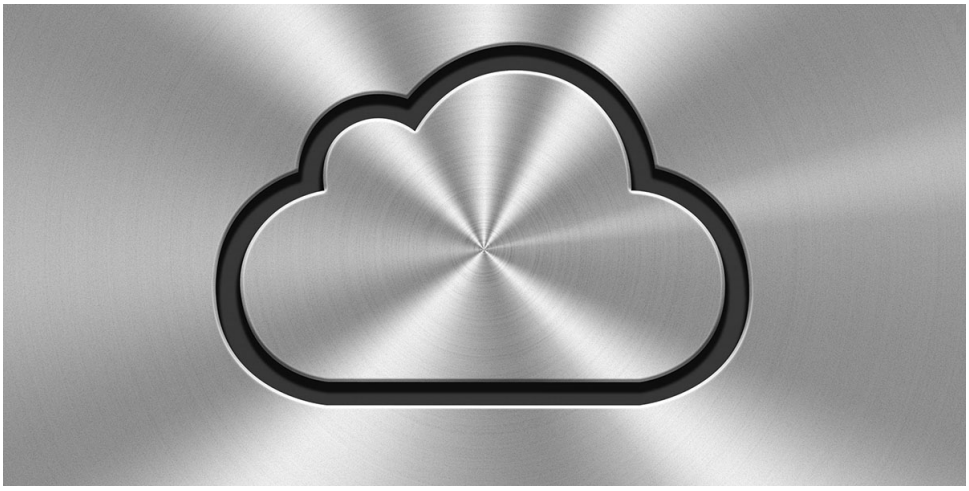
18 mois de prison pour le pirate qui a publié des photos intimes de célébrités



18 mois de prison pour le pirate qui a publié des photos intimes de célébrités

Aux États-Unis, la justice a condamné à un an et demi de prison l'auteur d'une vaste campagne de phishing qui a débouché sur la diffusion de photos intimes de plusieurs dizaines de célébrités en 2014. Un an et demi de prison ferme.…[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.

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

Contactez-nous

Réagissez à cet article

Multiples vulnérabilités dans les produits Apple

…[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.

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

Contactez-nous

Réagissez à cet article

Faille de sécurité pour le

PARTI SOCIALISTE – Avertissement Public de la CNIL

Faille de sécurité pour le PARTI SOCIALISTE – Avertissement Public de la CNIL

Le 26 mai 2016, la CNIL a été informée de l'existence d'une faille de sécurité entraînant une fuite de données sur le site du Parti Socialiste. Lors d'un contrôle en ligne réalisé dès le lendemain, la CNIL a constaté que les mesures garantissant la sécurité et la confidentialité des données des primo-adhérents du PS étaient insuffisantes.

Les contrôleurs de la CNIL ont en effet pu accéder librement, par la saisie d'une URL, à la plateforme de suivi des primo-adhésions au Parti Socialiste effectuées en ligne. Ils ont notamment pu prendre connaissance des éléments suivants : nom, prénom, adresses électronique et postale, numéros de téléphone fixe et mobile, date de naissance, adresse IP, moyen de paiement et montant de la cotisation de certains adhérents.
Cette faille avait été rendue possible par l'utilisation d'une technique non sécurisée d'authentification à la plateforme. Elle a concerné plusieurs dizaines de milliers de primo-adhérents.
Alerté le même jour par la CNIL de cette faille, le PS a immédiatement pris les mesures nécessaires pour y mettre fin.
Un second contrôle réalisé cette fois dans les locaux du PS le 15 juin 2016, destiné à comprendre les raisons de la faille, a permis de constater que les mesures élémentaires de sécurité n'avaient pas été mises en œuvre initialement. En effet, il n'existait pas de **procédure d'authentification** forte au site ni **de système de traçabilité** permettant notamment d'identifier l'éventuelle exploitation malveillante de la faille.
Le contrôle a aussi permis de constater que le PS conservait sans limitation de durée les données personnelles de la plateforme, ce qui avait accru la portée de la fuite de données. La base active contenait des demandes d'adhésion effectuées depuis 2010 qui auraient dû a minima être stockées en archive.

En conséquence, la Présidente de la CNIL a décidé d'engager une procédure de sanction en désignant un rapporteur. La formation restreinte de la CNIL a prononcé un avertissement public car elle a estimé que le Parti Socialiste avait manqué à ses obligations :
• de veiller à la sécurité des données à caractère personnel des primo-adhérents, en méconnaissance de l'article 34 de la loi Informatique et Libertés ;
• de fixer une durée de conservation des données proportionnelle aux finalités du traitement en méconnaissance de l'article 6-5 de la loi Informatique et Libertés.

