# Alerte : Un ransomware qui verrouille votre appareil en changeant le code PIN Android | Le Net Expert Informatique


## Alerte : Un ransomware qui verrouille votre appareil en changeant le code PIN Android

**La société ESET a récemment publié un rapport alarmant sur la prolifération des ransomwares sur les appareils mobiles, aux États-Unis pour la plupart. Ces derniers se font passer pour des applis pornos réclamant des permissions quelque peu douteuses. Une fois ces dernières accordées, votre appareil est tout simplement verrouillé.**

Nous vous parlions en début de semaine d'une application porno qui prenait ses utilisateurs en photo, puis leur demandait une rançon. Ce ransomware virulent se cachait derrière un fichier .apk que le détenteur du smartphone visé installait, sans le savoir, depuis un site pas très catholique.

Les chercheurs de la société ESET (qui édite des antivirus) viennent de pointer dans un billet de blog le fait que les ransomwares évoluent et se révèlent de plus en plus difficiles à contrer. Le dernier en date, Porn Droid, se présente comme souvent sous la forme d'un lecteur de contenus pour adultes. Ce dernier se télécharge au format .apk depuis un market alternatif, comme la plupart des applications du genre. Ce Porn Droid cache en vérité un ransomware qui va, en vous demandant les privilèges administrateur discrètement, bloquer votre appareil. Un message du FBI (classique) s'affichera et vous réclamera la modique somme de 500 $ à payer rapidement. Ce message stipule d'ailleurs (classique aussi) que vous avez hébergé du contenu pornographique interdit.

Une fois la menace passée, ce ransomware va bloquer votre appareil préféré par l'intermédiaire d'un Code Pin que vous ne connaissez évidemment pas. Pire encore, si vous avez l'habitude d'utiliser cette sécurité pour protéger votre smartphone, le ransomware est capable d'en modifier le code. ESET propose une solution si Porn Droid fait des siennes avec votre cher appareil Android. Pour ce faire, il faut employer l'invite de commande et la passerelle de débogage Android pour modifier le fichier chargé de traiter le code PIN de votre appareil. De plus, votre terminal doit être rooté, ce qui rajoute une condition supplémentaire. Notez que ce ransomware est tellement virulent qu'il est capable de fermer les antivirus installés sur votre mobile qui tournent en tâche de fond. En définitive, la meilleure solution reste la prévention. Méfiez-vous des portails proposant des applications à télécharger .apk et appliquez les 10 commandements de la sécurité pour garder son appareil à l'abri de toutes menaces. Si le porno mobile vous intéresse, consultez notre article qui lui est consacré.

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
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.android-mt.com/news/porn-droid-ransomware-android-43752

---

# 100% des montres connectées présentent des failles de sécurité | Le Net Expert Informatique

100% des montres connectées présentent des failles de sécurité

**Les montres équipées de connexion réseau et de fonctions de communication représentent une nouvelle cible pour les cyberattaques. Tel est le principal résultat de l'étude, menée par HP Fortify, qui révèle que 100% des montres testées recèlent d'importantes vulnérabilités, comme par exemple des fonctions d'authentification insuffisantes, un manque de capacités de chiffrement, et des soucis dans la protection des données personnelles1. Dans ce rapport, HP recommande un certain nombre d'actions pour améliorer la sécurité dans la conception et l'utilisation des montres, à la maison ou dans son environnement de travail.**

Avec le déploiement de l'Internet des Objets, les smartwatches gagnent en popularité en raison de leur côté pratique et des nouvelles fonctionnalités qu'elles proposent. En devenant des objets usuels, ces montres vont collecter de plus en plus d'informations personnelles sensibles, comme des données de santé. La possibilité de les connecter avec des applications disponibles sur smartphone risquent prochainement de leur donner accès à encore plus d'informations, comme par exemple les codes permettant d'ouvrir votre maison ou votre véhicule.
« Les montres connectées commencent à peine à entrer dans nos vies. Elles offrent déjà de nouvelles fonctionnalités innovantes qui pourraient ouvrir la voie à de nouvelles menaces sur des informations et des activités sensibles », a déclaré Jason Schmitt, Directeur Général Fortify de l'entité HP Security. « Avec l'accélération de l'adoption des smartwatches, cette plate-forme va devenir bien plus attrayante pour tous ceux qui voudraient en faire une utilisation frauduleuse. Il devient nécessaire de prendre des précautions lors de la transmission des données personnelles ou du raccordement de ces équipements aux réseaux d'entreprise. »
L'étude HP s'interroge ainsi sur la capacité des smartwatches à stocker et à sécuriser les données sensibles pour lesquelles elles ont été conçues. HP s'est appuyé sur HP Fortify on Demand pour évaluer 10 montres connectées à des applications mobiles et un cloud Android ou iOS.

