# Droit à l'oubli : mode d'emploi pour demander la suppression de contenu ou photo | Le Net Expert Informatique

## Droit à l'oubli : mode d'emploi pour demander la suppression de contenu ou photo

**Comment demander la suppression d'un résultat de recherche Google, concernant une personne physique, qui enfreint le droit au respect de la vie privée.**

Vous êtes victime d'une atteinte à votre réputation sur internet, d'une atteinte à votre image (par la publication de photos compromettantes ou tendancieuses), ou vous vous voulez faire supprimer des informations personnelles vous concernant des résultats de recherche de Google (par exemple le fait que vous avez eu une grave maladie, tel qu'un cancer, afin d'obtenir plus facilement une assurance de prêt immobilier). Voici la démarche à suivre.

Conformément à la décision de la Cour de justice de l'Union européenne du 13 mai 2014 (n°C-131/1), l'internaute français peut désormais signaler au moteur de recherche Google – qui concentre à lui seul 90% des requêtes faites sur le web – une demande de suppression d'un résultat de recherche qui contient à son égard des propos diffamations, inexacts, mensongers ou encore des informations confidentielles et personnelles sans son accord. C'est une obligation fondée sur le droit au respect de la vie privée, y compris lorsque cela concerne un compte Facebook.

En Europe, pour exercer le droit à l'oubli, il convient de s'adresser directement à Google, mais la CNIL peut aussi intervenir après un dépôt de plainte.

Toutefois, en juillet 2015, Google a fait savoir qu'il refusait d'étendre le droit à l'oubli aux noms de domaine dont l'extension est en « .com », c'est-à-dire la grande majorité des sites internet, déplore la CNIL ! Sur le blog européen du groupe, le responsable des questions de vie privée chez Google explique que le droit à l'oubli n'a pas à être appliqué à l'échelle globale, privant ainsi des centaines d'internautes français de leur droit.

Lire la suite….

---

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

---



Source :
http://www.net-iris.fr/veille-juridique/actualite/33376/droit-a-oubli-mode-emploi-pour-demander-la-suppression-de-contenu-ou-photo.php
Par Carole Girard-Oppici,

# La propriété intellectuelle à l’épreuve de l’impression 3D. Par Augustin Deschamps, Juriste. | Le Net Expert Informatique

| | |
|---|---|
|  | La propriété intellectuelle à l’épreuve de l’impression 3D |

**Le Conseil Supérieur de la Propriété Littéraire et Artistique (CSPLA) a introduit en juillet 2015 une nouvelle commission dédiée à l'impression en trois dimensions. Présidé par le conseiller d'Etat Olivier Japiot, ce nouveau cercle de travail aura pour mission de rédiger un rapport pour le mois de juin 2016 sur les nouveaux enjeux de la propriété intellectuelle soulevés par la démocratisation de l'imprimante 3D.**

L'impression 3D est donc en passe de devenir personnelle : il est aujourd'hui possible d'imaginer, dessiner, modéliser puis fabriquer un objet quelconque. De manière plus troublante, il sera bientôt concevable de scanner n'importe quel objet acheté dans le commerce, pour le reproduire à l'infini. Par exemple, la copie d'un fauteuil dessiné par Philippe Starck est aujourd'hui techniquement possible. Sans aller jusqu'à parler d'une « quatrième révolution industrielle », il est certain qu'un changement de paradigme s'opère peu à peu, ce qui soulève des enjeux évidents en matière de propriété intellectuelle.
Car même si beaucoup d'acteurs de ce nouveau marché se positionnent en faveur d'une libre diffusion des contenus imprimables, en open source ou via les licences Creative Commons, le développement de l'impression 3D provoque déjà de nombreuses atteintes aux droits de propriété intellectuelle des artistes, inventeurs et de tous les auteurs d'oeuvres de l'esprit.

**L'ensemble des composants de la propriété intellectuelle sont concernés par l'impression en trois dimensions**

Le bouleversement lié à l'apparition du MP3 sur le marché de la musique ne touchait que le droit d'auteur, tandis que le l'impression 3D nécessite d'envisager l'ensemble de la propriété littéraire et artistique, ainsi que la propriété industrielle. L'enjeu réside autour de la contrefaçon des biens protégés : celle-ci sera caractérisée en fonction de l'usage affecté à l'objet imprimé.

