Alerte ! Campagne de pourriels avec documents Microsoft Office malveillants | Le Net Expert Informatique

	Alerte ! Campagne de pourriels avec documents Microsoft Office malveillants

Le CERT-FR alerte sur des pourriels qui se diffusent depuis une semaine en dépit des filtres antispam : attention aux macros malveillantes qu'ils diffusent !

Depuis une semaine, il est observé à l'échelle nationale une vague de pourriels dont le taux de blocage par les passerelles antispam est relativement faible.
Ces pourriels embarquent des documents Microsoft Office contenant des macros VBA malveillantes. Ces macros ont pour but d'infecter la victime avec Dridex, qui est un logiciel malveillant de type bancaire.
Selon les échantillons, le téléchargement de Dridex peut être effectué de deux façons différentes :
• la macro VBA télécharge puis exécute un script à partir du site pastebin.com. Ce dernier télécharge ensuite le binaire Dridex à partir d'un serveur malveillant ;
la macro VBA télécharge directement le binaire Dridex à partir d'un serveur malveillant.

Il est intéressant de noter que ces pourriels sont très souvent rédigés dans un français sans faute. Le sujet et le contenu du pourriel mentionnent des problèmes de facturation, dans la plupart des cas, pour inciter la victime à ouvrir la pièce jointe.

Le format utilisé dans cette campagne pour les documents malveillants est peu rencontré. En effet, si l'on connaît déjà bien les formats OLE et OpenXML, deux autres formats moins connus commencent à être de plus en plus utilisés pour la propagation de contenu malveillant. Il s'agit du format XML, déjà mentionné dans le bulletin d'actualité CERTFR-2015-ACT-017, et du format MIME HTML qui est le format utilisé dans cette campagne. Ces deux derniers formats ont l'avantage pour les attaquants d'être souvent moins bien détectés par les antivirus.
Bien sûr, les techniques classiques d'obfuscation du code VBA, telles que celles décrites dans le bulletin d'actualité précédemment mentionné, sont toujours utilisées.
A travers les échantillons qui ont pu nous être remontés, le CERT-FR a pu observer les URLs de téléchargement via pastebin suivantes (toutes les URLs suivantes ont été démilitarisées par l'adjonction du suffixe _BAD_ aux noms de domaines et adresses IP) :
http://pastebin.com._BAD_/download.php?i=2YzPHtum
http://pastebin.com._BAD_/download.php?i=wLeUenhF
http://pastebin.com._BAD_/download.php?i=umCDngcn
Pour les documents dont la macro VBA télécharge directement Dridex, le CERT-FR a pu observer les URLs de téléchargement suivantes :
http://www.adriatic-stone.hr._BAD_/64/11.exe
http://gb000424.ferozo.com._BAD_/25/10.exe
Enfin, les échantillons Dridex ainsi récupérés tentent de communiquer avec les serveurs suivants :
https://94.23.53.23._BAD_:2443/
https://176.99.6.10._BAD_:8443/
https://173.230.130.172._BAD_:2443/
https://203.151.94.120._BAD_:4443/
https://31.186.99.250._BAD_:8443/
https://146.185.99.250._BAD_:8443/
https://185.12.95.40._BAD_:7443/
https://50.63.174.16._BAD_:6443/
https://79.143.191.147._BAD_:6443/
https://37.143.9.63._BAD_:4433/
Afin de se protéger contre ce type de menace, les conseils habituels sont rappelés :
ne pas ouvrir les documents ou les pièces jointes non sollicitées ;
désactiver l'exécution automatique des macros dans les suites bureautiques ;
maintenir le système d'exploitation et l'anti-virus à jour.
La désactivation de l'exécution automatique des macros se paramètre dans le menu suivant :
Fichier / Options / Centre de gestion de la confidentialité / Paramètre du Centre de gestion de la confidentialité / Paramètres des macros / Désactiver toutes les macros avec notifications
Documentation
Recrudescence des attaques par macro « Visual Basic for Applications » dans les documents Microsoft Office – Bulletin d'actualité CERTFR-2015-ACT-017 :
http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-017/index.html
CVE-2012-0158 exploit evades AV in Mime HTML format :
http://blog.malwaretracker.com/2013/08/cve-2012-0158-exploit-evades-av-in-mime.html5
3

Afin de se protéger contre ce type de menace, les conseils habituels sont rappelés :
• ne pas ouvrir les documents ou les pièces jointes non sollicitées ;
• désactiver l'exécution automatique des macros dans les suites bureautiques ;
• maintenir le système d'exploitation et l'antivirus à jour.

