Des chercheurs découvrent un navigateur malveillant, il se présente comme une imitation de Chrome afin de tromper les utilisateurs | Le Net Expert Informatique

Des chercheurs découvrent un navigateur malveillant, il se présente comme une imitation de Chrome afin de tromper les utilisateurs

Face à la diversité des outils de détection de malwares, les pirates informatiques n'hésitent pas à faire preuve d'inventivité pour atteindre leurs objectifs. En effet, une société du nom de Claralabsoftware a mis en œuvre un navigateur du nom d'eFast. Ce navigateur est censé améliorer l'expérience de navigation en fournissant des résultats de recherche les plus pertinents, en affichant des réductions et bonnes affaires disponibles sur la toile, et en fournissant des outils de protection contre les phishings et divers malwares. Il est basé sur Chromium, le navigateur open source sur le lequel sont fondés plusieurs autres navigateurs dont Chrome, Opera, Vivaldi, etc.

Les utilisateurs voyant donc les caractéristiques d'eFast pourraient croire à une application dénuée de tout code malveillant, mais tant s'en faut. Selon le rapport de Malwarebytes, l'entreprise de sécurité informatique, lorsque vous installez eFast, ce dernier essaie automatiquement de prendre le contrôle du terminal sur lequel il est installé en cherchant à devenir le navigateur par défaut.

En plus de cette action, eFast s'associe par défaut avec les extensions de fichiers suivantes : gif, htm, html, jpeg, jpg, pdf, png, shtml, webp, xht, xhtml. La même association est effectuée pour les schémas, protocoles, et autres objets URL suivants : ftp, http, https, irc, mailto, mms, news, nntp, sms, smsto, tel, urn, webcal.

Lorsque ces extensions sont associées par défaut à eFast, pour toute tentative d'ouverture de fichier, d'appel d'un protocole ou toute action utilisant les objets listés plus haut, c'est le navigateur eFast qui exécutera l'action souhaitée.

En plus de cela, eFast redirigeraient les internautes vers des pages publicitaires ou d'autres pages web qui pourraient héberger des malwares. En outre, PCrisk rapporte qu'eFast est un aspirateur de données de navigation. Ces informations une fois collectées pourraient être partagées avec d'autres personnes et utilisées à mauvais escient afin de gâcher la vie d'un internaute.

Selon PCrisk, ce programme pourrait s'installer lors de l'installation de certains programmes. En effet, les développeurs pourraient cacher l'option d'installation de ce programme dans les paramètres personnalisés. C'est pourquoi il est recommandé de ne pas installer les applications en utilisant les paramètres de recommandation, mais plutôt les paramètres personnalisés.

Une des choses à ne pas négliger par ailleurs est que lors de l'installation d'eFast, celui-ci se charge de supprimer les raccourcis de Chrome sur le bureau et la barre des tâches et installe par la même occasion des raccourcis de YouTube, Amazon, Facebook, Wikipedia et Hotmail sur le bureau. Il faut noter qu'il est très similaire à Chrome aussi dans la présentation générale que dans les couleurs de l'icône.

Enfin, nous précisons qu'en voulant nous rendre sur le site de l'éditeur clara-labs afin d'effectuer des recherches supplémentaires, Chrome nous a envoyé une alerte afin de signaler que le site que nous voulons ouvrir contient des programmes dangereux. Ce n'est donc pas uniquement le produit de l'entreprise qui est étiqueté comme dangereux, mais même le site l'est également.

Source :
http://www.developpez.com/actu/91354/Des-chercheurs-decouvrent-un-navigateur-malveillant-base-sur-Chromium-il-se-presente-comme-une-imitation-de-Chrome-afin-de-tromper-les-utilisateurs/
par Olivier Famien

La Marine Américaine reprend la navigation céleste | Le Net Expert Informatique

	La Marine Américaine reprend la navigation céleste

Face à la menace croissante des cyberattaques, l'US Navy repasse au sextant qui fait ainsi son retour dans l'armée la plus moderne au monde.

Après près de 20 ans d'interruption, l'Académie navale américaine d'Annapolis (Maryland) recommence à former ses aspirants à la navigation astronomique, vu le danger de plus en plus imminent des cyberattaques, rapporte le Washington Post.

« Nous nous sommes entièrement informatisés, en renonçant au sextant en faveur des ordinateurs qui sont vraiment excellents. Le problème, c'est qu'il n'y a plus de solution de secours », a déclaré au journal le lieutenant-colonel Ryan Rogers, titulaire de la chaire de navigation à l'Académie.

Le bon vieux sextant fait son retour dans l'armée la plus moderne au monde, car cet instrument restera fiable en cas de cyberattaque. La réintroduction du sextant marque en quelque sorte la fin de la croyance en l'infaillibilité technologique.

L'été dernier, les aspirants de l'Académie d'Annapolis ont commencé à recevoir trois heures de cours hebdomadaires. La promotion 2017 sera la première à avoir des rudiments dans l'utilisation du sextant.

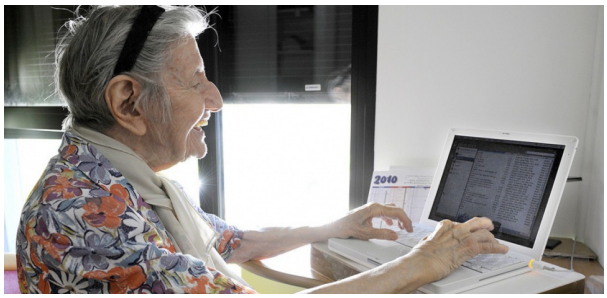
Dans le contexte des scandales d'espionnage informatique qui défraient la chronique depuis un certain temps avec les révélations sur l'activité de l'agence américaine NSA, bien des pays, dont la Russie, envisagent un retour aux vieilles méthodes.