De manière générale, l'usage collectif, public, ou même commercial d'un tel objet permettra de qualifier un acte de contrefaçon. Tout individu imprimant un objet portant atteinte au droit d'auteur, aux dessins et modèles ou même à un brevet sera qualifié de contrefacteur. Concernant l'utilisation illicite d'une marque déposée, la jurisprudence impose un usage dans la vie des affaires pour reconnaître une contrefaçon.

Dans le cas contraire, un usage strictement privé de l'objet imprimé permettra d'échapper aux sanctions rattachées à la contrefaçon. Plus spécifiquement, concernant le droit d'auteur, les objets imprimés en 3D bénéficient de l'exception de copie privée. Ce régime spécifique autorise « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective ». Actuellement, la copie privée s'applique majoritairement aux contenus audiovisuels et musicaux, ce qui pose la question de la congruence d'un tel régime avec l'impression 3D.

**L'exception de copie privée applicable en l'état ?**

Le Code de la propriété intellectuelle dispose en effet que les exceptions de copie privée « ne peuvent porter atteinte à l'exploitation normale de l'oeuvre ni causer un préjudice injustifié aux intérêts légitimes de l'auteur. » C'est sur ce fondement qu'un individu a été débouté par le juge de sa demande de faire lever les mesures techniques de protection (MTP) d'un DVD car il souhaitait en offrir une copie à ses parents. Il est dès lors possible de penser que les MTP, qui empêchent efficacement l'atteinte aux droits de propriété intellectuelle rattachés à un film DVD, pourraient s'appliquer de manière analogue aux fichiers 3D en limitant le nombre d'impressions. Cette protection semble d'autant plus souhaitable que l'impression 3D décuple les potentiels préjudices des titulaires de droits d'auteur. Le scan et l'impression 3D d'une douzaine de chaises design à partir d'une permettront une économie substantielle pour le copiste, et par conséquent un manque à gagner démultiplié pour le propriétaire des droits sur le design industriel du meuble reproduit. L'exception de copie privée appliquée à l'impression 3D voit dès lors son efficacité limitée par la possible multitude des copies. Bien sûr, il est possible de copier un album de musique à l'infini, mais il ne viendrait probablement pas à l'esprit du consommateur d'en acheter plusieurs pour en avoir un dans sa voiture, un chez lui et un au bureau. Le manque à gagner est réel pour les propriétaires des droits de l'album, mais moindre que pour un bien mobilier.

De surcroît, le Sénat a ce mois-ci rejeté l'idée d'une redevance copie privée pour les imprimantes 3D, telle qu'elle existe déjà pour les supports de stockage (CD vierges, clés USB…) pour compenser le préjudice des artistes. L'argument principal des parlementaires a été d'affirmer que la copie 3D est une contrefaçon, donc illicite, et qu'une redevance ne peut s'appliquer à une activité illégale. Le Ministre de l'économie a ajouté qu'il n'était pas souhaitable de freiner le développement des acteurs français du domaine de l'impression tridimensionnelle.

En revanche, lorsqu'un objet sera imprimé après avoir été dessiné par le consommateur lui-même, ou téléchargé en open source, il ne sera pas possible de caractériser un acte de contrefaçon. Une telle utilisation de l'imprimante 3D ne sera qu'une extension du « do it yourself » (DIY) qui est de plus en plus en vogue. Certains professionnels l'ont compris, à l'image de l'enseigne Castorama qui a pour projet de créer une plateforme en ligne dédiée aux fichiers 3D permettant l'impression de pièces détaché d'électroménager ou de bricolage directement chez soi. Ce nouveau service créera une concurrence sévère vis-à-vis des artisans et revendeurs de produits électroménagers.

**De nécessaires solutions pour protéger les titulaires de droits de propriété intellectuelle sans entraver l'avancement technologique**

Les auteurs ont déjà la possibilité de procéder à un dépôt en ligne de leurs fichiers 3D auprès d'une société de gestion de droit, ou directement chez un notaire ou un huissier qui rédigera un procès verbal qui justifiera de la date de création de l'oeuvre. Cette démarche a pour utilité de prouver l'antériorité de la création, mais ne prémunit pas l'auteur contre les risques de contrefaçon. À cette fin, il pourrait être efficace de développer des services de « streaming 3D », ne permettant l'impression d'un fichier qu'une seule fois, grâce à des mesures techniques de protection. Une telle restriction pourrait par ailleurs s'accompagner de l'impossibilité de modifier l'oeuvre imprimée, faisant ainsi respecter son intégrité.

