Entreprises, surveillez l’usage des réseaux sociaux !

Entreprises, surveillez l’usage des réseaux sociaux !

Selon Osterman Research, près de une entreprise sur cinq a été victime de malwares diffusés par le biais de réseaux sociaux.

Les réseaux sociaux sont des outils de communication clés pour les entreprises, mais ils constituent aussi un vecteur d'attaques informatiques encore trop souvent négligé par les organisations, observe le cabinet américain Osterman Research dans un livre blanc (Best Practices for Social Media Archiving and Security). Sponsorisée par Actiance, Gwava et Smarsh, l'enquête a été réalisée auprès d'un panel de professionnels IT et décideurs d'entreprises de taille moyenne et de grands groupes.
73 % des entreprises concernées par cette enquête utilisent Facebook dans le cadre professionnel, 64 % LinkedIn et 56 % Twitter. Plusieurs plateformes sont utilisées régulièrement. Du côté des réseaux sociaux d'entreprise (RSE), Microsoft Sharepoint est l'outil le plus largement cité (par 82 % des répondants). Il devance Jabber et WebEx de Cisco ou encore Yammer de Microsoft.

Une porte d'entrée pour les malwares
54 % des organisations ont adopté une politique relative à l'utilisation par leurs collaborateurs des réseaux sociaux tout public (ce taux passe à 51 % pour les RSE). Mais elles ne sont plus que 48 % à le faire lorsqu'il est question de l'usage professionnel des plateformes tout public. Si une majorité veille ou surveille cet usage, 27 % ne le font pas. Et ce malgré les cybermenaces et les risques juridiques auxquels les entreprises sont confrontées.
Dans ce contexte, 18 % ont constaté que leur compte « social » a été piraté ou ont été victime d'une attaque par malware, soit près d'un utilisateur de réseau social sur cinq en entreprise. Mais pour 80 % des répondants, c'est bien l'email qui constitue la première source d'infiltration de logiciels malveillants dans les systèmes et réseaux internes des organisations
[Lien vers l'article original partagé]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Sécurité : entreprises, surveillez l'usage des réseaux sociaux !*

Google fait semblant de ne rien comprendre à ce qu'exige la Cnil

Google fait semblant de ne rien comprendre à ce qu'exige la Cnil

---

Source : *Droit à l’oubli : Comment Google feint de ne rien comprendre à ce qu’exige la Cnil – Politique – Numerama*

Tout sur les arnaques et les piratages Informatiques sur @LCI ce 23 mai 2016 en direct de 9h15 à 10h avec Denis JACOPINI

Tout sur les arnaques et les piratages Informatiques sur @LCI ce 23 mai 2016 en direct de 9h15 à 10h avec Denis JACOPINI

Denis JACOPINI sera ce lundi 23 mai 2016 en direct sur LCI pour vous parler pendant près d'une heure des mails malveillants, des arnaques où les pirates se font passer pour EDF ou les impôts pour soutirer les données bancaires…

Le but de cette émission sera avant tout sera d'expliquer le phénomène en croissance incoercible de la cybercriminalité.
A cours de l'émission nous verrons les pièges à éviter, et quelques conseils à suivre pour se protéger des pirates informatiques.
Suivez le direct sur lci.tf1.fr

Le replay sera mis en ligne dans les jours qui suivront et accessible aussi sur cette page.

Vous pouvez également découvrir toutes les solutions de notre expert lors de ses formations et actions de sensibilisation à la cybersécurité, au piratage informatique, aux arnaques pour mieux vous en protéger.

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Ransomware*

Plus de 100 millions de mots de passe LinkedIn dans la nature… depuis 2012 !

	**Plus de 100 millions de mots de passe LinkedIn dans la nature… depuis 2012 !**

Une base de données, contenant 117 millions de combinaisons d'identifiants et de mots de passe, est vendue 2000 euros par des pirates. Le réseau social professionnel enquête.

Le piratage massif dont a été victime LinkedIn en 2012 revient hanter le réseau social professionnel. Une base de données contenant plus de 100 millions d'identifiants et de mots de passe est actuellement proposée à la vente sur une place de marché du dark web, «The Real Deal», rapporte le siteMotherBoard. Le fichier est proposé à la vente pour 5 bitcoins, soit un peu plus de 2000 euros. Il concerne 167 millions de comptes, dont 117 millions sont associés à un mot de passe.

