

Alerte ! Un phishing élaboré vise les utilisateurs de Gmail



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

En matière de phishing – les escroqueries consistant à se faire passer pour un tiers de confiance afin de dérober les informations bancaires ou personnelles de sa cible –, la dernière arnaque en cours contre les utilisateurs de Gmail, particulièrement répandue en 2016, s'avère très efficace, au point de duper des utilisateurs chevronnés.

Comme la majorité des tentatives, cette arnaque commence par l'envoi d'un email a priori banal, provenant généralement d'un contact de notre carnet d'adresse qui a déjà été victime de ce phishing. La manœuvre frauduleuse mise sur sa prétendue pièce jointe.

En cliquant sur ce fichier a priori inoffensif – qui est en réalité une capture d'écran avec un lien et pas une véritable pièce jointe – pour en avoir un aperçu, l'utilisateur se retrouve sur une nouvelle page qui l'invite à se reconnecter à son compte Gmail. Apparence, URL (un « data:text » suivi de l'adresse « <https://accounts.google.com> » rassurante mais qui ouvre en fait un script)... tout semble conforme à un véritable formulaire Google. Mais en tapant son adresse et son mot de passe, la cible vient de succomber au piège.

Une victime décrit ainsi son expérience malheureuse : « Les attaquants se connectent immédiatement à votre compte dès qu'ils en ont le mot de passe, et ils utilisent l'une de vos pièces jointes, combinée à un véritable titre de mail, pour l'envoyer à vos contacts. Ils ont par exemple accédé au compte d'un élève et en ont extrait un calendrier d'entraînement sportif pour en faire une capture d'écran et l'ont ensuite associée à un titre de mail relativement en rapport pour l'envoyer aux autres membres de l'équipe. »

GOOGLE RECOMMANDE LA VALIDATION À DEUX ÉTAPES

Pour éviter de devenir la dernière victime de ce phishing élaboré, la vigilance reste de mise, notamment en vérifiant systématiquement la présence du cadenas sécurisé dans la barre d'adresse. Mais surtout en activant la validation en deux étapes : à chaque connexion à Google, en plus de votre mot de passe, vous devez saisir un code qui vous est communiqué sur votre téléphone. Aaron Stein, de Google Communications, recommande d'ailleurs cette méthode dans un communiqué qui se veut rassurant : « Nous sommes au courant de ce problème et nous continuons d'améliorer notre défense. Nous contribuons à la protection des utilisateurs contre le phishing de multiples manières, notamment grâce à la détection de [mail frauduleux] par machine learning . »

Gmail permet aussi à ses utilisateurs, en quelques clics, de signaler qu'un contenu reçu dans sa boîte mail relève du phishing. Fin novembre, des professeurs et des journalistes avaient reçu une alerte de Google contre des tentatives d'intrusion.

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

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



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

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



[Contactez-nous](#)

Réagissez à cet article

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

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

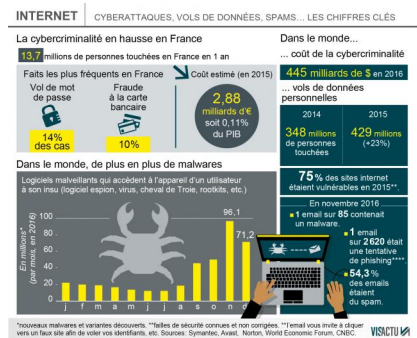


Comment a évolué la cybercriminalité en 2016 par rapport à 2015 ?

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

Les chiffres de la cybercriminalité ont de quoi faire peur. 13,7 millions de personnes ont été confrontées à la cybercriminalité en France en 2016, selon Norton, entreprise spécialisée dans la sécurité en ligne.

Vente de faux papiers d'identité, apologie du terrorisme, vols de mots de passe, de données personnelles, extorsion de fonds ou encore trafic d'armes : le terme cybercriminalité couvre de multiples activités illicites.



