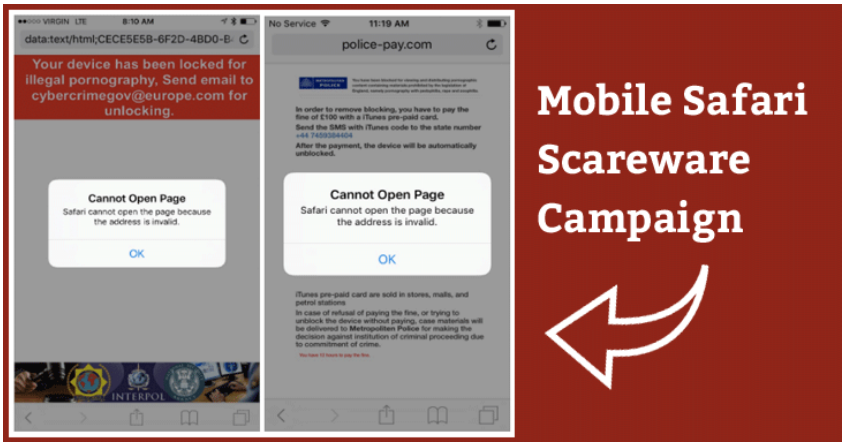
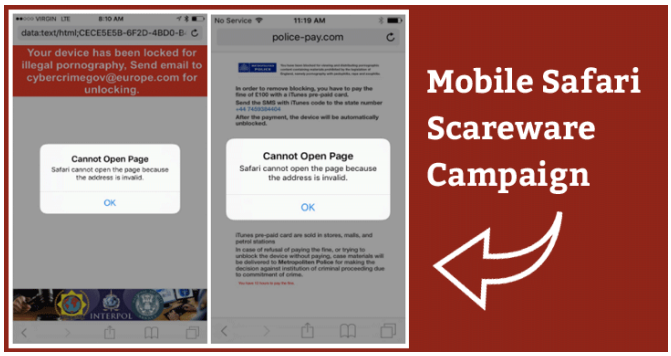
Apple iOS 10.3 Fixes Safari Flaw Used in JavaScript-based Ransomware Campaign



Apple iOS 10.3 Fixes Safari Flaw Used in JavaScript-based Ransomware Campaign

If you own an iPhone or iPad, it's possible you could see popup windows in a sort of endless cycle on your Safari browser, revealing your browser has been locked and asking you to pay a fee to unlock it. Just do not pay any ransom.



A new ransomware campaign has been found exploiting a flaw in Apple's iOS Safari browser in order to extort money from users who view pornography content on their phones or attempt to illegally download pirated music or other sensitive content.

However, the good news is that Apple patched the web browser vulnerability on Monday with the release of iOS version 10.3.

The vulnerability resides in the way Safari displayed JavaScript pop-up windows, which allowed ransomware scammers to display an endless loop of pop-up windows, preventing victims to use the browser, researchers from mobile security provider Lookout said in a blog post published on Monday.

The victims eventually would end up on an attacker website that masquerades itself as a legitimate law enforcement site informing victims that they have to pay a fine for viewing illegal content in order to regain access to their browser.

Lookout researchers called the exploit « scareware, » as the attack doesn't actually encrypt any data and hold it ransom. Rather the attack just scares victims into paying the ransom fee to unlock the browser.

« The scammers abused the handling of pop-up dialogs in Mobile Safari in such a way that it would lock out a victim from using the browser, » Lookout explains.

« The attack would block the use of the Safari browser on iOS until the victim pays the attacker money in the form of an iTunes Gift Card. During the lockout, the attackers displayed threatening messaging in an attempt to scare and coerce victims into paying. »

The scammers effectively used fear as a factor to get victims pay the fee before they realized that there was no real risk to their data and it's very easy to overcome this issue.

While overcoming the threat for users is as simple as clearing their browsing history and cache, iOS 10.3 users are no longer at risk of getting trapped in the endless cycle of JavaScript popups.

Lookout researchers shared the cause of this iOS exploit with Apple last month, and the company has promptly patched the issue with the release of iOS 10.3. Now, pop-up windows only take over a tab, instead of the entire app.

Those iOS 10.2 users who are already hit by this ransomware campaign can clear their browsing cache by navigating to Settings → Safari → Clear History and Website Data.

Swati Khandelwal

***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 : *Apple iOS 10.3 Fixes Safari Flaw Used in JavaScript-based Ransomware Campaign*

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*

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 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

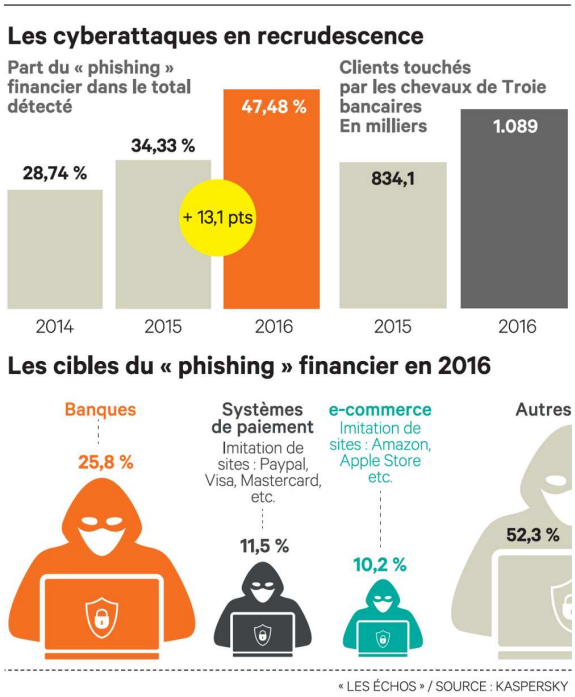
Source : *La riposte au cybercrime sur smartphone s'organise, Banque – Assurances*

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*

Formations en cybersécurité en France

À titre indicatif, voici la liste des formations en cybersécurité délivrant un titre reconnu par l'État (ministère en charge de l'enseignement supérieur ou CNCP) de niveau équivalent à Bac+3 (licence professionnelle) jusqu'à Bac+5 (master, ingénieur).

