Les Samsung Galaxy vulnérables aux cyber-attaques | Le Net Expert Informatique

Twin Design / Shutterstock.com	**Les Samsung Galaxy vulnérables aux cyber-attaques**

Les claviers virtuels SwiftKey, pré-installés sur les Samsung, pourraient être une porte ouverte pour les hackers. Une société de cybersécurité américaine a découvert une faille dans plus de 600 millions de portables.

Vous avez peut-être déjà été hacké

Le coupable : le clavier virtuel SwiftKey. Il appartient à la suite d'applis et de fonctionnalités que les Samsung rajoute à Android,. Comme toute application, SwiftKey subit des mises à jour fréquentes. La société de cybersécurité NowSecure a découvert que lorsque le téléphone recherche des mises à jour à effectuer, il communique ouvertement, sans chiffrer sa requête.

Pour étayer leur dires, les chercheurs de NowSecure ont réussi à se faire passer pour le serveur qui envoie les mises à jour aux téléphones Samsung et à y injecter des programmes permettant d'exploiter les appareils à l'insu des utilisateurs. Peut-être que, sans le savoir, vous avez déjà été hacké.

Impossible à désinstaller

Cette vulnérabilité concerne les modèles Galaxy S4, S4 Mini, S5 et S6. Le problème étant que l'application SwiftKey fait partie des programmes de base livrés avec le téléphone, au même titre que les applis de Google. Il est donc impossible de la désinstaller.

En attendant que le problème soit réglé, NowSecure conseille aux utilisateurs d'« éviter les réseaux Wi-Fi non sécurisés », ou plus radicalement d'« utiliser un autre appareil mobile ». Samsung a lui annoncé une future mise à jour de sa solution de sécurité Knox, pour combler cette faille.

Actuellement, un hackeur s'attaquant à votre téléphone pourrait avoir accès aux capteurs et aux ressources comme le GPS, l'appareil photo et le micro, installer secrètement des applications malveillantes, espionner les messages entrants et sortants ou les appels ou encore tenter d'accéder à des données personnelles sensibles comme les photos ou les textos.

Qu'en est-il en France ?

Contactée par Le Figaro, la société NowSecure confirme que le phénomène est «mondial», et donc que la France est concernée. Elle a notifié cette faille à Samsung en décembre 2014, ainsi qu'à l'équipe de sécurité d'Android.

Si Samsung a publié un correctif début 2015, « on ne sait pas si les opérateurs téléphoniques ont implémenté ce correctif dans les appareils de leurs réseaux », explique NowSecure. L'entreprise n'a diffusé qu'une liste des opérateurs touchés aux États-Unis.

En France, seul Bouygues Télécom a pour l'instant été en mesure de fournir une réponse des plus inquiétantes, assurant que « Samsung n'a jamais fait remonter le problème à nos équipes techniques » et qu'il est désormais « très sérieusement à l'étude ».

Source : http://news.radins.com/actualites/les-samsung-galaxy-vulnerables-aux-cyber-attaques,13394.html

---

La lutte de la Cybercriminalité passe par la coopération et la formation des enquêteurs (Octopus 2015)

| Le Net Expert Informatique

Cybercriminalité: la lutte passe par la coopération et la formation des enquêteurs (Octopus 2015)

Une coopération internationale renforcée en matière de cybercriminalité et des enquêteurs mieux formés permettraient aux Etats de mieux lutter contre ce fléau, ont conclu vendredi des experts réunis à Strasbourg au Conseil de l'Europe.

Experts internationaux, juges, policiers, responsables gouvernementaux: réunis depuis mercredi à Strasbourg (est de la France), 300 participants à la conférence sur la cybercriminalité Octopus 2015 ont avancé plusieurs pistes de travail.
Parmi les domaines d'actions jugés prioritaires, une coopération internationale plus efficace, des outils et des capacités de lutte renforcés permettraient aux Etats d'être mieux armés pour poursuivre et faire condamner les auteurs d'infractions dans le cyberespace, a affirmé Gabriella Battaini-Dragoni, vice-présidente du Conseil de l'Europe, qui présentait les conclusions des participants à la conférence.
Le Conseil de l'Europe a annoncé qu'il allait « démultiplier » ses efforts pour aider les Etats qui le souhaitent à organiser un programme de formation pour juges et procureurs internationaux, a indiqué Mme Battaini-Dragoni.
L'organisation paneuropéenne, qui compte 47 Etats-membres, veut notamment aider les enquêteurs à se servir du « cloud-data », ces traces informatiques qui permettent d'identifier et de poursuivre les criminels.
Elle proposera dans un premier temps un « Guide des preuves électroniques », sous forme de glossaire informatique.
L'idée est aussi de permettre aux enquêteurs de « parler la même langue », selon Alexander Seger, chef de la division de la lutte contre la cybercriminalité au Conseil de l'Europe.
Selon M. Seger, les « territorialités » et les frontières continuent en effet de faire obstacle en matière de coopération entre enquêteurs, qui peuvent avoir besoin de trouver des éléments de preuve hébergés sur des serveurs informatiques à l'étranger.
Selon le Conseil de l'Europe, depuis 2001, 66 pays dont la France ont signé, ratifié la Convention de Budapest sur la cybercriminalité, ou ont été invités à y adhérer.
Plus de 120 pays au total coopérent avec le Conseil de l'Europe pour renforcer leur législation et leur capacité de lutte contre la cybercriminalité.