Cette étude révèle de nombreuses failles de sécurité parmi lesquelles les plus fréquentes et les plus faciles à corriger sont :

**L'insuffisance des fonctions d'autorisation et d'authentification des utilisateurs :**
Chaque montre connectée testée était couplée à une interface sur téléphone mobile qui ne gérait pas l'authentification à deux facteurs, et qui ne verrouillait pas les comptes après 3 ou 5 saisies de mots de passe infructueux. Trois montres sur dix, c'est à dire 30%, étaient vulnérables aux tentatives de moisson de comptes utilisateurs, ce qui veut dire qu'un pirate informatique pourrait obtenir le contrôle de la montre et de ses données en profitant d'une politique de mots de passe faible, du non blocage des comptes, ou en énumérant des listes de comptes utilisateur potentiels.

**Le manque de chiffrement lors du transfert de données :**
Le chiffrement lors du transport d'information est essentiel, dans la mesure où des informations personnelles sont envoyées vers de multiples destinations dans le cloud. Même si 100 pourcents des montres testées intégraient le chiffrement lors transport avec le protocole SSL/TLS, environ 40% des connexions vers le cloud restaient vulnérables à l'attaque POODLE, permettant l'utilisation d'outils de déchiffrement peu puissants, ou encore le protocole SSL v2.

**Interfaces peu sécurisées :**
30% des montres testées utilisaient des interfaces web accessibles en mode cloud, et toutes présentaient des risques d'énumération de comptes utilisateur. Dans un test spécifique, 30% ont également révélé des risques d'énumération de comptes utilisateur depuis leurs applications sur mobile. Cette défaillance permet aux hackers d'identifier des comptes utilisateurs valides en s'appuyant sur les informations reçues via les mécanismes de réinitialisation de mots de passe.

**Logiciels et microcode peu sécurisés :**
70% des montres ont révélé des failles dans la protection des mises à jour de microcode, comme par exemple la transmission en clair des mises à jour, sans chiffrer les fichiers. Cependant, plusieurs mises à jour étaient protégées par une signature, évitant ainsi l'installation d'un microcode contaminé. Même si des updates malicieuses ne peuvent être installées, le manque de chiffrement permet aux fichiers d'être téléchargés puis analysés.

**Soucis sur la protection des données personnelles :**
Toutes les montres collectent des données personnelles – comme le nom, l'adresse, la date de naissance, le poids, le sexe, la fréquence cardiaque, et bien d'autres informations relatives à la santé de l'utilisateur. Si l'on rapproche ceci des problèmes relevés sur l'énumération des comptes utilisateur ou l'utilisation de mots de passe faiblement sécurisés sur certaines montres, le risque de diffusion des données personnelles depuis une montre connectée devient un problème réel.

En attendant que les fabricants incorporent les dispositifs nécessaires permettant de mieux sécuriser leurs smartwatches, les utilisateurs sont priés d'examiner scrupuleusement les fonctions de sécurisation existantes avant de choisir un modèle de montre connectée. HP recommande aux utilisateurs de ne pas activer les fonctions de contrôle des accès sensibles, comme par exemple l'accès à leur domicile ou leur véhicule, sauf si un mécanisme d'autorisation performant est proposé par la montre. De plus, en activant la fonctionnalité passcode, en imposant des mots de passe sophistiqués et en introduisant une authentification à deux facteurs, il est possible d'éviter des accès frauduleux aux données. Au delà de la protection des données personnelles, ces mesures sont essentielles dès lors que la smartwatch va être utilisée dans un environnement de travail et connectée au réseau de l'entreprise.

**Méthodologie**
Réalisée par HP Fortify, l'étude HP Smartwatch Security Study a utilisé la méthodologie HP Fortify on Demand IoT testing methodology, combinée avec des tests manuels et d'autres outils de test automatisés. Les équipements et les composants testés ont été évalués sur la base de l'outil OWASP Internet of Things Top 10 et des vulnérabilités spécifiques associées à chacune des 10 premières catégories.
Toutes les données et les tous les pourcentages inclus dans l'étude ont été extraits des tests menés sur les 10 montres évaluées. Malgré l'existence d'un nombre croissant de fabricants et de modèles de smartwatches, HP pense que les résultats obtenus sur cet échantillon de 10 modèles donne un bon indicateur du niveau de sécurité des smartwatches actuelles du marché.

Des conseils complémentaires sur la sécurisation des smartwatches sont disponibles dans le rapport complet (http://go.saas.hp.com/fod/internet-of-things)

Pour toute information complémentaire, il est possible de consulter le premier rapport de la série sur l'Internet des Objets, 2014 HP Internet of Things Research Study, qui passe en revue le niveau de sécurité des 10 objets connectés les plus courants du marché. De plus, l'étude 2015 HP Home Security Systems Report (http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-7342ENW&cc=us&lc=en) examine les 10 systèmes les plus répandus en matière de protection connectée du domicile.
(1) "HP Internet of Things Security Report: Smartwatches," HP, Juillet 2015.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

---

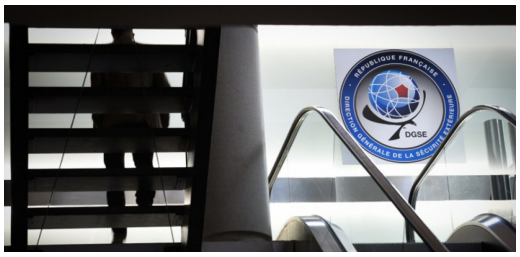
Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