Enfin, la formation restreinte a décidé de rendre publique sa décision en raison de la gravité des manquements constatés, du nombre de personnes concernées par la faille et du caractère particulièrement sensible des données en cause qui permettaient notamment d'avoir connaissance de leurs opinions politiques.

Pour en savoir plus

Délibération de la formation restreinte n°2016-315 du 13 octobre 2016 prononçant un avertissement à l'encontre du PARTI SOCIALISTE
[PDF-312.22 Ko]

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 le 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.

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Faille de sécurité de données sensibles en ligne : Avertissement public pour le PARTI SOCIALISTE | CNIL

Des attaques DDoS de plus de 10 Tbit/s en vue ?

L'arsenal des attaques DDoS (Distributed Denial of Service) vient de s'enrichir d'une nouvelle arme : le LDAD.…[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.

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

Contactez-nous

Réagissez à cet article

ESET sensibilise les TPE aux risques informatiques et au RGPD

ESET sensibilise les TPE aux risques informatiques et au RGPD

Par manque de sensibilisation à la sécurité informatique, les TPE qui ne disposent de moyens humains dédiés, s'exposent à un risque plus élevé pouvant avoir de graves conséquences pour leur entreprise.

« Récemment, un cabinet médical s'est adressé à nous après s'être retrouvé infecté par un ransomware causant la perte de l'ensemble des données de ses patients. Il n'avait pas installé de solutions de sécurité car il n'en voyait pas l'utilité. Il devient urgent que les TPE prennent conscience de l'importance des données qu'ils détiennent », explique Benoît Grunemwald, Directeur des Opérations chez ESET France.
Avec l'arrivée du RGPD (2018) les TPE devront, au même titre que les grands comptes, s'approprier le texte qui vise à protéger les données personnelles qu'ils détiennent. A ce titre, des mesures imposées par le règlement européen devront être mises en place sous peine de sanctions.
La première démarche consiste à réaliser une cartographie des données et attribuer un niveau de sensibilité aux informations (voir pièce jointe). Pour appliquer les mesures, l'expert juridique viendra en soutien des actions entreprises par la société. Il restera alors la mise en place des systèmes de sécurité.
Les experts ESET ont mis au point un produit accessible aux besoins des TPE, ne nécessitant pas une connaissance accrue des systèmes de sécurité : ESET Smart Security Premium.
Au-delà des fonctions primaires qu'il propose (antivirus, anti-phishing, protection contre les attaques par script, antispam…), nos experts ont ajouté 3 fonctions permettant d'accompagner ces entreprises dans la mise en place de systèmes de sécurité répondant aux exigences du RGPD :
• Le chiffrement des données pour éviter les fuites éventuelles
• La protection du réseau domestique afin de connaître l'identité des appareils connectés
• Le gestionnaire de mots de passe afin de protéger tous les accès par des mots de passe efficaces
…[lire la suite]

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 le 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.

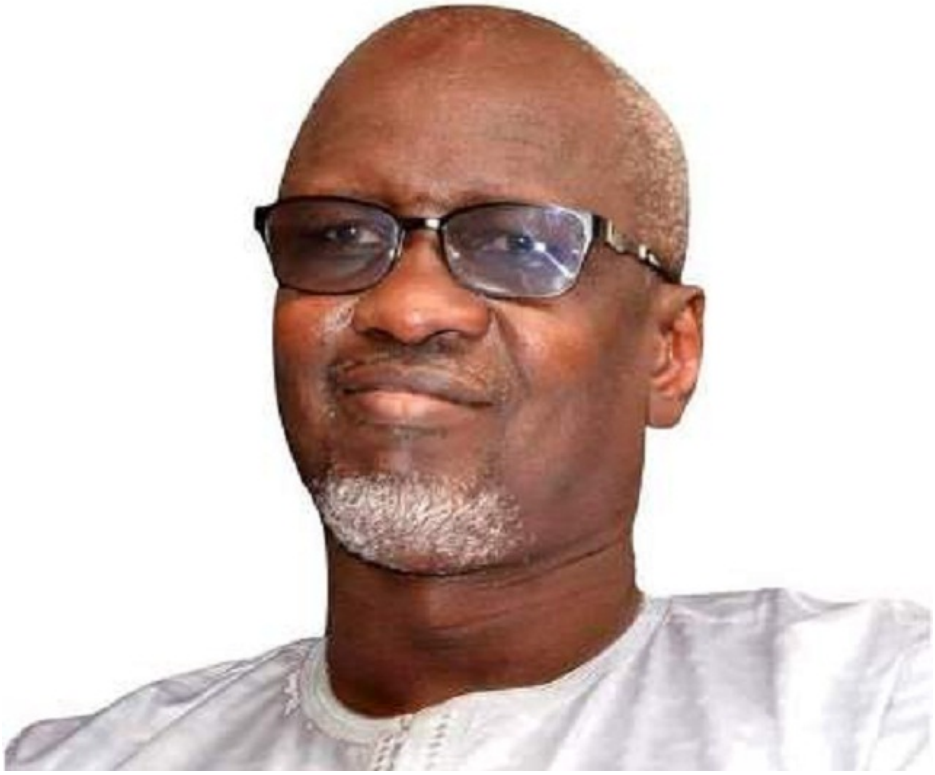
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : La sécurité Internet

Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie



Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie

L'enquête sur le piratage de la plate-forme de transfert d'argent de la Poste se poursuit. Après avoir entendu plusieurs responsables de la boite, la section de recherches de Colobane (Dakar) a reçu hier dans ses locaux le directeur général, Ciré Dia. D'après le quotidien sénégalais L'Observateur qui donne l'information dans sa livraison du jour, un important arsenal technique a été mis à contribution pour remonter la filiale.

En s'introduisant dans le système de transfert international du réseau, les cybercriminels avaient emporté près de 400 millions de francs CFA. Un coup dur pour la société qui traverse actuellement des moments difficiles selon L'Enquête qui fait état de problèmes de recouvrement des montants dus par les sociétés de transfert d'argent au groupe, des montants estimés entre 4 et 5 milliards CFA.

Réagissez à cet article

Original de l'article mis en page : Enquête sur le piratage à La Poste du Sénégal: le DG auditionné par la Gendarmerie hier | CIO MAG

Pourquoi les objets connectés sont un danger pour l’Internet ?

Pourquoi les objets connectés sont un danger pour l’Internet ?

Plusieurs grands sites Internet ont vu leurs services perturbés vendredi soir suite à une attaque contre une partie de l'infrastructure du réseau global. Cette attaque est particulièrement inquiétante car elle n'est que la dernière manifestation d'un phénomène en plein essor : le piratage d'objets connectés mal sécurisés pour constituer des réseaux offensifs. Un fléau qu'il sera difficile d'endiguer.

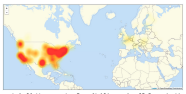
Une attaque de grande ampleur a eu lieu vendredi 21 octobre 2016, mettant hors service pendant quelques heures plusieurs grands sites Internet comme Amazon, Netflix, Twitter, Reddit, Spotify ou Tumblr. Ces sites n'étaient pas directement sous le coup d'une attaque, ils ont été les victimes collatérales d'une attaque contre Dyn, une entreprise dont les services font d'elle une infrastructure critique d'Internet : Dyn gère un service DNS (système de noms de domaine), qui permet de corréler un nom de domaine (comme « usine-digitale.fr ») en une adresse IP et vice versa.

UNE ATTAQUE BASIQUE MAIS SURPUISSANTE GRÂCE AUX OBJETS CONNECTÉS

Ce qui est notable ici, c'est qu'il ne s'agissait pas d'une attaque sophistiquée, soigneusement mise en oeuvre par un groupe d'experts. Non, il s'agissait d'une attaque par déni de service distribué (DDoS) – autrement dit une attaque ayant pour but de rendre un service indisponible en le noyant d'informations inutiles – s'appuyant principalement sur le botnet Mirai, qu'a identifié le cabinet d'analyse Flashpoint. Les botnets ne sont pas nouveaux, il s'agit de réseaux de machines dont un malware a pris le contrôle et qui peuvent être utilisés à tout moment pour mener une attaque coordonnée. Traditionnellement, les machines infectées étaient des ordinateurs dont les mises à jour de sécurité n'avaient pas été faites. Mais les progrès en matière d'antivirus et de solutions d'atténuation d'attaques DDoS limitent aujourd'hui sérieusement l'intérêt d'utiliser un botnet constitué d'ordinateurs (long et difficile à mettre en place) pour ce type d'opération (peu rentable car les rançons sont désormais rarement payées).

