires, bien que leur application de ces fonctionnalités soit largement différente en ce qui concerne ce qu'ils peuvent faire dans leurs rôles spécifiques ». Bref, la confusion règne.

Des performances à démontrer

Et cela d'autant plus que, selon Gartner, les spécialistes de l'analytique appliquée à la sécurité peinent encore à faire la démonstration de la valeur de leurs solutions. Lors d'échanges, ceux-ci cherchent surtout à se différentier en évoquant l'étendue ou le volume de leurs échantillons de données, le framework analytique utilisé ou encore la technologie analytique employée – apprentissage machine, deep learning, et intelligence artificielle sont là largement mis à contribution. Las, si le cabinet voit là des « facteurs importants et des sujets de discussions divertissants », tous « échouent à constituer un différentiateur majeur » car, pour Avivah Litan et Eric Alhm, « les éditeurs devraient d'abord se concentrer sur la manière dont le recours à l'analytique rend leur technologie meilleure en termes de résultats, de manière mesurable. Par exemple, dans quelle mesure trouver des attaques inconnues est plus efficace en pourcentage avec l'analytique que chercher à trouver un logiciel malveillant inconnu sans ».

Une inéluctable consolidation

Pour autant, les deux analystes ne contestent pas la valeur intrinsèque que l'analytique apporte à la détection de brèches. Mais ils soulignent l'importance des étapes suivant la détection. D'où la convergence anticipée entre acteurs de la détection basée sur l'analytique et de l'orchestration/réaction. Et c'est peut-être là que le SIEM est appelé à jouer une nouvelle carte, pour dépasser des limites bien connues. Dès lors, pour Gartner, les acteurs de détection devaient « soit prévoir de nouer formellement des partenariats avec des acteurs du SIEM […] ou se préparer à reprendre des fonctions clés du SIEM ».

Le cabinet s'attend donc clairement à une consolidation prochaine de systèmes de détection de menaces basés sur les comportements, mais il n'exclue pas l'émergence de solutions de type plateforme dédiées à l'investigation et à la réponse aux incidents. Des solutions sur lesquelles les composant de détection et de réponse viendraient se greffer. Et n'est-ce pas justement ce que cherche à proposer un Phantom Cyber ?

Article de Valéry Marchive

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

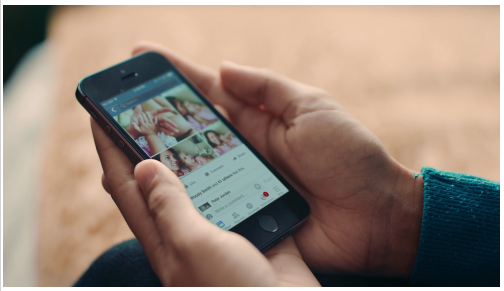
Réagissez à cet article

Source : *L'adoption de l'analyse comportementale appelée à s'étendre*

Facebook vous traque sur le Web même si vous n'êtes pas membre

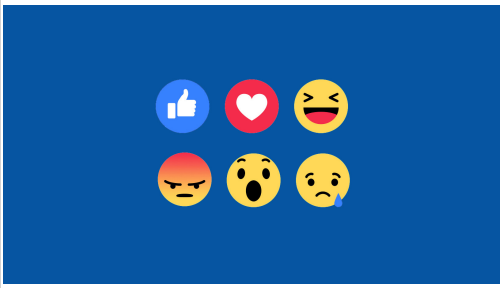
Facebook vous traque sur le Web même si vous n'êtes pas membre

Facebook devient une régie publicitaire ouverte aux sites tiers, et affichera des publicités ciblées y compris pour les internautes qui ne sont pas inscrits sur le réseau social. Il utilisera ses scripts présents sur de nombreux sites pour suivre l'internaute dans ses déplacements sur le Web, et comprendre ce qui l'intéresse.

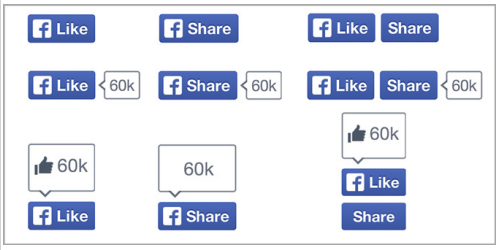


On connaît tous une ou deux personnes qui se refusent à utiliser Facebook et échappent encore et toujours aux griffes du réseau social. Mais l'empire de Mark Zuckerberg ne cesse de s'étendre et touchera bientôt même ces irréductibles qui n'ont jamais ouvert de compte sur la plateforme.

L'entreprise a annoncé qu'elle allait diffuser des annonces à tous les visiteurs de sites utilisant sa régie publicitaire Facebook Audience Network, concurrente de Google Adsense. Autrement dit, même les personnes qui ne sont pas inscrites sur Facebook et celles qui n'y sont pas connectées seront ciblées par des publicités qui, jusqu'ici, n'étaient visibles que par les personnes connectées au réseau social.
Ce n'est un secret pour personne, la force de Facebook réside dans sa capacité à récolter des données sur ses utilisateurs. Grâce à cela, il peut facilement montrer des publicités ciblées et adaptées sur mesure en fonction des préférences identifiées. Une aubaine pour les annonceurs qui ne perdent ainsi pas de temps et d'effort à diffuser tous azimuthes leurs contenus.