---

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

Source : http://www.itrnews.com/articles/157450/100-montres-connectees-presentent-failles-securite.html et ITRmobiles.com

# En exclusivité, la nouvelle loi sur les écoutes de la DGSE – L'Obs | Le Net Expert Informatique



## En exclusivité, la nouvelle loi sur les écoutes de la DGSE

**La commission de la Défense de l'Assemblée Nationale rendra publique, jeudi 10 septembre, une proposition de loi très sensible dont « L'Obs » a pu se procurer le texte. Celui-ci définit les modalités d'autorisation et de contrôle des écoutes internationales de la DGSE et de ce fait les légalise pour la première fois.**

Cette proposition de loi (dite « relative aux mesures de surveillance des communications électroniques internationales ») fait suite au rejet, le 23 juillet, par le Conseil Constitutionnel des dispositions sur le même sujet inscrites dans la loi sur le renseignement.

L'article avait été retoqué par les Sages au motif notamment qu'il renvoyait à un décret secret (dont « l'Obs » avait révélé l'existence). La représentation nationale n'avait donc pas une idée assez précise du fonctionnement de ces grandes oreilles ni de leur contrôle. Cette nouvelle proposition de loi répond, semble-t-il, à l'exigence de (relative) transparence formulée par le Conseil Constitutionnel.

**La proposition de loi apporte les clarifications suivantes :**

**La France préservée**

Il est redit qu'il s'agit des communications « émises ou reçues de l'étranger » et que la DGSE ne peut cibler la France. Plus précisément, le texte stipule que si, du fait du trajet aléatoire des signaux électroniques, le service de renseignement intercepte des communications échangées entre personnes ou équipement « utilisant des numéros d'abonnement ou des identifiants rattachables au territoire national, y compris lorsque ces communications transitent par des équipements non rattachables à ce territoire, ces interceptions sont instantanément détruites. »

**Le Premier ministre au centre du dispositif**

Cet article est le plus important pour la DGSE. Il stipule que la décision générale d'écouter tel ou tel « système de communication » revient au Premier ministre qui en assume donc la responsabilité. Autrement dit, c'est le chef du gouvernement qui désormais autorise l'interception des flux provenant des satellites de communication et des câbles sous-marins.

Cette disposition oblige également la DGSE à obtenir l'autorisation des Premiers ministres futurs si elle veut écouter de nouveaux moyens de communication. Le but est notamment d'éviter que ne se reproduise l'épisode de 2008. A l'époque, la loi ne permettait pas à la DGSE d'écouter les câbles sous-marins. Pour passer outre, elle avait obtenu à l'insu de la représentation nationale la signature du décret secret évoqué dans la précédente mouture de la loi.

**Le big data légalisé**

Le Premier ministre « autorise l'exploitation non individualisée des données de connexion interceptées ». Il s'agit de la reconnaissance publique que la DGSE intercepte des flux et pas seulement des communications individuelles et qu'elle analyse les « big data » ainsi récoltées. Le texte ajoute que « ces autorisations [délivrées pour un an] déterminent la ou les finalités poursuivies ainsi que les types de traitements automatisés pouvant être mis en œuvre. »

**Les pays cibles des grandes oreilles**

Le paragraphe le plus novateur stipule que le Premier ministre autorise l'écoute de « zones géographiques [donc des pays ou des régions] », d' »organisations », de « personnes » ou de « groupes de personnes ». C'est la première fois qu'un texte officiel confirme que la France écoute elle aussi le monde, que la DGSE agit comme la NSA (avec, certes, moins de moyens). On remarquera que le législateur n'interdit pas l'écoute de dirigeants étrangers, ennemis ou amis…

**Contrôle théorique**

La Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR) « dispose d'un accès permanent, complet et direct aux renseignements collectés, aux transcriptions et extractions réalisées […] et peut contrôler à sa demande les dispositifs techniques ». Sur le papier, les écoutes de la DGSE sont donc bien contrôlées. Tout dépendra des moyens dont la future CNCTR va disposer.

**Destruction possible**

La CNCTR peut recommander au Premier ministre la destruction d'écoutes non conformes. Si celui-ci refuse, elle peut saisir le Conseil d'Etat pour trancher. Une disposition originale.

**Recours individuel**

Comme pour les écoutes intérieures, « toute personne souhaitant vérifier qu'aucune mesure de surveillance [par la DGSE] n'est irrégulièrement mise en œuvre à son égard » peut saisir la CNCTR. Celle-ci notifie à la personne en question qu'il a procédé aux vérifications nécessaires « sans confirmer ou infirmer la mise en œuvre de mesures de surveillance ».

**Délais de conservation**

La loi définit des délais de conservation des interceptions qui s'étalent entre un an pour les communications à huit pour les renseignements chiffrés en passant par six pour les données de connexion.

