La France moins sensible aux arnaques des faux supports techniques

La France moins sensible aux arnaques des faux supports techniques

Selon une enquête de Microsoft, seuls 5% des utilisateurs français se font arnaquer par les faux supports techniques. Contre 20% en moyenne.

Après l'arnaque au président, les faux supports techniques ? C'est la tendance en vogue chez les cybercriminels qui y trouvent une nouvelle source de revenus en se faisant passer pour un service de maintenance d'un éditeur ou constructeur afin d'accéder à distance au PC de la victime. Une fois le contact établi, il leur suffit de demander à leur proie d'installer un logiciel de contrôle à distance pour bloquer l'accès à la machine ou la rendre instable et demander une rançon pour la libérer. L'escroquerie qui se déroulait par démarchage téléphonique jusqu'à présent se décline aujourd'hui par e-mail, depuis des pages web et autres pop-up aux allures de messages d'erreur système qui poussent l'utilisateur à composer le numéro de téléphone affiché à l'écran pour contacter le faux service de support technique. D'où l'accélération de la propagation de l'arnaque ces derniers temps.
Microsoft, premier éditeur concerné par ces escroqueries en vogue, s'est penché sur le comportement des utilisateurs face à ce qu'on appelle les *Tech Support Scam*. Car il faut bien comprendre que, comme toute arnaque, elle ne fonctionne qu'en exploitant la naïveté de la personne ciblée. Le premier éditeur mondial a donc mené un sondage dans 12 pays*, dont la France. Et il s'avère que nous ne serions pas trop crédules face à ces filouteries. Selon Redmond, un utilisateur sur deux en France (51%) ne donne pas suite à ces sollicitations malveillantes. Ce qui signifie tout de même que quasiment autant y a porté attention. Mais seuls 5% des utilisateurs français sont tombés dans le panneau. Dont 4% reconnaissent avoir subi des dommages financiers en cédant à la demande de rançon…[lire la suite]
* *Afrique du Sud, Allemagne, Australie, Brésil, Canada, Chine, Danemark, France, Inde, Royaume Uni, Singapour, et Etats-Unis*

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 France moins sensible aux arnaques des faux supports techniques

---

Les données de santé, la nouvelle cible des cybercriminels

	Les données de santé, la nouvelle cible des cybercriminels

---

Face au développement massif des nouvelles technologies, nos données personnelles sont aujourd'hui entièrement informatisées. De notre dossier médical jusqu'à nos données bancaires en passant par nos loisirs et notre consommation quotidienne, chaque minute de nos vies produit une trace numérique sans même que l'on s'en aperçoit.

Pendant des années nos données de santé étaient éparpillées entre médecins, laboratoire d'analyses, hôpitaux, dentistes dans des dossiers cartonnés qui s'accumulaient au coin d'un bureau ou sur une étagère. En 2012 la loi « hôpital numérique » avait permis un premier virage en obligeant la numérisation des données de santé par tous les professionnels pour une meilleure transmission inter-service. Depuis un an, la loi « santé 2015 » oblige à une unification et une centralisation des données de santé dans des serveurs hautement sécurisés constituant ainsi le Big Data.

Une centralisation des données qui n'est pas sans risque

Appliqué à la santé, le Big Data ouvre des perspectives réjouissantes dans le croisement et l'analyse de données permettant ainsi d'aboutir à de véritables progrès dans le domaine médical. Mais cela n'est pas sans risque.

Le statut strictement confidentiel et extrêmement protégé donne à ces données une très grande valeur. Nos données médicales deviennent ainsi la cible d'une nouvelle cybercriminalité, cotées sur le Dark Web.

Le Dark Web ou Deep Web est l'underground du net tel qu'on le connait. Il est une partie non référencée dans les moteurs de recherche, difficilement accessible où le cybertrafic y est une pratique généralisée. Sur le Dark Web les données personnelles sont cotées et prennent ou non de la valeur selon leur facilité d'accès et leur rendement.

Là où les données bancaires détournées sont de plus en plus difficiles à utiliser suite aux nombreuses sécurisations mise en place par les banques, l'usurpation d'identité et la récolte de données médicales prennent une valeur de plus en plus grande. Selon Vincent TRELY, président-fondateur de l'APSSIS, Association pour la Sécurité des Systèmes d'information, interviewer sur France Inter le 8 septembre 2016, le dossier médical d'une personne aurait une valeur actuelle qui peut varier entre 12 et 18 $.

Si l'on rapporte cette valeur unitaire au nombre de dossiers médicaux abrités par un hôpital parisien, on se rend compte que ceux-ci abritent une potentielle fortune pouvant aller jusqu'à des millions de dollars. Aussi pour protéger ces données, les organismes de santé se tournent vers des sociétés certifiées proposant un stockage dans des Datacenters surveillés, doublement sauvegardés, ventilés avec une maintenance 24h/24. Le stockage a donc un coût qui peut varier entre quelques centaines d'euros jusqu'à des centaines de milliers d'euros pour un grand hôpital. Le coût d'hébergement peut alors devenir un vrai frein pour des petites structures médicales où le personnel présent est rarement qualifié pour veiller à la sécurité numérique des données. Et c'est de cette façon que ces organismes deviennent des cibles potentielles pour les cybercriminels.

Des exemples il en existe à la Pelle. Le laboratoire Labio en 2015 s'est vu subtilisé une partie des résultats d'analyse de ses patients, pour ensuite devenir la victime d'un chantage. Les cybercriminels demandaient une rançon de 20 000 euros en échange de la non divulgation des données. Peu de temps après c'est le service de radiologie du centre Marie Curie à Valence qui s'est vu refuser l'accès à son dossier patients bloquant ainsi toute une journée les rendez-vous médicaux initialement fixés. Peu de temps avant, en janvier 2015, la Compagnie d'Assurance Américaine Anthem a reconnu s'être fait pirater. Toutes ses données clients ont été cryptées en l'échange d'une rançon.

