Piratage d’un stimulateur cardiaque, point de départ de la prochaine Grande Guerre ? | Le Net Expert Informatique

12

	Piratage d’un stimulateur cardiaque, point de départ de la prochaine Grande Guerre ?

Le piratage à distance en 2020 du stimulateur cardiaque d'un dirigeant d'un grand pays est le point de départ de la nouvelle « Café, Wi-Fi et la Lune » de Nikolas Katsimpras, qui a été primée ce mardi 17 mars par le Conseil Atlantique. Les candidats étaient invités par ce think tank de Washington, à présenter des textes courts, fictifs, de « unes » de journaux, sur le déclenchement du prochain conflit majeur, en s'inspirant des événements qui ont emporté le monde dans la Grande Guerre en 1914.

Le choix du jury souligne deux consensus. En premier, nous devrions à très court terme être immergés dans une multitude d'Objets Connectés, senseurs et capteurs qui nous aideront sur de nombreux aspects de notre vie. En second, la sécurisation de cet Internet des Objets face à des actes de maladresse comme de malveillance, pose encore de nombreux problèmes techniques et politiques. Enfin, le Conseil Atlantique ouvre par cette initiative la question de la contribution de l'art et de la littérature à ce débat, en terme de communication ou pour faciliter la prise de conscience par le grand public du travail restant à faire dans le domaine de la cyber-sécurité et du respect de la sphère privée.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.bulletins-electroniques.com/actualites/78150.htm

Arte victime d’une attaque informatique jeudi | Le Net Expert Informatique

	Arte victime d’une attaque informatique jeudi

Le lendemain de l'attaque informatique qui a frappé TV5 Monde mercredi, Arte à Strasbourg a également subi une intrusion dans son réseau. Fort heureusement, il ne s'agissait pas d'une attaque menée par des cyber-djihadistes autoproclamés, mais d'un cas classique de « ransom ware », autrement dit de racket par l'intermédiaire d'un virus.

Rançon contre les fichiers

Téléchargé jeudi en milieu d'après-midi via la messagerie, un virus du type « crypto-wall » ou « cryptolocker » s'est installé sur trois ordinateurs d'Arte Culture avant de rapidement se propager. Un salarié témoigne :

« On a vu nos fichiers et nos dossiers devenir inaccessibles, ils avaient tous une taille de 0 octet. On a appelé le service informatique qui a identifié la menace et a mis en quarantaine tout le service culture et éteint nos ordinateurs. Quelques heures après, on a pu reprendre le travail à partir de sauvegardes. »

Une trentaine de postes ont été isolés pendant le reste de la journée. Les fichiers infectés sont rendus illisibles par le virus, qui les crypte les uns après les autres. Il n'y a aucun moyen de les récupérer, sauf à accepter de payer une rançon, généralement via la monnaie Bitcoin qui a l'avantage d'être difficile à tracer. Arte disposait de sauvegardes pour ses fichiers, mais tout de même 500 Go de données ont été corrompues.

Le service informatique d'Arte n'a pas pu déterminer d'origine à cette attaque, relativement fréquente. Il a renouvelé ses consignes de sécurité auprès des employés, qui consistent essentiellement à se méfier des fichiers envoyés par des inconnus.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.rue89strasbourg.com/index.php/2015/04/10/breve/arte-victime-dune-attaque-informatique-jeudi/

Les 6 plaintes les plus courantes reçues par la CNIL | Le Net Expert Informatique

Les 6 plaintes les plus courantes reçues par la CNIL

Que faire quand on vous refuse la suppression d'une information personnelle qui se retrouve sur Internet ? Contacter la Commission nationale informatique et libertés (CNIL), le « Zorro » des internautes dont la e-réputation est en péril. Daniela Parrot, chef du service des plaintes de la commission, a établi le top 7 des plaintes les plus courantes, concernant les données des internautes.
e-réputation : comment effacer vos casseroles numériques

1 – Les photos et commentaires mis en ligne sans votre accord sur les réseaux sociaux
Certes les procédures mises en place par les administrateurs des réseaux sociaux sont efficaces. « Par exemple sur Facebook, il est facile de demander la suppression et/ou de signaler les abus », confirme la Commission nationale informatique et libertés (CNIL). Mais pour éviter les mauvaises surprises, le bon réflexe c'est de paramétrer votre profil en soumettant par exemple les photos et les écrits de vos amis à votre validation avant publication.

