

JT 20H – La Poste se lance dans la livraison par drones



JT 20H – Après près de deux ans de tests, La Poste a décidé de faire un grand pas vers l'avant dans son mode de livraison en adoptant la livraison par drones...[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 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

Une nouvelle doctrine en matière de cybersécurité



Une nouvelle doctrine en matière de cybersécurité

Jean-Yves Le Drian, ministre de la Défense, a inauguré hier un nouveau bâtiment de 9 000 m² au centre DGA maîtrise de l'information à Bruz, près de Rennes. À cette occasion, il a dévoilé les grandes lignes de la nouvelle doctrine cyber des armées françaises. Elle reposera sur trois piliers : le renseignement, la protection/défense et la lutte informatique offensive.

« L'irruption du numérique dans toutes les activités de la vie quotidienne nous oblige à repenser en profondeur l'art de la guerre. » Hier, à Bruz, au sud de Rennes, dans les locaux de DGA maîtrise de l'information, « le cœur battant du ministère de la Défense », Jean-Yves Le Drian a présenté les grandes lignes de la nouvelle doctrine cyber des armées françaises.

Des combattants numériques

Cette doctrine s'appuiera sur trois piliers, a expliqué le ministre de la Défense. D'abord le renseignement, « pour détecter les actions hostiles et leurs auteurs. ». Ensuite, la protection et la défense : « Nous devons bâtir d'épaisses murailles numériques. » Enfin, la lutte informatique offensive : « Nous avons besoin de combattants numériques pour riposter et neutraliser les cyber agresseurs. »

Jean-Yves Le Drian a annoncé la création, en janvier 2017, d'un commandement français des opérations cyber (le « CyberCom »), placé sous la responsabilité directe du chef d'état-major des armées.

Ministre de la Cyberdéfense

C'est donc un Jean-Yves Le Drian, « ministre de la Cyberdéfense », qui a passé la journée de lundi en Bretagne. Il a commencé par inaugurer officiellement le Pôle d'excellence cyber à Rennes. Cette association regroupe les chercheurs, les écoles et universités, les entreprises, les collectivités et les industriels qui œuvrent dans le numérique, la cybersécurité et la cyberdéfense.

Deuxième inauguration, un peu plus tard, dans les locaux de la DGA (direction générale de l'armement), à Bruz, au sud de Rennes. C'est ici que sont mis au point tous les systèmes d'information et de communication et les équipements électroniques des forces armées.

Le bâtiment baptisé Louis Pouzin – du nom d'un ingénieur français, précurseur d'Internet – est un bâtiment « de haute qualité cyber » qui accueille 270 experts sur 9 000 m². Il est équipé de plus de 7 000 capteurs de sécurité, de 4 000 prises de réseau, dont 2 000 en fibre optique, le tout enveloppé dans 7 000 m³ de béton. Ici, des ingénieurs travaillent, entre autres, à détecter et à mettre hors d'état de nuire, les ennemis qui veulent capter les conversations téléphoniques des personnalités françaises, ou qui entendent prendre la main, à distance, sur la conduite des véhicules...[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.



Réagissez à cet article

Original de l'article mis en page : Le Drian annonce une nouvelle doctrine en matière de cybersécurité

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 DRTEF 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

Votre caméra IP peut-elle être piratée ?



Deux équipes de chercheurs ont découvert des failles de sécurité qui affectent des dizaines de modèles de caméras IP professionnelles et grand public.

Le malware Mirai n'a pas fini de lever des armées d'objets connectés corrompus pour lancer des attaques DDoS. Des chercheurs autrichiens de SEC Consult ont découvert que pas moins de 80 modèles de caméras IP Sony étaient accompagnées de backdoor d'origine exploitable par des pirates.

