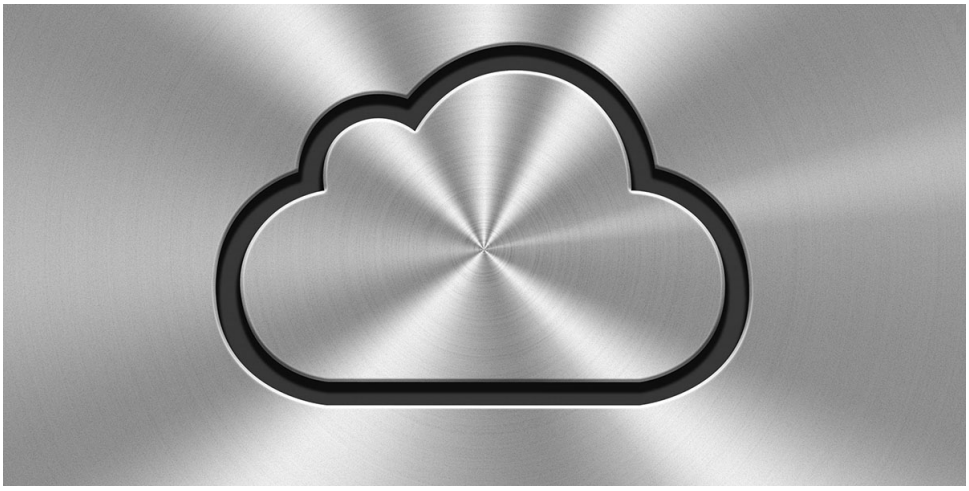
18 mois de prison pour le pirate qui a publié des photos intimes de célébrités



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

Des attaques DDoS de plus de

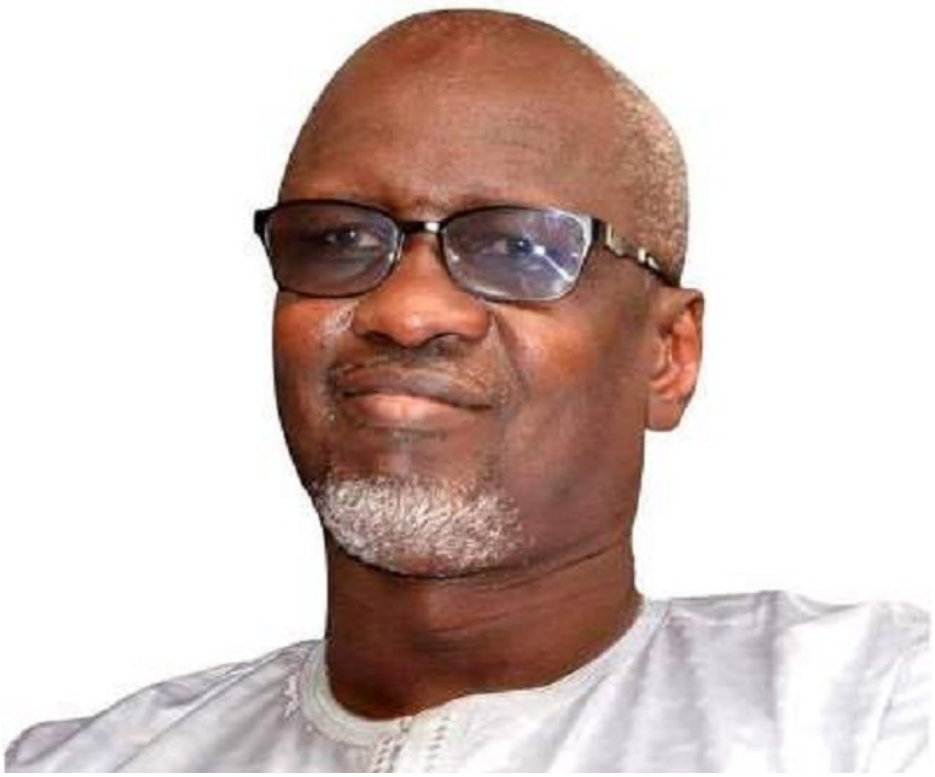
10 Tbit/s en vue ?