Le bulletin d'actualité du CERT-FR détaille les formats de documents et techniques utilisées ainsi que les parades à mettre en place.
Note :
*VBA : Visual Basic for Application est une implémentation de Microsoft Visual Basic intégrée dans l'ensemble des applications de Microsoft Office.

Pour aller plus loin :
Consulter les bulletins d'actualité sur le site du CERT-FR, le bulletin du 15 juin à : http://www.cert.ssi.gouv.fr/site/CERTFR-2015-ACT-024/index.html

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.ssi.gouv.fr/actualite/campagne-de-pourriels-avec-documents-microsoft-office-malveillants/
Par l'ANSSI

Amazon pourrait vous proposer de devenir livreur | Le Net Expert Informatique

Amazon pourrait vous proposer de devenir livreur

Après les drones, l'impression 3D et les coffres de voitures, Amazon cherche de nouveaux moyens de livrer rapidement un colis. Le groupe américain pourrait permettre à n'importe qui de livrer un produit.

Devenir livreur occasionnel, voilà ce que pourrait prochainement proposer Amazon. Le groupe américain réfléchirait à un nouveau moyen de conduire un colis d'un point A vers un point B. Baptisé en interne « Sur ma route », le dispositif s'ouvrirait à n'importe quelle personne.
Selon le Wall Street Journal, ceux qui désirent devenir livreur d'un jour disposeront d'une application mobile. Cet outil sera chargé de recenser les personnes qui attendent leur colis et les lieux qui disposent d'une commande en attente. On pense par exemple aux points relais ou à d'autres intermédiaires.
Cet outil soulève naturellement des questions quant à la sélection des livreurs. A l'instar d'Uber ou d'eBay, Amazon pourrait introduire un système de notation des personnes participantes. Néanmoins, la question de la responsabilité en cas de perte du colis reste entière.
La problématique du paiement des livreurs occasionnels est également importante. Amazon devra en effet les inciter à participer sans que cela fasse grimper la facture globale. L'an dernier, le groupe avait testé la livraison par le biais des véhicules Uber et des conducteurs de taxis en facturant 5 dollars le transport de chaque colis. L'expérience s'est toutefois arrêtée à l'état de test dans la seule ville de San Francisco.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://pro.clubic.com/entreprises/amazon/actualite-770702-amazon-livraison.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_18/06/2015&partner=-&svc_position=1024725737&svc_misc=-&crmID=639453874_1024725737&estat_url=http%3A%2F%2Fpro.clubic.com%2Fentreprises%2Famazon%2Factualite-770702-amazon-livraison.html

Votre identité complète ne coûte que 70 dollars sur le Dark Web | Le Net Expert Informatique

La croissance galopante de la cybercriminalité n'a d'égal que la sophistication de ses techniques. L'objectif de ces attaques: le vol de données personnelles afin de les revendre au plus offrant. Des chercheurs en sécurité informatique ont sondé pendant plusieurs mois le Darkweb afin de dévoiler les dessous des marchés cybercriminels et d'en dévoiler les tarifs en vigueur.

Les bas-fonds du web regorgent de produits illicites: drogues, armes, tueurs à gages, malwares… sont autant de biens et services qu'il est possible de vendre ou d'acheter à des prix variables en toute impunité puisque ces transactions sont intraçables. Car comme nous l'explique Jérôme Granger, chargé de la communication de ce groupe d'experts qui a fouillé ces marchés parallèles (comme Silkroad Reloaded, DeepBay, Pandra ou encore Agora), «les vendeurs accordent beaucoup d'importance à leur réputation et ils vont du coup proposer des prix défiant toute concurrence pour 'un produit de qualité'». À l'heure où des entreprises payent des mille et des cents pour les obtenir afin de nous bombarder de publicités ciblées, nous nous sommes déjà tous demandé ce que valaient nos vies privées sur le marché noir. Des chercheurs du G DATA SecurityLabs ont enquêté et ont passé au crible le fonctionnement de ces lieux d'échanges où moult produits et services illégaux sont disponibles. Et les résultats sont édifiants «puisque nos identités ne valent rien», nous glisse M.Granger.