Le texte du projet de loi :
proposition loi surveillance publié par NouvelObs.com

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
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://tempsreel.nouvelobs.com/monde/20150909.OBS5547/exclusif-la-nouvelle-loi-sur-les-ecoutes-de-la-dgse.html
Par Vincent Jauvert

# Le certificat électronique est une arme efficace contre la Cybercriminalité | Le Net Expert Informatique

| | |
|---|---|
| | Le certificat électronique est une arme efficace contre la Cybercriminalité |

**Lutter contre la cybercriminalité est un axe stratégique pour les entreprises et les institutions. En effet, nous assistons quotidiennement à des attaques toujours plus sophistiquées qui viennent durablement compromettre l'intégrité et la confidentialité des échanges réalisés sur le net.  Bien entendu, nombre d'entreprises et d'institutions mettent en place des dispositifs pour se protéger, mais en laissant «certains trous dans la raquette» qui sont immédiatement utilisés par les pirates pour mener à bien leurs actions.**

Très répandues, ces pratiques créent des désastres financiers et montrent bien que les flux sortants sont tout aussi exposés que les flux entrants. Il est donc nécessaire de les prendre en compte dans la mise en œuvre de dispositifs de protection efficace.

L'usage du certificat électronique ID (pour personne physique) est la piste à privilégier. Il est d'ailleurs largement plébiscité par l'Etat et les collectivités avec la norme RGS. Véritable rempart contre l'usurpation d'identité, il permet au destinataire d'un mail d'en vérifier l'émetteur, il permet également de garantir la confidentialité des données échangées. L'autre avantage tient à sa simplicité d'utilisation sur les mobiles et tablettes. Avec un certificat, les envois de mails à partir d'un smartphone ne représentent plus une faille de sécurité mais sont protégés efficacement.

Au regard de ces éléments, institutions et entreprises doivent accélérer le déploiement de certificats pour sécuriser leurs échanges de données. Une prise de conscience dans ce domaine permet de colmater des brèches importantes et complète des dispositifs traditionnels de type Firewall qui jouent pour leur part un rôle de filtrage pour les données entrantes.  Avec les certificats électroniques, les flux sortants sont parfaitement sécurisés, leur apport dans la lutte contre la cybercriminalité est donc stratégique, d'autant que leur coût d'acquisition n'est pas onéreux.

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

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.edubourse.com/finance/actualites.php?actu=89518

---

# Les entreprises doivent se préparer à une nouvelle génération de cyber-risques |

# Le Net Expert Informatique


## ALes entreprises doivent se préparer à une nouvelle génération de cyber-risques

**Les entreprises doivent se préparer à une nouvelle génération de cyber-risques qui progressent rapidement, passant de menaces avérées de violations de données, problèmes de confidentialité et atteintes à la réputation, à l'interruption d'activité et même à des pertes potentielles catastrophiques, en passant par des dommages opérationnels.**

Dans un nouveau rapport — A Guide to Cyber Risk : Managing The Impact of Increasing Interconnectivity —, l'assureur spécialisé Allianz Global Corporate & Specialty (AGCS) observe les dernières tendances en matière de cyber-risques et les dangers émergents au niveau mondial. Le cyber-risque est l'une des principales menaces auxquelles font face les entreprises et connaît une croissance rapide. La cybercriminalité à elle seule coûte approximativement 445 milliards de $ par an à l'économie mondiale et les 10 plus grandes économies représentent plus de la moitié de ce montant (3 milliards de $ pour la France).
« Il y a à peine 15 ans, les cyber-attaques étaient assez rudimentaires et généralement l'œuvre de hacktivistes, mais avec l'accroissement de l'interconnectivité, de la mondialisation et de la commercialisation de la cybercriminalité, la fréquence et la gravité des cyber-attaques ont pris une ampleur considérable », déclare Chris Fischer Hirs, PDG d'AGCS. « La cyber-assurance ne remplace pas une sécurité informatique solide, mais elle crée une seconde ligne de défense qui limite les incidents. AGCS observe une augmentation de la demande pour ces services, et nous nous engageons à collaborer avec nos clients afin de mieux comprendre l'exposition croissante aux cyber-risques et d'y faire face. »