Une autre option consisterait à implanter dans toutes les imprimantes 3D un système de vérification de la licéité de l'impression. Connectée à internet, l'imprimante pourrait rechercher l'existence de droits de propriété intellectuelle sur l'objet, ainsi que l'absence de caractère dangereux. En effet, les pièces détachées d'armes à feu sont facilement reproductibles, ce qui a pour principale conséquence l'absence de numéro de série et donc l'impossibilité de toute traçabilité. Il est cependant nécessaire de noter qu'une telle surveillance constituerait une immixtion manifeste dans la vie privée des utilisateurs, ajoutant une nouvelle dimension au problème de l'exploitation des données personnelles.

Aujourd'hui, la distance entre l'objet original et la copie imprimée en 3D demeure importante, de telle sorte que la confusion n'est pas possible. Il est concevable de reproduire une forme, mais pas encore les mécanismes intérieurs, qui relèvent pour certain de la « 4D ». De nombreuses contraintes techniques demeurent mais la rapidité des progrès accomplis permet d'entrevoir l'étendue des enjeux juridiques de demain, et il ne fait aucun doute que ce sujet, qui alimente beaucoup de fantasmes, sera l'objet de débats passionnés.

---

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

---



Source : http://www.village-justice.com/articles/propriete-intellectuelle-epreuve,20280.html
Par Augustin Deschamps juriste chez LegaLife

---

# Les cyber-attaques provenant du Dark Web empruntent de plus en plus le réseau Tor | Le Net Expert Informatique

Les cyber-attaques provenant du Dark Web empruntent de plus en plus le réseau Tor

I**BM Sécurité vient de dévoiler les résultats de son rapport Q3 2015 IBM X-Force Threat Intelligence. Celui-ci pointe les dangers grandissants provoqués par les cyber-attaques provenant du Dark Web à travers l'utilisation du réseau Tor (The Onion Router), ainsi que les nouvelles techniques mises en place par les criminels pour les attaques avec rançon. Rien que depuis le début de l'année, plus de 150 000 événements malveillants provenant de Tor ont eu lieu aux Etats-Unis.**

Même si on entend davantage parler des fuites de données que des demandes de rançon, les « ransomware » représentent une menace grandissante. Comme la sophistication des menaces et des attaquants croît, leur cible fait de même, et ainsi certains attaquants se sont par exemple spécialisés dans la demande de rançon concernant les fichiers de joueurs de jeux en lignes populaires. Le rapport dévoile que les agresseurs peuvent maintenant également bénéficier de « Ransomware as a Service » en achetant des outils conçus pour déployer de telles attaques.
Comme les hauts fonds des océans, le Dark Web demeure largement inconnu et inexploré, et il héberge des prédateurs. L'expérience récente de l'équipe IBM Managed Security Services (IBM MSS) montre que les criminels et d'autres organisations spécialisées dans les menaces utilisent Tor, qui permet d'anonymiser les communications aussi bien en tant que vecteur d'attaques que d'infrastructure, pour commander et contrôler les botnets. La façon dont Tor masque le cheminement offre des protections supplémentaires aux attaquants en les rendant anonymes. Ils peuvent aussi masquer la location physique de l'origine de l'attaque, et même la remplacer par une autre de leur choix.
Le rapport étudie également Tor lui-même, et fournit des détails techniques permettant de protéger les réseaux contre les menaces, intentionnelles ou non, véhiculées par Tor.
Le rapport est accessible ici.

---

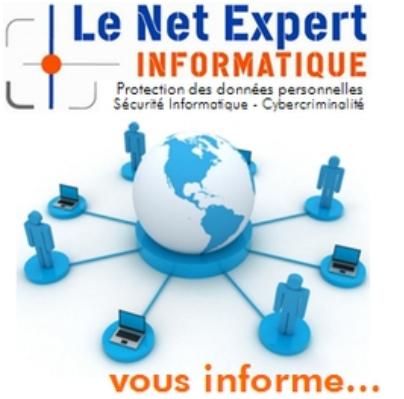


---



Source : http://www.infodsi.com/art
icles/157784/cyber-attaques-provenant-dark-web-emprunt
ent-plus-plus-reseau-tor.html

# Pourquoi est-il impossible de protéger vos données personnelles contre le piratage | Le Net Expert Informatique




## Pourquoi est-il impossible de protéger vos données personnelles contre le piratage

**Que ce soit les gouvernements ou les services comme Ashley Madison, aucune entreprise, organisation ou personne n'est à l'abri d'une cyberattaque.**

