# 12 % des entreprises belges victimes d’attaques informatique…| Le Net Expert Informatique


## 12 % des entreprises belges victimes d’attaques informatique…

**Quelque 12% des PME belges ont déjà été confrontées au moins une fois à une attaque par déni de service, également appelée DDoS, suivies de près (11%) par les PME plus petites ou unipersonnelles.**

Les entreprises de plus grande taille obtiennent, quant à elles, un résultat légèrement meilleur, avec 9%, ressort-il mercredi d'une étude de Kaspersky Lab, société spécialisée dans la sécurité des systèmes d'information. Au niveau mondial, un quart des attaques a entraîné la perte de données sensibles.

De telles attaques visent à rendre un serveur, un service ou une infrastructure indisponibles en surchargeant la bande passante du serveur ou en accaparant ses ressources jusqu'à épuisement.

Le coût pour tout rétablir peut aller jusqu'à 367.000 euros. «En moyenne, une attaque DDoS coûte aux organisations plus de 40.000 euros en factures de restauration. Les grandes entreprises dépensent des montants encore supérieurs à la récupération après une perturbation externe ou attaque de cyber-espionnage. L'investissement moyen après une attaque DDoS s'élève ainsi à environ 367.000 euros contre les 546.000 euros dépensés en moyenne par ces entreprises pour se remettre d'autres formes d'attaques», détaille l'étude 'Corporate IT Security Risks Survey', réalisée par Kaspersky Lab et B2B International auprès de 5.500 entreprises à travers le monde.

Au niveau mondial, 9% des attaques qui paralysent un service durent de deux jours à une semaine et, dans 7% des cas, ce type d'attaque dure plusieurs semaines ou davantage. Mais les dommages ne se limitent pas au temps d'arrêt: ils peuvent également perturber totalement les activités des entreprises et provoquer, pour environ 7% des PME sondées, la perte de données confidentielles.

---

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.

Contactez-nous

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lavenir.net/cnt/dmf20151028_00726712

# Les disques durs chiffrés de Western Digital critiqués pour leurs failles de sécurité | Le Net Expert Informatique

## Les disques durs chiffrés de Western Digital c

**Dans un papier publié le mois dernier, trois chercheurs en cybersécurité se sont penchés sur le chiffrement offert par plusieurs disques durs externes de la marque Western Digital. Les modèles testés sont vulnérables à des attaques permettant de contourner le chiffrement proposé.**

Le chiffrement proposé par les disques durs Western Digital des gammes Passport et My Book souffre de nombreux défauts selon trois chercheurs en cybersécurité. Dans un papier publié il y a un mois, les trois experts se sont penchés sur les conditions d'implémentation du chiffrement dans les différents produits de ces deux gammes de disques durs externes, qui proposent un outil de chiffrement des données stockées sur le disque dur afin d'en protéger l'accès.
Ainsi, la plupart des disques de la gamme proposent un chiffrement s'appuyant sur un mot de passe connu par l'utilisateur. Ce mot de passe est haché grâce à la fonction de hachage SHA256 afin de générer une seconde clef, baptisée DEK ( Data Encryption Key), stockée sur le disque et permettant de chiffrer ou déchiffrer les données lors de leur utilisation par l'utilisateur.

**Nombreuses erreurs**

Mais cette implémentation, étudiée par les chercheurs, souffre de nombreuses vulnérabilités qui rendent possible pour un attaquant expérimenté d'accéder aux données chiffrées sur le disque dur. Ainsi, dans un des modèles analysés, le mot de passe enregistré par l'utilisateur était stocké en clair sur le firmware de l'appareil.
Les chercheurs relèvent également des erreurs dans la génération des chiffres aléatoires utilisés pour le chiffrement des données, qui se basent sur l'horloge interne de l'ordinateur, ou encore la possibilité d'extraire le hash présent sur certains modèles, ce qui ouvre la possibilité d'une attaque par bruteforce. Ces vulnérabilités nécessitent néanmoins que l'attaquant ait physiquement accès au disque dur en question pour pouvoir être exploitées.
Les chercheurs expliquent avoir informé Western Digital des différentes failles trouvées sur les disques durs de la gamme, mais n'avoir aucune information quant à un éventuel correctif prévu par le constructeur.

---



---



Source :
http://www.zdnet.fr/actualites/les-disques-durs-chiffres-de-western-digital-critiques-pour-leurs-failles-de-securite-39826890.htm

# Ces 2 nouvelles tendances dans la sécurité informatique que devez absolument connaître | Le Net Expert Informatique

| | |
|---|---|
| | Ces 2 nouvelles tendances dans la sécurité informatique que devez absolument connaître |

**Deux tendances appelées DevOps et DevSecOps sont apparues aux Etats-Unis ces dernières années dans le but de favoriser la collaboration, et se font progressivement une place dans les modèles de travail des entreprises en matière de sécurité informatique.**

La nécessité d' »agir ensemble » est l'un des messages forts de l'Agence Nationale de la Sécurité des Systèmes d'Information en cette fin d'année. Lors des Assises de la sécurité 2015, Guillaume Poupard, directeur général de l'ANSSI, soulignait le rôle clé de la collaboration – locale et internationale – pour optimiser la sécurité de nos entreprises et plus encore de nos Opérateurs d'Importance Vitale (OIV).

