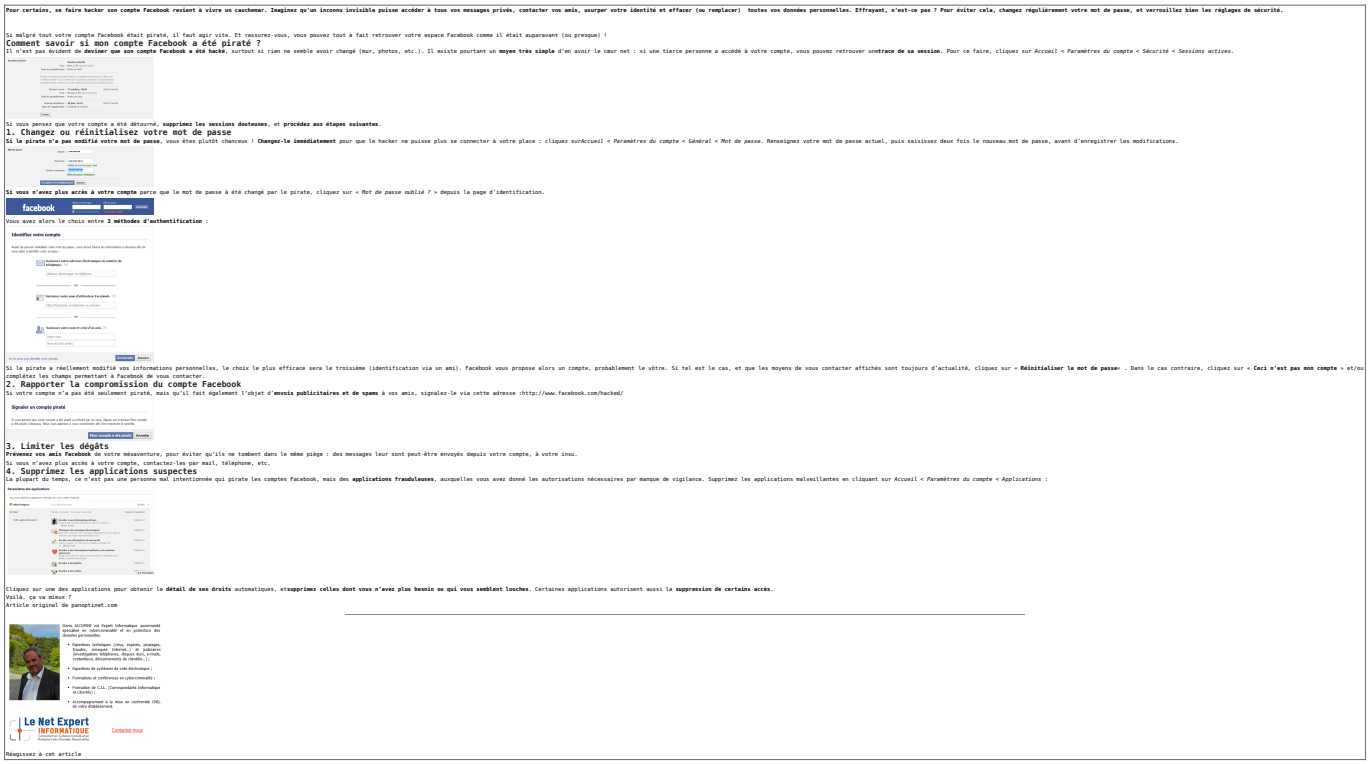
# Que faire quand son compte Facebook est piraté ?

| | |
|---|---|
|  | Que faire quand son compte Facebook est piraté ? |



**Pour certains, se faire hacker son compte Facebook revient à vivre un cauchemar. Imaginez qu'un inconnu invisible puisse accéder à tous vos messages privés, contacter vos amis, usurper votre identité et effacer (ou remplacer) toutes vos données personnelles. Effrayant, n'est-ce pas ? Pour éviter cela, changez régulièrement votre mot de passe, et verrouillez bien les réglages de sécurité.**

Si malgré tout votre compte Facebook était piraté, il faut agir vite. Et rassurez-vous, vous pouvez tout à fait retrouver votre espace Facebook comme il était auparavant (ou presque) !

**Comment savoir si mon compte Facebook a été piraté ?**

Il n'est pas évident de **deviner que son compte Facebook a été hacké**, surtout si rien ne semble avoir changé (mur, photos, etc.). Il existe pourtant un **moyen très simple** d'en avoir le cœur net : si une tierce personne a accédé à votre compte, vous pouvez retrouver une**trace de sa session**. Pour ce faire, cliquez sur *Accueil* < *Paramètres du compte* < *Sécurité* < *Sessions actives*.

Si vous pensez que votre compte a été détourné, **supprimez les sessions douteuses**, et **procédez aux étapes suivantes**.

**1. Changez ou réinitialisez votre mot de passe**

**Si le pirate n'a pas modifié votre mot de passe**, vous êtes plutôt chanceux ! **Changez-le immédiatement** pour que le hacker ne puisse plus se connecter à votre place : cliquez sur*Accueil* < *Paramètres du compte* < *Général* < *Mot de passe*. Renseignez votre mot de passe actuel, puis saisissez deux fois le nouveau mot de passe, avant d'enregistrer les modifications.

**Si vous n'avez plus accès à votre compte** parce que le mot de passe à été changé par le pirate, cliquez sur < *Mot de passe oublié ?* > depuis la page d'identification.

Vous avez alors le choix entre **3 méthodes d'authentification** :

Si le pirate a réellement modifié vos informations personnelles, le choix le plus efficace sera le troisième (identification via un ami). Facebook vous propose alors un compte, probablement le vôtre. Si tel est le cas, et que les moyens de vous contacter affichés sont toujours d'actualité, cliquez sur « **Réinitialiser le mot de passe**» . Dans le cas contraire, cliquez sur « **Ceci n'est pas mon compte** » et/ou compléter les champs permettant à Facebook de vous contacter.

