Quelques chiffres sur les risques du WiFi public

Quelques chiffres sur les risques du WiFi public

Aéroports, hôtels, cafés… Le WiFi public est très utilisé, mais pas sans risque. 30 % des managers ont fait les frais d'un acte cybercriminel lors d'un voyage à l'étranger, selon Kaspersky Lab.

Spécialiste des solutions de sécurité informatique, Kaspersky Lab publie les résultats d'une enquête réalisée par l'agence Toluna auprès de 11 850 salariés, cadres et dirigeants dans 23 pays, sur leur utilisation de terminaux et Internet à l'étranger. Tous ont voyagé à l'international l'an dernier, à titre professionnel ou personnel. Premier constat : 82 % ont utilisé des services WiFi gratuits, mais non sécurisés (aucune authentification n'étant nécessaire pour établir une connexion réseau), depuis un aéroport, un hôtel, un café… Or, 18 % des répondants, et 30 % des managers, ont fait les frais d'un acte cybercriminel (malware, vol de données, usurpation d'identité…) lorsqu'ils étaient à l'étranger.

Droit ou devoir de déconnexion ?

« Les businessmen assument que leurs terminaux professionnels sont plus sûrs du fait de la sécurité intégrée », a souligné l'équipe de Kaspersky Lab dans un billet de blog. Et si cela n'est pas le cas, ils considèrent que ce n'est pas leur problème. Ainsi *« un répondant sur quatre (et plus de la moitié des managers) pense qu'il est de la responsabilité de l'organisation, plutôt que de celle de la personne, de protéger les données. En effet, à leurs yeux, si les employeurs envoient du personnel à l'étranger, ils doivent accepter tous les risques de sécurité qui vont avec »*.

Si des données sont perdues ou volées durant leur voyage, la plupart des managers seraient prêts à blâmer leur département informatique. Et ce pour ne pas avoir recommandé l'utilisation de moyens de protection comme un réseau privé virtuel (VPN), des connexions SSL ou encore la désactivation du partage de fichiers lors d'une connexion WiFi… Quant au droit à la déconnexion, lorsqu'il existe, il se pratique peu. Pour 59 % des dirigeants et 45 % des managers *« intermédiaires »*, il y une attente de connexion quasi continue de la part de leur employeur.

Article original de Ariane Beky,

Réagissez à cet article

Original de l'article mis en page : Les voyageurs d'affaires ignorent les risques du WiFi public

Les géants d’internet contrôlent de plus en plus l’information

Les géants d’internet contrôlent de plus en plus l’information

Entre les médias et les lecteurs, l'information passe aujourd'hui le plus souvent par les algorithmes des géants d'internet, qui contrôlent de fait ce flux et une bonne partie des revenus qu'il génère. Au point de susciter des inquiétudes.

« Ces 18 derniers mois, (ces géants d'internet) qui avaient jusqu'ici une relation distante avec le journalisme sont devenus des acteurs dominants de l'écosystème de l'information », résume le Tow Center for Digital Journalism de l'Université américaine de Columbia, dans une étude publiée en juin 2016. Beaucoup proposent aux éditeurs de presse de publier directement leur contenu sur leurs plateformes, à l'instar des canaux Instant Articles de Facebook ou Discover de Snapchat, et sont*« désormais directement impliqués dans tous les aspects du journalisme »*, fait valoir l'étude. La plupart des médias nouent des partenariats avec ces nouveaux acteurs de l'information pour maintenir ou développer leur exposition sur les moteurs de recherche et les réseaux sociaux, mais les perspectives financières restent incertaines.
« Il y a des gens qui font de l'argent sur internet, mais pas les médias, qu'ils soient tous supports ou uniquement en ligne », affirme une autre étude, du centre indépendant Pew Research Center, publiée mi-juin. Elle souligne ainsi qu'en 2015, 65% des revenus publicitaires en ligne étaient concentrés par cinq places fortes du web, Google, Facebook, Microsoft, Yahoo et Twitter, une proportion en hausse par rapport à 2014 (61%). Tout comme le modèle économique, c'est aussi le contenu et sa hiérarchie qui leur échappent, soumis au filtre des algorithmes. *« L'impact que ces sociétés technologiques ont sur le secteur du journalisme va bien au-delà de l'aspect financier, jusqu'à ses composantes les plus essentielles »*, considère l'institut Pew.
Désormais, les géants d'internet *« supplantent les choix et les objectifs des sites d'information et leurs substituent (les leurs) »*, affirme l'étude. Si certains y voient l'occasion d'une démocratisation de l'information, d'autres s'inquiètent d'une altération de sa qualité. *« Vous n'avez aucune idée de ce que les gens vont voir et il se peut tout à fait que (ce soit) quelque chose d'assez léger plutôt que des informations majeures »*, prévient Dan Kennedy, professeur de journalisme à l'Université Northeastern.