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

Vol de mots de passe

En France, les actes les plus fréquents sont les vols de mots de passe (14 % des cas) et la fraude à la carte bancaire (10 % des cas). Mais entre les faits recensés et la réalité, il est très difficile de mesurer l'ampleur exacte du phénomène...

Certaines victimes ne savent tout simplement pas (encore) qu'elles ont été volées, d'autres n'ont pas porté plainte et ont préféré payer une rançon (parfois quelques centaines d'euros) pour récupérer des photos intimes par exemple.

Selon Symantec, célèbre pour ses logiciels antivirus, le nombre de cyberattaques dans le monde a diminué ces derniers mois. Elle en a recensé 291 000 pour le seul mois de novembre 2016 contre 1 461 000 en janvier 2015.

Gare aux malwares

Par contre, le nombre de nouveaux malwares explose. Ces logiciels malveillants qui accèdent à l'appareil d'un utilisateur à son insu (logiciel espion, virus, cheval de Troie, rootkits, etc.) dans le but de dérober des données sont partout.

Symantec dénombrait 20 millions de nouveaux malwares (et variantes) chaque mois début 2016, un chiffre qui a bondi en fin d'année pour atteindre les 96,1 millions en novembre et 71,2 millions de nouveaux malwares détectés en décembre.

Les vols de données de personnes en hausse

En novembre 2016, Symantec estimait qu'un email sur 85 contenait un malware, qu'un email sur 2 620 était une tentative de phishing (l'email vous invite à cliquer vers un faux site afin de voler vos identifiants, mots de passe, etc.) et que plus de la moitié des emails (54,3 %) étaient non sollicités (spam).

En 2015, elle estimait que 429 millions de personnes dans le monde s'étaient faites voler des données personnelles, un chiffre en hausse de 23 % par rapport à l'année précédente.

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

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



Réagissez à cet article

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

Pourquoi les DSI sont-ils inquiets à l'approche des

Fêtes de fin d'année ?

 Denis JACOPINI EXPERT JUDICIAIRE vous informe	Pourquoi les DSI sont-ils inquiets l'approche Fêtes de d'année ? à des fin
--	--

La dernière étude d'IFS sur les défis auxquels les DSI sont confrontés durant la période des fêtes de fin d'années révèle que 76% des sondés se sentent davantage préoccupés à l'approche de cette période et ce, pour plusieurs raisons : la disponibilité du personnel (41% des répondants), les risques de piratage liés à la sécurité IT (31%) ainsi que les besoins IT des collaborateurs travaillant à distance (31% également). Tout cela a un impact certain sur les processus et activités métier.

De tous, les plus inquiets quant à la disponibilité du personnel à la période des fêtes de fin d'année sont les français. 62% d'entre eux déclarent qu'il s'agit de l'une de leurs plus grandes préoccupations au cours de la saison des fêtes de fin d'année. À l'opposé, près de la moitié des répondants américains (48%) citent le piratage informatique.

Du côté des « besoins », 42% des décideurs IT sont en demande d'un budget plus important. La migration vers le Cloud (18%) et le recrutement de personnel IT (16%) sont également cités dans le top 3 de leurs besoins. Par ailleurs, un quart des répondants américains et suédois (respectivement 26% et 25%) souhaitent, à court terme, une accélération de la migration vers le Cloud, alors qu'ils ne sont que 11% et 14% en Australie et Allemagne à privilégier cet enjeu.

« Ce qui ressort clairement de notre étude est que de nombreux décideurs IT ont des craintes légitimes pour la période des fêtes de fin d'année : disponibilité du personnel, risque de piratage informatique, commente Mark Boulton, CMO d'IFS. Il est essentiel que toutes les entreprises, quelle que soit leur taille, se préparent à affronter les problèmes qui pourraient survenir et soient en mesure d'accompagner, à distance, leurs collaborateurs ». L'IoT et la migration vers le Cloud faisant partie des solutions possibles.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