**2. Rapporter la compromission du compte Facebook**

Si votre compte n'a pas été seulement piraté, mais qu'il fait également l'objet d'**envois publicitaires et de spams** à vos amis, signalez-le via cette adresse :http://www.facebook.com/hacked/

**3. Limiter les dégâts**

**Prévenez vos amis Facebook** de votre mésaventure, pour éviter qu'ils ne tombent dans le même piège : des messages leur sont peut-être envoyés depuis votre compte, à votre insu.

Si vous n'avez plus accès à votre compte, contactez-les par mail, téléphone, etc.

**4. Supprimez les applications suspectes**

La plupart du temps, ce n'est pas une personne mal intentionnée qui pirate les comptes Facebook, mais des **applications frauduleuses**, auxquelles vous avez donné les autorisations nécessaires par manque de vigilance. Supprimez les applications malveillantes en cliquant sur *Accueil* < *Paramètres du compte* < *Applications* :

Cliquez sur une des applications pour obtenir le **détail de ses droits** automatiques, et**supprimez celles dont vous n'avez plus besoin ou qui vous semblent louches**. Certaines applications autorisent aussi la **suppression de certains accès**.

Voilà, ça va mieux ?

Article original de panoptinet.com

Réagissez à cet article

Original de l'article mis en page : Que faire quand son compte Facebook est piraté ? | Panoptinet

---

# Les mots de passe disparaîtront progressivement d'ici 2025


Les mots de passe disparaîtront progressivement d'ici 2025

---

**La technologie de biométrie comportementale et d'authentification à deux facteurs sont à la hausse comme des alternatives plus sûres, selon une étude.**

Une étude de 600 professionnels en sécurité de l'opérateur de téléphonie mobile ID TeleSign a révélé que la protection du compte client est un souci majeur pour les entreprises, avec 72 % des personnes interrogées disant que les mots de passe seront éliminés progressivement d'ici à 2025. De plus en plus d'entreprises, selon le rapport, remplacent les mots de passe avec la biométrie comportementale et l'authentification à deux facteurs (2FA) avec 92 % des experts en sécurité affirmant que cela va améliorer la sécurité des comptes considérablement.

« La grande majorité des professionnels en sécurité ne font plus confiance aux mots de passe pour travailler », a déclaré Ryan Disraeli de TeleSign parce que 69 % des répondants ont dit qu'ils ne pensent pas que les noms d'utilisateur et mots de passe fournissent assez de sécurité. Les prises de contrôle de compte (ATO) étaient une préoccupation majeure pour 79 %, alors que 86 % sont préoccupés par l'authentification ID d'identité des utilisateurs du web et des applications mobiles avec 90 % étant touchées par des fraudes en ligne l'an dernier.

Plus de la moitié (54 %) des organisations disent qu'ils passeront à la biométrie comportementale en 2016 ou plus tard tandis que 85 % ont dit qu'ils mettraient en œuvre le 2FA dans les 12 prochains mois. Huit des 10 répondants croient que la biométrie comportementale ne dégradera pas l'expérience utilisateur.

Lire l'étude complète ici

https://iatranshumanisme.files.wordpress.com/2016/07/telesign-report-beyond-the-password-june-2016-1.pdf

Article original de Jaesa

---



Réagissez à cet article

Original de l'article mis en page : Les mots de passe disparaîtront progressivement d'ici 2025 | Intelligence Artificielle et Transhumanisme

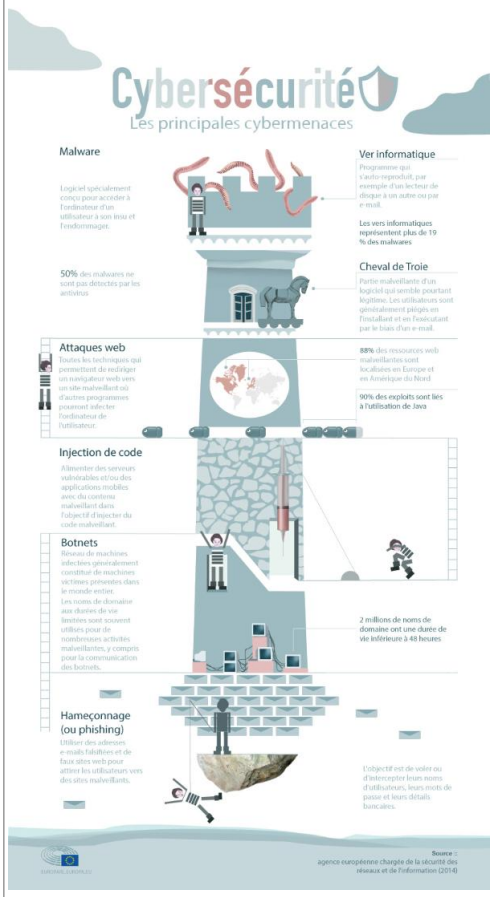
---

# Directive sur la sécurité des

# réseaux et des systèmes d’information

## Directive sur la sécurité des réseaux et des systèmes d’information

**Nos sociétés digitalisées reposent de plus en plus sur des réseaux électroniques qui peuvent faire l'objet de cyberattaques aux conséquences importantes. Afin de mieux faire face à ce type de menaces en ligne, le Parlement et le Conseil ont conclu en décembre dernier un accord sur les premières règles européennes en matière de cybersécurité. Celles-ci ont été soutenues par l'ensemble du Parlement réuni en session plénière ce mercredi 6 juillet.**




