Les avions, vraiment insensibles aux cyber-attaques ?

Les avions, vraiment insensibles aux cyber-attaques ?

Après le piratage des voitures connectées et la profusion des attaques cybernétiques à travers le monde, une question se pose : les appareils volants peuvent-ils être eux aussi victimes de ce genre d'incident ? Car force est de constater que les avions de nouvelle génération embarquent bon nombre de systèmes connectés. Sachez cependant que « c'est impossible » selon les experts. Si des tentatives de hacking sont bel et bien enregistrées, la conception de l'appareil permet d'y faire face.

Ces campagnes de hackings n'aboutissent jamais affirment les experts

Une cyber-attaque contre un avion et sa multitude de systèmes connectés est un formidable défi pour les hackers. Toutefois, aucune n'a eu d'effet, le risque étant pris en compte dès la conception des appareils, selon les experts.

En témoigne la déclaration de Pascal Andréï, qui affirme que les tentatives, même, si elles sont nombreuses, n'ont pas abouti jusqu'à maintenant. De plus, ce directeur de la sécurité aérienne du groupe Airbus rajoute que la plupart des hackers veulent juste faire le buzz en faisant savoir qu'ils peuvent contrôler un avion à distance. M. Andréï a annoncé ces propos durant le « Paris Air Forum « qui rassemble chaque année plusieurs experts du domaine de l'aéronautique.

Une équipe d'élite spécialement choisie pour venir à bout des hackers

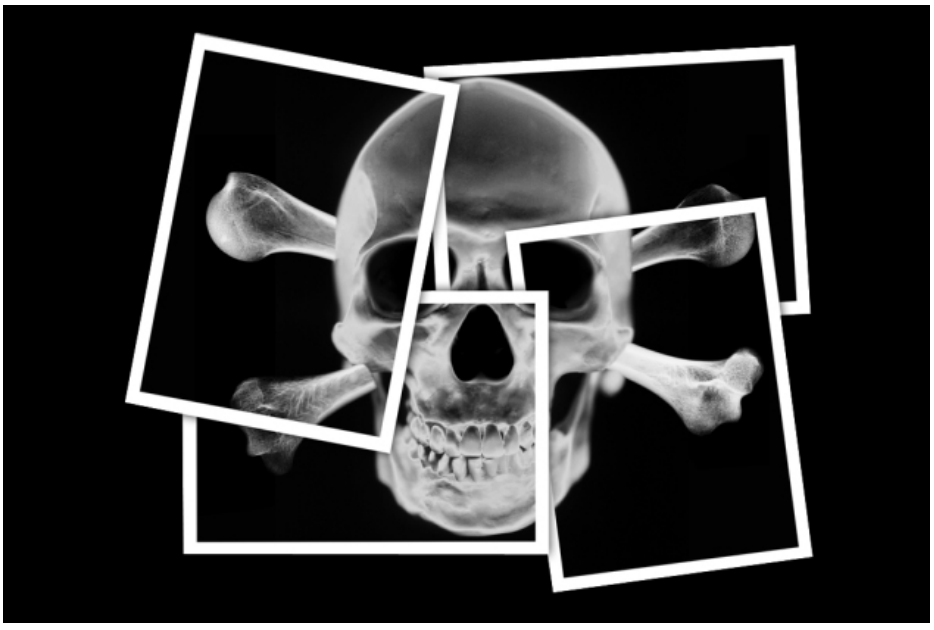
Pour faire face à ses nombreuses menaces, les constructeurs ont mis en place leurs propres armées de pirates informatiques. Thales, l'un des leaders européens de la cybersécurité et le leader mondial de la protection des données en déploient notamment plusieurs centaines pour contrôler la vulnérabilité de ses clients. Selon Marc Damon,directeur général délégué de Thales responsable des activités système d'information et de communication sécurisés, 4 plans de défense doivent être mis en place pour faire face aux attaques. Pour commencer,il y a « les règles fondamentales ». Celles-ci comprennent l'actualisation des serveurs, des logiciels, le changement permanent des mots de passe, la surveillance des téléchargements…Vient ensuite « l'intégration des systèmes de cyber-sécurité dès la conception », puis la « supervision des systèmes » et pour finir le « chiffrement des données »…[lire la suite]

