

Harcelée sur internet, une lycéenne d'Avignon se scarifie



Le ministère de l'Éducation Nationale se mobilise contre le harcèlement à l'école. Une lycéenne d'Avignon a été la cible d'insultes sur internet. Elle s'est scarifiée et témoigne de sa souffrance psychologique et physique...[Lire la suite]

Denis JACOPINI anime des conférences, des formations en Cybercriminalité et est régulièrement invité à des tables rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux Dangers liés à la Cybercriminalité (Arnaques, Piratages...) pour mieux s'en protéger (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Plus d'informations sur sur cette page.



Réagissez à cet article

Harcelée sur internet, une lycéenne d'Avignon se scarifie



Le ministère de l'Éducation Nationale se mobilise contre le harcèlement à l'école. Une lycéenne d'Avignon a été la cible d'insultes sur internet. Elle s'est scarifiée et témoigne de sa souffrance psychologique et physique...[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en protéger (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Plus d'informations sur sur cette page.

Réagissez à cet article

Harcelée sur internet, une lycéenne d'Avignon se scarifie



Le ministère de l'Éducation Nationale se mobilise contre le harcèlement à l'école. Une lycéenne d'Avignon a été la cible d'insultes sur internet. Elle s'est scarifiée et témoigne de sa souffrance psychologique et physique...[Lire la suite]

Denis JACOPINI anime des conférences, des formations en Cybercriminalité et est régulièrement invité à des tables rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux Dangers liés à la Cybercriminalité (Arnaques, Piratages...) pour mieux s'en protéger (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Plus d'informations sur sur cette page.



Réagissez à cet article

Que faire en cas de harcèlement en ligne ?



Que faire en cas de harcèlement en ligne ? de

Selon un rapport européen, près de 10 % de la population européenne a subi ou subira un harcèlement*. Voici quelques conseils si vous êtes victime de ces violences sur internet et les médias sociaux.

Qui sont les cyber-harceleurs ?

Une(e) internaute peut être harcelé(e) pour son appartenance à une religion, sa couleur de peau, ses opinions politiques, son comportement, ses choix de vie... Le harceleur peut revêtir l'aspect d'un « troll » (inconnu, anonyme) mais également faire partie de l'entourage de la victime (simple connaissance, ex-conjoint, camarade de classe, collègue, voisin, famille...).

À quoi ressemble une situation de cyber-harcèlement ?

- Happy slapping : lynchage en groupe puis publication de la vidéo sur un site
- Propagation de rumeurs par téléphone, sur internet.
- Création d'un groupe, d'une page ou d'un faux profil à l'encontre de la personne.
- Publication de photographies sexuellement explicites ou humiliante
- Messages menaçants, insulte via messagerie privée
- Commande de biens/services pour la victime en utilisant ses données personnelles
- ...

Comment réagir ?

Ne surtout pas répondre ni se venger

Vous avez la possibilité de bloquer l'accès de cette personne à vos publications, de la signaler auprès de la communauté ou d'alerter le réseau social sur un comportement qui contrevient à sa charte d'utilisation.

Verrouiller l'ensemble de vos comptes sociaux

Il est très important de limiter au maximum l'audience de vos comptes sociaux. Des options de confidentialité existent pour « ne plus me trouver », « ne pas afficher/partager ma liste d'amis ». Il est également possible de « bannir » les amis indésirables. Sur Facebook, une option vous permet d'être avertis si un autre utilisateur mentionne votre nom sur une photo (tag).