Ces pratiques étant nouvelles, on peut s'attendre à une recrudescence de ce type de criminalité dans l'avenir selon les conclusions en décembre 2014 de la revue MIT Tech Review…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées 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.

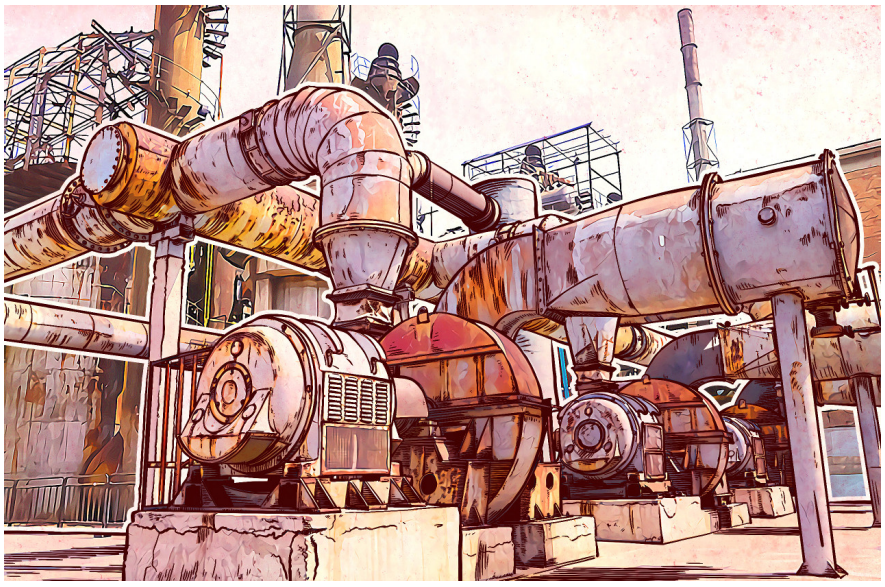
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les données de santé, le nouvel El-Dorado de la cybercriminalité

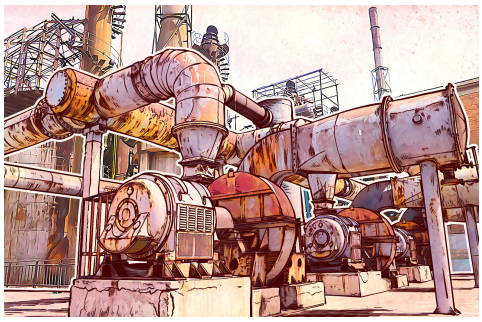
Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie



Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie

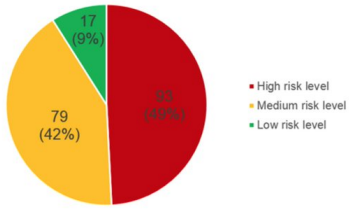
On ne cesse de vous le répéter, il est très important de rester au courant des dernières actualités concernant la cybersécurité et ses menaces. Mieux vaut prévenir que guérir.

Cependant, même ceux qui connaissent tout en matière de cybersécurité, qui utilisent des mots de passe fiables et qui les changent régulièrement, qui reconnaissent des messages d'hameçonnage au premier coup d'œil et qui protègent leurs dispositifs avec une excellente solution de sécurité, même ceux qui font *tout*, ne sont pas totalement à l'abri. Tout simplement parce que nous vivons en société.



Le problème est que nous avons le contrôle sur nos objets personnels, mais pas sur celui des équipements industriels, qui est loin de notre portée.

Vous avez dit cybersécurité ?
Nos experts en cybersécurité ont mené une étude afin de découvrir où nous en sommes concernant la sécurité des systèmes de contrôle industriel.
Shodan, le moteur de recherche pour les dispositifs connectés, nous a montré que 188 019 systèmes industriels dans 170 pays sont accessibles sur Internet. La majorité d'entre eux sont localisés aux Etats-Unis (30,5%) et en Europe, essentiellement en Allemagne (13,9%), Espagne (5,9%) et en France (5,6%).



ICS vulnerabilities in 2015 by risk level (CVSS v.2 and CVSS v.3)

92% (172 982) des systèmes de contrôle industriel (SCI) détectés sont vulnérables. Lamentablement, 87% ont un niveau de risque moyen de bugs et 7% connaissent des problèmes critiques.
Ces cinq dernières années, les experts ont méticuleusement examiné de tels systèmes et y ont découvert de nombreuses failles de sécurité. Durant ce laps de temps, le nombre de vulnérabilités dans les composants SCI a multiplié par dix.
Parmi les systèmes que nos experts ont analysés, 91,6% ont utilisé des protocoles non sécurisés, en donnant l'opportunité aux cybercriminels d'intercepter ou de modifier les données utilisant des attaques de l'homme du milieu.
Egalement, 7,2% (environ 13 700) des systèmes appartiennent à de grandes compagnies aéronautiques, des transports et de l'énergie, pétrolières et gazières, métallurgiques, de l'industrie alimentaire, de la construction et autres secteurs primordiaux.

En d'autres termes, des hackers qualifiés peuvent influencer n'importe quel secteur économique. Leurs victimes (les entreprises piratées) porteraient préjudice à des milliers ou millions de personnes en leur fournissant de l'eau contaminée ou de la nourriture immangeable, ou en leur coupant le chauffage en plein hiver.

Qu'est-ce que cela implique pour nous tous ?

