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

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.

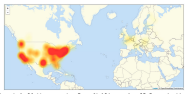
Une attaque de grande ampleur a eu lieu vendredi 21 octobre 2016, mettant hors service pendant quelques heures plusieurs grands sites Internet comme Amazon, Netflix, Twitter, Reddit, Spotify ou Tumblr. Ces sites n'étaient pas directement sous le coup d'une attaque, ils ont été les victimes collatérales 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. À 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 s'obscurcir l'Internet tout court, et ce de plus en plus souvent.

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

---

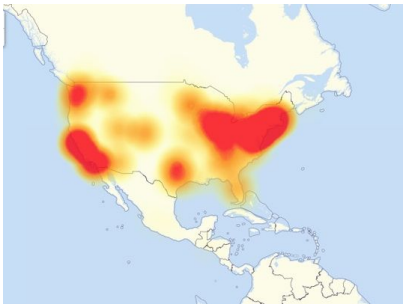
Quelques détails sur la cyberattaque massive dont ont été victime les états unis

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

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

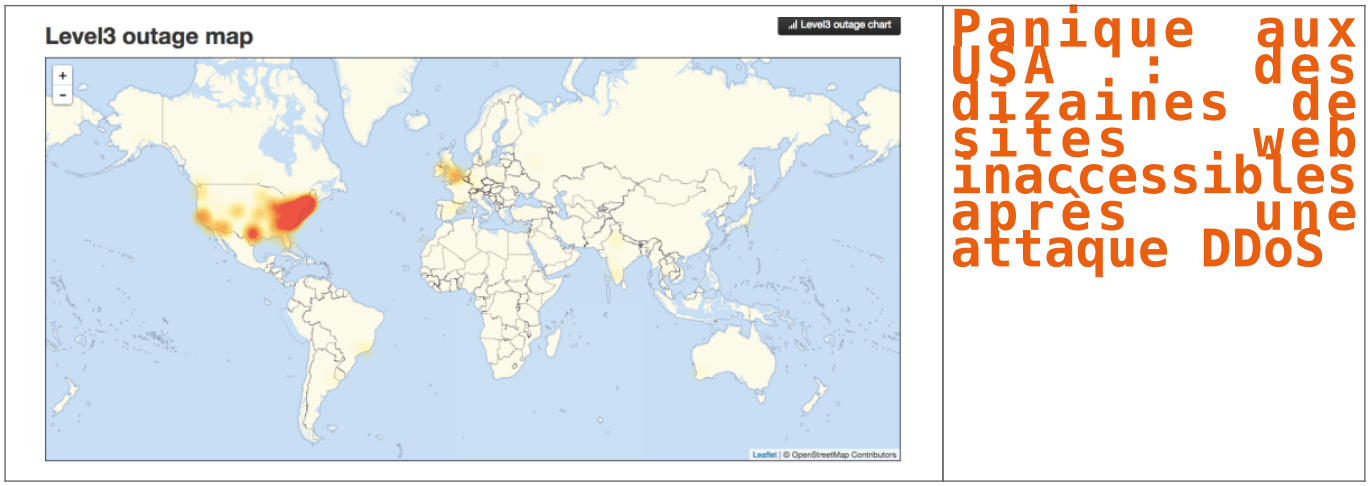
Contactez-nous

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

---

Panique aux USA : des dizaines de sites web inaccessibles après une attaque DDoS



Une attaque par déni de service aurait rendu une grande partie des sites web inaccessibles aux utilisateurs Américains. Le service Dyn, qui a subi l'attaque, est héberge un service de DNS particulièrement utilisé.…[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

Le fonctionnement d'une centrale nucléaire perturbé par une cyberattaque

Le fonctionnement d'une centrale nucléaire perturbé par une cyberattaque

C'est à l'occasion d'un déplacement en Allemagne que Yukiya Amano, patron de l'agence internationale de l'énergie atomique (AIEA) a indiqué qu'une attaque informatique avait, il y a deux ou trois, selon nos confrères de Reuters, affecté le fonctionnement d'une centrale nucléaire…[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

Vous avez des photos intimes sur une page perso Internet? Retirez-les vite, tout le monde peut les voir

On a trop vite tendance à l'oublier: tout ce que l'on place sur Internet, ce qu'on balance en dehors de nos disques durs sur des serveurs qui ne dépendent en rien de nous, sans prendre plus de précaution, est potentiellement accessible à tous.…[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.