Les paramètres conseillés sur Facebook :

PARAMÉTRAGE POSSIBLE	CHEMIN D'ACCÈS
Limiter la visibilité de vos photos	Ce type d'option ne fonctionne que photo par photo
Limiter la visibilité de vos informations de profil	Informations générales : page du profil > encart gauche > sélectionner « amis » ou « moi uniquement »
Cacher votre liste d'amis	Page du profil > onglet « amis » > « gérer section » > « modifier la confidentialité » > « liste d'amis » ou « moi uniquement »
Cacher vos mentions « j'aime »	Page du profil > Mentions j'aime (encart gauche) > « modifier la confidentialité » > « moi uniquement »
Être prévenu si quelqu'un vous « tague »	Paramètre > journal et identification > Paramètres d'identification et de journal > « examiner les identifications »
Limiter la visibilité de vos publications	Journal > sélectionner la publication > « moi uniquement » / ou « supprimer »
Examiner votre historique	Page du profil > « afficher l'historique personnel » > supprimer au cas par cas

• Capture écran des propos / propos tenus

Ces preuves servent à justifier votre identité, l'identité de l'agresseur, la nature du cyber-harcèlement, la récurrence des messages, les éventuels complices. Sachez qu'il est possible de faire appel à un huissier pour réaliser ces captures. Fiche pratique : comment réaliser une copie d'écran ?

• Portez plainte auprès de la Gendarmerie/Police si le harcèlement est très grave

Vous avez la possibilité de porter plainte auprès du commissariat de Police, de Gendarmerie ou du procureur du tribunal de grande instance le plus proche de votre domicile.

• En parler auprès d'une personne de confiance

La violence des termes employés par l'escroc et le risque d'exposition de votre vie privée peuvent être vécus comme un traumatisme. Il est conseillé d'en parler avec une personne de confiance.

Si quelqu'un d'autre est harcelé ?

Le fait de « partager » implique votre responsabilité devant la loi. Ne faites jamais suivre de photos, de vidéos ou de messages insultants y compris pour dénoncer l'auteur du harcèlement. Un simple acte de signalement ou un rôle de conseil auprès de la victime est bien plus efficace ! **Le chiffre : 61% des victimes indiquent qu'elles n'ont reçu aucun soutien quel qu'il soit de la part d'organismes ou d'une personne de leur réseau personnel.** * Source: rapport européen sur le cyber-harcèlement (2013)

Si vous êtes victime et avez moins de 18 ans ...

Composez le 3020. Il est ouvert du lundi au vendredi, de 9h à 19h (sauf les jours fériés). Le numéro vert est géré par la plateforme nonaharcèlement.education.gouv.fr qui propose de nombreuses ressources pour les victimes, témoins, parents et professionnels (écoles, collèges, lycées).

Si le harcèlement a lieu sur internet, vous pouvez également composer le 8000 200 000 ou vous rendre sur netecoute.fr. La plateforme propose une assistance gratuite, anonyme, confidentielle par courriel, téléphone, chat en ligne, Skype. Une fonction « être rappelé par un conseiller » est également disponible. La réponse en ligne est ouverte du lundi au vendredi de 9h à 19h.

Un dépôt de plainte est envisagé ? Renseignez vous sur le dépôt de plainte d'un mineur. Celui-ci doit se faire en présence d'un ou de plusieurs parents ou d'un représentant légal. N'hésitez pas à contacter les télé-conseillers du fil santé jeune au 8000 235 236.

Un droit à l'oubli pour les mineurs. L'article 40 modifié de la loi informatique et Libertés – au même titre que futur Règlement européen sur la protection des données – consacre un droit à l'oubli spécifique pour les mineurs. Un internaute âgé de moins de 18 ans au moment de la publication ou de la création d'un compte en ligne peut directement demander au site l'effacement des données le concernant et ce, dans les meilleurs délais. En pratique, si le responsable de traitement n'a pas effacé les données ou répondu à la personne dans un délai d'un mois, la personne concernée peut saisir la CNIL. Des exceptions existent, notamment dans le cas où les informations publiées sont nécessaires à liberté d'information, pour des motifs d'intérêt public ou pour respecter une obligation légale.

Quelles sanctions encourues par l'auteur de ces violences en ligne ?

L'auteur de tels actes est susceptible de voir sa responsabilité engagée sur le fondement du Droit civil, du Droit de la presse ou du Code pénal. **Quelques exemples de sanctions :**

- Une injure ou une diffamation publique peut être punie d'une amende de 12.000€ (art. 32 de la Loi du 29 juillet 1881).
- Pour le droit à l'image, la peine maximum encourue est d'un an de prison et de 45.000 € d'amende (art. 226-1, 226-2 du Code pénal).
- L'usurpation d'identité peut être punie d'un an d'emprisonnement et de 15.000€ d'amende (art. 226-4-1 du Code pénal).