…[lire la suite]

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées 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 : Piratage de l’électricité, de l’eau et de la nourriture : comment les cybercriminels peuvent ruiner votre vie. | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Des serveurs Linux attaqués par le ransomware Fairware

Des serveurs Linux attaqués par le ransomware Fairware

Des exploitants de serveurs Linux signalent des attaques qui entraînent la disparition du dossier Internet du serveur et la non disponibilité des sites pendant une durée indéterminée.

Les participants aux forums de BleepingComputer se plaignent également de l'attaque : d'après la description fournie par une des victimes, cela ressemble plus à une attaque via force brute contre SSH. Notons qu'à chaque fois, le dossier Internet est supprimé et il ne reste que le fichier read_me qui contient un lien vers une page Pastebin où apparaît la demande de rançon.
Les individus malintentionnés promettent de rendre les fichiers contre 2 bitcoins et expliquent que le serveur de la victime a été infecté par le ransomware Fairware. Toutefois, à en croire Lawrence Abrams de chez Bleeping Computer, cette affirmation pourrait ne pas être tout à fait exacte.
« Si l'attaquant télécharge un programme ou un script pour réaliser « l'attaque », il s'agit alors bel et bien d'un [ransomware]. Malheureusement, nous ne disposons pas pour l'instant des informations suffisantes. Tous les rapports montrent que les serveurs ont été compromis, mais je n'ai pas encore eu l'occasion de le vérifier » a déclaré l'expert.
La demande de rançon contient l'adresse d'un portefeuille Bitcoin. La victime est invitée à réaliser le paiement dans les deux semaines, sans quoi les individus malintentionnés menacent d'écouler les fichiers sur le côté. Le message publié sur Pastebin possède le contenu suivant : « Nous sommes les seuls au monde qui pouvons vous rendre vos fichiers . Après l'attaque contre votre serveur, les fichiers ont été chiffrés et envoyés vers un serveur que nous contrôlons. »
Le message contient également une adresse email pour l'assistance technique, mais il est interdit à l'utilisateur d'y envoyer un message uniquement pour confirmer si les attaquants possèdent bien les fichiers perdus. Lawrence Abrams affirme que pour l'instant, il ne sait pas ce que les attaquants font avec les fichiers. Vu que les fichiers sont supprimés, il serait plus logique pour les conserver de les archiver et de les charger sur un serveur et non pas de les chiffrer et de gérer des clés individuelles.
En général, les ransomwares sont diffusés via l'exploitation de vulnérabilités ou par la victime elle-même qui est amenée, par la ruse, à exécuter le malware. Dans le cas qui nous occupe, rien ne trahit ce genre d'activité. Une des victimes indiquait sur le forum de Bleeping Computer que son serveur Linux avait été épargné en grande partie par l'attaque et que les fichiers de la base de données avaient été préservés. Ce commentaire indiquait également que les individus malintentionnés avaient laissé le fichier read_me dans le dossier racine.
La suppression de fichiers et le refus de confirmer leur vol sont des comportements inhabituels pour des individus malintentionnés qui travaillent avec des ransomwares. « Il est tout à fait possible qu'il s'agisse d'une escroquerie, mais dans ce cas c'est un mauvais business pour les attaquants » explique Lawrence Abrams. « Si l'escroc ne respecte pas sa promesse après le paiement de la rançon, il aura mauvaise réputation et plus personne ne le paiera. »
Toutefois, le message sur l'infection via le ransomware et la menace de publier les données volées sont en mesure de confondre la victime et de l'amener à répondre aux exigences des attaquants. Fairware n'est pas la première cybercampagne accompagnée d'une telle menace. L'année dernière, les exploitants du ransomware Chimera, avaient adopté une astuce similaire, même si leur malware n'était pas en mesure de voler les fichiers ou de les publier sur Internet.
Lawrence Abrams explique que les victimes de ransomwares devraient s'abstenir de payer la rançon, mais si elles décident d'agir ainsi, elles doivent au moins confirmer que le bénéficiaire du paiement possède bien les fichiers.
Article original de Securelist

Réagissez à cet article

Original de l’article mis en page : Fairware attaque des serveurs Linux – Securelist

---

Alerte : Un canular sur Facebook qui diffuse de fausses informations terroristes

Alerte : Un canular sur Facebook qui diffuse de fausses informations terroristes

---

Les chercheurs ESET ont découvert une arnaque qui cible les utilisateurs de Facebook. D'abord répandu en République Tchèque et en Slovaquie, elle pourrait se propager dans d'autres pays

Les utilisateurs de Facebook en République Tchèque et en Slovaquie font face à une vague de fausses informations sur une attaque meurtrière à Prague. Quand l'utilisateur clique sur le canular, il est redirigé vers une page Internet de phishing qui essaye de le tromper en l'incitant à partager ses identifiants Facebook.

« D'après ce que nous savons à propos de cette campagne, l'attaque pourrait se propager dans plusieurs autres pays » met en garde Lukáš Štefanko, Malware Researcher chez ESET.

Cette prétendue attaque terroriste est facile à discréditer car la photo publiée ne ressemble pas à Prague, ni à aucune autre ville d'Europe. Malgré cela, l'arnaque se diffuse rapidement. « Les utilisateurs de Facebook partagent fréquemment des histoires sans les avoir lues. Les campagnes d'arnaques, si elles font appel à l'émotion, réussissent étonnamment bien à cause de notre empathie naturelle » commente Lukáš Štefanko.

Peu après le lancement de la campagne, Facebook a commencé à stopper les pages de phishing utilisées dans cette campagne. Les solutions de sécurité ESET sont conçues pour bloquer les pages Internet de phishing liées à ce type d'escroquerie ainsi que d'autres domaines enregistrés par cette même personne.