Deux tendances appelées DevOps et DevSecOps sont apparues aux Etats-Unis ces dernières années dans le but de favoriser la collaboration, et se font progressivement une place dans les modèles de travail des entreprises en matière d'informatique. En quelques mots, le DevOps est avant tout un concept et une philosophie que les entreprises sont complètement libres de s'approprier. Au sein d'une même entreprise, cela se traduit par la mise en place d'un groupe de travail composé de différentes entités (équipe réseaux, équipe projets, équipe sécurité pour le DevSecOps, etc.) pour collaborer sur un projet de développement spécifique. A une échelle plus large, le DevOps a pour vocation de favoriser la collaboration et le partage d'informations entre les entreprises, parfois même concurrentes. Ainsi, en partageant plus et mieux leurs données, les entreprises enrichissent mutuellement leurs solutions (applications, logiciels, etc.) et accélèrent ainsi leur développement et leur business.

La tendance du DevOps est en train d'être adoptée progressivement par les entreprises (25% des plus grandes entreprises mondiales sont déjà en train de l'adopter selon le Gartner). Les entreprises françaises semblent s'y intéresser également dans le cadre de projets bien spécifiques. Le Cabinet Vanson Bourne a ainsi établi que 95% des sociétés françaises planifient actuellement la mise en œuvre du DevOps afin d'accélérer le développement d'applications.

Le DevOps c'est bien, mais le DevSecOps c'est mieux… Le DevSecOps est tout simplement une extension du DevOps où la sécurité est intégrée au sein de projets collaboratifs dès le démarrage avec pour objectif d'augmenter le niveau de sécurité des projets (applications, produits, etc.). Pour l'entreprise, il s'agit de bénéficier d'une sécurité plus agile, et plus largement de collaborer avec d'autres entreprises sur un même marché pour augmenter le niveau de sécurité de ses futures solutions.

Cette tendance du DevSecOps peine à être adoptée en France. Comme souvent lorsque l'on parle de sécurité, les entreprises françaises ne sont pas aux avant-postes. Alors que le Gartner recommande de mieux intégrer la sécurité dans tous projets IT et que l'ANSSI fait de la collaboration l'un des grands axes de son discours auprès des entreprises et des professionnels de la sécurité, nos entreprises vont-elles enfin s'ouvrir à plus de collaboration et adopter massivement ces tendances ?

**Les entreprises ont tout intérêt à adopter ces tendances**

Sur le plan de la sécurité, les entreprises ont tout à gagner à adopter rapidement la tendance DevSecOps. Cela leur permettrait d'arriver plus rapidement à un très bon niveau de sécurité, et surtout à des délais de traitement des incidents beaucoup plus rapides.

Nous savons désormais que toutes les entreprises seront victimes d'une attaque informatique un jour ou l'autre, et que ces attaques peuvent avoir de sérieuses conséquences. Il s'agit donc de limiter la période de détection et de remédiation. Avec des organisations traditionnelles, ces délais sont trop longs et plus acceptables face à l'intensité de la menace actuelle. C'est aux responsables de la sécurité qu'il revient de faire adopter ces tendances dans leur entreprise.

**Les silos, le problème récurrent (et culturel) des entreprises françaises**

En France, les entreprises sont fortement pénalisées par des fonctionnements en silos pour leurs ressources IT (équipements / réseau). Sur un plan humain, les équipes projets, les métiers, ou encore la sécurité travaillent la plupart du temps chacune de leur côté, sans échanger les unes avec les autres. Le tout avec une gouvernance qui n'est généralement pas centralisée.

En France et en Europe, ce mode de fonctionnement, souvent hérité, est un problème maintes fois pointé du doigt, car il entraine un vrai facteur de blocage de l'innovation et de la collaboration dans et pour nos entreprises.

L'arrivée des tendances DevOps et DevSecOps peuvent nous laisser penser que les choses pourraient changer et que les barrières liées aux silos soient levées, pour permettre aux équipes de travailler ensemble.

**Aux Etats-Unis, la collaboration est devenue une arme business**

Lorsque les entreprises américaines ont pris conscience des perspectives business offertes par un travail plus collaboratif, même entres concurrents, elles ont rapidement établi de nouvelles approches (Kill chain par exemple et maintenant le DevOps/DevSecOps). Ainsi, ces grandes entreprises s'enrichissent du travail des autres pour accélérer leurs développements respectifs. Au final, elles ont simplement compris que l'outil informatique était un facilitateur de business.

