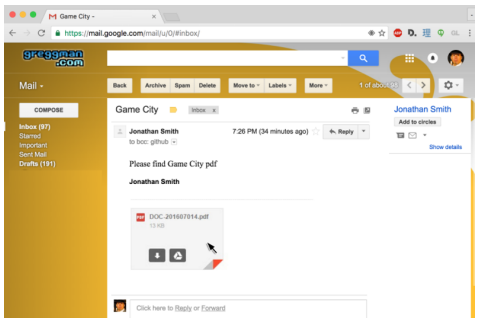
Comment se protéger d’une nouvelle arnaque au phishing sur Gmail ?

Comment se protéger d’une nouvelle arnaque au phishing sur Gmail ?

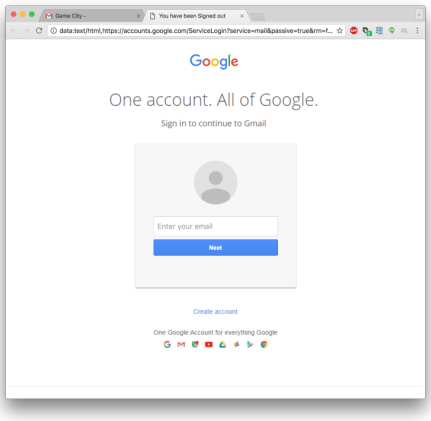
Une arnaque au phishing particulièrement élaborée vise les utilisateurs de la messagerie de Google.



Crédit : Greggman

Ce mail semble contenir une pièce jointe

Une arnaque au phishing au mode opératoire à la sophistication inédite sévit depuis plusieurs semaines sur la messagerie Gmail. L'attaque, qui vise à dérober des informations personnelles afin de les réutiliser à l'insu de l'utilisateur, prend la forme d'un mail envoyé par un contact contaminé. **Il continent une pièce-jointe et un message lapidaire du type « voici le pdf demandé ».** Un clic sur la pièce-jointe renvoie l'utilisateur vers une page à l'apparence de Google Drive et lui demande de s'identifier pour la visualiser. Une fois l'opération effectuée, l'assaillant prend possession du compte de la victime, peut à son tour envoyer le mail de hameçonnage à tous ses contacts et se livrer à des usurpations d'identité ou à des escroqueries.



Crédit : Greggman

Cette page ressemble à la page d'accueil Gmail

Comme l'explique un blogueur américain qui s'est fait piéger par l'arnaque, la pièce-jointe est en fait une image intégrée dans le corps du mail associée à un lien renvoyant automatiquement vers une page web. L'url contient « https://accounts.google.com » et laisse à penser qu'il s'agit du véritable site de Google. Mais elle débute par data « :text/html » et contient un script aspirant l'identifiant et le mot de passe de la victime lorsqu'ils sont renseignés dans le formulaire.

Dans un communiqué, Google dit avoir pris connaissance du problème. « Nous continuons de renforcer nos moyens de défense contre cela. Nous faisons de notre mieux pour protéger nos utilisateurs de différentes manières, en détectant les messages de phishing grâce au deep learning, en adressant des alertes de sécurité lorsque plusieurs liens suspicieux arrivent dans les mails, en repérant des tentatives de connexion douteuses, etc. Les utilisateurs peuvent aussi activer la validation en deux étapes pour ajouter une protection supplémentaire à leur compte », écrit Google dans un communiqué.

Comment fonctionne le phishing

Contraction des mots « fishing » (pêche en français) et « phreaking » (terme désignant le piratage des lignes électroniques) – le phishing est **une technique dite de « hameçonnage » basée sur de faux mails** qui visent à collecter les données bancaires ou les mots de passe des clients. À partir de ces documents, les pirates peuvent ensuite se livrer à des usurpations d'identité et à des escroqueries.

Ces faux courriels se présentent souvent comme des courriers envoyés par une source sûre, comme le Trésor public ou les banques. Trompées par l'expéditeur supposé, les victimes fournissent souvent elles-mêmes leurs propres données personnelles. Une autre possibilité consiste à envoyer des SMS ou des mails malveillants en masse qui contiennent un lien permettant d'installer, sans le savoir, un logiciel pirate qui pourra récupérer les données personnelles des personnes ainsi trompées.

