Cyberviolence: Comment sont contrôlés les groupes secrets sur Facebook ?

	Cyberviolence: Comment sont contrôlés les groupes secrets sur Facebook ?

Deux groupes ont été fermés pour avoir diffusé des photos volées de femmes nues…

Illustration Facebook – LODI FRANCK/SIPA

Ils partageaient des photos de leurs copines nues assorties de commentaires graveleux ou insultants. Deux groupes secrets sur Facebook, « Babylone 2.0 » et « Garde ta pêche », ont été fermés en fin de semaine dernière après leur découverte par une journaliste belge. Pour pouvoir entrer dans ces groupes, il faut être coopté et personne d'autre que leurs membres ne peuvent en voir le contenu. Ce qui pose un problème au réseau social, dont le principe de modération est basé sur les signalements des utilisateurs.

« Banalisation de la violence »

« Chaque utilisateur a la possibilité de signaler tout contenu qu'il considère choquant, qu'il s'agisse d'un commentaire, d'un post, d'une page, d'un profil, etc. (…) Dès le premier signalement, le contenu est consulté et analysé par une équipe dédiée mobilisée 24 heures sur 24, 7 jours sur 7. Pour la France, nous disposons d'une équipe francophone », indique Facebook France. Il s'agit donc d'une modération *a posteriori*, qui n'intervient que lorsqu'un utilisateur du réseau alerte Facebook. Si tous les membres d'un groupe sont d'accord pour partager des contenus qui enfreignent « les standards de la communauté », il y a donc peu de chances pour que ceux-ci soient interdits.

« On sait que Facebook a des soucis de modération, estime Hélène Dupont, conseillère éditoriale sur le programme Internet sans crainte. On ne peut pas attendre de Facebook d'avoir la même vigilance qu'un média car ils n'ont pas de rédaction ou de comité éditorial. C'est pour cela que nous sommes favorables à l'éducation des utilisateurs en amont. » Chez les jeunes notamment, la connaissance des outils de signalement est importante. Mais lorsqu'ils voient un contenu qui les choque, ce n'est pas leur compétence technique qui fait défaut pour lancer une alerte : « On a vu que pour la cyberviolence ou le harcèlement, la tolérance est bien plus grande en ligne que dans la réalité, note Hélène Dupont. Il y a une banalisation de la violence sur Facebook et les jeunes en réfèrent peu à des adultes. »…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Cyberviolence: Comment sont contrôlés les groupes secrets sur Facebook

Combien valent vraiment vos données personnelles sur les réseaux sociaux ?

	Combien valent vraiment vos données personnelles sur les réseaux sociaux ?

Une extension pour navigateur développée par des chercheurs de l'université de Madrid vous permet de connaître en temps réel les revenus publicitaires générés par votre profil Facebook.

Sur Internet, comme le dit l'adage : si c'est gratuit, c'est vous le produit.
SUPERSTOCK/SUPERSTOCK/SIPA

MONÉTISATION. Dans le monde des *big data*, combien valent vraiment vos données personnelles sur Facebook ? Les recettes publicitaires du réseau social ne cessent de croître de façon exponentielle : 17 milliards de dollars pour 2015, contre 764 millions en 2009. Et combien d'euros gagnés grâce à votre propre activité ? Pour l'usager, il est souvent délicat de répondre à cette question, tant l'opacité sur les algorithmes utilisés par les plate-formes (dont réseaux sociaux) est grande. Mais une extension gratuite pour le navigateur Chrome (bientôt disponible aussi pour Opera et Firefox) développée par des chercheurs de l'Université de Madrid permet d'estimer en temps réel la valeur économique dégagée par votre profil au fur et à mesure du temps passé sur le site de Mark Zuckerberg… un travail de recherche qui interroge d'ailleurs la valeur commerciale globale de nos données et les modes de régulation possibles.