2 – Les faux profils ou le piratage
Pour vous prémunir des faux profils, mettez en place une « google alert » qui vous avertira par mail dès que votre nom sera cité sur la toile. Si vous avez été piraté, contactez là encore la CNIL, compétente pour l'ensemble des litiges lié à vos données personnelles sur Internet. Dans un cas extrême, la CNIL pourra faire appel au procureur de la République qui diligentera une enquête.

3 – La diffusion des données personnelles
Sachez-le, les forums ne sont pas si privés. Certains de vos commentaires sont indexés et remontent sur les moteurs de recherche. Soyez vigilant y compris lorsque vous diffusez votre CV sur le web. N'oubliez pas qu'il contient votre téléphone, adresse et mail ! « Si vous souhaitez faire disparaître ces données, adressez-vous au responsable du site et/ou vérifiez la procédure de référencement », indique la CNIL qui pourrait être votre dernier recours.

4 – Les vidéos
Soyez attentif, le pouvoir de YouTube est immense car il y a une très forte viralité. En cas de problème, adressez-vous au plus vite au site pour supprimer le contenu. Si cela ne marche pas, contactez la CNIL.

5 – Les journaux en ligne
Un article vous cite sans raison valable ? Contactez le journal et indiquez les motifs justifiant votre requête. « L'article peut être supprimé, anonymisé ou déréférencé », explique Daniela Parrot. Si le journal ne motive pas son refus, la CNIL renvoie l'affaire devant les tribunaux.

6 – Les décisions de justice
Faites attention, les décisions de justice sont parfois référencées sur la toile. Selon le délit, cela peut être gênant ! Contactez la CNIL pour demander à ce que la décision soit rendue anonyme.

---

*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 protection juridique du chef d'entreprise.*
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://actualites.cadremploi.fr/editorial/conseils/droit-du-travail/detail/article/e-reputation-les-7-plaintes-les-plus-courantes-recues-par-la-cnil.html#xtor=CS2-1016

Un drone qui pirate les smartphones | Denis JACOPINI

Un drone qui pirate les smartphones

Les drones civils commencent à gagner en popularité, et certains s'inquiètent déjà des atteintes à la vie privée qu'ils pourraient faciliter. Au-delà de la simple surveillance, un spécialiste en sécurité met en avant leur utilisation possible à des fins de piratage de données personnelles.

Des experts en sécurité de la société Sensepost ont développé un drone capable de pirater le contenu d'un smartphone depuis les airs. Glenn Wilkinson, qui l'a créé en collaboration avec Daniel Cuthbert, se définit comme un hacker consciencieux, et ses recherches ont pour but de pointer du doigt les failles de sécurité des objets connectés, et notamment des smartphones.
Il présente en ce moment ses travaux à la conférence Black Hat qui se tient à Singapour du 25 au 28 mars. La technologie installée sur le drone, baptisée Snoopy, cherche des appareils mobiles dont le Wi-Fi est activé. Il tire parti de la fonction de recherche de réseaux Wi-Fi auxquels l'appareil s'est déjà connecté, qui est intégrée par défaut à tous les smartphones et tablettes. Le drone prétend alors être l'un de ces anciens réseaux déjà connus, et dupe le smartphone (ou la tablette), interceptant toutes les informations qu'il envoie. Il peut de plus se connecter à plusieurs appareils simultanément, usurpant plusieurs réseaux au besoin.
Les informations interceptées vont des sites visités à tous les identifiants utilisés (Amazon, PayPal, etc.) en passant par les coordonnées bancaires, les données de géolocalisation, et d'autres informations critiques, y compris les noms de tous les réseaux auxquels il s'est déjà connecté.
Le site CNNMoney a récemment testé Snoopy avec son concepteur lors d'une virée à Londres. En à peine une heure, ses équipes ont collecté des informations provenant de 150 appareils mobiles. L'utilisation d'un drone rend cette technologie particulièrement impressionnante, car elle permet de suivre des cibles tout en restant hors de portée, pratiquement indétectable.

Ci-dessous une vidéo du drone en action réalisée par CNN :

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.industrie-techno.com/un-drone-qui-pirate-les-smartphones.29240
Par Julien BERGOUNHOUX

Colloque international sur la Cybercriminalité à Montpellier

Colloque international sur la Cybercriminalité à Montpellier

Principalement organisé par Adel JOMNI, ce colloque a eut lieu les 8 et 9 avril 2015 à l'Université de Montpellier (Maison des étudiants- Richter) .