Vols d'identité, faux sites web de banques, espionnage industriel ou inondation de données qui rendent un serveur incapable de répondre : les menaces en ligne sont nombreuses et visent tant les particuliers que les entreprises et les autorités publiques.
Les incidents et les attaques des systèmes d'information des entreprises et des citoyens pourraient représenter un coût de 260 à 340 milliards d'euros par an, selon les estimations de l'Agence européenne chargée de la sécurité des réseaux et de l'information.
Les cyberattaques menées contre certaines infrastructures clés de nos sociétés, comme les services bancaires, les réseaux d'électricité ou le secteur du contrôle aérien, peuvent avoir des conséquences particulièrement importantes sur notre quotidien.
Dans le cadre d'un Eurobaromètre publié en février 2015, les citoyens européens ont exprimé de fortes inquiétudes à propos de la cybersécurité : 89 % des internautes évitent de diffuser des informations personnelles en ligne. Selon 85 % des sondés, le risque d'être victime de cybercriminalité est de plus en plus important.

**Vote en plénière**
Les députés ont approuvé la directive sur la sécurité des réseaux et de l'information dans l'Union, qui définit une approche commune autour de la question de la cybersécurité.
Le texte prévoit une liste de secteurs dans lesquels les entreprises qui fournissent des services essentiels, liés par exemple à l'énergie, aux transports ou au secteur de la banque, devront être en mesure de résister aux cyberattaques.
La directive les oblige notamment à signaler les incidents de sécurité graves aux autorités nationales. Les fournisseurs de services numériques tels qu'Amazon ou Google devront également notifier les attaques majeures aux autorités nationales.
Ces nouvelles règles sur la cybersécurité visent également à renforcer la coopération entre États membres en cas d'incidents.

Téléchargez la directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil :
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Article original du Parlement Européen

---



Réagissez à cet article

Original de l’article mis en page : Cybersécurité : mieux faire face aux attaques en ligne

---

# Le Bénin, capitale de la cyber-arnaque en Afrique de l’Ouest


Le Bénin, capitale de la cyber-arnaque en Afrique de l’Ouest

---

**Au Bénin, les cybercriminels sont habituellement connus sous le nom de « Gaymans. » Les premières méthodes d'escroquerie concernaient les réseaux de jeunes se faisant passer pour des homosexuels, pour appâter des personnes de la même orientation sexuelle dans les pays occidentaux, d'où le nom de « Gayman » donné à la plupart des cybercriminels opérant à partir du Bénin.**

Le phénomène fait son apparition dans les années 2000 et se caractérise essentiellement par des arnaques en ligne par des individus sans connaissance particulière en informatique, mais avec de solides atouts en psychologie.

Pour Nicaise Dangnibo, le directeur de l''Office central de répression de la cybercriminalité (OCRC), une unité spéciale de la police béninoise, « le phénomène a pris ses racines à partir du Nigeria, l'un des tout premiers pays d'Afrique de l'Ouest confrontés au phénomène de la cybercriminalité. »

Avec les premières mesures de rétorsion mises en place par les autorités nigérianes, les cybercriminels se sont massivement délocalisés au Bénin et en Côte d'Ivoire.

Ces derniers copiaient sur Internet des photos de jeunes hommes « beaux et musclés » à la recherche de l'âme soeur.

Les méthodes d'escroquerie se sont ensuite diversifiées, pour s'étendre au love chat, au porno-chantage, puis à des montages complexes de fausses affaires.

***"Internet a certes révolutionné le monde au point qu'il serait difficile d'imaginer un autre monde sans internet ; mais, autant les coupeurs de routes existent et pourtant nous circulons sur nos routes, autant les flibustiers existent et pourtant nous naviguons sur les eaux ; autant les cybercriminels existeront toujours et nous allons toujours surfer sur le net."***

***Pierre Dovonou Lokossou***

***Gestionnaire de projets technologiques***

*Selon Pierre Dovonou Lokossou, gestionnaire de projets technologiques, « la première arnaque via l'Internet au Bénin a eu lieu deux ans après l'arrivée du web dans le pays. Il s'agissait d'un Nigérian se prénommant Christopher qui avait escroqué un pasteur américain (Jim), en se faisant livrer 40 ordinateurs, 10 imprimantes et un millier de bibles, en échange d'un chèque délivré par une banque fictive ».*

*Pierre Dovonou Lokossou raconte qu'à cette époque, « la plupart des mails indésirables (spams) provenant du Bénin étaient en anglais. La répression des actes de cybercriminalité au Nigéria avait vite fait de déverser au Bénin et dans la sous-région de jeunes Nigérians qui pouvaient désormais poursuivre en toute impunité leurs sales besognes… »*

*« Par la suite, ajoute-t-il, de l'anglais, les spams ont commencé à être rédigés dans un français approximatif, signe qu'avec le séjour de ces cybercriminels anglophones au Bénin, l'apprentissage de la langue française a été mis à contribution. »*

*Mais actuellement, à en croire le gestionnaire de projets, « le phénomène a pris de l'ampleur dans toute la sous-région ouest-africaine ». « Aussi bien des Béninois que des Togolais et des Burkinabè, des Nigériens et des Ivoiriens s'adonnent à cœur joie à ce cyber-banditisme », précise-t-il.*

***Offres de vente***

*Il s'agit le plus souvent de propositions de prêts, voire de dons ou d'offres de vente assez diversifiées diffusées sur des sites internet, ou parfois envoyées sous forme de spams aux internautes.*

*Les offres de vente vont des appareils électroménagers aux métaux précieux en passant par les téléphones portables, les ordinateurs, les véhicules, voire les animaux ou les domaines fonciers.*

*Une étudiante en Relations internationales, Adidjath Kitoyi, raconte avoir été contactée en 2012 sur le réseau social Facebook par « une Suissesse âgée de 83 ans atteinte d'un cancer au stade très avancé » qui souhaitait lui céder « une fortune héritée de ses parents et qui se trouve dans les coffres d'une banque à Genève ».*