Les spécialistes soulignent que du point de vue de la sécurité, toute sorte de communication électronique est vulnérable. On peut capter n'importe quelle information depuis un ordinateur, il existe des moyens de protection, mais sans garantie à 100 % de leur sûreté. Pour garder des secrets, la « méthode primitive » est préférable: la main humaine avec un stylo ou la machine à écrire.

Source :

http://fr.sputniknews.com/international/20151017/1018907696/usa-marine-sextant-cyberattaques.html

Pas assez connectée pour être menacée ? Madame Walsh s’est pourtant fait pirater | Le Net Expert Informatique

	Pas assez connectée pour être menacée ? Madame Walsh s’est pourtant fait pirater

Le piratage, ça n'arrive pas qu'aux autres. Et il n'y a pas besoin d'être ultra-connecté pour en être victime. C'est ce que raconte le « New York Times », avec l'exemple de Madame Walsh, vivant en Californie.

Cette grand-mère de six petits-enfants a accepté de servir de cobaye à deux hackeurs, se pensant à l'abri, puisque n'étant pas quelqu'un de « connecté ».
Mme Walsh explique ne disposer d'aucun objet connecté (montre, etc.), sa maison n'est équipée d'aucun appareil technologique récent (thermostat connecté ou autre), et elle n'est pas une grande adepte des gadgets électroniques. Bien sûr, elle dispose d'un compte Facebook, mais n'y publie jamais rien, et s'en sert uniquement pour rester en contact avec des amis. Et pourtant.

E-mail, PaylPal, télévision et garage piratés

Les hackeurs ont bien réussi à pirater Madame Walsh. Le quotidien raconte que les pirates ont successivement testé plusieurs pistes pour tenter de s'attaquer à la grand-mère. Si son compte Facebook se révèle bien protégé, la découverte d'un « J'aime » pour une page de la plateforme de pétitions Change a été le déclic.
Dix minutes plus tard, les hackeurs adressent à Mme Walsh un faux e-mail émanant de Change.org proposant de signer une fausse pétition. Bingo, la grand-mère clique, et entre son identifiant et son mot de passe. La voilà victime de « phishing ».
Madame Walsh confesse au « New York Times » utiliser le même mot de passe sur l'ensemble des services internet. Les pirates sautent sur la brèche et s'introduisent dans sa messagerie e-mail pour récupérer ses données de sécurité sociale et d'assurance maladie, et de ses comptes PayPal et Miles.
Pis, les hackeurs s'introduisent également dans le compte e-mail de sa fille, dont le code était « caché » dans un message. Enfin, ils laissent sur l'ordinateur de Mme Walsh un virus qui enregistre tout ce qui est tapé et remplace les publicités des sites visités afin de leur générer des revenus.
Pas repus, les deux hackeurs se sont attaqués à sa maison. En une heure et demie, ils ont pris le contrôle de sa télé (l'installateur du câble n'avait pas protégé la connexion) et trouvé un moyen d'ouvrir à distance la porte de son garage (via un procédé de « brute force » qui a essayé des centaines de combinaisons possibles avant de tomber sur la bonne pour la porte électrique).

Le phishing, risque numéro un

L'exemple du « New York Times » est extrême mais illustre bien que personne n'est à l'abri d'un piratage, même ceux qui se pensent « trop peu connecté pour être en danger ». Et le risque premier demeure le phishing, aussi appelé hameçonnage.
Aujourd'hui, plus de 90% des attaques dans le monde démarrent par un e-mail de phishing », affirme Ismet Geri, directeur général pour la France et l'Europe du Sud de Proofpoint, société spécialisée dans la sécurité des e-mails.
Un e-mail sur 392 serait une tentative de phishing, estime l'entreprise de sécurité informatique Symantec dans son dernier rapport. Au total, 37,3 millions d'internautes sont tombés dans le panneau dans le monde, affirme une enquête de la société de sécurité Kaspersky. La France se classe septième pays au monde dans les victimes avec un internaute sur 30 floué.

LIRE »J'ai cliqué » : chronique d'un phishing ordinaire

L'objectif des pirates est simple : récupérer des coordonnées bancaires, mais aussi des informations personnelles. Selon Symantec, au marché noir, les détails d'une carte de crédit se revendent entre 0,50 et 20 dollars, un passeport scanné 1 à 2 dollars, l'accès à un compte cloud 7 à 8 dollars, l'accès à un compte de jeux vidéo en ligne 10 à 15 dollars, etc.
L'utilisation de ces données est évidente. Les données bancaires permettent d'effectuer des achats en ligne, tandis que les informations personnelles vont permettre de s'identifier sur l'ensemble des services. Surtout que le sésame identifiant/mot de passe devient un Graal, quand on sait que 75% des Français utilisent toujours le même mot de passe.
Je m'estimais plutôt malin, je m'étais trompé ! », a confié le blogueur Thomas Messias au « Parisien » après un piratage de ses comptes. « Evidemment, j'utilisais le même mot de passe pour eBay et pour tous les autres sites… »
Voilà Madame Walsh prévenue. Et pour ce qui est de la maison, de nombreux experts en informatique démontraient régulièrement comment prendre le contrôle d'objets usuels. Cet été, le hackeur Samy Kamkar a démontré comment ouvrir des portes de garage à partir d'un jouet Mattel en moins de 10 secondes :

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://tempsreel.nouvelobs.com/tech/20151015.OBS7721/pas-assez-connectee-pour-etre-menacee-madame-walsh-s-est-pourtant-fait-pirater.html#xtor=EPR-1-ObsActu8h-20151016

Oups ! Uber dévoile les données personnelles de chauffeurs | Le Net Expert

Informatique

Oups ! Uber dévoile les données personnelles d

Un bug permettait de voir les données personnelles d'autres chauffeurs Uber. La société assure que seuls 700 conducteurs US ont été affectés et que la faille a été corrigée en seulement 30 minutes.