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.

Réagissez à cet article

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.

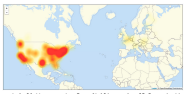
Une attaque de grande ampleur a eu lieu vendredi 21 octobre 2016, mettant hors service pendant quelques heures plusieurs grands sites Internet comme Amazon, Netflix, Twitter, Reddit, Spotify ou Tumblr. Ces sites n'étaient pas directement sous le coup d'une attaque, ils ont été les victimes collatérales 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 saboter 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 — Consultant en Cybercriminalité et en Protection des Données Personnelles

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

---

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.

Réagissez à cet article

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

---

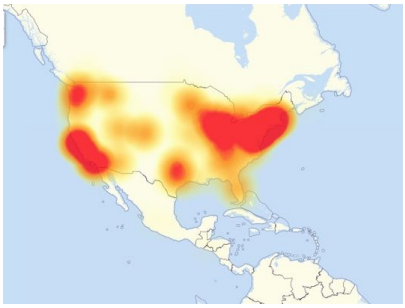
Quelques détails sur la cyberattaque massive dont ont été victime les états unis

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

Faut-il avoir peur des ransomwares ?

	Faut-il avoir peur des ransomwares ?

Depuis le premier virus détecté en 1986, le nombre d'attaque n'a cessé d'augmenter, devenant la menace la plus importante pour les entreprises.

En effet, cette forme d'attaque profite aux cybercriminels qui ont trouvé le bon filon pour gagner de l'argent. En constante mouvance, les formes d'attaques sont de plus en plus redoutables et ont généré un trafic de données important : les informations détenues par les entreprises sont désormais toutes disponibles en environnement virtuel et constituent l'élément essentiel pour l'économie de la société (données sensibles, fichiers clients, etc). Leur perte est inconcevable et cela, les cybercriminels l'ont bien compris. Au fil des ans, leurs techniques ont changé jusqu'à l'arrivée des ransomwares. Ce type d'attaque se révèle être la plus rentable pour les attaquants qui multiplient les variantes. La tendance est d'ailleurs à l'augmentation sur tous types de support connecté.
Parce que la perte de données en entreprise peut avoir des conséquences irrémédiables sur son activité si l'on prend en compte les paramètres suivants : perte de productivité, perte de données et la réputation liée à ces deux pertes, le non-paiement de factures émises, perte de confiance des salariés dans leur entreprise ; l'impact d'un ransomware peut être catastrophique. Le succès et les méthodes pour obtenir un paiement rapide de la rançon ont permis aux cybercriminels d'attirer l'attention des médias et d'entretenir ce climat de tension.
Il y a quelques mois, ESET a averti les utilisateurs qu'un nombre impressionnant d'e-mails infectés propageaient des ransomwares, submergeant ainsi les boîtes de réception dans le monde entier. Feignant de ne contenir que des fichiers inoffensifs, JS/TrojanDownloader.Nemucod essayait en réalité de forcer les victimes à télécharger et à installer des ransomwares tels que TeslaCrypt ou Locky. Cette stratégie fut efficace puisque les cybercriminels l'ont répété plusieurs fois, multipliant également les variantes utilisées tels que CTBLocker ou Filecoder.DG.
Heureusement les ransomwares ne sont pas toujours aussi dangereux que ceux cités ci-dessus. Beaucoup de cybercriminels amateurs surfent sur cette tendance et développent leur propre ransomware dont l'exécutable, de faible qualité, est facile à contrer. Ceci fut le cas de Petya et Jigsaw qu'ESET a analysé : tous deux contenaient des défauts de mise en œuvre qui ont permis aux victimes touchées de récupérer leurs fichiers sans payer un centime.

