# Enquête sur l’algo le plus flippant de Facebook

| | |
|---|---|
| | **Enquête sur l’algo le plus flippant de Facebook** |

**Si la section « Vous connaissez peut-être » vous faisait parfois flipper en vous proposant des profils précis et éloignés de vos réseaux habituels, vous n'avez encore rien vu.**

La section « Vous connaissez peut-être » (« People you may know ») de Facebook est une source inépuisable de spéculations. Cette fonction, en apparence sympathique puisqu'elle nous propose d'ajouter de nouveaux amis, semble détenir des informations très personnelles sur chacun d'entre nous.

• Une journaliste de la rédaction s'est ainsi vu proposer un flirt dont elle n'avait pas noté le téléphone dans son portable ;

• un autre collègue s'est vu proposer un pote qu'il n'a pas revu depuis 10 ans et qui venait de lui envoyer un mail ;

• une autre enfin, sa femme de ménage, dont elle a le numéro de téléphone dans son portable, mais avec laquelle elle n'a jamais eu aucune interaction en ligne.

Beaucoup ont aussi vu apparaître des gens rencontrés sur des applis de rencontre comme Tinder ou Grindr. Plutôt embarrassant, non ?

## Folles rumeurs

Entre nous, les mots de « magie noire » et « espionnage » sont prononcés. Sur Internet, les rumeurs les plus folles circulent sur la façon dont cet algorithme plutôt intrusif fonctionnerait.

• Il existerait un « profil fantôme » de chacun d'entre nous, pré-rempli et automatiquement activé dès notre inscription.

C'est la théorie d'un utilisateur de Reddit. Il raconte avoir créé un profil anonyme avec un mail jamais utilisé et s'être vu proposer plein de contacts connus.

• A Rue89, on en formule une autre pour se faire peur : Facebook nous proposerait aussi les personnes qui nous « stalkent » (espionnent en ligne) ou que nous avons récemment « stalkées ».

Je découvre que cette rumeur existe déjà, et que beaucoup d'utilisateurs y croient dur comme fer. Facebook l'a toujours démentie.

• Dans le même genre, la sérieuse BBC affirmait, via des témoignages concordant et une société de sécurité informatique, que Facebook se connectait à des applications type Tinder ou Grindr pour vous faire des suggestions d'amis.

Un journaliste du Huffington Post a fait la même hypothèse. Ce que le réseau social a nié avec force.

Fabrice Epelboin, spécialiste des médias sociaux et entrepreneur du Web, croit les dires de Facebook, comme Vincent Glad :

*« Ce serait très dangereux économiquement. Facebook n'est pas une société idiote, elle prend des risques calculés. »*

*Pour lui, l'explication est beaucoup plus simple :*

*« Quand on "date" quelqu'un sur Tinder, on lui donne bien son numéro avant, non ? Facebook se connecte en fait à votre répertoire. »*

*Ah bon ?*

## *Un aspirateur à données, via votre téléphone*

*On résume. Il faut imaginer l'algorithme de Facebook comme un aspirateur à données géant.*

*Visages et Facebook — Pixabay/CC0*

*Dans un article du Washington Post, qui fait référence en la matière, il est expliqué que l'algorithme de « Vous connaissez peut-être » est basé sur la « science des réseaux ».*

*En définissant les réseaux auxquels on appartient, Facebook calcule nos chances de connaître telle ou telle personne. Et il peut même prédire nos futures amitiés. Un peu de probabilités et c'est dans la boîte.*

*« Ce n'est pas de la magie, mais juste des mathématiques très pointues », apprend-on.*

*Avertissement de Messenger, dont la « synchronisation » permet au contact de « se connecter sur Facebook »*

*En fonction des amis que l'on a, de nos interactions plus ou moins fortes et fréquentes avec eux, de l'endroit où on vit, des lieux où on a étudié et travaillé, l'algorithme fait ses calculs. Il tente aussi de définir les personnes « clés » de votre réseau, celles qui vous présentent aux autres. Enfin, il utilise votre géolocalisation, ce qui a probablement mené ce lundi à l'arrestation du voleur de la voiture d'un internaute, qui est apparu dans ses suggestions d'amis.*

*Surtout, depuis qu'il est arrivé sur votre mobile, via les applis Facebook et Messenger, le réseau social a un tas d'autres informations à mettre sous la dent de leur algo : vos contacts téléphoniques et vos mails.*

*Vous l'avez autorisé, probablement sans en avoir conscience, au moment de l'installation de l'une et/ou l'autre application.*

