Qu’est ce que le Smishing ?

Qu’est ce que le Smishing ?

Smishing est la contraction de SMS et de Phishing. On l’appelle également Hameçonnage par SMS.
Tout comme le phishing, un message à caractère urgent est envoyé à un utilisateur pour qu’il entreprenne une action. Lors d’un Smishing, c’est un message texte qui est envoyé à un utilisateur sur son téléphone. Le texte du message demande généralement à l’utilisateur d’appeler un numéro de téléphone ou de se rendre sur un site Internet pour effectuer une action précise. La plupart du temps, lorsque vous composez ce numéro de téléphone, vous êtes automatiquement redirigé vers un serveur vocal interactif. Il est demandé à l’utilisateur de fournir des informations personnelles (mot de passe) ou bancaires (numéro de carte bancaire).
Souvent, cette forme de phishing implique un message de texte dans un SMS ou dans un numéro de téléphone. Le numéro de téléphone comporte un message automatisé à partir duquel vos informations commencent à être réellement recueillies. Ce qui rend particulièrement effrayant le smishing, c’est que l’on a plutôt tendance à faire confiance à un SMS qu’à un e-mail. La plupart des gens sont conscients des risques encourus pour la sécurité lorsqu’on clique sur des liens contenus dans des e-mails. Mais c’est moins le cas lorsqu’il s’agit de SMS.

Ne cliquez jamais sur les liens contenus dans ces messages et ne rappelez jamais ces numéros.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d’expertises, d’audits, de formations et de sensibilisation dans toute la France et à l’étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d’un Correspondant Informatique et Libertés (CIL) ou d’un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Que sont le Smishing et le Vishing ? | Aide Homelidays*

Les services Cloud au centre d’attaques d’entreprises par APT10

	Les services Cloud au centre d’attaques d’entreprises par APT10

Le groupe de pirates chinois APT10 a infiltré des services Cloud managés pour remonter aux serveurs des entreprises qui les utilisent.

La maturité des attaques ciblées contre les entreprises est montée d'un cran. *« Un groupe de piratage a mené l'une des campagnes d'espionnage les plus prolifiques depuis l'APT1 en 2013, employant de nouvelles tactiques pour atteindre une large audience »*, a alerté PwC (Pricewaterhouse Coopers) lundi 3 avril. En collaboration avec BAE Systems et le National Cyber Security Centre (NCSC) britannique, la branche réseau du cabinet d'audit a découvert ce qu'il considère comme *« l'une des plus importantes campagnes mondiales de cyber-espionnage jamais organisées »*. Pas moins.

De quoi s'agit-il ? Du piratage des infrastructures de fournisseurs de services managés à partir desquelles les cyber-attaquants remontent aux serveurs des organisations qui y ont recours. Une opération que PwC a baptisé 'Cloud Hopper'. Les cyber-criminels derrière ces agissements seraient le groupe de hackers chinois APT10. *« PwC et BAE Systems croient que le groupe de piratage largement connu sous le nom 'APT10' a mené la campagne d'espionnage en ciblant les fournisseurs de services informatiques externalisés comme une façon d'accéder aux organisations de leurs clients à travers le monde, leur conférant un accès sans précédent à la propriété intellectuelle et aux données sensibles »*, indique PwC dans son communiqué. APT10 est le nom donné par FireEye à un groupe de pirates chinois également référencé sous les appellations Red Apollo (par PwC UK), CVNX (par BAE), Stone Panda (par CrowdStrike), et menuPass Team (plus globalement).

Un grand volume de données exfiltrées

Les méthodes d'infection restent relativement classiques et s'appuient sur le spear-phishing, ou harponnage. Cette méthode de phishing ciblé fait appel à des techniques d'ingénierie sociale qui visent à tromper le destinataire d'un e-mail pour l'inciter à installer, à son insu, un malware ou visiter une page infectieuse, à partir desquels les pirates ouvrent une porte d'entrée sur le réseau. Objectif ici : prendre le contrôle des accès d'employés de prestataires Cloud, afin d'exploiter les canaux de communication existant entre les services managés de ces derniers et les serveurs des entreprises clientes. De la grande distribution aux technologies en passant par l'énergie, l'industrie manufacturière, le secteur public ou l'industrie pharmaceutique, tous les grands secteurs sont touchés par cette campagne…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Les services Cloud au centre d'attaques d'entreprises par APT10*

Les bonnes pratiques pour lutter contre la cybercriminalité

	Les bonnes pratiques pour lutter contre la cybercriminalité

Les entreprises modernes sont très vite confrontées aux dangers que représente un modèle commercial actif en permanence. Les clients ont de plus en plus recours à des outils en ligne pour accéder à des comptes, à des services ou à de l'expertise.