Le site LeakedSource, qui a eu accès au fichier, assure avoir réussi à déchiffrer en trois jours «90% des mots de passe». Ils étaient en théorie protégés par un procédé de hachage cryptographique, SHA-1, mais sans salage, une technique compliquant leur lecture en clair. Deux personnes, présentes dans le fichier, ont confirmé à un chercheur en cybersécurité que le mot de passe associé à leur identifiant était authentique.

LinkedIn avait reconnu en 2012 le vol des données de connexion, mais sans jamais préciser le nombre d'utilisateurs concernés. Un fichier, concernant 6,5 millions de comptes, avait à l'époque été mis en ligne. «À l'époque, notre réponse a été d'imposer un changement de mot de passe à tous les utilisateurs que nous pensions touchés. De plus, nous avons conseillé à tous les membres de LinkedIn de changer leurs mots de passe», commente aujourd'hui le réseau social professionnel sur son blog.

123456, linkedin, password, 123456789 et 12345678

En réalité, un porte-parole de LinkedIn avoue «ne pas savoir combien de mots de passe ont alors été récupérés». «Nous avons appris hier qu'un jeu de données supplémentaire qui porterait supposément sur plus de 100 millions de comptes et proviendrait du même vol de 2012, aurait été mis en ligne. Nous prenons des mesures immédiates pour annuler ces mots de passe et allons contacter nos membres. Nous n'avons pas d'éléments qui nous permettent d'affirmer que ce serait le résultat d'une nouvelle faille de sécurité», ajoute LinkedIn sur son blog.

Selon LeakedSource, la base de données aurait été détenue jusqu'alors par un groupe de pirates russes. Ces informations de connexion, même si elles remontent à 2012, ont encore une grande valeur. Elles peuvent être utilisées tout à la fois pour pénétrer dans d'autres comptes plus critiques (sites d'e-commerce, banque en ligne…) ou organiser des campagnes de phishing, une technique utilisée pour obtenir les renseignements personnels d'internautes. Nombre d'utilisateurs utilisent la même combinaison d'adresse email et de mot de passe sur tous les sites, et en changent peu souvent, ce qui démultiplie les effets de tels piratages.Preuve de cette imprudence générale, les cinq mots de passe les plus utilisés dans le fichier mis en vente étaient 123456, linkedin, password, 123456789 et 12345678… [Lire la suite]

Réagissez à cet article

Source : *Plus de 100 millions de mots de passe LinkedIn dans la nature*

Prise d’otage numérique par Rançongiciels, la nouvelle arme fatale des cyberpirates

Prise d’otage numérique par Rançongiciels, la nouvelle arme fatale des cyberpirates

---

Les prises d'otages numériques, avec demande de rançon, se multiplient. Payer est souvent la seule solution

Locky, Cryptolocker, Synolocker, Cryptowall, TeslaCrypt, Petya… Si vous n'êtes pas un spécialiste de la sécurité informatique, ces noms barbares ne vous disent probablement rien. Et pourtant, ils représentent la nouvelle menace qui pèse sur vos ordinateurs. Depuis quelques années, en effet, un nouveau type de logiciel malveillant a le vent en poupe: les rançongiciels – un néologisme 2.0 dérivé du mot «ransomware» dans la langue de Shakespeare. Ces virus prennent, à distance, le contrôle de PC, tablettes ou smartphones et bloquent l'ensemble de leurs données. Pour les récupérer, les propriétaires légitimes sont sommés de payer une rançon dans un délai très court, dans une monnaie virtuelle et non traçable comme les bitcoins.
Selon une étude d'Intel Security-McAffe, datant de mars 2016, ce type d'attaque a augmenté de 26% au dernier trimestre 2015, par rapport à l'année précédente.