Surveiller les mails et leur orthographe

Il s'agit donc de surveiller les mails et leur contenu. Les courriels émanant d'une structure officielle (la banque, EDF, ou la caisse d'allocations familiales par exemple) ne demandent jamais à leurs clients de saisir leurs informations personnelles directement dans un mail mais depuis un site Internet crypté. Dans ce cas, **un petit cadenas apparaît systématiquement à gauche de l'URL** du site pour garantir la confidentialité des informations.

Par ailleurs, en cas d'information importante, une banque ou un opérateur contactent généralement leurs clients par courrier ou par téléphone. Les mails utilisés dans le cadre des tentatives d'escroqueries font souvent état de **situations alarmistes** et comportent des **fautes d'orthographes** ou de syntaxe laissant penser que le message a été rédigé par un logiciel de traduction automatique.

Vérifier les adresses électroniques et les URL des sites internet

Dans certains cas de phishing, les victimes sont redirigées vers un faux-site, qui ressemble comme deux gouttes d'eau au site officiel. Il faut alors vérifier que l'URL est bien la même que celle du site copié. En général, elle est beaucoup plus longue et compliquée et on peut remarquer que, dans le corps du mail, le texte affiché sous forme de lien ne correspond pas du tout au lien réel, dont l'adresse s'affiche lorsqu'on positionne le curseur dessus. Dans le cas de l'arnaque aux faux mails de la Cpam, on peut s'apercevoir que l'adresse de réclamation ne correspond pas à celle d'un organisme officiel puisqu'elle se termine en « gmail.com ».

Original de l'article mis en page : Une nouvelle arnaque au phishing sur Gmail, comment s'en protéger

---

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

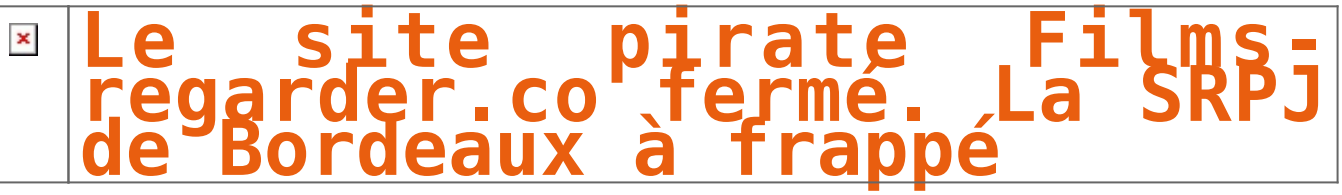
Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Une nouvelle arnaque au phishing sur Gmail, comment s’en protéger

---

Le site pirate Films-regarder.co fermé. La SRPJ de Bordeaux à frappé



Sa mise hors-ligne avait questionné plusieurs internautes sur Twitter depuis quelques heures. L'explication nous est venue de l'ALPA : le site de streaming films-regarder.co a baissé pavillon, suite à l'interpellation de son administrateur.

L'Association pour la lutte contre la piraterie audiovisuelle (ALPA) nous indique en effet que « *les investigations menées par la Direction interrégionale de la police judiciaire de Bordeaux ont abouti à la fermeture du site films-regarder.co* ».

Pour l'ALPA, « bras armé » de l'industrie du cinéma et de l'audiovisuel, ce site créé en 2013 « *dont la popularité n'a cessé d'augmenter proposait l'accès à près de 800 films et 700 séries télé piratés. Les titres étant régulièrement renouvelés en fonction des nouvelles sorties* ».

Il profitait d'une certaine popularité, un million de visiteurs uniques par mois (chiffres Médiamétrie NetRatings) et d'après les calculs de l'association, il « *totalisait 2, 2 millions de visionnages d'œuvres contrefaites dans le même temps* ». Du coup, le préjudice calculé par les ayants droit, selon les nouvelles normes en vigueur depuis notamment la loi sur la contrefaçon, est estimé à 30 millions d'euros.

