Microsoft foutu dehors par Pékin sur des doutes d’espionnage…

	Microsoft foutu dehors par Pékin sur des doutes d’espionnage…

C’est la première fois que les autorités chinoises pointent officiellement du doigt l’entreprise depuis le lancement d’une enquête antimonopole le mois dernier.

L’étau chinois se resserre lentement mais sûrement sur Microsoft. Après Google, et Qualcomm, spécialiste de la technologie 4G, c’est l’entreprise fondée par Bill Gates qui se retrouve dans le viseur de Pékin. Un haut responsable des autorités de la concurrence chinoise a accusé le géant américain de l’informatique de manque de «transparence» dans ses ventes de logiciels.
Zhang Mao, le chef de la puissante administration d’État de l’industrie et du commerce (SAIC) exige que Microsoft fasse toute la lumière sur ses chiffres de ventes de logiciel «Media Player» et son moteur de recherche. C’est la première fois que les autorités pointent officiellement du doigt l’entreprise depuis le lancement d’une enquête antimonopole le mois dernier. Ces dernières semaines, les enquêteurs ont opéré des raids surprises dans sept bureaux à travers le pays et devraient délivrer leur verdict, «en temps voulu». Avec, à la clé, une possible amende pesant 10 % du revenu chinois de l’entreprise.
Microsoft est pris en otage dans la « cyberguerre » entre Washington et Pékin suite à l’affaire Snowden
Microsoft subit une offensive tous azimuts dans l’empire du Milieu, puisque les autorités viennent d’annoncer le lancement d’un système d’exploitation visant à remplacer Windows en octobre. Depuis le mois de mai, la dernière version du logiciel, Windows 8, est bannie de toutes les administrations publiques, au nom de la lutte contre l’espionnage. Microsoft est pris en otage dans la «cyberguerre» entre Washington et Pékin suite à l’affaire Snowden.
L’interdiction de Windows 8 a été annoncée quelques jours après la mise en cause de cinq militaires chinois pour espionnage par la justice américaine, le 19 mai dernier. «En représailles, la Chine renforce ses contrôles sur les firmes étrangères dans le secteur technologique et va donner la préférence aux entreprises locales dans tous les domaines où il y a des données sensibles», analyse Ian Bremmer, président du cabinet de conseil américain Eurasia Group.
Après la mise au ban de Google, qui avait refusé de collaborer avec le régime en matière de cybersurveillance des citoyens, Microsoft craint à son tour d’être éclipsé du marché chinois. Le moteur de recherche de Google est depuis victime de multiples obstacles techniques ainsi que d’attaques qui ralentissent son fonctionnement et sa part de marché a fondu.
Parallèlement à Microsoft, l’entreprise californienne Qualcomm est également visée par une enquête de l’antitrust. Soupçonné d’imposer des prix trop élevés, son président Derek Aberle a promis des «améliorations», après avoir rencontré les autorités.
Pékin examine cette semaine une nouvelle loi visant à renforcer son arsenal juridique contre le cyberespionnage. Un impératif de sécurité nationale qui fleure le protectionnisme économique et dont les entreprises locales doivent profiter. «La priorité est de développer notre propre système d’exploitation pour mettre nos informations à l’abri.»
Côté industriel, «l’ambition est de briser le monopole étranger en devenant le quatrième système d’opération aux côtés de ceux d’Apple, Google et Microsoft», explique Ni Guangnan, membre de l’Académie chinoise d’ingénierie, dans le Global Times, quotidien proche du Parti.
Ces annonces laissent sceptiques certains experts et de nombreux internautes chinois qui doutent des capacités du secteur public à accoucher d’un système fiable. «Est-on en Corée du Nord?» lance provocateur l’un d’eux sur Weibo.
Au début des années 2000, le régime avait lancé son propre «moteur de recherche du peuple». Un échec retentissant, mais le rival privé Baidu, moteur de recherche chinois, avait lui profité pleinement de l’éclipse de Google pour contrôler aujourd’hui plus de 70 % du plus grand marché du monde en ligne. C’est aujourd’hui le site le plus consulté de Chine.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lefigaro.fr/secteur/high-tech/2014/08/26/01007-20140826ARTFIG00374-pekin-pousse-microsoft-vers-la-sortie.php