Même sans cliquer sur les pubs, un internaute rapporte

L'outil madrilène, baptisé FDVT (pour *Facebook Data Visualisation Tools*), permet de quantifier l'évolution de la valeur publicitaire d'un profil en fonction du temps passé sur le réseau social. Il s'appuie sur le projet TYPES, financé par l'Europe dans le cadre de l'initiative Horizon 2020, qui se préoccupe de la transparence de la publicité en ligne dans l'économie numérique. *« Chacun a une valeur différente sur le marché selon son profil, de sorte que l'outil ne fournit qu'une estimation des profits »*, expliquent Ángel et Rubén Cuevas, professeurs à l'Université Charles III de Madrid et créateurs de l'extension. *« Lorsque vous vous connectez à Facebook et recevez une publicité, nous déterminons la valeur qui lui est associée, le prix que ces annonceurs paient pour afficher ces publicités et chacun de vos clics sur une de ces publicités. »* Les deux chercheurs ont notamment constaté que le coût d'un utilisateur américain est à peu près deux fois supérieur à celui d'un utilisateur espagnol. Et ce n'est pas tout : ils ont également mis en évidence que même sans jamais cliquer sur un lien sponsorisé, Facebook générait néanmoins de la valeur à partir de votre profil.

Capture d'écran de l'extension : après quelques minutes seulement d'activité et sans cliquer sur aucune pub, l'auteur de ces lignes a déjà cédé près d'un dollar de revenu publicitaire à Facebook.

Une commodité marchande comme les autres ?

À l'heure où les données personnelles s'échangent pour une poignée de dollars (et notamment en Chine, on l'on peut acquérir les données personnelles de citoyens américains pour à peine 100 dollars), se pose la question de leur valorisation. Un rapport écrit fin 2016 par le Oxford Internet Institute s'interrogeait ainsi sur la chaîne de valeur des données personnelles (c'est à dire, l'évolution de leur valeur de leur création à leur utilisation dans l'économie numérique), et sur les types de régulation possibles, par exemple via une possible taxation de l'usage des données personnelles. Une démarche qui n'aurait rien d'évident, au vu de la nature internationale et dématérialisée des échanges de données…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Sur les réseaux sociaux, combien valent vraiment vos données personnelles ? – Sciencesetavenir.fr

---

Prévisions cybercriminalité pour 2017

	Prévisions cybercriminalité pour 2017

Nous sommes tombés sur cet article sur le site Internet « Informaticien.be » et n'avons pas pu nous empêcher de le partager avec vous tant il est en accord avec les prévisions ressorties de nos analyses. Aux portes de 2017, les entreprises, administrations et association non seulement vont devoir s'adapter à une réglementation Européenne risquant s'impacter lourdement la réputation des établissements qui devront signaler à la CNIL qu'elle viennent d'être victime de piratage, mais également, l'évolution des techniques de piratage vont augmenter les risques qu'auront les organismes à se faire pirater leurs systèmes informatiques. N'hésitez pas à consulter notre page consacrée aux bons conseils que nous prodiguons depuis de nombreuses années sur https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles.
Denis JACOPINI