Les modèles IPELA Engine de Sony affectés

Les experts de SEC Consult ont précisément découvert deux comptes utilisateurs, et leurs mots de passe, non documentés, pour accéder aux caméras IPELA Engine du constructeur japonais. Des systèmes de vidéo surveillance principalement utilisés par les entreprises et les autorités. Ces comptes, baptisés « primana » et « debug » installés par défaut, pourraient être utilisés par des pirates pour prendre le contrôle du serveur Web intégré dans le périphérique depuis Internet (via Telnet/SSH, les services de commandes à distance des objets connectés) en plus d'un accès depuis le réseau local.

Ces « portes dérobées » sont généralement introduites par les développeurs du constructeur à des fins de maintenance ou de test à distance. Ou parfois par des organisations étatiques (comme dans le cas de la backdoor de la NSA sur des routeurs Juniper). Un accès distant qui se transforme en faille de sécurité quand il tombe entre de mauvaises mains (ce qui fut le cas pour Juniper, notamment).

Le correctif de Sony à appliquer en urgence

Pour SEC Consult, il ne fait aucun doute que ces accès backdoor « permettent à un attaquant d'exécuter du code arbitraire sur les caméras IP concernées [et les] utiliser pour pénétrer le réseau et lancer d'autres attaques, perturber la fonctionnalité de l'appareil, envoyer des images manipulées, ajouter des caméras dans un botnet type Mirai ou espionner les gens ». La référence à Mirai n'est pas neutre. Le malware s'était emparé de centaines de milliers d'objets connectés, essentiellement des caméras IP, pour lancer des attaques contre le fournisseur de services DNS Dyn, des clients d'OVH ou encore le site du journaliste spécialisé en sécurité Brian Krebs.

Sony a fourni une mise à jour du firmware. A installer avant que des individus malveillants ne se chargent de reconfigurer l'accès des caméras. Selon l'outil en ligne Censys.io, plus de 4 500 de ces caméras Sony vulnérables sont accessibles directement depuis Internet. Dont 1 510 aux Etats-Unis et 256 en France.

Des centaines de milliers de caméras résidentielles

Sony est loin d'être le seul acteur concerné par la sécurité de ses caméras IP. En parallèle, des chercheurs de la firme israélienne Cybereason déclarent avoir découvert au moins deux failles zero day dans une douzaine de familles de caméras IP vendues en marque blanche dans la grande distribution et notamment sur eBay ou Amazon. D'une part, ils ont identifié que le mot de passe du compte par défaut était le même pour tous les modèles de périphérique (« 888888 » en l'occurrence pour l'identifiant « admin »). Mot de passe qu'il est impossible de renforcer puisque le système refuse la combinaison de différents types de caractères (soit uniquement des chiffres, soit des caractères en minuscule ou en majuscule). Une fois identifié, l'utilisateur peut injecter des commandes dans la caméra à partir d'un serveur Web.

D'autre part, les experts ont trouvé un moyen d'accéder à l'objet même si celui-ci est protégé derrière un firewall, en passant par le serveur web du vendeur qui offre un service Cloud (pour visualiser les images à distance sur un PC ou smartphone). Les chercheurs ne détaillent pas la façon dont ils ont procédé. Mais, sur leur blog, ils assurent que « cet exploit affecte des centaines de milliers de caméras dans le monde entier et nous ne voulons pas que les personnes malintentionnés utilisent nos recherches pour attaquer des gens ou utiliser ces caméras dans de futures attaques botnet ».[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, contenu, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DCTEF n°18 0361 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Original de l'article mis en page : Backdoor et Zero Days pour plusieurs milliers de caméras IP

Une entreprise touchée toutes les 40 secondes par une attaque par Ransomware en 2016

Denis JACOPINI



vous informe

Une entreprise
touchée toutes
les 40 secondes
par une attaque
par Ransomware
en 2016

Entre janvier et septembre 2016, la fréquence des attaques de ransomware contre les entreprises a triplé, passant d'une toutes les deux minutes une toutes les 40 secondes. Pour les particuliers, cet intervalle s'est réduit de 20 à 10 secondes. Avec l'apparition de plus de 62 nouvelles familles de logiciels rançonneurs au cours de l'année, le ransomware est la menace désignée comme fait marquant de l'année 2016. La rubrique Story of the Year fait partie de l'édition annuelle du Kaspersky Security Bulletin retraçant les principales menaces et statistiques de l'année écoulée et établit des prévisions sur ce que nous réserve 2017.

