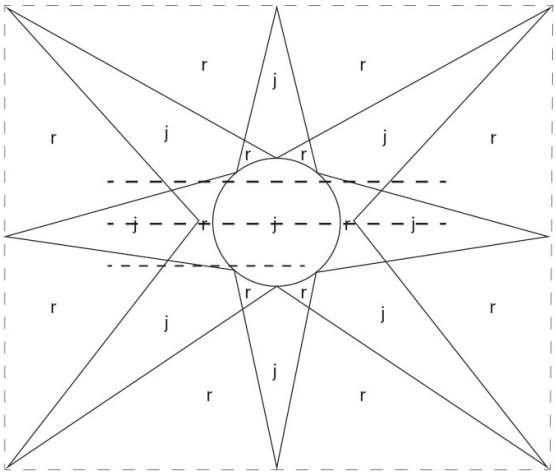
Cyber-harcèlement mortel avec un gif animé



j :
r :
--- : zone texte
v : vitesse j > r > j > r

Cyber-harcèlement mortel avec un gif animé

Un journaliste américain a été victime d'une très violente crise d'épilepsie en regardant une image animée envoyée, à dessein, par un troll. Le responsable, arrêté, risque dix ans de prison.

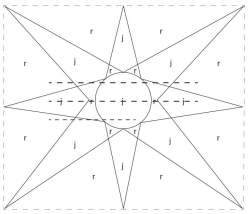
On connaissait le gif comme objet de plaisanterie web, il pourra désormais être aussi considéré comme une arme pouvant tuer. Le tribunal de Dallas s'apprête à juger John Rayne Rivello, utilisateur de Twitter et harceleur présumé du journaliste Kurt Eichenwald. L'arme du – presque – crime : une image animée envoyée à l'attention du reporter, provoquant une crise d'épilepsie qui aurait pu être mortelle.
Comme l'explique le blog Big Browser du *Monde*, le journaliste, collaborateur de *Newsweek* ou *Vanity Fair*, était connu pour ses positions anti-Donald Trump, qu'il relayait également sur Twitter. Il ne cachait pas non plus sa condition épileptique.
Mi-décembre, à la suite d'une discussion animée sur Fox News, où il était interviewé par l'éditorialiste (très) conservateur Tucker Carlson, Eichenwald subit les assauts de plusieurs soutiens à Trump sur son compte Twitter. Une journée malheureusement normale sur les réseaux sociaux, mais qui s'est très mal terminée. L'un des trolls, répondant au nom clairement antisémite de @jew_goldstein, lui envoie un gif stroboscopique, agrémenté du message : *« Tu mérites une crise pour ton message. »*
La femme d'Eichenwald trouvera peu après son mari sur le sol de bureau, le message Twitter clignotant sur son écran, comme le rapporte son avocat au *New York Times*. Après avoir appelé les secours, elle a répondu à l'envoyeur : *« C'est sa femme qui parle. Vous avez causé une attaque. J'ai récupéré vos informations. J'ai appelé la police et leur ai fait part de votre agression. »*
Suivre


Kurt Eichenwald
✔@kurteichenwald
@jew_goldstein This is his wife, you caused a seizure. I have your information and have called the police to report the assault.
05:31 – 16 Dec 2016
•
•
2 6942 694 Retweets
•
4 0594 059 j'aime

La réaction épileptique de Kurt Eichenwald, qui a duré huit minutes selon le *Dallas News*, a été particulièrement violente : incapacité de travailler durant plusieurs jours, perte de la sensation de la main gauche et trouble de l'élocution durant plusieurs semaines. De quoi pousser la police de Dallas et le FBI à mener une enquête sérieuse.

Un iPhone, son Cloud et des preuves

Un mandat de recherche a été émis à l'encontre de @jew_goldstein et a permis de remonter la piste de plusieurs messages privés envoyés par le compte anonyme au sujet de Kurt Eichenwald. Dans ses échanges, l'utilisateur parlait de la condition médicale du journaliste et espérait *« qu'il fasse une crise »* voire *« qu'il meure »*. La police a été capable de relier le compte Twitter à un numéro de téléphone, puis à un modèle de smartphone – un iPhone 6 – qui les a ensuite menés, après avoir cité Apple à comparaître, au Cloud appartenant à un certain John Rayne Rivello.
Dans ses données, les enquêteurs ont trouvé une liste de preuves accablantes : l'image animée qui a provoqué la crise, une capture d'écran du tweet en question et de la réponse de la femme du journaliste, une capture d'écran de la page Wikipédia de Kurt Eichenwald, modifiée avec une fausse date de décès (le jour de l'envoi du tweet), une autre capture d'une liste d'éléments pouvant déclencher une crise d'épilepsie ou encore l'adresse du domicile du journaliste.
Pour l'avocat de Kurt Eichenwald, interrogé par *Newsweek*, l'action de Rivello sur Twitter *« n'est pas différente de celle de quelqu'un qui envoie par courrier une bombe ou des enveloppes remplies d'anthrax »*.
John Rayne Rivello s'apprête à passer devant le tribunal de Dallas avec une accusation tout à fait inédite. Le troll de 29 ans est accusé de cyber-harcèlement avec *« utilisation d'une arme mortelle »*, en l'occurrence l'image animée. Rivello encourt jusqu'à dix ans de prison. Ou quand le gif ne fait plus rire du tout.