Trend Micro présente son rapport annuel des prévisions en matière de sécurité: 'The Next Tier – 8 Security Predictions for 2017'. L'année prochaine sera marquée par des attaques de plus grande envergure à tous les niveaux. Les cybercriminels adopteront des tactiques différentes pour tirer parti de l'évolution du paysage technologique.
« Nous pensons que la General Data Protection Regulation (GDPR) va non seulement changer fondamentalement la manière dont les entreprises gèrent leurs données, mais aussi induire de nouvelles méthodes d'attaque. La tactique du ransomware va également s'étendre pour toucher plus d'appareils, tandis que la cyberpropagande influencera de plus en plus l'opinion publique", déclare Raimund Genes, CTO de Trend Micro.
En 2016, l'on a assisté à une formidable augmentation des vulnérabilités d'Apple avec pas moins de 50 fuites. A cela s'ajoutent 135 bugs Adobe et 76 bugs Microsoft. Alors que Microsoft continue d'améliorer ses facteurs limitatifs et qu'Apple est de plus en plus considéré comme le système d'exploitation prépondérant, ce déplacement apparent des 'exploits' des logiciels vulnérables va encore s'accentuer en 2017.
L'IoT et l'IIoT – dans la ligne de mire des attaques ciblées
L'Internet of Things (IoT – internet des objets) et l'Industrial Internet of Things (IioT – internet industriel des objets) seront de plus en plus dans la ligne de mire des attaques ciblées en 2017. Ces attaques tirent parti de l'engouement croissant suscité par les appareils connectés en exploitant les failles et les systèmes non protégés et en perturbant des processus d'entreprise. L'usage croissant d'appareils mobiles pour surveiller les systèmes de production dans les usines et les milieux industriels, combiné au nombre important de vulnérabilités dans ces systèmes constitue une réelle menace pour les organisations.
Explosion de l'extorsion professionnelle
Le Business E-mail Compromise (BEC) et le Business Process Compromise (BPC) représentent de plus en plus une forme relativement simple et économiquement rentable d'extorsion professionnelle. En incitant un employé innocent à verser de l'argent sur le compte bancaire d'un criminel, une attaque BEC peut rapporter 140.000 dollars. Bien que le piratage direct d'un système de transaction financière exige plus d'efforts, cela représente une manne de pas moins de 81 millions de dollars pouvant tomber aux mains des criminels.
Autres faits marquants du rapport
Le nombre de nouvelles familles de ransomware ne progresse que de 25 %. Mais le ransomware s'étend désormais aux appareils IoT et aux terminaux informatiques autres que les desktops (par exemple les systèmes POS ou les distributeurs automatiques).
Les fournisseurs ne parviendront pas à protéger à temps les appareils IoT et IIoT pour éviter des attaques DoS (refus de service) ou d'autres types d'attaques.
Le nombre de failles découvertes dans les technologies Apple et Adobe augmente, ce qui vient s'ajouter aux « exploit-kits ».
46 pour cent de la population mondiale est aujourd'hui reliée à l'internet : la cyberpropagande ne va cesser d'augmenter, à présent que les nouveaux dirigeants des grands pays sont en place. L'opinion publique risque donc d'être influencée par de fausses informations.
Comme ce fut le cas lors de l'attaque de la Banque du Bangladesh plus tôt cette année, les cybercriminels parviennent à modifier des processus d'entreprise via des attaques BPC, et à en tirer largement profit. Les attaques BEC restent d'actualité pour extorquer des fonds à des employés qui ne se doutent de rien.
Le GDPR produira des changements de politique et administratifs qui auront un lourd impact sur les coûts. Cela exigera aussi des examens complexes des processus de données pour assurer la conformité réglementaire.
De nouvelles méthodes d'attaques ciblées déjoueront les techniques de détection modernes, permettant aux criminels de s'attaquer à différentes organisations.
Original de l'article mis en page : Le ransomware s'étend aux appareils connectés et à l'internet des objets – Press Releases – Informaticien.be

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
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 : Le ransomware s’étend aux appareils connectés et à l’internet des objets – Press Releases – Informaticien.be

---

Piratage de ses comptes de réseaux sociaux. Comment réagir ?

	Piratage de ses comptes de réseaux sociaux. Comment réagir ?

Vos comptes sociaux abritent une somme considérable de données personnelles. Veillez à bien les sécuriser pour éviter les piratages d'individus malveillants.

Prévenir un piratage

1.

Choisissez des mots de passe complexes, différents et non-signifiants !

Aucune personne ou ordinateur ne doit être en mesure de le deviner. La CNIL publie des conseils pour créer un mot de passe efficace, le retenir et le stocker dans une base.

2.

Ne communiquez pas votre mot de passe

Il est vivement déconseillé de communiquer votre mot de passe à une tierce personne, de l'enregistrer dans un navigateur si vous n'avez pas défini de mot de passe maitre ou dans une application non sécurisée.

3.

Activez un dispositif d'alerte en cas d'intrusion

La double authentification est une option activable sur la plupart des réseaux sociaux. Lorsque vous vous connectez depuis un poste informatique inconnu, le réseau social vous demandera de confirmer l'accès en entrant un code que vous aurez reçu par sms ou par courrier électronique. D'autres fonctions proposent simplement de vous alerter si une personne extérieure tente de se connecter à votre compte depuis un terminal inconnu (PC, smartphone, tablette, mac).

4.

Déconnectez à distance les terminaux encore liés à votre compte

Là encore, cette option disponible sur la plupart des réseaux sociaux vous permet d'identifier l'ensemble des terminaux avec lesquels vous vous êtes connectés à votre compte. Lorsque cela est possible, il est conseillé de désactiver le lien avec les terminaux dont vous ne vous servez plus. Une connexion identifiée depuis un navigateur inconnu ou une ville inconnue pourra vous mettre la puce à l'oreille.