---

Attaque informatique : JPMorgan et plusieurs autres banques ciblées

Attaque informatique : JPMorgan et plusieurs autres banques ciblées

Si au cours des derniers mois, les pirates semblaient avoir comme cibles de prédilection les entreprises des secteurs de la distribution et de la santé, ils n'en oublieraient pas pour autant les acteurs de la finance.

Selon le Wall Street Journal, le FBI enquêterait sur une série d'attaques informatiques visant des établissements financiers, dont JPMorgan, la plus grande banque des Etats-Unis et la sixième dans le monde (source : Forbes).

Une enquête aurait été ouverte début août. Des données auraient en effet été dérobées à la banque par l'intermédiaire de code malveillant injecté par des hackers dans l'ordinateur personnel d'un employé de JPMorgan.

Mais l'entreprise ne serait pas la seule ciblée. Selon des sources proches de l'enquête, deux à cinq autres banques pourraient elles aussi avoir été attaquées. Les établissements bancaires font des proies de choix pour les cybercriminels. Plusieurs d'entre eux ont déjà été visés cette année, dont Wells Fargo, J.P. Morgan Chase, Bank of America, Citigroup, et HSBC.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/jpmorgan-et-plusieurs-autres-banques-attaquees-39805373.htm

---

La dangereuse faille informatique Heartbleed constitue toujours une menace

La dangereuse faille informatique Heartbleed constitue toujours une menace

Près de cinq mois après la révélation de la vulnérabilité Heartbleed, IBM dresse un premier bilan, avec le rapport trimestriel de sa division X-Force, en s'appuyant sur les informations retirées des infrastructures des clients de ses services de sécurité managés. Et celui-ci s'avère contrasté.

La bonne nouvelle, c'est que l'intérêt malveillant pour la vulnérabilité semble s'être sensiblement tassé : si IBM a enregistré jusqu'à plus de 300 000 attaques par jour exploitant Heartbleed le 15 avril dernier, le chiffre est rapidement retombé, à quelques centaines d'incidents par jour fin avril. L'effet de grandes entreprises qui ont été capables de mettre rapidement en œuvre des contre-mesures. De quoi pousser les attaquants à déplacer leurs efforts sur d'autres vulnérabilités. Pour autant, l'activité malveillante liée à Heartbleed se maintient, explique IBM, estimant qu'environ « 50 % des serveurs potentiellement vulnérables ont été laissés sans correctif ». De quoi faire, pour le groupe, de la vulnérabilité « une menace continue et critique ».
Mais pour IBM, le plus important est peut-être à chercher du côté de la gestion de la réaction : « disposer d'un plan de réaction aux incidents – et d'une base de données à jour des actifs – s'est avéré absolument critique pour réduire l'exposition au risque. » En outre, selon le groupe, si les pare-feux ont pu rapidement offrir une protection pour les systèmes concernés, les dispositifs de détection et de prévention des intrusions ont pu « fournir une protection encore plus importante en bloquant les attaques au niveau des paquets ». D'autant plus que les attaquants semblent avoir privilégié la carte de l'exploitation distribuée de la vulnérabilité Heartbleed, rendant plus difficile la protection par des pare-feux.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