Les grands groupes de l'IT tels que Google, Amazon ou encore LinkedIn ont fait partis des pionniers en la matière, et ils ont ensuite rapidement été suivis par des grandes organisations, telles que la NASA, Starbucks, etc.

En France, nous sommes encore loin de ce niveau de collaboration, même si nos start-ups suivent de plus en plus cette mouvance, d'enrichissement de la donnée par des solutions complémentaires, pour obtenir des niveaux de détection plus fins et des temps de remédiation plus rapides. C'est une excellente approche, qui permet d'aller dans le bon sens, notamment en matière de sécurité. Dans les années à venir, le Cloud devrait être un moteur important de cette tendance DevSecOps, puisqu'il va permettre de plus en plus d'automatiser la sécurité.

**Le DevSecOps offre de multiples avantages**

Le DevSecOps a pour finalité d'optimiser la sécurité et le business des entreprises et plus globalement, le niveau de qualité des technologies de sécurité du marché.

Concrètement, le DevSecOps permet aux entreprises et aux professionnels de s'ouvrir aux autres, et en interne d'accélérer l'automatisation, pour notamment mieux utiliser les ressources humaines sur des tâches d'optimisation de fonds. Le DevSecOps c'est aussi mieux protéger les clients finaux grâce à une sécurité renforcée grâce à une sécurité basée sur des critères objectifs, puisqu'elle est définie sur la base d'un travail collaboratif avec les diverses entités (réseau / métiers / sécurité, etc.), et beaucoup plus orientée sur les nouvelles menaces.

En terme de conformité, DevSecOps permet également de faire le lien entre les experts qui gèrent la sécurité dans des SOC (Security Operations Center) et les opérationnels de l'entreprise, ce qui apporte un avantage indéniable en matière de sensibilisation sur les questions de sécurité.

Ces tendances sont à notre disposition, il ne tient qu'à nous de nous les approprier !

---

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

---



Source : http://bfmbusiness.bfmtv.com/01-business-forum/ces-2-nouvelles-tendances-dans-la-securite-informatique-que-devez-absolument-connaitre-922865.html
Par Arnaud Cassagne

# Le hack étonnant qui peut tromper Siri, Cortana et Google Now grâce aux ondes radio | Le Net Expert Informatique

| | |
|---|---|
| | Le hack étonnant qui peut tromper Siri, Cortana et Google Now grâce aux ondes radio |

**Deux hackers français ont montré qu'il était possible d'injecter des commandes vocales par l'émission d'ondes radioélectriques. Mais cette attaque nécessite quand même un peu de matériel.**

Les assistants vocaux sont bien pratiques et déployés sur pratiquement tous les smartphones aujourd'hui, qu'il s'agisse de Siri pour iOS, de Google Voice pour Android ou de Cortana pour Windows 10 Mobile. Mais ces interfaces présentent des vulnérabilités que deux chercheurs en sécurité de l'ANSSI – José Lopes Esteves et Chaouki Kasmi – ont mis en lumière dans un article publié par le magazine scientifique IEEE Electromagnetic Compatibility. Ils ont également présenté leurs recherches en juin dernier, à l'occasion de la conférence académique SSTIC, qui s'était déroulée à Rennes.

Les deux chercheurs ont montré qu'il était possible d'injecter des commandes vocales dans ces systèmes par l'intermédiaire d'ondes radio. Comment? Au travers des écouteurs du kit mains-libres. « Le câble des écouteurs est une bonne antenne pour des fréquences comprises entre 80 et 108 MHz », explique José Lopez Esteves, dans la vidéo de leur présentation SSTIC. L'idée du hack est donc d'enregistrer une commande vocale, de la moduler en amplitude sur une onde porteuse de la bande 80-108 MHz et de l'envoyer vers les écouteurs. Ce rayonnement va induire dans le câble un signal électrique qui va automatiquement être traité par le système de commandes vocales, après avoir été filtré et amplifié. Au final, « on obtient un signal relativement proche du signal vocal original », précise M. Lopes Esteves.

Cette attaque fonctionne avec tous les principaux systèmes vocaux disponibles, à savoir Cortana, Siri et Google Voice. Il y a néanmoins une condition nécessaire, c'est que la commande vocale soit activée, c'est-à-dire que l'on puisse interroger l'assistant virtuel par un simple mot-clé (« OK Google », « Dis Siri » ou « Hey Cortana »), ce qui n'est pas une option par défaut sur les smartphones.

L'impact de l'attaque dépendra de l'état du téléphone. Il sera maximal s'il est déverrouillé. L'assistant vocal pourra alors accéder au carnet d'adresse, envoyer un message, ouvrir une page web, lancer une application, etc. « On pourra par exemple envoyer une commande pour que l'appareil ouvre un site web malveillant », souligne M. Lopes Esteves. Le mieux dans cette affaire, c'est que l'utilisateur pourrait ne rien remarquer du tout car la commande vocale injectée est totalement silencieuse pour lui. Seul l'assistant vocal l'entendra.