Selon Caleb Barlow, vice-président d'IBM Security, la raison est pourtant simple : alors que la culture du secret fait partie des mœurs du monde des affaires depuis ad vitam æternam, le partage d'information est ce qui permet aux pirates de réaliser des percées en la matière au quotidien.
Alors que la culture du secret fait partie des mœurs du monde des affaires, le partage d'information est ce qui permet aux pirates de réaliser des percées au quotidien.
«Nous sommes confrontés à une pandémie. Elle fait les manchettes tous les jours», a-t-il déclaré au blogue Tech Insider. «Et il nous faut comprendre que ce n'est que la pointe de l'iceberg.»
«80% des attaques [aux États-Unis] ne sont pas perpétrées par des pays étrangers, elles sont le fruit du crime organisé», affirme Barlow. «Des regroupements criminels hautement organisés travaillent dans des cubicules, font du 9 à 5 et profitent de leurs weekends de congés. Ils collaborent entre eux afin de s'aider mutuellement. Comme l'on pourrait collaborer avec d'autres personnes d'une même industrie afin d'apprendre les uns des autres et s'aider mutuellement.»
À son avis, si les entreprises souhaitent réellement se prémunir contre de futures cyberattaques, elles auraient intérêt à faire la même chose. Voilà pourquoi Barlow emploie la métaphore d'une pandémie.
«Si la situation était traitée comme la crise d'Ebola, les médecins collaboreraient activement entre eux à trouver des outils et traitements efficaces contre les infections», croit-il. «Afin de lutter contre le problème, les données de base sur des choses comme le niveau d'infections et les origines de celles-ci doivent être démocratisées. Ce n'est qu'une fois que l'on détermine le traitement efficace, une fois que l'on passe à l'étape de la pharmaceutique, que l'on peut se faire concurrence. Mais ce n'est pas du tout la façon dont la cybersécurité fonctionne aujourd'hui.»
Les plus importantes données concernant de telles cyberattaques et menaces sont généralement conservées par des institutions privées, principalement des entreprises spécialisées en cybersécurité. Cette information n'est pratiquement jamais partagée, et lorsque c'est le cas, c'est généralement parce que les données sont devenues obsolètes.

Afin de pallier le problème, IBM a récemment lancé X-Force Exchange, une plateforme cherchant à colliger et diffuser ce type de données, gratuitement. La base de données est composée à la fois de données antérieures et de données générées en temps réel. Les utilisateurs peuvent ainsi y observer le déploiement de cyberattaques et de maliciels en direct.

Aux dires d'IBM, les données qu'elle partage ainsi gratuitement représentent 700 téraoctets. Elle met au défi le reste de la communauté spécialisée en cybersécurité d'en faire autant.

X-Force Exchange est consultable sur https://exchange.xforce.ibmcloud.com/

---



---

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

Source : http://branchez-vous.com/2015/08/25/pourquoi-il-impossible-de-proteger-vos-donnees-personnelles-le-piratage/
Par Laurent LaSalle

# E-réputation entre liberté et responsabilité pour les commentaires des internautes | Le Net Expert Informatique

| | |
|---|---|
| | E-réputation entre liberté et responsabilité pour les commentaires des internautes |

**Un long arrêt de la Cour européenne des Droits de l'homme (organe du Conseil de l'Europe, à ne pas confondre avec à Cour de justice de l'Union européenne, cour suprême de l'Union), est venu rappeler, le 16 juin dernier, les rôles et limites respectifs entre la liberté d'expression et la responsabilité de l'hébergeur et/ou de l'éditeur de site. Une clarification importante pour les questions d'e-réputation par voie de commentaires ou d'avis de consommateurs.**

**Les faits**

Sur le portail d'actualité estonien Delfi, un article concernant une compagnie maritime propriétaire de ferries avait été publié et violemment commenté et critiqué par les internautes, notamment par des propos injurieux ou menaçants. À la demande de la compagnie, les commentaires ont fini par être retirés, mais seulement après que le portail les ait laissés en ligne plus de 6 semaines. La Cour d'État de l'Estonie (équivalent de notre Cour de cassation) avait confirmé la responsabilité du portail d'information, estimant qu'il contrôlait la publication de ces commentaires, refusant de lui appliquer la responsabilité allégée des hébergeurs prévue par la directive européenne de 2000/31/CE.

**Rappels de la CEDH**

La Cour de Strasbourg pose plusieurs pistes de principe qu'il importe de bien observer, compte tenu de la position suprême de cet organe judiciaire.

