La Cybersecurité des banques européennes bientôt soumises à un stress-test ?

	La Cybersecurité des banques européennes bientôt soumises à un stress-test ?

Les attaques visant les systèmes bancaires connectés au réseau Swift soulèvent de vastes inquiétudes au point que les autorités européennes pourraient être appelées à conduire un stress-test visant à éprouver leur cybersécurité.

Recommander les autorités locales des pays membres de l'Union européenne à soumettre les systèmes de sécurité informatique des institutions financières à des stress-tests. C'est l'idée qu'a avancé Andrea Enria, président de l'Autorité Bancaire Européenne, l'autorité indépendante chargée de garantir un niveau de surveillance prudentiel efficace et cohérent à l'échelle de l'Union, à l'occasion d'un échange avec nos confrères de Reuters.
Dans ce cadre, il estime que les banques pourraient avoir à provisionner des réserves supplémentaires afin de se protéger, financièrement, du risque associé à des attaques informatiques. Le risque informatique doit d'ailleurs être explicitement pris en compte dans le cadre des règles Pilier 2. Celles-ci font partie des accords Bâle II et portent justement sur la surveillance prudentielle ainsi que la gestion des risques.
Et la prise en compte des risques associés aux attaques informatiques apparaît particulièrement importante qu'ils sont appelés à être de plus en plus considérés dans les analyses de solvabilité des agences de notation. Moody's et Standard & Poor l'ont ainsi ouvertement indiqué à l'automne dernier.
Fin 2013, les banques britanniques ont été soumises à un stress-test IT, après un premier en 2011. Mais l'opération n'avait pas manqué de soulever plusieurs critiques, certains experts estimant notamment qu'elle devrait survenir plus régulièrement. D'autres s'interrogeaient sur la manière dont étaient définies les attaques imaginées pour l'exercice.
Très récemment, la patronne du gendarme des marché boursiers américains a de son côté estimé que le risque d'attaque informatique constitue la principale menace pour le système financier mondial, notamment après les opérations qui ont visé dernièrement les systèmes plusieurs banques connectés au réseau Swift… [Lire la suite]

Merci à Valery Marchive pour son article

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 : *Vers un stress-test de la cybersécurité des banques*

européennes ?

Et si charger la batterie de son smartphone via un port USB était dangereux ?

	**Et si charger la batterie de son smartphone via un port USB était dangereux ?**

On s'est tous probablement retrouvés un jour ou l'autre dans une situation où il nous restait peu de batterie sur notre téléphone et que nous n'avions pas de chargeur à portée de main. Le pire, c'est ce que ça nous est arrivé au moment même où on en avait le plus besoin, comme attendre un appel important, un message ou un e-mail, etc.

Il parait donc tout à fait normal de chercher une source d'électricité à proximité lors d'une telle situation, par exemple utiliser un port USB. Mais est-ce bien sûr ? Non, en réalité cela peut s'avérer dangereux. Via une connexion USB, n'importe qui peut s'emparer de vos fichiers, infecter votre smartphone d'un virus ou même le rendre inutilisable.

Chevaucher la foudre

Avant d'aborder le problème des hackers, il est important de préciser que toute les sources d'électricité ne sont pas forcément bonnes pour votre téléphone. Il existe beaucoup de plaintes sur Internet, principalement d'utilisateurs tentant de charger leur téléphone dernier cri en les connectant à des adaptateurs ou des chargeurs d'occasion (ou non originaux). Dans certains cas, les téléphones ont été rendus inutilisables. Dans certains cas encore plus étranges, des personnes prenant leur téléphone alors qu'ils étaient en charge ont été sérieusement blessées ou même tuées.

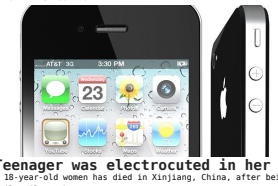
Follow

Daily Mail Online

@MailOnline

Teen dies after being electrocuted in her sleep while charging her iPhone http://dailym.ai/1o7Eia5

2:10 PM – 31 Jul 2014



Teenager was electrocuted in her sleep while charging her iPhone

A 18-year-old women has died in Xinjiang, China, after being electrocuted in her sleep while charging her iPhone 4s. It is not known if she was using an authentic Apple phone charger.

dailymail.co.uk

•

•

140140 Retweets

•

2424 likes

Malheureusement, il s'agit plus que de simples accidents. Par exemple, l'année dernière un appareil a été baptisé à juste titre : le tueur USB. Il contenait un impressionnant ensemble de condensateurs hébergés dans une carte mémoire flash USB, qui déchargeait 220 V dans le port USB auquel il était connecté. Une telle décharge pourrait dans le meilleur des cas détruire le port USB et dans le pire sans doute la carte mère de tout l'ordinateur. Nous doutons que vous souhaitiez tester la durabilité de votre téléphone de cette façon.