Cette liste de formations a vocation à informer les étudiants sur l'ensemble des programmes accessibles. Ne figurent dans cette liste ni la formation continue, ni les titres non reconnus officiellement par l'État (DU, masters spécialisés, BADGE, etc.).
Les éléments fournis ci-dessous sont issus d'une récolte de données multiples et éparses dans l'ensemble des établissements d'enseignement supérieur en France. Cette liste n'est plus maintenue et sera supprimée en juillet 2027.

En savoir plus sur SecNumedu, le label de formations initiales en cybersécurité de l'enseignement supérieur

FORMATIONS RECENSÉES DE NIVEAU LICENCE

NOM ETABLISSEMENT	NOM FORMATION	SITE INTERNET
Cnam Bretagne	Licence Pro « Analyste en Sécurité des Systèmes Télécoms Réseaux et Informatiques » ASSTRI	http://cnamsecuritedefense.fr/formation-securite-telecoms-reseaux/
Université d'Aix-Marseille	Licence Pro « Administration et sécurité des réseaux d'entreprises »	http://iut.univ-amu.fr/diplomes/licence-professionnelle-reseaux-telecommunications-specialite-administration-securite
Université d'Artois	Licence Pro « Systèmes informatiques et logiciel – Sécurité informatique »	http://formations.univ-artois.fr/cdm33rc2/ws7_cmd=getFormation&_oid=FR_RNE_0623957F_FR_L3LSEIN291&_redirect=voir_fiche_programS_lang=fr-FR&_onglet=Description
Université de Clermont-Ferrrand 1	Licence Pro « Administration et Sécurité des Réseaux »	http://iutweb.u-clermont1.fr/xfTest?xml/formation?idFormation=16824
Université de Grenoble Joseph Fourier	Licence Pro « Réseaux Sans Fil et Sécurité »	https://iut1.ujf-grenoble.fr/formation-et-metier/licence-professionnelle/reseaux-et-telecommunications
Université de Grenoble Pierre Mendès France	Licence Pro « Administration et Sécurité des réseaux »	http://www.iut-valence.fr/licence-professionnelle-asur
Université de Haute-Alsace	Licence Pro « Administration et Sécurité des réseaux »	http://www.iutcolmar.uha.fr/fr/LP-RT-ASUR-260.html
Université de la Réunion	Licence Pro « Réseaux Sans Fil et Sécurité »	http://www.iut-lareunion.fr/licences/reseaux-a-telecommunications
Université de la Rochelle	Licence Pro « Administration et sécurité des réseaux »	http://www.iut-larochelle.fr/licences-professionnelles/lp-administration-et-securite-des-reseaux
Université de Valenciennes et du Hainaut Cambrésis	Licence Pro « Collaborateur de Défense et Anti Intrusion des Systèmes Informatiques (CDAISI) »	http://formations.univ-valenciennes.fr/cdm/program/FR_RNE_0593279U_FR_SOF-5899
Université de Montpellier 2	Licence Pro « Administration et sécurité des réseaux »	http://www.iutbeziers.univ-montp2.fr/licence-pro-reseaux-et-telecoms.html
Université de Lorraine	Licence Pro « Réseaux Sans Fil et Sécurité »	http://iutnb.univ-lorraine.fr/index.php?op=lbaccplus3/lp_rt_reseaux.htm
Université de Nantes	Licence Pro « Administration et sécurité des réseaux »	http://www.iutlaroche.univ-nantes.fr/70407600/0/fiche___formation/&RH=IUTRY_FR1
Université Paris Est Créteil Val de Marne	Licence Pro « Réseaux informatiques, mobilité, sécurité (R3MS) »	http://www.u-pec.fr/pratiques/universite/formation/licence-professionnelle-reseaux-informatiques-mobilite-securite-rims-641083.kjsp
Université Paris 13	Licence Pro « Administration et Sécurité en Réseaux »	http://www.iutv.univ-paris13.fr/formations/licences-pro/reseaux-et-telecommunications.html
Université de Paris Sud	Licence Pro « Sécurité des Réseaux et Systèmes informatiques »	http://www.iut-orsay.u-psud.fr/fr/formations/licences_professionnelles/info_lp_srsi.html
Université de Rennes 1	Licence Pro « Administration et Sécurité des Réseaux »	http://sfc.univ-rennes1.fr/informatique/lp_administration-securite-reseaux.html#.U-R2OVRX6lB
Université de Rouen	Licence Pro « Administration Sécurité des Réseaux »	http://iutrouen.univ-rouen.fr/licence-professionnelle-administration-et-securite-des-reseaux-279942.kjsp
Université de Toulouse 2	Licence Pro « Réseaux Sans Fil et Sécurité »	http://www.univ-tlse2.fr/accueil/formation-insertion/decouvrir-nos-formations/licence-professionnelle-reseaux-sans-fil-et-securite-885.kjsp
Université de Tours	Licence Pro « Qualité – Sécurité des Systèmes d'Information »	http://iut-blois.univ-tours.fr/formations/qualite-securite-des-systemes-d-information-92850.kjsp
Université de Versailles Saint-Quentin	Licence Pro « Administration et Sécurité des Réseaux »	http://www.uvsq.fr/licence-professionnelle-metiers-des-reseaux-informatiques-et-telecommunications-parcours-administration-et-securite-des-reseaux-341092.kjsp?RH=1271771445917
Université de Pau et des Pays de l'Adour	Licence Pro « Administration et Sécurité des Réseaux »	http://iutpa.univ-pau.fr/live/RT/LP/LP+ASUR
Université de Bordeaux 1	Licence Pro « Administration et Sécurité des Réseaux »	http://www.univ-bordeaux.fr/formations/programme.jsp?f=0&t=3000&p=2213
Université des Antilles et de la Guyane	Licence Pro « Administration et Sécurité des Réseaux »	http://sut.univ-ag.fr/formations/licences-professionnelles/lp-asur/