1. La pratique des commentaires fait partie du modèle économique du portail et constitue un gage de sa rentabilité.
2. Les internautes n'ont pas la possibilité de modifier ou retirer leurs commentaires une fois postés ; seul le portail peut le faire : il n'est donc pas qu'un hébergeur mais endosse bien la responsabilité d'un éditeur.
3. Le portail ne permet pas de retrouver systématiquement l'identité du commentateur, empêchant ainsi toute éventuelle poursuite pénale des auteurs en cas d'infraction au droit de la presse.
4. Enfin, la condamnation à une amende modique (320 €) ne constitue pas une mesure telle qu'elle constitue un obstacle à la liberté d'expression dont doit toujours jouir le portail.

**La liberté d'expression n'exclut pas la responsabilité**

Cette solution nous paraît juste et équilibrée. Elle rend justice à la liberté d'expression, toujours de principe dans les pays membres du Conseil de l'Europe, signataires de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales de 1950 qui dans son article 10 garantit cette liberté.

Précisément, l'alinéa 2 de cet article précise notamment : « L'exercice de ces libertés comportant des devoirs et des responsabilités peut être soumis à certaines formalités, conditions, restrictions ou sanctions prévues par la loi, qui constituent des mesures nécessaires, dans une société démocratique (…) ».

Notre Déclaration des droits de l'homme et du citoyen de 1789 dispose pareillement, dans son article 11 : « La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme : tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la Loi ».

Dans les deux cas, la notion d'abus de droit est présente et vient justifier que face à cette belle liberté d'expression, puisse être envisagé un simple régime de responsabilité.

Cette responsabilité peut donc parfaitement cohabiter avec la liberté d'expression sans qu'il y ait contradiction.

De la sorte, la décision rend aussi justice à la responsabilité, pour peu que celle-ci ne devienne pas un instrument de contrainte au point d'étouffer la liberté d'expression. C'est l'application équilibrée de la notion d'abus de droit.

Des conséquences au regard des portails et forums d'avis de consommateurs

Cette décision vient donc clairement délimiter et faire coexister les notions de liberté d'expression et de responsabilité. Une solution que vont devoir méditer tous les responsables de portails qui nous opposent souvent la liberté d'expression des consommateurs pour refuser de retirer des propos injurieux ou mensongers à l'encontre de commerçants injustement mis en cause sur leurs plateformes.

**En savoir plus**

Voir l'arrêt fleuve de la CEDH du 16 juin 2015 dans la base HUDOC de la CEDH :
http://hudoc.echr.coe.int/fre#{%22documentcollectionid2%22:[%22GRANDCHAMBER%…
Et sur le site Legalis.net :
http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4675
Voir la présentation qui en est faite sur ce même site :
http://www.legalis.net/spip.php?page=breves-article&id_article=4678

---

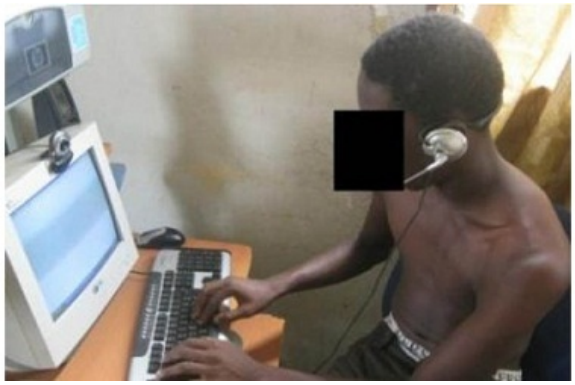


---



Source :
http://www.les-infostrateges.com/actu/15082042/e-reputation-entre-liberte-et-responsabilite-pour-les-commentaires-des-internautes
Par Didier FROCHOT

# Des brouteurs sur Internet maintenant aussi au Togo | Le Net Expert Informatique

| | |
|---|---|
|  | Des brouteurs sur Internet maintenant aussi au Togo |

**La cybercriminalité, on le dira jamais assez, connaît une proportion inquiétante ces derniers jours à Lomé. Jadis arnaque ficelée et entretenue par des Nigérians et des Ivoiriens, cette activité illicite et criminelle gagne du terrain et devient aussi le principal « job » de certains jeunes togolais.**