Grosse quantité à petits prix

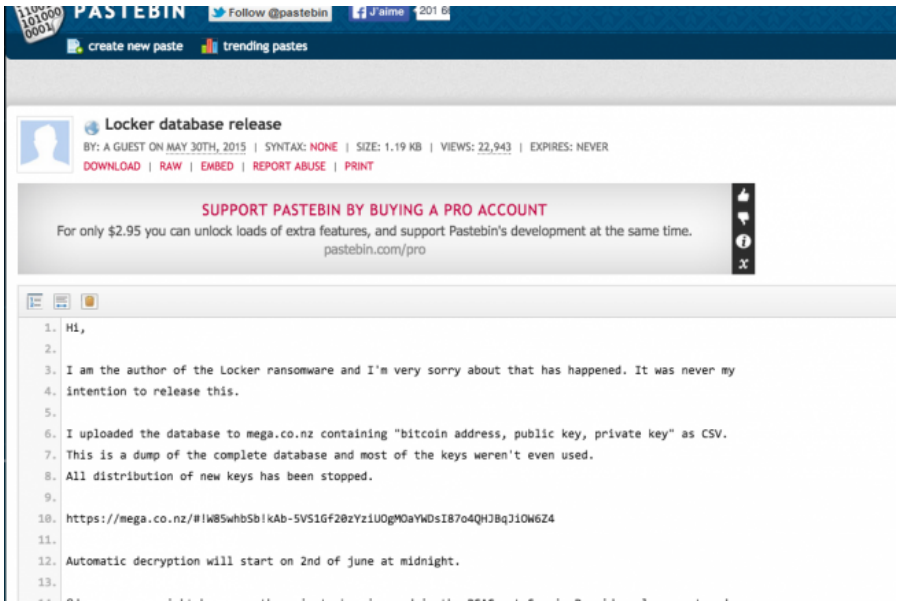
Si vous désirez lancer une cyberattaque, vous pouvez trouver un kit du parfait pirate ou tout simplement vous octroyer les services d'un pirate expérimenté. Alors que tous les tutoriels vous sont gracieusement offerts, l'installation d'un programme malware vous coûtera 70 $, tandis qu'une attaque DDoS vous sera facturée 100 $. Mais la denrée la plus convoitée reste l'adresse email parce qu'elle permet de mener des opérations de spam ou d'hameçonnage. Comptez seulement 75 $ pour un million d'adresses valides et 70 $ l'identité complète (nom, prénom, adresse postale, données de cartes bancaires, comptes email, comptes bancaires). Les accès à ces adresses -identifiants et mots de passe- sont eux légèrement plus chères: 20 $ pour un lot de 40.000 comptes. Un prix abordable pour celui qui désire usurper des identités afin de se lancer dans des escroqueries de plus haut vol. Pour les hackers fainéants, des données financières prêtes à l'emploi sont également disponibles, mais elles se payent plus cher à l'image d'une carte bancaire ou un compte Paypal qui sera monnayé à 50 $ pièce. Quant aux produits matériels illicites, ils sont également pléthore sur le Darkweb: le site 01Net nous apprend par exemple «qu'une fausse carte d'identité d'un pays européen se négocie aux alentours de 1.000 €, qu'il faudra verser 4.000 € pour un passeport et qu'au rayon drogues, un gramme de cocaïne de qualité (Amérique du Sud) se vend à partir de 75 € alors qu'un gramme d'ecstasy avec taux de pureté de 84% vaut 19 €».

Représailles compliquées

La lutte contre cette criminalité cachée s'avère aride pour plusieurs raisons. D'abord parce que ces cybercriminels sont difficilement identifiables de par l'utilisation de systèmes qui garantissent leur anonymat (comme Tor, I2P, des VPN ou des Proxy). Ensuite, les opérations menées par les différentes forces policières sont généralement trop lentes et «les sites sont hébergés sur d'autres serveurs en seulement quelques heures», selon Jérôme Granger qui indique qu'«à côté d'une protection redoutable, la seule solution réside dans une sensibilisation constante aux cyberdangers». D'autant plus que la recherche de ces cybercriminels se heurte souvent au droit international car si la coopération européenne est efficace, plusieurs pays comme la Russie et la Chine refusent toujours de céder une partie de leur souveraineté numérique. Un problème qui ne fera que s'amplifier avec le développement fulgurant des objets connectés qui sont déjà les nouvelles victimes de virus et autres logiciels malveillants.

Source : http://fr.metrotime.be/2015/06/11/must-read/votre-identite-complete-ne-coute-que-70-dollars-sur-le-darknet/
Par Gaëtan Gras

Des clés pour débloquer des milliers d’ordinateurs victimes d’un ransomware – Le Monde Informatique | Le Net Expert Informatique



Des clés pour débloquer des milliers d’ordinateurs victimes d’un ransomware

L'auteur présumé du ransomware Locker présente ses excuses pour les actions commises et affiche les clefs pour déchiffrer les fichiers verrouillés avec son outil.