Uber l'assure, ses services sont bons pour l'économie et créent de l'emploi – pas salarié cependant, les chauffeurs ne signant pas de contrat de travail avec la multinationale. En France, la société a dû faire face au mécontentement, et pas des taxis cette fois, mais des chauffeurs eux-mêmes. La faille de sécurité dont a été victime cette semaine le service devrait probablement moins affecter ces travailleurs que la diminution tarifaire imposée par Uber. La société a ainsi, accidentellement, divulgué les données personnelles de plusieurs centaines de chauffeurs.

Un bug de débutant, mais des conséquences mineures

Cette fuite de données est la conséquence d'un bug logiciel. Elle a abouti à la divulgation de l'identité de conducteurs Uber, dont leurs numéros de sécurité sociale, parmi d'autres données sensibles. En enregistrant des documents d'assurance auprès d'Uber, des chauffeurs ont constaté que s'affichaient les informations d'autres utilisateurs de la plateforme.

Mais pas de panique, assure la société américaine. Selon cette dernière, qui a notamment été interrogée par The Register, moins de 700 chauffeurs américains sont concernés par cet incident. Et par ailleurs, poursuit Uber, le bug a été corrigé dans les 30 minutes qui ont suivi sa découverte.

Selon Gawker, ce bug pourrait être lié à la sortie d'une nouvelle application : Uber Partner. Celle-ci permet aux conducteurs de gérer leurs comptes et de suivre leurs courses, mais aussi de transmettre des données pour l'enregistrement des nouveaux chauffeurs.

En comparaison de la faille de sécurité du début d'année, la dernière semble mineure. Une base de données de 50.000 chauffeurs Uber avait en effet fuité sur GitHub. La société a été critiquée à plusieurs reprises pour ses pratiques en matière de sécurité et de confidentialité des données.

Pour redorer son blason et améliorer la sécurité de ses développements, Uber a créé cette année un poste de responsable de la sécurité informatique (RSSI) et embauché deux hackers renommés, Charlie Miller et Chris Valasek.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.zdnet.fr/actualites/oups-uber-devoile-les-donnees-personnelles-de-chauffeurs-39826600.htm

Piratage de TV5 Monde: une facture très salée | Le Net Expert Informatique

	Piratage de TV5 Monde: une facture très salée

L'attaque subie par la chaîne francophone internationale en avril lui aura coûté plus d'une dizaine de millions d'euros. De quoi obliger TV5 à tailler dans son budget 2016.

« La sécurité informatique coûte cher, mais combien coûte l'absence de sécurité? », pourrait-on s'interroger, en paraphrasant Lincoln.

Chez TV5 Monde, on commence à avoir une idée du coût du piratage subi par la chaîne le 8 avril dernier: il dépassera largement la dizaine de millions d'euros.

Création d'une cellule de sécurité informatique

Précisément, ce piratage entraînera un surcoût de 4,8 millions d'euros cette année; de 2,4 millions d'euros l'an prochain; et pour les années suivantes 2 à 2,5 millions d'euros par an.

En pratique, la chaîne internationale a dû bien sûr investir pour renforcer la sécurité de ses réseaux. Un plan a été élaboré à partir des recommandations de l'ANSSI (Agence nationale de sécurité des systèmes d'information). Ce plan comprend notamment la création d'une cellule permanente dédié à la sécurité informatique qui n'existait pas auparavant. Une équipe de six nouveaux salariés est actuellement en cours de recrutement.

Sites web « sinistrés »

Mais ce n'est pas tout. La chaîne francophone fonctionne encore « en mode dégradé », indique son budget 2016. Interrogée, la chaîne n'a pas précisé ce que cela signifiait précisément. Mais le budget 2016 indique que de nombreuses missions (notamment la mise en ligne des émissions sur le site web), jusqu'à présent réalisées automatiquement, se font désormais manuellement, ce qui nécessite du personnel supplémentaire. « Les sites internet de la chaîne sont sinistrés », indique le budget.

Evidemment, de telles sommes sont significatives au regard du budget de la chaîne (110 millions d'euros). Des économies ont donc dû être recherchées sur d'autres postes. « Les budgets d'opérations (programmes, sous-titrage, marketing, communication) » ont été réduits. Notamment, « les budgets destinés aux acquisitions de programmes et au sous-titrage sont fortement affectés ».

La publicité sur internet « s'effondre »

Les malheurs de la chaîne ne s'arrêtent pas là. Le site web, dont l'audience déjà en chute libre depuis plusieurs années, a été inaccessible, puis ensuite rétabli avec un contenu réduit, ce qui accéléré la chute de l'audience. Au total, les visites ont chuté de 13% au premier semestre, et les vidéos vues de 15%. « La baisse significative des audiences numériques risque de s'accentuer dans les mois à venir », prévient le budget. Conséquence logique: « les recettes publicitaires sur le numérique s'effondrent ».