**Limité à quelques mètres**

En revanche, si le téléphone est verrouillé, l'assistant vocal n'aura qu'un accès limité, comme par exemple interroger l'appli météo ou appeler un numéro. Ce qui n'est pas rien quand même, car il est possible alors de passer des coups de fil en douce pour générer des revenus frauduleux (via des numéros surtaxés) ou pour simplement espionner les conversations environnantes.

Si ce piratage est relativement simple sur le principe, il nécessite quand même du matériel. Avec un équipement radio de la taille d'un sac à dos, le rayon d'action est de seulement deux mètres. Pour atteindre cinq mètres, il faut déjà une camionnette. Et dans ce cas, mieux vaut ne pas se trouver à proximité de l'émetteur, car le niveau de rayonnement sera alors plutôt intense.

---

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.01net.com/actualites/siri-cortana-et-google-voice-sont-vulnerables-aux-attaques-radio-922670.html
Par Gilbert KALLENBORN

# La stratégie du gouvernement pour la sécurité du numérique | Le Net Expert Informatique


## La stratégie du gouvernement pour la sécurité du numérique

**Le gouvernement a présenté vendredi sa stratégie pour la sécurité du numérique, un document qui fait la synthèse des différentes mesures en place pour lutter contre les hackers et protéger la vie numérique des citoyens, et met l'accent sur la formation.**

Les « cyberattaques sont susceptibles de désorganiser des activités vitales de notre pays, de déstabiliser des entreprises, de vampiriser leur savoir-faire », a souligné le Premier ministre Manuel Valls, évoquant comme conséquence directe « la destruction de nombreux emplois, de valeur industrielle et culturelle ».
« Les citoyens sont également exposés, que ce soient des tentatives d'escroquerie, qui s'accompagnent parfois de chantage, ou la captation de données personnelles », a-t-il remarqué.
Le document de 40 pages présenté vendredi par le chef du gouvernement, vient remplacer un premier « pensum » publié début 2011, et mis à jour car « la donne a fondamentalement évolué (…) en quatre ans, parce que le monde va très vite ».
La menace est polymorphe, venant tout aussi bien de petits escrocs, de groupes mafieux, d'islamistes radicaux ou encore de services étrangers –y compris alliés.
La spectaculaire attaque, en avril, de la chaîne francophone TV5Monde, a donné toute la mesure du danger. Car les hackers ne chôment pas, comme l'a rappelé le directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi, chargée depuis 2009 de coordonner la défense française face aux cybercriminels), Guillaume Poupaud.
« Des attaques du niveau de TV5, on en a tous les quinze jours », a-t-il indiqué à des journalistes. « Seulement, ce n'est pas du sabotage, mais de l'espionnage », moins spectaculaire.

**– Sensibiliser, former, informer –**

L'une des idées fortes est donc logiquement de **renforcer la défense contre les cybermenaces** en consolidant la sécurité numérique de ses infrastructures, à commencer par les entreprises vitales au pays.
Et on va **sensibiliser les Français aux menaces du cyberespace**, dès l'école. Former. Informer.
« On n'imagine plus des constructeurs automobiles proposer des véhicules sans freins et sans ceintures de sécurité. Mais aujourd'hui, sur ce qu'on appelait les autoroutes de l'information, la plupart des voitures sont sans freins et sans ceintures de sécurité », a relevé Guillaume Poupaud, qui s'étonne de voir des gens « parcourir ces autoroutes de l'information à vélo, et sans casque, alors que des poids lourds passent à côté ».
La stratégie gouvernementale présentée vendredi est « un bon équilibre entre la prise en compte de la sécurité et dynamisme économique » et un « bon équilibre entre sécurité et liberté », a jugé Manuel Valls.
Le chef du gouvernement s'en est d'ailleurs pris à la « position caricaturale » de ceux qui opposent « le numérique », qui devrait être le monde de la liberté absolue, à la +sécurité+, qui se traduirait nécessairement par une restriction dangereuse des libertés fondamentales ». Une position observée selon lui lors du débat sur la loi sur le renseignement.
Si cette loi dote les services de renseignement de moyens de surveillance des citoyens, le gouvernement « reste favorable » à ce que les acteurs privés « continuent de bénéficier pleinement » de « toutes les ressources qu'offre la cryptologie légale », a relevé M. Valls.
Des dirigeants des principaux opérateurs internet français –Bouygues Telecom, Free, Orange, La Poste et SFR-Numericable– ont même signé dans la foulée une charte les engageant à crypter les courriels de leurs clients circulant entre leurs serveurs, afin de pallier une grande faiblesse de la sécurité informatique.
Le gouvernement, qui a fait de la protection de la vie numérique des citoyens un objectif majeur, entend aussi les aider en cas de problème, avec notamment la création l'an prochain d'un « **dispositif national d'assistance » aux victimes d'actes de cybermalveillance**, pour les PME et les particuliers (des procédures étant déjà en place pour les institutions de l'Etat et les grandes entreprises).
Un groupe d'experts doit également être constitué pour mieux faire émerger les nouvelles technologies de sécurité informatique et améliorer les formations dans l'enseignement supérieur.
Enfin, la stratégie française vise aussi à muscler une filière déjà dynamique. Car la lutte contre les cyber-criminels est un secteur d'avenir.