*Appâtée, Adidjath s'était empressée d'envoyer à une adresse indiquée (qui se révèlera inexistante) tous les documents administratifs réclamés par son interlocuteur avant d'effectuer à l'attention d'un « intermédiaire » basé en Côte d'Ivoire un transfert de 150 000 FCFA représentant « les frais de dossiers ».*

*Par la suite, il ne lui était plus possible de communiquer avec la Suissesse donatrice, ni avec l'intermédiaire en Côte d'Ivoire.*

*La mésaventure d'Adidjath Kitoyi n'est qu'un cas parmi des centaines, voire des milliers d'autres victimes des cybercriminels.*

***Pierre Dovonou Lokossou distingue trois catégories de cybercriminels.***

*« La première est celle de ces jeunes qui n'ont pas un emploi légal connu et qui ne fréquentent que les cybercentres ou qui sont toujours avec leur ordinateur portatif et qui ont un train de vie largement au-dessus de la moyenne. Ils changent souvent de motos ou de voitures. Ils peuvent disparaître du quartier pendant des mois et réapparaître pour faire croire aux gens qu'ils étaient en France ou à Abidjan, alors qu'ils étaient en prison ou en cavale; la deuxième catégorie est celle des jeunes qui vont, soit au collège, soit à l'université, ou qui ont un emploi, mais s'adonnent à la cybercriminalité et à divers autres actes d'escroquerie; la troisième catégorie comporte les jeunes qui sont embauchés souvent par les cyber-bandits de la première ou deuxième catégorie et qui jouent le rôle d'assistants. Ce sont eux qui vont récupérer l'argent à la banque, qui jouent le rôle de secrétaire, d'avocat, de notaire pour confirmer au téléphone que le patron ou "son client" est quelqu'un de "bonne foi"…*

***Dispositif législatif***

*De 1997 à ce jour, ce qui n'était alors qu'un cas isolé à l'époque s'est mué en un cas d'école. De 2005 à 2010 notamment, le nombre de jeunes quittant les bancs au profit des cybercafés a considérablement augmenté.*

*Aujourd'hui encore, le phénomène est palpable et les nombreuses descentes de la police ne découragent pas les malfaiteurs.*

*A la sous-direction des crimes économiques et financiers de la police béninoise (ex-Brigade économique et financière-BEF), la cellule de lutte contre la cybercriminalité a déjà eu à effectuer plusieurs arrestations.*

*De source proche de ce service de police, quelques-uns des auteurs de ces forfaits via le web croupissent en prison.*

*La loi portant lutte contre la corruption, adoptée en 2011, qui y consacre tout son chapitre XV (« Des infractions cybernétiques, informatiques et de leur répression »), condamne fermement la cybercriminalité.*

*L'article 124 dispose notamment : « Quiconque a procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, est puni d'un emprisonnement d'un an à cinq ans et d'une amende de deux millions de francs CFA à vingt millions. »*

*Mais du dispositif législatif à la réalité sur le terrain, semble exister un grand fossé.*

*La note d'alerte de l'ambassade de France au Bénin citée plus haut est sans ambages :*

*Toutefois, des réflexions existent sur le plan local en faveur de la lutte contre la cybercriminalité.*

*En 2010, le professeur agrégé de droit, Joseph Djogbénou, concluait ainsi une étude intitulée « la cybercriminalité : enjeux et défis pour le Bénin » :*

*« Le cybermonde appelle la cybercriminalité. A la lumière de l'ensemble de ces considérations, la réponse nationale devra répondre à une double exigence de cohérence. En premier lieu, elle doit, et il ne saurait en être autrement, tenir compte de la convention de Budapest avec laquelle elle doit nécessairement être compatible. En second lieu, elle doit forcément s'inscrire dans un environnement régional propice. La situation est donc mûre (à notre sens) pour un instrument régional en la matière. Toutefois, il faut sur ce sujet un changement d'approche. En effet, l'examen des travaux réalisés jusqu'ici montre que la cybercriminalité n'est pas traitée de façon spécifique, mais comme un aspect particulier de la criminalité organisée. Ici encore c'est aux experts béninois et africains de mettre en exergue la nécessité et l'exigence d'une approche spécifique de la question. C'est à ce prix que l'Afrique parviendra à s'arrimer à la révolution post-industrielle en cours. »*

*Pour sa part, le gestionnaire de projets technologiques, Pierre Dovonou Lokossou appelle à éviter le piège de la résignation : « Internet a certes révolutionné le monde au point qu'il serait difficile d'imaginer un autre monde sans internet ; mais, autant les coupeurs de routes existent et pourtant nous circulons sur nos routes, autant les flibustiers existent et pourtant nous naviguons sur les eaux ; autant les cybercriminels existeront toujours et nous allons toujours surfer sur le net. »*

*Le plus urgent, selon lui, « c'est que nos autorités prennent le taureau par les cornes pour freiner de façon drastique ce fléau qui n'honore pas le Bénin et la sous-région ouest-africaine. »*

*Article original de Virgile Ahissou*

---



*Réagissez à cet article*

Original de l’article mis en page : Le Bénin, capitale de la cyber-arnaque en Afrique de l’Ouest – SciDev.Net Afrique Sub-Saharienne

---

# Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »


Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

---

**Locky, TeslaCrypt, Cryptolocker, Cryptowall… Depuis plusieurs mois, les rançongiciels (« ransomware »), ces virus informatiques qui rendent illisibles les données d'un utilisateur puis lui réclament une somme d'argent afin de les déverrouiller, sont une préoccupation croissante des autorités. Le commissaire François-Xavier Masson, chef de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, une unité de la police spécialisée dans la criminalité informatique, explique au Monde les dangers de cette menace.**