Le secret des algorithmes

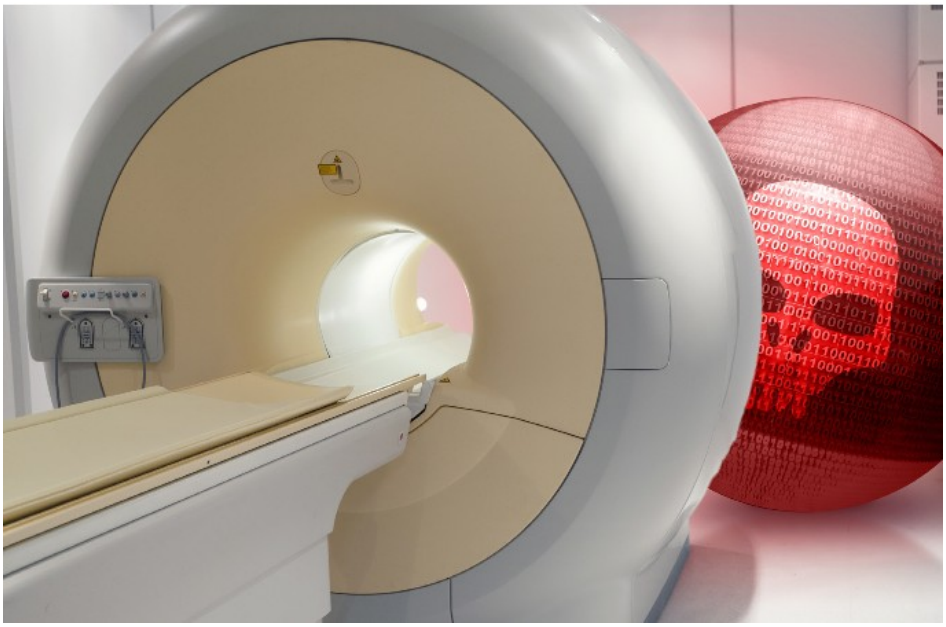
Une étude réalisée par Nic Newman du Reuters Institute a fait état de*« préoccupations liées à la personnalisation des informations et une sélection algorithmique qui pourraient passer à côté de nouvelles importantes et de points de vue différents »*, selon le blog de son auteur. Mais *« les jeunes préfèrent les algorithmes aux éditeurs »* qui organisent l'information, constate-t-il. Ce pouvoir croissant des incontournables d'internet a attiré l'attention début mai lorsque le site d'information Gizmodo a accusé, témoignages à l'appui, Facebook d'avoir manipulé son fil de tendances. Après enquête interne, le plus grand réseau social du monde a conclu qu'il n'y avait pas eu de démarche concertée ou de manipulation, mais s'est engagé à préserver la neutralité de sa plateforme.
« Nous sommes une entreprise technologique, pas un média », a expliqué récemment la directrice d'exploitation de Facebook, Sheryl Sandberg, lors d'une table ronde à Washington. *« Nous n'essayons pas de recruter des journalistes ou de rédiger des nouvelles »*, a-t-elle martelé. Pour autant, l'intervention humaine reste nécessaire, selon elle, *« parce que sans cela, tous les jours à midi, le déjeuner serait une tendance »*. Même si la hiérarchisation des informations est largement automatisée sur ces plateformes, les programmes qui régissent ce processus sont bien rédigés par des humains qui opèrent, pour ce faire, des choix. Cela pose, dès lors,*« des questions quant à la transparence »* de l'ensemble, souligne Nicholas Diakopoulos, professeur de journalisme à l'université du Maryland. *« Il pourrait être intéressant de savoir de quelles données se nourrit le logiciel ou quels sites il suit »*, estime l'universitaire, pour qui *« il faut réfléchir à des normes de transparence ».*
Une étude publiée l'an dernier a révélé que le trafic des principaux sites d'information en provenance de Facebook avait chuté de 32% après une modification des algorithmes du réseau social. *« Il est vrai que Facebook peut faire décoller ou tuer un site d'information selon la façon dont il calibre son algorithme »*, reconnaît Nikki Usher, professeure de nouveaux médias à l'Université George Washington. *« D'un autre côté, les médias n'ont jamais eu à rendre de compte sur les décisions qu'ils prenaient »* en matière éditoriale, fait-elle valoir.

Article original de Joël Ignasse

Réagissez à cet article

Original de l'article mis en page : Les géants d'internet contrôlent de plus en plus l'information – Sciencesetavenir.fr

Risques d’infection dans le médical des Objets Connectés



Risques d’infection dans le médical des Objets Connectés

La faible sécurité des équipements de santé connectés entraîne la résurgence des vieux virus comme Conficker.

Un des problèmes de la montée en puissance de l'Internet des objets ? La sécurité.
Spécialistes, constructeurs, éditeurs répètent à longueur de conférences qu'il faut absolument que l'IoT soit « secure by design ». Entendez par là que les capteurs, le protocole de communication, la plateforme de traitement de l'information, l'architecture soient sécurisés dès leur conception.
Oui mais voilà, c'est sans compter sur le fameux héritage technique. Le monde de la santé rentre typiquement dans ce cadre et tout particulièrement les outils médicaux connectés. On pense ici aux IRM, scanners, radios, ou pompes à insuline. Ces équipements sont de plus en plus ciblés par les cyberattaquants, car ils sont moins bien protégés que des PC ou des serveurs.
Conséquence de cette faible sécurité, les vieux virus se rappellent aux bons souvenirs des administrateurs et des RSSI. Un rapport de la société de sécurité TrapX Labs, disséquant une attaque baptisée MEDJACK.2, montre que les attaques utilisent des malwares comme networm32.kido.ib ou le ver Conficker en complément de menaces plus sophistiquées. Moshe Ben Simon, co-fondateur de TrapX, résume bien ce paradoxe : « *un loup intelligent déguisé avec des vieux habits de mouton* ».