Comment vaincre cette peur du ransomware ?
Avoir peur du ransomware ne vous en protègera pas pour autant et payer la rançon ne résoudra pas forcément vos problèmes. Si vous en arrivez à ce stade, c'est que vous n'avez pas appliqué toutes les précautions nécessaires.
La meilleure façon de ne plus avoir peur des ransomwares est de se protéger avec une solution efficace et reconnue, et de s'assurer de couvrir 3 domaines complémentaires : technologique, politique de sécurité et éducation des employés. Sous l'impulsion de l'Etat et des agences de sécurité, les entreprises sont encouragées à adopter des mesures de protection. Les textes, dont le RGPD, étant là pour cadrer l'utilisation et la sécurité des données détenues par les entreprises. En particulier, les investissements dans la recherche et le développement de nouvelles technologies nécessitent un plan de sécurité permettant d'évaluer et de décrire leur sécurité.
Par conséquent, avec des attaques de plus grande envergure et l'émergence de nouvelles vulnérabilités, le plus grand défi de 2016 est de mettre l'accent sur la protection des réseaux et l'accès aux données. Les meilleures pratiques de sécurité doivent donc être appliquées pour protéger les données, les informations et la vie privée. Il s'agit là d'un travail transversal qui exige une participation active des plus hautes fonctions de l'entreprise.
Faut-il avoir peur des ransomwares ? La réponse est non pour tout dirigeant préparé à cette éventualité.
Source : Benoît Grunemwald – Directeur des Opérations ESET France

---

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 : Charts | ESET Virusradar

Les jeunes ne seraient pas plus prudents sur le web que leurs grands-parents

Les jeunes ne seraient pas plus prudents sur le web que leurs grands-parents

Selon une enquête Ipsos, les 18 – 34 ans sont les premiers touchés par les arnaques en ligne, bien devant leurs grands-parents.

Les natifs du numérique ne sont pas tout à fait aussi prudents sur le net qu'on pourrait le supposer nous disent Microsoft et Ipsos. Même s'ils sont plus à l'aise avec les nouvelles technologies que leurs aînés, les 18 – 34 ans sont également les premiers touchés par les arnaques en ligne, les fameux *scams*.

VOUS ÊTES LE 1 000 0000 0000E VISITEUR ! ! ! ! ! ! !

La moitié des victimes d'arnaque en ligne ont en effet moins de 35 ans selon une étude publiée par Ipsos. Derrière les jeunes gens, on retrouve les 36 – 54 ans qui représentent 34 % des victimes et enfin les plus vieux, plus de 55 ans, ne représentent eux que 17 % du total des victimes.

Le sondage d'Ipsos porte sur une population internationale de 12 000 personnes, dans plus de 12 pays et a été réalisée pour Microsoft.
Les arnaques du web sont aussi vieilles que la technologie, néanmoins leur prolifération ne semble guère être ralentie par les nouveaux usages. Les mails d'arnaque sont devenus des profils Facebook, des messages d'erreurs sur mobile ou d'autres hameçons modernes que l'on retrouve au fil des modes sur différentes plateformes. Si les usages changent, la présence des arnaques, elle, ne fait que s'adapter indéfiniment.
Le rapport met en lumière une des plus importantes arnaques de notre siècle, dans laquelle la victime reçoit un message prétendument adressé par Microsoft, Apple, Dell ou HP, ou d'autres firmes reconnues de la tech grand public. Il explique invariablement que l'appareil du possesseur est infecté, et que l'installation d'un logiciel tiers est nécessaire…[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 : Les jeunes ne seraient pas plus prudents sur le web que leurs grands-parents – Tech – Numerama

---

Données personnelles en danger : pourquoi il est très important de supprimer vos comptes en ligne que vous n'utilisez plus ?

Données personnelles en danger : pourquoi il est très important de supprimer vos comptes en ligne que vous n'utilisez plus ?

Atlantico : Le 22 septembre dernier, Yahoo ! révélait que 500 millions de boîtes emails avaient été piratées à la fin de l'année 2014. Quels sont les risques de se voir piraté par une intrusion via des comptes emails dont on ne se sert plus, mais toujours actifs ?