TRAQUER LES HABITUDES DE TOUS LES INTERNAUTES
Mais comment Facebook peut-il en faire de même avec les personnes qui ne se trouvent pas dans son réseau ? Il va utiliser plusieurs outils à sa disposition pour traquer efficacement un maximum d'internautes, comme le fait Google. Facebook va ainsi se servir de cookies, de ses propres boutons et plugins de partage affichés sur les sites, ainsi que d'autres informations collectées sur les sites tiers.
« Nos boutons et nos plugins envoient des informations de base sur les sessions de navigation des utilisateurs. Pour les non-membres de Facebook, auparavant nous ne les utilisions pas. Maintenant nous allons les utiliser pour mieux comprendre comment cibler ces personnes », assume très clairement Andrew Bosworth, vice-président de Facebook en charge des publicités et de la plateforme commerciale.



Ce dispositif permettra à Facebook de repérer les habitudes des internautes en insérant des bouts de codes dans les cookies et dans les boutons ou autres contenus « embeddés », qui permettront d'identifier l'internaute, soit directement en tant que membre de Facebook, soit par un numéro unique qui lui sera attribué. Si vous visitez régulièrement un site de cuisine, Facebook affichera des publicités pour une cocotte-minute ou une friteuse sur les autres sites que vous fréquentez, en rémunérant le site qui les affiche.

QUELLE LÉGALITÉ EN EUROPE ?
Ce changement de politique de Facebook va certainement mécontenter une partie de la communauté des internautes, y compris chez les membres qui pourront continuer à être suivis même lorsqu'ils sont déconnectés du réseau social. Elle pourrait surtout déclencher les foudres des autorités si le système est déployé en Europe.
Lorsque la justice belge avait condamné Facebook à ne plus tracer les Belges non-membres de Facebook, le réseau social s'était fait fort de crier à l'injustice, en prétendant que son cookie (le DATR) avait pour seul intérêt de lutter contre le spam. « Nous utilisons le cookie datr depuis plus de 5 ans pour sécuriser Facebook pour 1,5 milliard de personnes à travers le monde », s'était agacé le réseau social. Or six mois plus tard, Facebook prouve que les autorités avaient raison de s'inquiéter.
En France aussi, la Cnil a demandé à Facebook de ne plus tracer les internautes qui ne sont pas inscrits et connectés sur le réseau social. Avec d'autres homologues, elle avait estimé que Facebook devait « se conformer à ce jugement (belge) sur tout le territoire de l'Union européenne ».
Selon la législation européenne, il est illégal de réaliser un traitement de données personnelles à des fins commerciales, sans le consentement explicite de la personne. Or si ce consentement peut être donné à l'inscription par Facebook, il ne peut certainement pas l'être par les non-membres… [Lire la suite]

Article de Omar Belkaab

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

Source : *Facebook vous traquera sur le Web même si vous n'êtes pas membre – Business – Numerama*

Les six choses à faire pour éviter 95% des attaques informatiques

Les six choses à faire pour éviter 95% des attaques informatiques

---

La cybersécurité est essentielle, d'accord, mais par où commencer ? Pour vous aider à faire le premier pas, nous avons identifier 6 principes clés qui, lorsqu'ils sont suivis, peuvent éviter la grande majorité des attaques.

1/ FAIRE DE LA SÉCURITÉ UN PROCESS (CE N'EST PAS UN PRODUIT)

« Je dois protéger mon entreprise ? Certes. Quel produit faut-il que j'achète ? » La réflexion peut sembler naturelle. Après tout, autant faire appel à des professionnels. Le problème, c'est qu'on ne sécurise pas son entreprise en signant un chèque. La cybersécurité est avant tout une façon de penser, et passe par une organisation, par la mise en place de règles et méthodes. Elle implique de connaître son système d'information sur le bout des doigts pour en cartographier la surface d'attaque, de savoir tout ce qui est connecté (et ce qui ne doit pas l'être). Elle implique aussi de déterminer quels sont les services et les données qui sont réellement cruciaux au fonctionnement de la structure pour s'assurer que l'on concentre ses forces là où elles doivent l'être, sans s'évertuer à défendre plus que nécessaire des ressources non critiques. *« La sécurité est une composante au service du coeur de métier,* explique Eric Filiol, directeur du laboratoire de virologie et de #cryptologie opérationnelles de l'école d'ingénieurs ESIEA. *Il faut comprendre son métier et ce qui est critique. »* La stratégie doit être sensée pour que les ressources engagées (financières, humaines, temporelles) soient utilisées au mieux.

