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

	Kaspersky annonce être victime d’une Cyberattaque

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

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

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

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

Les hébergeurs Français inquiets du projet de loi renseignement | Le Net Expert Informatique

Le projet de loi sur le renseignement, adopté par le Sénat mardi 9 juin, pourrait mettre en péril la compétitivité des hébergeurs français, alors que le marché est en pleine croissance.

Le Sénat à voté mardi 9 juin, le projet de loi sur le renseignement, présenté par le gouvernement au nom de la lutte contre le terrorisme. 251 sénateurs, en majorité à droite mais aussi à gauche, ont voté pour, 68 contre, et les autres se sont abstenus. Cette loi controversée permettrait à l'État d'« imposer aux opérateurs la mise en œuvre sur leurs réseaux d'un dispositif destiné à détecter une menace terroriste sur la base de traitements automatisés » (Art. L. 851-4).
Ces « boites noires », comme les appellent les opposants, filtreront les données qui circulent à l'aide d'un algorithme validé par une commission composée de parlementaires, de juristes et d'experts. Les services de renseignement collecteront alors des métadonnées donnant la possibilité de traquer toutes les activités de n'importe quel internaute.

L'objectif affiché par le gouvernement est de pouvoir détecter plus efficacement toute menace terroriste. Les services de renseignement pourront par exemple détecter les connexions à un site internet terroriste, ou capter les communications vers des pays jugés sensibles.
Personne ne conteste le besoin d'une surveillance accrue des réseaux. Mais cette loi ne fait cependant pas l'unanimité. Les premiers à se sentir lésés sont les hébergeurs français. Après avoir attiré, pendant tout ce temps, des clients en leur expliquant qu'en France leurs données resteraient confidentielles et ne risquaient pas d'être interceptées, voilà que l'État s'octroie un libre accès à leurs réseaux et à tout ce qui y circule.
Certains menacent maintenant, dans un communiqué destiné au Premier ministre, de délocaliser leurs infrastructures dans des pays moins intrusifs, en amenant avec eux emplois et vecteurs de croissance économique, dénonçant les risques que cette loi peut apporter à leur industrie.

Vers des délocalisations massives ?
Outre le scepticisme autour de la capacité de l'État à traiter et analyser une quantité massive de données, le débat sur le caractère liberticide de cette loi et les risques d'abus, de dérives et de fuites qui pourrait avoir lieu, les craintes qu'ont les hébergeurs concernent en grande partie la réaction qu'auront leurs clients face à ces mesures.
En effet, ils jugent que « les entreprises et les particuliers choisissent un hébergeur sur des critères de confiance et de transparence qu'il ne sera plus possible de respecter ». Un grand travail a été fait pour rassurer le grand public, ainsi que les entreprises, sur la confidentialité des données hébergées dans des datacenters français, car il s'agit bien ici d'un avantage compétitif primordial qu'ont les hébergeurs locaux face aux grands acteurs américains du cloud, qui est menacé aujourd'hui.
Dans leur communiqué, ces six hébergeurs français affirment que 30 à 40 % de leurs clients sont étrangers et ont choisi la France pour l'importance accordée à la protection des données. Ils rappellent aussi qu' « il leur faudra entre 10 minutes et quelques jours pour quitter leur hébergeur français » et migrer dans un pays où les garanties de confidentialité pour les clients seront plus importantes.
Les hébergeurs français seraient donc face au même phénomène qu'ont connu leurs homologues américains lors de la mise en place aux États-Unis du Patriot Act. Face à la comparaison inévitable faite entre ces deux lois, Matignon se défend en rappelant que le gouvernement ne met pas en place un dispositif de surveillance massif des données sur Internet ou des conversations privées comme c'est le cas aux États-Unis, et assure vouloir éviter tout abus ou dérive en créant une commission de contrôle indépendante, appelée CNTCR, qui devra toujours donner son avis préalable à la mise en œuvre de la technique de renseignement et pourra exercer un contrôle a posteriori.
Nous parlons bien d'un marché avec une croissance à deux chiffres (+20 % en 2014) qui risque de prendre du plomb dans l'aile. En plus des hébergeurs français qui risquent de retirer certains investissements de France, j'imagine facilement de grands acteurs européens ou mondiaux choisir de s'implanter ailleurs qu'en France par souci de confidentialité des données.
On pourrait penser à terme que les petits hébergeurs seraient bloqués dans une situation où leurs clients voudraient migrer, mais en réalité ils pourront toujours louer des mètres carrés à l'étranger en fonction des demandes.
En résumé, les pure players pourront plus ou moins s'adapter face à un éventuel exode de leurs clients. Le grand perdant de cette histoire semble être donc pour moi être l'économie numérique française.