Quels sont les recours auprès de la CNIL ?

La qualification et la sanction de telles infractions relève de la seule compétence des juridictions judiciaires. En parallèle de telles démarches, vous pouvez demander la suppression de ces informations à chaque site ou réseau social d'origine, en faisant valoir votre droit d'opposition, pour des motifs légitimes, sur le fondement de l'article 38 de la loi du 6 janvier 1978 modifiée dite « Informatique et Liberté ». Le responsable du site dispose d'un délai légal de deux mois pour répondre à votre demande. La majorité des sites propose un bouton « signaler un abus ou un contenu gênant ». Si aucun lien n'est proposé, contactez directement par courriel ou par courrier le responsable du site en suivant la procédure expliquée sur notre site. Par ailleurs, si ces informations apparaissent dans les résultats de recherche à la saisie de vos prénom et nom, vous avez la possibilité d'effectuer une demande de déréférencement auprès de Google en remplissant le formulaire. En cas d'absence de réponse ou de refus, vous pourrez revenir vers la CNIL en joignant une copie de votre demande effectuée auprès du moteur de recherche incluant le numéro de requête Google.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la Protection des Données Personnelles (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACQUINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement. Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Réagir en cas de harcèlement en ligne | CNIL

Le réseau informatique des

drones militaires américains piraté ?

x	Le réseau informatique des drones militaires américains piraté ?
---	--

Le 9 septembre dernier, le réseau informatique de la base Creech de l'US Air Force, dans le Nevada, est tombé en panne, peut-être en raison d'un acte de piratage. C'est de là que sont conduites les opérations de surveillance et de bombardement par drones. Le réseau n'est toujours pas rétabli complètement.

L'armée américaine s'est-t-elle fait pirater le réseau de communication qu'elle utilise pour piloter à distance sa flotte de drones tueurs, qui bombardent quotidiennement dans de multiples pays du monde dont l'Afghanistan, la Syrie, le Pakistan, la Somalie, ou l'Irak ? La question se pose alors que BuzzFeed dévoile que l'US Air Force a reconnu que le réseau informatique de sa base Creech Air Force, dans le Nevada, était tombé en panne le 9 septembre dernier, et qu'il n'avait toujours pas pu être rétabli complètement depuis.

La base Creech Air Force est celle qui abrite les militaires qui, joystick à la main et yeux rivés sur un écran, déclenchent les frappes aériennes à des milliers de kilomètres de distance – parfois en utilisant uniquement des collectes de métadonnées pour présumer de l'identité des cibles, l'armée ayant développé des algorithmes pour les détecter. Les drones sont pilotés à travers des liaisons satellite qui permettent de relayer les ordres du Nevada jusqu'aux théâtres de guerre, avec un minimum de temps de latence et en toute sécurité.

Mais le système repose au moins partiellement sur le réseau SIRPnet (*Secret Internet Protocol Router Network*), une sorte de réseau Internet privé de l'armée américaine, utilisé pour véhiculer des informations confidentielles en toute sécurité. Or selon un appel d'offres étonnamment détaillé publié par l'armée, « *le système SIRPNet actuellement en opération à Creech AFB a échoué et des services essentiels ont été touchés* ». Elle précise que « *les systèmes ont été quelque peu restaurés avec l'utilisation de plusieurs appareils moins puissants* », et que « *cette solution temporaire a stabilisé les services, mais ne sera pas capable de satisfaire la demande encore très longtemps* ». Or, « *si cette solution échoue, il n'y actuellement aucun système de sauvegarde* »...[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Un système essentiel pour les drones tueurs américains est tombé en panne – Politique – Numerama

Les géants du web s'accordent pour bloquer les contenus illégaux

✕	Les géants du web ensemble pour bloquer les contenus illégaux
---	---

Alors que les propos haineux sont malheureusement légion sur les réseaux sociaux, plusieurs géants du web ont trouvé un accord avec la Commission Européenne pour respecter un code de conduite. Toutefois, cette solution ne semble pas à ce jour convenir à plusieurs associations de défense des droits.