Mise en place de backdoors

Premier constat, les équipements médicaux connectés à Internet fonctionnent avec des versions de Windows non corrigées allant de XP (qui n'est plus supporté par Microsoft) aux versions 7 et 8. Des cibles de choix pour les anciens virus. « *Ces vieux virus sont utilisés avec des malwares (en l'occurrence MEDJACK.2) plus élaborés pour installer des backdoors dans l'établissement de santé et ensuite mener une campagne par exfiltration de données, voire se transformer en #ransomware* », souligne le rapport.
Les échantillons de Conficker que les experts de la société de sécurité ont analysé, montrent que le ver a été modifié pour avoir une meilleure capacité à se déplacer dans un réseau. Pire, son évolution fait qu'il est devenu indétectable pour les équipements médicaux. Dans son enquête auprès de 3 hôpitaux, TrapX relève qu'aucune alerte n'a été remontée par les établissements sur la présence de Conficker. A son apogée en 2009, Conficker avait infecté entre 9 et 15 millions d'ordinateurs. Il avait, comme capacité, de casser les mots de passe, d'enrôler les PC dans des botnets, etc. La version actuelle est diffusée par phishing envoyé aux personnels de l'hôpital.

Les données patients : la ruée vers l'or

L'objectif de ces attaques : obtenir les dossiers patients. Des informations très demandées sur le Dark Web et affichant une forte valeur marchande au marché noir. « *Les cybercriminels peuvent voler l'identité d'un patient pour se faire rembourser par les assurances des traitements coûteux et, en plus, revendre ces traitements au marché noir* ». TrapX estime qu'un dossier médical se monnaye entre 10 et 20 dollars sur le marché, contre 5 dollars pour une information financière. En début de semaine, on apprenait le vol de 9,3 millions de données de santé de citoyens américains. Le calcul est vite fait…
Article original de Jacques Cheminat

Réagissez à cet article

Original de l’article mis en page : Sécurité : Conficker revient infecter l’IoT médical

---

Cybersécurité : êtes-vous bien protégé?

Cybersécurité : êtes-vous bien protégé?

De nos jours, impossible d'imaginer travailler dans le secteur des valeurs mobilières sans système informatique. Mais avec cet incontournable outil viennent plusieurs risques, qui peuvent faire un tort considérable aux conseillers et à leurs clients.

« Ces dommages peuvent nuire à la réputation d'un cabinet, l'exposer à des pertes financières et perturber gravement ses activités », prévient l'Association canadienne des courtiers de fonds mutuels (ACFM) dans un bulletin sur la cybersécurité publié la semaine dernière.
Selon des sondages réalisés aux États-Unis en 2011 et 2014 par le Financial Industry Regulatory Authority (FINRA), le secteur des valeurs mobilières est exposé à trois menaces de cybersécurité principales :
1. Les pirates informatiques qui infiltrent les systèmes d'une entreprise;
2. Les initiés qui compromettent les données d'un cabinet ou de ses clients;
3. Les risques opérationnels.

QUE FAIRE?
Pour se prémunir contre ces menaces, l'ACFM suggère à ses membres de se doter d'un cadre de cybersécurité, adapté à la taille de leur cabinet, en cinq étapes :
1. Identifier les biens qui doivent être protégés, de même que les menaces et les risques à leur égard;
2. Protéger ces biens à l'aide des mesures appropriées;
3. Détecter les intrusions et les infractions à la sécurité;
4. Intervenir s'il se produit un évènement de cybersécurité potentiel;
5. Évaluer l'incident et améliorer les mesures de sécurité à la lueur des évènements.
Pour mener à bien ce plan, l'ACFM propose de nombreuses pistes d'action que les cabinets peuvent suivre selon l'envergure de leurs activités.
Parmi elles, assurer la sécurité physique des lieux, notamment contre les menaces humaines, mais aussi environnementales, s'avère un incontournable, tout comme la mise en place de mesures de protection des systèmes (pare-feu récents, chiffrement des réseaux sans fil, processus de sauvegarde et de récupération, protocoles de mots de passe, etc.).
L'Association suggère également de se doter d'une procédure d'enquête sur le personnel, les sous-traitants et les fournisseurs, ainsi que d'instaurer une politique de cybersécurité et une formation continue obligatoire à ce sujet. Former une équipe d'intervention en cas d'incident peut aussi s'avérer une bonne idée.
Il importe de tester régulièrement la vulnérabilité des systèmes pour en détecter les failles et mieux les corriger. En cas d'incident, il est essentiel de le divulguer, rappelle l'ACFM, notamment au commissaire à la protection de la vie privée dans certains cas.
Finalement, il existe des assurances spécifiquement pour les menaces de cybersécurité.
Article original de conseiller.ca

Réagissez à cet article

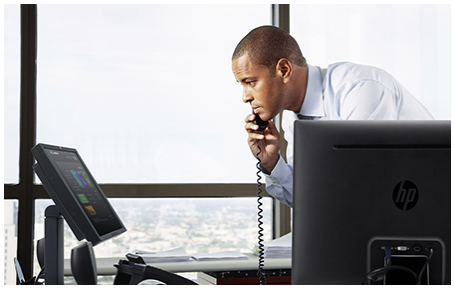
Original de l’article mis en page : Cybersécurité : êtes-vous bien protégé? | Conseiller

---

Protection contre la Fuite des données, priorité pour les entreprises ?