---

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

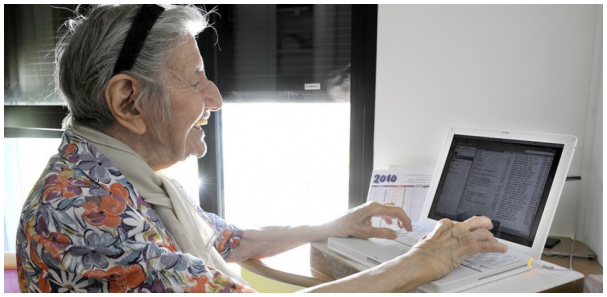
---



Source :
http://www.leparisien.fr/flash-actualite-politique/cybersecurite-valls-presente-la-strategie-de-la-france-16-10-2015-5191401.php#xtref=https%3A%2F%2Fwww.google.com%2F

---

# Pas assez connectée pour être menacée ? Madame Walsh s'est pourtant fait pirater | Le Net Expert Informatique



# Pas assez connectée pour être menacée ? Madame Walsh s'est pourtant fait pirater

**Le piratage, ça n'arrive pas qu'aux autres. Et il n'y a pas besoin d'être ultra-connecté pour en être victime. C'est ce que raconte le « New York Times », avec l'exemple de Madame Walsh, vivant en Californie.**

Cette grand-mère de six petits-enfants a accepté de servir de cobaye à deux hackeurs, se pensant à l'abri, puisque n'étant pas quelqu'un de « connecté ».
Mme Walsh explique ne disposer d'aucun objet connecté (montre, etc.), sa maison n'est équipée d'aucun appareil technologique récent (thermostat connecté ou autre), et elle n'est pas une grande adepte des gadgets électroniques. Bien sûr, elle dispose d'un compte Facebook, mais n'y publie jamais rien, et s'en sert uniquement pour rester en contact avec des amis. Et pourtant.

**E-mail, PaylPal, télévision et garage piratés**

Les hackeurs ont bien réussi à pirater Madame Walsh. Le quotidien raconte que les pirates ont successivement testé plusieurs pistes pour tenter de s'attaquer à la grand-mère. Si son compte Facebook se révèle bien protégé, la découverte d'un « J'aime » pour une page de la plateforme de pétitions Change a été le déclic.
Dix minutes plus tard, les hackeurs adressent à Mme Walsh un faux e-mail émanant de Change.org proposant de signer une fausse pétition. Bingo, la grand-mère clique, et entre son identifiant et son mot de passe. La voilà victime de « phishing ».
Madame Walsh confesse au « New York Times » utiliser le même mot de passe sur l'ensemble des services internet. Les pirates sautent sur la brèche et s'introduisent dans sa messagerie e-mail pour récupérer ses données de sécurité sociale et d'assurance maladie, et de ses comptes PayPal et Miles.
Pis, les hackeurs s'introduisent également dans le compte e-mail de sa fille, dont le code était « caché » dans un message. Enfin, ils laissent sur l'ordinateur de Mme Walsh un virus qui enregistre tout ce qui est tapé et remplace les publicités des sites visités afin de leur générer des revenus.
Pas repus, les deux hackeurs se sont attaqués à sa maison. En une heure et demie, ils ont pris le contrôle de sa télé (l'installateur du câble n'avait pas protégé la connexion) et trouvé un moyen d'ouvrir à distance la porte de son garage (via un procédé de « brute force » qui a essayé des centaines de combinaisons possibles avant de tomber sur la bonne pour la porte électrique).

**Le phishing, risque numéro un**

L'exemple du « New York Times » est extrême mais illustre bien que personne n'est à l'abri d'un piratage, même ceux qui se pensent « trop peu connecté pour être en danger ». Et le risque premier demeure le phishing, aussi appelé hameçonnage.
Aujourd'hui, plus de 90% des attaques dans le monde démarrent par un e-mail de phishing », affirme Ismet Geri, directeur général pour la France et l'Europe du Sud de Proofpoint, société spécialisée dans la sécurité des e-mails.
Un e-mail sur 392 serait une tentative de phishing, estime l'entreprise de sécurité informatique Symantec dans son dernier rapport. Au total, 37,3 millions d'internautes sont tombés dans le panneau dans le monde, affirme une enquête de la société de sécurité Kaspersky. La France se classe septième pays au monde dans les victimes avec un internaute sur 30 floué.