5.

Désactivez les applications tierces connectées à votre compte

Il arrive que les applications tierces connectées à votre compte soient vulnérables à une attaque extérieure. Il est conseillé de désactiver les applications tierces dont vous avez autorisés l'accès par le passé et qui ne vous servent plus.

6.

Réglez vos paramètres de confidentialité

En devinant votre nom, votre fonction, votre liste d'amis, une personne mal intentionnée pourrait facilement déduire des informations qui servent à réinitialiser votre compte ou simplement à usurper votre identité afin de changer votre mot de passe par exemple.

Repérer un piratage

- votre mot de passe est invalide
- des tweets/posts imprévus sont envoyés depuis votre compte
- des messages privés sont envoyés de façon non volontaires
- des comportements inhabituels ont lieu sur votre compte sans consentement (comme suivre, se désabonner, ou bloquer)
- une notification de la part du réseau social vous informe que « Vous avez récemment changé l'adresse électronique associée à votre compte. »

Réagir en cas de piratage

1. Signalez le compte piraté auprès du réseau social
2. Demandez une réinitialisation de votre mot de passe
3. Une fois votre compte sécurisé, n'oubliez pas de parcourir les rubriques « sécurité » proposées par ces réseaux sociaux

---

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur 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 réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) 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 : Prévenir, repérer et réagir face au piratage de ses comptes sociaux | CNIL

---

14 millions de Français victimes des pirates

Informatiques en 2016

	14 millions de Français victimes des pirates Informatiques en 2016

La prolifération des cyberattaques a un corollaire : aucune classe d'âge et aucune profession ne sont aujourd'hui épargnées. Explications.

Dans un rapport publié mercredi 16 novembre, l'éditeur d'antivirus Symantec-Norton pointe l'ampleur que le phénomène « cybercriminel » a prise en 2016. Selon cette étude, 13,7 millions de Français auront été victimes d'attaques informatiques cette année. Le fait d'avoir baigné dans l'univers numérique depuis sa naissance ne change rien à la donne. Les « digital natives » (comme les experts désignent les jeunes qui manipulent des ordinateurs depuis le berceau) sont aussi démunis face à cette menace que leurs aînés.
La génération Y, celle des 18-34 ans, fait ainsi partie des plus touchées par le problème. Il faut dire que cette catégorie de population se comporte sur le Web de manière particulièrement risquée. Or, pour les professionnels de la cybersécurité, la négligence des internautes serait en cause dans la plupart des attaques informatiques dont ils sont victimes.

Des internautes imprudents

Bien que 77 % des Français sachent qu'ils doivent protéger leurs données en ligne, les utilisateurs gardent de mauvaises habitudes sur le Web. Les réflexes d'élémentaire prudence sont de peu de poids face à l'attrait de certains liens… même d'origine douteuse. Ainsi, 65 % des Français reconnaissent avoir déjà ouvert une pièce jointe postée d'un expéditeur inconnu. Et quasiment un internaute sur cinq partage ses mots de passe avec d'autres utilisateurs. Faut-il, dès lors, s'étonner qu'un Français sur deux se résigne à l'idée qu'il est désormais plus probable qu'une personne accède frauduleusement à ses appareils domestiques connectés qu'à son logement ?
D'après Laurent Heslault, directeur des stratégies numériques chez Symantec, les internautes ont bien conscience des dangers mais « n'ont pas envie de prendre les précautions adéquates pour assurer leur sécurité ». Alors que les cybercriminels, eux, disposent de techniques de plus en plus recherchées pour arriver à leurs fins.
Il ne s'agit pas seulement de paresse chez les internautes. 31 % d'entre eux sont dépassés par la quantité d'informations qu'ils ont à protéger. La plupart considèrent d'ailleurs que la question de la gestion sécurisée des données ne les concerne pas et qu'il appartient aux fournisseurs d'accès à Internet et aux entreprises du secteur des nouvelles technologies de résoudre ces problèmes.