Protection contre la Fuite des données, priorité pour les entreprises ?

Prévention des pertes de données des collaborateurs mobiles. Quand la mobilité oblige à la Data Loss Prevention.



La mobilité est à la fois un besoin et un défi pour les entreprises qui se battent pour créer une force de travail réellement fluide et entièrement digitale. Aujourd'hui, presque tous les collaborateurs travaillent avec un ou plusieurs périphériques mobiles contenant des informations d'entreprise, qu'il s'agisse d'un téléphone mobile, d'un ordinateur portable ou d'une tablette. L'un des premiers défis qui en découlent pour la direction informatique tient au fait que l'accès à distance aux données et aux e-mails se fait, par nature, « hors » du périmètre de l'entreprise, et qu'il est par conséquent très difficile de s'en protéger. La multitude des périphériques utilisés, en elle-même, complique la surveillance et le suivi des données d'entreprise consultées, partagées ou utilisées.

Data Loss Prevention : se concentrer sur les données

L'une des approches, choisie dans certaines entreprises, consiste à intégrer ces périphériques à une stratégie d'environnement de travail en BYOD. Les utilisateurs peuvent choisir le périphérique, le système d'exploitation et la version de leur choix, puisqu'il s'agit de leur propre périphérique. Malheureusement, cette approche peut en réalité créer des problèmes supplémentaires de sécurité et de DLP (prévention des pertes de données). En effet, de nombreux utilisateurs n'apprécient pas (voire interdisent) que leur employeur gère et/ou contrôle leur périphérique, pire encore, d'y installer des logiciels professionnels comme les programmes d'antivirus et de **VPN**.

Par conséquent, pour réussir, la stratégie de protection des données doit se concentrer sur la sécurisation des données uniquement, quel que soit le périphérique ou le mode d'utilisation. Dans un environnement d'entreprise, une grande majorité des données sensibles transitent dans les e-mails et leurs pièces jointes. Ainsi, une stratégie de protection des données réussie doit chercher à gérer et contrôler la passerelle par laquelle transitent les données, à savoir, ici, le compte d'e-mail d'entreprise.

Autre option : implémenter une suite d'outils de gestion de la sécurité mobile, ce qui permet de placer des mécanismes de sécurité sur la passerelle d'e-mail, et d'autoriser la création de règles de sécurité pour surveiller et contrôler la façon dont les informations d'entreprise sont traitées sur chaque périphérique.

Data Loss Prevention : Stratégie DLP tridimensionnelle

Une stratégie « DLP tridimensionnelle », surveille et contrôle le contenu transféré via un périphérique sur la base de critères précis. Par exemple, on peut limiter l'accès au contenu ou aux fichiers depuis le compte e-mail d'entreprise en fonction du pays, puisque les utilisateurs qui voyagent avec leur périphérique sont susceptibles d'accéder aux données et aux systèmes sur des réseaux Wi-Fi non sécurisés. Il est également possible de contrôler le contenu sur la base des mots clés qui figurent dans les e-mails (comme des numéros de sécurité sociale ou des numéros de contrat), afin d'interdire les pièces jointes ou le contenu incluant ce type d'information sur les périphériques mobiles. Comme les pièces jointes d'e-mail contiennent la majorité des informations sensibles transmises d'un périphérique à un autre, ce point est crucial lorsqu'il s'agit de protéger l'utilisation des périphériques dans l'environnement de travail. La troisième dimension est la surveillance du contexte, qui permet d'identifier et d'interdire le contenu pour des expéditeurs/destinataires spécifiques.

Ce type de considération permet de limiter les risques liés aux pertes de données et aux problèmes de sécurité pour cette partie des activités professionnelles Bien que cette approche ne suffise pas à contrôler et à sécuriser entièrement les banques de données d'une entreprise, la sécurité mobile va jouer un rôle de plus en plus vital pour la réussite des stratégies complètes de protection des données, au fur et à mesure que davantage de périphériques s'intègrent à nos habitudes de travail. (Par Eran Livne, Product Manager LANDESK)

Article original de Damien Bancal

Réagissez à cet article

Original de l’article mis en page : Data Loss Prevention – Data Security BreachData Security Breach

---

Bulletin sécurité du 13 juin 2016 du CERTFR

Bulletin sécurité du 13 juin 2016 du CERTFR

La S . G . D . S . N (Agence nationale de la sécurité des systèmes d'information) met régulièrement à notre disposition ses avis et alertes sur de nouvelles vulnérabilités détectées.
Voici le dernier bulletin d'actualité : CERTFR-2016-ACT-024

1 – Sonde de détection d'intrusions réseau – Comment implémenter les points de mesure ?

Une sonde de détection d'intrusions réseau est un équipement passif, elle ne s'insère donc pas en coupure sur un flux de production. Il est donc nécessaire, pour implémenter les points de mesure définis, d'assurer une duplication en temps réel de l'activité réseau à analyser.
Deux techniques différentes existent pour dupliquer un trafic réseau : la première, généralement appelée « port miroir », est logicielle, et s'appuie sur les équipements réseau déjà en place ; la seconde, généralement appelée « tap », s'appuie sur des boîtiers matériels dédiés à cette fonction. Nous allons voir les avantages et les inconvénients de ces deux solutions.