Quant aux employés, ils souhaitent pouvoir se connecter à distance et à tout moment aux réseaux de leur entreprise. D'où l'aspiration à un accès quotidien plus simple et plus pratique. Mais cette souplesse à aussi son revers. Les hackers, qui l'ont également bien compris, créent par conséquent des virus et des logiciels malveillants, dans l'unique intention de nuire. À la lumière des récentes révélations de l'organisme britannique Office for National Statistics selon lequel plus de 5,8 millions d'incidents de cybercriminalité ont eu lieu l'an dernier, il est crucial que les entreprises protègent les données de leur personnel et de leurs clients contre la cybercriminalité.
Dans ce contexte, quelles sont les principales activités de cybercriminalité dont les entreprises ont à se prémunir, et que faire pour les combattre ?

La manipulation sociale (Social engineering)
À l'ère du numérique, les pratiques de manipulation sociale sont devenues un problème préoccupant. Du fait que l'internet offre aux fraudeurs un voile d'anonymat, il est important que les sociétés qui détiennent des données clients sensibles soient au courant des pratiques les plus répandues parmi les hackers qui utilisent la manipulation sociale.
Le phishing aussi appelé hameçonnage, est peut-être la forme la plus connue de piratage de fraude par abus de confiance. Il recourre les tentatives de fraudeurs qui généralement déploient de multiples moyens pour acquérir des données sensibles telles que les noms d'utilisateur, les mots de passe et les détails de paiement en se faisant passer pour une personne connue ou des organismes de confiance par courrier électronique ou une autre forme de communication numérique. Récemment, les cas de hameçonnage beaucoup plus ciblé, où les hackers se présentent comme des personnes de confiance, sont à la hausse. En cas de succès de l'attaque, les données des clients ou les documents sensibles d'une entreprise et donc sa réputation - sont en danger.
En effet, la recherche par Get Safe Online indique que la fraude liée au phishing à contribué aux organisations britanniques qui ont perdu plus de 1 milliard de livres sterling au cours de la dernière année en raison de la cybercriminalité.
Selon l'enquête, réalisée avec Spectum.Mp et dévoilée en exclusivité par Europe 1, 84% des sociétés française ont été ciblées par des pirates informatiques en 2015.
Le vishing et le smishing sont les variantes du phishing passant respectivement par les communications téléphoniques et SMS. Dans un cas comme dans l'autre, le principe est de récupérer les données sensibles de vos clients ou de votre entreprise. Compte tenu de l'impact dévastateur que peut avoir l'utilisation de la manipulation sociale par les cybercriminels sur les entreprises modernes, les dirigeants d'entreprise et les responsables informatiques doivent être très attentifs à ce type d'activités.

Menaces internes
À l'instar de la manipulation sociale qui peut porter préjudice aux entreprises de l'extérieur, il est légitime de se méfier également des menaces internes. Votre personnel peut disposer de privilèges d'accès aux données sensibles et en faire usage pour nuire à votre entreprise. Les employés où à l'heart, les prestataires présents ou le personnel de maintenance sur site pourraient également représenter un danger pour votre société.
Les problèmes posés par les activités malveillantes des sociétés ne sont pas toujours visibles immédiatement mais ils ne sauraient pour autant être ignorés. Prenons le cas d'un employé qui s'est d'être licencié ou de perdre son poste dans une entreprise pour une autre raison. Il est possible que cette décision provoque chez lui de la colère et l'amène à vouloir exprimer son ressentiment envers son ancienne société. S'il possède toujours les droits d'accès au stockage partagé ou à des documents, il a la possibilité de modifier, supprimer ou falsifier les données stockées. Il peut également exercer sur le site et auquel un mot de passe inoubliable a été attribué les restrictions pour une courte durée pour représenter et nuire. De ce n'agissant de corruption ou de communication de données financières, d'informations clients ou bien de droits d'authentification, les agissements de tels salariés peuvent faire des ravages sur les entreprises de toutes tailles.
Dépendant, comme c'est le cas avec les dangers de la manipulation sociale, le fait de connaître et de mesurer la menace potentielle des acteurs malveillants peut permettre de faire un grand pas en avant dans la prévention des activités de cybercriminalité ciblant les entreprises. Les responsables informatiques et les dirigeants d'entreprises doivent rester vigilants en accordant aux utilisateurs des droits d'accès limités à leurs besoins et se méfier des récentes évolutions des techniques frauduleuses pour protéger leur entreprise contre les intentions malveillantes des cybercriminels.