Un problème mondial

Une étude réalisée en octobre, par le Ponemon Institute pour le compte de l'éditeur de logiciels professionnels Varonis Systems, démontre qu'il ne s'agit pas d'un problème strictement hexagonal. Si 37 % (seulement !) des internautes français indiquent qu'ils prennent toutes les mesures appropriées pour protéger les données auxquelles ils accèdent et qu'ils utilisent, la même réponse est donnée par 50 % chez les collaborateurs allemands, 39 % des employés britanniques et 35 % des employés américains.
Le nombre d'entreprises ayant fait l'expérience des ransomwares l'an dernier est en hausse constante. Ces logiciels rançonneurs, dont le FBI a révélé qu'ils avaient généré, au premier semestre 2016, plus de 209 millions de dollars de butin, ont infecté les serveurs de 12 % des entreprises allemandes, contre 17 % aux États-Unis, 16 % en France et 13 % au Royaume-Uni. Le nombre de cas de perte ou de vol de données au cours des deux dernières années a, lui aussi, explosé… Et l'on ne compte plus les cyberbraquages signalés chaque semaine à travers la planète.
De quoi inciter les États à renforcer leur arsenal pour lutter plus efficacement contre les gangs à l'oeuvre sur la Toile. Les 68 pays signataires de la convention de Budapest, le premier traité international abordant la question de la lutte contre la cybercriminalité adopté en 2001, se sont d'ailleurs réunis les 14 et 15 novembre derniers pour renforcer leur coopération en la matière. Un protocole additionnel à la convention sera adopté courant 2017 pour mettre en place un nouvel outil juridique permettant de collecter des preuves électroniques sur le « cloud », quelle que soit la localisation du serveur qui l'héberge… Preuve, s'il en était besoin, que les gouvernements du monde entier ont pris la mesure de la menace.

Quels sont les cyberdélits les plus fréquents en France ?

• Le vol de mot de passe (14 %)
• le piratage électronique (11 %)
• le piratage des réseaux sociaux (10 %)
• la fraude à la carte de crédit (9 %)
• le ransomware ne représente que 4 % des actes de cybercriminalité contre les particuliers (mais 12 % des entreprises), soit environ 548 000 cas en 2015. 30 % des victimes de ransomware ont payé la rançon demandée et 41 % d'entre eux n'ont pas pu, malgré tout, récupérer leurs fichiers. [Article Original du Point]

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 le 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 : Cybersécurité : un

Français sur cinq victime de hackers en 2016

10 points à connaître sur l’attaques DDoS des États-unis

10 points à connaître sur l’attaques DDoS des États-unis

Le vendredi 21 Octobre, une série d'attaques par déni de service (DDoS) a provoqué une importante perturbation de l'accès aux sites Internet aux États-Unis. Les attaques ont ciblé les serveurs DNS (qui livrent les informations aux bonnes adresses), rendant de nombreux sites inaccessibles pendant plusieurs heures. Parmi eux figurent des sites permettant d'effectuer des achats en ligne, des réseaux sociaux, et d'écouter de la musique.

10 points à connaître sur l'attaque DDoS

ESET dresse un bilan des 10 points à retenir sur cette attaque. En voici un extrait, la version détaillée étant disponible sur WeLiveSecurity (version anglaise).

1. Les attaques ont ciblé la société Dyn, un important fournisseur de serveur DNS utilisé par de grands groupes comme Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, Comcast, et le réseau Playstation.
2. Les attaquants ont piraté des milliers d'appareils connectés mal-protégés tels que les routeurs domestiques et les caméras de surveillance, pour former un réseau botnet.
3. L'attaque a été facilitée par la négligence des utilisateurs qui n'ont pas changé le mot de passe par défaut de leurs appareils.
4. L'exploitation d'appareils numériques par un code malveillant peut perturber l'activité économique d'un pays : il est probable que plusieurs millions de dollars de vente ligne soient perdus.
5. De nombreuses personnes malveillantes sont prêtes à nuire à l'activité économique d'un pays au moyen d'un code malveillant, et ce pour de multiples raisons.
6. L'information et l'éducation des utilisateurs sont primordiales.
7. La réduction du nombre d'appareils connectés vulnérables est un objectif réalisable et auquel les entreprises peuvent contribuer. Voici d'ailleurs 4 mesures recommandées par l'US CERT :

• Remplacer tous les mots de passe par défaut par des mots de passe forts ;
• Mettre à jour les objets connectés ;
• Désactiver l'UPnP (universal plug and play) des routeurs sauf en cas d'absolue nécessité ;
• Acheter des objets connectés auprès d'entreprises certifiant de fournir des dispositifs sécurisés.