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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Cyber-harcèlement : quand le gif animé devient une arme mortelle – L'actu Médias / Net – Télérama.fr*

« iPhone à 1 € !!!! » : l'Europe épingle Facebook, Twitter et Google sur les

publicités mensongères

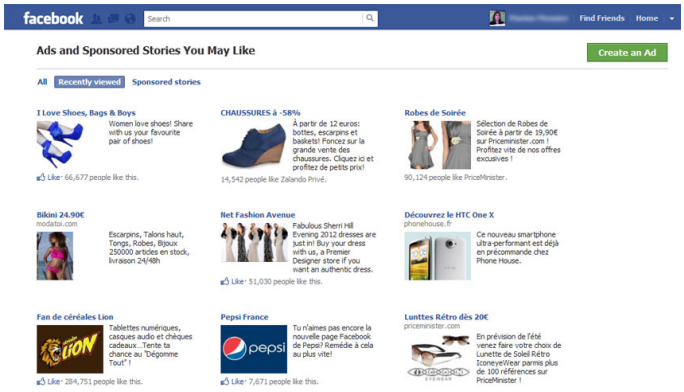
	« iPhone à 1 € !!!! » : l'Europe épingle Facebook, Twitter et Google sur les publicités mensongères

Publicités, confidentialité ou encore respect des droits des consommateurs : Bruxelles a souhaité mettre au clair ses demandes auprès des grands réseaux sociaux. Épinglés par l'Union sur différent dossiers, Facebook, Google et Twitter ont désormais un mois pour appliquer les changements exigés.

Ce vendredi, la Commission européenne a finalement mis en demeure les trois principaux réseaux sociaux (Facebook, Twitter et Google+) qui agacent Bruxelles sur de nombreux dossiers.
Avertie notamment par les régulateurs de concurrence des pays de l'UE, la Commission voulait mettre fin à de nombreuses pratiques publicitaires illégales au sein des frontières européennes. Mais Bruxelles ne s'en est pas tenu à une simple auscultation des publicités des réseaux, l'exécutif européen a également tenu à évaluer minutieusement la gestion des données personnelles et la réactivité des réseaux face aux contenus illégaux.

UN MOIS POUR EN FINIR AVEC LES IPHONE À 1€

Désormais, après avoir rencontré ce jeudi les autorités européennes, les entreprises, Facebook, Twitter et Google, disposent d'un mois pour changer leurs pratiques en adéquations avec les exigences légales. Les autorités auraient proposé aux dirigeants certains aménagements pour s'adapter au cadre juridique européen selon Reuters.
Dans le viseur de la Commission, les procédures juridiques entre consommateur européen et société américaine. Pour Věra Jourová, commissaire européenne chargée de la justice, « *il est inacceptable que les consommateurs de l'Union puissent seulement saisir une juridiction californienne en cas de litige.* »



Mais elle n'a pas épargné la publicité mensongère, les arnaques, et le contenu sponsorisé mal identifié : la Commission a notamment visé les fameuses arnaques qui proposent « ***des iPhone ou iPad à 1 euro mais étant associées à un abonnement de longue durée caché, pour plusieurs centaines d'euros par an*** » explique les autorités bruxelloises qui prennent très au sérieux cette affaire.
Du côté des grandes entreprises américaines, Google assure déjà procéder à un examen approfondi de ces conditions. Facebook et Twitter préfèrent encore garder le silence sur les requêtes de Bruxelles.
En dehors des dossiers publicitaires, qui sont nécessairement sensibles pour les deux sociétés, la question de la modération et de la gestion de contenus calomnieux reste un problème douloureux du côté de Facebook comme du côté de Twitter. Les deux réseaux sont par ailleurs également pressés par l'Allemagne qui exigera prochainement une réactivité forte dans la lutte contre la désinformation et la calomnie sur les plateformes, sous peine sinon de voir la République Fédérale pénaliser Facebook d'une amende pouvant aller jusqu'à 50 millions d'euros.

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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *« iPhone à 1 € !!!! » : l'Europe épingle Facebook, Twitter et Google sur les publicités mensongères – Politique – Numerama*

Wikileaks révèle comment la CIA a piraté des MacBook et iPhone neufs

Wikileaks révèle comment la CIA a piraté des MacBook et iPhone neufs

---

L'organisation fondée par Julian Assange publie un second corpus de documents présentés comme émanant de la CIA qui décrivent les méthodes de l'agence pour pirater des ordinateurs Apple et des iPhone.