Source : http://www.notretemps.com/internet/cybercriminalite-la-lutte-passe-par-la,i88427

Montres connectées : vos données personnelles sont peut-être en danger | Le Net Expert Informatiquedc

Montres connectées : vos données personnelles sont peut-être en danger

Des chercheurs en sécurité n'ont pas eu trop de mal à récupérer des données personnelles à partir des montres connectées LG G Watch et Samsung Gear 2 Neo.

Les révélations sur les possibilités d'intrusion et de récupération de données personnelles dans les téléphones portables par les agences de renseignement américaines dévoilées dans les documents d'Edward Snowden ont conduit les éditeurs de plates-formes mobiles à relever les niveaux de sécurité, notamment par le chiffrement systématique des données personnelles et documents dans les appareils mobiles.
Et pour les montres connectées, ces gadgets qui fleurissent (ou aimeraient le faire) sur les poignets ? Une publication de chercheurs de l'Université de New Haven suggèrent que si des hackers ont besoin d'information, ils feraient bien de commencer par cette porte d'entrée.
Il n'ont pas rencontré énormément de difficultés pour obtenir différentes informations personnelles, que ce soit avec la LG G Watch (agenda, contacts, adresses email, données du podomètre) sous Android Wear ou la Samsung Gear 2 Neo (messages, emails, contacts, données de santé) sous Tizen OS….d'autant plus que ces données n'étaient pas chiffrées.
Avec la multiplication des objets connectés qui seront autant de points d'entrée théoriques à différents types de données personnelles, cette petite expérience a de quoi faire réfléchir, alors que des objets comme les montres connectées ont justement besoin d'un large accès aux données personnelles pour être pleinement efficaces, comme dans le cas de Google Now sur Android Wear.
Chiffrer les données sur les montres connectées (et les objets connectés en général) serait une bonne chose, mais encore faut-il que ce soit fait correctement, préviennent les chercheurs. Un certain nombre de failles exploitées par les agences de renseignement (mais aussi les méchants hackers) sont justement des attaques de type man-in-the-middle qui outrepassent ces protections sans même avoir à les casser.
A voir si la montre Apple Watch, en cours d'analyse à l'Université de New Haven, saura mieux préserver la vie privée de son possesseur. Il vaudrait mieux, étant donné les volumes de plusieurs dizaines de millions d'unités qui son censés être écoulés dès cette année…

Source : http://www.generation-nt.com/lg-watch-samsung-gear-montre-protection-donnees-actualite-1915829.html

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://gb000426.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 sollicités ;
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 sollicités ;
• 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 plaît ? 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

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

V

Votre identité complète ne coûte que 70 dollars sur le Dark Web

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 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

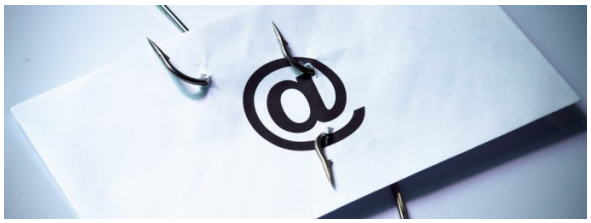
Un ordinateur de Merkel touché par la cyberattaque contre le Bundestag

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

Kaspersky annonce être victime d’une Cyberattaque | Le Net Expert Informatique

	Kaspersky annonce être victime d’une Cyberattaque

L'éditeur de sécurité indique qu'une cyber-attaque a ciblé ses propres installations par le biais d'une nouvelle version du malware baptisé Duqu. Pour Eugene Kaspersky, le patron et fondateur de la société, cette offensive a pu être soutenue par un Etat.

Eugene Kaspersky prend la parole pour livrer les détails de l'attaque qui a visé les installations de l'éditeur de sécurité. Au cours d'une conférence de presse, le fondateur de la société a indiqué que les pirates ont utilisé une nouvelle variante d'un ver baptisé Duqu. Selon le patron de l'éditeur russe, le malware a été développé par une organisation très qualifiée, possiblement soutenue par un gouvernement étranger.
Eugene Kaspersky indique que ses équipes sont actuellement en train de rassembler l'ensemble des éléments pour comprendre l'attaque. Le responsable se veut toutefois rassurant. « Cette attaque n'a rien compromis pour nos clients mais également nos partenaires. Nous ne disposons pas encore de toutes les informations sur cette attaque mais je lance un avertissement clair, ne me hackez pas, c'est une mauvaise idée ».
L'éditeur s'est rendu compte de l'attaque grâce à une version Alpha de sa nouvelle solution censée lutter contre les menaces dites persistantes (ou APT pour advanced persistent threat). Pour Kaspersky le but des pirates était d'ailleurs d'espionner sa technologie permettant de traquer ce type de cyber-attaques.
Selon les spécialistes, Duqu est une variante de Stuxnet, un élément malveillant qui avait été utilisé pour attaquer des systèmes critiques dits SCADA. Stuxnet avait même permis d'organiser une cyber-attaque contre des installations informatiques présentes au sein d'une centrale nucléaire en Iran.
Toujours est-il qu'Eugene Kaspersky considère que le nouveau Duqu exploite plusieurs vulnérabilités 0-Day. Le fait d'être en mesure d'utiliser plusieurs failles jusqu'à présent inconnues est, selon le responsable, un élément important. Cela lui permet d'affirmer que les équipes derrière ce malware disposent non seulement de très solides connaissances techniques, mais également de soutiens « officiels » d'un gouvernement étranger.