Les actions énoncées ci-dessous que pourraient mener d'éventuels pirates informatiques sont illicites et ne constituent en rien une incitation. Les communiquer a pour seul objectif de sensibiliser des utilisateurs mal informés.

Denis Jacopini : On néglige trop souvent les conséquences d'un piratage de sa propre boite e-mail.

Donnez vos identifiants et vos mots de passe à un pirate Informatique, vous verrez tout ce qu'il peut en faire…

Tout d'abord, il est possible que vous utilisiez la fonction de carnet d'adresse, notamment parce qu'elle est généralement fournie en même temps que la boite à courriers électroniques et parce que c'est du coup bien pratique. Un pirate peut alors par exemple, en votre nom (usurpation d'identité), faire croire au destinataire que c'est vous qui écrivez. Ceci pourra avoir pour effet d'inciter la victime à ouvrir une pièce jointe piégée, cliquer sur un lien piégé ou lui venir en aide à la suite d'un vol de papiers, de téléphone etc. Forcément, si vous recevez un e-mail de la part d'un de vos contacts, puisque vous le connaissez, vous n'allez pas vous méfier de la pièce jointe à ouvrir, ni du lien à cliquer et ni de la demande invoquée. Trop tard vous êtes piégé. Le pirate informatique pourra alors injecter un petit malware (programme malveillant) dans votre ordinateur, et s'adonner à de multiples occupations dont scruter la totalité des informations que votre ordinateur, vos ordinateurs ou réseaux, renferment, et pourquoi pas espionner leurs frappes clavier, faire des captures d'écran, écouter votre microphone, activer et consulter de manière invisible votre webcam….

Ensuite, il pourra par exemple consulter les e-mails que vous avez soigneusement conservés ou que vous avez délicatement classés afin d'en savoir un petit peu plus sur votre vie et votre potentiel financier.

Il pourra également probablement demander à des sites Internet encore liés à cette adresse e-mail, de renvoyer des mots de passe oubliés et pourra alors recevoir des liens pour les réinitialiser.

Enfin, si le pirate connaît votre identifiant et votre mot de passe, il tentera d'utiliser ces informations sur d'autres sites Internet sur lesquels vous auriez pu également vous inscrire tels que Facebook, Twitter, Linked-in, ou d'autres sites bancaires ou de vente en ligne.

Quels signes doivent nous pousser à nous inquiéter d'un éventuel « hacking » de nos boîtes mails inactives ? Quelles sont les solutions permettant de se prémunir face à de telles intrusions ?

Si votre boite e-mail n'est plus active parce que vous ne l'utilisez plus, les signes d'un éventuel « hacking » sont multiples.

D'abord, le signe qui me parait le plus important est celui d'une personne qui soit vous signale le piratage de votre boite e-mail, soit qui fait référence à un e-mail que vous n'avez jamais envoyé.

Ensuite, la presse et les médias spécialisés n'hésitent pas à relayer les annonces de piratages de boites.

Vous pouvez alors conserver une oreille attentive en vous abonnant à l'un d'eux. Attention aux lanceurs d'alertes de failles de sécurité tels que leakedsource.com. Ce site était rapidement devenu la référence et le meilleur lanceur d'alerte en cas de fuites de données massives suite à un piratage (leak). Bien que créé dans un but louable à la base, le business semble avoir pris le dessus et ce site peut devenir une véritable base de données en libre accès pour les cybercriminels.

Enfin, si vous connaissez encore l'identifiant et le mot de passe de vos boites email, en général les fournisseurs de services vous permettent de visualiser un historique d'utilisation. Le consulter vous permettra de vérifier si ce compte soi-disant inutilisé l'est vraiment.

Avec Hotmail (ou Outlook.com), cliquez sur « Vérifier l'activité récente » dans la section « Sécurité et confidentialité ».

Si vous utilisez Gmail, accédez à vos activités récentes sur Google en allant sur le site https://security.google.com/settings/security/activity ou consultez vos dernières activités sur votre compte Gmail en allant sur la page d'accueil de votre messagerie. Vous aurez un lien « Détails » en bas à droite.