Wikileaks remet le couvert. Près de deux semaines après avoir mis en ligne « Vault 7, Year Zero », un ensemble de plusieurs milliers de documents internes détaillant des dizaines de programmes d'espionnage électronique et informatique de la CIA, l'organisation fondée par Julian Assange a publié une deuxième vague d'archives décrivant les techniques utilisées par l'agence du renseignement extérieur américain pour pirater des produits Apple. Baptisé « Dark Matter », ce second volet explique comment la CIA peut pirater un ordinateur Apple, même si son propriétaire y installe un nouveau système d'exploitation, ou un iPhone neuf en pénétrant le réseau d'approvisionnement et de distribution de la marque à la pomme.
• Wikileaks : 5 questions pour comprendre les dernières révélations

Un logiciel indétectable et impossible à effacer

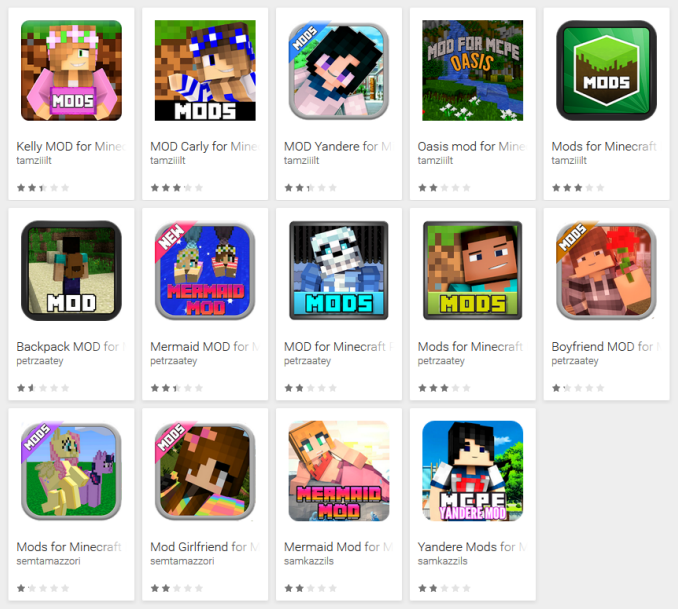
Selon les documents dévoilés par Wikileaks, la CIA a développé un outil en 2012 nommé « Sonic Screwdriver » permettant de passer outre le processus de démarrage d'un MacBook à partir des accessoires périphériques comme une clé USB ou un adaptateur Ethernet branché dans le port Thunderbolt. L'agence pouvait alors **introduire un micro indétectable dans le logiciel profond** (firmware) de l'ordinateur et **bénéficier d'un accès permanent à son contenu** car même une réinstallation du système d'exploitation ou un reformatage de l'appareil ne pouvait suffire à l'effacer. La CIA devait avoir accès physiquement aux appareils visés pour les infecter.
Un autre document montre que la CIA avait conçu cet outil dès 2008 pour l'installer physiquement sur des iPhone neufs. Selon Wikileaks, il est par conséquent « probable que beaucoup d'attaques physiques par la CIA aient infecté la chaîne d'approvisionnement » d'Apple « en bloquant des commandes ou des livraisons ». L'agence américaine « peut faire cadeau à une cible d'un MacBook Air sur lequel a été installé ce micro », indique un document daté de 2009. « L'outil prendra la forme d'un implant/relais opérant dans le (logiciel) profond du MacBook Air et nous permettant d'avoir les moyens de (le) commander et de (le) contrôler », peut-on lire dans ces documents.

Les produits actuels vraisemblablement pas concernés

Apple n'a pas encore réagi à ces révélations. La plupart des documents datant de plus de sept ans et concernent les premières générations d'iPhone. Il apparaît peu probable que les produits actuels du groupe soient vulnérables à ces techniques. La méthode « Sonic Screwdriver » utilisée pour infecter des MacBook rappelle la faille « Thunderstrike » découverte fin 2014, qui permettait de contaminer un Mac lors de l'allumage à l'aide d'un appareil Thunderbolt vérolé, et corrigée par Apple depuis.
Le 9 mars, Wikileaks avait déjà diffusé près de 9.000 fichiers mettant à nu les capacités d'espionnage de la CIA et le recours à des pratiques particulièrement intrusives pour transformer des télévisions et des voitures connectées en mouchards, espionner des iPhone et des smartphones Android ou contourner des antivirus commerciaux. La CIA n'a jamais authentifié les documents mais de nombreux experts les jugent crédibles. Apple avait fait savoir qu'elle avait corrigé les failles évoquées dans ces documents. Wikileaks affirme détenir des informations sur plus de 500 programmes au total et promet de les publier dans les prochaines semaines.
Benjamin Hue, Journaliste RTL

Source : *Wikileaks montre comment la CIA a piraté des MacBook et iPhone neufs*

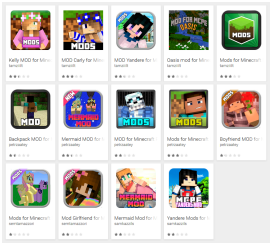
Alerte : Faux mods de Minecraft dans le Google Play

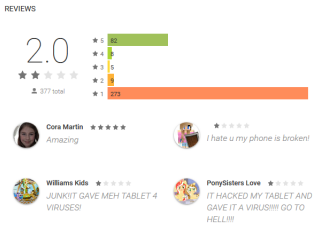


Alerte : Faux mods de Minecraft dans le Google Play

Les chercheurs ESET® découvrent plus de 80 applications malveillantes sur Google Play® déguisées en mods[1] de Minecraft® et ayant généré pas loin d'un million de téléchargements.