Les contenus illégaux bientôt bannis d'Internet ?

Depuis de longs mois maintenant, la Commission Européenne s'était fixée comme objectif d'éradiquer une majorité des propos haineux circulant sur la Toile.

Dans ce cadre, elle est parvenue à un accord avec YouTube, Microsoft, Twitter et Facebook pour l'établissement et le respect d'un code de conduite. Ainsi, les différents acteurs se sont engagés à bloquer les contenus gênants dans les 24 heures suivant leur signalement officiel.

En acceptant ce code de conduite pour bloquer les contenus illégaux, les acteurs du web montrent qu'ils ont bien conscience que leurs outils sont utilisés pour diffuser la violence et la haine mais aussi pour recruter des individus susceptibles de rejoindre leurs groupes.

Point positif, ce code de conduite ne vient pas entraver la liberté d'expression sur la Toile, celle-ci étant très importante en particulier pour les géants du web qui l'ont toujours prônée.

Un code de conduite pas suffisant selon les associations de défense des droits

Si la Commission Européenne s'est d'ores et déjà réjouie de l'accord trouvé avec les grandes entreprises du web, celui-ci ne fait assurément pas que des heureux.

En effet, Access Now et European Digital Rights (EDRi), deux associations de défense des droits, ont vivement critiqué cet accord estimant qu'il se contente de rappeler des règles déjà existantes à savoir celles qui consistent à supprimer des contenus illégaux.

Selon ces associations, il aurait donc fallu que le texte aille beaucoup plus loin et qu'il prévoit des poursuites contre ceux qui profèrent des propos haineux sur la Toile. En effet, Joe McNamee, Directeur Exécutif de l'EDRi, juge qu'« il est ironique que la Commission menace les Etats membres de les traduire en justice pour ne pas respecter les lois contre le racisme et la xénophobie alors qu'ils persuadent des entreprises comme Google et Facebook de glisser les infractions sous le tapis ».

Tout est dit...

Article original



Réagissez à cet article

Original de l'article mis en page : Les géants du web ensemble pour bloquer les contenus illégaux

Retrouver les traces d'une attaque informatique peut s'avérer complexe et coûteuse



Selon l'un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l'univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu'à l'auteur de l'attaque, se révèle souvent compliqué.



Lorsqu'un incident survient, il est généralement difficile pour l'entreprise de définir qui a accès à son système d'information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d'utilisateurs internes bénéficiant d'un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau. Que l'incident soit le résultat d'une action malveillante d'un utilisateur interne, d'une erreur humaine ou d'une faille, dès lors que l'entreprise n'est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l'enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
 Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins coûteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l'incident.

L'examen approfondi des logs : remonter les étapes d'une attaque
 Lorsqu'une faille est avérée, l'entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l'attaque. En pratique, trier les informations peut prendre des jours – en d'autres termes, cela revient à chercher une aiguille dans une botte de foin.

L'intégrité des logs : le respect du standard des preuves
 Si les logs ont été modifiés et qu'ils ne peuvent pas être présentés dans leur format original, l'intégrité des données de logs peut être remise en question lors d'une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n'ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.

Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l'information cruciale peut manquer et ce chaînon manquant peut empêcher l'entreprise de reconstituer tout le cheminement de l'incident et ainsi de retrouver la source initiale du problème.


Les comptes à privilèges : une cible fructueuse pour les cybercriminels
 En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

L'analyse comportementale : un regard nouveau pour les entreprises
 Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l'analyse comportementale permettent aux entreprises d'analyser l'activité de chacun des utilisateurs, et notamment les événements malveillants, dans l'intégralité du réseau étendu.

Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.

Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.

Lorsque ces journaux sont complétés par de l'analyse comportementale, cela offre à l'entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel... [Lire la suite]



Magistrez à cet article

Source : *Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse – JDN*

Darknet: qu'est ce qu'on y trouve et comment y accéder ?