MIRAI, COMMENT ÇA MARCHE ?

La différence avec Mirai, c'est qu'il s'attaque aux objets connectés. Son *modus operandi* est on ne peut plus simple : il parcourt Internet en cherchant à se connecter à toutes les adresses telnet qu'il trouve avec une liste de 62 logins/mots de passe par défaut (dont le classique admin/admin). Une fois l'appareil infecté, Mirai en bloque certains ports pour empêcher qu'on en reprenne le contrôle. Le malware est basique, rapide, efficace, et surtout disponible gratuitement pour quiconque souhaite s'amuser avec, car son créateur en a rendu le code public. De plus, contrairement aux ordinateurs, un botnet d'objets connectés n'a aucune utilité réelle autre qu'effectuer des attaques par déni de service. Le fait que les objets connectés ont tendance à être allumés 24h/24 et 7j/7 facile aussi cet usage.



Impact de l'attaque contre Dyn, établie par Level3 Communications

CAMÉRAS ET ENREGISTREURS NUMÉRIQUES EN CAUSE

Le résultat est une arme dont la puissance est absolument démesurée par rapport à son accessibilité. En septembre 2016, le blog du journaliste spécialisé Brian Krebs avait été frappé par une attaque record atteignant un débit de 620 Gb/s. Une semaine plus tard, c'est l'hébergeur français OVH qui avait été visé, avec une puissance de frappe estimée à 1,5 Tb/s. L'attaque contre Dyn, survenue un mois plus tard, semble être à nouveau montée d'un cran. Quels sont les objets connectés utilisés par Mirai ? On y trouve beaucoup de caméras de surveillance et d'enregistreurs numériques (DVR), principalement fabriquées par une seule entreprise : Hangzhou XiongMai Technology. A noter que d'autres botnets pourraient également avoir participé à l'attaque. On connaît l'existence d'au moins un autre malware au fonctionnement similaire à Mirai, baptisé Bashlight.

PAS DE SOLUTION EN L'ÉTAT

Le problème est que ces appareils sont pratiquement impossible à protéger en l'état. Pour une partie d'entre eux, les identifiants sont codés « en dur » dans le firmware et ne sont pas modifiables. Et même pour les autres, le fait qu'ils utilisent le protocole telnet (en ligne de commande, sans interface graphique) les rend difficile à configurer pour les utilisateurs. D'après une analyse de Flashpoint, plus de 515 000 objets connectés seraient aujourd'hui vulnérables et susceptibles d'être incorporés dans un botnet. Certains experts ont proposé des solutions radicales, notamment de développer un malware plus rapide que Mirai, capable d'infecter un objet connecté vulnérable avant lui lors d'un redémarrage de ce dernier, et de le saborder pour le mettre définitivement hors service. Une mesure aussi drastique qu'illégale, mais qui souligne à quel point la situation désempare l'industrie.

Il y a eu beaucoup de mises en garde face au danger que représente l'Internet des Objets, mais, comme souvent, celles-ci n'ont servi à rien. Puisqu'il est clair que l'essor des objets connectés n'est pas prêt de s'arrêter, il est impératif que les acteurs majeurs de cette industrie mettent en place des normes et des bonnes pratiques au plus tôt, faute de quoi l'Internet des Objets continuera à scléroser l'Internet tout court, et ce de plus en plus souvent.

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

Le Net Expert INFORMATIQUE

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Le retour des botnets ou pourquoi les objets connectés sont un danger pour l'Internet

---

Que prévoit la loi pour les Hackers éthiques ?

Que prévoit la loi pour les Hackers éthiques ?

La loi pour une République numérique protège les hackers éthiques et confirme le rôle central de l'Anssi dans le signalement de failles informatiques. Les explications de l'avocat François Coupez.

En complétant le code de la défense, la loi du 7 octobre 2016 pour une République numérique entérine la protection des hackers éthiques. En tout cas ceux qui signalent une faille informatique découverte par leurs soins à l'Agence nationale pour la sécurité des systèmes d'information (Anssi). La législation confirme ainsi le rôle central de cette dernière dans le signalement des vulnérabilités.
« Ce texte va surtout permettre une officialisation », explique à *Silicon.fr* François Coupez, avocat associé du cabinet Atipic. *« L'Anssi apparaît bien comme le second point de contact officiel, en plus du responsable du système d'information objet des vulnérabilités »*. Ce point de contact *« est utile pour les cas où les 'hackers éthiques' supposeraient qu'ils ne peuvent joindre directement l'entité dont le SI est vulnérable, quelle qu'en soit la raison : responsable supposé peu réceptif, responsable déjà contacté en vain, etc. »*.