Au total, les 87 faux mods ont donné lieu à 990 000 téléchargements avant d'être signalés par ESET les 16 et 21 mars 2017. Les applications répertoriées se divisent en deux catégories : le téléchargement de publicités (Android/TrojanDownloader.Agent.JL) et les fausses applications redirigeant les utilisateurs vers des sites Internet frauduleux (Android/FakeApp.FG).
Pour Android/TrojanDownloader.Agent.JL, ESET signale **14 fausses applications ayant causé 80 000 téléchargements, contre 910 000 installations pour les 73 applications malveillantes** agissant sous Android/FakeApp.FG. Comme elles ne disposent pas de fonctionnalités réelles et qu'elles affichent de nombreuses publicités agressives, les avis négatifs apparaissent clairement sur Google Play.





Si un utilisateur a téléchargé des mods de Minecraft, il se peut qu'il ait rencontré l'une des 87 applications malveillantes. **Il est facile de reconnaître ce type d'escroqueries :** l'application ne fonctionne pas et un message apparaît avoir cliqué sur le bouton de téléchargement. Pour les fausses applications qui téléchargent des publicités, il n'y a pas non plus de fonctionnalités permettant de jouer et l'appareil continue d'afficher des publicités injustifiées. **Toutefois, comme l'application malveillante est capable de télécharger des applications supplémentaires sur des périphériques infectés, la charge utile responsable des annonces peut, par la suite, être remplacée par des malwares plus dangereux.**
Bien que ce qui suit ne soit pas encore entré dans les habitudes des Français, **les chercheurs ESET [NDLR : et Denis JACOPINI] rappellent qu'il est important d'équiper son téléphone portable avec une solution de sécurité efficace** et adaptée aux mobiles. Il n'y a pas que les ordinateurs qui peuvent être infectés par un logiciel malveillant. En 2016, ces derniers ont augmenté de 20% sur Android™. Une solution de sécurité pour mobile permet, au même titre que celle dédiée aux ordinateurs, de détecter et supprimer les menaces.
Si un utilisateur souhaite supprimer les menaces manuellement, il doit désactiver les droits d'administrateur du périphérique pour l'application et le module téléchargés en allant dans Paramètres -> Sécurité -> Administrateur de périphériques. Il suffit ensuite de désinstaller les applications en allant dans Paramètres -> Gestionnaire d'applications.
Si vous souhaitez plus d'informations notamment sur le fonctionnement de ces logiciels malveillants, nous vous invitons à cliquer ici ou à nous contacter pour une demande d'interview. Nous vous proposons également de visualiser cette courte vidéo qui montre **l'installation de l'une de ces fausses applications.**

---

[1] « Jeu vidéo créé à partir d'un autre, ou modification du jeu original, sous la forme d'un greffon qui s'ajoute à l'original, le transformant parfois complètement. » Source : https://fr.wikipedia.org/wiki/Mod_(jeu_vid%C3%A9o)

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 d'expertises, d'audits, de formations et de sensibilisation 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

Risque de cyberattaque

terroriste très élevé

© Dieter Telemans

Risque de cyberattaque terroriste très élevé

Le commissaire chargé de la Sécurité nous explique ce que l'Europe a fait pour améliorer la sécurité de ses citoyens. Il avoue craindre « tous les types de menaces ».

Il est « Le Dernier des Mohicans ». L'ultime commissaire britannique envoyé par Londres avant le Brexit. Dans son bureau du Berlaymont placé sous haute sécurité, trônent deux grandes photographies de Sa Majesté. Sur le sofa, des coussins décorés de l'Union Jack. « No doubt », c'est bien ici une partie de l'île encore arrimée à l'Europe.
Julian King, formé à la fois à Oxford et à l'ENA, est l'un des plus brillants diplomates du Royaume. Sa mission? Créer l'Union européenne de la sécurité ainsi que gérer la lutte contre le terrorisme et le crime.
L'Echo l'a rencontré, un an après les attentats terroristes à Bruxelles.

Comment avez-vous vécu les attaques du 22 mars?
J'étais ambassadeur du Royaume-Uni en France. Je revenais du marché de Rungis. C'était tôt le matin. J'ai mis du temps à me remettre de cette nouvelle. Dès mon retour à la résidence, j'ai demandé qu'ils mettent le drapeau en berne.

Qu'avez-vous ressenti?
Je craignais de nouveaux attentats depuis mon entrée en fonction à Paris. C'est arrivé dans la capitale du pays voisin, là où ma femme vit et travaille. Son bureau n'était pas loin de Maelbeek. J'ai eu peur que mes amis m'appellent pour m'apprendre une mauvaise nouvelle.
Trop de gens qui ont grandi dans nos pays sont partis se radicaliser en Syrie et en Irak. La prévention de la radicalisation est la clé.