FORMATIONS RECENSÉES DE NIVEAU MASTER

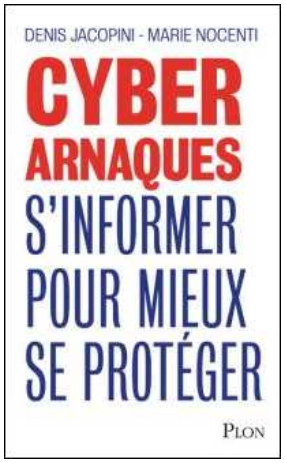
NOM ETABLISSEMENT	NOM FORMATION	SITE INTERNET
Université de Basse Normandie	Master « Réseaux et sécurité des systèmes informatiques »	http://www.unicaen.fr/formations/formations-proposees/master-pro-rech-informatique-specialite-reseaux-et-securite-des-systemes-informatiques-388756.kjsp
Université de Bordeaux 1	Master « Cryptologie et sécurité informatique »	http://www.math.u-bordeaux1.fr/~gzemor/dossier_CSI/
Université de Bretagne Sud (ENSIBS)	Ingénieur « Management et Ingénierie de sécurité des systèmes – cyberdéfense »	http://www-ensibs.univ-ubs.fr/devenir-ingenieur-en-cyberdefense-debouches-356662.kjsp?RH=1351525595668&RF=1351525595668
Université Grenoble Alpes et Grenoble-INP/Ensimag	Master « Cryptologie, sécurité et codage de l'information »	http://www-fourier.ujf-grenoble.fr/enseignement/spip.php?rubrique19
Université Grenoble Alpes	Master « Sécurité, audit, informatique légale – SAFE »	http://www.ujf-grenoble.fr/formation/diplomes/masters/domaine-sciences-technologies-sante/master-mention-mathematiques-informatique-specialite-securite-audit-informatique-legale-safe-p-838102.htm
Université Grenoble Alpes et Grenoble-INP/Ensimag	Master « Cybersecurité »	http://cybersecurity.imag.fr/
Université de Limoges	Master « Sécurité de l'Information et Cryptologie – CRYPTIS »	http://www.cryptis.fr/
Université de Lorraine (Mines Nancy, Telecom Nancy, ENSEM)	Master « Security of Computer Systems »	http://www.mines-nancy.univ-lorraine.fr/content/master-science-msc-security-computer-systems
Université de Lorraine	Master « Services, sécurité des systèmes et des réseaux »	http://msm.univ-lorraine.fr/content/master-informatique-ssr
Université de Lorraine	Master « Sécurité des systèmes d'information et de communication – SSIC »	https://formations.univ-lorraine.fr/fr-FR/fiche/presentation/UL-PROG2654/UL-PROG3211
Université de Lyon 1	Master SAFIR, parcours « Sécurité des systèmes informatiques en finance et en assurance – S2IFA »	http://isfa.univ-lyon1.fr/parcours_S2IFA
Université de Lyon 2	Master « Organisation et protection des systèmes et des réseaux – OPSIE »	http://www.univ-lyon2.fr/master-informatique-specialite-informatique-decisionnelle-et-statistique-opsie-264018.kjsp
Université de Nice Sophia Antipolis	Ingénieur « CryptograAphie, Sécurité, et vie Privée dans les Applications et Réseaux »	http://www.polytechnice.fr/informatique/page251.html
Université de Paris 8, en partenariat avec Paris Diderot (Paris 7)	Master « Mathématiques fondamentales et protection de l'information »	https://www.univ-paris8.fr/Master-Mathematiques-pour-la-protection-de-l-information
Université de Paris-Diderot (Paris 7) — en partenariat avec Paris 8	Master « Mathématiques, Informatique et applications à la Cryptologie – MIC »	http://www.math.univ-paris-diderot.fr/formations/masters/mic/index
Université de Paris-Est Créteil (Paris 12)	Master « Sécurité des systèmes informatiques »	http://www.lacl.fr/ens/master.html
Université de Poitiers	Master « Management des risques informationnels et industriels »	http://irisaf.univ-poitiers.fr/formation/master-management-des-risques-des-systemes-d-information/master-professionnel-et-recherche-sciences-technologies-sante-mention-gestion-des-risques-specialite-management-des-risques-des-systemes-d-information-11079.kjsp
Université de Reims Champagne-Ardenne	Master spécialité informatique, parcours « Administration et sécurité des réseaux »	http://www.master-informatique.net
Université de Rennes 1	Master « Sécurité des Systèmes d'Information – ISTIC »	http://etudes.univ-rennes1.fr/masterInformatique/themes/SecondeAnnee/Specialites/SSI
Université de Rennes 1, Université de Bretagne Sud, Université de Bretagne Occidentale, ENS Rennes, ENIB, ENSTA Bretagne, INSA Rennes, CentraleSupélec, Télécom Bretagne	Master « Sécurité des contenus et des infrastructures informatiques »	http://master.irisa.fr/index.php/fr/parcoursprog-fr/parcours-rennes-3-fr