Montrez-moi vos fichiers

Deuxièmement, les ports USB n'ont pas été conçus uniquement pour la charge, mais aussi pour transférer des données. Les téléphones consommant le plus de données sont ceux conçus sur la plateforme Android 4 *x* et les versions antérieures, ils se connectent sur le mode MTP (Media Transfer Protocol) par défaut, exposant tous les fichiers de l'appareil.

En moyenne, il faut plus d'une centaine de kilo octets de données rien que pour le système hôte des fichiers et dossiers du téléphone. Pour vous donner une idée, il s'agit de la taille d'une copie de l'e-book d'*Alice au pays des merveilles*.

Bloquer votre téléphone vous éviterait de courir un tel risque mais honnêtement seriez-vous prêt à vous passer de votre téléphone pendant qu'il est en charge ? Et à toujours le débrancher du port USB lorsque vous recevez un message par exemple ?

A présent, jetons un coup d'œil de plus près aux données qui sont transmises du port USB même lorsque le mobile est en mode (bloqué) « charge seule ». La taille de ces données varie, dépendant de la plateforme du mobile et du système d'exploitation de l'hôte. Mais dans tous les cas, il s'agit plus que d'une « simple charge ». Comme nous l'avons découvert, ces données incluent le nom du mobile, le nom du fournisseur et le numéro de série.

Accès complet et au-delà

Vous devez sûrement penser que vous ne voyez pas où est le problème, seulement il y en a un, puisque nous avons trouvé en cherchant des informations accessibles au public qu'un fournisseur en particulier autorise beaucoup plus que ce qui est spécifié par le système.

Comment est-ce possible ?

Cela est rendu possible via un ancien système de commandes appelées commandes AT. Ces dernières ont été développées il y a quelques dizaines d'années afin de permettre les communications des modems et ordinateurs. Plus tard, elles ont été intégrées au standard du GSM et désormais sont toujours utilisées sur les smartphones.

Pour vous donner une idée de l'usage des commandes AT, laissez-moi vous donner quelques exemples que nous avons été en mesure de découvrir à la surface d'Internet : elles permettent à un hacker d'obtenir votre numéro de téléphone et de télécharger les contacts enregistrés dans la carte SIM. Ces commandes permettent d'établir un appel à n'importe quel numéro, et ce à vos frais, bien entendu. Et si vous êtes en roaming, de tels appels inattendus peuvent vite faire grimper la facture. Dépendant du vendeur, le mode du roaming peut faciliter l'accès à un hacker d'installer n'importe quel type d'applications, y compris malveillantes.

Tout ce qu'on vient de mentionner est possible, même si votre smartphone est bloqué !

En résumé, ne vous fiez pas aux apparences d'un port USB car il pourrait bien « cacher des choses ». Il s'agit d'un système qui collecte les données des appareils auxquels il est connecté, peu importe les raisons. C'est une source d'énergie bancale, tel un puissant condensateur ou un ordinateur qui installe une porte dérobée sur votre appareil. Une chose que vous ignorez jusqu'à ce que vous le branchiez.

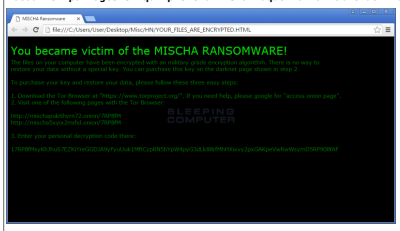
Article de Alexey Komarov

Source : *Les dangers de charger la batterie de son smartphone via un port USB – Kaspersky Daily – | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.*

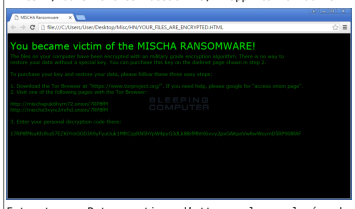
Mischa, le ransomware successeur de Petya