Darknet: qu'est ce qu'on y trouve et comment y accéder ?

Au fil de nos CyberBalades, notre souris s'est arrêtée sur un article très intéressant sur le DarkNet. Pour votre plus grand plaisir, veuillez trouver ci-dessous un extrait et le lien permettant de le consulter en entier.

Qu'est-ce qu'on trouve dans le Darknet ?

Ce qui frappe en premier c'est la **quantité de contenus illégaux**. On compte environ un tiers de porno (dont une bonne partie de pédopornographie et d'autres trucs louches), un autre tiers de contenu illégal (culture de drogue, négationnisme, numéro de carte bancaire, comment faire un petit engin explosif, etc.) et un dernier tiers de sites inclassables... [Lire la suite]

Liste des URL intéressantes pour explorer le darknet

- **Moteur de recherche** : <http://hss3uro2hsxfogfq.onion>
 - **Hidden wiki**: http://zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
 - **Annuaire des liens** : <http://torlinkbgs6aabns.onion>
 - **Facebook pour Tor**: <https://facebookcorewwi.onion>
 - **Moteur de recherche Darknet**: <http://grams7enufi7jmdl.onion>
 - **Vente des mobiles débloqués**: <http://mobil7rab6nuf7vx.onion>
 - **Location des services d'un hacker**: <http://2ogmrlfzdthnwkez.onion>
 - **Moteur de recherche DuckDuckGo**: <http://3g2upl4pq6kufc4m.onion>
- [Lire la suite]

Réagissez à cet article

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

Quel sont nos principales activités ?

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS
- RECHERCHE DE PREUVES

▪ **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES

- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)



Source : *Darknet: qu'est ce qu'on y trouve et comment y accéder ?*

Auteur : Ahmed EL JAOUARI

Un piratage sur Tor par le FBI prive les victimes d'une justice



Un
piratage
sur Tor
par le
FBI
prive
les
victimes
d'une
justice

La lutte contre la pédocriminalité est une absolue nécessité, qui exige une absolue rigueur. Un juge américain a dû invalider un mandat utilisé par le FBI pour pirater les ordinateurs de membres d'un site pédopornographique hébergé derrière le réseau Tor, privant les victimes et leurs proches de la possibilité d'un procès.

C'est un coup très dur pour le FBI, mais surtout pour les familles des victimes. Dans un jugement prononcé mercredi, un tribunal américain situé au Massachusetts a invalidé le mandat que la police fédérale avait utilisé pour maintenir un site pédopornographique en ligne et procéder au piratage des ordinateurs de plus d'un millier de ses membres. Le site en question, Playpen, n'était accessible qu'à travers le célèbre réseau d'anonymisation Tor, qui masquait l'adresse IP véritable des visiteurs, rendant très difficile leur identification et leur poursuite.

C'est sur un argument purement juridictionnel que s'est appuyé le magistrat pour dénoncer l'illégalité du mandat employé par le FBI. Selon le code de procédure pénal américain, les magistrats n'ont pas l'autorité suffisante pour émettre des mandats situés en dehors de leur compétence géographique. C'est pourtant ce qu'il s'est produit dans au moins l'un des cas de l'affaire Playpen.

Le site The Intercept, qui se fait l'écho des conclusions de la décision, explique en effet que le mandat a été émis au départ par un juge se trouvant en Virginie. Or, l'un des suspects qui a été attrapé par le FBI dans le cadre de l'enquête vit dans le Massachusetts. Les éléments contre lui – qui est à l'origine de la plainte visant à obtenir l'invalidation du mandat – ne peuvent donc pas être retenus comme preuves, car ils ont été obtenus sans mandat valable.

Le verdict rendu cette semaine risque fort de réduire à néant toute la stratégie du FBI pour faire fermer Playpen et mettre la main sur ses visiteurs américains. La décision est tout à fait susceptible de faire tache d'huile. D'autres accusés pourraient très bien se mettre à attaquer la légalité du mandat sur le même argument juridictionnel, ce qui ferait tomber des preuves à charge contre eux. Christopher Soghoian, membre de l'American Civil Liberties Union, une association de protection des droits et libertés aux États-Unis, indique que le piratage du site pédopornographique a permis de constituer 1 300 dossiers en attente. À supposer que tous vivent aux USA, combien se trouvent dans des États qui sont en dehors de la compétence géographique de la Virginie ? Sans doute une grande majorité.