Les PME ne sont pas préparées
«Les demandes de rançons après un piratage sont en plein essor dans le monde et en Suisse, résume Ilia Kolochenko, CEO et fondateur de l'entreprise genevoise High-Tech Bridge, spécialisée dans la sécurité informatique. C'est devenu une véritable industrie.»
De fait, les exemples se multiplient – proches de nous. En avril 2016 par exemple, Ralph Eberhard, patron de la gérance Immogeste basée à Genève, témoigne dans le journal *Le Temps* avoir dû payer 1800 francs à des hackers. Le même mois, un peu plus loin d'ici, dans le Béarn, le PDG d'une entreprise raconte peu ou prou la même histoire, dans le journal *La République des Pyrénées*.
En effet, à chaque fois la scénario est identique. Un matin, en allumant leurs ordinateurs, les salariés voient s'afficher sur leur moniteur un message martial, généralement rouge sur fond noir, qui dit en substance: «Tous les fichiers de votre disque dur ont été cryptés. Pour les déchiffrer et les récupérer, vous devez nous payer.» La plupart du temps, les montants exigés ne s'avèrent pas dissuasifs: de quelques centaines de francs pour des particuliers à quelques milliers pour les PME. Mais parfois les sommes demandées sont astronomiques. En février 2016, un ransomware a infecté un hôpital de Los Angeles, bloquant l'ensemble des données médicales des patients. Pour remettre le système d'information d'aplomb, les pirates ont réclamé 9000 bitcoins, soit l'équivalent de 3,6 millions de dollars!
«Auparavant, les hackers s'attaquaient à de grosses entreprises, afin de toucher le jackpot, rappelle Ilia Kolochenko. Aujourd'hui, ils se recentrent sur les PME et les particuliers, parce qu'ils ont compris que même si les sommes obtenues sont moindres, l'activité se révèle moins risquée et plus facile. Si vous attaquez une grande banque, vous devez d'abord déjouer une sécurité informatique de premier plan. Et si vous y parvenez, vous pouvez être certain qu'elle ne vous lâchera jamais. Elle vous traquera pendant des années s'il le faut. A l'inverse, les particuliers et les PME ne sont absolument pas préparés à ce type d'attaque et en plus ne disposent pas des moyens nécessaires pour retrouver les auteurs.» Selon un rapport de Symantec publié en avril 2016, 57% de ces attaques ciblent des entreprises de moins de 250 salariés.
Mais comment ces logiciels malveillants se diffusent-ils? «Ces chevaux de Troie accèdent à l'ordinateur par le biais de courriels infectés ou de sites Internet piratés», explique la centrale Melani. Concrètement, «les hackers possèdent des robots informatiques, les botnets, qui scrollent l'ensemble des pages Internet – un peu comme Google – à la recherche de failles connues, explique Ilia Kolochenko. Lorsqu'une vulnérabilité est découverte, le virus s'installe et attend sa victime, en affichant par exemple un nouveau lien. Lorsque quelqu'un clique sur ce dernier, le virus passe sur son ordinateur et crypte l'ensemble des données.»
Faut-il payer la rançon ou pas?
Face à cette situation, la centrale Melani recommande de «ne pas céder à l'extorsion car, en payant la rançon, vous participez au financement de l'activité des criminels et leur permettez d'améliorer l'efficacité de leurs prochaines attaques. De plus, il n'existe aucune garantie que les criminels respecteront leur engagement et vous enverront réellement la clé vous permettant de récupérer vos données.»
En pratique, les choses s'avèrent plus compliquées, notamment pour les PME qui, privées de leurs fichiers clients, voient toute leur activité bloquée. «Si vous êtes infectés, il n'existe pas 3000 solutions, reconnaît Ilia Kolochenko. La première consiste à faire des recherches sur Internet, afin de savoir s'il existe déjà une clef de décryptage contre le rançongiciel. Malheureusement, c'est rarement le cas. La seconde, c'est payer. Si vous vous adressez à une entreprise comme la nôtre, nous finirons par remonter jusqu'au coupable et nous parviendrons peut-être à récupérer vos données. Mais cela va prendre beaucoup de temps. Même si cela peut paraître immoral, c'est moins coûteux pour une PME de régler la rançon que de lancer des investigations.» (TDG)
[Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises Techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Contactez-nous

Réagissez à cet article

Source : *Sécurité informatique: Rançongiciels, la nouvelle arme fatale des cyberpirates – News High-Tech: Hard-/Software – tdg.ch*

Hoverboards, solowheels et autres gadgets roulants se préparent à conquérir Noël

Hoverboards, solowheels et autres gadgets roulants se préparent à conquérir Noël m

---

Noël 2016 sera encore placé sous le signe des gadgets roulants électriques. Au MedPi, les constructeurs alignent leurs gammes .

On ne découvre pas vraiment des produits que l'on ne connaissait pas au MedPi, mais comme il s'agit avant tout du supermarché des professionnels de la distribution, il est possible de sentir les tendances qui se dessineront pour les événements commerciaux français à venir – et en particulier la rentrée et Noël. Quand on découvre un gadget incroyable et qu'il n'est pas disponible en France, on sait que son adoption sera lente, réservée aux passionnés. Ici, nous sommes dans le réel, dans les rayons des grands magasins. Et le réel, en 2016, c'est beaucoup de choses qui roulent.
Si vous aviez des enfants en âge de commander un hoverboard à Noël dernier, vous pouvez être sûr qu'ils ne passeront pas à côté de la deuxième génération de ces produits qui ont envahi les rayons et se classent en premier rang des vidéos de chutes ridicules sur YouTube. En tout cas, au MedPi, on ne peut pas parcourir une allée sans voir au moins une marque ou un importateur qui cherche à placer dans les rayons ses engins à roues uniques, double roues parallèles, double roues sur un axe, double roues sur un axe avec selle… la liste est longue.