Rappelons que de nombreuses erreurs avaient été mises à jour après le piratage. Le site spécialisé Zataz a assuré avoir signalé à la chaîne publique une dizaine de failles depuis deux ans. Selon 01net.com, le réseau bureautique et le réseau de production télé de TV5 n'étaient pas totalement cloisonnés, ce qui a permis au piratage du premier de contaminer le second, entraînant un écran noir…

Enfin, Arrêt sur images avait relevé que les mots de passe étaient affichés sur le mur. Filmés lors d'un reportage effectué dans les locaux par France 2 suite à l'attaque, ils avaient été donc été potentiellement vus par des centaines de milliers de téléspectateurs… Le mot de passe du compte YouTube était ainsi lemotdepassedeyoutube… TV5 avait admis « une bourde » et assuré que les mots de passe n'étaient pas affichés ainsi avant le piratage.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Source : http://bfmbusiness.bfmtv.com/entreprise/piratage-de-tv5-monde-une-facture-tres-salee-922231.html
Par Jamal Henni

Surveillance : le spyware FinFisher détecté dans 32 pays | Le Net Expert Informatique

Le spyware FinFisher détecté dans 32 pays

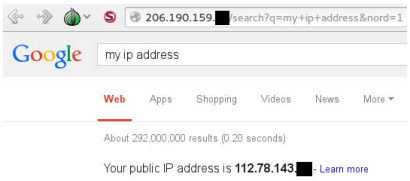
Malgré les mesures prises pour en dissimuler l'existence, le Citizen Lab a réussi à remonter à nouveau la trace du spyware FinFisher vendu aux autorités policières de nombreux états dans le monde, y compris dans des pays autoritaires.

Le business de l'espionnage des communications électroniques fonctionne toujours très bien. Alors que le piratage spectaculaire de la société Hacking Team n'a semble-t-il eu aucun effet notable sur ses relations commerciales avec les autorités qui exploitent ses services, son concurrent britannique FinFisher n'a visiblement lui non plus aucun problème à continuer ses activités, malgré la divulgation de ses codes sources et d'autres données internes en 2014.
Les gouvernements continuent de faire confiance à ces entreprises privées qui proposent ça et là des outils permettant de placer sur écoute des smartphones, d'accéder aux données d'un PC, de collecter toutes les touches frappées sur un clavier, d'activer discrètement des webcams, de géolocaliser des appareils, ou encore d'accéder au contenu de conversations en principe privées et chiffrées. Les intérêts pour la sécurité nationale priment sur les quelques questions éthiques que peuvent poser certaines méthodes, qui valent à ces firmes d'être placées sur une liste des « sociétés ennemis d'internet » par Reporters Sans Frontières.

Car les services qu'elles vendent ne sont pas achetés que par des démocraties bien sous tous rapports, malgré les restrictions à l'exportation qu'elles sont censées respecter.

Le laboratoire Citizen Lab a ainsi publié de nouvelles démonstrations de la présence des outils de Finfisher dans au moins 32 pays, dont plusieurs états peu recommandables du point de vue du respect des droits fondamentaux, comme la Malaisie, l'Arabie Saoudite, le Kazakhstan, l'Ethiopie, le Maroc ou le Bengladesh.
Déjà en 2012, le laboratoire avait prouvé que la suite d'outils d'espionnage Finfisher vendue à l'époque par la société britannique Gamma International (elle a depuis donné son indépendance à Finfisher GmbH, basée à Munich), était utilisée par au moins une quinzaine d'États dans le monde. Parmi eux figuraient déjà des pays autoritaires comme le Bahreïn, l'Ethiopie, l'Indonésie, le Turkménistan, ou les Emirats-Arabes Unies.
Comme Hacking Team, Finfisher assure qu'elle respecte l'arrangement de Wassenaar qui limite les possibilités d'exporter les outils de surveillance vers des pays autoritaires qui peuvent en faire un usage non conforme aux droits de l'homme, par exemple pour traquer des opposants politiques ou rechercher les sources de journalistes hostiles au régime. Mais la présence continue de ses outils sur des serveurs appartenant à des régimes dictatoriaux permet, au minimum, de douter de la véracité de telles affirmations.
Depuis les révélations de 2012, FinFisher a amélioré ses méthodes de dissimulation et systématiquement caché ses outils derrière des serveurs proxys, configurés pour paraître inoffensifs. Mais les chercheurs du Citizen Lab ont regorgé d'ingéniosité pour les trouver.
Depuis décembre 2014, l'organisation a scanné un maximum d'adresses IPv4 pour trouver des serveurs dont certaines caractéristiques correspondaient à ce qu'ils connaissaient de FinFisher. Ils ont trouvé 135 serveurs, dont la plupart étaient des serveurs proxys qui affichaient la page d'accueil de Google ou Yahoo. Ces serveurs là, qui servent uniquement de relais intermédiaire, n'avaient aucun intérêt puisqu'ils masquaient la géolocalisation des serveurs « maîtres » sur lesquels étaient installés les outils de FinFisher. Mais aux yeux de Google et Yahoo, c'est bien l'adresse IP du serveur maître qui communique.