## *Le test ultime : le Nokia de Xavier de La Porte*

*Comme c'était un jour de pluie, j'ai voulu tester la puissance de cet algorithme qui marche donc sur deux pieds :*

*• La « science des réseaux » ;*

*• des tonnes de données « scrapées » de notre mobile notamment.*

*Je décide de créer un compte avec un numéro de téléphone et avec un faux nom. Le mien est déjà lié à un compte, donc Facebook le refuse.*

*En effet, il est interdit, en théorie, de créer un faux compte ou de doublonner, selon sa politique de « l'identité réelle » — les personnes transgenres en savent malheureusement quelque chose.*

*Il y a une personne dans ces bureaux qui n'a pas lié son compte Facebook à son numéro. J'ai nommé : Xavier de La Porte. Il possède un charmant Nokia cassé sur le dessus.*

*Le téléphone de Xavier, bolide de la protection des données*

*« J'ai 20 contacts dessus, seulement ma famille et mes amis proches », jure-t-il.*

*Il n'est évidemment pas question d'applications quelconques. Avec le numéro de Xavier, Facebook accepte la création du compte de « Mathilde Machin », 21 ans.*

*« Mathilde Machin », couverture très discrète*

*Et là, un truc vraiment effrayant arrive : des dizaines de contacts sont proposés, amis, famille, collègues de bureau, sources de Xavier. Ils ne sont pas dans son répertoire. Et ne sont pas non plus tous amis avec lui sur Facebook. A partir de là, deux hypothèses s'offrent à moi :*

*• Son compte a été lié un jour à ce numéro de téléphone, et Facebook se rend compte qu'il s'agit de la même personne. Il lui propose logiquement d'ajouter les amis du compte de Xavier.*

*Mais, Facebook refuse d'ouvrir deux comptes avec le même mail ou le même numéro. Il s'agirait d'une sorte de faille de sécurité, puisque le téléphone sert justement à sécuriser votre compte. Et cela n'expliquerait pas pourquoi Mathilde Machin se voit proposer des personnes qui ne sont pas dans les amis Facebook de Xavier.*

*• Les contacts proposés sont ceux qui possèdent le numéro de Xavier dans leur répertoire. Et qui ont donné à Facebook l'autorisation de scraper leurs données. Ce qui veut dire que l'algorithme de suggestion est tellement puissant qu'il réussit, en quelques secondes, à « inverser » la recherche.*

*Facebook, après s'être creusé les méninges un moment — c'est un peu technique —, me confirme la dernière hypothèse.*

*C'est vertigineux. Mais inscrit noir sur blanc dans les flippantes **« Confidentialités et conditions »** de Facebook. Qui autorisent l'application à utiliser les « données que vous importez ou synchronisez de votre appareil », type répertoire, mais aussi :*

*« Les contenus et informations que **les autres personnes** fournissent lorsqu'elles ont recours à nos services notamment des informations vous concernant, par exemple **lorsqu'elles partagent une photo de vous, vous envoient un message ou encore lorsqu'elles téléchargent, synchronisent ou importent vos coordonnées.** »*

## *Un algo gourmand*

*Facebook m'explique donc que l'algorithme se nourrit aussi des données que les autres ont sur vous (votre mail, votre numéro). Pour le dire autrement, quelqu'un qui a votre contact et l'importe dans son appli Facebook va probablement apparaître dans vos suggestions d'amis. C'est aussi fou que les rumeurs. Facebook insiste sur le fait que :*

*• Le processus est transparent ;*

*• l'algorithme, gentil, ne cherche qu'à vous faire retrouver vos amis et échanger avec eux ;*

*• « Facebook ne possède pas et n'utilise pas » votre numéro de téléphone, il s'en sert pour mettre en relation des profils ;*

*• et les paramètres de votre compte sont personnalisables.*

*Un samedi soir, vous êtes tombée amoureuse d'un ami d'ami. Le lendemain, vous demandez à l'ami commun son numéro. Vous hésitez à envoyer un message, vous bloquez plusieurs jours. Sachez donc que ce mec, à qui vous n'avez rien envoyé, vous a peut-être déjà vu apparaître dans « Vous connaissez peut-être ». Et qu'il a déjà peur de vous.*

*Article original de Alice Maruani Rue 89*

---

*Réagissez à cet article*

Original de l’article mis en page : Enquête sur l’algo le plus flippant de Facebook – Rue89 – L’Obs