Joe, 27 ans n'exerce officiellement aucune profession. Puisque n'ayant rien appris comme métier depuis qu'il a arrêté ses études sur le campus. Pour nombre de ceux qui le connaissent, c'est un bon-à-rien.
Mais il a bel et bien une activité qui n'a rien à envier aux salariés. Il passe tout son temps au cyber à arnaquer des gens, un « métier » (comme ils se plaisent à l'appeler) qu'il a appris de ses amis ivoiriens.
«Il passe tout son temps dans les cybercafés. Au début, on croyait qu'il faisait des recherches, puisqu'il était étudiant. C'est par la suite qu'on a vraiment su ce qu'il faisait réellement, surtout lorsqu'il a commencé par emmener des amis Ivoiriens et Nigerians à la maison, en organisant des soirées qui sont hors de sa portée », nous explique-t-il.
Autrefois étudiant, il a décidé d'interrompre ses études après avoir réussi à arnaquer 500£ (327.972 CFA) à une blanche qu'il prétend aimer ! Et depuis son envie pour l'enrichissement facile et illicite ne cesse de s'agrandir.
Comme Joe, ils sont très nombreux ces jeunes togolais qui excellent dans cette sale besogne. Apparemment, ils gagnent plus d'argent dans cette activité d'arnaque qu'on ne peut le penser. Les réseaux sociaux, surtout les sites de rencontre sont leurs terrains de chasse. Et pour ce faire, ils utilisent plusieurs modes opératoires pour « attraper leurs pigeons « , expressions qu'ils ont créé eux-mêmes.
A en croire Jean-Christophe (Sociologue), il y a plusieurs méthodes pour pour ces types de personne pour tromper la vigilance de leurs victimes. Et c'est une question d'expérience.
« D'autres cybercriminels, plus habiles, se font passer pour des femmes, en publiant sur leurs profils (sur des sites ou réseaux sociaux, etc.) des photos érotiques qui ne laissent aucun homme indifférent !! Face donc à la beauté de ces photos, les « pigeons » cèdent à la tentation en répondant favorablement aux mails accrochant qu'on les envoie sous le pseudonyme féminin», nous confie une victime.
Une fois la confiance établie, ils font croire à leurs cibles par des mails d'amour sous le pseudonyme féminin, qu'ils sont aptes à débuter une histoire d'amour très sérieuse avec eux. Ils leurs communiquent par la suite un numéro de téléphone. Commencent alors les grandes opérations de manipulation ».
La victime ajoute aussi que certains très expérimentés, crée même des sociétés écrans, ou des associations à but non lucratif et font croire à leur « pigeon » avec des preuves vraisemblables à l'appui (preuves falsifiées bien sûres), qu'ils ont des projets humanitaires ou qu'ils ont fondé une ONG pour aider les enfants orphelins et dont ont besoin de fonds. « Et souvent ça marche », nous souligne-t-il.
De nombreuse personnes sont déjà victimes de ces cybers-délinquants. Ils déplument sans pitié, leurs pigeons. Et la plupart de ces victimes, par peur d'être à la risée de tout le monde, préfèrent garder leurs mésaventures pour eux-mêmes.
C'est d'ailleurs le silence de la plupart des victimes qui encouragent ces arnaqueurs. Selon David (un converti), pour réussir son arnaque, « il faut être connecté sur le net constamment», sinon on peut rater sa cible.
Bien qu'étant conscients du phénomène, les propriétaires des cybercafés ne se préoccupent nullement pas de ce que peuvent faire les clients dans leur structure. L'essentiel pour eux, c'est de se faire des sous. C'est pourquoi on les voit ouvrir leur porte 24h /24h. Ce qui permet à ces criminels d'opérer de jour comme de nuit.
Plus les gens passent beaucoup d'heures sur les machines, plus ces gérants de cybers font de belles affaires.
« Ce n'est pas mon travail de vérifier ce qu'ils font. On interdit juste l'ouverture de sites pornographiques à nos clients. Le reste ne nous regarde pas », se défend-il.
Bien que l'internet soit un outil fondamental de développement d'un pays, la capacité de nuisance de l'homme l'a rendu en même temps dangereux. Ces « assassins » ont plusieurs modes opératoires et ils sont capables de les changer au jour le jour. Vigilance donc !