Le temps de l'optimisation légal
Autour de toutes ces discussions, je vois bien la confidentialité d'accès aux données représenter une nouvelle opportunité commerciale pour les hébergeurs qui proposeront à leurs clients de géolocaliser leurs données en fonction de la législation locale. Ils vont devoir proposer la solution qui garantit au mieux la confidentialité d'accès aux données pour gagner quelques affaires.
Les acteurs européens par exemple, donnent depuis toujours la possibilité à leurs clients français et européens de choisir dans quels pays héberger leurs données avec des datacenters répartis dans toute l'Europe afin d'optimiser au mieux leurs besoins en confidentialité, sécurité et respect des règles et lois locales.
En somme, cette loi pénalise les acteurs franco-français en réduisant leurs marges de manœuvre du fait des contraintes imposées par l'État et met en péril leur compétitivité en tant qu'acteur national en les mettant au même niveau que les autres acteurs internationaux.
Il serait peut-être plus judicieux aujourd'hui d'établir un partenariat gagnant-gagnant entre l'État français et les hébergeurs locaux qui se disent tous prêts à collaborer pour assurer la sécurité sur le territoire, en mettant en place une infrastructure règlementaire moins disproportionnée et plus ciblée sur les objectifs de l'État en évitant de la même manière de mettre en péril leur avantage sur le sol français.

Source : http://www.lesechos.fr/idees-debats/cercle/cercle-133763-loi-sur-le-renseignement-quel-avenir-pour-les-hebergeurs-1126557.php
Par France Weill / Director IT & Cloud Services Channels Europe – COLT

Interdictions de stade : le PSG à nouveau épinglé par la CNIL | Le Net Expert Informatique

Interdictions de stade : le PSG à nouveau épinglé par la CNIL

Le Paris-Saint-Germain (PSG) est à nouveau épinglé dans le traitement de certains de ses supporteurs. La Commission nationale de l'informatique et des libertés (CNIL) a publié, mercredi 10 juin, un communiqué officiel pour signifier une nouvelle mise en demeure à l'encontre du club de football de la capitale. Il s'agit de la deuxième procédure de ce type en deux ans.

La Commission, chargée de sanctionner les manquements à la loi informatique et libertés, reproche aux dirigeants du club francilien de ne pas s'être « borné à gérer la liste des interdits de stade à l'intérieur du cadre légal, mais d'avoir décidé d'exclure les personnes faisant l'objet de ces mesures, après l'expiration de celles-ci, pendant une durée au moins équivalente ».

Pas de sanctions pour l'instant

La CNIL pointe notamment l'interdiction de stades de certains supporteurs parisiens, ainsi que la conservation de données personnelles au-delà du délai de l'interdiction. Or, seuls le préfet ou le juge peuvent prendre, ou étendre, des mesures d'interdiction de stade.

Dans son communiqué, la CNIL rappelle que cette mise en demeure n'est pas synonyme de sanction. « Aucune suite ne sera donnée à cette procédure si la société [le PSG] se conforme à la loi dans le délai imparti d'un mois », peut-on lire. Dans le cas contraire, l'organisme de défense des libertés individuelles et publiques pourrait nommer un rapporteur qui sera chargé de proposer une sanction à l'égard du champion de France en titre.

En janvier 2014, la CNIL avait autorisé le club dirigé par Nasser Al-Khelaïfi à créer un fichier afin de lister les supporteurs exclus du stade par les autorités selon des motifs bien précis comme « l'existence d'un impayé, le non-respect des règles de billetterie, l'activité commerciale dans l'enceinte sportive en violation des conditions générales de ventes, etc. », précise le communiqué.

.