---

# 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

---

# 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 entraînerait 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

---

# Faut-il que les robots et les Intelligences Artificielles payent des cotisations sociales ?


---

**Comment financer la sécurité sociale lorsque les employés mis aux chômage par les robots ne versent plus de cotisations ? Pour Mady Delvaux, auteure dun projet de résolution qui sera débattu au Parlement européen, il est temps de faire cotiser les robots.**

Faut-il reconnaître un droit spécifique des robots ? La commission du Parlement européen en charge des affaires juridiques (JURI), qui a établi un groupe de travail sur la robotique et l'intelligence artificielle, le pense. Elle prépare actuellement un rapport rédigé par l'eurodéputée luxembourgeoise Mady Delvaux (S&D), déposé le 31 mai dernier, qui demande à la Commission d'élaborer une proposition de directive sur des règles de droit civil sur la robotique. Le texte n'a pas encore été adopté en commission JURI, et devrait être débattu en séance plénière du Parlement européen le 12 décembre prochain.
Parmi ses dispositions, la proposition de résolution invite l'exécutif à réfléchir à la manière dont le modèle social européen peut évoluer, alors que « le développement de la robotique et de l'intelligence artificielle pourrait avoir pour conséquence l'accomplissement par des robots d'une grande partie des tâches autrefois dévolues aux êtres humains ».


Mady Delvaux, députée luxembourgeoise au Parlement Européen (groupe Socialistes & Démocrates)

**UNE SITUATION PRÉOCCUPANTE POUR L'AVENIR DE L'EMPLOI ET LA VIABILITÉ DES RÉGIMES DE SÉCURITÉ SOCIALE**
Actuellement, l'essentiel du financement de sécurité sociale, qu'il s'agisse du socle de base de l'assurance santé, de la retraite ou de l'assurance chômage, est assis sur une ponction d'une partie conséquente des salaires versés aux employés. C'est le salarié chargé de faire l'inventaire dans un hypermarché qui cotise pour être protégé le jour où son employeur jugera plus rentable de faire faire l'inventaire par un robot intelligent.
Paradoxe des paradoxes, l'employeur lui-même complète les cotisations par ses propres versements qui sont proportionnels aux salaires versés, ce qui fait qu'il doit cotiser lorsqu'il continue à payer l'humain (et cotiser d'autant plus lorsqu'il le paye bien), mais qu'il n'a plus rien à payer lorsqu'il le remplace par un robot.

**DÉCLARER LES GAINS DE PRODUCTIVITÉ POUR MIEUX LES TAXER ?**
Dès lors, si l'on considère que les emplois deviennent plus rapides à détruire qu'à créer dans une société toute obnubilée par l'ubérisation et les gains de productivité, cette « hypothèse s'avère préoccupante pour l'avenir de l'emploi et la viabilité des régimes de sécurité sociale, si l'assiette de contributions actuelle est maintenue », s'inquiète le rapport Delvaux.
L'eurodéputée luxembourgeoise propose donc à la Commission « d'envisager la nécessité de définir des exigences de notification de la part des entreprises sur l'étendue et la part de la contribution de la robotique et de l'intelligence artificielle à leurs résultats financiers, à des fins de fiscalité et de calcul des cotisations de sécurité sociale ». Dit autrement, les entreprises seraient taxées sur la part de leur chiffre d'affaires imputable aux productions automatisées, pour alimenter le pot commun de la sécurité sociale.

**UN REVENU UNIVERSEL DE BASE FINANCÉ PAR LES ROBOTS**
« Eu égard aux effets potentiels, sur le marché du travail, de la robotique et de l'intelligence artificielle, il convient d'envisager sérieusement l'instauration d'un revenu universel de base », ose même la députée socialiste, alors que la Suisse vient de rejeter la proposition par référendum, et qu'en France le débat est souhaité par Manuel Valls mais sans cesse repoussé.
Mais comment calculer les cotisations que les entreprises devraient reverser ? La question est extrêmement complexe et n'est pas aidée par l'annexe du rapport, où il est simplement précisé que les entreprises devraient être tenues de déclarer à l'administration :
• Le nombre de « robots intelligents » qu'elles utilisent ;
• Les économies réalisées en cotisations de sécurité sociale grâce à l'utilisation de la robotique en lieu et place du personnel humain ;
• Une évaluation du montant et de la proportion des recettes de l'entreprise qui résultent de l'utilisation de la robotique et de l'intelligence artificielle.