Port miroir

La majorité des commutateurs du marché permettent de configurer une recopie logicielle de tout ou partie du trafic sur un ou plusieurs ports physiques dédiés. Le port miroir peut être un choix peu coûteux, si les équipements existants d'un réseau disposent déjà de cette fonctionnalité.
Toutefois, la recopie logicielle du trafic n'est pas sans risque. En effet, si l'équipement atteint sa limite de capacité sur ses fonctions « principales » (comme par exemple : la commutation de paquets, le routage, etc.), des fonctions annexes comme la recopie de paquets peuvent être dégradées, entraînant dans un tel cas des pertes sur l'activité à superviser.
La recopie logicielle peut également altérer le signal, car les couches basses réseau sont analysées et traitées par les commutateurs. Cette technique ne garantit donc pas la recopie de l'intégralité du trafic commuté sur le réseau de production. Étant donné qu'un seul paquet perdu sur un flux volumineux peut empêcher l'analyse par la sonde ou l'évader, il est primordial de considérer ce problème et de superviser la charge des commutateurs, si cette technique est mise en place.
La mise en place d'un port miroir sur un équipement du réseau augmente aussi la consommation de ressources : cela peut donc également dégrader le réseau de production. Une attention particulière doit être apportée au fond de panier, car le débit total commuté par l'équipement est décuplé.
D'autre part, il est important d'intégrer les ports miroirs dans les procédures d'exploitation : lors du remplacement d'un équipement ou d'un changement de configuration, il faut s'assurer que la recopie est toujours opérationnelle et qu'il n'y a pas de perte d'une partie des flux.
Une erreur de configuration peut également autoriser des communications depuis le réseau de duplication, voire même entre la sonde et le réseau de production.
Par contre, la mise en oeuvre d'un port miroir peut se faire sans interruption du réseau en production à superviser, à condition de disposer de suffisamment de ports physiques libres au niveau des commutateurs où les points de mesure sont effectués.

TAP

Un TAP garantit la recopie stricte du signal reçu : aucune analyse des couches au-delà de celle physique n'est réalisée. Le signal est régénéré électriquement pour des TAP cuivre, et la lumière est divisée sur deux chemins pour les TAP fibre. La mise en oeuvre d'une duplication de trafic sur un réseau en production nécessite une brève interruption du lien à superviser : celle-ci correspond au temps nécessaire pour placer le boîtier TAP en « coupure », c'est-à-dire sur le chemin de câble.
Pour les TAP alimentés, un défaut d'alimentation arrête la duplication, mais le TAP reste passant pour le lien coupé, moyennant généralement une microcoupure de quelques millisecondes.
Pour les TAP fibre, une partie de la lumière incidente étant réfléchie et l'autre réfractée, le signal est affaibli en fonction de proportions précisées dans la documentation du TAP.
Contrairement au port miroir, le TAP garantit également l'isolation entre le réseau de production et le réseau de détection.
Le prix d'un boîtier de duplication de trafic (TAP) varie entre une centaine d'euros et un millier, en fonction du type de média à dupliquer.

Conclusion

En conclusion, bien que ces deux méthodes permettent la duplication du trafic, il est conseillé de privilégier l'utilisation d'équipement dédié afin de garantir la séparation entre le réseau de production et le réseau de détection, ainsi qu'une recopie à l'identique des flux réseau.

2 – Rappel des avis émis

Dans la période du 06 au 12 juin 2016, le CERT-FR a émis les publications suivantes :

- CERTFR-2016-AVI-190 : Vulnérabilité dans VLC Media Player
- CERTFR-2016-AVI-191 : Multiples vulnérabilités dans Google Android (Nexus)
- CERTFR-2016-AVI-192 : Multiples vulnérabilités dans Wireshark
- CERTFR-2016-AVI-193 : Multiples vulnérabilités dans Mozilla Firefox
- CERTFR-2016-AVI-194 : Multiples vulnérabilités dans les produits Symantec
- CERTFR-2016-AVI-195 : Multiples vulnérabilités dans PHP
- CERTFR-2016-AVI-196 : Multiples vulnérabilités dans SCADA les produits Siemens
- CERTFR-2016-AVI-197 : Vulnérabilité dans Citrix Xenserver
- CERTFR-2016-AVI-198 : Multiples vulnérabilités dans les produits VMware
- CERTFR-2016-AVI-199 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

---

Réagissez à cet article

Original de l’article mis en page : Bulletin d’actualité CERTFR-2016-ACT-024

Alerte ! Un nouveau malware infecte plus de 850.000 terminaux Android

Alerte ! Un nouveau malware infecte plus de 850.000 terminaux Android

Particulièrement actif en Asie, ce malware est notamment parvenu à se frayer un chemin jusqu'au Google Play Store.

Android a pourtant initié depuis plusieurs années un grand nettoyage de son Google Play Store et a revu les règles et procédures d'accès des applications, mais certains malwares parviennent encore à contourner les garde-fous mis en place. Trend Micro alerte ainsi sur une famille de malware baptisés Godless, qui sont distribués entre autres via le Google Play Store et des applications malveillantes.