L'idée derrière ces engins ne différencie pas vraiment entre les modèles : il s'agit d'exploiter les performances actuelles des moteurs électriques et des batteries pour proposer des engins qui répondent aux problématiques de la mobilité urbaine. Il faut pouvoir se déplacer rapidement, sans risque majeur de chute… et sans effort. Ce dernier point pourrait paraître regrettable, mais nous nous sommes aperçus dans notre premier test d'une trottinette électrique qu'elle ne remplaçait pas, naturellement, les trajets que l'on aurait fait à pied ou en vélo, mais bien plus volontiers les trajets en transports en commun. En somme, les plus pénibles.
Bien entendu, sur ce secteur, le bon grain côtoie l'ivraie. Les marques les plus réputées comme Ninebot, qui possède Segway, ont des brevets et de nombreuses innovations dans leur portefeuille en plus d'avoir des appareils de grande qualité, autostabilisés. Les autres rattrapent leur retard ou proposent des ersatz de technologies pas vraiment convaincantes (ni légales), laissant sur le carreau tout le côté stable des engins qu'ils proposent, les faisant entrer dans la catégorie « jouets pour ados » plus que dans celle de la mobilité urbaine. Et pour un Ninebot ou équivalent, il y a au moins 3 constructeurs aux noms étranges dans les allées du MedPi.
Plusieurs problématiques restent d'ailleurs à résoudre pour que ce marché explose véritablement. La première, c'est bien entendu la question de la sécurité des utilisateurs : les hoverboards qui ont assailli l'Europe et les États-Unis l'an passé étaient loin d'être tous conformes aux régulations en vigueur en matière d'électronique et plusieurs affaires de batteries défectueuses ou anormalement inflammables avaient conduit au bannissement de certains modèles, notamment vendus par Amazon.
Ensuite vient la route – ou les trottoirs. Où doivent rouler ces engins ? Sur les trottoirs, ils peuvent être dangereux pour les piétons et pour eux-mêmes, dans la mesure où les voies piétonnes sont pavées d'obstacles contre lesquels les personnes en chaise roulante doivent lutter depuis longtemps, malheureusement. Sur la route, c'est l'utilisateur qui devient vulnérable, debout en équilibre, lancé à plusieurs dizaines de kilomètres par heure. On l'imagine mal à l'aise dans les croisements. Si les voies pour les vélos étaient massivement installées, comme chez nos voisins hollandais, la question ne se poserait pas.
En France, elle est encore ouverte : peut-être est-il temps que les municipalités s'en emparent avant que nous ayons à écrire des articles sur les premiers accidents graves. Même si les hoverboards ne volent (presque) toujours pas… [Lire la suite]

Réagissez à cet article

Source : *Hoverboards, solowheels et autres gadgets roulants se préparent à conquérir Noël – Tech – Numerama*

Vers une nouvelle plainte européenne contre Google

Vers une nouvelle plainte européenne contre Google

Google n'en a pas encore fini avec sa série de déboires judiciaires. Alors que le géant américain fait l'objet d'investigations à propos de son moteur de recherche et de sa plate-forme Androïd pour abus de position dominante, on apprend que le groupe américain pourrait être visé par une nouvelle enquête toujours de la part de la Commission européenne. Cette fois, cela concerne le cœur de l'entreprise, à savoir les services publicitaires.

Le site generation-nt.com qui reprend Bloomberg indique que la nouvelle procédure serait indépendante de deux précédentes et suivre son propre cours. Elle découle d'une procédure lancée depuis 2010 et qui concernerait des contrats avec des clients de Google dont le but était d'écarter l'utilisation de services concurrents.

Seulement, l'action annoncée pourrait être très coûteuse pour le géant américain parce qu'elle touche un domaine qui représente la majeure partie des solides revenus de Google, soit plus de soixante-quatorze milliards de dollars, seulement pour l'année 2015. Une perspective à laquelle il serait très difficile d'échapper puisque generation-nt.com nous apprend que Google a déjà épuisé ses possibilités de négociations avec la Commission européenne…. [Lire la suite]

Réagissez à cet article

Source : *Vers une nouvelle plainte européenne contre Google | CIO-MAG*

Conficker : un virus de 8 ans toujours vivace !