Comment riposter
La lutte contre la cybercriminalité devrait dominer les débats et les plans stratégiques des dirigeants d'entreprise dans les années à venir. Pour optimiser leurs chances de l'emporter, les entreprises peuvent prendre plusieurs mesures.
1. Abandonner la technique des mots de passe, trop simple, au profit d'un système d'authentification forte en entreprise : Les hackers qui dérobent le nom d'utilisateur et le mot de passe d'un employé peuvent la plupart du temps parcourir le réseau sans être repérés et charger des programmes malveillants ou bien voler ou enregistrer des données. Pour protéger les systèmes et les données, les entreprises ont besoin d'un système d'authentification forte qui ne repose pas exclusivement sur une information connue de l'utilisateur (mot de passe). Au moins un autre facteur d'authentification doit être utilisé, par exemple un élément que possède l'utilisateur (ex: un jeton d'ouverture de session informatique) et/ou qui le caractérise (ex: une solution d'identification biométrique ou comportementale). Il est également encourageable d'abandonner totalement les mots de passe et d'envisager cartes, jetons ou biométrie.
2. Profitez de la commodité accrue d'un modèle d'authentification forte mobile : Les utilisateurs sont de plus en plus désireux d'une solution d'authentification plus rapide, plus transparente et plus pratique que celle offerte par les mots de passe à usage unique (OTP). Les cartes d'affichage et autres dispositifs physiques. Désormais, les jetons mobiles peuvent figurer sur une même carte utilisée pour d'autres applications, ou être combinés sur un téléphone avec des dispositifs d'identification unique pour accéder à des applications cloud. Il suffit pour l'utilisateur de présenter sa carte ou son téléphone à une tablette, à un ordinateur portable ou à un autre périphérique pour l'authentifier sur un réseau, après quoi l'OTP devient inutilisable. Plus aucun jeton à mettre en place et à gérer. L'utilisateur final n'a qu'un seul dispositif à porter et n'a plus besoin de garder en mémoire ou de taper un mot de passe complexe.
3. Utiliser une stratégie de sécurité informatique par niveaux qui garantit des niveaux d'atténuation des risques appropriés : Pour une efficacité optimale, les entreprises ont intérêt à adopter une approche de la sécurité par niveaux, en commençant par authentifier l'utilisateur (employé, associé, client), puis en authentifiant le dispositif, en protégeant le navigateur et l'application, et enfin en authentifiant la transaction en recourant à l'intelligence basée sur les fichiers signatures ci mémorisée. La mise en œuvre de ces niveaux nécessite une plateforme d'authentification polyvalente et intégrée dotée de moyens de détection des menaces en temps réel. Cette plateforme, associée à une solution antivirus, apporte le plus haut degré de sécurité possible face aux menaces actuelles.

[1]
[2]
Chip Epps est Vice President, Product Marketing, IAM Solutions de HID Global
_[Lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus,) et vous assister dans ses démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertise, d'audits, de formations et de sensibilisation dans toute la France et à l'Étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.- (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03861 84)
Plus d'informations sur : https://www.lemetiegen7.fr/formations-cybercriminalite-protection-des-donnees-personnelles

[1]
[2]
Réagissez à cet article

Source : *Les bonnes pratiques pour lutter contre la cybercriminalité Chip Epps, HID Global*

Alerte : Faux mods de Minecraft dans le Google Play

Alerte : Faux mods de Minecraft dans le Google Play

Les chercheurs ESET® découvrent plus de 80 applications malveillantes sur Google Play® déguisées en mods[1] de Minecraft® et ayant généré pas loin d'un million de téléchargements.