PREMIÈRE ASTUCE :
« DIS-MOI MON ADRESSE IP »

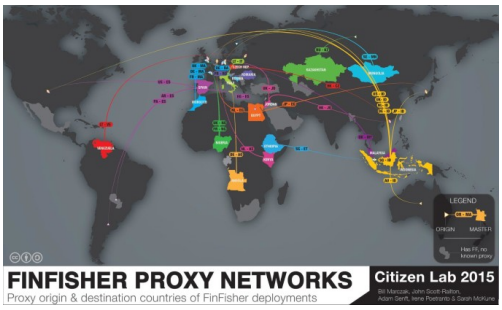


Lorsque Google était affiché, il suffisait d'exécuter la requête « my IP adress » (qui ne fonctionne pas avec Google France) pour que Google réponde au serveur maître, et que celui-ci renvoie la réponse au serveur relais, qui lui-même l'affichait à Citizen Lab. Ils ont ainsi pu trouver des adresses IP de serveurs maîtres installés dans différents pays, et découvrir leur géolocalisation.

DEUXIÈME ASTUCE :
« DIS-MOI QUEL TEMPS IL FAIT »

Sur Yahoo, la commande n'existe pas. Mais le service sait afficher la météo qui correspond au lieu qu'il associe à l'adresse IP de l'internaute. Les chercheurs ont donc demandé à Yahoo d'afficher la météo et découvert que, par exemple, un serveur qui était censément installé en Lituanie renvoyait la météo de Caracas, au Venezuela. Un pays où les journalistes sont régulièrement persécutés. Ca ne permettait pas d'obtenir en direct l'adresse IP, mais au moins de savoir où elle était attachée.

La carte des proxys :



Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

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

Source : http://www.numerama.com/tech/126760-surveillance-le-spyware-finfisher-detecte-dans-32-pays.html
Par Guillaume Champeau
Crédit photo de la une : Thibaut Démare

Alerte de cyberattaques dans les avions | Le Net Expert Informatique

Alerte de cyberattaques dans les avions

L'Agence européenne de sécurité aérienne (AESA) estime que l'aviation est vulnérable et qu'il faut mettre en place des structures dédiées pour lutter contre cette nouvelle menace.

En mai dernier, lorsque le hacker Chris Roberts avait fait les gros titres avec son histoire de piratage d'un avion en plein vol, les compagnies aériennes ont rétorqué en cœur qu'une telle action serait totalement impossible. Elle estimaient que M. Roberts n'était qu'un vantard mythomane. Mais les instances de régulation commencent à voir les choses d'un œil différent, à commencer par celles de l'Union européenne.

Interrogé par l'association des journalistes de la presse aéronautique et spatiale (AJPAE), le directeur exécutif de l'Agence européenne de sécurité aérienne (AESA) Patrick Ky a souligné la vulnérabilité de l'aviation à un éventuel acte de piratage. « C'est un risque auquel il faut qu'on se prépare, l'aviation est vulnérable. Dire que l'aviation n'est pas sujette au cyber-risque, c'est se voiler la face », a-t-il déclaré. Selon le patron de l'agence, il faut mettre en place des « réseaux spécifiques » de spécialistes en cyberattaques pour « informer de la menace et des moyens de s'en prévenir ».

L'AESA fait appel à un hacker

M. Ky a affirmé avoir pu lui-même constater les capacités d'un hacker à pénétrer le réseau de communication d'une compagnie aérienne. « J'ai fait appel à un hacker qui a la particularité d'avoir également une licence de pilote commercial, a-t-il expliqué auprès des Echos. En moins de 5 minutes, il est parvenu à rentrer dans le réseau Acars ». Acars (Aircraft Communication Addressing and Reporting System) est un système de communication et de surveillance par radio basé sur l'échange de messages entre un avion et une station au sol. Il intervient dans la gestion du trafic aérien et permet de s'assurer du bon fonctionnement des équipements de l'aéronef. Mais le hacker ne s'est pas arrêté là. « Il ne lui a fallu que deux ou trois jours pour pénétrer dans le système de contrôle d'un avion au sol. Pour des raisons de sécurité, je ne vous dirai pas comment il a fait », ajoute Patrick Ky.

En décembre dernier, cinq grandes organisations internationales de l'aviation (OACI, ACI, CANSO, IATA et ICCAIA) avaient adopté une feuille de route commune pour harmoniser leurs mesures respectives en matière de cybermenaces, et souligné que « la sécurité et la sûreté du système aéronautique mondial » étaient « potentiellement vulnérables aux attaques de pirates informatiques et autres cybercriminels ».

Denis JACOPINI est Expert Informatique, formateur et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://hightech.bfmtv.com/internet/l-europe-sonne-l-alerte-sur-le-risque-de-cyberattaques-dans-les-avions-920964.html
Par Gilbert Kallenborn

Attaque par phishing simulée au PMU : 120 employés piégés | Le Net Expert Informatique

	Attaque par phishing simulée au PMU : 120 employés piégés

La pièce jointe que l'on ouvre et qui diffuse un virus dans toute l'entreprise demeure le vecteur principal des attaques informatiques. Le PMU a testé les réactions de ses collaborateurs en mai dernier en leur envoyant un email de ce type conçu par ses soins. 22% ont cliqué dans la pièce jointe.

Le hack, c'est trop facile. Environ 120 collaborateurs du PMU se sont laissés piéger par un faux email leur proposant de gagner un iPad. Ils ont cliqué dans le lien présent dans l'email et donné leurs coordonnées.