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

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



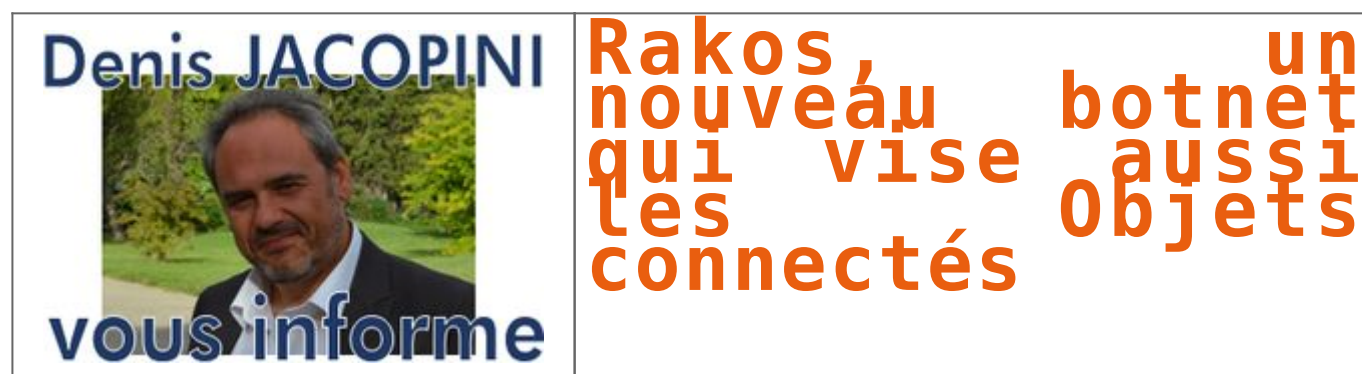
[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Pourquoi les DSI sont-ils inquiets à l'approche des Fêtes de fin d'année ?

Rakos, un nouveau botnet qui vise aussi les objets connectés



Après Mirai, voici venir Rakos, un malware infectant des serveurs et des réseaux d'objets connectés, tournant sous Linux, afin de créer des botnets. ET, demain, lancer des attaques DDoS.

Comme le tristement célèbre malware Mirai, Rakos prend pour cible l'Internet des objets (IoT). Ces deux logiciels malveillants compromettent en effet des serveurs sous Linux et des réseaux d'appareils connectés. La capacité de nuisance de ces botnets contrôlés à distance est bien réelle. Si Mirai se propage essentiellement via les ports logiciels Telnet, Rakos vise lui les ports SSH. Les périphériques embarqués et les serveurs ayant un port SSH ouvert ou un mot de passe très faible sont les plus exposés. Rakos a été découvert cet été par les chercheurs de ESET.

À ce jour, Rakos est utilisé pour mener des attaques par force brute, indique l'entreprise dans un billet de blog. Et ce, afin d'ajouter d'autres appareils compromis à son réseau de machines zombies. Mais le programme pourrait également servir à mener des campagnes de spam ou des attaques par déni de service distribué (DDoS) d'ampleur, comme l'a fait Mirai...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Rakos, un nouveau botnet IoT en constitution

Six secondes suffisent pour pirater une carte bancaire



Six
secondes
suffisent
pour
pirater
une carte
bancaire

En multipliant les tentatives sur différents sites, des chercheurs sont parvenus à contourner facilement les systèmes de paiement sécurisés mis en place et ce sans même posséder la carte bancaire physique utilisée.



Votre carte bleue n'est en sécurité nulle part. Sans connaître aucun détail de celle-ci, des pirates peuvent facilement pirater un compte en banque. Il leur suffit simplement d'un ordinateur, d'un accès à Internet et de six secondes, révèlent les chercheurs de l'université de Newcastle, au Royaume-Uni, dans une étude publiée dans le journal académique *IEEE Security & Privacy* (IEEE signifiant Institute of Electrical and Electronics Engineer).