Le ransomware est devenu un réel business

Entre autres choses, 2016 a révélé à quel point le modèle RaaS (Ransomware as a Service) séduit désormais les criminels qui ne possèdent pas les compétences ou les ressources nécessaires pour développer leur propre malware ou n'en ont tout simplement pas envie. Le principe consiste pour les créateurs du code malveillant à offrir celui-ci « à la demande », en se bornant à vendre des versions modifiées à leurs clients qui les diffusent via du spam ou des sites web et reversent une commission à l'auteur, le principal bénéficiaire financier. « Le modèle classique de l'affiliation paraît aussi efficace pour le ransomware que pour les autres types de malware. Les victimes paient souvent la rançon, de sorte que l'argent coule à flots. Inévitablement, cela a conduit à l'apparition quasi quotidienne de nouveaux logiciels de cryptage », commente Fedor Sinitsyn, analyste senior en malware chez Kaspersky Lab.

L'évolution du ransomware en 2016

En 2016, le ransomware a poursuivi ses ravages à travers le monde, devenant de plus en plus élaboré et diversifié pour renforcer son emprise sur les données, les appareils, les particuliers et les entreprises :

- Les attaques sur les entreprises ont nettement augmenté. Selon l'étude Kaspersky Lab, une entreprise sur cinq au niveau mondial a subi un incident de sécurité informatique à la suite d'une attaque de ransomware et une petite entreprise sur cinq n'a jamais récupéré ses fichiers, même après avoir versé une rançon.
- Si certains secteurs d'activité ont été plus durement touchés que d'autres, notre étude indique que personne n'est véritablement épargné par le risque : le plus fort taux d'attaques frappe l'enseignement (de l'ordre de 23 %) et le plus faible, la grande distribution et les loisirs (16 %).
- Le ransomware « éducatif », conçu pour donner aux administrateurs système un outil permettant de simuler des attaques de ce type, a été rapidement et impitoyablement exploité par des criminels, donnant notamment naissance à Ded_Cryptor et Fantom.
- Parmi les méthodes de rançonnage observées pour la première fois en 2016 figure le cryptage de disque, consistant pour les auteurs des attaques à bloquer l'accès, non pas à quelques fichiers, mais à la totalité d'entre eux simultanément. Petya Dcryptor, alias Mamba, va encore plus loin en verrouillant l'ensemble du disque dur, grâce à des attaques de mots de passe par force brute pour accéder à distance aux appareils des victimes.
- Le ransomware Shade a montré sa capacité à changer d'approche vis-à-vis d'une victime si l'ordinateur infecté s'avère appartenir à des services financiers, pour télécharger et installer un spyware au lieu de crypter les fichiers.
- Les codes malveillants ont sensiblement perdu de leur qualité : c'est ainsi que de simples chevaux de Troie rançonneurs, présentant des erreurs de programmation et des fautes grossières dans les demandes de rançon, multiplient les risques pour les victimes de ne jamais récupérer leurs données...[lire la suite]

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

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

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



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

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRETEP 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 : Ransomware : Kaspersky Lab recense une attaque toutes les 40 secondes contre les entreprises en 2016 – Global Security Mag Online

Naissance de l'intelligence artificielle idiote



La course à la maîtrise de l'intelligence artificielle s'accélère. Cette semaine Uber a acquis Geometric Intelligence, une start-up qui va lui permettre d'atteindre une nouvelle dimension dans cette discipline...[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 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

Alerte ! Des publicités Internet contaminées par des malwares

	<p>Alerte ! Des publicités Internet contaminées par des malwares</p>
---	---

De très nombreux sites Internet à forte notoriété ayant des millions de visiteurs quotidiens sont touchés. Les systèmes de détection ESET montrent qu'au cours des deux derniers mois, Stegano a été affiché auprès de plus d'un million d'utilisateurs. Stegano se cache dans les images publicitaires affichées sur les pages d'accueil des sites Internet.