Trend Micro explique que Godless dispose de plusieurs exploits lui permettant d'affecter les appareils Android, ce qui le rend potentiellement dangereux pour tous les téléphones disposant d'une version antérieure à Android 5.1.
Le malware est généralement distribué via des applications proposées sur le Google Play store. La présence de celui-ci n'est pas détectée, car lorsque l'application est uploadée vers le playstore, elle ne contient aucun code malveillant à proprement parler. Mais une fois l'application installée, celle-ci va se mettre à jour et télécharger alors le « payload » contenant l'exploit de la vulnérabilité choisie par les cybercriminels.
Le malware tentera d'exploiter celle-ci pour acquérir les droits root sur la machine : il s'en sert par la suite pour installer des applications ou pour diffuser des publicités.
La France est relativement épargnée par ce malware, qui est principalement actif en Asie, notamment en Inde et en Indonésie. Mais Trend Micro estime que plus de 850.000 terminaux Android ont été infectés par ce malware à travers le monde. Outre les applications qui parviennent à le distribuer sur le Google Play Store officiel, celui-ci est évidemment diffusé sur les magasins d'application tiers.
Article original de Louis Adam

Réagissez à cet article

Original de l'article mis en page : Godless : un nouveau malware qui infecte plus de 850.000 terminaux Android – ZDNet

Pourquoi protéger votre connexion sur le Wifi gratuit ?

Pourquoi protéger votre connexion sur le Wifi gratuit ?

Quelques trucs et astuces simples, mais efficaces, pour protéger votre ordinateur, téléphone et tablette.

Wifi gratuit ? Votre meilleur ennemi ! En général, les réseaux Wi-Fi que l'on trouve dans les lieux publics ne sont pas bien protégés. Ils se basent souvent sur des protocoles de chiffrement trop simples ou parfois pas chiffrés du tout. Les pirates peuvent ainsi accéder à chacune des informations que vous envoyez sur Internet : e-mails importants, données de carte bancaire, voire données d'identification permettant d'accéder à votre réseau d'entreprise. Une fois que les pirates disposent de ces renseignements, ils peuvent accéder à vos systèmes en votre nom, diffuser des programmes malveillants, ou facilement installer des logiciels infectés sur votre ordinateur si le partage de fichiers a été activé.

Quelques bons gestes à respecter face à un Wifi gratuit

D'abord, utilisez un réseau privé virtuel (VPN). Un VPN est indispensable lorsque vous accédez à une connexion non sécurisée, comme un point d'accès wifi. Même si un pirate réussit à se placer en plein milieu de votre connexion, les données qui s'y trouvent seront chiffrées, donc illisibles. Mails, mots de passe, ou simplement ce que vous visitez ne seront pas lisibles. J'utilise moi même plusieurs dizaines de VPN différents. Je peux vous proposer de tester Hide My Ass, ou encore VyprVPN. Un test de VPN disponibles pour votre ordinateur, tablette ou encore smartphone dans cet article. Dernier conseil, même si vous ne vous êtes pas activement connecté à un réseau, le matériel wifi équipant votre ordinateur, votre téléphone portable, votre tablette continuent de transmettre des informations. Bref, désactivez la fonctionnalité wifi si vous ne l'utilisez pas.

Activez l'option « Toujours utiliser HTTPS » sur les sites Web que vous visitez fréquemment ou qui nécessitent de saisir des données d'identification. Les pirates ne savent que trop bien que les utilisateurs utilisent les mêmes identifiants et mots de passe pour les forums, leur banque ou leur réseau d'entreprise.

Pour finir, lorsque vous vous connectez à Internet dans un lieu public, via un Wifi gratuit il est peu probable que vous souhaitiez partager quoi que ce soit. Dans ce cas, vous pouvez désactiver les options de partage dans les préférences système. (Kaspersky)

Article original de Damien Bancal

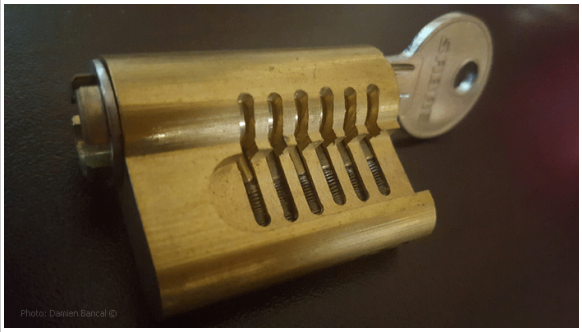
Réagissez à cet article

Original de l'article mis en page : Wifi gratuit, protégez votre connexion – Data Security Breach

Comment devenir maître dans l’art de protéger sa vie privée sur le net ?

Comment devenir maître dans l’art de protéger sa vie privée sur le net ?

Vol de ses données personnelles – Plusieurs sources ont révélé récemment la mise en vente sur le web de plus de 117 millions de profils d'utilisateurs LinkedIn dérobés en 2012. Ce type d'actualité rappelle que personne n'est à l'abri d'un vol de ses données personnelles qui risquent d'être utilisées à des fins illicites. Cette question est d'autant plus cruciale à l'heure où le nombre de logiciels malveillants, ransomwares et autres virus explose. Aujourd'hui, 67 % des Français sont soucieux quant à la protection de leurs informations personnelles sur internet et 83 % d'entre eux sont hostiles à la conservation de ces données (Source : Institut CSA).