Mischa, le ransomware successeur de Petya

Apparu au mois de mars, le ransomware Petya a ouvert une nouvelle voie dans le développement des ransomwares. Il s'agissait du premier cas d'un malware qui allait au-delà du chiffrement des fichiers sur les disques locaux et partagés et qui préférait s'attaquer à la table de fichiers principale



Ceci étant dit, Petya n'était pas infaillible et les chercheurs ont été rapidement en mesure de créer un outil de restauration de certains des fichiers chiffrés par ce malware. Les individus malintentionnés n'ont pas perdu leur temps et ils ont trouvé le moyen de contourner une autre lacune de Petya : sa dépendance vis-à-vis de la volonté de la victime qui doit octroyer au malware les autorisations d'administrateur pour accéder à la table de fichiers principale (MFT).
Un nouveau programme d'installation de Petya a été détecté la semaine dernière. Celui-ci utilise un scénario de réserve. Si le malware n'obtient pas les autorisations d'administrateur au lancement, c'est un autre ransomware qui sera installé sur la machine infectée, en l'occurrence Mischa.
D'après les explications de Lawrence Abrams, de chez Bleeping Computer, les autorisations d'administrateur indispensables au fonctionnement de Petya figurent dans le manifeste de la version originale. Dans les commentaires envoyés à Threatpost, Lawrence Abrams explique « qu'avant l'exécution du code, Windows affiche la boîte de dialogue UAC qui sollicite ces autorisations. Si le service UAC est désactivé, l'application est exécutée automatiquement avec [les autorisations d'administrateur]. Si l'utilisateur clique sur « No » dans la fenêtre UAC, l'application n'est pas exécutée et, par conséquent, l'installation de Petya n'a pas lieu ».
Pour les exploitants de Petya, ces échecs représentent un gaspillage de ressources d'après Lawrence Abrams. Pour rectifier le tir, ils ont empaqueté un autre ransomware avec le programme d'installation. Il s'agit de Mischa qui sera exécuté si l'option « Petya » n'a pas pu être mise en œuvre.
Le manifeste de la nouvelle version indique que le fonctionnement requiert les données du compte utilisateur. Dans ce cas, Windows autorise le lancement de l'application sans afficher d'avertissement UAC. Comme l'explique Lawrence Abrams, « au lancement du programme d'installation, il sollicite les autorisations d'administrateur conformément à ses paramètres. La boîte de dialogue UAC s'affiche et si l'utilisateur choisit « Yes », ou si UAC est désactivé, l'application obtient les autorisations d'administrateur et installe Petya. Dans le cas contraire, c'est Mischa qui sera installé. Cette méthode est très intelligente ».



Entre temps, Petya continue d'attaquer les employées des services des ressources humaines allemands à l'aide de messages non sollicités qui contiennent des liens vers un fichier malveillant dans le cloud. Au début, les individus malintentionnés utilisaient Dropbox, mais depuis le blocage des liens Dropbox malveillants, ils se sont rabattus sur le service allemand TelekomCloud. Le fichier exécutable se dissimule sous les traits d'un fichier PDF qui serait un prétendu CV d'un candidat à un poste libre. Il contient même une photo.
« Lorsque l'utilisateur télécharge le fichier exécutable, l'icône PDF s'affiche, ce qui laisse penser qu'il s'agit bien d'un CV au format PDF » explique Lawrence Abrams. Toutefois, lorsque ce fichier est ouvert, il tente d'installer Petya. Et si cela ne marche pas, il installe le ransomware Mischa.
Le comportement de Mischa est identique à celui des autres ransomwares standard. Il analyse le disque local à la recherche de fichiers portant certaines extensions. Il chiffre les fichiers à l'aide d'une clé AES et ajoute à leur nom une extension de 4 caractères, par exemple 7GP3. Lawrence Abrams explique que « lorsque Mischa chiffre le fichier, il conserve la clé de chiffrement à la fin du fichier obtenu. Il convient de noter qu'il ne chiffre pas uniquement les fichiers traditionnels dans ce genre d'attaque (PNG, JPG, DOCX, etc.), mais également les fichiers EXE. »
Une fois qu'il a chiffré les fichiers, Mischa exige le versement d'une rançon de 1,93 bitcoins (environ 875 dollars américains) pour le déchiffrement. La somme doit être payée via le site Tor. Il n'existe pas encore d'outil de déchiffrement pour ce ransomware. « Nous conseillons aux victimes de vérifier avant tout la conservation des clichés instantanés à l'aide de Shadow Explorer. Ils pourraient être utile pour restaurer une ancienne version des fichiers chiffrés » conclut Lawrence Abrams.