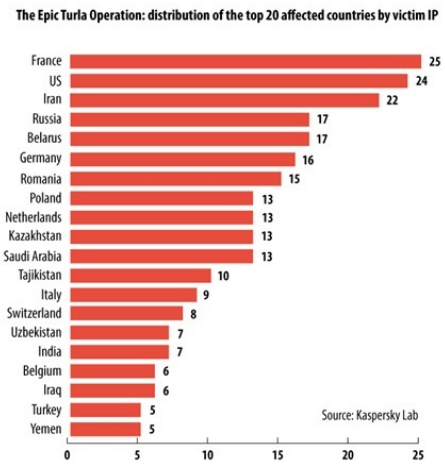
Source :
http://www.lemagit.fr/actualites/2240227500/Heartbleed-constitue-toujours-une-menace?asrc=EM_MDN_33243175&utm_medium=EM&utm_source=MDN&utm_campaign=20140827_L%27essentiel%20IT%20:%20Premi%e8re%20politique%20globale%20de%20s%e9curit%e9%20en%20France%20-%20VMWare%20se%20convertit%20aux%20appli_

La France en première ligne de cyber-espionnage face à Epic Turla

La France en première ligne de cyber-espionnage face à Epic Turla

Selon le centre de recherche de Kasperky, notre pays est le plus touché par une attaque de cyber-espionnage connue sous le nom d'Epic Turla.
Selon Kaspersky Labs, la France est le pays le plus visé par une attaque de cyber-espionnage référencée sous le nom d'Epic Turla ou UroBuros, ou encore snake, pour d'autres éditeurs de logiciels de sécurité. La plupart des cibles sont des entités gouvernementales ou des ambassades sises en Europe ou au Moyen-Orient.

Une APT assez classique
Techniquement, l'attaque suit le schema classique d'une APT (Advanced Persistent Threat) avec hameçonnage par du spear phishing, l'utilisation d'exploits zero day, du social engineering et du waterholing par des sites infectés. Une fois dans la place, Epic se connecte au serveur de command and control et envoie les informations sur le système de l'utilisateur. Le système est ensuite compromis avec des outils spécifiques, des fichiers préconfigurés avec des commandes. L'attaque se déplace ensuite latéralement pour obtenir les bonnes accréditations et prendre la main pour soutirer les informations voulues. Selon le laboratoire, l'attaque est toujours en cours.
Tous les détails techniques ici :
https://securelist.com/analysis/publications/65545/the-epic-turla-operation/



Les statistiques d'infection par Epic Turla

par Bertrand Garé, le 22 août 2014 14:42

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.linformaticien.com/actualites/id/33931/cyber-espionnage-la-france-en-premiere-ligne-face-a-epic-turla.aspx

---

Orange piraté : Le rapport de la Cnil et les sanctions à l'encontre de l'opérateur historique

Orange piraté : Le rapport de la Cnil et les sanctions à l'encontre de l'opérateur historique

L'autorité chargée de la protection des données personnelles publie un avertissement sans conséquences à l'encontre d'Orange. La Cnil critique l'opérateur pour avoir permis à des pirates de faire la copie des données personnelles concernant 1,3 million de clients.

La Cnil adresse un avertissement, sans sanction financière, à l'encontre d'Orange. L'autorité indique qu'en avril dernier, l'opérateur avait permis d'avoir accès aux noms, prénoms, date de naissance, adresse électronique et numéro de téléphone fixe ou mobile de 1,3 million de clients.
Pour Orange, la plateforme visée servait en particulier pour ses campagnes commerciales, notamment pour l'envoi de courriers électroniques et de SMS. Après que la société a admis ces dysfonctionnements, la Cnil a mené une enquête auprès de l'opérateur. Elle livre désormais ses conclusions.
Elle estime que les dysfonctionnements ayant engendré la faille de sécurité ont certes depuis été corrigés. « Toutefois, plusieurs lacunes en termes de sécurité des données ont été identifiées et ont justifié l'engagement d'une procédure de sanction », précise-t-elle. La Cnil reproche par exemple à Orange de n'avoir pas fait réaliser d'audit de sécurité avant d'utiliser la plateforme technique de son prestataire.
Second point à la charge d'Orange, l'organisme rapporte dans une note que la société a envoyé de manière non sécurisée à ses prestataires les mises à jour de ses fichiers clients et « qu'aucune clause de sécurité et de confidentialité des données n'avait été imposée à son prestataire ». La sécurité des données n'était donc pas assurée dans l'ensemble de la chaîne, ce que reproche la Cnil en émettant cet avis à l'encontre d'Orange.