Objet du colloque

Présentation du projet Européen CAMINO (Comprehensive Approach to cyber roadMap CoordInation and develOpment),une conférence internationale sur l'innovation et la Cybercriminalité (draft programme joint à cette invitation)

Programme

Session 1 : Innovations numériques, Cybercriminalité et Cyber terrorisme : Enjeux et défis : quelles stratégies ?

– Lord Carlile of Berriew, Membre du Parlement du Royaume--Uni,
– Général Watin--Augouard, Directeur du centre de recherche de l'Ecole des Officiers de la Gendarmerie Nationale (EOGN)
– Andy Archibald, Directeur adjoint de l'unité nationale cybercriminalité de l'Agence Nationale de la Criminalité du Royaume--Uni
– Marco Lozano, Représentant INCIBE (Espagne)

Session 2: Les menaces cybernétiques : Analyse des risques et des stratégies

– Etat des lieux des cyber menaces par Jean--Dominique Nollet
– EC3--Europol L'investigation et la coopération entre les organisations internationales (Interpol, Europol,..) par Valérie Maldonado, OCLCTIC
– Analyse des réseaux sociaux et sécurité nationale par Thomas Delavallade, THALES – Comment améliorer la résilience face à la cybercriminalité et au cyber--terrorisme (Projet Européen CAMINO – FP7) Michal Choras, ITTI

Session 3: Enjeux et risques liés au développement des monnaies virtuelles; Irruption de l'innovation numérique dans la finance

– Flux illicites et monnaies virtuelles par Myriam Quéméner, Magistrate, cour d'appel de Versailles
– Crypto--monnaies et Blockchain : nouvelles opportunités d'investigation forensique sur le Darknet par Intervenant Camino ou Courage
– Monnaie virtuelle et crypto monnaie : quels enjeux et réponses réglementaires en Europe ? Quelles préconisations pour les utilisateurs et les entreprises? par Cathie--Rosalie Joly, Avocat, Barreau Paris et Bruxelles

---

Session 4: Big data, Internet des objets et sécurité : le pouvoir de l'anticipation au service de la cybersécurité par Adel Jomni, Enseignant-- chercheur, Université de Montpellier

– Le droit est--il un frein pour le développement du Big Data ? par Francesca Bosco, UNICRI
– Objets connectés et santé : l'innovation au service ou au détriment du citoyen par Corinne Thierache, Avocat associé
– Le Big Data pour lutter contre les attaques persistantes par Fraser Sampson, West Yorkshire Police

---

Session 5 : Projets européens, coopération internationale, recherche et formation dans le domaine de la lutte contre la Cybercriminalité et le Cyberterrorisme

– Défis majeurs de la recherche dans le domaine de la cybercriminalité et le cyber terrorisme par Akhgar Babak, Projet Européen COURAGE
– Nouvelles méthodes d'investigation et de formation forensique dans un environnement virtuel (cloud) (projet D--FET) par Bill Buchanan, Professeur, Université Napier d'Edimbourg
– La coopération internationale pour renforcer les capacités de protection des infrastructures d'information critiques 2015--2020 (CIIP) par Jean--Christophe Letoquin, Expert auprès du Conseil de l'Europe, Président de SOCOGI
– Projet ePOOLICE par Estelle de Marco
– L'entraide judiciaire en matière de traitement judiciaire de la Cybercriminalité à l'échelle Européenne et internationale par Victoria CATLIFF

Cet événement organisé en partenariat avec les membres des projets européens CAMINO et COURAGE (Cybercrime and Cyberterrorism European Research Agenda), s'inscrit dans une démarche de réflexion et d'échange visant à promouvoir une

vision européenne de la cybersécurité et à renforcer la lutte contre la Cybercriminalité et le Cyberterrorisme, priorité de l'Union Européenne pour laquelle les deux projets ont été élaborés.