Dans une sortie particulièrement étonnante sur Pastebin, l'auteur présumé du ransomware Locker, également connu sous le nom CryptoLocker V, a publiquement présenté ses excuses aux milliers de victimes du malware. Dans la foulée, il a publié une base de données avec les clés capables de déverrouiller les machines et les fichiers infectés. Ce geste est particulièrement rare dans le petit monde des développeurs de ransomwares qui sont parmi les plus impitoyables sur Internet.
Le nombre de victimes de Locker n'est pas très clair (le fichier .csv de clés / adresses Bitcoin semble avoir 62 000 entrées), mais les machines bloquées pourraient être beaucoup plus nombreuses. Pendant des mois, le programme avait discrètement infecté des utilisateurs en utilisant une version piégée de Minecraft. Les fichiers ciblés comportaient des extensions : .doc, .docx, .xlsx, .ppt, .jpg, cru, .odf, .rtf, .dbf, .odb et DBF.

Un déverrouillage complexe
Seul un petit pourcentage du nombre total de victimes aura payé la rançon, exigé en Bitcoins, mais le développeur a également publié des documents indiquant que les demandes de paiements pourraient être dix à vingt fois plus importantes. « Je suis l'auteur du ransomware Locker et je suis vraiment désolé de ce qui est arrivé. Il n'a jamais été dans mon intention de propager ceci », a annoncé quelqu'un se faisant appeler «Poka BrightMinds », dans un message sur Pastebin le jour de la publication des clefs de chiffrement.
Malheureusement, le processus de déverrouillage se révèle être particulièrement complexe. Pour toutes les personnes qui ont encore le malware sur leur PC, la commande de déblocage aurait été automatiquement envoyée le 2 juin, après quoi ils auront reçu le message suivant à travers le logiciel lui-même : « Je suis désolé pour le chiffrement, vos fichiers sont déverrouillés gratuitement. Soyez bon pour le monde et n'oubliez pas de sourire:). » Cependant, tous ceux qui ont désinstallé manuellement le logiciel malveillant en utilisant un utilitaire anti-virus devront utiliser l'outil Locker Unlocker développé par un chercheur qui peut être téléchargé à partir du site Bleeping Computer (http://www.bleepingcomputer.com/forums/t/577953/locker-developer-releases-private-key-database-and-3rd-party-decrypter-released).

Des intentions inconnues
Les chercheurs et les analystes en sécurité ont exprimé leur énorme surprise et leur perplexité quant aux dernières déclarations de l'auteur de ce logiciel malveillant. « Cela n'est jamais arrivé auparavant ! », a déclaré Stu Sjouwerman de KnowBe4, un cabinet de conseil américain qui a dressé une liste des victimes du ransomware. « L'auteur semble avoir soit gagné tellement d'argent qu'il se retire de cette campagne criminelle, ou bien il craint de se faire attraper par les forces de l'ordre, ou il aurait été menacé par une cybermafia locale », a-t-il dit. « Maintenant, tout cela semble assez plan-plan. Si vous écrivez ce type de code, vous savez très bien ce que vous faites. Le fait qu'il ait été conçu comme un malware dormant dénote une planification minutieuse étalée sur de longs mois. »
Il y a un point indiscutable. Tous les gens infectés ne verront pas le message indiquant qu'ils pourront inverser le processus, et tous ceux qui ont déjà payé une rançon en bitcoins doivent bien être conscient qu'ils ne seront jamais remboursés. Le mal a déjà été fait.

Source : http://www.lemondeinformatique.fr/actualites/lire-des-cles-pour-debloquer-des-milliers-d-ordinateurs-victimes-d-un-ransomware-61394.html
Par Serge Leblal

Quelques conseils pour préserver votre e-réputation | Le Net Expert Informatique

	Quelques conseils pour préserver votre e-réputation

Sur le web, rien ne se perd. Toutes les données qui vous concernent sont potentiellement accessibles par tous. Qu'il s'agisse des photographies de votre vie étudiante festive, des archives du blog que vous aviez tenu lors d'un voyage à l'étranger, de votre participation sur la liste électorale d'un parti politique sulfureux lors d'élections locales ou encore du jugement relatant une condamnation pénale : vous laissez des traces.