Source : http://www.lemonde.fr/ligue-1/article/2015/06/10/interdictions-de-stade-le-psg-a-nouveau-epingle-par-la-cnil_4651214_1616940.html
Par Kozi Pastakia

Conférence Octopus 2015 sur la cybercriminalité : Le

Conseil de l’Europe se penche sur l’accès de la justice aux données | Le Net Expert Informatique

Conférence Octopus 2015 sur la cybercriminalité : Le Conseil de l’Europe se penche sur l’accès de la justice aux données

Comment assurer l'accès aux données, enquêter efficacement sur les infractions commises par le biais d'Internet et engager des poursuites à l'encontre de leurs auteurs lorsque les éléments de preuve se trouvent dans le « cloud » ? Du 17 au 19 juin, le Conseil de l'Europe réunira des experts du monde entier, des responsables gouvernementaux, des fonctionnaires de police et des professionnels d'internet en vue de renforcer la coopération internationale pour lutter contre la cybercriminalité.

Cette conférence portera également sur les défis liés à la protection des enfants contre leur sollicitation en ligne à des fins sexuelles (« grooming ») et sur la radicalisation sur internet.
Les 300 participants examineront, dans le cadre d'une série d'ateliers partiellement ouverts à la presse, les questions suivantes :

– Le renforcement des capacités en matière de cybercriminalité: bonnes pratiques et futurs programmes (*)
– Les preuves électroniques : accès de la justice pénale aux données
– Les victimes de la cybercriminalité: qui s'en soucie ? (*)
– La législation en matière de cybercriminalité et la mise en œuvre de la Convention de Budapest
– La coopération internationale: améliorer le fonctionnement des points de contact accessibles 24 heures sur 24 et sept jours sur sept
– Les modes opératoires normalisés pour le traitement des preuves électroniques
– Les politiques, activités et initiatives adoptées en matière de cybercriminalité par les organisations internationales et les organisations du secteur privé
– La radicalisation sur internet : le point de vue de la justice pénale
– La protection des enfants contre la violence sexuelle en ligne
Les discussions s'appuieront notamment sur un rapport publié récemment et qui se penche sur les difficultés des autorités pénales à obtenir des preuves électroniques.
La conférence sera ouverte notamment par le Secrétaire Général du Conseil de l'Europe, Thorbjørn Jagland, la Représentante Spéciale du Secrétaire Général des Nations Unies sur la violence à l'encontre des enfants, Marta Santos Pais, et le Préfet chargé de la lutte contre les cybermenaces (France), Jean-Yves Latournerie.

Contexte
La Convention sur la cybercriminalité (« Convention de Budapest ») est le seul traité international juridiquement contraignant dans ce domaine. Elle a eu des répercussions dans le monde entier, où elle a conduit au renforcement et à une plus grande harmonisation de la législation relative à la cybercriminalité.
Depuis 2001, 66 pays ont signé, ratifié ou ont été invités à adhérer à la Convention. Plus de 120 pays coopèrent avec le Conseil de l'Europe au renforcement de leur législation et de leur capacité de lutte contre la cybercriminalité.
Programme – Fiche d'information – Encore plus d'information
Lien vers la retransmission (17 juin de 9h à 12h30 dans l'hémicycle et discussions en salle 1) #octopus2015

Trois tendances de sécurité

informatique à retenir pour 2015 | Le Net Expert Informatique

Trois tendances de sécurité informatique à retenir pour 2015

De nombreuses études placent la sécurité au cœur des TI pour 2015. Retrouvez ci-dessous trois tendances à retenir pour cette année :

Les attaques seront inévitables!
La question n'est plus de se demander si on sera attaqué et quand, mais plutôt de se préparer aux impacts d'une attaque, car cette attaque arrivera de toute façon.
Il faut donc avant tout s'assurer de minimiser les impacts d'une attaque potentielle et être proactif. Pour faire face à ces nombreuses tentatives d'attaques, les organisations doivent mettre en place un SOC (pour Security Operations Manager en anglais) ou du moins constituer des ressources qui vont gérer les opérations de sécurité quotidiennement et en temps réel.
Ces ressources vont être aidées dans leur travail par des outils innovateurs, mais doivent s'appuyer sur une expertise poussée pour analyser la masse d'activités. Par exemple, il ne suffit pas d'avoir un SIEM, mais il faut savoir le gérer.