200 000 euros perçus pendant 18 mois

« *L'administrateur du site a reconnu avoir agi seul et avoir perçu environ 200 000 euros pendant les 18 derniers mois d'activité du site. Les revenus provenaient de régies publicitaires étrangères et étaient versés sur des comptes à l'étranger* ». Il a été présenté au procureur de la République de Toulouse, qui a sollicité l'ouverture d'une information judiciaire. « *L'intéressé a été mis en examen et placé sous contrôle judiciaire* » ajoute l'ALPA dans son communiqué.

Conformément au Code de la propriété intellectuelle, il risque, outre les dommages et intérêts, jusqu'à trois ans de prison et 300 000 euros d'amende.

Libertyland.co, voirfilms.org et voirfilms.co

Soulignons que l'ALPA a également adressé à Google Inc une notification DMCA pour lui demander le déréférencement de Libertyland.co, voirfilms.org et voirfilms.co.

Seulement, suivant à la lettre la demande, l'entreprise américaine s'est contentée de déréférencer uniquement les pages d'accueil de ces sites, non les sous sections qui restent indexées sur les différentes versions du moteur.

Original de l'article mis en page : Films-regarder.co fermé, son administrateur interpellé et mis en examen

---

Réagissez à cet article

L’Anssi épingle le fichier biométrique défendu par Cazeneuve

L’Anssi épingle le fichier biométrique défendu par Cazeneuve

Très décrié depuis sa découverte, le décret instituant le fichier TES (Titres Électroniques Sécurisés) a entraîné un intense débat en France sur l’usage de la biométrie et la protection des données qui y sont attachées.…[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l’étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif 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).

Plus d’informations sur notre page formations.

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

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

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

Contactez-nous

Réagissez à cet article

Alerte ! Un phishing élaboré vise les utilisateurs de Gmail

Alerte ! Un phishing élaboré vise les utilisateurs de Gmail

Une attaque au phishing particulièrement élaborée sévit depuis quelque temps contre les utilisateurs de comptes Gmail, ce qui amène amène plusieurs spécialistes à inviter le public à la prudence.

En matière de phishing – les escroqueries consistant à se faire passer pour un tiers de confiance afin de dérober les informations bancaires ou personnelles de sa cible –, la dernière arnaque en cours contre les utilisateurs de Gmail, particulièrement répandue en 2016, s'avère très efficace, au point de duper des utilisateurs chevronnés.
Comme la majorité des tentatives, cette arnaque commence par l'envoi d'un email a priori banal, provenant généralement d'un contact de notre carnet d'adresse qui a déjà été victime de ce phishing. La manœuvre frauduleuse mise sur sa prétendue pièce jointe.
En cliquant sur ce fichier a priori inoffensif – qui est en réalité une capture d'écran avec un lien et pas une véritable pièce jointe – pour en avoir un aperçu, l'utilisateur se retrouve sur une nouvelle page qui l'invite à se reconnecter à son compte Gmail. Apparence, URL (un « data:text » suivi de l'adresse « https://accounts.google.com » rassurante mais qui ouvre en fait un script)… tout semble conforme à un véritable formulaire Google. Mais en tapant son adresse et son mot de passe, la cible vient de succomber au piège.
Une victime décrit ainsi son expérience malheureuse : « Les attaquants se connectent immédiatement à votre compte dès qu'ils en ont le mot de passe, et ils utilisent l'une de vos pièces jointes, combinée à un véritable titre de mail, pour l'envoyer à vos contacts. Ils ont par exemple accédé au compte d'un élève et en ont extrait un calendrier d'entraînement sportif pour en faire une capture d'écran et l'ont ensuite associée à un titre de mail relativement en rapport pour l'envoyer aux autres membres de l'équipe. »