6% ont donné leurs coordonnées

C'est le résultat d'un test mené en vraie grandeur par le PMU en mai dernier pour mesurer la résistance à une attaque par phishing de ses collaborateurs. Résultat : 22% des salariés ont ouvert la pièce jointe associée à un faux email d'invitation à participer à un jeu pour gagner un iPad.

Et 6% – soit environ 120 personnes – ont cliqué sur le lien présent à l'intérieur et donné leurs coordonnées pour gagner le lot. La pièce jointe affichait un faux message destiné à effrayer durant quelques minutes ceux qui l'avaient ouverte en leur faisant croire que leur PC est en danger et va être vidé.

Le test a été réalisé de façon anonyme, par un prestataire externe, en revanche, on sait que ce sont des personnes de tous les services qui ont cliqué dans l'email.

L'attaque contre TV5 monde

La DRH a donné le feu vert à l'opération car le test a été réalisé juste après les incidents de TV5 Monde qui avait vu la chaîne être bloquée durant une journée à la suite d'une attaque informatique.

Le résultat est à la fois inquiétant et rassurant. Inquiétant car test est intervenu après que le PMU ait procédé à deux ou trois campagnes de sensibilisation au phishing, en expliquant aux collaborateurs qu'il ne faut pas cliquer sur les liens présents dans les emailings. Rassurant, car le fait que le PMU communique de tels résultats permet de sensibiliser l'ensemble des entreprises à ce type de risques.

Le phishing est banal

Le phishing est une attaque informatique qui consiste à envoyer des emails imitant ceux de sociétés reconnues – banques, organismes sociaux – afin de recueillir les coordonnées bancaires des personnes ciblées.

Les attaques qui propagent des virus informatiques dans les entreprises – appelées APT (Advanced Persistent Threat) – passent majoritairement par l'ouverture de pièces jointes qui diffusent ensuite un code informatique malveillant entre les machines du réseau de l'entreprise.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.larevuedudigital.com/2015/10/03/simulation-dune-attaque-par-phishing-120-employes-du-pmu-pieges/

Qui est responsable de la cybersécurité : le RSSI, le DSI, le PDG ou vous ? | Le Net Expert Informatique

La menace informatique est changeante et les décideurs IT peinent à s'adapter à un danger croissant. La cybermenace, certes significative, ne constitue qu'un élément de la sécurité de l'entreprise. Dès lors, qui devrait être responsable de la sécurité et comment les entreprises peuvent adopter une approche plus proactive face aux menaces ? Cinq experts IT donnent leur avis.

1. Faites de la sécurité la responsabilité de tous les salariés

« Le directeur général, et n'importe qui d'autre » répond David Allison à la question de savoir qui est responsable de la sécurité au sein de l'entreprise. Le responsable des systèmes métier pour Aggregate Industries estime que le PDG devrait être responsable de la sécurité, mais que chaque salarié a une responsabilité personnelle.

« La sécurité, ce n'est pas le confinement et la prévention » juge Allison, même si les pare-feu, les antivirus et les autres mesures IT doivent être considérés comme acquis. « Une grande sécurité, c'est affaire d'éducation, de sensibilisation et de responsabilité individuelle. »

Pour lui, le dirigeant de l'entreprise doit s'engager personnellement pour disposer d'une équipe en place formant le personnel dans un large éventail de domaines comme la gestion des courriels, la détection des liens suspects et l'adoption de bonnes pratiques pour les mots de passe.

« La sécurité a besoin d'être une culture diffusée au sein de l'organisation » souligne David Allison. « Le PDG met en place cette culture. Le responsable de la sécurité informatique (RSSI) définit et exécute la stratégie répondant à ce besoin – et chaque salarié est responsable de s'assurer d'adopter et de suivre les pratiques requises. »

2. Ne vous reposez pas sur des produits technologiques

Tim Holman, le président de l'ISSA, une association britannique de sécurité des SI, estime que la responsabilité au sein d'une entreprise se situe toujours au niveau des propriétaires ou des comités de direction. Certains Comex peuvent désigner un DSI, RSSI ou un directeur IT comme le responsable de la sécurité, mais ces individus ne peuvent jamais être tenus pour responsables.

« Les entreprises doivent avoir conscience de l'ampleur de la menace lorsqu'elles font du commerce sur Internet ou stockent leurs données sur le Cloud » déclare Holman. « Les entreprises peuvent charger un DSI d'implémenter une solution Cloud, mais elles resteront toujours responsables si quelque chose tourne mal. »

Face aux cybermenaces, les firmes doivent adopter une attitude proactive, et elles peuvent le faire au travers d'une simple analyse de risques, ou en suivant des standards comme IASME ou Cyber Essentials. D'après Tim Holman, la compréhension des enjeux liés à la sécurité progresse en consacrant du temps avec des dirigeants et en leur expliquant en termes simples les risques inhérents au business en ligne.

« La cybermenace ne peut pas être résolue en achetant des produits. Une approche de bon sens consistant à réduire le volume de données sensibles stockées, à éjecter les fournisseurs non-sécurisés, à restreindre l'accès aux données et à souscrire une cyber-couverture sera souvent dix fois plus efficace et dix fois moins chère que la dernière génération d'appliance de sécurité vendue par les experts de la vente. »

3- Gardez sous contrôle les périls des terminaux mobiles

David Reed, directeur des services d'information et de l'infrastructure à la Press Association (PA), juge complexe la discussion autour de la sécurité, mais est d'avis que la responsabilité commence au sommet de l'IT. « Si en tant que DSI, vous n'êtes pas en mesure de percevoir les dangers liés à la sécurité, vous ne faites pas un assez bon travail » tranche-t-il.