**Des réglementations plus strictes et de nouveaux cyber-dangers**

Une prise de conscience croissante des expositions aux cyber-risques ainsi qu'une adaptation de la réglementation vont propulser la croissance future de la cyber-assurance. Avec moins de 10 % des entreprises qui achètent actuellement des cyber-polices spécifiques, AGCS prévoit une augmentation des primes de cyber-assurance à l'échelle mondiale de 2 milliards de $ par an aujourd'hui à plus de 20 milliards de $ au cours de la prochaine décennie, soit un taux de croissance annuel de plus de 20 %.
« Aux États-Unis, la croissance a déjà commencé, portée par des règles relatives à la protection des données qui attirent l'attention sur le problème. Dans le reste du monde, de nouvelles dispositions législatives et des niveaux de responsabilité plus élevés seront des moteurs de croissance », affirme Nigel Pearson, responsable mondial de la cyber-assurance chez AGCS. « La tendance générale tend à opter pour une protection des données plus strictes et elle est soutenue par la menace d'amendes importantes en cas d'infraction. » Hong Kong, Singapour et l'Australie, par exemple, travaillent sur de nouvelles lois ou en appliquent déjà. Même si l'Union européenne ne parvient pas à se mettre d'accord sur ses règles paneuropéennes de protection des données, on peut s'attendre à des directives plus strictes à l'échelle de chaque pays.
Auparavant, l'attention se focalisait largement sur la menace de violation de données d'entreprise et d'atteinte à la vie privée, mais la nouvelle génération de cyber-risques est plus complexe : les menaces futures porteront sur le vol de propriété intellectuelle, la cyber-extorsion et l'impact de l'interruption d'activité après une cyber-attaque, ou sur une défaillance opérationnelle ou technique — un risque qui est souvent sous-estimé. « La prise de conscience des risques d'interruption d'activité et de l'assurance relative aux cyber-risques et à la technologie ne cesse de croître. Dans les cinq à dix prochaines années, l'interruption d'activité sera perçue comme un risque majeur et un élément principal du paysage des cyber-assurances », déclare Georgi Pachov, expert cyber dans l'équipe de souscription mondiale Dommages aux Biens d'AGCS. Dans le contexte des cyber-risques et des risques informatiques, la couverture interruption d'activité peut être très étendue, incluant les systèmes informatiques d'entreprise, mais aussi les systèmes de contrôle industriel (SCI) utilisés par des entreprises du secteur de l'énergie, ou encore les robots utilisés dans la production.

**La connectivité engendre le risque**

L'interconnectivité accrue des appareils que nous utilisons au quotidien et la dépendance croissante à la technologie et aux données en temps réel au niveau personnel comme à l'échelle de l'entreprise, connue sous le nom d'« Internet des objets », créent d'autres vulnérabilités. Certaines estimations suggèrent qu'un billion d'appareils pourraient être connectés d'ici 2020 et 50 milliards de machines pourraient échanger des données quotidiennement. Les SCI sont un autre sujet de préoccupation étant donné que nombre de ces systèmes qui sont toujours utilisés aujourd'hui ont été conçus avant que la cyber-sécurité devienne un problème prioritaire. Une attaque contre un SCI pourrait donner lieu à des dommages matériels comme un incendie ou une explosion, ainsi qu'à une interruption d'activité.

**Evénements catastrophiques**

Alors que des violations de données très importantes ont déjà eu lieu, la perspective d'une perte catastrophique est devenue plus probable, mais il est difficile de prédire ce qu'elle impliquera exactement. Les scénarios comprennent une attaque réussie contre l'infrastructure de base d'Internet, une violation grave des données ou une panne de réseau chez un fournisseur de cloud, alors qu'une cyber-attaque importante impliquant une entreprise d'énergie ou de services publics pourrait se traduire par une interruption significative des services, des dommages matériels ou même des pertes humaines à l'avenir.

**Couverture autonome**

D'après Allianz, la portée de la cyber-assurance doit également évoluer en vue de fournir une couverture plus étendue et plus approfondie, prenant en charge l'interruption d'activité et comblant les lacunes entre la couverture traditionnelle et les cyber-polices. Alors que les exclusions des cyber-risques dans les polices IARD vont vraisemblablement devenir monnaie courante, la cyber-assurance autonome va continuer d'évoluer pour devenir la source principale de couverture complète. On observe un intérêt croissant dans les secteurs des télécommunications, de la distribution, de l'énergie, des services publics et du transport, ainsi que de la part des institutions financières.

La formation — en termes de compréhension de l'exposition de l'entreprise comme de connaissances en souscription — doit s'améliorer pour permettre aux assureurs de répondre à une demande croissante. De plus, comme pour tout autre risque émergent, les assureurs doivent en outre faire face à des défis concernant la tarification, les libellés des polices non testés, la modélisation et l'accumulation des risques.

**Réponse aux cyber-risques**

Le rapport d'AGCS expose les démarches que les entreprises peuvent entreprendre pour couvrir les cyber-risques. L'assurance ne peut être qu'une partie de la solution, avec une approche globale de la gestion des risques en guise de fondement de la cyberdéfense. « Le fait de contracter une cyber-assurance ne signifie pas que vous pouvez ignorer la sécurité informatique. Les aspects technologiques, opérationnels et assurantiels de la gestion des risques vont de pair », explique Jens Krickhahn, expert Cyber & Fidelity chez AGCS Central & Eastern Europe. La gestion des cyber-risques est trop complexe pour être l'apanage d'un seul individu ou département, de sorte qu'AGCS recommande la constitution d'un groupe de réflexion pour combattre les risques, au sein duquel différentes parties prenantes dans toute l'entreprise collaboreraient pour partager leurs connaissances.