Impartir sa sécurité
Puisque les attaques sont de plus en plus sophistiquées, l'expertise demandée par les ressources opérationnelles est de plus en plus poussée.
De plus, le temps à consacrer aux activités quotidiennes augmente de manière significative. Il est donc plus logique de faire appel à un fournisseur externe pour assurer ces activités afin que les ressources de l'organisation puissent se consacrer à la portion stratégique de la sécurité.
L'année 2015 verra de plus en plus d'impartition des opérations de sécurité sur la base du mode sécurité à la demande (SaaS).

Priorité à la sécurité applicative
Les réseaux sont de plus en plus protégés, car le cœur de l'infrastructure des organisations est sécurisé grâce aux nombreuses années d'évolution à ce sujet.
Par définition, les attaques ciblent toujours les points faibles d'une organisation et dans bien des cas, les applications Web sont les plus vulnérables : code non sécuritaire, failles non corrigées, mises à jour non appliquées… De nombreuses raisons peuvent s'ajouter à la liste.
Or, les applications Web représentent l'image de l'organisation et constituent bien souvent un accès privilégié aux données sensibles. La protection ciblée des applications Web sera mise de l'avant en 2015.

Source : http://www.directioninformatique.com/blogue/securite-informatique-trois-tendances-2015/36154
Par Matthieu Demoor

Démantèlement d’un réseau de cybercriminalité bancaire-Europol | Le Net Expert Informatique

Démantèlement d’un réseau de cybercriminalité bancaire-Europol

Europol a annoncé mercredi l'arrestation de 49 personnes soupçonnées d'appartenir à un groupe de cybercriminels actifs dans plusieurs pays d'Europe qui auraient dérobé plusieurs millions d'euros sur des comptes bancaires européens. Les présumés coupables agissaient en Belgique, Espagne, Italie, Pologne et Royaume-Uni ainsi qu'en Géorgie, précise dans un communiqué l'agence de police européenne basée à La Haye.

Des perquisitions ont eu lieu dans 58 lieux différents. Des ordinateurs, des téléphones et divers documents ont été saisis.

Les arrestations ont eu lieu mardi.
« Les enquêtes menées en parallèle ont révélé une fraude d'ampleur internationale d'un montant total de six millions d'euros accumulés sur une très courte période », lit-on dans le communiqué.
Les suspects, principalement originaires du Nigeria, du Cameroun et d'Espagne, transféraient leurs « profits illicites » hors de l'Union européenne via un réseau sophistiqué de transactions visant au blanchiment de l'argent, précise le communiqué d'Europol.

Lire la suite….

Source : http://www.boursorama.com/actualites/demantelement-d-un-reseau-de-cybercriminalite-bancaire-europol-ce20264eef326a073c96c7b8763fdd9a
Par Anthony Deutsch; Danielle Rouquié pour le service français

---

iOS 9 impose un code d'accès à 6 chiffres – Le Monde Informatique | Le Net Expert Informatique

iOS 9 impose un code d'accès à 6 chiffres

Sous iOS 9, le verrouillage des terminaux se fera avec un code à six chiffres. « En passant d'une clef de 4 chiffres à une clef de 6 chiffres, le nombre de combinaisons possibles passe de 10 000 à 1 million », a déclaré Apple.