« Au cours des dernières semaines, il y a eu 84 domaines enregistrés par la même personne. La plupart d'entre eux possède une fonction de phishing, tandis que d'autres pourraient être utilisées à l'avenir lors d'une attaque à plus grande échelle » ajoute Lukáš Štefanko.

Voici les recommandations des experts ESET pour ceux qui pensent avoir été escroqué en partageant leurs identifiants Facebook :

– Changez votre mot de passe Facebook et utilisez les deux facteurs d'authentification fournis par Facebook

– Si vous avez utilisé le même mot de passe pour plusieurs services, changez-le partout – et mettez un terme à cette pratique très dangereuse.

Denis JACOPINI vous recommande les outils de protection suivants :

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

Les pirates informatiques recrutent des complices chez les opérateurs télécoms

Les pirates informatiques recrutent des complices chez les opérateurs télécoms

Un rapport de Kaspersky détaille les nombreuses menaces qui ciblent les opérateurs de télécommunications, réparties en deux catégories : celles qui les ciblent directement (DDoS, campagnes APT, failles sur des équipements, ingénierie sociale…) et celles qui visent les abonnés à leurs services. Parmi les premières, le recrutement de complicités internes, sous la menace ou par appât du gain, progressent, même si elles restent l'exception.

Les opérateurs de télécommunications constituent une cible de choix pour les cyberattaques. Ils gèrent des infrastructures de réseau complexes utilisées pour les communications téléphoniques et la transmission de données et stockent de grandes quantités d'informations sensibles. Dans ce secteur, les incidents de sécurité ont augmenté de 45% en 2015 par rapport à 2014, selon PwC. Dans un rapport intitulé « Threat intelligence report for the telecommunications industry » publié cette semaine par Kaspersky, l'éditeur de logiciels de sécurité détaille les 4 principales menaces qui visent les opérateurs de télécommunications et fournisseurs d'accès Internet (FAI) : les attaques en déni de service distribué (en hausse), l'exploitation de failles dans leur réseau et les terminaux clients, la compromission d'abonnés (par ingénierie sociale, phishing ou malware) et, enfin, le recrutement de personnes capables d'aider les cyber-criminels en interne, au sein même des entreprises attaquées.

Lorsque les attaques passent par des collaborateurs contactés par les cybercriminels, il est difficile d'anticiper ces risques car les motivations sont diverses : appât du gain, collaborateur mécontent, coercition ou tout simplement négligence. Certains de ces relais internes agissent de façon volontaire, d'autres y sont forcés par la menace ou le chantage. Chez les opérateurs de télécoms, on demande principalement à ces « insiders » de fournir un accès aux données, tandis que chez les fournisseurs d'accès Internet (FAI), on les utilise en appui à des attaques contre le réseau ou des actions de type man-in-the-middle (MITM). Même si le recours à des collaborateurs indélicats reste rare, cette menace progresse, selon Kaspersky, et ses conséquences peuvent être extrêmement critiques car elle peut ouvrir une voie directe vers les données ayant le plus de valeur. Le chantage est l'un des vecteurs de recrutement le plus efficace. A ce sujet, le spécialiste en technologies de sécurité remet en mémoire l'intrusion sur le site de rencontres extra-conjugales Ashley Madison, l'été dernier. Celle-ci a permis le vol de données personnelles que les attaquants ont pu confronter à d'autres informations publiquement accessibles pour déterminer où les personnes travaillaient et les compromettre.

Même des pirates inexpérimentés peuvent mener des attaques DDoS

D'une façon générale, Kaspersky répartit en deux catégories l'ensemble des menaces visant les opérateurs télécoms à tous les niveaux : d'une part, celles qui les ciblent directement (DDoS, campagnes APT, failles sur des équipements, contrôles d'accès mal configurés, recrutement de complicités internes, ingénierie sociale, accès aux données), d'autre part celles qui visent les abonnés à leurs services, c'est-à-dire les clients des opérateurs mobiles et des FAI. Les attaques en déni de service distribué ne doivent pas être sous-estimées, rappelle Kaspersky, car elles peuvent être un signe précurseur d'une deuxième attaque, plus préjudiciable. Elles peuvent aussi servir à affecter un abonné professionnel clé, ou encore à ouvrir la voie à une attaque par ransomware à grande échelle. Le 1er cas a été illustré par l'intrusion subie en 2015 par Talk Talk, l'opérateur de télécoms britannique, résultant dans le vol d'1,2 millions d'informations clients (noms, emails, dates de naissance, données financières…). L'enquête a montré que les pirates avaient dissimulé leurs activités derrière l'écran de fumée d'une attaque DDoS. L'un des éléments préoccupants de ces menaces, c'est que même des attaquants inexpérimentés peuvent les organiser de façon relativement efficace, rappelle Kaspersky.

Des équipements vulnérables et des malwares difficiles à éliminer

Les vulnérabilités existant dans les équipements réseaux, les femtocells (éléments de base des réseaux cellulaires) et les routeurs des consommateurs ou des entreprises fournissent aussi de nouveaux canaux d'attaques, de même que les logiciels exploitant des failles dans les smartphones Android. Ces intrusions mettent en œuvre des malwares difficiles à éliminer. En dépit des nombreux vols de données perpétrés au cours des 12 derniers mois, les attaques se poursuivent, exploitant souvent des failles non corrigées ou nouvellement découvertes. En 2015, par exemple, le groupe Linker Squad s'est introduit chez Orange en Espagne à travers un site web vulnérable à une injection SQL et a volé 10 millions de coordonnées sur les clients et les salariés. Par ailleurs, dans de nombreux cas, les équipements utilisés par les opérateurs présentent des interfaces de configuration auxquelles on accède librement à travers http, SSH, FTP ou telnet et si le pare-feu n'est pas configuré correctement, ils constituent une cible facile pour des accès non autorisés, explique encore Kaspersky.