GOOGLE RECOMMANDE LA VALIDATION À DEUX ÉTAPES
Pour éviter de devenir la dernière victime de ce phishing élaboré, la vigilance reste de mise, notamment en vérifiant systématiquement la présence du cadenas sécurisé dans la barre d'adresse. Mais surtout en activant la validation en deux étapes : à chaque connexion à Google, en plus de votre mot de passe, vous devez saisir un code qui vous est communiqué sur votre téléphone.
Aaron Stein, de Google Communications, recommande d'ailleurs cette méthode dans un communiqué qui se veut rassurant : « Nous sommes au courant de ce problème et nous continuons d'améliorer notre défense. Nous contribuons à la protection des utilisateurs contre le phishing de multiples manières, notamment grâce à la détection de [mail frauduleux] par machine learning . »
Gmail permet aussi à ses utilisateurs, en quelques clics, de signaler qu'un contenu reçu dans sa boîte mail relève du phishing.
Fin novembre, des professeurs et des journalistes avaient reçu une alerte de Google contre des tentatives d'intrusion.

Vous souhaitez organiser une campagne de sensibilisation pour vos salariés, agents ou membres , n'hésitez pas à nous solliciter.

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Prudence : un phishing élaboré vise les utilisateurs de Gmail – Tech – Numerama

La moitié des écoles de Bordeaux victimes d’un ransomware

La moitié des écoles de Bordeaux victimes d’un ransomware

Les ransomwares font de nouvelles victimes. Un établissement de santé gérant 5 hôpitaux de l'est de Londres et une quarantaine d'écoles de Bordeaux sont tombés dans leurs filets.
Selon nos confrères de Sud-Ouest, pas loin d'une école bordelaise sur deux a été la victime d'une attaque informatique. Le phénomène a démarré en septembre et s'est accéléré jusqu'aux vacances de Noël, pour toucher au total les serveurs d'environ 40 établissements sur les 101 écoles que compte la préfecture de la Gironde. Un audit est en cours pour tenter de déterminer l'origine de l'infection. L'adjointe au maire en charge de l'éducation, Emmanuelle Cuny, parle d'une attaque « *sans précédent* ».

S'il est encore trop tôt pour se montrer catégorique, l'infection semble provenir d'un ransomware qui s'est diffusé de machine en machine. Comme le note le site spécialisé DataSecurityBreach, l'Académie de Bordeaux dispose d'un contrat avec l'éditeur d'antivirus TrendMicro, pour le produit Internet Security. Reste à savoir si cette protection a été dupée par les cybercriminels ou si – comme c'est plus probable -, elle n'a pas été correctement installée dans les établissements victimes du fléau. Selon Sud-Ouest, les données pédagogiques sont menacées par cette épidémie…[lire la suite]

Denis JACOPINI : Nous allons rentrer en contact avec l'adjointe au maire en charge de l'éducationà la Mairie de Bordeaux pour voir comment nous pouvons leur venir en aide.

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : La moitié des écoles de

Bordeaux victimes d’un ransomware

Le nombre de serveurs MongoDB infectés augmente chaque jour…

L'irruption d'un groupe de cybercriminels spécialisé dans le ransomware a encore dopé le nombre de piratages des bases MongoDB. Une quinzaine d'acteurs malveillants exploitent désormais le filon.

Déjà en nette expansion la semaine dernière, l'infection touchant les bases de données MongoDB laissées librement accessibles sur Internet tourne à l'épidémie. Alors que les deux chercheurs suivant cette attaque, Victor Gevers et Niall Merrigan, recensaient un peu plus de 10 000 serveurs pris en otage vendredi, le total dépasse désormais les 28 300. Cette soudaine inflation est en grande partie due à l'entrée d'une scène d'un groupe de cybercriminels spécialistes des ransomwares, Kraken. Ce dernier, responsable à lui seul de 16 000 infections, serait entré en lice vendredi dernier, après avoir probablement pris conscience de la simplicité d'exploitation de ce nouveau filon. Selon les éléments recensés par Victor Gevers et Niall Merrigan dans un tableau récapitulant les données relatives à la quinzaine de groupes impliqués dans des attaques de ce type, Kraken aurait déjà convaincu 67 organisations de lui verser une rançon de 0,1 Bitcoin (86 euros environ) ou, dans certains cas, de 1 Bitcoin.
Rappelons que l'attaque ne consiste pas à déployer un ransomware, mais exploite la (très discutable) configuration par défaut des bases MongoDB, au sein duquel l'accès n'est pas protégé par une authentification. Lorsque que ces bases sont librement accessibles sur Internet, les pirates se contentent d'exporter le contenu des bases non sécurisées, d'effacer les données du réceptacle originel et d'y déposer un fichier comportant les informations poussant à la victime à payer une rançon (entre 0,1 et 1 Bitcoin) afin de retrouver ses données. Notons que MongoDB a publié un billet de blog expliquant comment paramétrer sa solution pour éviter ce type de mésaventure.