De cette manière, différentes perspectives sont remises en question et d'autres scénarios sont pris en considération : ceux-ci peuvent par exemple inclure le risque découlant des développements de l'entreprise comme les fusions et acquisitions, ou de l'utilisation de services externalisés ou d'un cloud. De plus, la contribution intersociétés est essentielle pour identifier les actifs clés en matière de risque et, surtout, pour développer et tester des plans d'action solides en cas de crise.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
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.globalsecuritymag.fr/Allianz-Global-Corporate-Specialty,20150909,55621.html

# Le vol d'identité en tête des attaques en cybercriminalité | Le Net Expert Informatique


## Le vol d'identité en tête des attaques en cybercriminalité

**Selon l'étude Breach Level Index pour le premier semestre 2015 publié par le leader mondial de la sécurité numérique Gemalto, il apparaît 888 failles de données signalées au cours de cette période, compromettant ainsi 246 millions d'enregistrements de données dans le monde.**

Les failles de sécurité ont augmenté de 10 % par rapport au premier semestre de l'année précédente, alors que le nombre d'enregistrements de données compromis diminuait de 41 % au cours des six premiers mois. Cette nette amélioration peut être attribuée à la diminution du nombre de méga-failles à très grande échelle ayant touché le commerce de détail et la distribution, comparativement à la même période de l'année écoulée.

Malgré la diminution du nombre de données compromises, les failles les plus importantes ont touché des volumes considérables d'informations personnelles. L'incident le plus important constaté au cours du premier semestre – niveau 10 sur l'échelle de gravité du Breach Level Index –, a concerné un vol d'identité dont a été victime l'assureur-santé Anthem Insurance aux États-Unis, qui a impacté 78,8 millions de fichiers, soit le tiers (32 %) de l'ensemble des fichiers de données volés au cours du premier semestre. Parmi les autres failles notables recensées au cours de la période d'analyse, il faut citer une attaque touchant 21 millions de fichiers de l'US Office of Personnel Management (9,7 sur l'échelle BLI) ; une attaque touchant 50 millions de fichiers de la Direction générale de la population et des affaires de la citoyenneté en Turquie (9,3 sur l'échelle BLI) ; et une défaillance affectant 20 millions de fichiers du site de rencontre russe Top Face (9,2 sur l'échelle BLI). Les dix principales cyber-attaques ont représenté 81,4 % de l'ensemble des fichiers compromis.

« Nous sommes obligés de constater le fort retour sur investissement des attaques sophistiquées que mènent les hackers, qui affectent des volumes considérables de données. Les cybercriminels continuent de s'approprier, la majeure partie du temps en toute impunité, des jeux de données extrêmement précieux. A titre d'exemple, les failles qui ont touché le secteur de la santé au cours du premier semestre leur ont permis de recueillir en moyenne plus de 450 000 fichiers de données, soit une augmentation de 200 % par rapport à la même période de 2014 », explique Jason Hart, vice-président et directeur de la technologie, en charge du pôle protection des données chez Gemalto.

**Incidents par source**

Le nombre d'attaques conduites à l'instigation ou avec la bénédiction d'un État ou d'un service gouvernemental n'ont représenté que 2 % de l'ensemble des incidents enregistrés. Le nombre de fichiers affectés par ces épisodes représente toutefois 41 % de l'ensemble des fichiers compromis, en raison notamment de l'attaque ayant ciblé Anthem Insurance et l'US Office of Personnel Management. Alors qu'aucune des dix principales failles enregistrées au premier semestre 2014 n'était le résultat d'une action soutenue par un État, trois des principaux incidents recensés cette année ont été menés à l'instigation de services gouvernementaux et notamment les deux premiers en termes de sévérité.

Les intrusions malveillantes menées à titre individuel ont cependant été la principale cause des failles de données enregistrées au premier semestre 2015, représentant 546 ou 62 % des attaques informatiques, contre 465 ou 58 % au premier semestre de l'année écoulée. 116 millions (soit 46 %) des fichiers affectés globalement l'ont été en raison d'intrusions malveillantes, ce qui constitue un net recul sur les 298 millions d'incidents (71,8 %) répertoriés en 2014.

**Incidents par type**

Le vol d'identité demeure, au premier semestre, la principale cible des cybercriminels, représentant 75 % de tous les fichiers affectés, et un peu plus de la moitié (53 %) des failles de données enregistrées. Cinq des dix principales failles, y compris les trois premières – toutes trois classées au niveau « catastrophique » sur l'échelle BLI –, ont porté sur des vols d'identité, contre sept sur dix au cours du premier semestre 2014.

**Incidents par secteur**

De tous les domaines d'activité recensés, les secteurs gouvernementaux et de la santé ont payé le plus lourd tribut à la cybercriminalité, puisqu'ils représentent environ les deux tiers (31 % et 34 % respectivement) des fichiers de données compromis. La santé ne représente toutefois que 21 % des atteintes informatiques enregistrées cette année, contre 29 % au cours du premier semestre de l'année précédente. Le secteur du commerce de détail et de la distribution connaît une nette diminution du nombre de fichiers volés, représentant seulement 4 %, contre 38 % au cours de la même période de l'année écoulée. En termes de localisation géographique, les États-Unis sont le pays le plus touché, avec plus des trois quarts (76 %) des failles de données enregistrées, et près de la moitié (49 %) de l'ensemble des fichiers affectés par des attaques. La Turquie représente 26 % des compromissions de données, avec notamment une attaque massive ciblant la Direction générale de la population et des affaires de la citoyenneté, au cours de laquelle quelque 50 millions de fichiers numériques ont été forcés dans le cadre d'une intrusion malveillante.