Qu'est-ce que les attentats ont changé?
Après chaque attaque, à Paris, Bruxelles et Nice, j'ai été frappé de voir à quel point nos villes sont résilientes. Ces événements sont horribles. Très difficiles à vivre pour les victimes mais aussi pour les gens qui doivent monter en première ligne et tous les habitants de la ville. Je suis touché par la capacité des Belges et des Français à dépasser le drame. À reprendre leur vie. Et le lien profond qu'ils ont avec leur communauté.

Qu'a fait l'Europe, depuis lors, pour améliorer la sécurité de ses citoyens?
Nous avons commencé par renforcer les frontières extérieures. Nous avons créé un corps de garde-frontières et de garde-côtes, déployé du personnel de Frontex et d'Europol pour soutenir les autorités en Grèce et en Italie, adopté une directive sur le contre-terrorisme qui criminalise les allers-retours d'Irak et de Syrie. Nous avons renforcé le code Schengen pour contrôler systématiquement toute personne qui entre dans l'espace Schengen, y compris les citoyens Européens.
Nous avons proposé de créer un système interactif pour contrôler les nationaux des pays tiers, c'est à l'étude au Parlement. Nous allons aussi mettre en place un système de précontrôle des étrangers n'ayant pas besoin de visas, appelé Etias et calqué sur le modèle Esta des Etats-Unis.
Nous avons renforcé notre capacité de connaître ceux qui arrivent dans l'espace européen, et c'est un élément vital pour notre sécurité.

Qu'avez-vous fait pour accroître la sécurité intérieure?
Nous avons renforcé les capacités des forces de l'ordre. Nous avons mis plus d'argent, de personnel et de moyens dans Europol. Nous avons consolidé les bases de données policières et réformé la plus importante: le système Schengen. Nous voulons obliger les polices nationales à partager leurs informations à travers ce système. Dans les faits, ils le font de plus en plus. Mais ce sera encore plus vrai lorsque l'obligation d'échanger sera adoptée par le Conseil européen.
Nous devons aussi accroître la capacité des agents d'aller chercher une information là où elle se trouve.
Pour éviter, comme après les attaques de Paris, qu'un terroriste comme Salah Abdeslam puisse déjouer les contrôles…
Oui. Les renseignements existaient mais lors de ce fameux contrôle entre Paris et Bruxelles, la police n'a pas été capable d'aller les chercher. Nous allons proposer un paquet de mesures pour améliorer la qualité des informations, le traitement de données, l'utilisation plus fréquente de la biométrie et accroître la rapidité d'obtention des informations.
La moitié des business européens ont déjà subi une cyber-attaque.

Quand allez-vous proposer ces mesures?
Mon équipe y travaille, son rapport devrait être prêt d'ici avril. Nous ferons ensuite des propositions.

Les États européens appliqueront-ils ces mesures?
Nous insistons beaucoup là-dessus. Pour la première fois depuis mon arrivée l'été dernier, la Commission a lancé des procédures d'infraction contre plusieurs États qui n'appliquent pas les mesures convenues l'an dernier. Trois procédures contre des États qui n'ont pas appliqué la directive sur les explosifs et cinq procédures contre des États qui n'ont pas appliqué l'arrangement de Prüm sur les échanges d'information.

Que pensez-vous de la création d'un « FBI Européen », comme le préconise Guy Verhofstadt?
Je ne suis pas persuadé que cela arrive dans un futur immédiat. Il y a des questions légales, des difficultés constitutionnelles à lever. Mon objectif, pour le moment, est de construire une coopération pratique entre les agences de renseignements nationales. Certains prétendent qu'il n'existe aucun échange entre elles, mais ce n'est pas vrai. Cette collaboration existe, les agences européennes ont d'ailleurs depuis peu une plateforme commune aux Pays-Bas.

Vous n'aimez pas parler du Brexit. Mais dites-moi, le Royaume-Uni continuera-t-il à coopérer avec l'UE après son départ?
Je l'espère. Je ferai tout durant les deux années à venir pour renforcer notre sécurité commune contre le terrorisme, le cyberterrorisme et le crime organisé. Ces menaces affectent tous les pays d'Europe, qu'ils soient ou pas dans Schengen ou dans l'UE, et c'est le cas en particulier des cyberattaques. Notre combat sera plus efficace si nous le menons ensemble. Ce sera vrai demain, dans deux ans et dans cinq ans. Il est important qu'après le Brexit l'Union européenne et le Royaume-Uni conservent une coopération étroite en matière de lutte contre le terrorisme.

Quant à la coopération entre l'Europe et les Etats-Unis, résistera-t-elle à l'arrivée de Donald Trump?
Jusqu'à présent, tous les représentants des Etats-Unis que j'ai rencontrés ont été clairs. Ils comprennent l'importance de notre coopération et veulent la maintenir.

Quel est le niveau de risque d'attentat terroriste à Bruxelles?
Nous ne sommes pas chargés d'évaluer ce niveau, mais nous écoutons ce que chaque État nous dit. Et il est clair que la menace terroriste dans un État qui a subi une attaque est très très élevée. Il est très important de ne pas donner l'impression que la menace a disparu. Ou que nous avons réduit la menace à zéro.