**LIRE »J'ai cliqué » : chronique d'un phishing ordinaire**

L'objectif des pirates est simple : récupérer des coordonnées bancaires, mais aussi des informations personnelles. Selon Symantec, au marché noir, les détails d'une carte de crédit se revendent entre 0,50 et 20 dollars, un passeport scanné 1 à 2 dollars, l'accès à un compte cloud 7 à 8 dollars, l'accès à un compte de jeux vidéo en ligne 10 à 15 dollars, etc.
L'utilisation de ces données est évidente. Les données bancaires permettent d'effectuer des achats en ligne, tandis que les informations personnelles vont permettre de s'identifier sur l'ensemble des services. Surtout que le sésame identifiant/mot de passe devient un Graal, quand on sait que 75% des Français utilisent toujours le même mot de passe.
Je m'estimais plutôt malin, je m'étais trompé ! », a confié le blogueur Thomas Messias au « Parisien » après un piratage de ses comptes. « Evidemment, j'utilisais le même mot de passe pour eBay et pour tous les autres sites… »
Voilà Madame Walsh prévenue. Et pour ce qui est de la maison, de nombreux experts en informatique démontraint régulièrement comment prendre le contrôle d'objets usuels. Cet été, le hackeur Samy Kamkar a démontré comment ouvrir des portes de garage à partir d'un jouet Mattel en moins de 10 secondes :

---

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

---



Source :
http://tempsreel.nouvelobs.com/tech/20151015.OBS7721/pas-assez-connectee-pour-etre-menacee-madame-walsh-s-est-pourtant-fait-pirater.html#xtor=EPR-1-ObsActu8h-20151016

# Encore une faille 0-day sur Flash Player menaçant vos ordinateurs | Le Net Expert Informatique

Encore une faille 0-day sur Flash Player menaçant vos ordinateurs

**Ces derniers mois, Flash Player a subi les foudres de grands noms de l'informatique suite à de nombreuses vulnérabilités découvertes en plus des innombrables précédentes corrigées auparavant. Déjà alors, certaines institutions comme Facebook réclamaient l'abandon du plug-in Flash alors cet aveu issu de la société de développement Adobe ne risque pas d'arranger le sort de son Flash Player.**

Un rapport publié par la société Adobe a été publié mercredi et confirme la présence d'une faille critique au sein de la dernière version du Player mais aussi des précédentes. Celle-ci peut être employée « lors d'attaques limitées et ciblées ». Sont concernées les dernières versions,19.0.0.207 incluse mais également toutes les précédentes itérations sur Windows et Mac, Adobe Flash Player Extended Support Release pour l'intégralité des versions 18 ainsi que les versions pour Linux.

En plus des vulnérabilités 0-day employés par la Hacking Team, cette faille avait été décelée au cours de l'été par TrendMicro qui mettait alors au jour une attaque informatique de grande envergure orchestrée par le groupuscule Pawn Storm, pirates visant différents ministères des affaires étrangères à travers le monde ainsi que certains média.

Si cette attaque reposait principalement sur l'utilisation de malwares, des méthodes de phishing et exploitait une faille inhérente à Java (la première repérée depuis des années), le magazine spécialisé a par la suite découvert que les hackers s'appuyaient aussi sur une faille présente dans Flash Player.

Confirmée par Adobe, celui-ci a aussitôt assuré se mettre à l'élaboration d'un correctif. Initialement prévu pour une distribution au 16 octobre, ce patch devrait finalement être disponible vers le 19 du même mois. Reste que la plus sûre des solutions en attendant sa mise à jour consiste à désinstaller complètement le lecteur. Si la faille ne concerne pas directement la personne lambda mais principalement les hautes institutions, le principe d'action pourrait tout de même être repris par d'autres pirates et appliqués à une plus grande partie de la population. Prudence.

---

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;

• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;

• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

http://www.phonandroid.com/flash-player-encore-faille-0-day-menacant-ordinateurs.html

# Alerte de cyberattaques dans les avions | Le Net Expert Informatique

## Alerte de cyberattaques dans les avions

**L'Agence européenne de sécurité aérienne (AESA) estime que l'aviation est vulnérable et qu'il faut mettre en place des structures dédiées pour lutter contre cette nouvelle menace.**

En mai dernier, lorsque le hacker Chris Roberts avait fait les gros titres avec son histoire de piratage d'un avion en plein vol, les compagnies aériennes ont rétorqué en cœur qu'une telle action serait totalement impossible. Elle estimaient que M. Roberts n'était qu'un vantard mythomane. Mais les instances de régulation commencent à voir les choses d'un œil différent, à commencer par celles de l'Union européenne.