Conficker : un virus de 8 ans toujours vivace !

D'après des chercheurs de Check Point, le ver Conficker est toujours bien présent et à l'origine de nombreuses infections. Pourtant, la faille exploitée par ce malware a été corrigée en 2008.

Le mois dernier, il a été à l'origine de plus d'une attaque sur six d'après les mesures réalisées par l'éditeur de sécurité Check Point. Et pour cela, nul besoin d'être le programme malveillant le plus récent.

En effet, ce malware n'est autre que Conficker, apparu pour la première fois en 2008 – même si de nombreuses variantes ont été signalées ensuite. Comment après tant d'années, un virus peut-il rester toujours aussi actif ?

C'est avec les vieux virus qu'on fait les meilleures infections

Certes, à l'époque, Confiker était présenté comme « le plus complexe et sophistiqué » virus jamais réalisé. Mais si de telles menaces persistent, c'est car les failles logicielles exploitées par celles-ci persistent également.

Or, la vulnérabilité liée à Conficker a été corrigée par Microsoft fin 2008. Mais sur de nombreux postes Windows et réseaux, des brèches de sécurité demeurent permettant ainsi à ce malware de provoquer des attaques.

Mais Conficker n'est pas un cas isolé. Toujours selon Check Point, le virus Sailty et le ver Zeroaccess, apparus respectivement en 2003 et 2011, continuent eux aussi de cibler des machines Windows. Avec Conficker, ce sont les trois familles de malware les plus impliquées dans des attaques reconnues.

En 2015, selon le patron du CERT britannique, Chris Gibson, Conficker a été à l'origine de plus de 500.000 incidents de sécurité. Un bilan « excessivement déprimant » déplorait ce spécialiste… [Lire la suite]

Réagissez à cet article

Source : *Conficker : un virus de 8 ans toujours vivace ! –*

ZDNet

BMW lance un défi aux startups françaises pour améliorer la voiture de demain

	**BMW lance un défi aux startups françaises pour améliorer la voiture de demain**

Le BMW Tech_Date, prévu pour le 9 juin prochain, est un concours ouvert aux startups françaises. Ces dernières doivent y présenter des innovations intégrables dans les voitures intelligentes conçues par le constructeur.

BMW sollicite les startups françaises. Le constructeur automobile organise le 9 juin prochain la première édition du BMW Tech_Date dans son magasin des Champs Élysées à Paris. L'objectif : accélérer la construction de la mobilité des cent prochaines années.
Ce concours permettra aux startups de présenter des innovations qu'elles pensent pouvoir intégrer aux futures voitures intelligentes de BMW. C'est en tout cas ce que souhaite le constructeur.
« Nous avons les technologies pour rendre la voiture intelligente mais nous sommes en recherche constante de solutions qui peuvent rendre l'usage de la voiture plus intelligent », explique Pierre Jalady, responsable marketing de BMW en France, dans une interview au Journal du Net. L'entreprise souhaite en effet adapter ses services pour qu'ils soient plus centrés sur l'utilisateur.
Les startups ont jusqu'au 30 mai pour candidater. Une vingtaine d'entre elles seront sélectionnées pour le Tech_Date afin de présenter leurs technologies devant un jury qualifié.

Trois vainqueurs seront désignés en fonction de plusieurs critères dont :
• niveau d'innovation de la solution proposée
• le délai d'intégration potentiel pour BMW
• D'autres éléments seront pris en compte tels que le niveau préexistant de relations commerciales avec l'industrie automobile, la solidité de la société et la communauté fédérée par les startups sur les réseaux sociaux.
Les trois gagnants « seront reçus pendant une semaine au siège de Munich, où ils rencontreront toutes les équipes qui auront un intérêt à travailler avec eux, des achats au marketing. Ils seront aussi mis en avant au Mondial de l'automobile de Paris en octobre prochain », affirme Pierre Jalady.
Ce concours a également pour but de célébrer le siècle d'existence de BMW qui fêtait son anniversaire en mars dernier. Le constructeur estime que le Tech_Date est une occasion de mettre en lumière les innovations françaises et déclare vouloir travailler en partenariat avec les entreprises les plus créatives.
Crédit photo de la une : BMW… [Lire la suite]