Un des domaines les plus importants pour Press Association est ainsi la gestion du mobile. Les journalistes de la société ont à traiter des informations extrêmement sensibles, et la menace de piratage d'un terminal, bien que sérieuse, n'est pas aussi répandue qu'une simple perte ou un vol. PA travaille avec EE pour implémenter une stratégie mobile COPE (un terminal de l'entreprise pour un usage personnel et professionnel) utilisant des Samsung S4 Mini et le système de sécurité Knox.

« Un conteneur peut être créé sur chacun des téléphones pour stocker séparément documents de travail, courriels et contacts et éléments personnels. Nos journalistes disposent principalement de deux zones sur leurs téléphones : une pour l'usage personnel et l'autre pour le travail » précise David Reed.

« Chez PA, nous aidons les journalistes en recommandant des apps. Nous avons appliqué ce principe pour les jeux du Commonwealth de 2014 en envoyant aux journalistes présents sur l'évènement un message pour télécharger l'app Team GB. L'appli était en liste blanche et installée simplement dans le conteneur. »

4- Obtenez le soutien du dirigeant pour les démarches de gouvernance

Pour Omid Shiraji, ex-DSI de Working Links, la responsabilité de la sécurité est totalement liée à l'entreprise et à la nature de ses activités. Il n'est pas persuadé de la nécessité de disposer d'un RSSI dans la majorité des organisations.

« La sécurité IT est une commodité. Vous pouvez acheter des produits et de l'expertise auprès d'un fournisseur » juge-t-il. « La même chose est vraie en ce qui concerne la sécurité des entreprises dans de nombreux cas – les processus et la gouvernance sont une marchandise que vous pouvez acheter comme un service géré. »

Omid Shiraji préférerait consacrer son budget IT limité aux opérations en première ligne, et ensuite s'appuyer sur une expertise spécifique pour l'aider à protéger ses données et guider son personnel. La société a récemment été certifiée ISO 27001 et le support du PDG s'est révélé essentiel.

« Les individus changent leur comportement car ils entendent le PDG parler des conséquences majeures des activités non protégées » déclare-t-il. « La sécurité IT est en fait le travail de chaque employé, mais le patron doit soutenir chaque initiative en matière de sécurité et de gouvernance dans l'entreprise. Et c'est ce qui s'est passé chez Working Links. »

5. Créez une culture du risque pragmatique

Julian Self, un DSI expérimenté qui a travaillé pour de nombreux acteurs de la finance, fait lui une analyse différente et estime que l'importance du RSSI dans l'entreprise continue de grandir. Selon lui, il est du ressort du DSI de promouvoir auprès des dirigeants les avantages d'un spécialiste de la sécurité.

« Dans un monde déjà hyper-connecté, et avec l'avènement de l'Internet des Objets, le travail de sécurisation des données de l'entreprise devient infiniment plus complexe avec des flux de données qui entrent et sortent de nombreux terminaux » commente Julian Self, pour qui le panorama de la menace continue d'évoluer.

« Les RSSI ne réussiront pas à moins d'avoir l'adhésion et l'engagement des métiers. Sans cela, ils seront simplement perçus comme des freins à l'activité et leurs efforts seront contournés. »

« Fondamentalement, les RSSI ont besoin de créer une prise de conscience et une culture pragmatique du risque afin que la sécurité de l'information soit appliquée de façon inconsciente dans tous les domaines de l'entreprise. Cette approche doit aller de pair avec une réponse à incidents qui soit proportionnée et sans alarmisme, et la gestion et la réaction au risque, restaurant in fine la confiance de l'entreprise. »

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://www.zdnet.fr/actualites/qui-est-responsable-de-la-cybersecurite-le-rssi-le-dsi-le-pdg-ou-vous-39826198.htm

---

Comment réagir face à une cyberattaque | Le Net Expert Informatique

Comment réagir face à une cyberattaque

Choc, sidération, déni… Une attaque informatique paralyse souvent les entreprises qui en sont victimes. L'idéal est donc de s'y préparer pour avoir les bons réflexes le moment venu. « Au début, une cyberattaque ne fait pas de bruit. L'entreprise continue apparemment à fonctionner normalement. Les cellules de crise classiques ont donc du mal à se mobiliser. Il faut s'adapter en prenant en compte la dimension cyber de l'attaque », remarque Gérôme Billois, expert en cybersécurité chez Solucom.

1 MONTER UNE CELLULE DE CRISE CYBER

La cellule de crise décisionnelle (direction générale, service juridique, RH, informatique, communication…) doit être secondée par une cellule de crise cyber. Idéalement, cette équipe est pilotée par le responsable sécurité des systèmes d'information (RSSI). Elle regroupe des membres de la direction informatique et les responsables des applications informatiques liées aux métiers de l'entreprise. Tous ces protagonistes doivent être sensibilisés à travers des exercices spécifiques, organisés annuellement.