Dans la pratique, les chercheurs ont utilisé une attaque par force brute pour contourner les mesures de sécurité visant à protéger le système de paiement en ligne des fraudeurs. Connectée sur différents sites, l'équipe de chercheurs a généré de façon répétée et continue des variations des différentes informations sécurisées de cartes de paiement (numéro de carte, date d'expiration et cryptogramme visuel) jusqu'à obtenir un résultat favorable. D'après l'étude, c'est vraisemblablement une attaque du genre qui était au cœur de l'attaque informatique contre la filiale bancaire du géant britannique de la distribution Tesco, dont 20.000 clients ont été victimes.

Deux petites faiblesses qui en font une grosse

Si l'attaque parvient à réussir, c'est parce que le système ne détecte en effet pas les échecs répétés sur une même carte si cela se produit sur différents sites, d'autre part, tous les sites ne demandent pas les mêmes informations au même moment, ce qui permet de deviner un champ à la fois.

« Ce type d'attaque exploite deux faiblesses qui ne sont pas trop graves d'elles-mêmes mais lorsque utilisées simultanément présentent un sérieux risque pour l'ensemble du système de paiement », explique dans le communiqué Mohammed Ali, étudiant en doctorat à l'école d'informatique de l'université de Newcastle et auteur principal de l'étude.

Simplement en partant des six premiers numéros de la carte de paiement, qui servent à indiquer la banque et le type de carte et sont donc identiques pour chaque fournisseur unique, « un pirate peut obtenir les trois informations essentielles pour réaliser un achat en ligne en tout juste six secondes ». Le délai peut être extrêmement réduit dans les cas où le pirate dispose des numéros de cartes, ce qui risque d'arriver de plus en plus souvent au vu de la récente vague d'intrusions informatiques survenues dans les plus grandes entreprises. Il leur suffit dans ce cas de deviner la date d'expiration – moins de 60 essais puisque la plupart des cartes de crédit sont valides cinq ans au maximum -, puis le cryptogramme visuel composé de trois chiffres – ce qui prend dans le pire des cas 1.000 essais.

Mohammed Ali souligne toutefois que cette technique d'attaque par force brute ne marche qu'avec le réseau VISA, « le réseau centralisé de MasterCard a été capable de détecter l'attaque après moins de 10 essais – même lorsque les paiements étaient répartis sur différentes réseaux ». Autre point faible de la technique : la confirmation par SMS, que demandent bon nombre de sites d'e-commerce en France...[lire la suite]

Rapport 2015 de l'Observatoire de la sécurité des cartes de paiement

Original de l'article mis en page : Il suffit de six secondes pour pirater une carte bancaire

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



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

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



[Contactez-nous](#)



Réagissez à cet article

Prévisions cybercriminalité pour 2017

Denis JACOPINI



vous informe

Prévisions
cybercriminalité
pour 2017

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

Denis JACOPINI

Trend Micro présente son rapport annuel des prévisions en matière de sécurité: 'The Next Tier – 8 Security Predictions for 2017'. L'année prochaine sera marquée par des attaques de plus grande envergure à tous les niveaux. Les cybercriminels adopteront des tactiques différentes pour tirer parti de l'évolution du paysage technologique.

« Nous pensons que la General Data Protection Regulation (GDPR) va non seulement changer fondamentalement la manière dont les entreprises gèrent leurs données, mais aussi induire de nouvelles méthodes d'attaque. La tactique du ransomware va également s'étendre pour toucher plus d'appareils, tandis que la cyberpropagande influencera de plus en plus l'opinion publique», déclare Raimund Genes, CTO de Trend Micro.

En 2016, l'on a assisté à une formidable augmentation des vulnérabilités d'Apple avec pas moins de 50 fuites. A cela s'ajoutent 135 bugs Adobe et 76 bugs Microsoft. Alors que Microsoft continue d'améliorer ses facteurs limitatifs et qu'Apple est de plus en plus considéré comme le système d'exploitation prépondérant, ce déplacement apparent des 'exploits' des logiciels vulnérables va encore s'accroître en 2017.