Or comment savoir, par exemple, si un rendez-vous enregistré dans l'agenda par Siri ou Cortana est un gain de productivité imposable au titre de la robotisation, parce qu'il aurait pu être inscrit par un(e) secrétaire, ou directement par le patron ou le cadre à travers un logiciel plus ou moins automatisé ? La fiscalité traditionnelle est déjà d'une complexité impressionnante, mais ce n'est rien en comparaison de ce que propose le rapport. Et pourtant, il faudra bien y réfléchir et trouver des solutions. À moins que la crise que nous traversons soit véritablement conjoncturelle et que se créent rapidement de nouveaux emplois durables difficilement remplaçables à court ou moyen terme. « Des emplois qui répondent à des besoins d'humanité », comme le défend le roboticien sud-coréen Jeakweon Han.
Crédit photo de la une : Stephen Chin
Article original de Guillaume Champeau

Réagissez à cet article

# Original de l'article mis en page : Faut-il que les robots et les IA payent des cotisations sociales ? – Politique – Numerama

# Les Smart TV, nouvelle cible des ransomwares ?

| | |
|---|---|
| | Les Smart TV, nouvelle cible des ransomwares ? |

**Si les ransomwares sont chaque jour plus nombreux à venir « pourrir » le quotidien des particuliers comme des entreprises, voilà que ces derniers ne s'en prennent plus seulement aux ordinateurs et aux smartphones. En effet, Frantic Locker s'attaque également aux Smart TV.**

# Frantic Locker, le rançongiciel qui bloque les Smart TV

Alors que les ransomwares font de nombreuses victimes, le spécialiste de la sécurité informatique Trend Micro révèle que le rançongiciel Frantic Locker s'en prend désormais aux Smart TV.

Présent sur le marché depuis avril 2015, il n'a cessé d'évoluer et un grand nombre de variantes différentes ont développées lui permettant de s'ouvrir à de nouveaux horizons.

Ainsi, dernièrement, Frantic Locker, aussi connu sous le nom FLocker, est diffusé via des campagnes de spam par SMS ou bien par un site web préalablement piégé. Bien évidemment, l'objectif des cybercriminels est toujours le même : faire télécharger des applications malveillantes par l'intermédiaire de clics sur des liens frauduleux.

Mais là où le rançongiciel étonne, c'est qu'il ne bloque pas que les ordinateurs et les smartphones tournant sous Android. En effet, les cybercriminels ont fait des Smart TV leurs nouvelles victimes. Autrement dit, de nombreux téléspectateurs peuvent désormais vivre la mauvaise expérience de voir leur télévision laisser apparaître un message informant qu'une rançon de 200 dollars (en cartes-cadeaux iTunes) était nécessaire pour débloquer leur appareil.

Si tel n'est pas le cas, l'écran restera figé.

# Un type d'attaque qui épargne encore certains pays

Depuis son lancement au printemps 2015, le rançongiciel Frantic Locker n'a cessé de se propager au point de cibler un nombre croissant de terminaux.

Concernant les Smart TV, toutes sont potentiellement vulnérables au ransomware FLocker mais selon Trend Micro, il s'autodétruirait en s'installant sur les Smart TV localisées dans plusieurs pays de l'Est de l'Europe comme la Russie, l'Ukraine, la Biélorussie, la Géorgie, la Bulgarie, l'Arménie, l'Azerbaïdjan, le Kazakhstan ou encore la Hongrie.

Article original de Jérôme DAJOUX

---

Réagissez à cet article

Original de l'article mis en page : Les Smart TV, nouvelle cible des ransomwares ?

# Patch Tuesday Juin 2016 – Data Security Breach

**Patch tuesday juin – 16 bulletins de Microsoft pour corriger plus de 40 vulnérabilités pour le mois de juin 2016. Flash souffre d'un 0Day très dangereux.**