Source :
Adel JOMNI et Denis JACOPINI

Alerte : La campagne d'un annonceur de Google détournée par des pirates | Le Net Expert Informatique

Alerte : La campagne d'un annonceur de Google détournée par des pirates

Des chercheurs en sécurité de la société néerlandaise Fox-IT ont repéré une campagne malveillante quand les annonces diffusées par Engage Lab, un partenaire de Google en Bulgarie, ont commencé à rediriger les utilisateurs vers le Nuclear Exploit Kit. Les kits d'exploit sont des plates-formes d'attaques basées sur le web dont l'objectif est d'exploiter les vulnérabilités des navigateurs et de leurs plug-ins pour infecter les ordinateurs des utilisateurs avec des malwares.

LNuclear Exploit Kit cible spécifiquement les vulnérabilités dans Flash Player d'Adobe, Java d'Oracle et Silverlight de Microsoft. « On dirait que l'ensemble du domaine engagelab.com, sa publicité et sa zone d'ID, est actuellement redirigé vers un domaine qui, à son tour, redirige vers le Nuclear Exploit Kit, attestant d'un éventuel piratage de ce revendeur de services de publicité partenaire de Google », a déclaré le chercheur de Fox-IT, Maarten van Dantzig dans un blog.
Ces redirections ont été stoppées tard dans la journée, ce qui montre que Google ou Engage Lab ont pris certaines mesures. Mais aucun n'a répondu aux demandes de commentaire de nos confrères d'IDG News Service. On ne sait pas combien de sites, ni combien d'utilisateurs ont été touchés, mais, selon Maarten van Dantzig, Fox-IT « a détecté une quantité relativement importante d'infections et de tentatives d'infection de nos clients par ce kit d'exploit ». Les chercheurs de Fox-IT n'ont pas encore identifié le malware distribué par cette campagne. Le problème du « malvertising », ces campagnes de fausses publicités qui détournent les internautes vers des pages web infectées, existe depuis plusieurs années et ne cesse de prendre de l'ampleur.
Et, même si les grands réseaux de publicités affirment avoir mis en place des défenses sophistiquées, les attaquants trouvent toujours de nouveaux moyens pour les contourner. Ces attaques sont particulièrement dangereuses, car elles n'ont pas besoin de rediriger les internautes vers des sites Web obscurs pour diffuser leur malware. Une fois que les attaquants parviennent à pousser leurs annonces malveillantes sur un grand réseau de publicité, celles-ci s'affichent sur des sites populaires dans lesquels les utilisateurs ont généralement confiance.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-la-campagne-d-un-annonceur-de-google-detournee-par-des-pirates-60793.html
Par Jean Elyan

Infectée par un cryptolocker, la police du Massachusetts paie 500$ de rançon | Le Net Expert Informatique

Infectée par un cryptolocker, la police du Massachusetts paie 500$ de rançon

La police de la ville de Tewksbury, dans le Massachusetts, victime d'un cryptolocker, a du régler 500$ pour déchiffrer les fichiers conservés sur un serveur afin de remettre ses équipes au travail.

Un Département de police du Massachusetts, celui de la ville de Tewksbury, a du verser 500 $ à un cyberpirate pour débloquer les fichiers chiffrés avec un cryptolocker, le ransomware qui verrouille les disques durs jusqu'à ce que les propriétaires paient une rançon. Après plusieurs jours d'essais infructueux, les services informatiques de la police de Tewksbury ont réalisé qu'ils ne pouvaient pas casser le chiffrement et payé la rançon pour obtenir la clef privée permettant d'accéder aux données.
« Ils ont rendu inopérant le logiciel que nous utilisons pour assurer le fonctionnement du Département de la police », a déclaré le chef de la police, Timothy Sheehan, au journal Tewksbury Town Crier. L'incident est survenu à la fin de l'année dernière, l'infection a démarré le 7 décembre sur un poste de travail.

Une attaque très ciblée
Les attaquants ont exploré le réseau jusqu'à corrompre le serveur principal du Département. Les services de Police sauvegardent leurs fichiers sur un disque dur externe qui a également été touché par le ransomware, de sorte qu'ils avaient le choix de payer 500 $ ou de perdre toutes les données.
La police de l'État et le FBI se sont penchés sur cette affaire, tout comme Delphi Technology Solutions et Stroz Friedberg, des sociétés spécialisées dans la police scientifique. Aucune des deux n'a réussi à casser le cryptage de sorte que le Département a payé, indique le journal local. Stroz Friedberg a converti les 500 $ de la rançon en bitcoins avant de l'envoyer de la part du Département de police.