Université de Rouen	Master « Sécurité des Systèmes Informatiques (SSI) »	https://dpt-info-sciences.univ-rouen.fr/index.php/accueil-mssi
Université de Valenciennes	Master « Informatique, réseaux et sécurité – IRS »	http://formations.univ-valenciennes.fr/cdm/program/FR_RNE_0593279U_FR_SOF-7415
Université de Versailles-Saint-Quentin	Master « Sécurité des contenus, des réseaux, des télécommunications et des systèmes – SeCReTS »	http://www.master-secrets.uvsq.fr/
Université d'Orléans	Master « Informatique Nomade, intelligence et sécurité »	http://formation.univ-orleans.fr/fr/formation/offre-de-formation/master-lmd-XR/sciences-technologies-sante-STS/master-informatique-specialite-informatique-nomade-intelligence-et-securite-finalite-professionnelle-et-recherche-program-sciesf2-502-2.html
Université du Havre	Master « Systèmes informatiques, Réseaux et Sécurité – MATIS »	http://matis.univ-lehavre.fr/
Université Pierre et Marie Curie (Paris 6) — avec l'AFTI	Master « Informatique, spécialité SFPN, filière sécurité informatique — MSI »	http://www-master.ufr-info-p6.jussieu.fr/lmd/specialite/sfpn/
Université Technologique de Troyes	Master « Sécurité des systèmes d'information »	http://www.utt.fr/fr/formation/master-en-sciences—technologies—sante/specialite-ssi.html
Université de Valenciennes et du Hainaut-Cambrésis	Master « Cyber-défense et sécurité de l'information – CDSI »	http://formations.univ-valenciennes.fr/cdm/program/FR_RNE_0593279U_FR_SOF-15674
ENSICAEN	Ingénieur « Monétique et sécurité des systèmes »	https://www.ensicaen.fr/formations/masteres-specialises-cpa/masteres-monetique-et-transactions-securisees/
EPITA	Ingénieur « Systèmes, réseaux et sécurité – SRS »	http://srs.epita.fr/
EPSI	Programme Ingénierie informatique – option Sécurité Informatique	http://www.epsi.fr/Programmes/Programme-Ingenierie/Ingenierie-5eme-annee
ESAIP	Ingénieur « Informatique et réseaux, spécialité cybersécurité »	http://www.esaip.org/formations/ingenieur-informatique
ESGI	Mastère « Sécurité informatique »	http://www.esgi.fr/master-informatique/master-securite-informatique.html
ESIEA	Ingénieur parcours « Fondamentals of Security (SEC) »	http://www.esiea.fr/formation-ingenieurs/majeures-ecole-ingenieurs/
ESIGELEC	Ingénieur « Architecture et sécurité des réseaux – ASR »	http://www.esigelec.fr/fr/dominantes
ETNA-Alternance	Ingénieur « Architecte système réseaux et sécurité »	http://www.etna-alternance.net/formation-2e-annee.aspx
EURECOM	Ingénieur de spécialisation en « sécurité des systèmes informatiques et des communications »	http://www.eurecom.fr/fr/les-formations/ingenieur-de-specialisation/securite-des-systemes-informatiques-et-des-communications
IIA Laval	Manager en ingénierie informatique (M2I) option « Management de la sécurité des systèmes d'information (MSSI) »	http://iia-laval.fr/ecole-superieure-en-informatique/l3m1m2-diplome-m2i/bac5-diplome-m2i/
INSA Centre Val de Loire	Ingénieur « Sécurité et technologies informatiques »	http://www.insa-centrevaldeloire.fr/formation/securite-et-technologies-informatique
IONIS-STM	Master « Ingénierie informatique & Management : Sécurité informatique »	http://ionis-stm.com/master-securite-informatique.aspx
ISIMA-Université Blaise Pascal	Ingénieur « Réseaux et Sécurité Informatique »	http://www.isima.fr/f5-reseaux-et-securite/
Supélec (Rennes)	Ingénieur « Systèmes d'information sécurisés »	http://www.rennes.supelec.fr/ren/fi/sis/
Télécom Lille	Ingénieur « Sécurité des réseaux et des systèmes »	http://www.telecom-lille.fr/specialisations-sciences-et-technologies
Télécom SudParis	Ingénieur « Sécurité des systèmes et des réseaux »	http://www.telecom-sudparis.eu/p_fr_formations-post-grade_MS_1178.html?idm=65
Toulouse Ingénierie	Ingénieur « TLS-SEC »	http://tls-sec.github.io/tls-sec/

À voir aussi

- Formations labellisées SecNumedu
- Profils métiers de la cybersécurité
(Lien ne mène)

[block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : *Formation et cybersécurité en France | Agence nationale de la sécurité des systèmes d'information*

Le cyber-espionnage, en tête

des menaces en 2017 ?