Les terroristes se concentrent sur les espaces publics, les métros ou les aéroports. Comment sécuriser de tels lieux?
Chaque État a développé de très bonnes pratiques dans la gestion de la sécurité des espaces publics. Nous mettons ensemble tous les experts pour tirer les leçons des meilleures pratiques et nous dressons une liste de lignes directrices. Nous allons continuer ce travail et le faire avec les meilleurs praticiens.

Vous craignez des menaces d'isolés ou des groupes organisés?
Tous les types de menaces. Celles de loups solitaires, et c'est pourquoi la lutte contre la radicalisation est une partie importante de nos travaux. Mais aussi les menaces d'attaques organisées inspirées par Daech, qui ne sont pas réduites parce ce qu'ils sont en difficulté sur le terrain en Syrie et en Irak.

La plupart des auteurs des attaques à Bruxelles et Paris étaient Européens…
Trop de gens qui ont grandi dans nos pays sont partis se radicaliser en Syrie et en Irak. La prévention de la radicalisation est la clé.

Que fait l'Europe pour lutter contre la radicalisation?
Nous agissons à deux niveaux. D'abord nous nous attaquons à la propagande de Daech sur internet, qu'ils continuent à déverser malgré leur déroute sur le terrain. Nous travaillons pour l'instant avec les plus grands groupes du web. Nous avons besoin de leur aide pour trouver des moyens industriels qui arrêtent cette propagande.
L'autre risque majeur ce sont les gens qui, au sein des communautés, cherchent à pousser les plus fragiles à la violence. Le moyen le plus efficace pour les empêcher d'agir est de travailler localement. Nous avons développé, au niveau européen, des moyens pour œuvrer avec ces communautés, soit pas des fonds, soit par la mise en place d'un réseau d'organisations où ils reçoivent du soutien.

Craignez-vous une cyberattaque terroriste, par exemple contre une centrale nucléaire ou une tour de contrôle aérienne?
Les terroristes comme Daech n'utilisent pas, pour l'instant, de tels moyens. Mais le risque d'une cyberattaque terroriste est très élevé. La cybercriminalité augmente de manière exponentielle. Au Royaume-Uni, un pays que je connais bien, la moitié des crimes connus sont des cybercrimes. Si vous regardez l'Europe, la moitié des business européens ont déjà subi une cyberattaque.

Comment affrontez-vous ce risque?
Notre première ligne de défense consiste à avertir le public du danger de manipulation sur internet. Nous devons ensuite construire une résilience, à chaque niveau. Apprendre aux individus à protéger leurs appareils, changer leur code. Il faut aussi mettre en place les moyens nécessaires pour protéger les infrastructures critiques, comme les unités de production d'énergie, exposées aux cyberattaques. Nous travaillons à la création d'une agence européenne qui planifie la protection des infrastructures et mette en place un réseau d'échange d'information, le tout en application de la directive NIS.
Nous travaillons aussi avec le secteur privé, généralement très avancé sur ces questions de sécurité, et lancer des partenariats. Nous allons mobiliser 1,8 milliards d'euros pour des recherches en cybersécurité d'ici 2020. C'est un effort important.
Nous préparons également des exercices conjoints avec l'Otan pour contrer les cyberattaque.
*Enfin, j'espère que nous pourrons faire un examen complet de tout notre travail sur la cybersécurité sous présidence estonienne, avant la fin de cette année…**[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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *« Le risque d'une cyberattaque terroriste est très élevé » | L'Echo*

Les Français plus vulnérables aux virus propagés par clé USB

Les Français plus vulnérables aux virus propagés par clé USB

Les logiciels malveillants s'adaptent et les menaces en matière de cybersécurité varient d'un pays à l'autre, révèle une étude menée par la société de sécurité informatique Avira.

Vols de mots de passe, chevaux de Troie, ver, applications indésirables… En matière de cybersécurité, chaque pays «cultive» son défaut et son logiciel malveillant : tel est le principal enseignement d'une étude publiée lundi par la société de sécurité informatique Avira.
Le talon d'Achille de la France – l'un des cinq pays étudiés avec les Etats-Unis, le Royaume-Uni, l'Allemagne et l'Italie – se trouverait… dans la clé USB. Infestée de «vers».
Avira a en effet remarqué que le logiciel malveillant le plus fréquent en France était un ver, ou *worm* en anglais, de son nom technique Verecno.Gen. Son mode de contamination favori ? L'utilisation de clés USB. Celui-ci «n'est pas sans risque, rappelle la société dans son étude. Le ver Verecno est ainsi capable de se propager automatiquement dès que la clé USB est insérée dans l'appareil. Savez-vous d'où vient la clé USB qui vous est tendue ?» Avira délivre un conseil particulier aux Français : «Ne sur-socialisez pas».