Au total, les 87 faux mods ont donné lieu à 990 000 téléchargements avant d'être signalés par ESET les 16 et 21 mars 2017. Les applications répertoriées se divisent en deux catégories : le téléchargement de publicités (Android/TrojanDownloader.Agent.JL) et les fausses applications redirigeant les utilisateurs vers des sites Internet frauduleux (Android/FakeApp.FG).
Pour Android/TrojanDownloader.Agent.JL, ESET signale **14 fausses applications ayant causé 80 000 téléchargements, contre 910 000 installations pour les 73 applications malveillantes** agissant sous Android/FakeApp.FG. Comme elles ne disposent pas de fonctionnalités réelles et qu'elles affichent de nombreuses publicités agressives, les avis négatifs apparaissent clairement sur Google Play.
Si un utilisateur a téléchargé des mods de Minecraft, il se peut qu'il ait rencontré l'une des 87 applications malveillantes. **Il est facile de reconnaître ce type d'escroqueries :** l'application ne fonctionne pas et un message apparaît avoir cliqué sur le bouton de téléchargement. Pour les fausses applications qui téléchargent des publicités, il n'y a pas non plus de fonctionnalités permettant de jouer et l'appareil continue d'afficher des publicités injustifiées. **Toutefois, comme l'application malveillante est capable de télécharger des applications supplémentaires sur des périphériques infectés, la charge utile responsable des annonces peut, par la suite, être remplacée par des malwares plus dangereux.**
Bien que ce qui suit ne soit pas encore entré dans les habitudes des Français, **les chercheurs ESET [NDLR : et Denis JACOPINI] rappellent qu'il est important d'équiper son téléphone portable avec une solution de sécurité efficace** et adaptée aux mobiles. Il n'y a pas que les ordinateurs qui peuvent être infectés par un logiciel malveillant. En 2016, ces derniers ont augmenté de 20% sur Android™. Une solution de sécurité pour mobile permet, au même titre que celle dédiée aux ordinateurs, de détecter et supprimer les menaces.
Si un utilisateur souhaite supprimer les menaces manuellement, il doit désactiver les droits d'administrateur du périphérique pour l'application et le module téléchargés en allant dans Paramètres -> Sécurité -> Administrateur de périphériques. Il suffit ensuite de désinstaller les applications en allant dans Paramètres -> Gestionnaire d'applications.
Si vous souhaitez plus d'informations notamment sur le fonctionnement de ces logiciels malveillants, nous vous invitons à cliquer ici ou à nous contacter pour une demande d'interview. Nous vous proposons également de visualiser cette courte vidéo qui montre **l'installation de l'une de ces fausses applications.**

---

[1] « Jeu vidéo créé à partir d'un autre, ou modification du jeu original, sous la forme d'un greffon qui s'ajoute à l'original, le transformant parfois complètement. » Source : https://fr.wikipedia.org/wiki/Mod_(jeu_vid%C3%A9o)

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Risque de cyberattaque terroriste très élevé

© Dieter Telemans	Risque de cyberattaque terroriste très élevé

Le commissaire chargé de la Sécurité nous explique ce que l'Europe a fait pour améliorer la sécurité de ses citoyens. Il avoue craindre « tous les types de menaces ».

Il est « Le Dernier des Mohicans ». L'ultime commissaire britannique envoyé par Londres avant le Brexit. Dans son bureau du Berlaymont placé sous haute sécurité, trônent deux grandes photographies de Sa Majesté. Sur le sofa, des coussins décorés de l'Union Jack. « No doubt », c'est bien ici une partie de l'île encore arrimée à l'Europe.
Julian King, formé à la fois à Oxford et à l'ENA, est l'un des plus brillants diplomates du Royaume. Sa mission? Créer l'Union européenne de la sécurité ainsi que gérer la lutte contre le terrorisme et le crime.
L'Echo l'a rencontré, un an après les attentats terroristes à Bruxelles.

Comment avez-vous vécu les attaques du 22 mars?
J'étais ambassadeur du Royaume-Uni en France. Je revenais du marché de Rungis. C'était tôt le matin. J'ai mis du temps à me remettre de cette nouvelle. Dès mon retour à la résidence, j'ai demandé qu'ils mettent le drapeau en berne.

Qu'avez-vous ressenti?
Je craignais de nouveaux attentats depuis mon entrée en fonction à Paris. C'est arrivé dans la capitale du pays voisin, là où ma femme vit et travaille. Son bureau n'était pas loin de Maelbeek. J'ai eu peur que mes amis m'appellent pour m'apprendre une mauvaise nouvelle.
Trop de gens qui ont grandi dans nos pays sont partis se radicaliser en Syrie et en Irak. La prévention de la radicalisation est la clé.

Qu'est-ce que les attentats ont changé?
Après chaque attaque, à Paris, Bruxelles et Nice, j'ai été frappé de voir à quel point nos villes sont résilientes. Ces événements sont horribles. Très difficiles à vivre pour les victimes mais aussi pour les gens qui doivent monter en première ligne et tous les habitants de la ville. Je suis touché par la capacité des Belges et des Français à dépasser le drame. À reprendre leur vie. Et le lien profond qu'ils ont avec leur communauté.