Celles-ci peuvent se révéler encombrantes. Comment faire pour qu'elles soient déréférencées des moteurs de recherche et ainsi rendues inaccessibles ?
Tout d'abord, il peut être utile de consacrer quelques minutes au paramétrage de la confidentialité de son compte sur les réseaux sociaux, afin de préserver le caractère privé de ses publications. Celles-ci ne seront alors pas accessibles par le biais des moteurs de recherche mais réservées à vos amis et relations.
Dans le cas où le contenu visé est publié sur un site web tiers, tel qu'un éditeur de presse, un blog ou un forum de discussion, il est possible de demander sa suppression en s'adressant directement à l'éditeur du site concerné ou, lorsque celui-ci ne réagit pas ou n'a pu être identifié, à l'hébergeur (qui assure le stockage du site sur ses serveurs).
En cas d'échec de cette démarche, les moteurs de recherche pourront être sollicités au titre du droit à l'oubli, par le biais des différents formulaires qu'ils proposent désormais [1].
Les principaux refus opposés par les moteurs de recherche sont justifiés par le fait que l'information litigieuse est toujours d'actualité, qu'elle ne concerne pas une personne physique, que l'internaute est un personnage public ou que le plaignant est un personnage public.
En dernier recours, le Tribunal compétent pourra être saisi. Attention toutefois, le juge saisi analyse en détail la demande présentée afin de s'assurer qu'elle ne porte pas atteinte à la liberté d'information du public. Ainsi, le Tribunal de grande instance de Paris a rejeté une demande de suppression et de désindexation d'un article en ligne du quotidien 20 Minutes [2]. L'article litigieux, accessible sur le site internet du quotidien, intitulé « Un cavalier accusé de viol », relatait le placement en garde à vue d'un cavalier de niveau international soupçonné d'être impliqué dans le viol d'une stagiaire.
Les juges ont rejeté la demande de droit à l'oubli, en faisant prévaloir la liberté d'information et l'intérêt légitime à divulguer des informations visant une personne exerçant une profession faisant appel au public et encadrant une activité proposée, notamment, à des enfants.
Au contraire, dans une décision précédente, la même juridiction avait ordonné à la société Google de retirer de ses résultats de recherche un lien vers un article du Parisien évoquant la condamnation, datant de 2006, d'une internaute pour escroquerie à une peine de trois ans de prison dont trois mois fermes. La plaignante, à la recherche d'un emploi, s'était tournée vers la Justice à la suite du refus préalablement opposé par le géant américain.
Lorsque votre demande est rejetée par le tribunal saisi, il reste possible de faire appel à des structures spécialisées qui tenteront de renvoyer au-delà de la troisième page de résultats, le contenu qui vous gêne.
A l'heure où de plus en plus de plateformes proposent aux internautes de redevenir propriétaires de leurs données personnelles et de gagner de l'argent en louant leurs profils [3] aux marques et annonceurs, il est plus que jamais important de permettre aux internautes de retrouver la maîtrise de leur e-réputation.

Source : http://www.village-justice.com/articles/Quelques-conseils-pour-preserver,19708.html

---

3D Prod, le nouveau site web qui vous permet d'imprimer en 3D vos pièces en vous donnant accès à toutes les technologies industrielles actuelles | Le Net Expert Informatique

3D Prod, le nouveau site web qui vous permet d'imprimer en 3D vos pièces en vous donnant accès à toutes les technologies industrielles actuelles

L’impression 3D professionnelle maintenant accessible en 3 clics3D Prod démocratise l’impression 3D professionnelle grâce à son nouveau site internet www.3dprod.com. Toutes les solutions actuelles d’impression 3D sont maintenant accessibles à travers une interface de commande entièrement en ligne.