**Combien y a-t-il d'attaques par rançongiciel en France ?**
On ne le sait pas avec précision, nous n'avons pas fait d'étude précise à ce sujet. Statistiquement, le rançongiciel ne correspond pas à une infraction pénale précise et il recoupe parfois l'intrusion dans un système automatisé de traitement de données. Il faudrait affiner le cadre car nous avons besoin de connaître l'état de la menace.
**Avez-vous quand même une idée de l'évolution du phénomène ?**
L'extorsion numérique est clairement à la hausse, c'est la grande tendance en termes de cybercriminalité depuis 2013. Tout le monde est ciblé : les particuliers, les entreprises, même l'Etat. Les attaques gagnent en sophistication et en intensité. Il y a aussi une industrialisation et une professionnalisation. La criminalité informatique est une criminalité de masse : d'un simple clic on peut atteindre des millions de machines. Désormais, il n'y a plus besoin de vous mettre un couteau sous la gorge ou de kidnapper vos enfants, on s'en prend à vos données.
**Les victimes ont-elles le réflexe de porter plainte ?**
Certaines victimes paient sans porter plainte. Ce calcul est fait par les entreprises qui estiment que c'est plus pratique de payer la rançon – dont le montant n'est pas toujours très élevé, de l'ordre de quelques bitcoins ou dizaines de bitcoins – et qu'en portant plainte, elles terniront leur image et ne récupéreront pas nécessairement leurs données. Elles pensent aussi que payer la rançon coûtera moins cher que de payer une entreprise pour nettoyer leurs réseaux informatiques et installer des protections plus solides. C'est une vision de court terme. Nous recommandons de ne pas payer la rançon afin de ne pas alimenter le système. Si l'on arrête de payer les rançons, les criminels y réfléchiront à deux fois. C'est la même doctrine qu'en matière de criminalité organisée.
**Qu'est-ce qui pousse à porter plainte ?**
Chaque cas est unique mais généralement, c'est parce que c'est la politique de l'entreprise ou parce que le montant de la rançon est trop élevé.
**Qui sont les victimes ?**
Il s'agit beaucoup de petites et moyennes entreprises, par exemple des cabinets de notaires, d'avocats, d'architectes, qui ont des failles dans leur système informatique, qui n'ont pas fait les investissements nécessaires ou ne connaissent pas forcément le sujet. Les cybercriminels vont toujours profiter des systèmes informatiques vulnérables.
**Quel est votre rôle dans la lutte contre les rançongiciels ?**
La première mission, c'est bien sûr l'enquête. Mais nous avons aussi un rôle de prévention : on dit que la sécurité a un coût mais celui-ci est toujours inférieur à celui d'une réparation après un piratage. Enfin, de plus en plus, nous offrons des solutions de remédiation : nous proposons des synergies avec des entreprises privées, des éditeurs antivirus. On développe des partenariats avec ceux qui sont capables de développer des solutions. Si on peut désinfecter les machines nous-mêmes, on le propose, mais une fois que c'est chiffré, cela devient très compliqué : je n'ai pas d'exemple de rançongiciel qu'on ait réussi à déverrouiller.
**Quel rapport entretenez-vous avec les entreprises ?**
On ne peut pas faire l'économie de partenariats avec le secteur privé. Nous pourrions développer nos propres logiciels mais ce serait trop long et coûteux. Il y a des entreprises qui ont des compétences et la volonté d'aider les services de police.
**Parvenez-vous, dans vos enquêtes, à identifier les responsables ?**
On se heurte très rapidement à la difficulté de remonter vers l'origine de l'attaque. Les rançongiciels sont développés par des gens dont c'est le métier, et leur activité dépasse les frontières. On a des idées pour les attaques les plus abouties, ça vient plutôt des pays de l'Est. Mais pas tous.
**Parvenez-vous à collaborer avec vos homologues à l'étranger ?**
Oui, c'est tout l'intérêt d'être un office central, nous sommes le point de contact avec nos confrères internationaux. Il y a beaucoup de réunions thématiques, sous l'égide de l'Office européen de police (Europol), des pays qui mettent en commun leurs éléments et décrivent l'état d'avancement de leurs enquêtes. C'est indispensable de mettre en commun, de combiner, d'échanger des informations. Il peut y avoir des équipes d'enquête communes, même si ça ne nous est pas encore arrivé sur le rançongiciel.
**De plus en plus d'enquêteurs se penchent sur le bitcoin – dont l'historique des transactions est public – comme outil d'enquête. Est-ce aussi le cas chez vous ?**
C'est une chose sur laquelle on travaille et qui nous intéresse beaucoup. S'il y a paiement en bitcoin, il peut y avoir la possibilité de remonter jusqu'aux auteurs. C'est aussi pour cela que l'on demande aux gens de porter plainte même lorsqu'ils ont payé.
Article original de Martin Untersinger

---

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

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

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Rançongiciels : « Désormais, plus besoin de kidnapper vos enfants, on s’en prend à vos données »

---

# Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet

Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet

---

**Sans utiliser la moindre carte de crédit, deux hommes ont volé 1,7 millions d'euros à la First Commercial Bank de Taïwan.**

Les « casses du siècles » deviennent de plus en plus cocasses et subtiles à l'ère du tout numérique. Chaque mois ou presque, on peut trouver un exemple de vol de banque, qui mêle développement logiciel et matériel. Cette fois le crime n'implique pas le vol ou la copie de cartes de crédit : à Taïwan, deux pirates ont réussi à retirer l'argent de 30 distributeurs sans se faire prendre. La somme volée s'élève à 70 millions de dollars taïwanais.
Leur méthode était particulièrement rodée. En moins de 10 minutes, les voleurs ont exécuté un programme dans le système du distributeur de billet qui, bien gentiment, a offert ses devises sans demander de compte. Le logiciel a ensuite pris soin d'effacer toute trace du larcin. Et les voleurs sont repartis, à 30 reprises, avec le gros lot. Les enquêteurs ne savent toujours pas comment les pirates ont fait pour déployer leur code aussi rapidement sur les distributeurs, ni quel moyen a été utilisé pour se connecter aux machines – un smartphone est évoqué.