Protéger le hacker dit « éthique »

Pour distinguer le hacker éthique du pirate (l'article 323-1 du code pénal sanctionne le piratage frauduleux d'au moins deux ans d'emprisonnement et de 60 000 euros d'amende), l'article 47 de la loi numérique complète le code de la défense par un article L2321-4 ainsi rédigé :
« Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.
L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.
L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

Sécuriser les agents de l'Anssi

Rappelons que l'article 40 du code pénal cité dans cet article L2321-4 indique : *« Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. »*
Or, dans la loi portée par Axelle Lemaire, cette obligation prévue à l'article 40 ne s'applique pas aux *white hats*. Ce qui arrivait déjà, en fait, avant la promulgation du texte. *« D'après ce qu'a pu indiquer à certaines occasions l'Anssi elle-même, la pratique interne était déjà de ne pas appliquer l'article 40 dans les hypothèses similaires à celles visées par cet article L2321-4 du code de la défense nouvellement créé. Et ce afin de faciliter les remontées d'informations. Ce que la loi République numérique légitime dorénavant via cet article, et c'est une très bonne chose pour la sécurité juridique des agents de l'Anssi »*, ajoute François Coupez…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Hacker éthique : la législation française enfin claire ?

Cash investigation ne comprend rien à la cybersécurité

Cash investigation ne comprend rien à la cybersécurité

La cybersécurité est une science complexe qui croise les compétences techniques et la compréhension des mécanismes humains. L'art de la guerre numérique dépasse de très loin ce que Cash Investigation a tenté de montrer.

La cybersécurité est un sujet suffisamment sensible pour qu'il mérite d'être traité par les journalistes avec rigueur et sérieux. En la matière, l'approximation et la sous-estimation de sa complexité conduisent inévitablement à des contre-vérités médiatiques et à des biais de représentation.
C'est précisément ce que l'émission de France 2 Cash Investigation Marchés publics : le grand dérapage nous a fourni le mardi 18 octobre à 20h55, tant les approximations et les contre-vérités se succédaient à grande vitesse tout au long du reportage sur le système d'exploitation des ordinateurs du Ministère de la Défense.
Je dois avouer qu'il en faut en général beaucoup pour me choquer mais que ce beaucoup a été très vite atteint par l'équipe de Cash Investigation ! Jamais réalité n'avait été à ce point tordue et déformée dans l'unique but d'entrer par le goulot étroit du format préfabriqué de la désinformation. En clair, on a voulu se payer les balourds du Ministère de la Défense et les militaires qui ont choisi le système d'exploitation Windows (Microsoft) pour équiper leurs machines…

Un piratage en trois clics ?

Pensez donc, Madame, en trois clics et deux failles de sécurité, Élise Lucet nous démontrait qu'elle pouvait prendre le contrôle des ordinateurs du Ministère de la Défense pour déclencher dans la foulée la troisième guerre mondiale…. Il est vrai qu'elle venait de pirater sans pression l'ordinateur de l'un de ses collègues, avec l'aide de deux experts en cybersécurité de l'ESIEA. Et comme chacun le sait, si l'opération fonctionne avec la machine Windows de madame Michu, ça marchera tout pareil avec les machines de la Grande Muette.
Dans le cadre d'un renouvellement de contrat, Microsoft a remporté en 2013 le marché public du Ministère de la Défense concernant l'équipement en systèmes d'exploitations du parc informatique des Armées. Windows est donc installé sur 200 000 ordinateurs de l'armée française.
Partant de cette réalité, Élise Lucet et son équipe en ont déduit que cela constituait un choix risqué en matière de cybersécurité & cyberdéfense tant ce système d'exploitation est truffé de vulnérabilités et de Back Doors (portes dérobées) installées par les méchants espions américains de la NSA.