	**Le cyber-espionnage, en tête des menaces en 2017 ?**

Selon Trend Micro, l'augmentation des ransomware et des attaques menées par des Etats constituent un risque croissant pour les infrastructures critiques.

La dernière étude menée par Trend Micro, soutient que 20 % des entreprises mondiales classent le cyber-espionnage comme la plus forte menace pour leur activité, 26 % luttant pour suivre et anticiper l'évolution rapide des différentes menaces. Aux Etats-Unis, 20 % ont déjà subi une attaque de ce type en 2016.
L'étude révèle que le cyber-espionnage arrive en tête des préoccupations de sécurité pour 2017, suivi par les attaques ciblées (17 %) et le phishing (16 %). Les entreprises situées en Italie (36 %), en France (24 %), en Allemagne (20 %) et aux Pays-Bas (17 %) sont celles qui craignent le plus le cyber-espionnage, ce qui s'explique notamment par la tenue d'élections dans chacun de ces pays cette année.
Huit pays sur dix ont mentionné le caractère de plus en plus imprévisible des cybercriminels (36 %) comme étant le plus grand frein à la protection contre les cyber-menaces. Ils sont également 29 % à faire état de lacunes concernant la compréhension des dernières menaces, et 26 % à s'efforcer de suivre l'évolution rapide des menaces et la sophistication croissante des activités cybercriminelles.
Selon l'étude, près des deux tiers (64 %) des entreprises avaient subi une cyber-attaque majeure « connue » au cours des 12 derniers mois. En moyenne, elles en avaient même connu quatre. Les menaces de type ransomware étaient de loin les plus courantes, 69 % des personnes interrogées indiquant avoir été attaquées au moins une fois au cours de la période. En réalité, seul un quart (27 %) des entreprises interrogées n'avait pas été ciblé par un ransomware.

Autre fait notable : à peine 10 % des entreprises pensent que les attaques de type ransomware constitueront une menace en 2017, alors que l'année 2016 a été marquée par une augmentation de 748 % de ces attaques, avec 1 milliard de dollars de pertes pour les entreprises à travers le monde. On estime que le nombre de ransomware va augmenter d'encore 25 % en 2017, s'attaquant à divers appareils tels que les téléphones portables, les objets connectés (IoT) et les dispositifs d'IoT industriel (IIoT)…[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 : *Le cyber-espionnage, en tête des menaces en 2017* |

Alerte : Nouvelle vulnérabilité dans les navigateurs Microsoft

Alerte : Nouvelle vulnérabilité dans les navigateurs Microsoft

Une vulnérabilité a été découverte dans les navigateurs Microsoft. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

1 – Risque(s)

• exécution de code arbitraire à distance

2 – Systèmes affectés

• Internet Explorer 11 pour Windows 7
• Internet Explorer 11 pour Windows 8.1
• Internet Explorer 11 pour Windows 10
• Internet Explorer 11 pour Windows Server 2012 et 2016
• Microsoft Edge pour Windows 10

3 – Résumé

Une vulnérabilité a été découverte dans les navigateurs Microsoft. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.

4 – Contournement provisoire

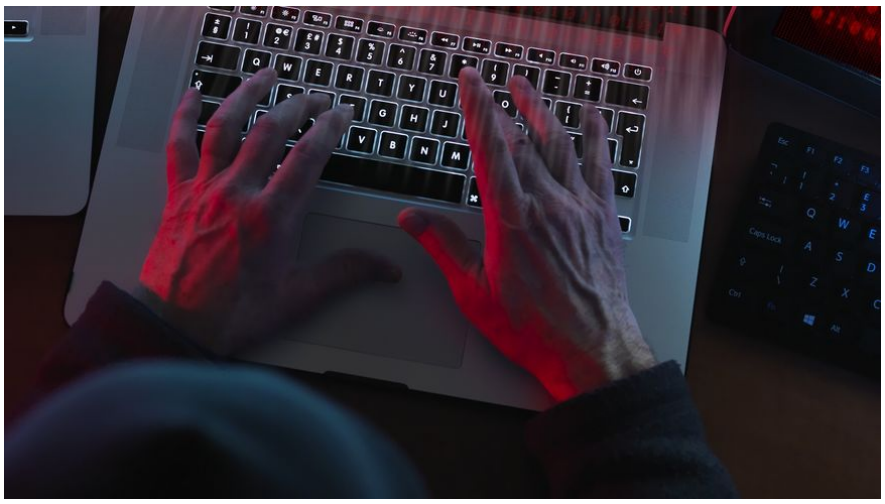
Une vulnérabilité présente dans les navigateurs Internet Explorer et Edge permet à un attaquant d'exécuter du code arbitraire depuis une page internet malveillante.
Cette vulnérabilité exploite une faille de type confusion de type et peut être déclenchée en définissant des valeurs particulières pour les propriétés d'un objet tableau dans une page Web spécialement conçue.
On notera que cette vulnérabilité est atténuée par l'utilisation de la mesure de sécurité de Windows Control Flow Guard (CFG) au sein de l'application. Un attaquant souhaitant exploiter la vulnérabilité devra ainsi mettre en oeuvre un contournement de la contre-mesure CFG.
Aucun correctif n'est prévu par Microsoft avant la publication mensuelle des correctifs de sécurité du mois de mars. Dans l'attente de la disponibilité d'un correctif de sécurité, le CERT-FR recommande de privilégier l'utilisation de navigateurs autres qu'Internet Explorer ou Edge pour la navigation sur Internet.