Réagissez à cet article

Source : *Les avions, insensibles aux cyber-attaques –*

@Sekurigi

Non, NotPetya n’est pas un ransomware… mais un logiciel de sabotage



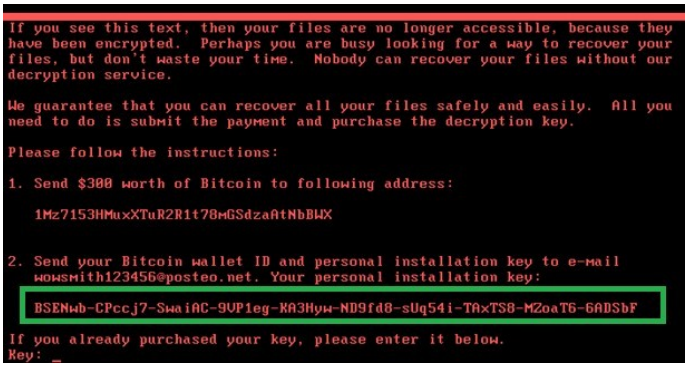
Non, NotPetya n’est pas un ransomware… mais un logiciel de sabotage

---

Le déchiffrement des machines impactées est impossible. La demande de rançon n'était donc qu'un leurre pour camoufler un cybersabotage. La piste d'un acte politique, probablement réalisé par une agence gouvernementale, émerge.

Mauvaise nouvelle pour toutes les victimes de NotPetya. Les dernières analyses des chercheurs en sécurité montrent que ce malware est en réalité un logiciel de sabotage déguisé en ransomware. Les victimes ne pourront donc retrouver leurs données, à moins qu'un expert arrive à détecter une faille dans le processus de chiffrement.

Plusieurs indices prouvent que les auteurs de NotPetya n'ont jamais eu l'intention d'envoyer une quelconque clé de déchiffrement. Le premier concerne l'identifiant unique affiché dans le message de rançonnage et que la victime doit envoyer aux pirates après avoir effectué le paiement en bitcoins. En théorie, cet identifiant doit permettre aux auteurs de NotPetya d'identifier la victime. Il doit, par conséquent, contenir des informations sur les clés de chiffrement utilisées sur la machine en question. Mais selon les chercheurs de Kaspersky, il s'avère que cet identifiant est totalement aléatoire. *« Les attaquants ne peuvent extraire une quelconque information de déchiffrement d'une telle suite de caractères aléatoire »*, soulignent-t-ils dans une note de blog.



Kaspersky – L'identifiant unique affiché est totalement aléatoire

De son côté, le chercheur en sécurité Matt Suiche a découvert que les données de la zone d'amorçage ne sont sauvegardées nulle part, mais simplement remplacées par autre chose. Le système de fichier du disque serait donc de toute façon irrécupérable. *« La version actuelle de Petya a été réécrite pour être un wiper, et non un ransomware »*, souligne l'expert….[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Non, NotPetya n’est pas un ransomware… mais un logiciel de sabotage*

La montre connectée, l’objet connecté portable largement en tête des ventes

La montre connectée, l’objet connecté portable largement en tête des ventes

---

De tous les objets connectés portables, c'est la montre connectée qui emporte massivement l'adhésion des acheteurs selon le cabinet d'analystes IDC pour les 4 ans qui viennent. Les montres connectées représenteront 67% des objets connectés portables vendus en 2021.

Les bracelets connectés à petite vitesse

Ce sera loin devant les bracelets connectés, qui représenteront 21,7% des achats. En troisième position, vient une catégorie nouvelle : les vêtements connectés, qui pèsent toutefois à peine 9% des achats. Entre 2017 et 2021, le nombre d'objets connectés portables achetés va doubler. Il se vendra 125,5 millions d'objets connectés portables cette année. Cela montera à 240,1 millions en 2021. Cela représente une croissance annuelle moyenne de 18,2%.

Le défi des objets connectés portables désormais est de disposer du bon logiciel pour collecter, analyser et présenter des informations importantes à partir des données. Ces objets connectés doivent proposer la bonne expérience à l'utilisateur. L'heure est aux développeurs et aux entreprises pour délivrer les bons services et les bonnes Apps.

Des montres connectées multi-applications

Les ventes de montres connectées haut de gamme capables d'accepter des applications tierce partie, comme l'Apple Watch, la Samsung Gear, et toutes les montres sous Android, seront dopées par la présence des réseaux mobiles plus disponibles.

Quant aux bracelets connectés, la croissance de leurs ventes sera faible. Les acheteurs opteront pour les montres lorsqu'ils voudront des fonctions supplémentaires et du multi-usage.