Le rapport de la CNIL du 7/08/2014

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://pro.clubic.com/legislation-loi-internet/cnil/actualite-722731-orange-recoit-carton-jaune-cnil.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_26/08/2014&partner=-&svc_position=64542616S&svc_misc=-&crmID=639453874_64542616S&estat_url=http%3A%2F%2Fpro.clubic.com%2Flegislation-loi-internet%2Fcnil%2Factualite-722731-orange-recoit-carton-jaune-cnil.html

---

La Xbox Live et le Vatican attaqués par les pirates informatiques de Lizard Squad

La Xbox Live et le Vatican attaqués par les pirates informatiques de Lizard Squad

Probablement l'œuvre de mauvais farceurs, les attaques répétées sur les réseaux de jeux en ligne continuent. Même le Saint-Siège se retrouve en ligne de mire des hackers.

Jusqu'où iront les pirates de « Lizard Squad » ? Après avoir attaqué, durant ce week-end, un certain nombre de services de jeux en ligne comme Sony Online, Blizzard et Battle.net, le groupe de pirates a changé de cible et pris en ligne de mire le site du Vatican.
Il a revendiqué une attaque par déni de service distribué (DDoS) il y a une dizaine d'heures. Comble du mauvais goût, le groupe fait référence, dans son message Twitter, à l'idéologie radicale de l'Etat Islamique. Ainsi, il estime que « tous les non-musulmans doivent mourir » (« all kuffar shall die »), ajoutant une série de mots-clés comme #ISIS, #Jihad, #ISIL et #IS. Visiblement, l'opération a été couronnée de succès, car, d'après plusieurs témoignages sur Twitter, le site du Saint-Siège était déconnecté ce matin.
Il ne l'est plus à l'heure actuelle.

Article de Gilbert Kallenborn01netle 25/08/14 à 17h34

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.01net.com/editorial/625416/apres-sony-les-pirates-de-lizard-squad-attaquent-xbox-live-et-le-vatican/#?xtor=EPR-1-NL-01net-Actus-20140825

Les fraudes bancaires touchent plus d'une entreprise sur six

Un peu moins de 20% des entreprises victimes d'une fraude bancaire.

Les entreprises sont de plus en plus les cibles d'escrocs bancaires. Avec un préjudice estimé à ce jour à 250 millions d'euros, les pouvoirs publics et les organisations professionnelles tirent le signal d'alarme.

1 entreprise sur 6 affirme avoir été victime d'au moins une tentative de fraude en 2013. Ce chiffre est le résultat d'une étude interne au secteur bancaire publiée aujourd'hui par . Les grandes PME sont les cibles préférées des escrocs. En effet, une entreprise sur deux qui compte entre 500 et 1.000 salariés et qui a un chiffre d'affaires supérieur à 75 millions d'euros a déclaré avoir été la cible d'une tentative de fraude. Un chiffre qui retombe entre 10 et 15% pour les plus petites entreprises. Autre phénomène: si ces fraudes touchent tous les secteurs d'activité sans exception, elles visent très fréquemment le commerce, en raison du grand nombre de transactions réalisées dans ce secteur.