Le « piège » de Microsoft

En conclusion, toujours selon Élise Lucet, les militaires français sont tombés dans le piège tendu par Microsoft qui dispose désormais de toutes les entrées possibles pour la prise de contrôle à distance des ordinateurs sensibles du Ministère et de leurs secrets Défense. La théorie du complot n'est pas très éloignée dans tout cela, surtout lorsque l'hypothèse d'Élise Lucet se trouve plus ou moins confirmée par les déclarations de l'expert cryptologue Éric Filiol, retraité des services de renseignement et actuellement directeur du centre de recherche en cybersécurité de l'ESIEA.
Ce que dit Éric Filiol durant ses courtes interventions n'est pas contestable : il effectue une démonstration de prise de contrôle à distance d'un ordinateur équipé du système Windows 7 à la suite d'un clic de l'utilisateur (la cible) sur un lien malveillant transmis par mail. La démonstration qu'il donne d'une prise de contrôle n'appelle aucune critique puisqu'elle est un classique du genre, connue de tous les étudiants préparant un Master en cybersécurité.

Quelle preuve des failles de sécurité ?

C'est l'usage qui en est fait qui devient très contestable : puisque la manipulation fonctionne sur l'ordinateur doté de Windows de mon collègue journaliste (qui, au demeurant, a le clic facile et l'antivirus laxiste), c'est qu'elle fonctionne également avec l'ensemble du parc informatique relevant du Ministère de la Défense (cqfd). Preuve est donc faite de l'incompétence des services de l'État, de services chargés de la cybersécurité des infrastructures militaires et de l'ensemble des experts, ingénieurs et chercheurs qui œuvrent chaque jour en France pour sécuriser les systèmes…
Le reportage pousse encore un peu plus loin sa courageuse investigation en allant interroger très brièvement l'Officier Général Cyberdéfense, le vice Amiral Coustillière. Ce dernier est interrogé entre deux portes sur le choix improbable d'installer Windows sur des machines qui font la guerre.

White Hat au grand cœur

N'écoutant que leur sagacité et leur expertise autoproclamée, nos journalistes hackers « White Hat » au grand cœur (donc toujours du bon côté de la Force) donnent pour finir une leçon de cyberstratégie à l'Amiral responsable de la sécurité des infrastructures numériques militaires, tout en le faisant passer pour un amateur déconnecté des réalités informatiques… C'est à ce point que l'on touche au paroxysme de la désinformation du spectateur que l'on considère comme un consommateur compulsif de dysfonctionnements et malversations étatiques…
Et bien non, Madame Lucet, non, le choix de Windows n'est pas plus ou moins défendable que celui d'un système open source. Linux et ses dérivés souffrent également de vulnérabilités, subissent des attaques et des correctifs. C'est le triste destin de tout système complexe que d'avoir été créé imparfait, ouvert aux agressions extérieures exploitées par des individus mal intentionnés ou en quête d'information.

On ne clique pas tous sur les malware

Non, Madame Lucet, ce n'est pas parce qu'un de vos collègues journalistes clique facilement sur un lien malveillant que tout le monde le fait. Ce n'est pas parce que son antivirus ne détecte pas un malware qu'aucun autre antivirus ne le détectera. Ce n'est pas parce que Windows possède des vulnérabilités que les autres systèmes d'exploitation n'en possèdent pas.
Ce n'est pas parce que Microsoft a pu transmettre ou vendre certaines données aux services gouvernementaux américains que cette firme cherche obsessionnellement à piéger l'armée française. Enfin, non chère Élise, l'armée française ne découvre pas les problématiques de sécurité numérique avec votre reportage et ne sous-estime pas les risques de vol de données sensibles. C'est quelque part faire injure aux spécialistes civils et militaires qui œuvrent quotidiennement à la défense des intérêts numériques de la nation.
La cybersécurité est une science complexe qui croise les compétences techniques et la compréhension des mécanismes humains. L'art de la guerre numérique dépasse de très loin ce que ce triste reportage a tenté de montrer.

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 le 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.

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

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Cash investigation ne comprend rien à la cybersécurité | Contrepoints

---

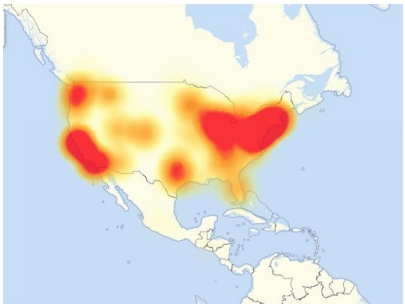
Quelques détails sur la cyberattaque massive dont ont été victime les états unis

Quelques détails sur la cyberattaque massive dont ont été victime les états unis

---

Pendant plusieurs heures, une vaste attaque informatique a paralysé de nombreux sites internet outre-Atlantique, vendredi 21 octobre.