Les vêtements connectés sont la nouveauté du classement d'IDC. Ce marché est dynamisé par les fabricants chinois souligne IDC. Ils fournissent des chemises, ceintures, chaussures, chaussettes, le tout connecté. Ces objets sont surtout employés par des sportifs professionnels afin d'améliorer leurs performances et non par le grand public. Le projet Jacquard de Google avec Levi's pour des blousons connectés cette année pourrait changer cette situation…[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

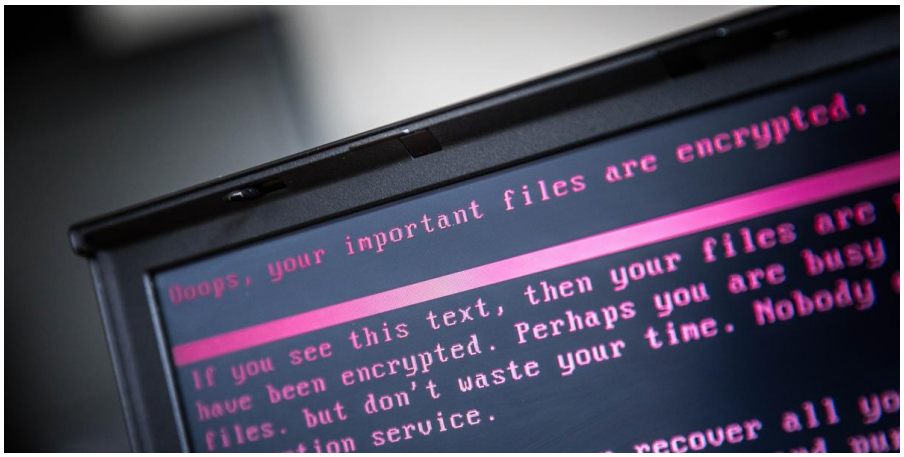
Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *La montre connectée, l'objet connecté portable largement en tête des ventes | La Revue du Digital*

Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?



Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?

Il s'est répandu à très grande vitesse, et est plus évolué que son prédécesseur, WannaCry.

Après WannaCry, Petya. Pour la deuxième fois en quelques semaines, un « rançongiciel » (*ransomware*, en anglais) s'est largement propagé sur Internet, rendant inutilisable de nombreux ordinateurs et perturbant lourdement le fonctionnement de plusieurs grandes entreprises.
Le code de ce rançongiciel a été disséqué par de nombreux experts et entreprises de sécurité informatique ces dernières heures, permettant de mieux comprendre la manière dont il fonctionne.

Que fait-il exactement ?

Petya est un rançongiciel visant les systèmes Windows : il rend indisponibles les données d'un ordinateur, qui ne peuvent être déverrouillées qu'en versant une rançon. Il s'agit d'une variation très modifiée d'une souche apparue au printemps 2016.
A la différence de WannaCry, Petya commence par s'attaquer à la toute petite partie du disque dur – qui recense tous les fichiers présents dans la mémoire d'un ordinateur – et la chiffre, les rendant inutilisables. Ensuite, il s'en prend à la partie du disque dur qui permet de lancer le système d'exploitation, le logiciel qui fait fonctionner l'ordinateur. Cette partie est modifiée de manière à ce que l'ordinateur ne puisse plus démarrer en utilisant le système d'exploitation prévu. Lorsqu'on allume l'ordinateur, c'est Petya qui se lance, et le rançongiciel fait son travail. Un message s'affiche alors, réclamant que soient envoyés 300 dollars en bitcoin, la monnaie électronique, pour obtenir la clé de déchiffrement.
Il est extrêmement déconseillé de verser la rançon : outre le fait que payer entretient les réseaux mafieux qui se cachent souvent derrière les rançongiciels, l'adresse e-mail qui servait aux auteurs de Petya à rentrer en contact avec les victimes a été désactivée par le fournisseur de messagerie, rendant tout versement parfaitement inutile.

Comment se propage-t-il ?