5 – Documentation

• Rapport de Bogue de Project Zero du 23 février 2017
https://bugs.chromium.org/p/project-zero/issues/detail?id=1011
• Référence CVE CVE-2017-0037
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0037
.

Source : *Vulnérabilité dans les navigateurs Microsoft*

Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle



Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle

Elles ont beaucoup fait parler d'elles durant la campagne présidentielle américaine : certaines pratiques malveillantes sur Internet pourraient aussi peser sur l'élection en France. Voici en quoi elles consistent.
Interview par Marina Cabiten (France Bleu)

Des pirates informatiques qui œuvrent contre Hillary Clinton, et donc en faveur de Donald Trump, le tout commandité par le Kremlin : il ne s'agit pas d'un scénario de film mais d'une accusation très sérieuse formulée par les autorités américaines lors de la campagne présidentielle. Internet est un outil puissant pour les manipulations informatiques, à différents degrés. Et la France est, selon plusieurs acteurs de la cybercriminalité, très mal préparée à ces usages détournés. Voici comment des personnes mal intentionnées pourraient perturber la campagne.

Inonder les réseaux sociaux de faux utilisateurs : l'astroturfing

Tout un chacun peut utiliser son compte Facebook ou Twitter pour s'exprimer, et éventuellement partager ses opinions politiques. Mais cette utilisation des réseaux sociaux peut être bidonnée. Ce phénomène est appelé astroturfing, du nom d'une marque de pelouse synthétique pour les stades : Astroturf. Autrement dit, il s'agit de faire prendre aux internautes du faux gazon pour de l'herbe naturelle… Comment ? **En inondant les réseaux sociaux de faux comptes automatisés, les "bots"**, qui diffusent des messages rédigés par les initiateurs de cette technique de "marketing politique" qui ne dit pas son nom, et garantit l'anonymat.
N'importe quel internaute peut créer et animer des faux comptes. Avec un peu plus de moyens financiers, il peut payer pour qu'un réseau social comme Facebook donne plus de visibilité à une page ou à un post via un algorithme qui fera apparaître le message sur davantage de "murs" d'utilisateurs, qui n'ont rien demandé. Sur Twitter, il peut acheter des "followers" (personnes qui suivent le compte) pour donner une fausse légitimité à ses comptes artificiels. Le degré ultime est de se payer un logiciel qui fait ça tout seul, voire d'employer quelqu'un pour l'exploiter. Cela existe, au sein d'entreprises privées mais parfois aussi de partis politiques. **C'est une forme de propagande de plus en plus répandue.** Le gouvernement français a annoncé récemment son intention de surveiller les réseaux sociaux pour éventuellement repérer des "mouvements" suspects de ce type.

Quand des sites partisans se font passer pour des organes de presse : les « fake news »

L'expression "Fake news", qui se traduit littéralement par « fausses informations », est très en vogue depuis la présidentielle américaine et vient de la diffusion sur Internet de prétendus articles de presse, qui ne sont en réalité pas rédigés par des journalistes. Des articles contenant des informations non vérifiées, parfois erronées, voire carrément mensongères dans le but bien précis de manipuler l'opinion.
La mécanique est la même que pour l'astroturfing, tout faire pour que ces "fake news" soient largement vues sur Facebook et les autres réseaux sociaux ou forums. Selon les calculs du site Buzzfeed, les articles relayant de fausses informations **(comme le faux soutien du pape François à Donald Trump, ou la révélation imaginaire de ventes d'armes par Hillary Clinton à l'organisation Etat islamique)** ont suscité 8,7 millions d'interactions sur Facebook durant la campagne américaine, contre 7,3 millions pour les articles de la presse traditionnelle.
En France récemment, plusieurs médias ont fait part de leur volonté de lutter contre ce phénomène, allant même pour certains jusqu'à nouer un partenariat avec Facebook et Google. ***"Le problème c'est que la rumeur court toujours beaucoup plus vite que la rectification ou la suppression du contenu"***, objecte Denis Jacopini, diplômé en cybercriminalité et sécurité de l'information, ***"laissant s'installer dans l'esprit de l'électeur ces fausses affirmations."***

De vrais contenus, mais dérobés et diffusés sans autorisation : le vol de données

La menace la plus sophistiquée reste le vol d'informations numériques. C'est l'exemple des pirates informatiques (hackers) qui ont récupéré près de 20.000 courriels de responsables du parti d'Hillary Clinton. Ils sont entrés dans les serveurs du parti démocrate dès l'été 2015, accumulant ces données parfois embarrassantes sans que personne ne s'en aperçoive, pour les publier au moment opportun pour déstabiliser le camp démocrate. Une cyberattaque venue de Russie pour aider Donald Trump à gagner l'élection, affirme la CIA dans un rapport révélé par la presse américaine. ***"Aucun parti politique français n'est actuellement protégé contre une telle malveillance"***, assure Denis Jacopini.
Selon le Canard Enchaîné (numéro du 8 février 2017), **les services secrets français s'inquiètent de cyberattaques russes** durant la Présidentielle, qui auraient pour but d'aider la campagne de Marine Le Pen. De son côté, le secrétaire général du mouvement « En Marche ! » Richard Ferrand a affirmé publiquement que les pirates russes visent particulièrement Emmanuel Macron et ont déjà attaqué à plusieurs reprises son site web.