2/ PATCHER, PATCHER, PATCHER

Les révélations sur les méthodes de la NSA ou les gros titres sur les attaques contre des opérateurs d'importance vitale qui s'étalent sur des mois voire des années peuvent laisser penser que les hackers exploitent systématiquement des failles complexes et jamais référencées (appelées « zero days ») pour s'infiltrer dans un SI. Rien n'est moins vrai. Ces zero days ne sont utilisés qu'extrêmement rarement et seulement pour les cibles les plus importantes. La très grande majorité des attaques ciblent au contraire des failles bien connues et pour lesquelles existent déjà des correctifs de sécurité, souvent depuis des années. C'est pourquoi il est capital de faire systématiquement ces mises à jour (aussi bien pour le système d'exploitation que les frameworks ou les applications), et de concevoir son SI autour de cette nécessité. *« Il faut savoir que les criminels font du reserve engineering sur les patchs dès leur sortie pour exploiter les failles qu'ils corrigent. Auparavant cela leur prenait des mois, aujourd'hui ce ne sont plus que des heures,* détaille Thomas Tschersich, director of IT security chez Deutsche Telekom.*Et ils automatisent ensuite le processus pour toucher de très nombreuses cibles. »* Et ce besoin reste le même dans le cas d'un environnement de production industriel qui se doit d'être opérationnel 365 jours par an. La perception selon laquelle les environnements industriels sont fondamentalement différents des environnements de bureau est fausse et contribue à renforcer leur vulnérabilité.

3/ NE PAS SE CROIRE NON CONCERNÉ

Si les réseaux industriels sont de plus en plus visés par des attaques informatiques, c'est parce qu'ils y sont particulièrement vulnérables. La faute à l'évolution dramatique de la connectivité à Internet au cours des 20 dernières années. Lors de leur conception, il était assumé que ces systèmes ne couraient pas de risques car ils n'étaient pas visibles. Quand bien même ce fut jamais vrai, ce n'est définitivement plus le cas. Des services gratuits comme shodan.io permettent depuis des années de chercher parmi des centaines de milliers de systèmes ouverts, connectés à Internet sans aucune protection. Cela va de simples caméras de surveillance (résidentielles ou industrielles) jusqu'aux ICS qui supervisent le parc machine, que les opérateurs laissent sans protection car ils veulent pouvoir en prendre facilement le contrôle à distance. *« Il y a beaucoup de négligence et de mauvaises pratiques,* assène Frédéric Planchon, PDG de FPC Ingénierie. *Cela laisse des portes ouvertes à des malwares qui ne sont normalement pas si nocifs. »* Peu importe la taille de votre installation ou la nature de votre activité, si vous êtes vulnérables, vous serez tôt ou tard attaqué. Et ce même lorsqu'il n'y a rien à en obtenir, car de nombreux hackers agissent simplement « pour le sport ».

4/ PROTÉGER SES DONNÉES

La meilleure façon de garantir la sécurité de ses données, que ce soit contre le vol ou contre des attaques de type ransomwares, c'est de prendre les mesures adéquates en amont. Cela passe par deux axes clés : le chiffrement et la sauvegarde. Le chiffrement garantit que seuls les individus autorisés peuvent accéder aux données, même si le canal de communication ou le support de stockage est compromis. Ainsi, même en cas de vol, les dégâts restent minimaux. De son côté, la sauvegarde évite la perte de données, qu'elle soit dûe à un accident ou à un acte de malveillance. Une politique de sauvegarde rigoureuse et régulière peut faire la différence entre « plus de peur que de mal » et « la clé sous la porte ».

5/ FORMER SES TROUPES

Une vaste majorité d'attaques ont un point commun : l'erreur humaine. Un collaborateur qui ouvre le mauvais email ou clique sur le mauvais lien. Un autre qui perd son appareil ou sa clé USB. Un troisième qui laisse traîner ses identifiants de connexion (ex. post-it sur l'écran) ou les communique par erreur/inattention… La sécurité n'est pas innée, elle s'enseigne. Il est impératif de former les équipes aux bonnes pratiques à adopter et de les sensibiliser aux conséquences que la négligence peut avoir. Les rendre personnellement responsables de la protection de leurs données et appareils au travers de mesures simples peut suffire à largement diminuer les accidents.

6/ SÉCURISER AUSSI LES ACCÈS PHYSIQUES

Une #attaque informatique n'est pas forcément menée depuis l'autre bout du monde. Il faut donc s'assurer en premier lieu que le périmètre de l'entreprise est sécurisé pour limiter les accès non autorisés en interne. Car le « social engineering », qui consiste à obtenir accès à un système en trompant son interlocuteur, est au coeur de nombreuses attaques. Il suffit parfois de mettre un uniforme de réparateur, de prendre une boîte à outils et de demander poliment l'accès à un local technique pour qu'on vous ouvre. Ou de mettre un costume et de se tenir devant une porte les bras chargés de documents. *« Nous appelons ça les attaques 'femme de ménage', et cela permet de prendre le contrôle d'un serveur en 5 secondes, »* explique Eric Filiol. Autre exemple, lorsque le réseau Wi-Fi interne d'une usine, non protégé car l'accès au bâtiment est restreint, peut aussi être capté depuis le parking… Les cas de figure sont nombreux et leur exploitation bien documentée. Ces éléments doivent donc systématiquement être pris en compte.

Article de Julien BERGOUNHOUX

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

Source : *Cybersécurité : Les six choses à faire pour éviter 95% des attaques*