Qu'a fait l'Europe, depuis lors, pour améliorer la sécurité de ses citoyens?
Nous avons commencé par renforcer les frontières extérieures. Nous avons créé un corps de garde-frontières et de garde-côtes, déployé du personnel de Frontex et d'Europol pour soutenir les autorités en Grèce et en Italie, adopté une directive sur le contre-terrorisme qui criminalise les allers-retours d'Irak et de Syrie. Nous avons renforcé le code Schengen pour contrôler systématiquement toute personne qui entre dans l'espace Schengen, y compris les citoyens Européens.
Nous avons proposé de créer un système interactif pour contrôler les nationaux des pays tiers, c'est à l'étude au Parlement. Nous allons aussi mettre en place un système de précontrôle des étrangers n'ayant pas besoin de visas, appelé Etias et calqué sur le modèle Esta des Etats-Unis.
Nous avons renforcé notre capacité de connaître ceux qui arrivent dans l'espace européen, et c'est un élément vital pour notre sécurité.

Qu'avez-vous fait pour accroître la sécurité intérieure?
Nous avons renforcé les capacités des forces de l'ordre. Nous avons mis plus d'argent, de personnel et de moyens dans Europol. Nous avons consolidé les bases de données policières et réformé la plus importante: le système Schengen. Nous voulons obliger les polices nationales à partager leurs informations à travers ce système. Dans les faits, ils le font de plus en plus. Mais ce sera encore plus vrai lorsque l'obligation d'échanger sera adoptée par le Conseil européen.
Nous devons aussi accroître la capacité des agents d'aller chercher une information là où elle se trouve.
Pour éviter, comme après les attaques de Paris, qu'un terroriste comme Salah Abdeslam puisse déjouer les contrôles…
Oui. Les renseignements existaient mais lors de ce fameux contrôle entre Paris et Bruxelles, la police n'a pas été capable d'aller les chercher. Nous allons proposer un paquet de mesures pour améliorer la qualité des informations, le traitement de données, l'utilisation plus fréquente de la biométrie et accroître la rapidité d'obtention des informations.
La moitié des business européens ont déjà subi une cyber-attaque.

Quand allez-vous proposer ces mesures?
Mon équipe y travaille, son rapport devrait être prêt d'ici avril. Nous ferons ensuite des propositions.

Les États européens appliqueront-ils ces mesures?
Nous insistons beaucoup là-dessus. Pour la première fois depuis mon arrivée l'été dernier, la Commission a lancé des procédures d'infraction contre plusieurs États qui n'appliquent pas les mesures convenues l'an dernier. Trois procédures contre des États qui n'ont pas appliqué la directive sur les explosifs et cinq procédures contre des États qui n'ont pas appliqué l'arrangement de Prüm sur les échanges d'information.

Que pensez-vous de la création d'un « FBI Européen », comme le préconise Guy Verhofstadt?
Je ne suis pas persuadé que cela arrive dans un futur immédiat. Il y a des questions légales, des difficultés constitutionnelles à lever. Mon objectif, pour le moment, est de construire une coopération pratique entre les agences de renseignements nationales. Certains prétendent qu'il n'existe aucun échange entre elles, mais ce n'est pas vrai. Cette collaboration existe, les agences européennes ont d'ailleurs depuis peu une plateforme commune aux Pays-Bas.

Vous n'aimez pas parler du Brexit. Mais dites-moi, le Royaume-Uni continuera-t-il à coopérer avec l'UE après son départ?
Je l'espère. Je ferai tout durant les deux années à venir pour renforcer notre sécurité commune contre le terrorisme, le cyberterrorisme et le crime organisé. Ces menaces affectent tous les pays d'Europe, qu'ils soient ou pas dans Schengen ou dans l'UE, et c'est le cas en particulier des cyberattaques. Notre combat sera plus efficace si nous le menons ensemble. Ce sera vrai demain, dans deux ans et dans cinq ans. Il est important qu'après le Brexit l'Union européenne et le Royaume-Uni conservent une coopération étroite en matière de lutte contre le terrorisme.

Quant à la coopération entre l'Europe et les Etats-Unis, résistera-t-elle à l'arrivée de Donald Trump?
Jusqu'à présent, tous les représentants des Etats-Unis que j'ai rencontrés ont été clairs. Ils comprennent l'importance de notre coopération et veulent la maintenir.

Quel est le niveau de risque d'attentat terroriste à Bruxelles?
Nous ne sommes pas chargés d'évaluer ce niveau, mais nous écoutons ce que chaque État nous dit. Et il est clair que la menace terroriste dans un État qui a subi une attaque est très très élevée. Il est très important de ne pas donner l'impression que la menace a disparu. Ou que nous avons réduit la menace à zéro.