Malgré cette méfiance, dans un monde où l'utilisation d'Internet est devenue omniprésente, les utilisateurs ont tendance à exposer très facilement leur vie privée et leurs données personnelles – parfois par paresse ou par mégarde, mais souvent par manque d'information. Il existe cependant des moyens simples et efficaces de limiter ces risques.
Michal Salat, Threat Intelligence Manager chez Avast, commente : « ***Les sphères privées et professionnelles se fondent de plus en plus, poussant fréquemment les utilisateurs à accéder à leurs plateformes de travail depuis des terminaux personnels ou à utiliser leurs appareils professionnels à la maison par exemple. Or, en adoptant ces comportements, les internautes exposent davantage leurs données personnelles.***«

Vol de ses données personnelles
Pour éviter que cela n'arrive, les utilisateurs doivent d'abord se protéger des menaces extérieures à leur appareil en commençant par créer un mot de passe ou un code PIN sur les écrans et les applications mobiles, limitant ainsi l'accès aux données en cas de perte ou de vol. Mais encore faut-il qu'il soit suffisamment compliqué pour ne pas être déchiffré trop facilement. C'est pourquoi il est recommandé d'utiliser des mots de passes complexes – combinant lettres, chiffres, caractères spéciaux et majuscules – et qui ne reprennent pas non plus des informations personnelles facilement accessibles en ligne, telle que la date de naissance ou le prénom de ses enfants. Il est également important de changer ses codes régulièrement.
Il faut garder en tête que les cybercriminels sont à l'affût de la moindre faille à exploiter pour récolter des gains et cherchent très souvent à récupérer des informations bancaires. C'est pourquoi les internautes doivent à tout prix éviter de sauvegarder leurs coordonnées bancaires dans leurs terminaux, quels qu'ils soient. A titre d'exemple, beaucoup d'utilisateurs PayPal ont perdu de grosses sommes d'argent lorsque des hackers ont réussi à se connecter à leurs PC via un compte TeamViewer piraté et se sont servi des identifiants enregistrés pour transférer l'argent depuis les comptes PayPal.

Les pirates parviennent à créer des e-mails d'hameçonnage très sophistiqués notamment grâce à la collecte d'informations personnelles publiques disponibles sur le web – accessibles sur les réseaux sociaux par exemple. Il est alors essentiel pour l'utilisateur de poster le moins d'informations possibles sur Internet ou de s'assurer que celles-ci sont en mode privé. Il est également crucial de supprimer ses comptes s'ils ne sont plus utilisés, car bien qu'abandonnés, ces profils restent en ligne et des personnes malintentionnées pourraient usurper l'identité de l'internaute ou nuire à sa réputation en ligne en utilisant des informations sensibles contre lui.
La protection de la vie privée et des données personnelles (vol de ses données personnelles) implique une modification du comportement des internautes à commencer par de meilleures méthodes de gestion de mots de passe, une vigilance accrue sur leur utilisation d'Internet et des informations personnelles partagées publiquement – comme sur les réseaux sociaux. Au-delà des bonnes pratiques, il existe des solutions qui répondent aux problématiques liées à la vie privée. Cependant face aux menaces, il n'appartient qu'à nous de nous discipliner et de tout mettre en œuvre pour protéger nos données personnelles.

Article original de Damien Bancal

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

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Devenir maître dans l'art de protéger sa vie privée sur le net – Data Security BreachData Security Breach

Attention ! Le Cloud est espionné

	Attention ! Le Cloud est espionné

Les agences gouvernementales peuvent exploiter la 'fonctionnalité' d'écoute des hyperviseurs pour récupérer des données depuis le cloud. Si vous n'êtes pas propriétaire du hardware, vous n'êtes pas propriétaire des données, selon une étude de Bitdefender.

L'éditeur de solutions de sécurité informatique affirme que les agences gouvernementales peuvent exploiter la 'fonctionnalité' d'écoute des hyperviseurs pour récupérer des données depuis le cloud. Les révélations de l'affaire Snowden sur les capacités d'interception des données de la part de la NSA et de ses agences partenaires ont incité les propriétaires d'infrastructures et les fournisseurs de services, ainsi que les utilisateurs, à s'assurer que leurs données sont échangées sans encourir de risque de confidentialité et qu'elles sont stockées sous forme chiffrée. Régulièrement, les chercheurs s'attaquent à des protocoles très utilisés ou à leur mode de mise en œuvre. Des failles sont ainsi découvertes de manière récurrente et corrigées à plus ou moins brèves échéances, comme dans le cas de vulnérabilités bien connues telles que Heartbleed ou Logjam, qui ont entraîné le déploiement massif de correctifs à une échelle jusque-là inédite.
Mais les entreprises, et par conséquent, leurs clients, sont-elles vraiment protégées une fois que ces failles sont corrigées ? Existe-t-il des méthodes dissimulées et plus ou moins légales que les organismes d'État et certaines grandes entreprises bien informées seraient susceptibles d'utiliser pour passer outre les protocoles TLS / SSL, censés protéger les échanges d'informations ? Bref, espionnage dans le Cloud possible ?
Le 26 mai 2016, lors de la Conférence HITB à Amsterdam, Radu Caragea, Chercheur en sécurité des Bitdefender Labs, a démontré lors d'un POC (preuve de concept), que la communication protégée peut être déchiffrée en temps réel, en utilisant une technique qui ne laisse pratiquement aucune empreinte et qui reste invisible pour presque tout le monde, sauf peut-être pour des auditeurs de sécurité particulièrement vigilants.