1. Le code malveillant infectant les routeurs n'est pas nouveau et a déjà été repéré en mai 2015 par les équipe ESET.
2. Les nouvelles générations d'attaques DDos amplifient leur portée dans le fait qu'elles s'appuient sur de nombreux objets connectés.
3. Cette dernière attaque nous montre à quel point un pays peut être vulnérable en cas d'attaque de son système d'informations.

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 le 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 : ESET livre les 10 points à connaître sur l’attaque DDoS – Global Security Mag Online

---

Une série de clics suffisent à vous identifier

	Une série de clics suffisent à vous identifier

Corréler l'historique des pages Web visitées aux profils Twitter permet d'identifier les internautes, expliquent des chercheurs de Princeton et de Standford. Ou quand le Big Data vient lever ce qui restait d'anonymat sur le Web.

L'anonymat sur Internet, un vœu pieux ? C'est en somme la démonstration d'une équipe de chercheurs des universités de Princeton et Standford. Ces derniers ont imaginé une extension pour le navigateur Chrome qui permet aux utilisateurs de prendre conscience de l'intérêt des traces qu'ils laissent sur le Net pour des publicitaires ou des espions. L'utilitaire, appelée Footprints, collecte les liens cliqués par l'utilisateur au cours des 30 derniers jours et, à partir de ces seules informations, renvoie une liste de 15 profils Twitter susceptibles de coller à cet usage. Ensuite, l'extension s'efface d'elle-même, assurent les chercheurs.
Professeur assistant à l'université de Standford, Sharad Goel explique que l'objectif de cet outil est avant tout éducatif : « *nous n'envisageons pas de rendre cet outil accessible à d'autres, il s'agit avant tout de réveiller les consciences.* » Un outil de ce type permettrait par exemple à une entreprise traçant déjà ses utilisateurs – soit la totalité des sites marchands notamment – de deviner l'identité des internautes, par corrélation avec leur usage d'un réseau social. En effet, si les publicitaires ou les spécialistes du marketing analysent déjà les traces laissées par les utilisateurs pour personnaliser l'expérience des clients online, ils ne sont en général pas en mesure de remonter jusqu'à l'identité réelle de l'internaute. Les chercheurs montrent que cette anonymat déjà tout relatif pourrait en pratique être levé, grâce à des analyses statistiques et au Big Data.

Dis-moi ce que tu cliques, j'en déduirai qui tu es

Dans un billet de blog, une étudiante de Standford ayant participé à la conception de Footprints, Jessica Su, explique le principe de la méthode : « *Partant de la combinaison unique de pages Web qu'un individu a visitées, nous déterminons les fils de réseau social similaires à cet historique, calculant une liste d'utilisateurs qui ont toutes les chances d'avoir produit cette série de clics. De cette façon, nous pouvons relier l'identité réelle d'une personne à un jeu de liens visités, y compris les liens qui n'ont jamais été postés publiquement sur aucun réseau social.* »…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Une série de clics et Twitter suffisent à vous identifier

Alerte, découverte d’un virus qui se propage principalement via les Réseaux Sociaux

	Alerte, découverte d’un virus qui se propage principalement via les Réseaux Sociaux

Afin de voler leurs données, le malware utilise une campagne de diffusion massive ciblée en renvoyant les victimes vers un site gouvernemental libyen compromis et contenant le malware

Malgré le manque de sophistication du malware et un mécanisme de propagation rudimentaire, les auteurs de cette menace ont démontré qu'ils étaient capables de compromettre des sites gouvernementaux avec succès.
Au cours de leurs recherches, les **experts ESET** ont découvert que les attaquants compromettent des profils de réseaux sociaux (Facebook, Twitter…) et postent des liens amenant au téléchargement de logiciels malveillants. Le post est rédigé en arabe et explique : « le premier ministre a été capturé à deux reprises, dont cette fois-ci dans une bibliothèque ».