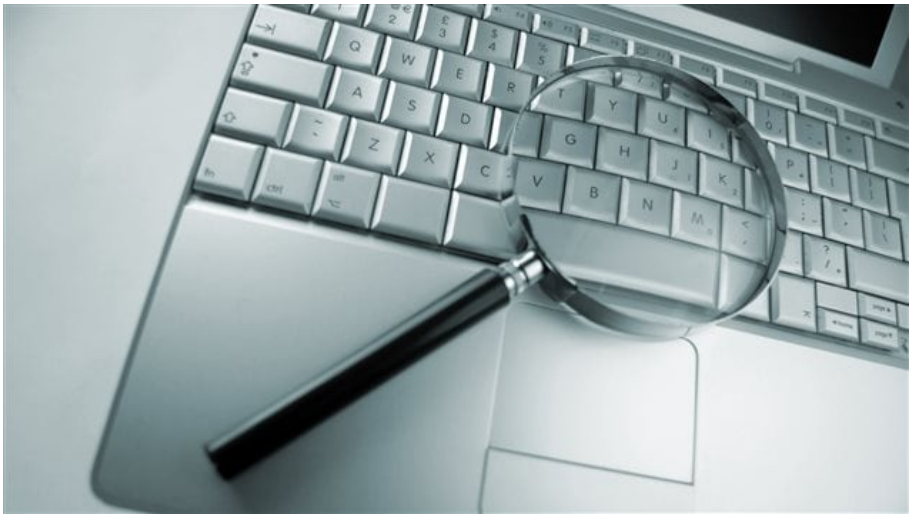
- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation 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

Écrire au clavier en conversant sur Skype… risque d’espionnage



Écrire au clavier en conversant sur Skype… risque d’espionnage

Un texte d'Alain Labelle Dans un article publié dans la revue arXiv, le Pr Gene Tsudik de l'Université de la Californie à Irvine et ses collègues italiens décrivent une faille de sécurité par laquelle le son des textes que vous écrivez peut être enregistré au cours d'une conversation trans…[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

Sednit : dissection d’un groupe de cyber-espions

Sednit : dissection d’un groupe de cyber-espions

Les chercheurs ESET annoncent la publication d'un vaste document de recherche en 3 parties « En route with Sednit ». L'observation de l'utilisation simultanée d'un bootkit et d'un rootkit par les cybercriminels a permis d'analyser leurs cibles et méthodes.

Ce groupe aussi connu sous le nom d'APT28, Fancy Bear ou Sofacy, agit depuis 2004. Son principal objectif **est le vol d'informations confidentielles de cibles spécifiques :**

• Partie 1 : « En route with Sednit : Approaching the Target » se concentre sur la cible des campagnes de phishing, les méthodes d'attaque utilisées ainsi que la première phase de l'attaque utilisant le malware SEDUPLOADER, composé d'un compte à rebours et d'une charge utile associée.

• Partie 2 : « En route with Sednit : Observing the comings and goings » couvre les activités de Sednit depuis 2014 et détaille la boîte à outils d'espionnage utilisée pour la surveillance à long terme des ordinateurs compromis. Cela est rendu possible grâce à deux backdoor SEDRECO et XAGENT, ainsi qu'à l'outil réseau XTUNNEL.

• Partie 3 : « En route with Sednit : a mysterious downloader » décrit le logiciel permettant la première phase de l'attaque DOWNDHELPH qui selon nos données de télémétrie n'aurait servi que 7 fois. A noter que certains de ces déploiements ont requis des méthodes de « persistances avancées » : Windows bootkit et Windows rootkit.

« L'intérêt d'ESET pour ces activités malveillantes est née de la détection d'un nombre impressionnant de logiciels personnalisés déployés par le groupe Sednit au cours des deux dernières années », déclare Alexis Dorais-Joncas, Security Intelligence team lead chez ESET et dédié à l'exploration des activités du groupe Sednit. « L'arsenal de Sednit est en constante évolution. Le groupe déploie régulièrement des logiciels et techniques de pointe, tandis que leur malware phare a également évolué de manière significative au cours des dernières années ».

Selon les chercheurs ESET, les données collectées à partir des campagnes de phishing menées par Sednit montrent que plus de **1.000 profils d'individus hauts-placés impliqués dans la politique d'Europe de l'EST ont été attaqués.** « Contrairement aux autres groupes d'espionnage, le groupe Sednit a développé son propre « exploit kit » et utilisé un nombre étonnamment important d'exploits 0-day», conclut Alexis Dorais-Joncas.

Les activités du groupe cybercriminel de ces dernières années envers les personnalités hauts-placées, ont suscité l'intérêt de nombreux chercheurs. **Le document réalisé par les experts ESET fournit une description technique accessible et contenant les indicateurs de compromission (IOCs), à destination des chercheurs et des entreprises afin de vérifier qu'ils n'ont pas été compromis par le groupe Sednit**.

La première partie de cette recherche est disponible sur WeLiveSecurity, l'intégralité l'étant sur le Github ESET.

Réagissez à cet article

Original de l’article mis en page : Boîte de réception (2) – denis.jacopini@gmail.com – Gmail