Il faudra des mots de passe à six chiffres pour déverrouiller les appareils mobiles d'Apple qui tourneront sous le futur système d'exploitation IOS 9. Et si iOS 8 permet déjà aux utilisateurs de choisir un mot de passe de plus de quatre chiffres, dont des symboles et des lettres, ce mode de codage reste optionnel, ce qui ne sera pas le cas du futur iOS. En exigeant un code d'accès à six chiffres, Apple multiplie par 100 le nombre de combinaisons possibles, « rendant ainsi les terminaux beaucoup plus difficiles à pirater », comme on peut le lire sur le site du constructeur.
Ce saut à un code d'accès plus long risque de ne pas plaire non plus aux autorités américaines qui craignent que le renforcement des mesures de sécurité et du cryptage complique leurs investigations et rende plus difficile l'accès à des informations sensibles où le facteur temps est important, notamment dans le cadre de la lutte antiterroriste. Apple avait déjà renforcé le chiffrement d'iOS 8 afin de protéger les données les plus sensibles, et la firme de Cupertino avait mis en œuvre davantage de protections matérielles pour rendre l'accès aux terminaux plus difficile. Mais les experts en sécurité avaient estimé que l'utilisation d'un mot de passe à quatre chiffres ne suffisait probablement pas à protéger les données malgré les remparts mis en place par Apple. D'autant que, même si les utilisateurs savent qu'ils sont mieux protégés par des mots de passe plus longs, notamment parce que les séquences peuvent être plus personnalisées, ils choisissent rarement les mots de passe les plus compliqués.
Le changement de mots de passe concernera les terminaux équipés de l'ID Touch, le système d'empreintes digitales intégré aux dernières versions d'iPhone et d'iPad. L'ID Touch permet de se passer du déblocage, parfois fastidieux, du mobile avec le code à quatre chiffres, mais Apple oblige l'utilisateur à déverrouiller le mobile avec son code en cas de redémarrage du terminal. Les appareils iOS offrent d'autres fonctions de protection. Par exemple, si l'utilisateur tape un mauvais code de déverrouillage, l'iPhone peut être bloqué pendant une minute et plus, si plusieurs mots de passe sont saisis à la suite. Il est également possible de programmer l'effacement complet des données après 10 tentatives infructueuses. Le passage à un code à six chiffres pourrait grandement compliquer le travail des enquêtes judiciaires, surtout si l'appareil sous iOS 9 est configuré pour effacer les données après plusieurs tentatives erronées.

Source :
http://www.lemondeinformatique.fr/actualites/lire-ios-9-impose-un-code-d-acces-a-6-chiffres-61419.html
Par Jean Elyan

Cyberattaque de TV5 Monde : des pirates russes à la manœuvre ? | Le Net Expert Informatique

Cyberattaque de TV5 Monde : des pirates russes à la manœuvre ?

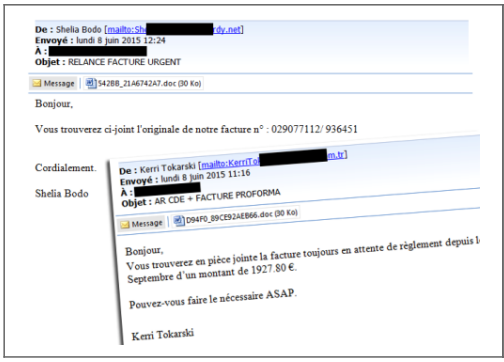
Cette cyberattaque avait été menée par des inconnus se réclamant de l'organisation Etat islamique. L'enquête se tourne désormais vers la Russie.

La piste jihadiste semble s'éloigner. L'enquête sur le piratage d'envergure subi le 8 avril par la chaîne de télévision francophone TV5 Monde s'oriente vers « un groupe de hackers russes », selon une source judiciaire, mardi 9 juin. Cette cyberattaque avait été menée par des inconnus se réclamant de l'organisation Etat islamique. Des messages de propagande jihadiste avaient été diffusés sur le site de la chaîne, ainsi que sur ses comptes Facebook et Twitter.
Le parquet antiterroriste avait alors ouvert une enquête préliminaire. Dans ce cadre, « les investigations conduisent à ce stade vers un groupe de hackers russes désignés sous le nom APT28 », d'après la même source. Ce groupe serait aussi parfois désigné sous les noms de « Pawn Storm » et « Sofacy group ».
Selon un rapport de la société américaine FireEye, APT28 est « un groupe aguerri de développeurs et d'opérateurs qui collectent des données relatives aux problématiques de défense et de géopolitique, des données qui ne pourraient être mises à profit que par un gouvernement ». L'ampleur des moyens déployés et le fait que cette cellule mène des attaques avec régularité depuis « au moins 2007 » témoignent, selon FireEye, du fait qu'elle est « soutenue par un gouvernement, plus précisément un gouvernement basé à Moscou ».

Un travail d'investigation sur les adresses IP
D'après ce même rapport, APT28 a notamment mené des attaques contre des ministères géorgiens. Selon un autre rapport de la société japonaise Trend Micro, Pawn Storm a aussi visé des dissidents russes ainsi que des intérêts américains, notamment des infrastructures militaires et des ambassades.
Les enquêteurs ont pu remonter la trace des hackers par « le travail d'investigation sur les adresses IP des ordinateurs d'où sont parties les attaques », selon une source proche du dossier. D'après les rapports des deux sociétés de cybersécurité, la cellule utilise des méthodes très sophistiquées, notamment pour recueillir mots de passe et codes d'accès. Ils enregistrent, par exemple, des noms de sites internet avec des adresses très proches de sites institutionnels reconnus afin de tromper leurs cibles.