Avec Yahoo, survolez avec la souris votre nom / pseudo en haut à droite, et dans le menu déroulant qui apparaît, cliquez sur « Infos compte ». Votre mot de passe est à nouveau demandé : saisissez-le. Dans la rubrique « Connexion et sécurité » , cliquez sur le dernier lien : « Consulter vos connexions récentes ».

En général de telles intrusions sont possibles soit si vous avez malencontreusement communiqué votre mot de passe à quelqu'un, soit s'il vous l'a volé en se faisant passer pour un tiers de confiance par la technique de phishing, soit, si le fournisseur de services s'est fait voler, pirater sa base de données, comme dans le cas présent avec plus de 500 millions de comptes Yahoo !

Pour se prémunir face à de telles intrusions, il est aujourd'hui essentiel de renforcer sa politique de gestion des mots de passe. Il y a à peine plus d'un mois, dans un article sur Atlantico je donnais toute une série de conseils sur la manière avec laquelle nous devons aujourd'hui choisir les mots de passe ou plutôt des phrases de passe. Ainsi, en cas de piratage d'un service Internet, vous n'aurez aucune inquiétude en cas de réutilisation de votre mot de passe sur d'autres services.

Enfin, vous pouvez aussi activer des fonctions de sécurité renforcée que certains services proposent. Vous recevrez alors soit un SMS qui vous avertira si un accès anormal à votre compte est détecté, soit un code reçu par SMS à saisir sur la page de connexion en plus de l'identifiant et du mot de passe.

Comment réagir si on s'aperçoit que nos boîtes mails obsolètes ont bel et bien été piratées ? Plus globalement, est-il préférable de supprimer nos comptes en ligne lorsque nous ne les utilisons plus ? Si oui, pourquoi et comment s'y prendre ?

Si on s'aperçoit que nos boîtes mails obsolètes ont bel et bien été piratées, à mon avis, c'est trop tard. Votre adresse e-mail et le mot de passe ont probablement déjà été partagés sur de nombreuses plateformes et ont même certainement fait plusieurs fois le tour du monde.

Demandez-vous d'abord quelle est votre priorité : vous protéger ou retrouver l'auteur du piratage ?

Pour retrouver l'auteur du piratage, l'objectif sera de toucher le moins de choses possibles afin de recueillir un maximum de preuves. Si votre priorité s'oriente vers la protection de vos comptes, suivez les conseils ci-dessous.

A ce stade, il est important de savoir si le mot de passe de votre boite e-mail piratée est utilisé ailleurs. Si c'est le cas, il faut changer les mots de passe de la boite e-mail piratée et le mot de passe de chaque service sur lequel ce mot de passe a aussi été utilisé, bien évidemment en veillant à choisir un mot de passe différent pour chaque service.

Ensuite, sans plus attendre, il est important de consulter le contenu de cette boite e-mail piratée et vérifier qu'elle ne renferme pas des informations sensibles tels que des informations bancaires ou des identifiants d'autres comptes internet.

Soit vous ne souhaitez pas conserver la boite e-mail, il faudra alors demander la suppression de votre compte, soit vous comptez la conserver, appliquez votre nouvelle politique de gestion des mots de passe.

Enfin, partez du principe que si votre compte a été volé, la réponse à la question secrète aussi. Prenez désormais l'habitude de choisir pour chaque service Internet des questions secrètes différentes car, piraté et disponible dans le DarkNet (Le Web sombre et illégal) et associée à votre adresse e-mail, ce secret pourrait aussi bien représenter une bonne porte d'entrée pour un futur pirate.

Sachez que la suppression du compte n'annule pas le piratage et n'efface pas réellement toutes les informations associées à votre compte.

Propos recueillis par Chloé Chouraqui

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 : Données personnelles en danger : pourquoi il est très important de supprimer vos comptes en ligne que vous n’utilisez plus (et pas seulement de les fermer) | Atlantico.fr