Les terroristes se concentrent sur les espaces publics, les métros ou les aéroports. Comment sécuriser de tels lieux?
Chaque État a développé de très bonnes pratiques dans la gestion de la sécurité des espaces publics. Nous mettons ensemble tous les experts pour tirer les leçons des meilleures pratiques et nous dressons une liste de lignes directrices. Nous allons continuer ce travail et le faire avec les meilleurs praticiens.

Vous craignez des menaces d'isolés ou des groupes organisés?
Tous les types de menaces. Celles de loups solitaires, et c'est pourquoi la lutte contre la radicalisation est une partie importante de nos travaux. Mais aussi les menaces d'attaques organisées inspirées par Daech, qui ne sont pas réduites parce ce qu'ils sont en difficulté sur le terrain en Syrie et en Irak.

La plupart des auteurs des attaques à Bruxelles et Paris étaient Européens…
Trop de gens qui ont grandi dans nos pays sont partis se radicaliser en Syrie et en Irak. La prévention de la radicalisation est la clé.

Que fait l'Europe pour lutter contre la radicalisation?
Nous agissons à deux niveaux. D'abord nous nous attaquons à la propagande de Daech sur internet, qu'ils continuent à déverser malgré leur déroute sur le terrain. Nous travaillons pour l'instant avec les plus grands groupes du web. Nous avons besoin de leur aide pour trouver des moyens industriels qui arrêtent cette propagande.
L'autre risque majeur ce sont les gens qui, au sein des communautés, cherchent à pousser les plus fragiles à la violence. Le moyen le plus efficace pour les empêcher d'agir est de travailler localement. Nous avons développé, au niveau européen, des moyens pour œuvrer avec ces communautés, soit pas des fonds, soit par la mise en place d'un réseau d'organisations où ils reçoivent du soutien.

Craignez-vous une cyberattaque terroriste, par exemple contre une centrale nucléaire ou une tour de contrôle aérienne?
Les terroristes comme Daech n'utilisent pas, pour l'instant, de tels moyens. Mais le risque d'une cyberattaque terroriste est très élevé. La cybercriminalité augmente de manière exponentielle. Au Royaume-Uni, un pays que je connais bien, la moitié des crimes connus sont des cybercrimes. Si vous regardez l'Europe, la moitié des business européens ont déjà subi une cyberattaque.

Comment affrontez-vous ce risque?
Notre première ligne de défense consiste à avertir le public du danger de manipulation sur internet. Nous devons ensuite construire une résilience, à chaque niveau. Apprendre aux individus à protéger leurs appareils, changer leur code. Il faut aussi mettre en place les moyens nécessaires pour protéger les infrastructures critiques, comme les unités de production d'énergie, exposées aux cyberattaques. Nous travaillons à la création d'une agence européenne qui planifie la protection des infrastructures et mette en place un réseau d'échange d'information, le tout en application de la directive NIS.
Nous travaillons aussi avec le secteur privé, généralement très avancé sur ces questions de sécurité, et lancer des partenariats. Nous allons mobiliser 1,8 milliards d'euros pour des recherches en cybersécurité d'ici 2020. C'est un effort important.
Nous préparons également des exercices conjoints avec l'Otan pour contrer les cyberattaque.
*Enfin, j'espère que nous pourrons faire un examen complet de tout notre travail sur la cybersécurité sous présidence estonienne, avant la fin de cette année…**[lire la suite]***

***Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.*
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *« Le risque d’une cyberattaque terroriste est très élevé » | L’Echo*

Les Français plus vulnérables aux virus propagés par clé USB

	Les Français plus vulnérables aux virus propagés par clé USB

Les logiciels malveillants s’adaptent et les menaces en matière de cybersécurité varient d’un pays à l’autre, révèle une étude menée par la société de sécurité informatique Avira.

Vols de mots de passe, chevaux de Troie, ver, applications indésirables… En matière de cybersécurité, chaque pays «cultive» son défaut et son logiciel malveillant : tel est le principal enseignement d’une étude publiée lundi par la société de sécurité informatique Avira.
Le talon d’Achille de la France – l’un des cinq pays étudiés avec les Etats-Unis, le Royaume-Uni, l’Allemagne et l’Italie – se trouverait… dans la clé USB. Infestée de «vers».
Avira a en effet remarqué que le logiciel malveillant le plus fréquent en France était un ver, ou *worm* en anglais, de son nom technique Verecno.Gen. Son mode de contamination favori ? L’utilisation de clés USB. Celui-ci «n’est pas sans risque, rappelle la société dans son étude. Le ver Verecno est ainsi capable de se propager automatiquement dès que la clé USB est insérée dans l’appareil. Savez-vous d’où vient la clé USB qui vous est tendue ?» Avira délivre un conseil particulier aux Français : «Ne sur-socialisez pas».