En résumé, les menaces visant les opérateurs de télécommunications existent à de nombreux niveaux – matériel, logiciel, humain – et les attaques peuvent venir de différentes directions. Les opérateurs doivent donc « regarder la sécurité comme un processus englobant tout à la fois la prédiction, la prévention, la détection, la réponse et l'enquête », conclut Kaspersky.

Article de Maryse Gros

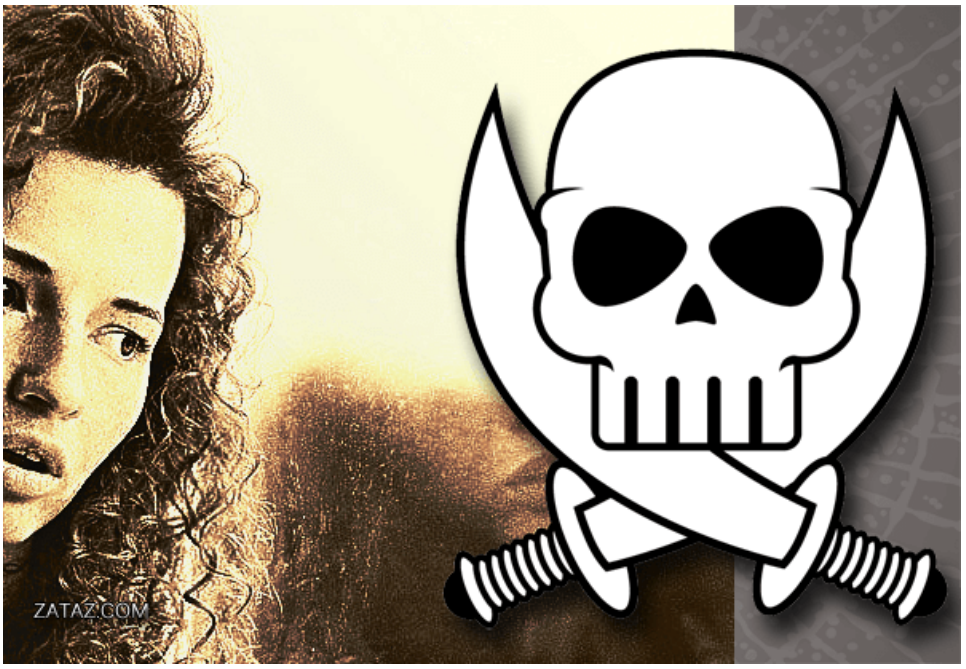
Réagissez à cet article

Original de l'article mis en page : Les pirates recrutent des complices chez les opérateurs télécoms – Le Monde Informatique

---

Des sites de rencontres

touchés par des attaques dites de leurre venant du réseau TOR



Des sites de rencontres touchés par des attaques dites de leurre venant du réseau TOR

Les chercheurs mettent en garde contre une augmentation d'attaques par leurre visant les sites de rencontres venant du réseau TOR.
Les attaques par leurre sont montées via un site de rencontres concurrent pour détourner les utilisateurs d'un site victime vers celui de l'attaquant. La plupart de ces attaques ciblent de multiples services de rencontres et diffusent des spams à un grand nombre d'utilisateurs, en les invitant à rejoindre d'autres sites, probablement tous contrôlés par le même pirate. La motivation de l'instigateur de ces attaques semble donc claire, écarter les utilisateurs d'un site victime et les attirer vers le sien.
Les chercheurs d'Imperva ont récemment assisté à une augmentation des pirates utilisant le réseau TOR pour dissimuler leur identité et mener à bien ce type d'attaques.
Les attaques par leurre venant du réseau Tor se caractérisent par des messages en provenance de clients Tor à un taux relativement faible (mais régulier), de 1 à 3 demandes chaque jour, probablement pour passer sous le radar des mécanismes de limite de vitesse et éviter les contrôles de détection automatique des navigateurs. Malgré le taux très faible des demandes qu'Imperva a pu observer, il est probable que le nombre total de celles-ci soit beaucoup plus élevé, avec seulement quelques demandes exposées dans l'aperçu du trafic utilisateurs Tor.
Il faut également prendre en compte le déficit d'image que représente ces attaques menées par les centaines de faux profils très attractifs qui harcèlent les utilisateurs du site victime et qui abaissent la crédibilité de celui-ci.
Selon Itsik Mantin, directeur de la recherche de sécurité à Imperva : « ***Ces attaques ont le potentiel de perturber considérablement le business des opérateurs de site de rencontres. En utilisant le réseau TOR les attaquants sont capables de cacher leur emplacement réel et leurs identités, ce qui les rends encore plus difficiles à détecter et à bloquer*** ».
Afin de se protéger contre les attaques par leurre, il est recommandé aux sites de rencontre de surveiller de près les faux comptes et de fermer tout ce qui pourrait être considéré comme illégitime. Il est également conseillé de monitorer l'ensemble du trafic TOR et de bloquer toute activité suspecte.
Article original de Damien Bancal