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 : *Comptes bidons, « fake news », vol de données : ces manipulations informatiques qui pourraient perturber la Présidentielle*

Cybersécurité dans le monde : à quoi peut-on s'attendre ?

Cybersécurité dans le monde : à quoi peut-on s'attendre ?

L'année 2016 a démontré que les mesures de sécurité traditionnelles ne suffisaient plus et que de nouvelles stratégies devaient être mises en place. 2017 va donc s'inscrire dans la continuité de ce qui a déjà été amorcé l'année passée, à savoir : toujours plus de sécurité pour toujours une protection maximisée. Les experts de NTT Security ont fait ressortir les tendances et les prévisions pour cette année qui débute.

Selon Garry Sidaway, Vice-Président Senior de la Stratégie de Sécurité

1. L'identité restera au cœur des enjeux

Au risque de nous répéter, les mots de passe fournissent aujourd'hui des garanties insuffisantes. À l'ère du digital et de la mobilité, commodité et sécurité ne font pas bon ménage. Certes, les mots de passe sont bien pratiques, mais ils sont de moins en moins perçus comme une preuve d'identité irréfutable. Devant l'utilisation croissante des smartphones et les exigences de simplicité des consommateurs et des professionnels, les solutions d'identité resteront donc au cœur des préoccupations en 2017. C'est ainsi que le mot de passe traditionnel cèdera du terrain face à la poussée du « multi-facteurs », une méthode combinant plusieurs facteurs d'authentification (localisation, possession d'un objet, d'une information, etc.). Cette association entre physique et digital, avec en toile de fond l'émergence de méthodes d'authentification avancées, favorisera le développement de nouvelles solutions de gestion des identités.

2. Le mobile sera omniprésent

Au royaume du digital, le mobile est roi. Un roi qui bouscule l'ordre établi dans de nombreux domaines, des méthodes de paiement jusqu'aux interactions sociales. Véritables hubs digitaux, nos smartphones constituent désormais non seulement une fenêtre de contrôle et d'interaction avec le monde mais aussi une interface d'identification et d'authentification. Dans un tel contexte, 2017 verra le curseur de la menace se déplacer des ordinateurs portables vers les appareils mobiles. Si, traditionnellement, les acteurs de la sécurité se sont concentrés sur les systèmes back-end et les conteneurs, ils devront revoir leur approche pour placer le mobile au cœur de leur dispositif.

3. Les entreprises surveilleront la menace interne

Le problème des menaces internes ne date pas d'hier. Côté défense, les progrès réalisés dans les domaines de l'analytique et de la détection des anomalies devraient se poursuivre en 2017. Dans un milieu de l'entreprise de plus en plus dynamique, définir les critères d'un comportement utilisateur « normal » restera un défi de taille. Toutefois, avec le développement de nouvelles techniques de machine learning, nous verrons l'analyse comportementale s'opérer directement au niveau des terminaux.

4. Fin de la détection basée sur les signatures

Antivirus nouvelle génération, solutions de sécurité des terminaux, solutions de détection et de réponse aux incidents… Peu importe leur nom, les solutions de protection des terminaux se projetteront bien au-delà de la détection basée sur des signatures statiques, à commencer par les outils d'analyses avancées que l'on retrouvera systématiquement sur ces solutions. Leur force résidera notamment dans leur capacité à exploiter la puissance du cloud pour partager l'information sur les menaces connues. La diversité et le volume sans précédent des malwares engendreront l'émergence d'une nouvelle approche. Destinée à enrayer le syndrome dit du « patient zéro », cette démarche reposera à la fois sur une collaboration internationale et l'utilisation d'une cyberveille prédictive et proactive pour libérer toute la force du collectif.

5. Le tout-en-un fera de plus en plus d'adeptes

Alors que le marché de la cybersécurité se consolide, les entreprises se tournent vers des solutions de sécurité couvrant l'intégralité des environnements TIC. Traditionnellement, la force des prestataires de sécurité managée (MSS) s'est située dans leur capacité à intégrer un maillage d'outils complexes et pointus. Aujourd'hui, la situation a changé. Tout l'enjeu consiste à intégrer le facteur sécurité à tous les échelons du cycle opérationnel de l'entreprise. Les clients chercheront donc un partenaire capable d'agir sur tous les fronts : applications métiers, infrastructure réseau, services cloud et de data center autour d'une console de gestion centralisée. En 2017, les solutions multifournisseurs apparaîtront comme datées. Les acteurs de la sécurité devront ainsi coordonner un service complet de bout en bout pour répondre aux enjeux de l'espace de travail digital.

Selon Stuart Reed, Directeur Senior Product Marketing

6. Les consommateurs exigeront plus de transparence

Une étude récente de NTT Security a mis en lumière les attentes croissantes des cyberconsommateurs en matière de transparence, tant sur le plan des pratiques que de la gestion des incidents. Ces conclusions traduisent notamment une sensibilisation accrue des consommateurs sur les questions de sécurité suite aux scandales de violations à répétition. La tendance est appelée à se poursuivre en 2017 et au-delà. Notons enfin que les entreprises dotées de politiques de sécurité et de plans d'intervention efficaces diminueront leur exposition au risque, tout en profitant d'un puissant levier de compétitivité.