Payer ou pas
Les applications affectées concernaient la répartition des tâches assignées aux différents agents, la gestion des documents, la main courante avec les arrestations et la conservation des appels au commissariat. La même mésaventure s'est déjà produite en 2013 dans un autre service de police à Swansea, toujours dans le Massachusetts ; 750$ avaient alors été réglés pour débloquer le système.
De nombreux experts estiment que les victimes auraient du refuser de payer, surtout s'ils s'agit des forces de l'ordre, mais après avoir examiné l'alternative, c'est-à-dire ne jamais revoir ses données, de nombreuses entreprises préfèrent payer afin de recommencer à travailler.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-infectee-par-un-cryptolocker-la-police-du-massachusetts-paie-500$-de-rancon-60783.html
Par Serge Leblal

Votre employeur peut espionner vos communications chiffrées, et la CNIL est d’accord | Le Net Expert Informatique

	Votre employeur peut espionner vos communications chiffrées, et la CNIL est d’accord

La Commission nationale informatique et libertés donne sa bénédiction au déchiffrement des flux HTTPS des salariés, à condition que cette pratique soit encadrée. Il reste néanmoins une zone de flou juridique côté pénal…

Saviez-vous que certains employeurs déchiffrent systématiquement les flux HTTPS de leurs salariés lorsqu'ils surfent sur Internet ? Ils disposent pour cela d'un équipement appelé « SSL Proxy » qui se place entre l'utilisateur et le serveur Web. Cette boîte magique déchiffre tous les échanges en usurpant l'identité du service interrogé (google.com, par exemple), par l'utilisation d'un certificat bidon. La pratique n'est pas du tout récente, mais se fait de manière un peu cachée en raison d'incertitudes juridiques et de l'impopularité de cette mesure auprès des salariés. Les directeurs informatiques n'ont, par conséquent, pas une folle envie d'en faire la publicité.
Mais l'employeur peut se rassurer : la CNIL vient de publier une note qui clarifie les choses. Ainsi, la Commission estime que le déchiffrement des flux HTTPS est parfaitement « légitime », car elle permet à l'employeur d'assurer « la sécurité de son système d'information », en bloquant les éventuels malwares qui s'y trouveraient. Evidemment, ce n'est pas la seule raison : ces équipements sont également utilisés pour prévenir les fuites d'informations. Un salarié qui enverrait des documents confidentiels à un concurrent pourrait, ainsi, être facilement repéré.

Infraction pénale ou pas ?
Toutefois, la CNIL met un (petit) bémol. L'utilisation de cette technique de surveillance doit être « encadrée ». Ainsi, les salariés doivent être informés en amont et de manière « précise » sur cette mesure : raisons invoquées, personnes impactées, nature de l'analyse effectuée, données conservées, modalités d'investigation, etc. L'employeur doit également mettre en place une « gestion stricte des droits d'accès des administrateurs aux courriers électroniques ». Autrement dit : éviter que tous les membres du service informatique puissent fouiller dans les messageries. Par ailleurs, les « traces conservées » doivent être réduites au minimum.
Il reste néanmoins une petite zone de flou juridique, nous explique la CNIL. En effet, le Code pénal interdit théoriquement « d'entraver ou de fausser le fonctionnement d'un système de traitements automatisés de données (STAD) ». Or, quand l'entreprise déchiffre les flux Gmail de ses salariés, on peut estimer que cela fausse le fonctionnement du STAD d'un tiers, à savoir Google. Cela pourrait donc constituer une infraction. Conclusion de la CNIL : il faudrait peut-être modifier le Code pénal pour que l'employeur puisse réellement surveiller ces flux chiffrés en toute tranquillité. Décidément, la situation n'est pas encore totalement claire…

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.01net.com/editorial/651057/votre-employeur-peut-espionner-vos-communications-chiffrees-et-la-cnil-est-d-accord/
Par Gilbert Kallenborn

La chaîne TV5 Monde victime d'un piratage de grande

ampleur par des individus se réclamant du groupe Etat Islamique | Le Net Expert Informatique

La chaîne TV5 Monde victime d'un piratage de grande ampleur par des individus se réclamant du groupe Etat Islamique