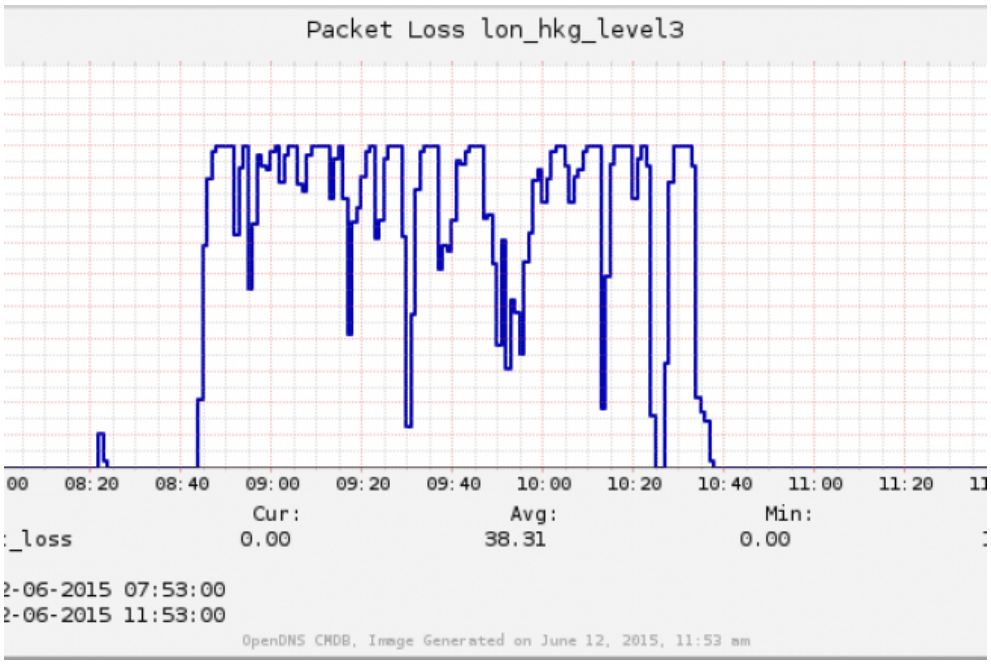
Après avoir uploadé un ou plusieurs fichiers 3D, le visiteur sélectionne la technologie d’impression qu’il souhaite appliquer (stéréolithographie, frittage laser de poudres, multi-jets ou dépôt de fils). Il précise ensuite les matériaux qui doivent être utilisés ainsi que les finitions qu’il souhaite apporter à ses pièces. Un prix et une date de livraison sont instantanément calculés en fonction des options choisies. Le client peut ensuite régler en ligne et faire livrer ses pièces à l’adresse de son choix.
Cette nouvelle interface facilite également les achats groupés, contenant plusieurs impressions distinctes. Il est ainsi possible de préciser des matériaux et finitions spécifiques pour chacune des pièces appartenant à une même commande.
Ce service est aujourd’hui disponible en France et sera bientôt déployé dans d’autres pays d’Europe.

A propos de 3D Prod :
Depuis 2005, 3D Prod développe son savoir-faire dans le domaine de l’impression 3D et réalise des prototypes, maquettes et petites séries pour les professionnels de nombreux secteurs, tels que l’industrie, le design ou encore l’architecture. 3D Prod maîtrise l’ensemble des solutions actuelles d’impression 3D, notamment la stéréolithographie, le frittage laser de poudres, le multi-jets ou encore le dépôt de fils. Ces technologies lui permettent de proposer un large éventail de rendus dans des délais réduits et à des coûts maîtrisés. Entreprise à la pointe des technologies actuelles, 3D Prod se réinvente en permanence afin de disposer des dernières avancées technologiques et proposer à ses clients les solutions les plus adaptées. Le développement de cette nouvelle interface de commande en ligne s’inscrit précisément dans cette démarche.

Source : http://www.lyon-communiques.com/communiques/3d-prod-le-nouveau-site-web-qui-vous-permet-d-imprimer-c122529.htm

---

Panne Internet géante provoquée par Telekom Malaysia | Le Net Expert Informatique



Panne Internet géante provoquée par Telekom Malaysia

Comme en mars dernier, un opérateur a ralenti et même bloqué les requêtes IP d'un très grand nombre d'Internautes dans le monde entier et en France vendredi matin.

L'analogie du papillon trouve une nouvelle fois un débouché sur le secteur des télécoms. Des erreurs de routage BGP de l'opérateur Telekom Malaysia ont ralenti et même bloqué certains services Internet en France dans la matinée.
Ce type d'erreur est courant sur le réseau des réseaux. En mars dernier c'est le FAI indien Hathway qui avait semé la panique. L'événement déclenché ce matin par l'opérateur malaisien a entraîné des pertes de paquets IP significatives dans toutes les parties du monde. Le réseau IP a connu une dégradation sévère entre la région Asie-Pacifique et le reste du monde quand Telekom Malaysia a commencé à transférer des requêtes erronées (près de 200000) à Level 3, un géant de l'Internet. Le service est revenu à la normal en fin de matinée.