Le Patch Tuesday juin 2016 arrive avec un cortège de 16 bulletins publiés par Microsoft pour résoudre plus de 40 vulnérabilités (CVE) différentes. Cela porte à 81 le nombre de bulletins pour les 6 premiers mois, ce qui laisse augurer plus de 160 bulletins d'ici fin 2016, un nouveau record pour la dernière décennie en termes de correctifs.
Votre attention doit se porter en priorité sur Adobe Flash. En effet, Adobe a reconnu qu'une vulnérabilité (CVE-2016-4171) au sein du lecteur Flash actuel est en cours d'exploitation en aveugle, si bien que l'éditeur a reporté le patch mensuel pour Adobe Flash. Dans son avis de sécurité APSA16-03. Adobe promet ce patch pour d'ici la fin de la semaine. Surveillez attentivement sa diffusion et déployez-le dès que possible. Si l'outil EMET est installé sur vos systèmes, vous êtes protégés. Pour information, c'est le troisième mois d'affilée qu'une faille 0-Day est découverte dans Flash, ce qui en fait le logiciel certainement le plus ciblé sur les points d'extrémité de votre entreprise.
Ce mois-ci, un ensemble de bulletins à la fois pour les serveurs et les systèmes clients va occuper cette semaine toute l'équipe IT qui devra sécuriser les systèmes de l'entreprise.

**Vulnérabilité critique**
La vulnérabilité la plus intéressante côté serveur est résolue dans le bulletin MS16-071. Ce dernier corrige une vulnérabilité critique unique sur le serveur DNS de Microsoft. En cas d'exploitation réussie, l'attaquant déclenche une exécution de code à distance (RCE) sur le serveur, ce qui est extrêmement fâcheux pour un service aussi critique que DNS. Les entreprises qui exécutent leur serveur DNS sur la même machine que leur serveur Active Directory doivent être doublement conscientes du danger que représente cette vulnérabilité.
Côté client, la vulnérabilité la plus importante est résolue dans le bulletin MS16-070 Elle corrige plusieurs problèmes dans Microsoft Office. Principale vulnérabilité associée au format Microsoft Word RTF, CVE-2016-0025 déclenche une exécution RCE au profit de l'attaquant. Le format RTF pouvant être utilisé pour attaquer via le volet d'aperçu d'Outlook, la faille peut être déclenchée à l'aide d'un simple email et sans interaction avec l'utilisateur.
Côté navigateur Web, les bulletins MS16-063 pour Internet Explorer, MS16-068 pour Edge et MS16-069 pour Javascript sur Windows Vista traitent plusieurs vulnérabilités RCE critiques qui sont exploitables lors d'une simple navigation sur le Web. Ces vulnérabilités constituent un vecteur d'attaque privilégié pour les cybercriminels et nous vous recommandons de les corriger dans les 7 prochains jours.
Les autres vulnérabilités concernées par ce Patch Tuesday juin sont toutes classées comme importantes. Elles sont généralement exploitées pour élever des privilèges une fois qu'un intrus est parvenu à exécuter du code sur la machine et sont donc associées avec une exécution de code à distance comme décrit ci-dessus. L'exception est MS16-076 qui résout une faille unique dans Windows Netlogon pouvant fournir une exécution RCE à l'attaquant. Sa gravité est moindre qu'une vulnérabilité RCE normale parce l'attaquant devra dans un premier temps prendre le contrôle du serveur Active Directory.

**Deux autres vulnérabilités côté serveur dans le patch tuesday juin**
Une élévation de privilèges sur le composant du serveur SMB résolue dans le bulletin MS16-075
Une faille dans Microsoft Exchange résolue dans le bulletin MS16-079 entraînant aussi une élévation de privilèges, certains étant liés au patch Oracle dans la bibliothèque Outside-in.
En résumé, il s'agit d'un Patch Tuesday relativement classique mais avec une menace 0-Day connue qui nécessite de surveiller impérativement la publication de la prochaine mise à jour de Flash. Corrigez les autres problèmes en fonction de vos priorités habituelles, mais faites particulièrement attention à la vulnérabilité qui affecte le serveur DNS et qui va forcément susciter des comportements indésirables. (*Wolfgang Kandek, CTO de Qualys).*

Article original de Damien Bancal

---

Réagissez à cet article

Original de l'article mis en page : Patch Tuesday Juin 2016 – Data Security Breach

---

# Si j'attrape le con qui a fait sauter le pont !

Si j'attrape le con qui a fait sauter le pont !