Stupeur à TV5 Monde. La chaîne publique francophone internationale est victime, mercredi 8 avril au soir, d'une importante attaque informatique menée par des militants islamistes se revendiquant de l'organisation Etat islamique (EI), a confirmé son directeur général Yves Bigot. « Nous ne sommes plus en état d'émettre aucune de nos chaînes. Nos sites et nos réseaux sociaux ne sont plus sous notre contrôle et ils affichent tous des revendications de l'Etat islamique », a-t-il indiqué

Propagande et documents postés sur Facebook

Les pirates ont posté des contenus de propagande sur la page Facebook de la chaîne, ainsi que des documents présentés comme des pièces d'identité et des CV de proches de militaires français impliqués dans les opérations contre l'EI. Après près de deux heures, les équipes de la chaîne ont pu reprendre la main sur la page de le TV5 Monde sur le réseau social. Les programmes ont par ailleurs été interrompus, tandis que le site internet de TV5 Monde est toujours indisponible.

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.francetvinfo.fr/monde/proche-orient/offensive-jihadiste-en-irak/la-chaine-tv5-monde-victime-d-un-piratage-de-grande-ampleur-par-des-individus-se-reclamant-du-groupe-etat-islamique_871789.html#xtor=EPR-51-la-chaine-tv5-monde-victime-d-un-piratage-de-grande-ampleur-par-des-individus-se-reclamant-du-groupe-etat-islamique_871789-20150408-bouton

---

Nouvelles formes d'attaques informatiques | Le Net Expert Informatique

Nouvelle formes d'attaques informatiques

Sévissant depuis l'année dernière, ce malware de nouvelle génération combine techniques informatiques sophistiquées, ingénierie sociale et intervention humaine pour que la fraude soit effective. Nom de code : Dyre Wolf

Entre 500 000 et 1,5 million de dollars par attaque. Tel est le butin ramassé lors de l'attaque réalisée à l'aide du malware Dyre qui sévit depuis le mois d'octobre dernier. Mais les criminels derrière ce programme ont récemment franchi une nouvelle étape qui permet au programme de retrouver une nouvelle jeunesse, au grand dam des entreprises qui en sont victimes.
L'attaque se déroule en plusieurs étapes. Dans un premier temps, des utilisateurs reçoivent un mail contenant une pièce jointe, elle-même infectée par le logiciel Upatre. Le but de ce logiciel est uniquement de permettre le téléchargement de Dyre, un programme beaucoup plus dangereux. Lorsque Dyre est téléchargé, il va essayer de se répandre le plus largement possible chez les autres employés de l'entreprise ou les amis de la personne infectée au travers du programme de messagerie Outlook. En parallèle, le logiciel va surveiller le travail de la personne infectée et attendre qu'elle se connecte à un parmi des centaines de sites bancaires que le maliciel est programmé pour surveiller.

Le voleur au bout du fil
Et c'est là que cela devient tout à fait nouveau. Lors de la tentative de connexion au site, Dyre va afficher un message indiquant que la connexion et le compte posent un problème et va inviter la personne à contacter un numéro de téléphone. Précisons que ceci se passe indépendamment du navigateur utilisé : Chrome, Firefox ou Internet Explorer. En effet, les trois navigateurs ont été usurpés.
En composant le numéro de téléphone, la victime ne va pas tomber sur un centre d'appel mais sur une vraie personne qui va se proposer de « l'aider » à régler son problème. Cette personne en apparence tout à fait bien intentionnée va donc vous demander des informations sur votre compte et pendant que vous discutez avec elle, elle procédera à un transfert de fonds depuis le compte bancaire de l'entreprise vers les propres comptes des criminels. « L'intervention d'un opérateur au téléphone en direct est unique», précise Caleb Barlow, vice-président d'IBM.

Et un petit DDOS pour bien masquer le tout
Enfin, simultanément au transfert de fonds, le site web de l'entreprise qui vient d'être pillée va être victime d'une attaque en DDOS. Le but de cette attaque est de détourner l'attention des services IT et de sécurité qui seront trop occupés à endiguer cette attaque pour s'occuper d'une escroquerie financière, du moins dans les premiers jours.
On le voit : l'imagination des cybercriminels est débordante. Comme à l'habitude, IBM répète une série de conseils, notamment de ne jamais fournir des informations bancaires à quiconque, les « vraies » banques ne demandant jamais ce type d'informations.

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.mag-securs.com/news/articletype/articleview/articleid/34604/dyre-wolf-nouvelle-etape-dans-la-cybercriminalite.aspx
Par Raphaël Stencher