Un défaut connu de longue date

Victor Gevers et Niall Merrigan signalent que certains groupes de cybercriminels se contentent d'effacer les données, sans les télécharger au préalable, rendant toute récupération de l'information illusoire pour les victimes. Selon Victor Gevers, 12 organisations ayant versé une rançon à Kraken n'ont pour l'instant obtenu aucune réponse du groupe de cybercriminels. Les deux chercheurs notent également que certains acteurs malveillants en concurrence sur ce segment n'hésitent pas à remplacer les fichiers de demande de rançon d'autres groupes de hackers. La conséquence ? Les victimes peuvent se retrouver à verser des bitcoins à des individus qui, de toute façon, ne détiennent pas leurs données…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Epidémie pour MongoDB : 28 000 serveurs pris en otage

---

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]

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

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

---

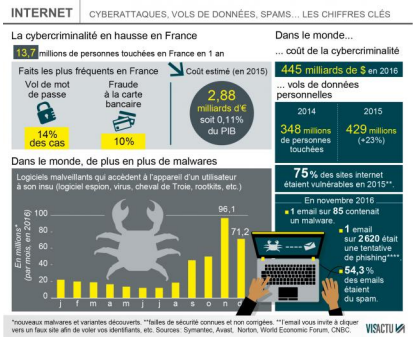
Comment a évolué la cybercriminalité en 2016 par

rapport à 2015 ?

	**Comment a évolué la cybercriminalité en 2016 par rapport à 2015 ?**

Il y a les cyberattaques à l'échelle des états et il y a la cybercriminalité qui peut toucher chaque citoyen. Vols de mots de passe, demandes de rançon, vols de données personnelles… Les chiffres sont en hausse partout dans le monde mais aussi en France.

Les chiffres de la cybercriminalité ont de quoi faire peur. 13,7 millions de personnes ont été confrontées à la cybercriminalité en France en 2016, selon Norton, entreprise spécialisée dans la sécurité en ligne.
Vente de faux papiers d'identité, apologie du terrorisme, vols de mots de passe, de données personnelles, extorsion de fonds ou encore trafic d'armes : le terme cybercriminalité couvre de multiples activités illicites.



Selon Symantec, célèbre pour ses logiciels antivirus, le nombre de cyberattaques dans le monde a diminué ces derniers mois. | Visactu

Vol de mots de passe

En France, les actes les plus fréquents sont les vols de mots de passe (14 % des cas) et la fraude à la carte bancaire (10 % des cas). Mais entre les faits recensés et la réalité, il est très difficile de mesurer l'ampleur exacte du phénomène…
Certaines victimes ne savent tout simplement pas (encore) qu'elles ont été volées, d'autres n'ont pas porté plainte et ont préféré payer une rançon (parfois quelques centaines d'euros) pour récupérer des photos intimes par exemple.
Selon Symantec, célèbre pour ses logiciels antivirus, le nombre de cyberattaques dans le monde a diminué ces derniers mois. Elle en a recensé 291 000 pour le seul mois de novembre 2016 contre 1 461 000 en janvier 2015.

Gare aux malwares

Par contre, le nombre de nouveaux malwares explose. Ces logiciels malveillants qui accèdent à l'appareil d'un utilisateur à son insu (logiciel espion, virus, cheval de Troie, rootkits, etc.) dans le but de dérober des données sont partout.
Symantec dénombrait 20 millions de nouveaux malwares (et variantes) chaque mois début 2016, un chiffre qui a bondi en fin d'année pour atteindre les 96,1 millions en novembre et 71,2 millions de nouveaux malwares détectés en décembre.