A chaque pays son point faible

Les utilisateurs des Etats-Unis sont davantage vulnérables aux chevaux de Troie modifiant le comportement des systèmes d'exploitation Windows de leurs ordinateurs, les Allemands aux kits d'exploitation prospérant sur les défauts de mise à jour, les Italiens aux vols de mots de passe via les emails et les Britanniques au téléchargement d'applications indésirables.

leparisien.fr

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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Cybersécurité : les Français plus vulnérables aux virus propagés par clé USB – Le Parisien*

Le ministère de la Défense confirme l'augmentation des tentatives de piratage informatique

Le ministère de la Défense confirme l'augmentation des tentatives de piratage informatique

---

L'armée sud-coréenne a récemment été la cible de tentatives accrues de piratage informatique sur fond de relations tendues avec la Chine et de comportement belliqueux de la Corée du Nord, a fait savoir ce mardi le porte-parole du ministère de la Défense Moon Sang-gyun.
«Récemment, les tentatives d'intrusion dans (notre) système informatique se sont quelque peu accrues», a déclaré le porte-parole lors d'un point de presse, tout en notant qu'il n'y a eu aucun dégât subi. Il n'a toutefois pas précisé l'origine des cybermenaces évoquées.
Plus tôt dans la journée, un quotidien sud-coréen a rapporté que le nombre de cyberattaques contre l'armée sud-coréenne a fortement augmenté depuis que celle-ci a acquis le mois dernier un terrain de golf du groupe Lotte, dans le sud-est du pays, pour le déploiement du système de défense antimissile à haute altitude THAAD (Terminal High Altitude Area Defense) des Etats-Unis. La Chine est fortement opposée au plan des deux pays alliés de renforcer leur capacité à intercepter les missiles nord-coréens.
Le nombre de tentatives de piratage informatique contre le réseau informatique de l'armée a été de 44 entre les 9 et 15 mars, selon le rapport. Moon n'a pas confirmé ce chiffre.
Il a écarté les inquiétudes sur l'éventuelle vulnérabilité de l'intranet de l'armée, en soulignant qu'il est complètement «séparé» du serveur Internet.
L'intranet de l'armée a subi pour la première fois une cyberattaque en septembre dernier dont le Nord serait également à l'origine.
lsr@yna.co.kr

Réagissez à cet article

Source : *Le ministère de la Défense confirme l'augmentation*

des tentatives de piratage informatique | Agence de presse Yonhap

---

Data Protection Officer : Qui seras-tu ?

Data Protection Officer : Qui seras-tu ?

Dès la mi-2018, la nouvelle directive européenne baptisée GDPR est appelée à remplacer les dispositions de la Loi Informatique et Libertés. Celle-ci va rendre obligatoire la nomination d'un DPO (Data Protection Officer) dans de nombreuses organisations pour lesquelles la protection des données représente un enjeu majeur. Selon l'étude « CIO Concern Management » de Janco Associates, la sécurité arrive en tête des préoccupations des DSI à hauteur de 68%. De la même manière, les fuites de données observées chez des majors du Web et largement relayées dans les médias ont participé à construire ce climat anxiogène.

Pour être efficace, un DPO doit considérer les deux fonctions principales de sa mission que sont la protection des données personnelles et la protection de la confidentialité des données.
La protection des données personnelles fait appel à des exigences en termes de moyens et processus à mettre en œuvre qui peuvent être très variables d'un pays à l'autre. Dans un contexte de développement à l'international, le DPO sera un soutien précieux afin d'appréhender les différents aspects réglementaires.
La protection de la confidentialité des données est quant à elle un peu plus poussée puisqu'il s'agit de garantir que chaque donnée soit protégée à hauteur de ses enjeux pour l'entreprise. Autrement dit, ce n'est plus la loi mais le client qui fixe les règles !
Toutes les données informatiques n'ont pas la même valeur. Une plaquette commerciale où le plan détaillé d'un prototype en cours de conception n'auront pas le même effet s'ils se retrouvent révélés. Le DPO doit donc, avec son client, mesurer le risque de divulgation de chaque donnée et son impact pour l'entreprise. De données « publiques » à « très secrètes », il doit être capable de garantir au client que ses exigences soient remplies en termes de sécurité… et même si l'on met en place assez facilement des méthodes de chiffrements sur les disques, cela ne résout pas tout !
La plus grande faille sécuritaire qu'il puisse exister réside finalement dans l'humain lui-même. Pour être totalement rassuré quant à la confidentialité de ses données, le client doit être certain que même les équipes système de son prestataire ne puisse pas les lire…[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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Data Protection Officer : Qui seras-tu ? – Global Security Mag Online*

Les Banques organisent la riposte au cybercrime sur smartphone

	Les Banques organisent la riposte au cybercrime sur smartphone

---

Les banques songent à intégrer des logiciels dans leurs applications pour sécuriser les smartphones de leurs clients.

La pédagogie est la clef pour décourager les clients qui seraient tentés de télécharger des applications sur des « Stores Android » non officiels, de s'aventurer à débloquer leur smartphone ou encore de se connecter sur leur application bancaire depuis le réseau wi-fi d'un café, non sécurisé. *« La carte bancaire a beau être sécurisée, si le client divulgue son code, nos efforts de sécurisation sont vains. Il en va de même pour les usages sur le mobile , il y a des principes élémentaires de sécurité à respecter »,* souligne Marc Zanoni, directeur sécurité des systèmes d'information du groupe BPCE.