---

**Des difficultés à vous connecter à l'Internet et à vos applications préférées, lundi ? Pas d'inquiétude, un ingénieur informatique s'est trompé dans les files !**
Plus possible de se connecter à Internet ? Non, ce n'est pas une blague. Un seul homme, un peu distrait, a réussi à mettre en carafe une partie de l'Internet Européen. Une panne au niveau du réseau Tier 1 du fournisseur suédois Telia. Cette société et son Tier 1 ne sont rien d'autre qu'une partie de l'Internet backbone. Bref, les gros tuyaux qui permettent de faire voyager d'énormes volumes de trafic de données. Selon le journal Britannique *The Register*, la panne est signée par un ingénieur informatique qui s'est planté dans la configuration d'un des routeurs de Telia. Bilan, les données prévues pour l'Europe sont parties se promener en Asie, et plus précisément à Hong Kong. Telia s'est depuis excusée. Bref, le Cloud n'a pas fini d'être notre meilleur ennemi.
Article original de Damien Bancal

---

Réagissez à cet article

Original de l'article mis en page : ZATAZ Si j'attrape le con qui a fait sauter le pont ! – ZATAZ

---

# La double authentification de Google contournée par des hackers

La double authentification de Google contournée par des hackers

**Alors que la double authentification semblait être la meilleure solution pour protéger les données personnelles des internautes, voilà que celle de Google a réussi à être contournée par des pirates. Autrement dit, les spécialistes de la sécurité vont encore devoir se creuser la tête pour trouver encore mieux !**

## La double authentification plombée par des pirates ?

Puisque la double identification implique qu'un utilisateur saisisse un mot de passe puis qu'il confirme son identité en saisissant un code préalablement reçu par SMS afin de pouvoir accéder à ses comptes, elle semblait être une solution fiable pour bien protéger les données des internautes.

Mais ça, c'était avant puisque des pirates ont réussi à contourner la double authentification de Google pour accéder aux comptes d'utilisateurs tiers.

Pour ce faire, les hackers ont mis en place une méthode plutôt astucieuse. En effet, s'ils disposent de l'adresse mail et du mot de passe, ils se font passer pour la firme de Mountain View, expliquent qu'une activité suspecte a été repérée et invitent l'utilisateur à renvoyer le code de sécurité qui leur a été envoyé.

Sans le savoir, les utilisateurs fournissent alors la clé de l'ultime protection aux pirates qui ont désormais le temps de commettre tous les actes malveillants qui désirent.

## Une porte d'entrée vers les terminaux mobiles des utilisateurs ?

En s'offrant un accès aux comptes de messagerie des internautes, les pirates s'offrent une vraie porte d'entrée vers les terminaux mobiles de leurs propriétaires.

En effet, s'ils contrôlent le compte mail de leurs victimes, ils pourront facilement envoyer des mails sur Gmail incluant des pièces jointes frauduleuses qui peuvent être des applications malveillantes. Si le mail est ouvert depuis le mobile, le terminal sera alors automatiquement infecté.

Autrement dit, le hacker pourra avoir un accès complet à l'ensemble des données qu'il contient. Incontestablement, la double authentification a donc ses limites…

Article original de Jérôme DAJOUX

---

Réagissez à cet article

Original de l’article mis en page : La double authentification de Google contournée par des hackers

---

# Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?

Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?

---

**Pour Nicolas Reys de la société de conseil en gestion des risques Control Risks, la question doit être soulevée en conseil d'administration.**

L'ancien directeur du FBI Robert Mueller déclarait en 2014: « il y a seulement deux types d'entreprises: celles qui ont été piratés et celles qui le seront un jour. » Ce message devient de plus en plus réel. L'attaque récente sur le principal fournisseur de services de messagerie de paiements pour les institutions financières SWIFT nous rappelle que même les organisations considérées les plus sûres ne sont pas infaillibles et que maintenant les cyberattaques font désormais partie intégrante du paysage du risque des entreprises modernes. Selon une étude récente, 1.673 brèches de données ont exposé plus de 707 millions de données diverses au cours de l'année 2015, à travers le monde. Une autre étude relève que 90% des grandes entreprises et 74% des petites et moyennes entreprises dans le monde ont subi une brèche de sécurité.

**Peut être très coûteux**

De nombreux dirigeants considèrent toujours la réponse à une cyberattaque comme un problème purement technique et non stratégique. Pourtant la fréquence et l'ampleur croissante des cyberattaques, ainsi que l'intérêt grandissant que les partenaires commerciaux et les autorités portent à la cybersécurité, exigent d'élever le problème au rang des conseils d'administration. Certes, le lexique associé aux cyberattaques peut être intimidant pour les chefs d'entreprises, des termes tels que « centre de commandement et de contrôle », « numéro de port TCP » et « injection SQL » peuvent laisser entendre qu'une cyber intrusion est un problème informatique et donc ne concernant pas le comité de direction. Toutefois, quel qu'en soit sa nature, ce type d'événement peut être très coûteux et une réponse mal gérée est susceptible d'augmenter de manière significative son impact commercial et opérationnel. L'Institut Ponemon estime que le coût moyen d'une fuite de données est de 3,79 millions de dollars par entreprise victime; en augmentation de 23% depuis 2013.