Ce message texte relativement court est suivi d'un lien vers le site gouvernemental compromis.

Figure 1 : Post sur Facebook renvoyant vers un lien comportant le malware

En plus de la diffusion massive de cette campagne, les cybercriminels mènent des attaques ciblées par l'envoi d'e-mail contenant une pièce jointe malveillante de type spearphishing. Pour convaincre les victimes d'exécuter le code malveillant, des astuces d'ingénierie sociale sont mises en œuvre, comme l'utilisation d'icônes MS Word et PDF à la place de celles des exécutables et de techniques de double extension dans les noms de fichier, comme .pdf.exe. Dans certains cas, le malware peut afficher un document leurre.
Les experts ESET ont identifié le malware comme appartenant à la famille des Chevaux de Troie qui tentent de recueillir diverses informations par le vol de données classiques. Il peut être déployé sous plusieurs configurations. **La version complète du logiciel malveillant peut enregistrer les frappes de clavier, collecter des fichiers de profil des navigateurs Mozilla Firefox et Google Chrome, enregistrer des sons à partir du microphone, réaliser des captures d'écran depuis la webcam, et recueillir des informations sur la version du système d'exploitation et du logiciel antivirus installé.** Dans certains cas, le logiciel malveillant peut télécharger et exécuter des outils tiers de récupération de mots de passe enregistrés à partir d'applications installées.
« Nous avons analysé un échantillon de ce malware qui est actif depuis au moins 2012 dans des régions spécifiques du globe. Par le passé, les auteurs de cette cybermenace utilisaient ce malware pour une diffusion massive. Il convient de noter qu'il est encore utilisé dans des attaques de spearphishing », explique Anton Cherepanov, malware researcher chez ESET.
Pour plus de détails sur ce malware, cliquez ici.
Source : ESET

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Comment Facebook manipule le contenu qu’il nous affiche ?

Censure d'une photo historique, choix d'articles qui renforcent les partis pris: les centaines de millions d'internautes qui s'informent via leurs «amis» sur Facebook, plutôt que par les médias classiques, courent le risque d'une information biaisée, selon des experts.

Dernier exemple en date, la censure par Facebook la semaine dernière de la célèbre photo d'une petite Vietnamienne nue brûlée au napalm, au nom de sa politique contre la nudité des enfants. Critiqué dans le monde entier, le groupe américain a rétabli la photo et promis de tenir compte à l'avenir du «statut d'icône» des clichés historiques.
Cette polémique a révélé l'importance prise par Facebook comme source d'information pour une majorité d'internautes dans le monde.
Un sondage international du Reuters Institute montre que 51% des personnes interrogées dans 26 pays s'informent par les réseaux sociaux, dont 44% par Facebook, et que 12% en ont fait leur première source d'information. En France, un Français sur deux consulte Facebook, surtout sur mobile, et peut y passer plusieurs heures par semaine.
Aucun des 1,7 milliard d'utilisateurs ne voit les mêmes informations dans son «newsfeed» (fil d'actualités), qui compile les messages de ses «amis»: un mélange de commentaires personnels et d'articles partagés, provenant aussi bien de grands médias que de blogues inconnus.
Entre les milliers de messages produits par ses amis, impossible de tout lire: c'est l'algorithme de Facebook qui, pour chacun, classe ceux placés en haut de page. Et donc ceux qui seront vus, car en moyenne l'utilisateur ne lit que 200 des 2000 messages de son fil.
Les utilisateurs ignorent le plus souvent l'existence et les critères de ce tri, qui ont changé sans cesse en 10 ans d'existence. En juin, Facebook a brusquement décidé de privilégier les messages personnels au détriment des partages d'articles, diminuant la place des médias classiques…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Comment Facebook filtre notre connaissance du monde | Laurence BENHAMOU | Internet

Comment préparer les enfants aux Réseaux Sociaux ?

	Comment préparer les enfants aux Réseaux Sociaux ?