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemondeinformatique.fr/actualites/lire-france-la-panne-internet-geante-provoquee-par-telekom-malaysia-61465.html
Par Serge Leblal

Des hôtels suisses victimes d'un piratage informatique. Le Wifi était-il sûr ? | Le Net Expert Informatique

Selon le groupe de sécurité informatique russe, Kaspersky, le logiciel d’espionnage « Duqu » a déjà servi à une cyberattaque en 2011. Crédit Reuters	**Des hôtels suisses victimes d’un piratage informatique. Le Wifi était-il sûr ?**

Nous vous avions déjà alerté sur les risques que pouvaient entraîner l'usage des Wifi public ou bien les Wifi ouverts des hôtels (cf : Est-il risqué de se connecter au wifi public ?). Voici ci-dessous exemple concret, par Atlantico, de mise en application par les pirates d'opérations d'espionnage en utilisant ces moyens de communications certes gratuits, mais non garantis en terme de sécurité et de confidentialité.
Denis JACOPINI

Les établissements qui ont abrité les négociations du P5+1 auraient été la cible de cyber-attaques, selon l'entreprise de sécurité informatique Kaspersky. Le Ministère public de la Confédération a ouvert une procédure pénale contre X.

Selon le groupe de sécurité informatique russe, Kaspersky, le logiciel d'espionnage « Duqu » a déjà servi à une cyberattaque en 2011.
Le porte-parole du Ministère public de la Confédération (MPC) André Marty a confirmé qu'une perquisition a été menée dans un hôtel genevois le 12 mai dernier et que du matériel informatique a été confisqué. « Le but de cette perquisition était d'une part de mettre à l'abri des informations et d'autre part de constater si des systèmes informatiques ont pu être infectés par des virus. »
Le MPC, qui soupçonne une activité interdite d'un service de renseignement étranger, a ouvert une procédure pénale contre X. L'entreprise de sécurité informatique Kaspersky affirme avoir découvert un virus espion très sophistiqué qui aurait touché trois des hôtels ayant accueilli les négociations sur le nucléaire iranien. L'Intercontinental et le Palais Wilson à Genève, le Beau Rivage à Lausanne ou le Royal Plaza à Montreux sont potentiellement des cibles de cette attaque. Et ces trois établissements ont un point commun : l'accueil des négociations sur le nucléaire iranien.
Selon le groupe de sécurité informatique russe, Kaspersky, le logiciel d'espionnage « Duqu » a déjà servi à une cyberattaque en 2011, montrant des similarités avec Stuxnet, un « ver » informatique qui a en partie saboté le programme nucléaire iranien en 2009-2010 en détruisant un millier de centrifugeuses servant à produire de l'uranium enrichi. Une autre attaque imputable à « Duqu », ajoute Kaspersky, est liée aux cérémonies du 70e anniversaire de la libération du camp d'Auschwitz-Birkenau, en janvier de cette année. Plusieurs chefs d'Etat et de gouvernement étaient présents.
Le P5+1 réunit les Etats-Unis, la Chine, la Russie, la France, la Grande-Bretagne, les cinq membres permanents du Conseil de sécurité des Nations unies, et l'Allemagne. « Les informations internationales sur l'implication d'Israël dans cette affaire sont sans fondement », a déclaré la vice-ministre des Transports Tzipi Hotovely. « Ce qui est beaucoup plus important », a-t-elle ajouté, « c'est d'empêcher un mauvais accord où au final, nous nous retrouvons avec un parapluie nucléaire iranien. »

Source : http://www.atlantico.fr/pepites/nucleaire-iranien-hotels-suisses-victimes-piratage-informatique-logiciel-duqu-2189164.html

Un ordinateur de Merkel touché par la cyberattaque contre le Bundestag | Le Net Expert Informatique

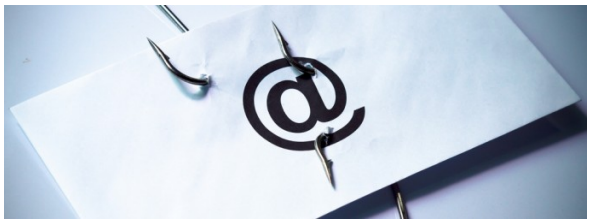
Un ordinateur de Merkel touché par la cyberattaque contre le Bundestag

Un ordinateur de la chancelière Angela Merkel a été touché par la cyberattaque sans précédent qui a visé en mai le Bundestag, la chambre basse du Parlement allemand, affirme le quotidien Bild dans son édition de dimanche.