Les vols de données de personnelles en hausse

En novembre 2016, Symantec estimait qu'un email sur 85 contenait un malware, qu'un email sur 2 620 était une tentative de phishing (l'email vous invite à cliquer vers un faux site afin de voler vos identifiants, mots de passe, etc.) et que plus de la moitié des emails (54,3 %) étaient non sollicités (spam).
En 2015, elle estimait que 429 millions de personnes dans le monde s'étaient faites voler des données personnelles, un chiffre en hausse de 23 % par rapport à l'année précédente.

Original de l'article : La cybercriminalité en hausse en France et dans le monde

---

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : La cybercriminalité en hausse en France et dans le monde

---

Un logiciel malveillant russe découvert dans un ordinateur

américain

Un logiciel malveillant russe découvert dans un ordinateur américain

Au lendemain de la passe d'armes diplomatique entre les Etats-Unis et la Russie, une entreprise américaine a fait savoir qu'un logiciel malveillant avait été découvert dans un de ses ordinateurs. Les autorités ont été alertées.
Nouvel élément dans la « guerre » que se mènent les Etats-Unis et la Russie ces derniers jours. Un programme malveillant associé à l'opération de piratage informatique russe, surnommée Grizzly Steppe par l'administration Obama, a été détecté dans un ordinateur portable lié à une compagnie d'électricité de l'Etat du Vermont. Celui-ci n'était cependant pas connecté au réseau électrique, a fait savoir l'entreprise Burlington Electric Department (BED).

« Nous avons pris aussitôt des mesures pour isoler l'ordinateur portable et avons alerté les autorités fédérales au sujet de la découverte », a dit l'entreprise BED, compagnie qui distribue l'électricité à Burlington dans le Vermont. « Notre équipe coopère avec les autorités fédérales pour remonter la piste de ce programme malveillant et empêcher toute autre tentative visant à s'introduire dans les ordinateurs du réseau électrique. Nous avons informé les autorités de l'Etat et coopérerons pleinement à l'enquête », a-t-elle ajouté.

Un seul cas connu

Le département américain de la Sécurité intérieure avait informé les compagnies d'électricité, jeudi 29 décembre, de l'existence du programme malveillant utilisé dans Grizzly Steppe. « Nous avons rapidement passé au crible l'ensemble des ordinateurs de notre système. Nous avons détecté le programme malveillant dans un seul ordinateur portable de Burlington Electric Department, non relié à la grille électrique de notre société », a indiqué la BED…[lire la suite]

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cyberattaque : un logiciel malveillant russe découvert dans un ordinateur américain – LCI

Quelles tendances en 2017 pour la sécurité du Cloud ?

Quelles tendances en 2017 pour la sécurité du Cloud ?

Comme chaque année, le grand jeu des prédictions des nouvelles tendances bat son plein. J'ai donc pris le parti de vous proposer quelques réflexions portant sur le marché du Cloud et celui de la sécurité en m'appuyant sur les dernières évolutions que j'ai pu constater.

Les menaces inhérentes à l'IoT obligeront les nations à s'engager dans la lutte internationale contre le piratage

Après les incidents qui ont frappé des infrastructures critiques en France, aux Etats-Unis et en Ukraine cette année, et face aux risques de piratage des machines de vote électroniques, les administrations de nombreux pays ont décidé de prendre le problème du cyberespionnage à bras-le-corps. Si les États-Unis ont réussi, par le biais de négociations diplomatiques à huis clos, à faire baisser le nombre d'attaques informatiques de la Chine à l'encontre des entreprises du secteur privé, le piratage des objets connectés représente un enjeu d'une tout autre ampleur. Sur le plan de la défense, l'Union européenne a adopté des dispositions législatives appelant à un minimum de mesures de cybersécurité pour protéger les infrastructures névralgiques, et les États-Unis devraient lui emboîter le pas en 2017.

Des réglementations strictes influent sur la politique de cybersécurité des entreprises.