7. L'innovation en moteur de consolidation

Du point de vue de l'offre comme des fournisseurs de cybersécurité, 2016 a été placée sous le signe de la consolidation. Au rang des plus grosses opérations, on citera l'acquisition de BlueCoat par Symantec, la série de rachats par Cisco et, plus proche de nous, la création de NTT Security autour de trois piliers : analytique de pointe, cyberveille avancée et conseils d'experts en sécurité. Derrière ce phénomène de consolidation, on retrouve une constante : l'innovation. Concrètement, les grandes entreprises ont racheté des spécialistes pour accéder à leurs compétences et les englober dans une offre plus aboutie. Ces grands acteurs profitent enfin d'économies d'échelle considérables – et de l'expertise et de l'efficacité qui en découlent – pour mener des programmes d'incubation qui viendront à leur tour stimuler l'innovation. Cette tendance de fond souligne bien l'importance de l'innovation pour évoluer au rythme des besoins de sécurité des clients.

8. L'identité des objets

Avec l'essor de l'IoT, la frontière entre physique et digital s'estompe peu à peu pour créer des expériences clients plus pratiques, rapides et efficaces. Seulement voilà, les cybercriminels ont eux aussi investi la sphère de l'IoT à l'affût de la moindre vulnérabilité. On a ainsi recensé des cyberattaques se servant d'objets connectés (caméras de vidéosurveillance, imprimantes…) pour lancer des attaques DDoS qui sont parvenues à paralyser des sites comme Twitter et Spotify. L'année 2017 verra sans doute une recrudescence des attaques perpétrées à l'encontre des objets connectés. D'où le besoin impérieux d'intégrer ces appareils à une politique de sécurité plus complète, notamment pour mieux contrôler l'identité et la légitimité de leurs utilisateurs.

9. L'analytique changera la donn

L'un des grands défis de la cybersécurité pourrait se résumer par cette question : comment produire une information cohérente à partir d'une avalanche de données issues de dispositifs multiples ? Si l'analyse de données a pour fonction première de « donner du sens », l'évolution des menaces doit nous inciter à revoir nos méthodes d'interprétation et de contextualisation de l'information. Dans cette optique, les outils avancés d'analyse du risque vous permettront de prendre les bonnes décisions. Au-delà des événements présents, ces outils ont pour fonction de décortiquer les données historiques pour faire ressortir des tendances, mais aussi d'utiliser l'intelligence artificielle pour identifier les schémas comportementaux annonciateurs d'une attaque. Fondées sur des technologies avancées de machine learning, des outils d'analyse automatiques et des experts en astreinte permanente, les solutions d'analytique de pointe promettent de changer la donne dans le secteur des MSS.

Selon Kai Grunwitz, Vice-Président Senior Europe Centrale

10. La cybersécurité va s'imposer comme un facteur clé de succès

Pour être reconnue comme tel par tous les acteurs concernés, la cybersécurité doit s'intégrer en amont à l'ensemble des processus métiers de l'entreprise. Dans un monde connecté où le digital gagne chaque jour en importance, les entreprises veulent pouvoir compter sur une sécurité parfaitement incorporée à leurs stratégies métiers et IT. Outre son rôle indispensable de gardienne des données sensibles, du capital intellectuel et des environnements de production, la cybersécurité sera également partie intégrante de l'innovation et de la transformation de l'entreprise.

La sécurité ne sera plus seulement le problème des DSI, mais s'invitera au cœur des processus métiers et constituera l'un des ressorts de la chaîne de valeur. Enfin, la gestion du cycle de sécurité constituera un différenciateur clé autant qu'une priorité essentielle dans le cadre d'une stratégie de sécurité orientée métiers. Elle procurera aux entreprises un avantage concurrentiel et un réel levier de valeur ajoutée.

Selon Chris Knowles, Directeur solutions

11. Le RGPD sera partout !

Si vous pensiez que le Règlement général sur la protection des données (RGPD) a été l'un des grands thèmes de 2016, attendez de voir ce que 2017 vous réserve. Alors que les fournisseurs proclameront les avantages de leurs technologies et que les équipes juridiques plancheront sur la définition d'une sécurité réellement irréprochable, les clients, eux, se lanceront dans les préparatifs.

12. Au royaume des aveugles, les borgnes sont rois… mais plus pour très longtemps !

Pour beaucoup d'entreprises, la sécurité se résume à la protection d'un périmètre au moyen de périphériques inline censés analyser l'intégralité du trafic et intervenir sur la base d'éléments visibles. Toutefois, la mobilité croissante des collaborateurs, associée à l'explosion du nombre d'applications cloud en entreprise, créent des « angles morts ». À commencer par le transit d'informations via des tunnels cryptés, le stockage et le traitement de données à l'extérieur de data centers sécurisés, ou encore les communications entre machines virtuelles qui échappent totalement à la surveillance des dispositifs de sécurité existants. En 2017, les entreprises se pencheront sur ce phénomène afin d'éliminer les angles morts et de reprendre le contrôle de leur sécurité.

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 DIRTE 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 dans le monde : à quoi peut-on s’attendre ?*