Bonjour,

Depuis le début du mois d'octobre 2016, des cybercriminels ciblent les utilisateurs d'Internet Explorer et analysent leur ordinateur pour détecter les vulnérabilités dans Flash Player. En exploitant leurs failles, ils tentent de télécharger et d'exécuter à distance différents types de malwares.

Ces attaques se rangent dans la catégorie des publicités malveillantes, c'est-à-dire que des codes malicieux sont distribués via des bannières publicitaires. La victime n'a même pas besoin de cliquer sur la publicité : il suffit qu'elle visite un site Internet l'affichant pour être infecté. Elle est alors renvoyée automatiquement vers un kit d'exploitation invisible permettant aux cybercriminels d'installer à distance des malwares sur son ordinateur. Vous trouverez ci-joint notre infographie expliquant la technique utilisée par Stegano pour infecter les ordinateurs.

« Certaines des charges utiles que nous avons analysées comprennent des chevaux de Troie, des portes dérobées et des logiciels espions, mais nous pouvons tout aussi bien imaginer que la victime se retrouve confrontée à une attaque par ransomware, » explique Robert Lipovsky, senior malware researcher chez ESET. « Cette menace montre combien il est important d'avoir un logiciel entièrement patché et d'être protégé par une solution de sécurité efficace et reconnue. Si l'utilisateur applique ces recommandations, il sera protégé contre ce genre d'attaque, » poursuit Robert Lipovsky.

« Stegano » fait référence à la sténographie, une technique utilisée par les cybercriminels pour cacher une partie de leur code malveillant dans les pixels d'images présents dans les bannières publicitaires. Ceux-ci sont masqués dans les paramètres contrôlant la transparence de chaque pixel. Cela entraîne un changement mineur des tons de l'image, rendant ces derniers invisibles à l'œil nu pour la victime potentielle.

Afin d'éviter de se retrouver infecté par le malware Stegano, ESET recommande aux utilisateurs de protéger leurs machines avec une solution de sécurité fiable et de mettre à jour les applications et le système d'exploitation.

Pour plus d'informations sur Stegano, nous vous invitons à consulter les deux articles suivants venant de WeliveSecurity. Le premier est l'analyse technique détaillée de Stegano, le second est une interview de Robert Lipovsky, Senior malware researcher chez ESET, expliquant la menace pour le grand public. Nous nous tenons à votre disposition pour plus de détails.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Denis JACOPINI réalise des audits et anime dans toute la France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.

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



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, contenus, 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 : Le malware Stegano infecte les machines à l'insu de ses victimes

Les « robots-avocats » : quand l'intelligence artificielle facilite les démarches juridiques

File not found

Why am I seeing this? ift.tt/fnf

Les « robots-
avocats » : quand
l'intelligence
artificielle
facilite les
démarches
juridiques

Jump to Navigation -A+A Revue de presse 6 décembre 2016 AVOCAT
www.franceinfo.fr, 5 déc....[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 **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** 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

Et si la publicité sur Internet était aussi infectée par des malwares ?

	<p>Et si la publicité sur Internet était aussi infectée par des malwares ?</p>
---	--

Les chercheurs ESET viennent de découvrir Stegano, un nouveau kit d'exploitation se propageant via des campagnes publicitaires. De très nombreux sites Internet à forte notoriété ayant des millions de visiteurs quotidiens sont touchés.

Les systèmes de détection ESET montrent qu'au cours des deux derniers mois, Stegano a été affiché auprès de plus d'un million d'utilisateurs. Stegano se cache dans les images publicitaires affichées sur les pages d'accueil des sites Internet.