Les conseils de Denis JACOPINI
Quelque soit l'e-mail reçu, ceci nous prouve une fois de plus qu'il est nécessaire de décupler notre vigilance. Sachez que le protocole d'envoi des e-mails, le fameux SMTP, se base sur la norme RFC 821 qui date de 1982. Ceci dit, vous comprendrez mieux si je vous dis que ce protocole ne prévoyait pas les dérives d'usages que nous connaissons aujourd'hui.
De nos jours, cette faille, exploitée à outrance par les pirates informatiques, autorise sans aucune difficulté l'usurpation d'identité. Avec les technologies d'aujourd'hui, n'importe qui peut se faire passer pour n'importe qui, et rien ne vous empêche de vous faire passer pour Larry Page ou Serguei Brin (les fondateurs de Google en 1998) en créant une adresse e-mail de type larry.page@gmail.com ou serguei.brin@gmail.com pour peu que ces adresses e-mail ne soient pas prises. Pire, vous pouvez recevoir un e-mail indiquant le vrai nom et la vraie adresse e-mail de votre meilleur ami alors que vous répondre à une adresse e-mail légèrement différente, celle du pirate usurpant l'identité de votre ami…
De qui peut-on encore se fier ?
Besoin de conseils ? de formation ?, contactez Denis JACOPINI

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 : ZATAZ Des sites de rencontres touchés par des attaques dites de leurre venant du réseau TOR – ZATAZ

Devez-vous changer votre mot de passe DropBox ?

Devez-vous changer votre mot de passe DropBox ?

On vous demande de créer un nouveau mot de passe sur dropbox.com. Pourquoi et que devez-vous faire ?
L'entité propose de faire des sauvegardes de ses fichiers dans le Cloud, le fameux nuage. Bref, des disques durs hors de chez vous, hors de votre entreprise, sur lesquels vous déposez vos données afin d'y accéder partout dans le monde, et peu importe le support : Ordinateur, smartphone…
Depuis quelques heures, une vague de courriels aux couleurs de DropBox vous indique « ***On me demande de créer un nouveau mot de passe sur dropbox.com. Pourquoi et que dois-je faire ?***« , si les plus paranoïaques ont jeté la missive de peur d'être nez-à-nez avec un phishing, je me suis penché sur le sujet, histoire de m'assurer que l'alerte valait la peine d'être lancée. Je vais être rapide avec le sujet, oui, il s'agit bien d'un courriel officiel de la firme US.

Lors de votre prochaine visite sur dropbox.com, vous serez peut-être invité à créer un nouveau mot de passe. Une modification « ***à titre préventif à certains utilisateurs*** » souligne Dropbox. Les utilisateurs concernés répondent aux critères suivants : ils ont créé un compte Dropbox avant mi-2012 et ils n'ont pas modifié leur mot de passe depuis mi-2012. Vous commencez à comprendre le problème ? Comme je vous le révélais la semaine dernière, des espaces web comme Leakedsource, le site qui met en danger votre vie privée, sont capable de fournir aux pirates une aide précieuse. Comment ? En diffusant les informations collectées dans des bases de données piratées.

Que dois-je faire ?
Si, quand vous accédez à dropbox.com, vous êtes invité à créer un nouveau mot de passe, suivez les instructions sur la page qui s'affiche. Une procédure de modification des mots de passe qui n'a rien d'un hasard. Les équipes en charge de la sécurité de DropBox effectuent une veille permanente des nouvelles menaces pour leurs utilisateurs. Et comme vous l'a révélé ZATAZ, Leaked Source et compagnie fournissent à qui va payer les logins et mots de passe d'utilisateurs qui utilisent toujours le même sésame d'accès, peu importe les sites utilisés. Bref, des clients Adobe, Linkedin … ont peut-être exploité le même mot de passe pour DropBox.
Bilan, les pirates peuvent se servir comme ce fût le cas, par exemple, pour ma révélation concernant le créateur des jeux Vidéo Rush et GarryMod ou encore de ce garde du corps de Poutine et Nicolas Sarkozy. Les informaticiens de Dropbox ont identifié « ***d'anciennes informations d'identification Dropbox (combinaisons d'adresses e-mail et de mots de passe chiffrés) qui auraient été dérobées en 2012. Nos recherches donnent à penser que ces informations d'identification sont liées à un incident de sécurité que nous avions signalé à cette époque***. » termine DropBox.
A titre de précaution, Dropbox demande à l'ensemble de ses utilisateurs qui n'ont pas modifié leur mot de passe depuis mi-2012 de le faire lors de leur prochaine connexion.
Article original de Damien Bancal

Les conseils de Denis JACOPINI
Comme tout e-mail reçu, la prudence est de rigueur. Avant de valider l'authenticité d'un e-mail envoyé par une firme telle que Dropbox, nous avons dû analyser l'entête de l'e-mail reçu et comparer les données techniques de celles répertoriées dans les bases de données connues.
J'imagine que vous n'aurez pas le courage d'apprendre à le faire vous même ni que vous trouverez l'intérêt de consacrer du temps pour ça.
Comme chaque mise à jour demandée par un éditeur ou un constructeur, comme tout changement de mot de passe recommandé par une firme, nous vous conseillons de le faire en allant directement sur le site concerné.
Dans le cas de « Dropbox », nous vous recommandons de rechercher « dropbox.com » dans google ou de taper « dropbox.com » dans votre barre d'adresse et de vous identifier. Vous serez ainsi sur le site officiel et en sécurité pour réaliser la procédure demandée.

Attention
Vous ne serez en sécurité que si votre ordinateur n'est pas déjà infecté. En effet, taper un nouveau mot de passe si votre ordinateur est déjà infecté par un programme espion revient à communiquer au voleur une copie de vos nouvelles clés. Taper l'ancien mot de passe revient aussi à donner au voleur la clé permettant peut-être d'ouvrir d'autres portes !!!