**Préjudice de réputation**

A l'extrémité de ce spectre, le distributeur américain Target, qui a subi une énorme perte de données clients en 2013, estime que le coût total de cette attaque s'est élevé à 162 millions de dollars. Un montant supplémentaire de 90 millions ayant par ailleurs été couvert par les assureurs du détaillant. Mais surtout, la marque a subi un préjudice de réputation considérable et Target a vu son rythme de croissance ralentir suite à cette crise. Il est donc possible que l'impact total sur l'entreprise sera encore plus significatif à moyen terme. D'ailleurs le PDG et le responsable de la sécurité des systèmes d'information (RSSI) de Target ont été licenciés à la suite de cet événement. Bien que comprendre les dimensions techniques de ce type de crise reste crucial pour les résoudre, il faut absolument prendre en compte les implications opérationnelles et commerciales associées aux cyberattaques.

Les gestionnaires de crise au sein de l'entreprise doivent s'interroger sur au moins trois points : « quel est l'impact opérationnel immédiat sur l'entreprise de cette attaque et avec quelle rapidité pouvons-nous revenir en ligne? Quelle est notre responsabilité juridique? Avons-nous un plan de communication en place? ». Le département informatique d'une entreprise est normalement en mesure de répondre à l'incident technique et de fournir les informations sur les accès ouverts, ce qui a été volé et ce qu'il faudra faire pour reconnecter les systèmes. Mais les informaticiens ont rarement l'expérience ou le mandat pour répondre aux questions de gestion opérationnelle qu'une cyberattaque suscite.

**Brèches souvent détectées par des tiers**

D'autant que, les « cyberattaques » peuvent rapidement prendre des proportions médiatiques mal maîtrisées puisque Mandiant relève que 53% des brèches de sécurité informatique sont détectées par des tiers plutôt que par les victimes.

Comment se protéger? D'abord en comprenant les capacités et motivations des acteurs prenant pour cible votre entreprise afin de formuler un plan de gestion de crise adapté et proportionné, envisageant les scénarios de crises les plus probables ainsi que les plus dangereux pour votre entreprise. Il est ainsi souhaitable d'établir avant une cyberattaque, un plan de gestion de crise et des procédures bien documenté. Assurez-vous que la réponse à l'incident technique soit complète et s'accompagne d'un plan de gestion commerciale et opérationnelle. Vérifiez donc que tous les acteurs principaux de l'entreprise connaissent ce plan et qu'ils peuvent rapidement l'actionner. Testez son fonctionnement en vous exerçant dans des conditions réelles, et posez-vous les questions suivantes: Tout le monde peut-il être contacté? Connaissent-ils leurs rôles et responsabilités face à une telle crise? Enfin soyez prêts, à vous procurer le soutien de spécialiste en gestion de crise pour vous aider si vous ne disposez pas des capacités techniques, juridiques, de communications, ou de gestion de crises nécessaires en interne.

Les attaques cybercriminelles ont doublé entre 2014 et 2015, il n'est donc plus possible d'ignorer la menace. Même si vous êtes une entreprise bien protégée, une cyberattaque a toute les chances de vous affecter dans un futur proche. La question n'est déjà plus « quand aura lieu une attaque? », mais plutôt « êtes-vous prêts à réagir? »

Nicolas Reys de la société de conseil en gestion des risques Control Risks.

Article original de Challenges.fr

Réagissez à cet article

Original de l'article mis en page : Dirigeants, êtes-vous prêts à réagir en cas de cyberattaque?

# Techniques et astuces pour la

# robustesse de vos mots de passe

| | |
|---|---|
| | **Techniques et astuces pour la robustesse de vos mots de passe** |

**Les experts en cybersécurité ont tendance à être quelque peu cyniques envers les utilisateurs « lambda », particulièrement lorsqu'il s'agit du choix des mots de passe. Cependant, selon certains experts en sécurité informatique au sein du CyLab, l'Institut Security & Privacy de l'Université de Carnegie Mellon, les utilisateurs ordinaires ne semblent pas être aussi stupides qu'il n'y paraît. En effet les erreurs commises peuvent être classées en 4 catégories spécifiques. Le travail de sensibilisation nécessaire ne devrait pas être une tâche insurmontable.**

La méthodologie de CyLab est la suivante : montrer aux gens des mots de passe par paires, et leur demander lesquels leur semblent les plus robustes. Ensuite, établir une corrélation entre leurs réponses et l'efficacité effective de ces derniers en utilisant *les méthodes les plus actuelles pour craquer les mots de passe*. Au final, sur 75 paires, les participants en ont correctement sélectionné 59. Il s'agit de 79%, soit en pratique un « B ».