Trois types de fraude font fureur

Les fraudes aux virements internationaux peuvent se présenter sous plusieurs formes, comme l'indique une note d'information publiée par le Service Régional de Police Judiciaire de Clermont-Ferrand (SRPJ). La première d'entre elles est appelée «escroquerie à la nigériane», en raison du lieu d'agissement des escrocs, qui opèrent depuis la côte ouest africaine. Ceux-ci détournent des transactions entre les entreprises françaises et leurs fournisseurs asiatiques. Leur méthode: envoyer des courriels aux entreprises en se faisant passer pour le fournisseur. Les fraudeurs parlent alors de «dysfonctionnements bancaires» et souhaitent que le prochain virement soit réalisé sur un compte «plus sécurisé», qui va donc tout droit dans leur poche.

Une autre technique de fraude est celle de l'«escroquerie au président» ou arnaque «au faux patron». Selon le SRPJ de Clermont, cette méthode est «la plus redoutable». Les escrocs exigent des virements des responsables d'une entreprise, en se faisant passer pour leur PDG. Comme le décrit le SRPJ, ce genre d'escroquerie nécessite «une autorité naturelle, un certain aplomb et, il faut bien le reconnaître, un don pour la comédie». Un don qui passe par plusieurs ruses. Selon Les Echos, la première est d'insister sur le caractère urgent de la requête dans le cas d'un futur contrôle fiscal, d'une OPA ou autres. Les escrocs ne manquent pas d'imagination. La seconde, dite de «l'ingénierie sociale», est d'effectuer une collecte d'informations sur l'entreprise via les réseaux sociaux pour en adopter les codes. Et s'ajoute à cette pointe de réalisme une touche de flatterie. Comme l'indique le SRPJ, la supercherie aura plus de chance de fonctionner si le comptable de l'entreprise se sent «flatté d'être dans la confidence du patron». Cette méthode qui ne fait toutefois que peu de victimes est de loin la plus redoutable car elle émane de bandes parfaitement organisées. Pour les petites entreprises, les méthodes de fraude les plus répandues restent toutefois celles liées aux actions du quotidien, comme la fraude à la carte bancaire volée ou usurpée.

Enfin la dernière ruse à la mode est celle qui profite de la norme Sepa, l'espace de paiement unique européen. Les escrocs se font alors passer pour le responsable informatique de la banque qui gère les comptes de l'entreprise ciblée. Ils arrivent alors à convaincre l'interlocuteur de la société d'effectuer une série de tests et, à distance, ils prennent le contrôle de l'ordinateur et effectuent des virements directement sur leur compte en banque. Cette technique est rendue possible par le système Sepa grâce auquel la banque n'a plus à se soucier de l'accord du client avant d'effectuer un virement. Celui-ci peut toutefois contester l'opération dans le cas où il constate un virement anormal.

60% des entreprises sont satisfaites de la réaction de leur banque

Même si ces trois techniques sont les plus répandues, les fraudeurs ne manquent pas d'imagination pour escroquer les entreprises qui, dans bien des cas, ne pourront pas se faire rembourser les montants dérobés. Une fois le virement réalisé, elles peuvent en effet contacter leur banque, mais les établissements ne peuvent pas s'immiscer dans les ordres de paiement. Toutefois, les entreprises sont majoritairement satisfaites de la réaction de leur banque, à hauteur de 60%. Un pourcentage qui diminue pour les petites entreprises de moins de 20 salariés mais qui passe à 80% pour les grandes entreprises. Un chiffre qui dépend également du type de banque choisi par l'entreprise, les taux de satisfaction étant en effet plus élevés pour ceux qui optent pour une banque commerciale par rapport à une banque mutualiste.

Pour lutter contre ces fraudes, la Fédération bancaire Française (FBF) a annoncé qu'elle rencontrerait prochainement, avec des représentants de la police et de la justice, ses homologues chinois, pays d'où proviennent un grand nombre de fraudes. Pour le moment, elle a fait savoir dans une vidéo que «plusieurs centaines de procédures sont en cours au sein de la police judiciaire» pour un montant des préjudices qui se chiffre à «plus de 250 millions d'euros».