Les développeurs de ce logiciel ont mis beaucoup de soin aux fonctionnalités d'infection de Petya, qui utilise plusieurs méthodes de propagation dites « *latérales* », vers les ordinateurs appartenant au même réseau que la machine infectée.
Une fois installé sur un ordinateur, Petya va chercher à y obtenir les plein pouvoirs et repérer les autres appareils branchés sur le même réseau. Le rançongiciel va ensuite fouiller dans l'ordinateur qu'il a infecté pour récupérer des identifiants et des mots de passe qu'il va pouvoir ensuite réutiliser dans le réseau pour prendre le contrôle de davantage d'appareils et démultiplier sa propagation. Ensuite, à l'aide de fonctionnalités classiques de Windows utilisées pour gérer les réseaux, il va se transférer vers d'autres machines.
Outre cette fonctionnalité, il utilise aussi deux outils – EternalBlue et EternalRomance – volés à la NSA, la puissante agence de renseignement américaine, qui, en exploitant une faille dans un protocole permettant aux ordinateurs de se « parler » au sein d'un même réseau, permettent sa propagation de machine en machine. EternalBlue était d'ailleurs déjà utilisé par WannaCry.
L'utilisation de plusieurs méthodes d'infection expliquerait pourquoi certaines machines pourtant immunisées contre EternalBlue et EternalRomance, car ayant installé les mises à jour de sécurité correspondantes de Microsoft, soient quand même infectées par Petya.
Son mécanisme de propagation à l'intérieur d'un réseau d'une entreprise fait que les postes de travail classiques ne sont pas les seuls à succomber à Petya. Des ordinateurs plus centraux, plus sensibles, sont aussi atteints, comme les serveurs sur lesquels fonctionnent les sites Web. C'est pour cette raison que plusieurs sites du groupe Saint-Gobain étaient inaccessibles mercredi 28 juin au matin, selon une source interne…[lire la suite]

Réagissez à cet article

Source : *Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?*

La SNCF et le groupe Auchan touchés par la cyberattaque mondiale

La SNCF et le groupe Auchan touchés par la cyberattaque mondiale

La France n’a pas été épargnée. La SNCF fait partie des entités subissant une cyberattaque mondiale en cours, mais celle-ci est « contenue », a indiqué ce mardi le groupe ferroviaire.…[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 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 sur cette page.

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

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

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

Contactez-nous

Réagissez à cet article

Voilà la prochaine cyberattaque

Voilà la prochaine cyberattaque

Après WannaCry et ses 200.000 demandes de rançon, une nouvelle cyberarme cible les réseaux électriques. Où sont les failles? Nos industries sont-elles parées? Enquête exclusive.

À lui seul, son nom file déjà des frissons. Baptisé “Industroyer” (contraction des termes anglais “industrial” et “destroyer”), un nouveau virus vient d’être identifié par des chercheurs en sécurité informatique. Il s’agit d’un puissant logiciel malveillant, voire une cyberarme de destruction massive. Ce virus industriel cible en effet le secteur de l’énergie. “C’est même la menace la plus puissante pour les systèmes de contrôle industriels depuis Stuxnet!”, enchérit le spécialiste slovaque en cybersécurité ESET, codécouvreur de cette nouvelle menace avec l’américain Dragos.
Pour rappel, le ver informatique Stuxnet, attribué aux services secrets américains et israéliens, a saboté une centrale nucléaire iranienne en 2010, provoquant même des explosions. Une première mondiale dans l’histoire du piratage informatique, qui aurait pu se solder selon les experts russes par un accident pire que celui de Tchernobyl. Le potentiel de cette super-mine numérique? D’après ces chercheurs européens et américains, Industroyer serait déjà responsable du piratage du réseau ukrainien en décembre 2016, qui avait privé une partie de Kiev d’électricité pendant plus d’une heure. “Ce nouveau virus peut être immédiatement adapté pour attaquer des réseaux en Europe et dans une partie du Moyen-Orient et de l’Asie”, avertit encore l’expert US. Cette cyberarme peut-elle dès lors frapper la Belgique, pays fortement nucléarisé et très densément électrifié? Se couvrant derrière le secret-défense, aucun opérateur belge ne se risque à y répondre…[lire la suite]

Bref commentaire de Denis JACOPINI :
Les années nous ont donné raison, nous les lanceurs d’alertes qui sensibilisons les décideurs et les élus depuis des années en tirant la sonnette d’alarme pour anticiper les risques. Chaque jour qui passe nous donne raison nous comptons les victimes de la cybercriminalité par milliers.
Le cybercrime peut prendre de nombreuses apparences, mais les décideurs et les élus, pénalement responsables aussi bien des fuites de données que de la perte des données doivent prendre les devants. Fort de nos années d’expérience dans ce domaine, nous organisons, en collaboration avec les CCI, les clubs d’entreprises et les centres de formations des sessions de sensibilisation aux risques informatiques et à la mise en conformité de vos données personnelles.
Contactez-nous

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Voilà la prochaine cyberattaque | Moustique.be*

---

198 millions de données personnelles d'Américains ont été exposées

198 millions de données personnelles d'Américains ont été exposées

---

Un chercheur en cybersécurité a découvert, le 12 juin, 1 téraoctet d'informations issues de fichiers électoraux ou d'analyses de données, librement accessibles en ligne. Derrière la faille, une société qui compte le Parti républicain parmi ses clients.