*LES VOLEURS SONT REPARTIS, À 30 REPRISES, AVEC LE GROS LOT*
*Les deux hommes seraient des étrangers : l'un d'eux a été identifié comme étant un citoyen russe qui s'est enfui de l'île dimanche et est recherché par Interpol. L'identité et la nationalité de l'autre homme ne sont pas connues. En attendant les experts de la compagnie allemande qui fournit les distributeurs à la banque taïwanaise qui a été prise pour cible, la décision de bloquer tous les distributeurs du même fournisseur a été prise par les autorités. 400 distributeurs de billet ont donc été rendus inactifs.*
*Article original de Julien Cadot*

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

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

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

Contactez-nous

*Réagissez à cet article*

Original de l’article mis en page : Deux hommes ont volé 1,7 million d’euros en piratant des distributeurs de billet – Tech – Numerama

---

# Huit bonnes pratiques pour bien sécuriser les objets connectés

Huit bonnes pratiques pour bien sécuriser les objets connectés

---

**Il existe aujourd'hui des failles de sécurité qui permettent d'accéder au capteur, de s'y connecter et d'y collecter des informations. Comment alors se protéger contre de telles intrusions ? Le point.**

Gartner prédit 26 milliards d'objets connectés d'ici 2020. En 2016 ce sont 4,9 milliards de dispositifs connectés qui devraient être déployés. Des objets qui seront potentiellement confrontés à un grand nombre d'attaques. En effet, le volume des cyber-attaques recensé par l'étude The Global State of Information Security® Survey 2016, réalisée par le cabinet d'audit et de conseil PwC en collaboration avec CIO et CSO, a progressé de 38 % dans le monde en 2015. Comment alors sécuriser au mieux ses objets connectés ?

**En appliquant quelques bonnes pratiques.**

Il existe aujourd'hui des failles de sécurité qui permettent d'accéder au capteur, de s'y connecter et d'y collecter des informations. Comment alors se protéger contre de telles intrusions ? Plusieurs zones « sensibles » sont donc à surveiller au sein des objets connectés notamment au niveau du capteur et au niveau du transfert des données.

Pour le capteur, l'un des moyens les plus efficaces pour se protéger consiste à sécuriser le hardware grâce à un Secure Element, qui empêche tout accès à l'information lorsqu'on se connecte au capteur. Un élément sécurisé repose sur une plate-forme matérielle inviolable qui héberge des données, cryptées ou non, en toute sécurité et en conformité avec les règles de sécurité fixées par les autorités de confiance. Certains de ces éléments, comme les cartes microSD, peuvent même être amovibles.

Pour sécuriser les données, il est indispensable d'utiliser des technologies de chiffrement robustes afin de lutter contre le piratage ou les interceptions. En effet, le chiffrement rend les données impossibles à lire pour qui ne possède pas la clé de déchiffrement de 128 bits ! Efficace pour repousser les hackers même les plus coriaces.

Une fois le capteur protégé et les données chiffrées, il est important d'assurer la sécurité de l'information lors de son transfert de bout en bout : du capteur jusqu'au portail client.

L'utilisation d'un système de clés multiples géré par un tiers de confiance tel que le propose le protocole LoRa s'avère une solution des plus fiables.

Un tiers de confiance fournit un système de gestion de clé – Key Management System (KMS) – qui permet de générer une AppKey unique pour chaque capteur. A chaque nouvelle session, une AppSKey – Application Session Key – dérivée de l'AppKey sert au chiffrement des données du client. L'opérateur n'a pas accès à ces 2 clés, elles ne sont connues que du tiers de confiance dans le KMS et du client bien sûr pour déchiffrer les données.

Une fois les données récupérées, l'utilisation d'un VPN est bien sûr conseillé.

En agissant à ces différents niveaux, vous appliquez une sécurité optimale à vos objets connectés. De plus, vous pouvez appliquer quelques conseils pour assurer une sécurité de bout en bout des processus :

1. Évaluez le bon degré de sécurité sur le capteur en fonction de la criticité de la donnée : selon l'information concernée, il n'est pas forcément nécessaire d'insérer un Secure Element dans le capteur.
2. Utilisez une technologie avec un protocole de chiffrement robuste de type AES128 par exemple.
3. Mettez en place des infrastructures intégrant l'état de l'art en termes de chiffrement.
4. N'écrivez pas vos clés de cryptage sur disque dur : privilégiez les éléments de sécurité non stockés et volatiles. Calculées « à la demande » par un algorithme, elles ne peuvent donc pas être piratées en cas d'attaque sur la base de données.
5. Optez pour un renouvellement de la clé de chiffrement à chaque connexion du capteur sur le réseau. Une clé renouvelée régulièrement à moins de risque d'être piratée.
6. Utilisez un portail sécurisé pour accéder à vos données applicatives chiffrées : vous avez ainsi, seul, la possibilité de déchiffrer les données. Toutefois, si vous choisissez de ne pas les déchiffrer vous-même, assurez-vous que votre prestataire le fasse sur un cloud sécurisé.
7. Choisissez des technologies en perpétuelle évolution : au sein de la LoRa Alliance, un groupe dédié fait évoluer en permanence le protocole afin d'être toujours à la pointe de la sécurité.
8. Optez pour un opérateur qui intègre les processus de sécurité recommandés par l'ANSSI dans la conception et l'exploitation de son réseau.