L'IoT et l'IIoT – dans la ligne de mire des attaques ciblées

L'Internet of Things (IoT – internet des objets) et l'Industrial Internet of Things (IIoT – internet industriel des objets) seront de plus en plus dans la ligne de mire des attaques ciblées en 2017. Ces attaques tirent parti de l'engouement croissant suscité par les appareils connectés en exploitant les failles et les systèmes non protégés et en perturbant des processus d'entreprise. L'usage croissant d'appareils mobiles pour surveiller les systèmes de production dans les usines et les milieux industriels, combiné au nombre important de vulnérabilités dans ces systèmes constitue une réelle menace pour les organisations.

Explosion de l'extorsion professionnelle

Le Business E-mail Compromise (BEC) et le Business Process Compromise (BPC) représentent de plus en plus une forme relativement simple et économiquement rentable d'extorsion professionnelle. En incitant un employé innocent à verser de l'argent sur le compte bancaire d'un criminel, une attaque BEC peut rapporter 140.000 dollars. Bien que le piratage direct d'un système de transaction financière exige plus d'efforts, cela représente une manne de pas moins de 81 millions de dollars pouvant tomber aux mains des criminels.

Autres faits marquants du rapport

Le nombre de nouvelles familles de ransomware ne progresse que de 25 %. Mais le ransomware s'étend désormais aux appareils IoT et aux terminaux informatiques autres que les desktops (par exemple les systèmes POS ou les distributeurs automatiques).

Les fournisseurs ne parviendront pas à protéger à temps les appareils IoT et IIoT pour éviter des attaques DoS (refus de service) ou d'autres types d'attaques.

Le nombre de failles découvertes dans les technologies Apple et Adobe augmente, ce qui vient s'ajouter aux « exploit-kits ».

46 pour cent de la population mondiale est aujourd'hui reliée à l'internet : la cyberpropagande ne va cesser d'augmenter, à présent que les nouveaux dirigeants des grands pays sont en place. L'opinion publique risque donc d'être influencée par de fausses informations.

Comme ce fut le cas lors de l'attaque de la Banque du Bangladesh plus tôt cette année, les cybercriminels parviennent à modifier des processus d'entreprise via des attaques BPC, et à en tirer largement profit. Les attaques BEC restent d'actualité pour extorquer des fonds à des employés qui ne se doutent de rien.

Le GDPR produira des changements de politique et administratifs qui auront un lourd impact sur les coûts. Cela exigera aussi des examens complexes des processus de données pour assurer la conformité réglementaire.

De nouvelles méthodes d'attaques ciblées déjoueront les techniques de détection modernes, permettant aux criminels de s'attaquer à différentes organisations.

Original de l'article mis en page : Le ransomware s'étend aux appareils connectés et à l'internet des objets – Press Releases – Informaticien.be

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

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



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 DRTF n°93 84 03041 84)
- Formation de C.I.L.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



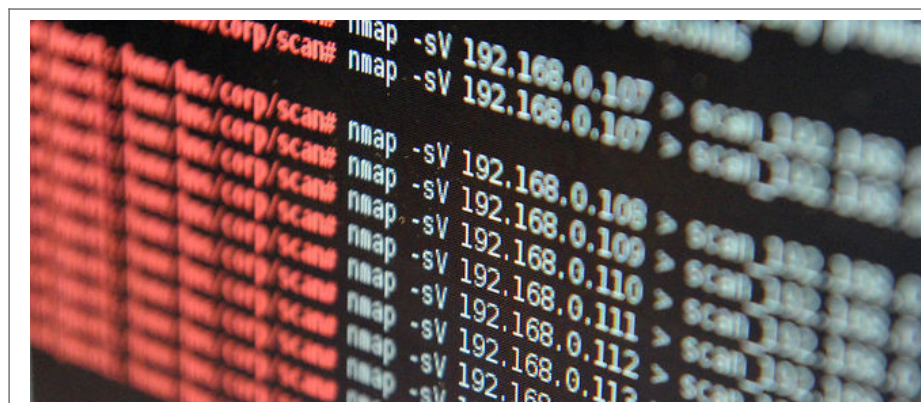
[Contactez-nous](#)