Noms, prénoms, dates de naissance, adresses postales et mail, numéros de téléphone, affiliations politiques et origines ethniques autodéclarées : autant de données personnelles qu'accumulent les (très bavards) fichiers électoraux américains. Et dont les deux grands partis, et les entreprises spécialisées dans le *big data* ou le pilotage de campagne électorale, font leur miel. Or le 12 juin, Chris Vickery, chercheur pour l'entreprise de cybersécurité Upguard, a découvert qu'une telle base de données concernant 198 millions d'électeurs, soit près de 99% des inscrits, était librement accessible en ligne, sans identifiant ni mot de passe, dans un espace de stockage loué à Amazon… Aux informations issues des fichiers électoraux s'ajoutaient en outre des éléments «prospectifs» issus d'analyses de données : la religion supposée, mais aussi la probabilité d'avoir voté Obama en 2012, ou d'adhérer à la politique «*America First*»de Donald Trump…[lire la suite]

Réagissez à cet article

Source : *Les données personnelles de 198 millions d'Américains ont été exposées – Libération*

Les entreprises du CAC 40 sont la cible de cyberattaques

Les entreprises du CAC 40 sont la cible de cyberattaques

Renault n'est pas la seule entreprise dans le viseur des cyberterroristes. Les champions de la défense et les géants de la Bourse peaufinent leur bouclier.
par Guerric PONCET

« En 2016, de gros industriels ont été touchés et des géants du CAC 40 ont pris conscience qu'ils pouvaient disparaître du jour au lendemain à cause d'une cyberattaque », nous confie Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi). « Je veux dire que, si leur piratage était dévoilé, ils étaient *OPAbles* le lendemain », précise-t-il. En effet, la révélation d'une telle attaque ferait immédiatement chuter le cours de la Bourse…
Nos champions de la cybersécurité, Airbus, Thales, Capgemini et Orange en tête, sont sollicités de toutes parts par les comités exécutifs. Mais leurs tarifs sont souvent hors de portée des PME : dans le cyber, la défense coûte cent fois le prix de l'attaque. Et, quand bien même, le budget ne fait pas tout : JP Morgan, Yahoo !, Adobe, Visa ou encore Sony ont beau avoir alloué des centaines de millions de dollars à leur sécurité informatique, ils ont tous vécu des intrusions gravissimes. « Il est impossible de créer un cyberbouclier infaillible », tranche Guillaume Poupard, pour qui il faut avoir « une bonne gouvernance avant même de parler technique ». « Jusqu'à présent, nous avons stoppé les attaques majeures qui nous visaient, mais, si l'une d'elles réussissait, ce serait une catastrophe, avec des conséquences sur la souveraineté économique de la France et, très rapidement, sur la sécurité des populations », nous glisse, sous le couvert de l'anonymat, le responsable de la sécurité informatique d'une entreprise classée « opérateur d'importance vitale » (OIV).
Des exercices de crise sont régulièrement menés pour anticiper et limiter les dégâts que créerait assurément une cyberattaque chez un OIV – panne générale dans la production électrique, paralysie des transports, implosion des télécoms… Des agents de l'Anssi jouent aux hackers, tentent de déjouer les systèmes de sécurité… et y parviennent : « La dernière fois, ils ont pris le contrôle d'une partie de notre système assez facilement, ils auraient pu créer des accidents graves », reconnaît, lui aussi en toute discrétion, le responsable informatique d'un autre OIV. Nous voilà rassurés…[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 : *Cyberguerre : le CAC 40 dans le viseur – Le Point*

Protégez-vous contre la cybercriminalité, les experts mettent en garde les business et le public Seychellois

Protégez-vous contre la cybercriminalité, les experts mettent en garde les business et le public Seychellois

Suite à la cyber-criminalité, une vigilance extrême a été conseillée aux hommes et femmes d'affaires et le public général aux Seychelles qui procèdent à des transactions monétaires en ligne.