Convaincre les clients

Comme pour la banque en ligne, les établissements veulent donc convaincre leurs clients de la nécessité de sécuriser leur smartphone. Certains les encouragent à télécharger des antivirus qui détectent les logiciels malveillants présents dans le téléphone et d'autres, comme Société Générale, promeuvent l'enregistrement du téléphone de leurs clients pour que la banque puisse vérifier, à chaque transaction, qu'il s'agit bien d'une demande officielle et non d'un pirate qui aurait capté des codes d'accès.
Ces outils restent optionnels car *« toute la difficulté est de garantir la sécurité sans dégrader l'expérience client. Nous ne voulons pas imposer de nouvelles pratiques brutalement »,* explique un autre responsable Sécurité d'une grande banque française. Ce qui veut dire que *« les banques vont devoir agir à la place de leurs clients car ils n'auront pas la maturité nécessaire sur ces questions »,* estime Clément Saad, fondateur de Pradeo, une jeune pousse spécialisée dans la cybersécurité…[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 d'expertises, d'audits, de formations et de sensibilisation 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

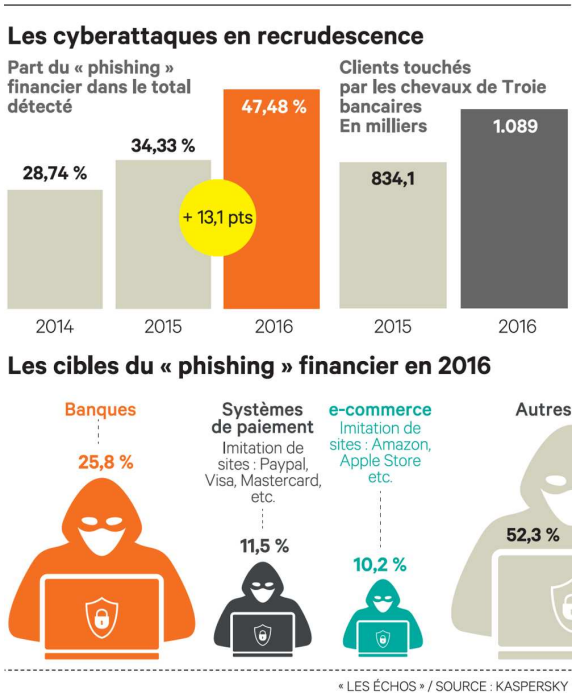
Source : *La riposte au cybercrime sur smartphone s'organise, Banque – Assurances*

Les pirates informatiques menacent les clients des banques

	Les pirates informatiques menacent les clients des banques

---

Les opérations de « phishing » ciblant les clients des banques augmentent. La montée en puissance de la banque mobile ouvre un nouveau terrain de jeu pour les cybercriminels.



En 2016, les cyberpirates ont marqué les esprits en parvenant, à plusieurs reprises, à déjouer les systèmes de sécurité des banques membres du réseau interbancaire SWIFT. Ces vastes opérations aux perspectives de gains étourdissantes n'ont pour autant pas remplacé les cyberattaques traditionnelles qui visent directement les clients des banques.

« Les plus petits groupes de cybercriminels ciblent toujours plus massivement les clients particuliers, petites ou moyennes entreprises avec des logiciels malveillants disponibles sur la Toile : après deux ans de baisse du nombre de clients attaqués, nous avons détecté une hausse significative du nombre de victimes parmi nos clients en 2016 », explique le spécialiste de la sécurité informatique Kaspersky dans son rapport annuel sur les services financiers.

Le « hameçonnage » progresse

Dans le détail, les opérations de « phishing » , c'est-à-dire l'envoi de courriels frauduleux à des clients pour obtenir leurs données de carte bancaire ou d'accès à leur compte en ligne, continuent de se développer. En 2016, la part des « phishings » financiers dans le total des e-mails frauduleux détectés par Kaspersky a progressé de plus de 13%. Les banques restent les principales victimes de ces méthodes qui dirigent les clients peu vigilants vers des sites mimant ceux des établissements.

En 2016, les banques ont été visées par près de 26% des e-mails financiers frauduleux, contre 10% à 11% pour les systèmes de paiements alternatifs et les e-commerçants. Chez Société Générale, l'équipe chargée de fermer les faux sites du groupe qui voient le jour sur la Toile en recense ainsi « *des centaines chaque mois et les chiffres augmentent* », indique un proche du groupe.

Chevaux de Troie

Autre menace qui se renforce pour les consommateurs : les chevaux de Troie bancaires qui se glissent dans les systèmes d'exploitation des clients et captent les données qui ouvrent l'accès aux espaces bancaires en ligne. En 2016, Kaspersky observe une hausse de 30,5 % de ces attaques dans le monde. « *Plus d'un million de clients ont été touchés, un chiffre qui croît avec le développement de la banque en ligne et de la banque mobile* », explique David Emm, Principal Security Researcher chez Kaspersky Lab…[lire la suite]

Sharon Wajsbrot, Les Echos

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 d'expertises, d'audits, de formations et de sensibilisation 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

Source : *Cybersécurité : menace accrue pour les clients des banques, Banque – Assurances*