Interrogé par l'association des journalistes de la presse aéronautique et spatiale (AJPAE), le directeur exécutif de l'Agence européenne de sécurité aérienne (AESA) Patrick Ky a souligné la vulnérabilité de l'aviation à un éventuel acte de piratage. « C'est un risque auquel il faut qu'on se prépare, l'aviation est vulnérable. Dire que l'aviation n'est pas sujette au cyber-risque, c'est se voiler la face », a-t-il déclaré. Selon le patron de l'agence, il faut mettre en place des « réseaux spécifiques » de spécialistes en cyberattaques pour « informer de la menace et des moyens de s'en prévenir ».

**L'AESA fait appel à un hacker**

M. Ky a affirmé avoir pu lui-même constater les capacités d'un hacker à pénétrer le réseau de communication d'une compagnie aérienne. « J'ai fait appel à un hacker qui a la particularité d'avoir également une licence de pilote commercial, a-t-il expliqué auprès des Echos. En moins de 5 minutes, il est parvenu à rentrer dans le réseau Acars ». Acars (Aircraft Communication Addressing and Reporting System) est un système de communication et de surveillance par radio basé sur l'échange de messages entre un avion et une station au sol. Il intervient dans la gestion du trafic aérien et permet de s'assurer du bon fonctionnement des équipements de l'aéronef. Mais le hacker ne s'est pas arrêté là. « Il ne lui a fallu que deux ou trois jours pour pénétrer dans le système de contrôle d'un avion au sol. Pour des raisons de sécurité, je ne vous dirai pas comment il a fait », ajoute Patrick Ky.

En décembre dernier, cinq grandes organisations internationales de l'aviation (OACI, ACI, CANSO, IATA et ICCAIA) avaient adopté une feuille de route commune pour harmoniser leurs mesures respectives en matière de cybermenaces, et souligné que « la sécurité et la sûreté du système aéronautique mondial » étaient « potentiellement vulnérables aux attaques de pirates informatiques et autres cybercriminels ».

---

Denis JACOPINI est Expert Informatique, formateur et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

---



Source :
http://hightech.bfmtv.com/internet/l-europe-sonne-l-alerte-sur-le-risque-de-cyberattaques-dans-les-avions-920964.html
Par Gilbert Kallenborn

# Il s’implante une puce NFC dans la main pour pirater des smartphones Android | Le Net Expert Informatique

| | |
|---|---|
| Glissée sous la peau, la puce NFC devient invisible après que la plaie a cicatrisé. DRPhoto: | Il s’implante une puce NFC dans la main pour pirater des smartphones Android |

**Les pirates ne reculent devant rien pour hacker des téléphones mobiles. Dernière expérience en date : s'implanter une puce NFC dans la main. Rien que ça.**

Seth Wahle est un ingénieur pour une société spécialisée dans les technologies sans fil, APA Wireless. A ses heures perdues, ce hacker teste la sécurité de ce type de dispositif. Et ne fait pas dans la demi-mesure : il est parvenu à s'implanter une puce NFC sous la peau de la main, à la jonction entre le pouce et l'index de sa main gauche. De la sorte, il est capable de hacker des smartphones Android rien qu'en les effleurant avec sa paume.

**Comment a-t-il fait ?**

Le magazine américain Forbes explique qu'il a trouvé une puce NFC que l'on peut implanter sans danger sous la peau d'un être humain. Dotée de seulement 888 bytes de mémoire, elle est encapsulée dans un petit récipient en verre vendu sur un site chinois et qui est usuellement utilisé pour implanter des puces RFID dans le bétail pour le marquer. Pour la somme de 40 dollars (35 dollars), il a ensuite trouvé une personne qui a accepté de lui injecter la puce sous la peau à l'aide d'une seringue spéciale. Ne restait plus ensuite qu'à attendre que la plaie créée cicatrise.

**Un simple contact téléphone-main et un programme s'installe discrètement**

Avec ce dispositif, Seth Wahle affirme qu'il est désormais capable de hacker n'importe quel smartphone Android doté de la technologie NFC (communication proche par simple contact). Il lui suffit de mettre le téléphone brièvement en contact avec la paume de sa main pour que celui-ci ne se rende sur une page web piratée qui va déclencher le téléchargement d'un petit programme. Et ce, sans alerter les systèmes de sécurité du smartphone.