« Suivant le scénario d'attaque, cela peut prendre la forme d'un exercice sur table de quelques heures à la simulation d'un début de crise », explique Gérôme Billois. Tout le monde doit être sur le pont. Les managers pour identifier les ressources à protéger, les RH pour répondre aux interrogations des collaborateurs, le service juridique pour évaluer les suites judiciaires, la communication si l'information de l'attaque a fuité…

2 DÉCONNECTER LES MACHINES INFECTÉES

Dès les premiers soupçons d'attaque, il faut réagir. Un grand industriel européen s'est mordu les doigts de ne pas avoir pris au sérieux les alertes remontées en 2012 par les autorités nationales. Résultat : le pirate a eu tout le loisir de sonder en profondeur son réseau informatique. « La crainte est qu'il ait eu accès au code source de nos outils informatiques qui permettent de gérer les infrastructures de nos clients », confie cet industriel. Il ne faut toutefois pas confondre vitesse et précipitation, prévient Jean-Yves Latournerie, préfet chargé de la lutte contre les cybermenaces au ministère de l'Intérieur. Les entreprises sont entre deux feux. D'une part, elles doivent isoler leur système de l'extérieur pour éviter la propagation de l'attaque. D'autre part, il faut éviter d'en effacer les traces. « Si on coupe et on efface les disques durs, les enquêteurs perdent les preuves et la possibilité de remonter aux auteurs de l'attaque », souligne le préfet.

La déconnexion peut être utile. Victime, en avril dernier, d'une attaque sévère qui a interrompu ses programmes, la chaîne de télévision TV5 Monde a agi ainsi pour limiter la casse. « Par chance, les équipes informatiques étaient présentes le soir de l'attaque. Elles ont pu déconnecter les machines infectées. Cela été salutaire. Selon l'Agence nationale de la sécurité des systèmes d'information (Anssi), l'objectif était de détruire notre société », précise Yves Bigot, le directeur général de la chaîne.

L'urgence passée, il faut rapidement faire appel à des professionnels expérimentés dans la neutralisation des attaques informatiques. L'Anssi dispose sur son site internet d'une liste de prestataires disposant du label CERT-FR (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques). Certains s'engagent à intervenir en moins de quatre heures.

3 PORTER PLAINTE ET ESTIMER LES PRÉJUDICES

« Les entreprises hésitent à porter plainte, car elles craignent que cela nuise à leur réputation. Or, sans cela, on ne peut traiter policièrement et judiciairement une affaire », déplore le « préfet cyber ». Il faut donc déposer plainte au commissariat ou à la brigade de gendarmerie locale. Certains disposent d'un investigateur en cybercriminalité qui fournira les conseils d'urgence. La seconde étape est de se rapprocher d'interlocuteurs techniques qui pourront apporter leur expertise.

Les entreprises en région parisienne doivent solliciter la Befti, la brigade d'enquête sur les fraudes aux technologies de l'information. Cette unité spécialisée conseille les entreprises victimes d'intrusion informatique ou de détournement de fonds… Les entreprises en province auront accès à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Il faut venir avec le maximum d'éléments qui vont aider les enquêteurs : le journal des connexions, la configuration des machines, les disques durs des machines infectées… « Il faut aussi estimer les préjudices subis sur la base d'éléments concrets. Cela permettra de présenter un dossier solide auprès du procureur de la République. C'est sur ce dossier qu'il décidera des suites à donner à l'enquête », explique le colonel Freyssinet, spécialisé dans la lutte contre les cybermenaces au ministère de l'Intérieur.

4 RECONSTRUIRE LA SÉCURITÉ INFORMATIQUE

Il faut agir sur les conséquences de l'attaque. Le grand industriel européen qui craignait qu'un pirate ait eu accès au code source de son outil de gestion à distance des infrastructures de ses clients n'a pas tergiversé. « Le code du produit a été totalement revu afin d'éviter la création d'un backdoor [une porte dérobée, ndlr] exploitable par les pirates. Nous avons également informé nos clients de l'attaque subie », confie-t-il. Après son attaque, TV5 Monde a remis à plat sa sécurité informatique. Elle a remplacé le matériel technique compromis et déployé des nouveaux équipements de sécurité.

Les 400 salariés suivent une formation pour apprendre les gestes de base dans ce domaine. La chaîne a imposé des mesures drastiques : suppression du Wi-Fi, interdiction de connecter des équipements électroniques personnels (tablette, smartphone…) aux ordinateurs de bureau, passage des clés USB au sas de décontamination… Soit, au total, une facture de 5 millions d'euros.

Pour soigner les machines infectées, l'Anssi préconise de réinstaller entièrement le système d'exploitation et d'appliquer tous les correctifs de sécurité avant de la reconnecter. Elle recommande de modifier les mots de passe de tous les comptes de l'entreprise sous peine de revoir débarquer le pirate informatique. L'agence incite également les entreprises victimes à communiquer avec leurs pairs. « Généralement, les pirates s'attaquent à plusieurs entreprises d'un même secteur, en réutilisant les mêmes techniques. En partageant son expérience, on renforce la sécurité collective », explique Guillaume Poupard, le directeur général de l'Anssi.

La messagerie sous écoute

Dans la panique, les membres de la cellule de crise communiquent par e-mails et s'échangent des fichiers via le réseau de l'entreprise. Grave erreur. Il y a de grandes chances pour que ces systèmes soient compromis et sous écoute. Le conseil pour communiquer en toute discrétion : ouvrir temporairement des comptes de messagerie à partir de services web. Les échanges informatiques doivent également se faire par l'intermédiaire d'un réseau de secours indépendant de celui de l'entreprise afin de garantir leur confidentialité.

Denis JACOPINI est Expert en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://www.usine-digitale.fr/article/comment-reagir-a-une-cyberattaque.N354821
Par HASSAN MEDDAH