Duqu, une nouvelle variante
Le malware Duqu avait déjà sévi en 2011. Mis en lumière par les équipes de Symantec, il était parvenu à se diffuser par le biais d'un fichier d'installation contenu dans un document Word (.doc) envoyé par e-mail. Une fois ouvert, ledit fichier exploitait une vulnérabilité du moteur d'analyse de font (TTF) Win32k TrueType et était ainsi capable d'infecter un poste informatique.
Microsoft avait par la suite été obligé de publier un patch de sécurité hors-cycle pour corriger les nouvelles vulnérabilités (0-Day) exploitées par le ver. A présent qu'une nouvelle variante du malware est détectée, la firme américaine pourrait à nouveau publier une mise à jour de sécurité pour l'ensemble de ses services.

Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-769814-kaspersky.html
Par Olivier Robillart

Les attaques informatiques s’achètent sur le blackmarket | Le Net Expert Informatique

	Les attaques informatiques s’achètent sur le blackmarket

De 75 dollars le million d'adresses e-mail à plusieurs milliers de dollars pour une faille zero day exploitable… G Data a plongé dans le « blackmarket » pour en ressortir les principaux tarifs du marché de la cybercriminalité.

G Data s'est penché sur le marché de la cybercriminalité pour en étudier fonctionnement et offres de contenus. Baptisé « blackmarket », cet environnement construit autour de sites spécialisés, de forums privés, de structures d'anonymisation (proxy, VPN anonymes, réseau Tor…), de messageries protégées, de serveurs bulletproof (peu regardants sur la nature des fichiers stockés), de moteurs de recherche spécialisés et autres places de marchés de produits illicites, permet d'accéder à des montagnes de données personnelles, des kits de piratages en tout genre et de services d'attaques à la demande.
Au bout de son plongeon dans le blackmarket, les experts du SecurityLabs de l'éditeur allemand spécialisé en solutions de sécurité en a ressorti quelques informations éclairantes sur la vitalité du marché de la cybercriminalité. Un marché dont les tarifs évoluent entre une poignée de dollars et plusieurs centaines. La vente de données personnelles illégalement collectées se situe dans la zone basse des tarifs et, surtout, se commercialisent en volumes. Ainsi les accès aux comptes e-mails (adresse, nom d'utilisateur et mot de passe) se négocient 5 dollars le lot de 10 000. Les seules adresses e-mails, celles que se font notamment dérober les opérateurs et qui seront essentiellement exploitées pour des campagnes de phishing, ne se revendent pas plus de 10 dollars par poignées de 100 000, autour de 75 dollars le million. Les profils numériques qualifiés sont, eux, d'autant plus rentables qu'ils se revendent à l'unité : autour de 50 dollars pour une carte bancaire valide de type Gold ou Premier, un compte bancaire ou Paypal; 70 dollars l'identité complète dite Fullz (nom, prénom, adresse postale, données de cartes bancaires, comptes email, comptes bancaires).

Plusieurs milliers de dollars la faille zero day exploitable
Les cybercriminels financièrement plus ambitieux orienteront leurs activités vers la vente de produits et services. L'installation d'un Bot, bien utile pour prendre le contrôle d'un réseau de PC infectés, se négocie autour de 50 dollars les 1000 machines à la soldes des cyberattaquants. Lesquels pourront également exploiter ces Bots pour organiser des attaques par déni de service distribué (DDoS). Un service proposé entre 10 et 200 dollars l'heure d'attaque. Le tarif pour une campagne de spam, non traçable (via un service de diffusion hébergé sur un serveur bulletproof) tombe en revanche autour de 5 dollars les 20 000 envois.
La création et l'hébergement (sur un serveur piraté) d'une page web infectieuse dans le cadre d'une campagne d'hameçonnage (phishing) se facture entre 10 et 30 dollars. Mais on trouve également des outils d'attaques plus onéreux (car censés être plus efficaces). Par exemple, le kit d'exploitation Nuclear, qui exploite les bannières publicitaires Google Ads pour dérouter l'utilisateur vers un site infectieux, est disponible autour de 1500 dollars. La palme revient aux outils capables d'exploiter les failles zero day de Windows à raison de plusieurs milliers, voire plusieurs dizaines de milliers de dollars, selon G Data.

Source : http://www.silicon.fr/besoin-dune-attaque-ddos-comptez-entre-10-200-dollars-de-lheure-118545.html
Par Christophe Lagane