Besoin de conseils ? de formation ?, contactez Denis JACOPINI

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 : ZATAZ Changez votre mot de passe DropBox – ZATAZ

La cybercriminalité a de belles années devant elle

La cybercriminalité a de belles années devant elle

Les prochaines années laissent entrevoir de beaux moments pour les cybercriminels de tout acabit. Les raisons expliquant cela sont nombreuses. Quelles sont-elles?

Suivre la scène de la sécurité informatique a ceci de particulier : c'est à la fois fascinant et grandement décourageant. C'est d'autant plus décourageant que les tendances présentes au cours des derniers mois laissent entrevoir de beaux jours pour les cybercriminels. Essentiellement, quatre raisons expliquent cela.

La multiplication des cibles potentielles

La première raison est assez évidente : il y a de plus en plus de cibles disponibles pour les criminels. La surmultiplication du nombre de plateformes exploitant Internet a pour effet de toutes les transformer en des opportunités potentielles pour des gens malintentionnés. La manifestation la plus flagrante de cette surmultiplication se transpose dans la fulgurante montée de l'Internet des objets.
Ce nouvel eldorado porte toutefois les gènes de sa propre insécurité. En effet, le marché est meublé par une multitude de joueurs, et leur intérêt porté à la chose sécuritaire est tout aussi variable. Ainsi, alors que l'objectif est d'occuper le marché le plus rapidement possible, bon nombre de joueurs impliqués dans la course à l'Internet des objets arrivent sur le marché avec des produits qui sont, volontairement ou involontairement, plus ou moins sécurisés.
Bref, nous sommes placés devant un cercle vicieux duquel nous ne pouvons pas nous sortir : plus de technologies signifient nécessairement plus de vulnérabilités et, conséquemment, plus d'opportunités criminelles. De plus, croire que l'on puisse mettre un frein à l'évolution technologique est illusoire.

Le difficile marché de la sécurité

Le contexte actuel rend les ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés.
Alors que le domaine apparaît comme extrêmement complexe, le manque criant de main-d'œuvre est de plus en plus problématique dans les entreprises. Forbes affirme pourtant que ce secteur vaudra sous peu 75 milliards de dollars US et que le marché créera plus d'un million d'emplois.
Non seulement manque-t-il de spécialistes en sécurité, mais il manque aussi de plus en plus de pirates black hat sur le marché, faisant en sorte que les cybercriminels eux-mêmes se tournent de plus en plus vers des modèles de sous-traitance pour effectuer leurs opérations.
Ce manque d'expertise a pour effet de rendre l'économie globalement plus ou moins axée sur la sécurité. Certes, certains secteurs ont les moyens de leurs ambitions, mais le contexte actuel rend ces ressources extrêmement difficiles à conserver ou à acquérir pour les petites et moyennes entreprises qui n'ont pas les moyens d'offrir des salaires élevés. Les effets sont bien sûr conséquents : la situation engendre une sécurité bien inégale, avec le lot de vulnérabilités qu'elle impose.

La rentabilité évidente

Autre point extrêmement important pour expliquer pourquoi la cybercriminalité aura le vent dans les voiles? C'est lucratif. La logique criminelle est relativement simple : il s'agit de faire le plus d'argent possible, le plus facilement possible. En somme, c'est le capitalisme en action.
Dans le domaine de la cybercriminalité, cela fonctionne décidément. On estime à 445 milliards de dollars US le marché de la cybercriminalité. Bon, je vous entends déjà geindre et dire que c'est fort de café. Soit. Admettons que ce soit la moitié moins, c'est tout de même 222 milliards, batinse!
Pour rappel, le budget du Canada est d'environ 290 milliards de dollars CA. C'est donc payant, et c'est bien dommage, mais les conséquences de la cybercriminalité sont minimes. Les chances d'arrêter les criminels sont plutôt basses (voir point suivant) et les peines encourues ne sont pas adaptées.

L'incapacité d'action des agences d'application de la loi

Les cybercriminels ont donc le beau jeu, puisque le risque de se faire prendre est extrêmement bas. En effet, les forces policières sont mal équipées pour confronter la cybercriminalité, faisant en sorte que trop souvent, elles doivent capituler devant les actions commises par les criminels. Dans les cas les plus extrêmes, les agences tenteront de déployer les efforts nécessaires pour faire culminer une enquête, mais cela se fera à grands coups de contrats avec le secteur privé afin de se procurer l'expertise nécessaire pour résoudre le crime en question. Le fait que le FBI ait versé un montant de 1,3 million à un groupe de «chercheurs en sécurité», considérés par plusieurs comme ayant des mœurs on ne peut plus douteuses, pour accéder aux données présentes dans l'iPhone du terroriste de San Bernardino en est, en soi, la manifestation la plus éloquente.
Lutter contre la cybercriminalité demande essentiellement quatre choses. Une culture particulière, une collaboration internationale, des moyens et des techniques disponibles, et des compétences de pointe dans le domaine des technologies. Le dur constat qu'il faut faire, c'est qu'outre la collaboration internationale, les autorités compétentes n'ont pas les moyens pour atteindre les trois autres prérequis. Par conséquent, la vaste majorité des corps policiers ne s'attaqueront aux cybercrimes que lorsque les infractions sont trop exagérées.

La somme de toutes les peurs

Au final, ce qui est le plus inquiétant dans cette situation, c'est que plus le temps avance, plus les réseaux de cybercriminels deviennent solides, sophistiqués et ont de plus en plus de moyens. Les laisser agir en toute impunité a pour effet de les rendre toujours plus coriaces, ce qui rendra la tâche de lutter contre eux d'autant plus difficile à long terme. Il faudra que l'on prenne le problème à bras le corps une fois pour toute, sinon, nous risquons d'avoir de mauvaises surprises dans les prochaines années.
Article original de branchez-vous.com

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 cybercriminalité a de belles années devant elle | Branchez-vous

---

Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?