Le niveau de chiffrement utilisé pour protéger les données exposées – capable de réduire considérablement le nombre et l'impact des failles de données –, a légèrement augmenté et se situe à 4 % pour toutes les attaques enregistrées, contre 1 % au cours du premier semestre 2014.

« Malgré la fluctuation du nombre de failles de données, la question reste la même : il ne s'agit pas de savoir 'si' vous allez être victime d'un vol de données, mais 'quand'. Les données collectées dans le cadre de l'étude Breach Level Index montrent que la majeure partie des sociétés ne sont pas en mesure de protéger leurs données dès lors que leur défense périmétrique a été mise à mal. Alors même qu'un nombre croissant d'entreprises procèdent à un chiffrement de leurs données, elles ne le font pas au niveau requis pour réduire l'ampleur et la gravité de ces attaques », explique Jason Hart. « Les entreprises doivent adopter une vision de la menace numérique centrée sur les données, à commencer par l'instauration de techniques de gestion des identités et de contrôle d'accès beaucoup plus efficaces, qu'il s'agisse de procédures d'authentification multifactorielle ou du chiffrement des données, pour rendre inutilisables les informations dérobées. »

Selon le cabinet Forrester, l'habileté et la sophistication croissantes des cybercriminels se traduisent par une érosion de l'efficacité des contrôles et techniques de sécurité classiques, essentiellement basées sur un contrôle périphérique. La mutation constante du paysage de la cybercriminalité nécessite donc de nouvelles mesures défensives, avec notamment la généralisation des technologies de chiffrement. Dans l'avenir, les sociétés procéderont par défaut à un chiffrement dynamique de leurs données, mais aussi lorsque leurs systèmes et leurs données seront au repos. Cette approche de la sécurité centrée sur les données s'avère beaucoup plus efficace pour lutter contre des cybercriminels déterminés. En adoptant le chiffrement des données sensibles, qui les rend inutilisables, les sociétés incitent les cybercriminels à aller chercher des cibles beaucoup moins bien protégées. Le chiffrement est appelé à devenir la clé de voûte de la sécurité informatique. Ce sera donc un élément stratégique central pour les responsables de la sécurité et de la gestion des risques au sein des entreprises.

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
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://afriqueinside.com/securite-numerique-les-vols-didentite-en-tete-de-la-cybercriminalite09092015/

# L’Afrique prend la mesure du danger de la Cybercriminalité | Le Net Expert Informatique

| | |
|---|---|
| | L’Afrique prend la mesure du danger de la Cybercriminalité |

**La cybercriminalité est un phénomène qui prend de l'ampleur sur le continent. Et de plus en plus d'États africains prennent des mesures répressives pour décourager ceux qui veulent se lancer dans cette nouvelle forme de délinquance.**

C'est dans ce sens que la Tanzanie  vient de rejoindre le cercle des pays africains, comme la Zambie, le Nigeria, l'Afrique du Sud, la Mauritanie et le Kenya, qui ont pris le problème de la cybercriminalité à bras-le-corps. En effet, la Tanzanie va introduire une loi prévoyant jusqu'à 10 ans de prison pour les cyberdélinquants.
En mai dernier, une nouvelle loi sur la cybercriminalité était devenue opérationnelle au Nigéria. Qui devenait ainsi le premier pays, en Afrique de l'Ouest, à introduire des règles visant à réglementer le cyberespace selon Pcworld.
La Mauritanie avait, aussi, voté un projet de loi contre la cybercriminalité en août dernier. Ce projet de loi intervenait pour combler un vide juridique, avait expliqué le ministre mauritanien des TIC.
Face à la montée des inquiétudes, plusieurs pays comme la Côte d'Ivoire et le Rwanda jouent la carte de la sensibilisation contre ce fléau.
Alors que la Tanzanie a l'un des taux de cybercriminalité, sur les médias sociaux, les plus élevés en Afrique, le président tanzanien, Jakaya Kikwete, a déjà approuvé la loi sur la cybercriminalité de 2015, qui deviendra opérationnelle cette semaine.
Avec un nombre de plus en plus important d'Africains qui utilisent Internet – en plus des efforts fournis par les États en vue de réduire la fracture numérique -, il devient primordial de lutter, sur le continent, contre la cybercriminalité. Ce sera à coup sûr l'un des défis majeurs à relever dans le domaine du numérique.