---



---

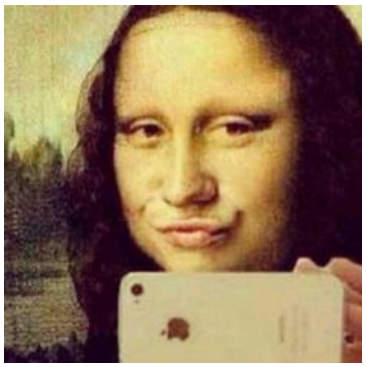


Source : http://news.icilome.com/?idnews=811403&t=Cybercriminalite-:-Les-brouteurs-gagnent–du-terrain
Par AKG (stagiaire)

---

# Le paiement par selfie en cours de test aux Pays-Bas |

# Le Net Expert Informatique



## Le paiement par selfie en cours de test aux Pays-Bas

**Mastercard a récemment présenté la technologie aux Etats-Unis, c'est maintenant au tour de 750 Néerlandais de tester le service de paiement par selfie jusqu'au 30 novembre prochain.**

Lors d'un achat en ligne via leur smartphone ou leur tablette, les clients pourront donc confirmer leur paiement au moyen d'une empreinte digitale ou d'un autoportrait. Mastercard collabore pour ce test avec CA technologies. En fonction des résultats, l'entreprise décidera si elle déploie la technologie sur l'ensemble du Vieux Continent.

---



---

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

Source : http://www.informaticien.be/index.ks?page=news_item&id=20948

# Les drones de Parrot peuvent facilement se faire hacker | Le Net Expert Informatique

## Les drones de Parrot peuvent facilement se faire hacker

**Il y a quelques semaines, nous vous faisons part des piratages de voitures et encore plus tôt dans l'année, d'avions… Aujourd'hui, c'est au tour des drones Parrot de succomber aux hackers !**

Ou plutôt à un hacker. Ryan Satterfield, connu pour sa chaîne Planet Zuda, qui a profité de la Def Con pour faire une démonstration. À l'aide de son smartphone et d'une simple clef, il a réussi à faire atterrir un AR.Drone 2.0.
Les drones de la société française n'ont malheureusement que trop peu de protections. Ces derniers tournent sous Linux avec des ports WiFi et Telnet ouverts, sans nécessiter un quelconque mot de passe pour s'y relier…. Il suffit de s'y connecter en utilisant le port 23 et de rentrer la commande « kill 1″. De suite, le drone redescend sur terre. Parrot a précisé qu'elle était consciente de ces failles de sécurité, mais n'a pourtant pas annoncé de correctif. Notez que le dernier drone, le Parrot Bebop, serait lui aussi touché, a annoncé le chercheur Michael Robinson.

---

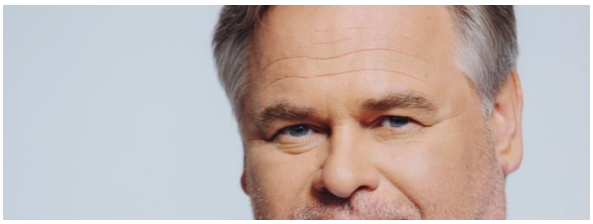
Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin 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.journaldugeek.com/2015/08/17/les-drones-de-parrot-peuvent-facilement-se-faire-hacker
Par 4ugeek

# Kaspersky trompe ses client avec de faux virus ? | Le Net Expert Informatique

| | |
|---|---|
|  | Kaspersky trompe ses client avec de faux virus ? |

**Deux ex-employés de l'éditeur accusent Kaspersky d'avoir inondé ses concurrents de fichiers spécialement conçus pour tromper leur algorithme de détection de malwares. Et créer de faux positifs chez les utilisateurs.**

Selon Reuters, Kaspersky a tenté de faire passer des fichiers bénins pour malicieux afin de tromper les capacités de détection de ses concurrents sur le marché des antivirus. Ces affirmations, très graves pour l'éditeur russe, se basent sur les déclarations à nos confrères de deux ex-employés de la société basée à Moscou, aujourd'hui parmi les leaders mondiaux des logiciels de sécurité.
Cette duperie, qui aurait démarré il y a plus de dix ans – avec un pic entre 2009 et 2013 -, ciblait notamment les antivirus de Microsoft, AVG ou Avast et visait à les inciter à effacer des fichiers importants sur les PC de leurs utilisateurs. Les deux sources de nos confrères, qui demeurent anonymes, affirment que des chercheurs ont été affectés à ces sabotages pendant des semaines ou des mois, avec pour tâche principale la rétro-ingénierie des technologies de détection des concurrents ciblés. Une étape indispensable à la mise au point de faux positifs.