Comment se prémunir de la cybercriminalité, ce risque sur Internet pour les particuliers et les professionnels ?

En pleine recrudescence, de nombreuses attaques ciblent les particuliers mais aussi les entreprises et les administrations. Elles visent à obtenir des informations personnelles afin de les exploiter ou de les revendre (données bancaires, identifiants de connexion à des sites marchands, etc.). Hameçonnage (phishing) et «Rançongiciel» (ransomware) sont des exemples connus d'actes malveillants portant préjudices aux internautes.
Pour s'en prémunir, des réflexes simples existent.

QUELS SONT LES DIFFÉRENTS TYPES D'ATTAQUES ?

Attaque par hameçonnage (phishing)

L'hameçonnage, phishing ou filoutage est une technique malveillante très courante sur Internet. L'objectif : opérer une usurpation d'identité afin d'obtenir des renseignements personnels et des identifiants bancaires pour en faire un usage criminel.

1. Le cybercriminel se « déguise » en un tiers de confiance (banques, administrations, fournisseurs d'accès à Internet…) et diffuse un mail frauduleux, ou contenant une pièce jointe piégée, à une large liste de contacts. Le mail invite les destinataires à mettre à jour leurs informations personnelles (et souvent bancaires) sur un site internet falsifié vers lequel ils sont redirigés.
2. La liste comprend un nombre si important de contacts et augmente les chances que l'un des destinataires se sente concerné par le message diffusé.
3. En un clic, il est redirigé vers le site falsifié qui va recueillir l'ensemble des informations qu'il renseigne.
4. Ces informations sont alors mises à disposition du cybercriminel qui n'a plus qu'à faire usage des identifiants, mots de passe ou données bancaires récupérées.

Voir la vidéo de la Mackacademy sur le phishing (CIGREF – partenariat ANSSI)

Pour s'en prémunir :

- N'ayez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
- Méfiez-vous des pièces jointes, elles pourraient être contaminées. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Ne répondez jamais à une demande d'informations confidentielles par mail.
- Passez votre souris au-dessus des liens, faites attention aux caractères accentués dans le texte ainsi qu'à la qualité du français ou de la langue pratiquée par votre interlocuteur (ex : orthographe).

Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.

Attaque par «Rançongiciel» (ransomware)

Les rançongiciels sont des programmes informatiques malveillants de plus en plus répandus (ex : Locky, TeslaCrypt, Cryptolocker, etc.). L'objectif : chiffrer des données puis demander à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

1. Le cybercriminel diffuse un mail qui contient des pièces jointes et / ou des liens piégés. Le corps du message contient un message correctement rédigé, parfois en français, qui demande de payer rapidement une facture par exemple.
2. En un clic, le logiciel est téléchargé sur l'ordinateur et commence à chiffrer les données personnelles : les documents bureautiques (.doc, .xls, .odf,etc), les photos, la musique, les vidéos…etc.
3. Les fichiers devenus inaccessibles, un message s'affiche pour réclamer le versement d'une rançon, payable en bitcoin ou via une carte prépayée, en échange de la clé de déchiffrement. Attention, rien n'indique que le déchiffreur en question soit efficace !

Pour s'en prémunir :

- N'ayez pas une confiance aveugle dans le nom de l'expéditeur de l'email. Au moindre doute, n'hésitez pas à contacter l'expéditeur par un autre biais.
- Méfiez-vous des pièces jointes et des liens dans les messages dont la provenance est douteuse. Au moindre doute, n'hésitez pas à contacter l'expéditeur pour en connaître la teneur.
- Effectuez des sauvegardes régulièrement sur des périphériques externes.
- Mettez à jour régulièrement tous vos principaux logiciels en privilégiant leur mise à jour automatique.

Pour aller plus loin, n'hésitez pas à consulter la page sur les conseils aux usagers qui reprend les bonnes pratiques à mettre en place pour sécuriser ses équipements et ses données.

VOUS ÊTES VICTIME D'UN RANSOMWARE OU DE FISHING ?

Suite à une escroquerie ou une cyberattaque, déposez plainte auprès d'un service de **Police nationale** ou de **Gendarmerie nationale** ou bien adressez un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

Munissez-vous de tous les renseignements suivants :

- Références du (ou des) transfert(s) d'argent effectué(s)
- Références de la (ou des) personne(s) contactée(s): adresse de messagerie ou adresse postale, pseudos utilisés, numéros de téléphone, fax, copie des courriels ou courriers échangés…
- Numéro complet de votre carte bancaire ayant servi au paiement, référence de votre banque et de votre compte, et copie du relevé de compte bancaire où apparaît le débit frauduleux
- Tout autre renseignement pouvant aider à l'identification de l'escroc

Vous pouvez également signaler les faits dont vous avez été victime via la plateforme de signalement « Pharos » ou le numéro dédié : 0811 02 02 17

Des services spécialisés se chargent ensuite de l'enquête :

- **Police nationale** : l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) qui dépend de la Sous-direction de lutte contre la cybercriminalité (SDLC) : 01 47 44 97 55
- **Gendarmerie nationale** : le centre de lutte contre les criminalités numériques (C3N) du Service Central du Renseignement Criminel (SCRC) :cyber@gendarmerie.interieur.gouv.fr
- **Préfecture de police** : la Préfecture de police de Paris, de la Direction centrale du renseignement intérieur (DCRI) et ses équipes de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) compétente uniquement pour Paris et petite couronne (75, 92, 93 et 94) : 01 40 79 67 50

Article original de gouvernement.fr

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

- Expertises techniques (virus, spyware, 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 : Cybercriminalité | Gouvernement.fr