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
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.afriq
ueitnews.com/2015/09/09/cybercriminalite
-lafrique-prend-mesure-danger/

# Jusqu’à 200 000 utilisateurs WhatsApp touchés par une cyberattaque | Le Net Expert Informatique


## Jusqu’à 200 000 utilisateurs WhatsApp touchés par une cyberattaque

**Jusqu'à 200 000 utilisateurs du service de messagerie WhatsApp pourraient avoir été touchés par une cyberattaque permettant aux pirates de compromettre les données personnelles en utilisant simplement son numéro de téléphone.**

Selon Checkpoint, une vulnérabilité dans la version web du service de messagerie WhatsApp aurait exposé jusqu'à 200 000 utilisateurs à une cyberattaque permettant aux pirates de compromettre les données personnelles. Pour cette attaque, les pirates ont simplement envoyé une vCard infectée à des numéros de téléphone au hasard.

Checkpoint précise que la faille dans la version web de WhatsApp pouvait être facilement exploitée par des personnes malveillantes, « sans aucun outil » spécifique.

Signalée à WhatsApp le 21 août dernier, la faille a été corrigée le 27 août. Ce n'est que maintenant que Checkpoint annonce sa découverte.

« Heureusement, WhatsApp a réagi rapidement et de manière responsable en déployant rapidement un correctif contre l'exploitation de cette faille dans le client web », écrit Oded Vanunu, gestionnaire de groupe de recherche de sécurité chez Checkpoint.

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

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 !

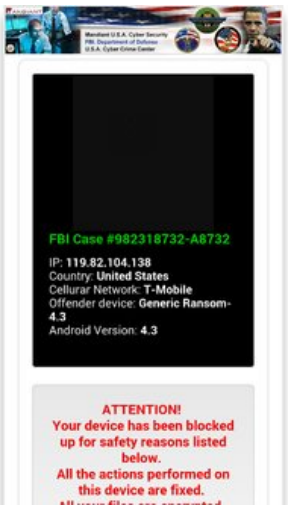
Un avis ? Laissez-nous un commentaire !

Source :
http://www.linformatique.org/whatsapp-jusqua-200-000-utilisateurs-touches-par-une-cyberattaque.html
Par Emilie Dubois

---

# Insolite : Une application porno fait du racket – Un Racketware ? | Le Net Expert

# Informatique




## Insolite : Une application porno fait du racket – Un Racketware ?

**Adult Player, une prétendue application mobile de pornographie, dérobe des clichés de ses utilisateurs avant de les obliger à payer 500 dollars pour débloquer leur smartphone.**

On le sait, smartphone et pornographie font bon ménage. Récemment, d'après une étude du cabinet Juniper Research, plus de 136 milliards de vidéos X devraient être consultées depuis des terminaux mobiles en 2015, soit 348 vidéos par utilisateur. Ce chiffre devrait s'élever à 193 milliards en 2020. Une application malveillante a choisi de surfer sur cette tendance.

Le spécialiste de la sécurité Zscaler explique sur son site avoir découvert l'application Adult Player, ciblant les smartphones Android. Il s'agit plus précisément d'un ransomware, c'est-à-dire que ses concepteurs effectuent une forme de racket auprès des victimes.


Adult Player se fait passer pour un lecteur de vidéos pornographiques mais effectue des clichés de ses victimes à leur insu en exploitant la caméra frontale de l'appareil. Par la suite, l'application bloque le smartphone et présente la photo sur l'écran de verrouillage tout en demandant une rançon de 500 dollars.

Pour désinstaller cette application malveillante, il faudra redémarrer le smartphone en safe mode, c'est-à-dire sans exécuter les applications tierces. Rendez-vous ensuite dans les Paramètres > Sécurité > Administrateur pour désactiver les droits alloués à Adult Player. Ensuite, toujours dans les paramètres, rendez-vous dans Applications > Désinstaller.


---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
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.clubic.com/insolite/actualite-778656-insolite-application-porno-racket.html#pid=22889469
Par Guillaume Belfiore

# Alerte : L’éditeur de Firefox victime d’un piratage | Le Net Expert Informatique

## Alerte : L’éditeur de Firefox victime d’un piratage

**La Fondation Mozilla, qui édite notamment le navigateur Firefox, a annoncé vendredi 4 septembre qu’elle avait été victime d’un piratage touchant Bugzilla, son outil de notification de bugs. « Quelqu’un est parvenu à voler des informations sensibles touchant à la sécurité [de Firefox]. Nous pensons que ces informations ont été utilisées pour mener des attaques informatiques contre des utilisateurs de Firefox », est-il écrit sur le site de la fondation.**

Les informations volées contenaient entre autres des détails sur une vulnérabilité présente dans une précédente version de Firefox, qui a été corrigée le 27 août dans la dernière mise à jour du logiciel.
Mozilla a également annoncé avoir renforcé la sécurité de Bugzilla, et a transmis les informations collectées lors de son enquête interne aux autorités. « L’ouverture, la transparence et la sécurité sont au cœur de notre mission, écrit la fondation. Et c’est pourquoi nous rendons publics les bugs que nous détectons une fois qu’ils ne sont plus dangereux, et que nous le disons publiquement lorsqu’il y a un accès non autorisé à nos infrastructures. »

---

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
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/2015/09/07/l-editeur-de-firefox-victime-d-un-piratage_4747961_4408996.html