Les experts aux Seychelles ont avertis, mercredi, lors d'une conférence de presse, que les messageries électroniques de certains hommes d'affaires sont piratées par des criminels internationaux très bien organisés, et des informations personnelles sont volées afin de détourner des transactions financières de leurs destinations d'origine.

Un représentant de l'Association des banquiers (la ***Bankers Association***), Norman Weber, explique que pour prévenir la perte d'argent par ce genre d'interception, il est de la responsabilité de l'homme d'affaire de vérifier l'authenticité des détails qui lui sont envoyés.

« Il est important de connaître le fournisseur avec lequel vous avez affaire. Si vous recevez, par email, de nouvelles instructions relatives à un transfert bancaire, cela ne coûte pas plus que ça de vérifier l'information par un appel », a exprimé N Weber.

Une autre arnaque populaire, qui a attiré l'attention de la police, concerne de faux profils sur les réseaux sociaux, généralement sur Facebook, que les criminels utilisent pour offrir des prêts attractifs à leurs potentielles victimes. Les membres du public ont été conseillés de ne pas entrer en contact avec ces arnaqueurs sur Facebook.

Avant que vous receviez le prêt « vous devrez payer les frais juridiques et administratifs. Au moment où vous vous rendrez compte [qu'il s'agit d'une arnaque] vous aurez déjà perdu beaucoup d'argent. » a déclaré le directeur de la cellule de renseignement financier des Seychelles (la **Financial Intelligence Unit** FIU), Philip Moustache.

P. Moustache a expliqué que ce qui rend ces transactions financières si difficiles à tracer, c'est qu'elles ne passent pas par les banques, l'arnaqueur demande que les transactions passent par **Western Union** ou Moneygram.

La police a annoncé mercredi qu'ils avaient reçu huit cas signalés cette année, où des locaux avaient été victimes de fraudes sur Internet et avaient perdu de grosses sommes d'argent. L'année dernière, 18 cas similaires ont été signalés.

Jusqu'à présent, il n'y a pas eu de cas rapportés relatifs à des transactions faites sur PayPal ou eBay.

« Les enquêtes réalisées ont montré que ces activités sont menées par des personnes dans des pays étrangers et que pour cette raison, il est presque impossible pour la police locale de lutter contre ce type de criminalité, comme nous n'avons pas juridiction dans ces pays », a déclaré Reginald Elizabeth, Commissaire de Police.

Comme il est difficile de mener une enquête dans ces pays, lorsque Interpol est impliqué, la piste de l'argent est devenue froide et l'argent a été retiré du compte bancaire.

La Banque Centrale des Seychelles (la CBS) travaille en étroite collaboration avec la police et l'Association des banquiers afin de mettre en place un programme de sensibilisation du public concernant ces transactions.

Le Premier Sous-Gouverneur de la Banque Centrale, Christopher Edmond, a informé que « la banque cherche un consultant en cyber-sécurité afin de réaliser une évaluation de ses systèmes en place, afin de s'assurer que ces fraudes n'aient pas lieu dans la juridiction des Seychelles. »…[lire la suite]

Réagissez à cet article

Source : *Protégez-vous contre la cybercriminalité, les experts mettent en garde les business et le public Seychellois. – Seychelles News Agency*

Comment fait le robot Handle à deux roues de Boston Dynamics pour tenir en équilibre ?

Comment fait le robot Handle à deux roues de Boston Dynamics pour tenir en équilibre ?

Cette vidéo de Boston Dynamics montre les prouesses de son tout dernier robot, présenté en février 2017. On en apprend un peu plus sur les capacités de cette étrange machine montée sur deux roues capable d'effectuer des bonds de 1,20 mètre de haut.

Cette vidéo de Boston Dynamics montre les prouesses de son tout dernier robot, présenté en février 2017. On en apprend un peu plus sur les capacités de cette étrange machine montée sur deux roues capable d'effectuer des bonds de 1,20 mètre de haut.
Début février 2017, une vidéo saisie lors d'une conférence de présentation à huis clos organisée par la société nord-américaine Boston Dynamics nous faisait découvrir leur dernière création : Handle, un robot bipède monté sur roues doté d'une agilité surprenante. L'entreprise spécialisée en robotique, filiale d'Alphabet (maison-mère de Google), vient de publier cette vidéo officielle qui livre un aperçu plus précis de ce que peut faire Handle…[lire la suite]

Commentaire de Denis JACOPINI :

Un objet connecté de plus à sécuriser…

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 : *Vidéo | Handle, le robot à deux roues de Boston Dynamics, dévoile d'étonnantes capacités*