UNE FAILLE LÉGISLATIVE BIENTÔT CORRIGÉE ?

Cette règle de la procédure pénale pourrait toutefois disparaître. Le département de la justice américain souhaite lever cette barrière afin que les juges puissent délivrer des mandats pour des recherches à distance sur des ordinateurs qui sont situés en dehors de leur juridiction ou lorsque leur emplacement géographique est inconnu.

Selon The Intercept, le changement législatif a de bonnes chances de passer et le feu vert de la Cour Suprême est très probable – il devrait survenir très bientôt – malgré les protestations des organisations de défense des libertés individuelles et de quelques sociétés, comme Google. Le Congrès aura ensuite six mois pour l'approuver ou la rejeter, sinon la modification entrera en vigueur.

L'AFFAIRE PLAYPEN ET LE PIRATAGE DU FBI

L'affaire Playpen remonte début 2015, quand le FBI parvient à prendre le contrôle des serveurs du site. Au lieu de le fermer tout de suite, la police choisit une autre approche, celle du honeypot : le site reste actif pendant environ deux semaines, sur les serveurs du FBI, afin de savoir qui se connecte sur Playpen. Tactique qui provoquera au passage un déluge de critiques sur le FBI.

C'est au cours de cette période que le FBI a procédé à la contamination des ordinateurs des visiteurs, afin de collecter des informations sur eux, comme leur véritable adresse IP, qui est habituellement masquée avec le réseau d'anonymisation. En effet, la connexion transite par une succession de relais afin de camoufler la géolocalisation du PC. C'est avec ces données que le FBI s'est ensuite adressé aux opérateurs pour obtenir l'identité des internautes – en tout cas ceux aux USA... [Lire la suite]



- Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles
- Expertises techniques et judiciaires
- Expertises de systèmes de vote électronique
- Formations en cybercriminalité
- Formation de C.I.L. (Correspondants Informatique et Libertés)
- Accompagnement à la mise en conformité CNIL de votre établissement

[Contactez-nous](#)

Réagissez à cet article

Source : *Pédopornographie : quand un piratage par le FBI sur Tor prive les victimes d'une justice*

Que risquent les enfants sur les réseaux sociaux ?



Que risquent les enfants sur les réseaux sociaux ?

Avoir des profils dans les réseaux sociaux peut représenter de nombreux dangers pour les enfants.

Denis JACOPINI, expert Informatique assermenté spécialisé en cybercriminalité a souhaité couvrir le sujet et a collecté quelques informations bien utiles pour comprendre le phénomène.

Quels sont les risques d'une trop grande exposition sur les réseaux sociaux?

Attardons nous rapidement sur quelques analyses bien inquiétantes :

- 38% des 9-12 ans ont un profil sur un réseau social, alors que la plupart de ces réseaux ne sont autorisés qu'à partir de 13 ans !
- 77% des 13-16 ans sont présents !
- 1/4 ont un profil public ;
- 1/5 y communique son adresse, son numéro de téléphone..
- Seulement 55% des jeunes discutent avec leurs parents de ce qu'ils font sur Facebook ;
- 92% des jeunes de 8 – 17 ans utilisent leur vraie identité sur Facebook et livrent des informations personnelles ;
- 25% des jeunes de 8 – 17 ans disent avoir déjà été victimes d'insultes ou rumeurs sur Facebook ;
- 36% ont déjà été choqués par certains contenus.

1°/ Les jeunes, trop peu sensibilisés, ont tendance à communiquer bien trop d'éléments (photos, éléments de leur vie). L'effet immédiat est que les cybercriminels auront tous les éléments dont ils auront besoin pour pouvoir usurper leur identité.