Source : http://www.francetvinfo.fr/culture/tv/cyberattaque-de-tv5-monde-des-pirates-russes-a-la-manoeuvre_944085.html
Par Francetv info avec AFP

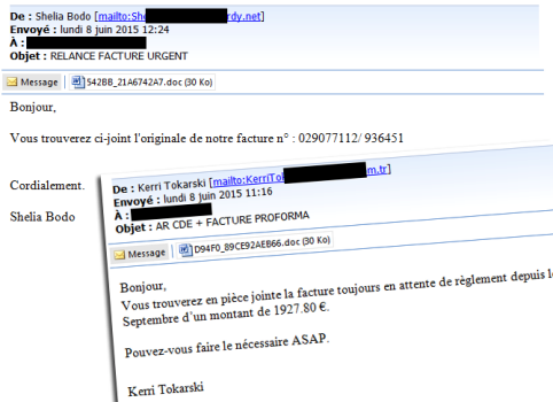
Alerte au Malware caché dans une pièce jointe Microsoft Office – Relayez l'info ! | Le Net Expert Informatique



Alerte au Malware caché dans une pièce jointe Microsoft Office – Relayez l'info !

En ce début de semaine, de nombreuses entreprises ont reçu un e-mail alarmant les informant qu'une facture impayée était à régler rapidement. Attention ! Le document Microsoft Office en pièce jointe dissimule un code d'attaque.

Vous trouverez ci-joint l'originale de notre facture », « vous trouverez en pièce jointe la facture toujours en attente de règlement », « un montant de 1927,80€ », etc.
Les e-mails, écrits dans un français très correct, sans faute d'orthographe, se ressemblent tous et contiennent un document Microsoft Word en pièce jointe. La notion d'urgence dans le ton employé incite à l'ouverture du document.
Une fois exécuté, le document Word téléchargera via un script en Visual Basic un code malveillant-relai Drixed.



Sa présence en mémoire compromet la sécurité du poste et de ses transactions, celui-ci pourra en effet évoluer de diverses manières : trojan bancaire, logiciel espion ou encore un cryptoware.
Vous l'aurez compris, il ne faut surtout pas ouvrir la pièce jointe de cet e-mail, même s'il semble en tout point réaliste. Le fait que vous ne connaissez pas l'expéditeur devrait suffire à vous mettre en garde.
En cas d'ouverture, n'éteignez pas votre ordinateur, déconnectez-le d'Internet et appelez votre département informatique.
Bitdefender détecte le malware en tant que Trojan.Downloader.Drixed.C.

Source : http://www.globalsecuritymag.fr/Le-trojan-Drixed-revient-en-force,20150609,53337.html

Alerte ! Des images informatiques infectées, le nouveau danger… | Le Net Expert Informatique

	**Alerte ! Des images informatiques infectées, le nouveau danger…**

Lors de la conférence Hack In The Box d'Amsterdam, un chercheur en sécurité informatique présente Stegosploit, un outil qui permet de cacher un code malveillant dans une image.

Imaginez, vous êtes en train de surfer quand soudain votre machine devient folle ! Un code malveillant vient d'être installé alors que vous avez un antivirus et vos logiciels à jour. Une image, affichait par un site que vous veniez de visiter vient de lancer l'attaque. De la science-fiction ? Pas avec les preuves de Saumil Shah, un chercheur en sécurité informatique.
L'ingénieur a expliqué lors de la conférence (HiP) Hack In The Box que des pirates étaient très certainement en train d'exploiter sa découverte. L'idée, cacher un code malveillant dans une image en utilisant la stéganographie (cacher une information dans un autre document, NDR). Des recherches de Shah est sorti Stegosploit, un logiciel qui code en Javascript un logiciel malveillant dans les pixels d'une image au format JPEG ou PNG.

Source : http://www.datasecuritybreach.fr/stegosploit-loutil-qui-cache-un-code-malveillant-dans-une-image/#axzz3cN0qvWLQ