En se réveillant vendredi 21 octobre, plusieurs millions d'Américains ont la désagréable surprise de se voir refuser l'accès à leurs sites préférés. Pendant de longues heures, impossible en effet de se connecter à **Twitter, Spotify, Amazon ou eBay**. Mais aussi à des grands médias, tels que le ***New York Times***, **CNN, le *Boston Globe*, le *Financial Times*** ou encore le célèbre quotidien anglais ***The Guardian***. En cause : une **cyberattaque massive** menée en plusieurs vagues qui a fortement perturbé le fonctionnement d'internet outre-Atlantique.
Le fait que tous ces sites mondialement connus soient hors d'accès ne révèle toutefois que la partie émergée de l'iceberg. En effet, les pirates **s'en sont pris en réalité à la société Dyn**, dont la notoriété auprès du grand public est beaucoup plus faible. Le rôle de la firme est de **rediriger les flux internet vers les hébergeurs** et traduit en quelque sorte des noms de sites en adresse IP. À 22h17, Dyn a indiqué que l'incident était résolu.



Le département de la sécurité intérieure (DHS) ainsi que le FBI ont annoncé dans la foulée **l'ouverture d'une enquête** « sur toutes les causes potentielles » de ce gigantesque piratage à l'envergure inédite. Des investigations qui s'annoncent de longue haleine, tant cette attaque se déplaçant de la côte est vers l'ouest du pays semble sophistiquée. « **C'est une attaque très élaborée**. À chaque fois que nous la neutralisons, ils s'adaptent », a expliqué Kyle Owen, un responsable de Dyn, cité sur le site spécialisé *Techcrunch*.

Qui est à l'origine de l'attaque ?

Pour l'heure, l'identité et l'origine des auteurs demeurent inconnues. Mais l'ampleur du piratage éveille les soupçons. « Quand je vois une telle attaque, je me dis que c'est un État qui est derrière », a estimé Eric o'Neill, chargé de la stratégie pour la société de sécurité informatique Carbon Black et ex-chargé de la lutte contre l'espionnage au FBI. Les regards se tournent inévitablement vers des pays comme la Russie ou la Chine, qui pourraient avoir intérêt à déstabiliser le géant américain, alors que les élections approchent.
Mais d'autres hypothèses circulent. Le site Wikileaks, qui a publié des milliers d'emails du directeur de campagne de la candidate démocrate à la présidentielle Hillary Clinton, a cru déceler dans cette attaque une marque de soutien à son fondateur Julian Assange, réfugié dans l'ambassade d'Équateur à Londres et dont l'accès à internet a été récemment coupé. « Julian Assange est toujours en vie et Wikileaks continue de publier. Nous demandons à nos soutiens d'arrêter de bloquer l'internet américain. Vous avez été entendus », a tweeté le site.

Comment les pirates ont-ils procédé ?

La technique utilisée vendredi pour plonger le web américain dans le chaos est dite de déni de service distribué (DDoS). Cette dernière consiste à rendre un serveur indisponible en le surchargeant de requêtes. Elle est souvent menée à partir d'un réseau de machines zombies – des « botnets » – elles-mêmes piratées et utilisées à l'insu de leurs propriétaires. En l'occurrence, les pirates ont hacké des objets connectés, tels que des smartphones, machines à café, des téléviseurs ou des luminaires.
« Ces attaques, en particulier avec l'essor d'objets connectés non sécurisés, vont continuer à harceler nos organisations. Malheureusement, ce que nous voyons n'est que le début en termes de 'botnets' à grande échelle et de dommages disproportionnés », prédit Ben Johnson, ex-hacker pour l'agence américaine de renseignement NSA et cofondateur de Carbon Black.

Quelles peuvent être les conséquences ?

La société Dyn était préparée à ce type d'attaque et a pu résoudre le problème dans des délais relativement brefs. Mais **les conséquences pourraient être bien plus graves** dans les secteurs de la finance, du transport ou de l'énergie, bien moins préparés, selon Eric o'Neill. Quelle qu'en soit l'origine, l'attaque a en effet mis en lumière **les dangers posés par l'utilisation croissante des objets connectés**, qui peuvent être utilisés à l'insu de leurs propriétaires pour bloquer l'accès à un site…[lire la suite]

Original de l'article mis en page : Trois questions pour comprendre la cyberattaque massive