A chaque pays son point faible

Les utilisateurs des Etats-Unis sont davantage vulnérables aux chevaux de Troie modifiant le comportement des systèmes d’exploitation Windows de leurs ordinateurs, les Allemands aux kits d’exploitation prospérant sur les défauts de mise à jour, les Italiens aux vols de mots de passe via les emails et les Britanniques au téléchargement d’applications indésirables.

leparisien.fr

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d’expertises, d’audits, de formations et de sensibilisation dans toute la France et à l’étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d’un Correspondant Informatique et Libertés (CIL) ou d’un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d’informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Cybersécurité : les Français plus vulnérables aux virus propagés par clé USB – Le Parisien*

Cyberattaques des présidentielles. Qui serait responsable ?

	Cyberattaques des présidentielles. Qui serait responsables ?

Les cyber-attaques que la Russie est soupçonnée de mener en France dans le cadre de la campagne présidentielle sont « une forme d'ingérence inacceptable », a estimé dimanche le ministre français des Affaires étrangères Jean-Marc Ayrault.

» Les cyberattaques russes, grande menace pour les États-Unis et l'Europe
Dans une interview au *Journal du Dimanche*, le chef de la diplomatie française a déclaré : « Il suffit de regarder pour quels candidats, à savoir Marine Le Pen ou François Fillon, la Russie exprime des préférences, dans la campagne électorale française, alors qu'Emmanuel Macron, qui développe un discours très européen, subit des cyberattaques. Cette forme d'ingérence dans la vie démocratique française est inacceptable et je la dénonce ».
« La Russie est la première à rappeler que la non-ingérence dans les affaires intérieures est un principe cardinal de la vie internationale. Et je la comprends. Et bien la France n'acceptera pas, les Français n'accepteront pas qu'on leur dicte leurs choix », a ajouté le ministre.

Quels éléments a-t-on pour de telles affirmations ?
Denis JACOPINI : Aujourd'hui la Russie, hier la Chine et demain qui ? Quels sont les éléments permettant d'affirmer de tels propos ?
L'adresse IP ?
Si c'est l'adresse IP qui est prise en compte, n'est-on nous pas en train de mélanger l'adresse IP ayant accédé aux systèmes informatiques et celle du commanditaire de l'attaque ?
Signatures et codages de caractères
Si ce sont les signatures présentes dans les codes ou les codages de caractères qui sont pris en compte, ne risque t-on pas de reproduire l'attribution hâtive de l'attaque de la chaîne TV5 monde à l'Etat islamique
alors même que très vite après l'attaque, de nombreux experts avaient mis en doute la crédibilité de la revendication.
A mon avis
En raison du refus de certains pays pour coopérer en matière de lutte contre la cybercriminalité, il devient très compliqué de remonter jusqu'aux ordinateurs utilisés pour mener de telles attaques, pire encore pour remonter jusqu'aux commanditaires des attaques informatiques. Les infos circulant encore ce matin font référence une fois de plus à des accusations qui sembleraient bien être sans preuve…
Malgré l'absence de preuve, Ayrault dénonce une «ingérence» de la Russie dans la présidentielle
Je serais bien intéressé
En tant qu'Expert judiciaire spécialisé en cybercriminalité, je serais bien intéressé pour expertiser les éléments concernés par cette affaire.
A bon entendeur…

Qu'en pensez-vous ? Merci de me laisser votre avis ou commentaire

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Paris dénonce à nouveau les cyberattaques de Moscou*

Des élèves de plus en plus confrontés au cyberharcèlement

Des élèves de plus en plus confrontés au cyberharcèlement

Brimades, insultes, sexting (envoi de messages et photos explicites)… un adolescent sur six, en moyenne, est confronté au harcèlement. Un sujet qui reste pourtant tabou. L'école IESPP a décidé de prendre le problème à bras-le-corps et de lancer des ateliers de sensibilisation auprès de ses plus jeunes élèves.