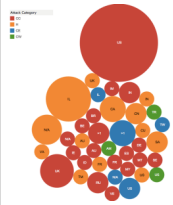
Réagissez à cet article

Source : *BMW lance un défi aux startups françaises pour améliorer la voiture de demain – Tech – Numerama*

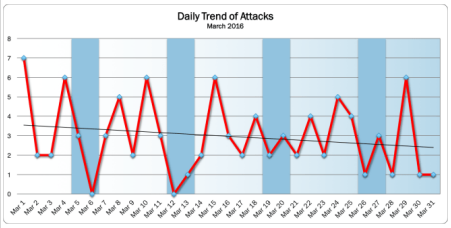
April 2015 Cyber Attacks Statistics – HACKMAGEDDON

Météo des cyberattaques de mars 2016

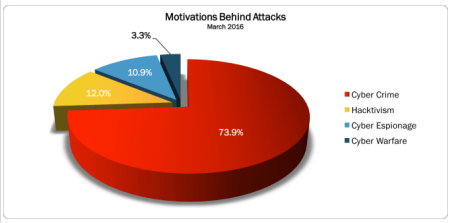
Afin de vous tenir informé de la météo des cyberattaques, nous avons souhaité partager avec vous l'étude récemment parue sur l'état des lieux des cyberattaques pour le mois de mars 2016 .



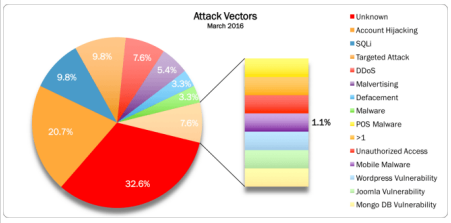
I finally found the time to aggregate the data of the timelines of March (part I and part II) into statistics.
As usual let's start from the **Daily Trend of Attacks**, which shows quite a sustained level of activity throughout the entire month, most of all during the first half.



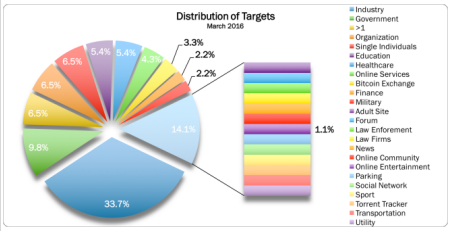
Cyber Crime ranks on top of the **Motivations Behind Attacks** chart with a noticeable 73.9%, a sharp increase compared with 62.7% of February. On the other hand hacktivists seem to have taken a temporary period of vacation in March (maybe due to the beginning of Spring), since Hacktivism reduces its quota to a modest 12%, less than one half of the percentage reported in February (28%). Cyber Espionage ranks at number three and also reports a noticeable growth (10.9% vs 5.3% in February). Last but not least, the attacks motivated by Cyber Warfare drop to 3.3% from 4% reported in February.



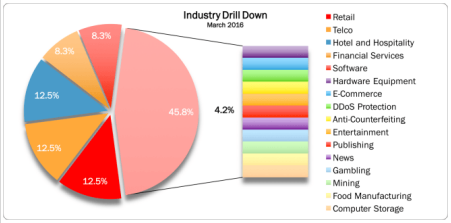
In the 32.6% of the cases the **Attack Vectors** are unknown. Account Hijackings rank at number one among the known attack vectors with 20.7% (was 12%, this growth is the effect of the numerous BEC and tax return scams reported in March). SQLi, an evergreen, confirms its momentum with 9.8% (was 10.7% in March), the same percentage of Targeted attacks (was 9.3% in March).



Industries lead the **Distribution of Targets** chart with 33.7% (was 29.3% in February). Governments rank at number two (9.8%, was 14.7% in February), whereas all the other targets are behind. Effectively this month the Distribution of Targets appear particularly fragmented.



The **Industry Drill Down** Chart is also particularly fragmented this month (tax scams do not privilege any particular sector) and is led by Retail, Telco and Hospitality (12.5% each). Software and Financial Services are behind (8.3%) and above all the other sectors.



As usual, the sample must be taken very carefully since it refers only to discovered attacks included in mytimelines, aiming to provide an high level overview of the "cyber landscape".
If you want to have an idea of how fragile our data are inside the cyberspace, have a look at the timelines of the main Cyber Attacks in 2011, 2012, 2013, 2014 and now 2015 (regularly updated). You may also want to have a look at the Cyber Attack Statistics.
Of course follow @paulsparrows on Twitter for the latest updates, and feel free to submit remarkable incidents that in your opinion deserve to be included in the timelines (and charts)… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *April 2015 Cyber Attacks Statistics – HACKMAGEDDON*