**Intoxiquer la concurrence**
Reuters assure que, dans certains cas, la décision a été prise par Eugene Kaspersky en personne (en photo ci-dessus), le fondateur de l'éditeur russe souhaitant se venger de concurrents qui, selon lui, se contentaient d'imiter sa technologie. La société a démenti ces pratiques, assurant « n'avoir jamais mené de campagne secrète pour tromper des concurrents avec de faux positifs (des fichiers bénins identifiés comme malwares, NDLR) ».
En 2010, Kaspersky s'était plaint de l'exploitation que ses concurrents faisaient de ces travaux. A l'appui de sa démonstration, l'éditeur avait créé 10 fichiers sans risque et les avaient déclarés comme malicieux à VirusTotal, l'outil de partage d'informations sur les menaces de Google. Une semaine et demi plus tard, 14 fournisseurs d'outils de sécurité estimaient ces fichiers dangereux, suivant aveuglément les conclusions de la société russe, selon Kaspersky.
D'après les deux sources de Reuters, Kaspersky ne se serait pas arrêté à cette opération de communication. La société injectait ainsi du code malicieux dans des fichiers fréquemment rencontrés sur les PC puis les signalait anonymement à VirusTotal dans l'espoir de voir les antivirus concurrents assimiler ces fichiers essentiels au fonctionnement d'un PC à des malwares.

**Pratiques connues**
Reuters affirme par ailleurs que Microsoft, AVG et Avast lui ont confirmé que des tiers non identifiés avaient tenté d'introduire de faux positifs dans leur mécanisme de détection au cours des dernières années. Dennis Batchelder, qui dirige la recherche antimalware de Microsoft, a ainsi expliqué à Reuters avoir identifié, à partir de mars 2013, des fichiers altérés afin de paraître malicieux. Et d'affirmer que ses équipes ont isolé des centaines, voire des milliers de cas de la sorte. Sans toutefois faire un quelconque lien avec Kaspersky. Plus largement, aucun concurrent du Russe n'a émis de commentaire sur l'implication éventuelle de la société moscovite.

---



---

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

Source : http://www.silicon.fr/kaspersky-accuse-infecte-concurrents-faux-virus-124122.html#LJcrRvhoptort4dm.99

# La France, 1ère cible des attaques DDoS de botnet en Europe | Le Net Expert Informatique

## La France, 1ère cible des attaques DDoS de botnet en Europe

**Kaspersky Lab nous apprend qu'au 2ème trimestre, la France était la 1ère cible des attaques DDoS de botnet en Europe.**

En effet, les trois quarts des ressources attaquées au cours du deuxième trimestre 2015 par des botnets se situent dans 10 pays seulement (source : Kaspersky DDoS Intelligence). En tête du classement, on trouve les Etats-Unis et la Chine qui enregistrent un grand nombre d'attaques en raison du faible coût d'hébergement de ces pays. Cependant, le nombre croissant de pays affectés par ce type d'attaque prouvent qu'aucun territoire n'est sécurisé face aux attaques DDoS.
Dans ce Top 10, la France figure en 6ème position, mais est aussi le premier pays européen avec 2,8% des attaques (en hausse par rapport au 1er trimestre), devant la Croatie (8ème avec 1,4% des attaques) et l'Allemagne (9ème avec 1% des attaques).
« Les techniques d'ingénierie sociale, l'apparition de nouveaux types d'appareils avec accès internet, les failles logicielles et la sous-estimation de l'importance d'une protection anti-malware ont contribué à la diffusion des botnets et à l'augmentation du nombre d'attaques DDoS, explique Evgeny Vigovsky, Directeur de Kaspersky DDoS Protection, chez Kaspersky Lab. Par conséquent, des entreprises complètement différentes peuvent être ciblées indépendamment de leur location, de leur taille ou de leur type d'activité. La liste des victimes protégées des attaques DDoS par Kaspersky Lab au second trimestre 2015 incluait des organisations gouvernementales, des institutions financières, des médias de masse et même des institutions éducatives ».
Kaspersky Lab a d'ailleurs noté une forte augmentation du nombre d'attaques au cours de la première semaine de mai, le pic d'attaques par jour (1960) ayant été enregistré le 7 mai.
Sur le plan technique, les cybercriminels impliqués dans ce type d'attaques investissent de plus en plus dans la création de botnets de produits réseaux comme les routeurs et les modems DSL. Ce qui préfigure certainement d'une augmentation du nombre d'attaques DDoS utilisant des botnets à l'avenir.

---



---



---



Source : http://www.infodsi.com/articles/157658/france-1ere-cible-attaques-ddos-botnet-europe.html