Il est vrai que l'échantillon des 165 utilisateurs du CyLab est certainement un peu plus technique que d'autres utilisateurs : ils ont été recrutés en ligne via le système du Turc Mécanique d'Amazon. De plus, CyLab ne dit pas en substance que tous les utilisateurs atteindront ce score, mais seulement que certains peuvent y arriver. Enfin, pour conclure, ces scores ne sont pas alarmants.

Les personnes sondées par CyLab savaient que des mots de passe sont robustes lorsque :

• Les majuscules sont utilisées au milieu du mot, plutôt qu'au début.
• Des chiffres et des symboles sont situés au milieu du mot plutôt qu'à la fin.
• Des séquences de chiffres aléatoires sont insérées à la place d'autres plus évidentes, telles que l'année en cours par exemple.
• Des noms sont ajoutés, différents des traditionnels prénoms et noms.
• Des noms faisant parties de la vie privée ne sont pas utilisés, tels que les prénoms de vos enfants.
• Des mots faisant référence de manière évidente au site ou au compte que vous êtes en train de protéger ne sont pas utilisés.

Bien sûr, il en reste 21% qui n'ont pas réussi à faire la distinction. Cela laisse en effet de belles opportunités **aux cybercriminels pour craquer vos mots de passe**. Quelles ont donc été les plus grosses erreurs commises ? :

1. **Les participants ont ajouté des chiffres à leurs mots de passe, en plus des lettres, en pensant les renforcer**. Dommage ! Les hackers savent bien que les internautes très souvent rajoutent à la fin des chiffres, du coup « brooklynqy » est plus sécurisé que « brooklyn16 ».
2. **Les participants ont pensé que le fait de changer tout simplement des lettres en chiffres rendrait leurs mots de passe plus robuste.** Dommage ! Les craqueurs de mots de passe « exploitent de plus en plus la tendance des utilisateurs à faire des substitutions prévisibles », ainsi « punk4life » n'est pas plus sûr que « punkforlife ».
3. **Les participants ont surestimé la sécurité procurée par les séquences présentes au niveau de leur clavier.**Dommage ! Les hackers de nos jours recherchent très rapidement les séquences des claviers telles que « qwertyuiop », tout comme d'autres patterns classiques, et pas seulement à base de mots.
4. **Les participants ont mal appréhendé la popularité de certains mots ou de certaines phrases.** Selon le CyLab, par exemple, les utilisateurs ont pensé que « ieatkale88 » et « iloveyou88 » étaient équivalent d'un point de vue sécurité. Pas vraiment : les craqueurs de mots de passe ont besoin de plus d'un milliard de tentatives en plus pour en venir à bout de « ilovekale ». Il est plus sûr de choisir un mot isolé rare plutôt qu'une phrase intégrant « iloveyou » or « ilove ». Les mots de passe utilisant le mot « love » sont incroyablement répandus …ce qui est plutôt une bonne intention si vous n'êtes pas responsable de la cybersécurité d'un site.

Qu'est ce qui pourrait aider les utilisateurs pour éviter les mauvaises stratégies de choix des mots de passe ? Selon l'auteur de l'étude :

*Une méthode qui semble être très efficace pour assister les utilisateurs dans l'évaluation de leurs mot de passe, vis-à-vis des pratiques courantes, est de leur fournir des feedbacks ciblés et explicites pendant la phase de création. Les calculateurs actuels de la force d'un mot de passe indiquent simplement aux utilisateurs si un mot de passe est faible ou fort, mais ne mentionne pas les raisons.*

*Les futurs travaux dans ce domaine pourraient s'inspirer d'une récente étude qui montrait la possibilité pour les utilisateurs de finir automatiquement le mot de passe partiel qu'ils viennent de taper … et pourrait également se baser sur une autre étude utilisant des arguments de motivation ou encore la pression de collègues pour inciter les utilisateurs à créer des mots de passe plus robustes.*

*Article original de Sophos France*

---

*Réagissez à cet article*

Original de l’article mis en page : Robustesse des mots de passes : techniques et astuces