On sait à quel point les enfants peuvent être cruels entre eux… mais désormais, avec les réseaux sociaux et les smartphones, les conflits qui éclatent à l'école se poursuivent jusqu'à la maison : « *Ils sont tellement connectés H24 qu'il n'existe plus cette frontière, ce temps de répit le soir*…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Des élèves de plus en plus confrontés au cyberharcèlement – Édition digitale de Charleroi*

Popcorn Time, un rançongiciel bien vicieux

Popcorn Time, un rançongiciel bien vicieux

Depuis peu, les rançongiciels (ou ransomware) constituent de véritables fléaux dans l'univers de l'informatique et du web. Ils touchent les données personnelles de millions de gens de par le monde. Les experts en sécurité se sont même mis à taxer 2016 comme étant « l'année des rançongiciels ».

Payez ou infectez vos amis

Sur cette année, il se peut que Popcorn Time soit le rançongiciel qui vienne clore la propagation de ces logiciels de chantage. Ce nouveau ransomware pose un gros dilemme à sa victime en lui imposant de payer une rançon ou d'infecter ses amis.

Pour commencer, il emprunte le nom d'une application de streaming vidéo ayant défrayé la chronique en 2015, ce qui incite au téléchargement de celle-ci. Ensuite, il infecte l'ordinateur de la victime par le biais d'un courriel piégé ou d'un lien malveillant, puis crypte ses données personnelles en usant d'un algorithme de chiffrement AES 256 bits.

Après que les données ont été cryptées, il impose à la victime de donner la valeur de 1 bitcoin (soit environ 700 €) ou de le transmettre sur l'ordinateur d'un ami. C'est une méthode toute nouvelle avec en plus une limite du nombre d'introductions de clé de déchiffrement. Entrer quatre fois la mauvaise clé ferait perdre définitivement ses données.

Les dossiers Windows sont les premières cibles

D'après la conclusion des enquêtes réalisées par le site Bleeping Computer sur ce rançongiciel, il ciblerait en premier les fichiers présents dans les dossiers Windows : Mes Documents, Images, Musiques et toutes les données sur le Bureau.

Afin de faire face à ce logiciel de rançon, la meilleure façon pour un utilisateur lambda est de prendre des précautions préventives basées sur les mesures de sécurité les plus basiques :

• faire des copies de ses données personnelles vers un support externe qui se débranche de l'ordinateur après chaque usage de ce dernier et sur les Clouds comme Dropbox, OneDrive, Google Drive, Mediafire, Mega, pCloud, Flipdrive… ;

• éviter d'ouvrir les mails aux destinateurs inconnus et contenant des liens ou des pièces jointes. Il est aussi possible que Popcorn Time provienne d'une personne de votre liste de contact. Prenez les mêmes réserves tant que le contenu n'a pas été formellement reconnu ;

• mettre à jour son système d'exploitation et son antimalware.

…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Certifié ISO 27005 Risk Manager, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

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

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

---

Réagissez à cet article

Original de l’article mis en page : Popcorn Time : le plus vicieux rançongiciel de cette année – @Sekurigi

---

Alerte ! Un virus informatique peut vider votre compte bancaire

	Alerte ! Un virus informatique peut vider votre compte bancaire

---

77% des ménages possèdent un ordinateur et 75% une connexion internet. A l'heure ou le numérique gagne toujours plus de terrain, de nouvelles menaces s'invitent dans nos foyers, les virus.
Quand les nouvelles technologies veulent nous simplifier la vie en numérisant toutes nos informations, les hackers eux, redoublent d'ingéniosité pour créer des virus de plus en plus performants. Tous les jours des dizaines ne milliers de nouveaux virus sont créés, et si l'efficacité des antivirus est parfois relative, il reste que nous manquons aussi de vigilance.

Avertissement de la gendarmerie
« En consultant internet, une mise en garde indique que votre ordinateur est infecté par le virus « Zeus ». La page d'alerte vous oriente alors vers le numéro de téléphone d'un spécialiste de la sécurité informatique. […] L'escroc, homme ou femme, recommande alors le nettoyage de votre ordinateur et l'intégration à distance d'un antivirus, moyennant une somme d'argent variant entre 99 et 249 euros. »

C'est le message que la gendarmerie du Cher a fait paraître sur son Facebook afin de prévenir la population. Ce nouveau virus est d'autant plus dangereux que le hacker, télécharge et utilise vos données bancaires pendant que vous payez l'antivirus recommandé. Prudence donc si ce message apparaît sur votre écran, n'appelez surtout pas et confiez votre ordinateur à un spécialiste…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Certifié ISO 27005 Risk Manager, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Original de l'article mis en page : « Zeus » : un virus informatique qui peut vider votre compte bancaire !