Article original de Franck Moine

---

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

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

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

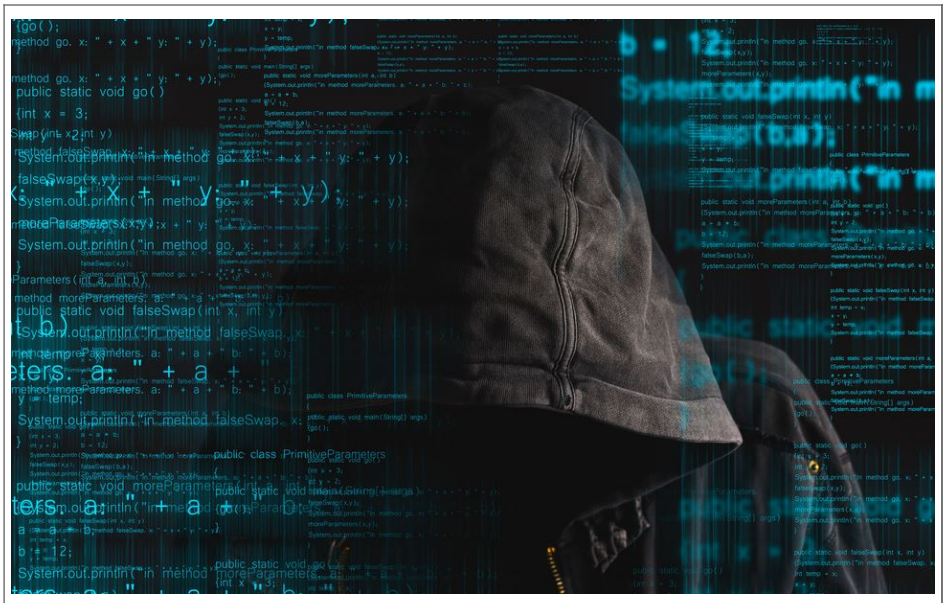
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Huit bonnes pratiques pour bien sécuriser les objets connectés – JDN

---

# Un cousin du malware Furtim cible les énergéticiens européens



Un cousin du malware Furtim cible les énergéticiens européens

---

**SentinelOne a découvert une variante du malware Furtim qui vise les sociétés européennes dans le domaine de l'énergie.**

En mai dernier, des chercheurs la société EnSilo ont découvert un malware baptisé Furtim qui devait son nom à une obsession virant à la paranoïa de ne pas être détecté par les outils de sécurité. De la préparation à son installation jusqu'à son implémentation, le malware scrute, analyse et bloque tout ce qui touche de près ou de loin à la sécurité IT.

Il semble que ce malware revienne sous une autre forme pour s'attaquer au système industriel des entreprises énergétiques européennes. Des chercheurs de SentinelOne l'ont détecté au sein du réseau d'un énergéticien européen. Cette menace a un nom, SFG, et a été trouvée à la fois par une remontée d'information des logiciels de SentinelOne, mais aussi sur des forums privés. Les experts ont travaillé sur les échantillons pour comprendre son fonctionnement. Les résultats de cette analyse montrent que le comportement, la sophistication et la furtivité du malware sont l'œuvre d'un Etat ou pour le moins d'une organisation soutenue par un gouvernement. Les experts penchent pour une initiative provenant de l'Europe de l'Est.

## Jusqu'au sabotage du réseau énergétique

Dans le détail, le cousin de Furtim s'appuie sur les mêmes exploits pour éviter d'être repéré par les outils de sécurité (antivirus, firewall next gen, solution endpoint, sandboxing). Plusieurs développeurs de haut niveau ont mis la main à la pâte pour perfectionner SFG.  L'objectif est multiple, extraire des données ou faire tomber le réseau d'énergie, sans laisser de traces. Le malware affecte toutes les versions de Windows, précise SentinelOne dans un blog. Il situe ses débuts au mois de mai dernier et il est encore actif.

Ce n'est pas la première fois que les entreprises énergétiques sont visées par des malwares ayant pour ambition le sabotage du réseau. On pense bien évidemment au premier virus qui visait les SCADA, Stuxnet. Mais plus récemment, l'Ukraine a été victime d'une panne de courant provoquée par une cyberattaque s'appuyant sur le malware Blackenergy. Ce type de menaces est pris très au sérieux par les gouvernements au point de forcer les entreprises à remonter leurs niveaux de sécurité. En France, l'ANSSI peaufine les arrêtés sectoriels sur la sécurité des OIV (opérateurs d'importance vitale) notamment dans le domaine de l'énergie.