L'attaque avait été constatée en mai et s'est avérée beaucoup plus importante et vaste que prévu, les services du Bundestag peinant à la contrôler. Selon les médias allemands, les pirates auraient pendant plusieurs semaines profondément infiltré le réseau informatique, parvenant à pirater des données.
Selon Bild, qui ne cite pas ses sources, l'attaque a notamment «infecté» l'un des ordinateurs du bureau dont dispose au Bundestag Mme Merkel, élue depuis 1990 de la circonscription de Stralsund (nord).
Selon le journal à gros tirage, cet ordinateur aurait été l'un des premiers sur lesquels l'attaque, de type «cheval de Troie», a été constatée.
Un porte-parole du groupe CDU, le parti conservateur de la chancelière, a indiqué au journal «ne pouvoir ni démentir ni confirmer» ces informations.
Interrogé sur un éventuel pillage des données de l'ordinateur de la chancelière, l'entourage de Mme Merkel n'a pas souhaité s'exprimer, rapporte Bild.
Les sites officiels de Mme Merkel, de la chancellerie et du Bundestag avaient déjà fait l'objet en janvier d'une cyberattaque, revendiquée par des pirates russes. Selon des médias allemands, la dernière attaque contre le Bundestag viendrait aussi de Russie et pourrait avoir été lancée par des services de renseignements de ce pays.
Jeudi, le président du Bundestag, le conservateur Norbert Lammert, a indiqué que, depuis deux semaines, plus aucune fuite de données n'avait été constatée, ce qui ne signifie pas qu'elles ont été «stoppées».
Selon Bild, la présence du «cheval de Troie» a été constatée vendredi sur quinze ordinateurs reliés au réseau informatique du Bundestag, qui a voté ce même jour une loi destinée à renforcer la sécurité informatique des grandes entreprises.
Des fuites de données ont été constatées sur cinq d'entre eux, poursuit le quotidien, selon lequel les «pirates» ont également utilisé le nom de la chancelière pour envoyer des courriels contenant des liens «contaminés».
L'administration du Bundestag a mis en garde les députés contre ces faux courriels usurpant le nom de la chancelière, écrit Bild.

Source : http://www.lapresse.ca/international/europe/201506/13/01-4877838-un-ordinateur-de-merkel-touche-par-la-cyberattaque-contre-le-bundestag.php

Phishing : Europol a pêché un gros morceau | Le Net Expert Informatique

	**Phishing : Europol a pêché un gros morceau**

Une coordination internationale pilotée par Europol a démantelé un réseau de cybercriminels suspectés d'avoir usé du phishing à des fins de fraude bancaire.

58 perquisitions pour 49 arrestations : c'est le bilan de l'opération Triangle, vaste action de police conduite ce mardi 9 juin sous la houlette du centre de lutte contre la cybercriminalité (EC3) d'Europol.
Supervisée depuis La Haye (Pays-Bas), l'opération a permis de démanteler un réseau de pirates informatiques actif en Italie, Espagne, Pologne, Royaume-Uni, Belgique et Géorgie.
Ces individus, pour la plupart originaires du Nigeria, du Cameroun et d'Espagne, sont suspectés de fraude financière : ils auraient amassé près de 6 millions d'euros en menant essentiellement des campagnes de phishing. C'est-à-dire des assauts contre des systèmes de messagerie électronique avec des e-mails d'apparence légitime, mais abritant une pièce jointe ou un lien malveillants.
Coordonnées par le J-CAT (présenté comme une cellule commando anti-cybercriminalité activée sous la tutelle de l'EC3), les autorités italiennes, espagnoles et polonaises ont saisi ordinateurs portables, disques durs, téléphones, tablettes, cartes de crédit, clés USB, cartes SIM et documents bancaires.
Autant de pièces à conviction qui devraient en dire davantage sur le mode opératoire supposé de ces cybercriminels. En l'occurrence, des attaques de type « man-in-the-middle » dans les systèmes informatiques de PME et grands comptes en Europe.
L'objectif des pirates était de s'ouvrir l'accès aux boîtes mail de « cibles d'intérêt ». Dans le cas présent, celles intervenant sur la chaîne des achats-ventes.
Toute transaction commerciale était repérée et entraînait l'envoi, au client non soupçonneux, d'ordres de paiement sur un compte en banque… contrôlé par les faussaires. Lesquels récupéraient alors les fonds et les transféraient hors de l'Union européenne en multipliant les virements.
Cet épisode est à mettre en parallèle avec l'un des constats établis par IBM dans l'édition 2015 de son rapport Cyber Security Intelligence Index : le phishing ne connaît pas la crise. Le taux de spams piégés par rapport à l'ensemble des courriels non sollicités à caractère commercial est de 4 % début 2015, alors qu'il n'avait jamais dépassé les 1 % jusqu'à l'été 2013.

Source : http://www.itespresso.fr/phishing-europol-peche-gros-morceau-98361.html