Dangers de l'Internet au-delà de logiciels malveillants, ou l'enlèvement des données par des ransomware. Sur le Net, le respect de la vie privée est mis à mal par les réseaux sociaux, les moteurs de recherche et la publicité. Dans le cas des mineurs, il y a des risques plus inquiétants, dont ils ne sont pas pleinement conscients, mais leurs parents, les enseignants et la société doivent assurer leur sécurité. Une étude récente, appelé Kids Connected, et menée par la firme de sécurité Kaspersky Lab avec iconKids et jeunesse, révèle des faits troublants sur la façon dont les enfants se comportent en ligne. Comportements qui peuvent conduire à provoquer plus de crainte.

Ce rapport montre que **les enfants âgés de 8 à 16 ans sont accros aux réseaux sociaux**. En outre, l'activité peut les mettre en danger, eux et leurs **familles**. 35% des enfants disent qu'ils ne veulent pas être sans réseaux sociaux, et sont désireux de rejoindre des groupes en leur sein, ils sont en mesure de partager beaucoup d'informations personnelles. **Le problème** est qu'ils le font sans avoir conscience que les données qu'ils partagent sont vues par de nombreux utilisateurs et peuvent être utilisées par des personnes potentiellement dangereuses.

Trop d'informations personnelles

Mais **qu'est-ce que les mineurs partagent le plus** ? La plupart des enfants, 66%, **montrent l'école** où ils étudient, 54% **des lieux qu'ils visitent**, et 22% partagent même **la gestion de leurs maisons**. Mais, 33% des enfants donnent également des **informations sur les effets de leur famille et de leurs parents**, sur leur travail (36%) ou sur **ce que leurs parents facturent** (23% des enfants).

Mais, outre le partage des données réelles, **les mineurs sont également prêts à mentir sur le réseau**, et ils le font surtout **si ça peut leur ouvrir des portes**. Un tiers des enfants est prêt à mentir au sujet de l'âge. 17% des enfants font semblant d'être plus âgés, et de modifient leur âge en fonction du web ou le service qu'ils veulent utiliser, étant donné que beaucoup d'entre eux ont des restrictions (très facile à sauter) d'âge.

Avec ces données, **les cybercriminels disposent d'informations suffisantes pour être utilisés à des fins malveillantes**. Parmi les activités criminelles qu'ils pourraient commettre, ils trouvent l'emplacement physique des mineurs. **Tous les enfants doivent apprendre à un âge précoce ce qu'ils devraient partager en ligne**, ou non. Et connaître les paramètres des réseaux sociaux de la vie privée, de sorte que seuls leurs amis peuvent voir leurs publications et leurs données.

Comprendre quelles sont vos données et la façon de les protéger

Tous les enfants et leurs parents doivent comprendre ce que sont les données personnelles, et **la façon dont on peut les protéger**. "Ceci est comparable aujourd'hui à lire et à écrire», dit Janice Richardson, consultant senior chez European Schoolnet, qui explique que **«les enfants ont besoin d'apprendre à un âge précoce que la vie privée est votre bien le plus précieux, et un droit fondamental ».**

Comme des **conseils de base** qui sont donnés par Kaspersky Lab afin d'éviter autant que possible les risques:

• Une bonne **communication est essentielle**. Il faut parler aux enfants au sujet de leurs expériences et préoccupations.

• **Réalisez les premières étapes dans les réseaux sociaux avec eux** pour créer le profil, activez les options de confidentialité, publiez votre premier poste …

• Les réseaux sociaux ont des **restrictions d'âge**. La plupart sont fixée à 13 ans. À cet âge, il est commode d'en profiter pour leur parler et leur expliquer leurs droits, les responsabilités et les préparer à l'entrée dans le monde numérique.

• Cela peut **devenir un jeu**, quelque chose que vous faites en famille: par exemple, l'impression de leur profil, accroché au mur, leurs postes … Ils pourront visualiser le public à qui est destiné chaque contenu.

• **Établir des règles** pour leur utilisation.

• **Encourager les enfants à communiquer avec vous**, ils vous apprendront de nouvelles applications récemment installées, les services qu'ils utilisent … Si cela devient une habitude depuis le début, il sera plus facile de partager des informations et de leur **parler de la vie privée et de sécurité**.

Réagissez à cet article

Original de l'article mis en page : La situation préoccupante des enfants dans le réseau: mentir pour accéder aux réseaux sociaux et y donner trop d'informations