Les lois sur la protection de la vie privée des consommateurs sont censées avoir un effet dissuasif et sanctionner les négligences sécuritaires entraînant une violation de données. Or, jusqu'à présent, les organismes de réglementation semblent s'être bornés à de simples réprimandes. Sous l'impulsion de l'Europe et du nouveau règlement général sur la protection des données (GDPR), les autorités chargées de la protection des données redoublent de vigilance et revoient le montant des amendes à la hausse. L'importance des sanctions financières infligées fin 2016 pour violation de la réglementation HIPAA et des directives de l'UE relatives aux données à caractère personnel donnent le ton pour l'année à venir. Nul doute que l'entrée en vigueur du GDPR en 2018 incitera les entreprises internationales à instaurer des contrôles supplémentaires pour la protection de la confidentialité.

Les compromissions de données touchant des fournisseurs de services Cloud sensibilisent les entreprises aux risques de la « toile logistique ». Le Cloud a transformé la chaîne logistique traditionnelle en « toile logistique » où les partenaires commerciaux échangent des données via des passerelles numériques sur Internet. Une entreprise moyenne traite avec 1 555 partenaires commerciaux différents via des services Cloud, et 9,3 % des fichiers hébergés dans le Cloud et partagés avec l'extérieur contiennent des données sensibles. Dans la nouvelle économie du Cloud, les données passent entre les mains d'un nombre d'intervenants plus élevé que jamais. Une violation de données peut ainsi toucher le partenaire externe d'une entreprise dont le département informatique et le service Achats n'ont jamais entendu parler.

Restructuration des directions informatiques avec la promotion des RSSI

Avec l'avènement de la virtualisation, les technologies de l'information occupent une place tellement stratégique au sein de l'entreprise que les DSI endossent désormais le rôle de directeur de l'exploitation et de PDG. En 2017, la sécurité s'imposera en tant que moteur d'activité stratégique, aussi bien au niveau des systèmes internes que des produits. Aujourd'hui, toutes les entreprises utilisent des logiciels, ce qui fait qu'elles ont besoin de l'expertise de fournisseurs de sécurité logicielle. En 2017, la sécurité confirmera son rôle d'atout concurrentiel en aidant les RSSI à réduire les délais de commercialisation des produits, et à assurer la confidentialité des données des clients et des employés.

Microsoft réduira l'écart avec Amazon dans la guerre des offres IaaS

AWS s'est très vite imposé sur le marché de l'IaaS, mais Azure rattrape son retard. 35,8 % des nouvelles applications Cloud publiées au 4e trimestre ont été déployées dans AWS, contre 29,5 % dans Azure. Les fournisseurs spécialisés se sont taillé 14 % de parts de marché, indépendamment de marques telles que Google, Rackspace et Softlayer.

Qui protège les gardiens ? Une entreprise sera victime du premier incident de grande ampleur dans le Cloud lié au piratage d'un compte administrateur

En fin d'année, des chercheurs ont, pour la première fois, découvert la mise en vente de mots de passe d'administrateurs Office 365 globaux sur le Dark Web. Les comptes administrateur représentent un risque particulier dans le sens où ils disposent de privilèges supérieurs en matière de consultation, de modification et de suppression des données. Les entreprises rencontrent en moyenne 3,3 menaces de sécurité liées à des utilisateurs privilégiés tous les mois. Nous devons par conséquent nous attendre à voir un incident de ce type faire la une des journaux en 2017.

Les pirates délaissent les mots de passe au profit de la propriété intellectuelle

Maintenant que les entreprises ont toute confiance dans le Cloud et se servent d'applications SaaS pour les plans de produits, les prévisions de ventes, etc., les cybercriminels disposent de données de plus grande valeur à cibler. 4,4 % des documents exploités dans les applications de partage de fichiers sont de nature confidentielle et concernent des enregistrements financiers, des plans prévisionnels d'activité, du code source, des algorithmes de trading, etc. Si le piratage de bases de données comme celles de Yahoo se distinguent par leur ampleur, les secrets industriels représentent une manne d'informations plus restreinte, mais néanmoins précieuse. Pour répondre aux inquiétudes sur la confidentialité des informations hébergées dans le Cloud, des fournisseurs tels que Box établissent une classification des données permettant d'identifier les ressources qui revêtent le plus de valeur pour les entreprises…[lire la suite]

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Sécurité du Cloud : quelles tendances en 2017 ? – Globb Security FR