Une fois celui-ci installé et actif, il est capable de récupérer n'importe quelles données du mobile et même de prendre des photos. Son système n'est pas encore optimal (il perd assez vite la connexion avec le téléphone piraté, notamment quand ce dernier est verrouillé ou redémarré) mais génère déjà de nombreuses questions et craintes pour le futur. Seth Wahle, qui a montré sa performance aux journalistes de Forbes, s'apprête à la présenter plus en détail lors d'une importante conférence de hackers qui se tiendra à Miami du 15 au 17 mai prochain. Nul doute que son intervention sera très suivie…

---

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---



Source :
http://www.metronews.fr/high-tech/pour-pirater-des-smartphones-android-il-s-implante-une-puce-nfc-dans-la-main/modD!v2YdgmEKKTEuE/

---

# Un nouveau logiciel malveillant cible les iPhone | Le Net Expert Informatique

## Un nouveau logiciel malveillant cible les iPhone

**Décidément, les terminaux à la pomme intéressent de plus en plus les pirates. Après la découverte le 4 février par les experts du cabinet de sécurité informatique Trend Micro du premier logiciel espion baptisé « XAgent » exploitant des failles sur les téléphones Apple non débridés (dits « non jailbreakés »), c'est au tour de l'unité de recherche 42 de l'entreprise de sécurité informatique Palo Alto Networks de publier dimanche 4 octobre une alerte sur un nouveau logiciel malveillant (malware) affectant les iPhones du commerce.**

Baptisé « YiSpecter », il attaque sans distinction les iPhone du commerce vendus avec le système d'exploitation officiel iOS d'Apple et ceux qui ont été débridés. Apple, qui a reconnu l'existence de ce malware, a indiqué lundi 5 octobre que les utilisateurs d'iOS 8.4 et d'iOS 9 étaient désormais protégés. La particularité de ce programme — qui serait actif depuis plus de 10 mois à Taïwan et en Chine continentale d'où il proviendrait — est d'utiliser des failles que l'on pensait impossible à exploiter, et de se propager de façon inédite, selon Palo Alto Networks.

**Un fonctionnement et une propagation inédits**

Détournant certaines interfaces de programmation propres au système d'exploitation iOS, cette nouvelle forme de logiciel malveillant ne laisse rien présager de bon pour l'avenir des terminaux mobiles à la pomme selon la firme de sécurité à l'origine de la découverte : « C'est le premier malware que nous avons vu en circulation qui abuse les API [interfaces de programmation] privées dans le système iOS pour mettre en œuvre des fonctionnalités malveillantes. »

En se propageant seul soit grâce à « Lingdun », un ver informatique sous Windows (qui se charge d'envoyer des liens malicieux de téléchargement d'YiSpecter à tous ses contacts), soit par le piratage des connexions WiFi des boîtiers des fournisseurs d'accès à Internet, cette nouvelle variante de malware inquiète la société californienne. Ses quatre composants, tous authentifiés par des certificats d'entreprises réels émanant de sociétés comme Verisign ou Symantec, s'installent de façon furtive sur les iPhone, en masquant ses programmes, mais aussi en dupliquant les noms et les logos des icônes système (Game Center, Météo, Notes, PassBook, Téléphone, etc.), piégeant même les utilisateurs les plus avertis.

Une fois installé, YiSpecter peut télécharger, installer et lancer des applications de l'App Store, mais aussi les modifier, par l'affichage de publicités en plein écran par exemple. Il permet également de collecter les données des utilisateurs, notamment celles utilisées dans le navigateur Internet Safari. S'il est découvert, sa suppression par méthode classique ne fonctionnera pas car il se réinstalle automatiquement après un redémarrage système. Enfin, peu d'espoir du côté des antivirus, qui ne détectent toujours pas sa présence sur les terminaux infectés.

**Des malwares aux origines peu claires**

Certains indices repérés par Palo Alto Networks font converger les soupçons vers « YingMob », une entreprise chinoise de publicité mobile ayant pignon sur rue, qui aurait programmé et diffusé ce malware à des fins publicitaires, n'hésitant pas à en faire sa promotion au grand jour. Mais la complexité et les méthodes de propagation de YiSpecter cachent peut-être des visées plus opaques.

Déjà le mois dernier, 344 applications iOS officielles présentes dans l'App Store, la boutique d'applications d'Apple, avaient été retirées en urgence car infectées par le malware « XcodeGhost », découvert le mercredi 16 septembre par les équipes sécurité du groupe chinois Alibaba. L'origine de ce malware est encore incertaine, mais les méthodes utilisées sont très similaires aux techniques de programmation qu'emploie la CIA — selon des documents publiés en mars par The Intercept.

Tout début septembre, c'était le logiciel malveillant « KeyRaider » également découvert par la société Palo Alto Networks, qui faisait parler de lui : selon la société de sécurité, plus de 225 000 comptes et identifiants Apple auraient été dérobés, uniquement sur des iPhone et iPad débridés.

La société de sécurité américaine est également à l'origine de la chute d'un mythe : c'est elle qui annonçait il y a moins d'un an, en novembre 2014, la découverte, toujours en Chine, de « Wirelurker », le tout premier malware pour iPhone touchant des téléphones non débridés. Depuis, il ne se passe pas un mois sans qu'une nouvelle alerte concernant les terminaux mobiles d'Apple ne soit lancée.

---

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.lemonde.fr/pixels/article/2015/10/07/un-nouveau-logiciel-malveillant-cible-les-iphone_4784509_4408996.html