Depuis le début du mois d'octobre 2016, des cybercriminels ciblent les utilisateurs d'Internet Explorer et analysent leur ordinateur pour détecter les vulnérabilités dans Flash Player. En exploitant leurs failles, ils tentent de télécharger et d'exécuter à distance différents types de malwares.

Ces attaques se rangent dans la catégorie des publicités malveillantes, c'est-à-dire que des codes malicieux sont distribués via des bannières publicitaires. **La victime n'a même pas besoin de cliquer sur la publicité** : il suffit qu'elle visite un site Internet l'affichant pour être infecté. Elle est alors renvoyée automatiquement vers un kit d'exploitation invisible permettant aux cybercriminels d'installer à distance des malwares sur son ordinateur.

« Certaines des charges utiles que nous avons analysées comprennent des chevaux de Troie, des portes dérobées et des logiciels espions, mais nous pouvons tout aussi bien imaginer que la victime se retrouve confrontée à une attaque par ransomware, » explique Robert Lipovsky, senior malware researcher chez ESET. « Cette menace montre combien il est important d'avoir un logiciel entièrement patché et d'être protégé par une solution de sécurité efficace et reconnue. Si l'utilisateur applique ces recommandations, il sera protégé contre ce genre d'attaque, » poursuit Robert Lipovsky.

« Stegano » fait référence à la sténographie, une technique utilisée par les cybercriminels pour cacher une partie de leur code malveillant dans les pixels d'images présents dans les bannières publicitaires. Ceux-ci sont masqués dans les paramètres contrôlant la transparence de chaque pixel. Cela entraîne un changement mineur des tons de l'image, rendant ces derniers invisibles à l'œil nu pour la victime potentielle.

Afin d'éviter de se retrouver infecté par le malware Stegano, ESET recommande aux utilisateurs de protéger leurs machines avec une solution de sécurité fiable et de mettre à jour les applications et le système d'exploitation.

Pour plus d'informations sur Stegano, nous vous invitons à consulter les deux articles suivants venant de WliveSecurity. Le premier est l'analyse technique détaillée de Stegano, le second est une interview de Robert Lipovsky, Senior malware researcher chez ESET, expliquant la menace pour le grand public. Nous nous tenons à votre disposition pour plus de détails.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Denis JACOPINI réalise des audits et anime dans toute la France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.

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



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 : Boîte de réception (31) – denis.jacopini@gmail.com – Gmail

Le FBI a désormais le droit de pirater n'importe quel ordinateur dans le monde !



Le FBI a
désormais
le droit
de pirater
n'importe
quel
ordinateur
dans le
monde !

Le FBI est désormais doté de nouveaux pouvoirs, à savoir l'extension de ses capacités actuelles en matière de piratage informatique. Sur la base d'un mandat spécial, les agents du bureau pourront s'introduire sur n'importe quel ordinateur, situé aux États Unis mais également dans le monde.



Applicable dès aujourd'hui, la réforme est à nuancer. En effet, l'application de la **règle 41** du *Federal Rules of Criminal Procedure* (équivalent de notre code de procédure pénale) est strictement encadrée par un **juge fédéral**, qui instruit au préalable le dossier. Il s'agira d'une procédure **exceptionnelle**, la spécificité de l'affaire devant justifier de l'**opportunité** d'une telle mesure.

L'intervention reste, en effet, une **intrusion dans la vie privée des gens** –qui ne sont pas forcément coupables de ce qui pourrait leur être reproché. Cela n'empêche pas les politiques américains de s'inquiéter sur des atteintes aux libertés personnelles, des abus possibles ou d'éventuelles finalités politiques.

Précisons que ce pouvoir n'est pas unique en son genre, il existe déjà en France où il est actuellement renforcé du fait du plan *vigipirate* au même titre que certains pouvoirs de surveillance.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Denis JACOPINI réalise des audits et anime dans toute la France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.

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



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 : Les nouveaux pouvoirs de
piratage informatique du FBI