Réagissez à cet article

Original de l'article mis en page : Le ransomware s'étend aux appareils connectés et à l'internet des objets – Press Releases – Informaticien.be

14 millions de Français victimes des pirates Informatiques en 2016



14 millions
de Français
victimes des
pirates
informatiques
en 2016

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

Dans un rapport publié mercredi 16 novembre, l'éditeur d'antivirus Symantec-Norton pointe l'ampleur que le phénomène « cybercriminel » a prise en 2016. Selon cette étude, 13,7 millions de Français auront été victimes d'attaques informatiques cette année. Le fait d'avoir baigné dans l'univers numérique depuis sa naissance ne change rien à la donne. Les « digital natives » (comme les experts désignent les jeunes qui manipulent des ordinateurs depuis le berceau) sont aussi démunis face à cette menace que leurs aînés.

La génération Y, celle des 18-34 ans, fait ainsi partie des plus touchées par le problème. Il faut dire que cette catégorie de population se comporte sur le Web de manière particulièrement risquée. Or, pour les professionnels de la cybersécurité, la négligence des internautes serait en cause dans la plupart des attaques informatiques dont ils sont victimes.

Des internautes imprudents

Bien que 77 % des Français sachent qu'ils doivent protéger leurs données en ligne, les utilisateurs gardent de mauvaises habitudes sur le Web. Les réflexes d'élémentaire prudence sont de peu de poids face à l'attrait de certains liens... même d'origine douteuse. Ainsi, 65 % des Français reconnaissent avoir déjà ouvert une pièce jointe postée d'un expéditeur inconnu. Et quasiment un internaute sur cinq partage ses mots de passe avec d'autres utilisateurs. Faut-il, dès lors, s'étonner qu'un Français sur deux se résigne à l'idée qu'il est désormais plus probable qu'une personne accède frauduleusement à ses appareils domestiques connectés qu'à son logement ?

D'après Laurent Heslault, directeur des stratégies numériques chez Symantec, les internautes ont bien conscience des dangers mais « n'ont pas envie de prendre les précautions adéquates pour assurer leur sécurité ». Alors que les cybercriminels, eux, disposent de techniques de plus en plus recherchées pour arriver à leurs fins.

Il ne s'agit pas seulement de paresse chez les internautes. 31 % d'entre eux sont dépassés par la quantité d'informations qu'ils ont à protéger. La plupart considèrent d'ailleurs que la question de la gestion sécurisée des données ne les concerne pas et qu'il appartient aux fournisseurs d'accès à Internet et aux entreprises du secteur des nouvelles technologies de résoudre ces problèmes.

Un problème mondial

Une étude réalisée en octobre, par le Ponemon Institute pour le compte de l'éditeur de logiciels professionnels Varonis Systems, démontre qu'il ne s'agit pas d'un problème strictement hexagonal. Si 37 % (seulement !) des internautes français indiquent qu'ils prennent toutes les mesures appropriées pour protéger les données auxquelles ils accèdent et qu'ils utilisent, la même réponse est donnée par 50 % chez les collaborateurs allemands, 39 % des employés britanniques et 35 % des employés américains.

Le nombre d'entreprises ayant fait l'expérience des ransomwares l'an dernier est en hausse constante. Ces logiciels rançonneurs, dont le FBI a révélé qu'ils avaient généré, au premier semestre 2016, plus de 209 millions de dollars de butin, ont infecté les serveurs de 12 % des entreprises allemandes, contre 17 % aux États-Unis, 16 % en France et 13 % au Royaume-Uni. Le nombre de cas de perte ou de vol de données au cours des deux dernières années a, lui aussi, explosé... Et l'on ne compte plus les cyberbraquages signalés chaque semaine à travers la planète.