Article original de Jacques Cheminat

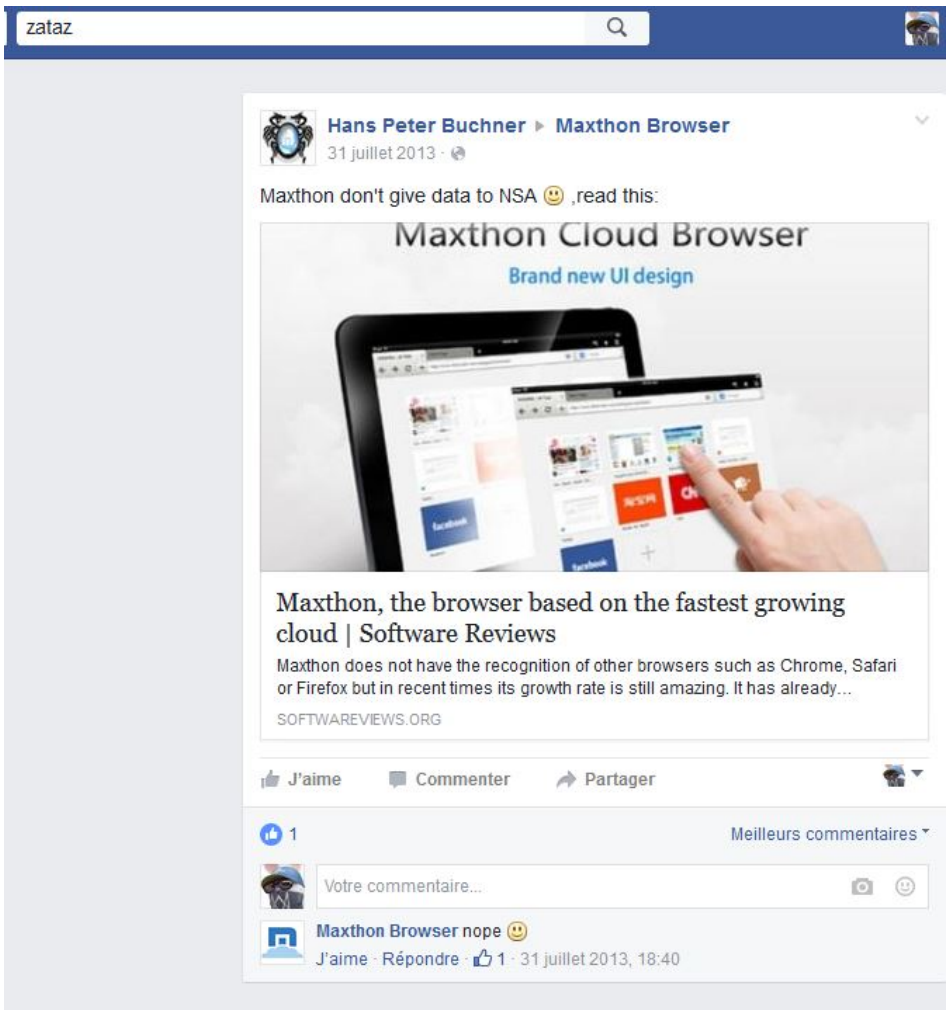
---



Réagissez à cet article

Original de l'article mis en page : Malware : un cousin de Furtim cible les énergéticiens européens

# Attention, le navigateur Maxhton espionne ses utilisateurs !




Attention, le navigateur Maxhton espionne ses utilisateurs !

**Le navigateur Maxhton ne serait rien d'autre qu'un outil d'espionnage à la solde de la Chine ?**

Des experts en sécurité informatiques de l'entreprise polonaise Exatel viennent de révéler la découverte de faits troublant visant le navigateur *Maxhton*. Ce butineur web recueille des informations sensibles appartenant à ses utilisateurs. Des informations qui sont ensuite envoyées à un serveur basé en Chine. Les chercheurs avertissent que les données récoltées pourraient être très précieuses pour des malveillants.

**Les données des utilisateurs de Maxhton envoyées en Chine !**
Et pour cause ! Les ingénieurs de *Fidelis Cybersecurity* et *Exatel* ont découvert que Maxthon communiquait régulièrement un fichier nommé ueipdata.zip. Le dossier compressé est envoyé en Chine, sur un serveur basé à Beijing, via HTTP. Une analyse plus poussée a révélé que ueipdata.zip contient un fichier crypté nommé dat.txt. Dat.txt  stocke des données sur le système d'exploitation, le CPU, le statut ad blocker, l'URL utilisé dans la page d'accueil, les sites web visités par l'utilisateur (y compris les recherches en ligne), et les applications installées et leur numéro de version.
En 2013, après la révélation du cyber espionnage de masse de la NSA, Maxhton se vantait de mettre l'accent sur la vie privée, la sécurité, et l'utilisation d'un cryptage fort pour protéger ses utilisateurs. (Merci à I.Poireau)
Article original de Damien Bancal

---



Réagissez à cet article

Original de l'article mis en page : ZATAZ Le navigateur Maxhton espionne ses utilisateurs – ZATAZ

# Un concessionnaire Lamborghini de Mulhouse piraté


Un concessionnaire Lamborghini de Mulhouse piraté

**Le vol de données peut souvent cacher des arnaques et attaques informatiques plus vicieuses encore. Exemple avec le piratage d'un concessionnaire de Lamborghini de l'Est de la France.**

Derrière un piratage informatique, 99 fois sur 100, se cache le vol des données que le malveillant à pu rencontrer dans son infiltration. Des données qui se retrouvent, dans l'heure, quand ce n'est pas dans les minutes qui suivent la pénétration du site dans des forums et autres boutiques dédiés à l'achat et revente d'informations subtilisées.Un concessionnaire de Lamborghini, à Mulhouse, vient d'en faire les frais.

Une fois les contenus dérobés exploités (phishing, escroqueries…) le pirate s'en débarrasse en les diffusant sur la toile. C'est ce qui vient d'arriver à un concessionnaire automobile de l'Est de la France. Ici, nous ne parlons pas de la voiture de monsieur et madame tout le monde, mais de Lamborghini.

**Prend son site web par dessus la jambe et finir piraté !**

Le concessionnaire se retrouve avec l'ensemble des pousses bouton de la planète aux fesses. De petits pirates en mal de reconnaissance qui profitent d'une idiote injection SQL aussi grosse que l'ego surdimensionné de ces « piratins ». Bilan, le premier pirate a vidé le site, revendu/exploité les données. Il a ensuite tout balancé sur la toile. Les « suiveurs » se sont jetés sur la faille et les données. J'ai pu constater des identifiants de connexion (logins, mots de passe) ou encore des adresses électroniques lâchées en pâture. Des courriels internes (webmaster, responsables du site…).

Article original de Damien Bancal

---

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

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

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : ZATAZ Un concessionnaire Lamborghini de Mulhouse piraté – ZATAZ