2°/ Sur Internet, tout peut être copié collé (et altéré dans le processus), il n'y a aucune garantie de confidentialité dans les échanges électroniques via les réseaux sociaux. Des photos prises lors de soirées ou dénudées peuvent facilement se retrouver à la vue de tout le monde, tout comme un message insultant, écrit dans un moment d'énergie. Les jeunes n'hésitent pas à « taguer » des amis sur les photos de groupe, sans se rendre compte que cette action impacte directement la vie privée des amis tagués.

3°/ Autre risque bien réel, s'exposer sur les réseaux sociaux augmente le risque de contact avec un pédophile cherchant avant tout à rencontrer des enfants ou des ados naïfs, crédules ou confiants.

4°/ Autre faits inquiétants, 25% des jeunes de 8 – 17 ans disent avoir déjà été victimes d'insultes ou rumeurs sur Facebook. Les cyberviolences, souvent initiée à l'école est souvent poursuivies sur les réseaux sociaux sont très courantes. Une publication d'albums de photos de vacances ou d'une soirée entre amis peut vite déraiper et se transformer en détournement obscène en ligne avec un impact sur la vie réelle. Intimidations, insultes, piratage de compte, commentaires humiliants, création de groupes de discussion pour moquer la victime – la violence des rapports entre jeunes peut pousser la victime jusqu'au suicide.

Le phénomène d'entraînement peut conduire les plus influençables à imiter des comportements violents et à se lancer dans des campagnes d'insultes contre le bouc émissaire désigné par le leader du groupe.

5°/ Enfin, risque souvent méconnu, les cybercriminels rivalisent d'ingéniosité pour concevoir des messages séduisants qui invitent à « Liker » un post viral avec un lien corrompu, des applications contenant des virus, des campagnes de phishing pour soutirer les informations de connexion, etc.

A la suite d'une exposition trop massive sur les réseaux sociaux, est-ce qu'un nouveau type de criminalité est né ?

Je répondrais à cela qu'un nouveau terrain de jeu est né !

Un espace rempli de prédateurs ou les jeunes sont des proies potentielles.

Comment optimiser la sécurité sur les réseaux sociaux?

Limitez la navigation et les échanges dans un périmètre adapté à l'âge et aux besoins du jeune. Si besoin, bloquez les réseaux sociaux jusqu'à ce qu'il soit en mesure de comprendre l'impact de ses interactions en ligne.

Discutez régulièrement avec votre enfant ou ado de ce qu'il fait sur Internet : quels sites il aime consulter, avec qui il tchatte, ce qu'il ou elle a découvert de nouveau. Expliquez-lui la différence entre de vrais amis et des connaissances numériques.

Apprenez aux enfants l'importance de la protection des informations personnelles, que ce soit les leurs ou celles de leurs amis. Informer le monde que l'on est seul ce week-end n'est peut être pas l'action la plus prudente, tout comme « taguer » ses amis sur une photo peu valorisante.

Vérifiez que les paramètres de protection de vie privée sont activés sur toutes les plates-formes utilisées par l'enfant. Expliquez que les traces numériques resteront dans le temps et qu'ils seront un jour ou l'autre confrontés à leurs actions en ligne. Soulignez l'importance de mesurer ses propos et de ne pas participer aux chasses à l'homme digitales.

Expliquez au jeune que si jamais il (ou elle) est victime d'harcèlement, ou bien s'il voit ses camarades s'acharner contre quelqu'un, il doit avertir le plus rapidement un adulte, parents ou professeur. Souvent les enfants n'osent pas avouer, par honte ou bien parce qu'ils sont manipulés par les harceleurs.

Pour plus d'informations, consultez le site du Ministère de l'Éducation Nationale Agir Contre le Harcèlement à L'École (<http://www.agircontreleharcelementalecole.gouv.fr>).



Réagissez à cet article

Sources :

Denis JACOPINI

http://www.e-enfance.org/actualite/enfants-et-reseaux-sociaux-prudence-_151.html

<http://www.e-enfance.org/enfants-danger-reseaux-sociaux.php>

<http://www.witigo.eu/controle-parental/dangers-reseaux-sociaux>