Espionnage dans le cloud : Quelles conséquences pour votre sécurité ?
Cette attaque permet à un fournisseur de services cloud mal intentionné (ou sur lequel on a fait pression pour qu'il donne des accès à des agences gouvernementales) de récupérer les clés TLS utilisées pour chiffrer chaque session de communication entre votre serveur virtualisé et vos clients (même si vous utilisez Perfect Forward Secrecy !). Si vous êtes un DSI et que votre entreprise externalise son infrastructure de virtualisation auprès d'un prestataire de service, considérez que toutes les informations circulant entre vous et vos utilisateurs ont pu être déchiffrées et lues pendant une durée indéterminée.
Il est impossible de savoir dans quelle mesure vos communications ont pu être compromises et pendant combien de temps, puisque cette technique ne laisse aucune trace anormale derrière elle. Les banques et les entreprises qui gèrent des dossiers de propriété intellectuelle ou des informations personnelles, ainsi que les institutions gouvernementales sont les secteurs susceptibles d'être particulièrement touchés par cette faille.

Espionnage dans le Cloud : Premières découvertes
Cette nouvelle technique, surnommée TeLeScope, a été développée par l'éditeur dans le cadre de ses recherches et permet à un tiers d'écouter les communications chiffrées avec le protocole TLS, entre l'utilisateur final et une instance virtualisée d'un serveur. Cette technique n'est opérationnelle qu'avec les environnements virtualisés fonctionnant au-dessus de l'hyperviseur. Ces infrastructures sont extrêmement répandues et sont proposées par les géants de l'industrie tels qu'Amazon, Google, Microsoft ou DigitalOcean, pour ne citer qu'eux. Si la plupart des experts de l'industrie s'accordent pour dire que la virtualisation est l'avenir, aussi bien en termes de stockage, que de déplacement et de traitement de gros volumes de données, ce type de solutions fait déjà partie du quotidien de nombreuses entreprises.
Plutôt que d'exploiter une faille dans le protocole TLS, cette nouvelle technique d'attaque repose sur l'extraction des clés TLS au niveau de l'hyperviseur par une inspection intelligente de la mémoire. Même si l'accès aux ressources virtuelles de la VM est une pratique déjà connue (accéder au disque dur de la machine, par exemple), le déchiffrement en temps réel du trafic TLS, sans mettre en pause la machine virtuelle de manière flagrante et visible, n'avait jamais été réalisé jusqu'alors.
La découverte de ce vecteur d'attaque a été possible en recherchant un moyen de surveiller des activités malveillantes depuis le réseau de honeypots de l'éditeur, sans altérer la machine et sans que les pirates puissent comprendre qu'ils sont surveillés. Un administrateur réseau ayant accès à l'hyperviseur d'un serveur hôte pourrait surveiller, exfiltrer et monétiser toutes les informations circulant depuis et vers le client : adresses e-mail, transactions bancaires, conversations, documents professionnels confidentiels, photos personnelles et autres données privées.

Espionnage dans le Cloud : Comment cela fonctionne-t-il ?
Normalement, la récupération des clés à partir de la mémoire d'une machine virtuelle nécessiterait de mettre en pause la VM et de décharger le contenu de sa mémoire sur un fichier. Ces deux processus sont intrusifs et visibles par le propriétaire de la VM (de plus ils enfreignent le SLA – Service Level Agreement). L'approche des chercheurs repose sur les mécanismes de Live Migration, disponibles au sein des hyperviseurs modernes, qui nous permettent de réduire le nombre de pages nécessaire pour le vidage de la mémoire de l'ensemble de la RAM, à celles modifiées lors de l'établissement d'une liaison TLS.
« ***Au lieu de mettre la machine en pause (ce qui entrainerait une latence notable) et de réaliser un vidage complet de la mémoire, nous avons développé une technique de différentiel de la mémoire qui utilise des fonctions de base déjà présentes dans les technologies de l'hyperviseur,*** » explique Radu Caragea. « ***Ensuite, bien que cela permette de réduire le volume de vidage mémoire de giga-octets à méga-octets, le temps nécessaire pour écrire une telle quantité de données sur un espace de stockage reste non négligeable (de l'ordre de quelques millisecondes) et c'est pourquoi nous montrons comment 'déguiser ' le processus pour le faire passer pour une latence du réseau, sans qu'il soit nécessaire de stopper la machine.*** »

Atténuation des risques
L'attaque TeLeScope n'exploite pas de faille lors de l'implémentation du protocole TLS et ne tente pas de contourner le niveau de chiffrement de l'implémentation TLS via des attaques par repli (downgrade attacks). Au lieu de cela, elle exploite une caractéristique de l'hyperviseur pour exfiltrer les clés utilisées par le protocole pour chiffrer la session. Notre POC révèle un écart fondamental qui ne peut être corrigé ou atténué sans réécrire les bibliothèques de cryptographie qui sont déjà en cours d'utilisation. La seule solution à ce jour est, en premier lieu, de bloquer l'accès à l'hyperviseur – en exécutant votre propre hardware à l'intérieur de votre propre infrastructure.
Article original de Damien BANCAL

Réagissez à cet article

Original de l'article mis en page : ZATAZ Espionnage dans le Cloud – ZATAZ