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.lefigaro.fr/conjoncture/2014/08/22/20002-20140822ARTFIG00233-les-fraudes-bancaires-touchent-plus-d-une-entreprise-sur-six.php

---

Alerte : Arnaque par téléphone d'un agent Microsoft

Alerte : Arnaque par téléphone d'un agent Microsoft

Depuis quelques temps, une arnaque au cours de laquelle un agent vous appelle afin de résoudre avec vous vos soucis d'informatique prend de l'ampleur à la Police.

Le principe?
De nombreuses personnes témoignent à présent du même mode opératoire : vous êtes appelé par un opérateur à l'accent anglophone, se faisant passer pour un employé de « Microsoft », ou bien de son service client « Customer Care Center ».
Selon cet opérateur, des messages d'erreur leur seraient parvenus via votre ordinateur, et pour y remédier, il vous suffit d'accéder, avec un code, à une page web « infosis.net » ou bien « logme120.com ». Ces noms changent régulièrement, c'est pourquoi c'est essentiellement le mode opératoire qui doit vous alerter.
L'agent vous demande alors d'installer un logiciel pour voir votre écran et commencer un tutoriel afin que vous puissiez résoudre ensemble votre problème informatique. Vous l'avez compris: ce programme n'est autre qu'un espion informatique chargé de s'introduire dans des relations bancaires ou des données de cartes de crédit.
Que faire?
Important :La société Microsoft a déjà réagi dans de nombreux pays, en précisant qu'elle ne contacte jamais les usagers, sans que ceux-ci ne l'aient préalablement sollicitée. De plus, l'aide de spécialistes de dépannage Microsoft ne vous est jamais facturée ainsi en ligne !
Afin de protéger un ordinateur contre diverses formes d'escroquerie, il est conseillé d'utiliser un outil de suppression de logiciels espions fiables.
Si vous n'avez pas reçu un faux appel de téléphone mais cela ne signifie pas que vous êtes protégé contre d'autres types d'escroquerie, c'est pourquoi il est conseillé d'utiliser un programme de prévention de spyware.
Dans le doute, passez en revue tous les programmes de votre ordinateur en vérifiant la fonctionnalité de chacun d'entre eux, de détecter les éventuels programmes « espions » afin de les supprimer.
Vous pouvez également signaler ces messages à la police judiciaire via Pharos : www.internet-signalement.gouv.fr
N'oubliez pas le numéro « Info Escroqueries » 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile)
! SOYEZ VIGILANT !

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Arnaque-via-un-appel-d-un-agent-Microsoft

L’utilisation juridique des documents numériques – Article de presse dans L’Echo du mardi du 12 08 2014


Consultants

Consultants

Nos experts ont la parole

Utilisation juridique des documents numériques

L’utilisation juridique des documents numériques

Article de presse dans L’Echo du mardi du 12/08/2014

L’utilisation juridique des documents numériques

«Dans le doute, après avoir numérisé un document officiel, vous avez probablement préféré conserver l’original dans son format matériel (bien souvent papier).

A l’heure de la dématérialisation à outrance (remplacement dans une entreprise ou une organisation de ses supports d’informations matériels, souvent en papier, par des fichiers informatiques et des ordinateurs, jusqu’à la création de « bureau sans papier » ou « zéro papier » quand la substitution est complète), il est temps de se poser des questions sur la valeur juridique des documents informatiques en cas de contestation ou de litige. Le traitement de documents dématérialisés présente un certain nombre d’avantages significatifs.»

Télécharger l’article complet

Cet article vous à plu ? Laissez-nous un commentaire (notre source d’encouragements et de progrès)

4,5 millions de données médicales dérobées aux Etats-Unis – Un vol de données de plus…

Community Health Systems, un spécialiste américain de la gestion des hôpitaux, a reconnu avoir été victime d’une attaque informatique entre avril et juin 2014. Résultats : 4,5 millions de données personnelles ont été dérobées. Un vol de données de plus…