De quoi inciter les États à renforcer leur arsenal pour lutter plus efficacement contre les gangs à l'oeuvre sur la Toile. Les 68 pays signataires de la convention de Budapest, le premier traité international abordant la question de la lutte contre la cybercriminalité adopté en 2001, se sont d'ailleurs réunis les 14 et 15 novembre derniers pour renforcer leur coopération en la matière. Un protocole additionnel à la convention sera adopté courant 2017 pour mettre en place un nouvel outil juridique permettant de collecter des preuves électroniques sur le « cloud », quelle que soit la localisation du serveur qui l'héberge... Preuve, s'il en était besoin, que les gouvernements du monde entier ont pris la mesure de la menace.

Quels sont les cyberdélicts les plus fréquents en France ?

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

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

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

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



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Cybersécurité : un Français sur cinq victime de hackers en 2016

Saint-Malo : la mairie victime d'un piratage téléphonique à 80.000 euros



Au printemps dernier, le standard téléphonique de la mairie de Saint-Malo, en Ille-et-Vilaine, a été piraté. Pendant plus de quatre jours, le ou les auteurs de l'arnaque ont passé des coups de fil à l'étranger aux frais de la Ville, pour un montant total de 80.000 euros....[Lire la suite]

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



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

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



[Contactez-nous](#)

Réagissez à cet article

**Saint-Malo : la mairie
victime d'un piratage
téléphonique à 80.000 euros**



Au printemps dernier, le standard téléphonique de la mairie de Saint-Malo, en Ile-et-Vilaine, a été piraté. Pendant plus de quatre jours, le ou les auteurs de l'arnaque ont passé des coups de fil à l'étranger aux frais de la Ville, pour un montant total de 80.000 euros....[Lire la suite]

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



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

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



[Contactez-nous](#)

Réagissez à cet article

Nouvelles menaces informatiques et évolution des protection

	Nouvelles menaces informatiques et évolution des protection
---	--

Destinés au grand public, ESET Internet Security et ESET Smart Security Premium apportent 5 nouvelles fonctions.

« Le tout nouveau produit ESET Internet Security vient s'ajouter à notre portefeuille de produits primés et offre aux utilisateurs les meilleures fonctionnalités en matière de détection, de vitesse et de convivialité. Ces nouveaux produits ajoutent à nos protections multi-couches existantes un ensemble de fonctionnalités centrées sur la protection de la vie privée » explique Eduard Kesely, Product Manager chez ESET.

ESET Internet Security, une protection optimale

ESET Internet Security s'adresse aux utilisateurs nécessitant une protection complète. Aux couches de sécurité déjà disponibles dans l'antivirus, s'ajoutent 3 nouvelles fonctionnalités :

- La protection contre les attaques par script.
- La protection Webcam qui signale les processus et les applications qui tentent d'accéder à la webcam de l'utilisateur et permet de les bloquer.
- La protection du réseau domestique qui permet à l'utilisateur de connaître l'identité des appareils connectés.

ESET Smart Security Premium, un produit haut de gamme

ESET propose un nouveau produit haut de gamme, ESET Smart Security Premium, destiné aux utilisateurs avancés et TPE. En plus des trois fonctionnalités ci-dessus, ESS Premium propose :

- Un gestionnaire de mots de passe.
- Le chiffrement des données pour les protéger en cas de vol ou de perte.

ESET cumule 3 récompenses prestigieuses : Pour la 98ème fois, ESET reçoit le prix VB100. De plus, il est le seul éditeur à avoir détecté 100% des menaces lors du test SE Labs (produits grand public) catégorie protection anti-malware. Enfin, le test réalisé par AV-Comparatives sur la protection anti-spam révèle qu'ESET est le N°1 haut la main.

La gamme ESET destinée aux particuliers, en plus de améliorations citées, couvre toujours macOS®, Android™ (antivirus et contrôle parental) afin de protéger l'intégralité de la famille.

Vous pouvez retrouver l'ensemble des fonctionnalités de nos produits sur <https://www.eset.com/fr/>

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

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

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



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

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



[Contactez-nous](#)

Réagissez à cet article