Article du Kaspersky Lab

Source : *Petya possède un suppléant : Mischa – Securelist*

L'adoption de l'analyse comportementale appelée à s'étendre

L'adoption de l'analyse comportementale appelée à s'étendre

Selon Gartner, les entreprises se tournent de plus en plus vers l'analyse comportementale pour améliorer la détection des incidents et renforcer l'efficacité de leurs SOC. De quoi pousser à une inéluctable consolidation du marché.

L'analyse comportementale – des utilisateurs comme des flux réseau ou des entités connectées à l'infrastructure – a fait une entrée remarquée sur le marché de la sécurité l'an passé. Mais selon Gartner, les solutions isolées actuellement proposées vont être rapidement appelées à s'intégrer, au point d'encourager à une consolidation des acteurs.

Dans une note d'analyse, Avivah Litan et Eric Ahlm résument la situation : « les besoins des acheteurs pour détecter les brèches de tout type vont pousser à la consolidation des systèmes de détection basés sur le comportement, tels que les systèmes d'analyse du comportement des utilisateurs et des entités (UEBA), de détection et de réponse sur les points de terminaison (EDR), et d'analyse du trafic réseau (NTA) ».

Des catégories bien distinctes

Dans la première catégorie, le cabinet mentionne par exemple Securonix, LightCyber, Exabeam et Gurucul. Le premier étant notamment utilisé par HP au sein du système de gestion des informations et des événements de sécurité (SIEM) ArcSight. Pour l'EDR, il prend pour exemples Hexis et Ziften, mais pourrait également évoquer SentinelOne, notamment. En matière de NTA, le cabinet fait référence à SS8 et Niara, mais il faut également compter avec Vectra Networks ou encore Darktrace, entre autres.

Mais voilà, comme le relèvent les deux analystes, les acheteurs de solutions de sécurité ne veulent pas seulement détecter les brèches, « mais aussi y répondre rapidement et efficacement ». S'il le fallait, l'édition 2016 de RSA Conference a fait la démonstration de cette tendance. Ce besoin doit conduire à une « collision du marché entre systèmes de détection basés sur le comportement et systèmes d'orchestration et de réaction ». Et cela parce que ni UEBA, ni EDR, ni NTA ne semble en mesure d'apporter, seul, une réponse complète aux besoins des entreprises.

Des capacités différentes

Ainsi, Avivah Litan et Eric Ahlm soulignent que la première catégorie est efficace pour identifier des compromissions de comptes utilisateurs ou des acteurs internes malveillants, mais peut montrer ses limites dans la détection des incidents impliquant des logiciels malveillants. De son côté, « l'EDR peut être efficace pour trouver les comportements mauvais sur un hôte et identifier les objets malicieux », mais plus faible lorsqu'il s'agit de mettre le doigt sur une menace interne. Enfin, les outils de NTA « peuvent être capables de trouver les conséquences de deux types d'événements, mais n'ont pas les données relatives aux utilisateurs ou aux hôtes nécessaires pour confirmer l'incident ».

Analyse comportementale : la clé de la sécurité ?

D'autres outils peuvent venir en outre compléter l'édifice, qu'il s'agisse des SIEM ou des systèmes de gestion du renseignement sur les menaces comme ceux d'Anomali, de ThreatConnect ou encore de ThreatQuotient. Au final, pour les analystes de Gartner, le marché s'avère « bruyant, chaotique et encombré », pollué notamment par des discours marketing qui s'articulent « autour des mêmes thèmes clés tels que analytique, machine learning, automatisation, et autres termes similaires, bien que leur application de ces fonctionnalités soit largement différente en ce qui concerne ce qu'ils peuvent faire dans leurs rôles spécifiques ». Bref, la confusion règne.

Des performances à démontrer

Et cela d'autant plus que, selon Gartner, les spécialistes de l'analytique appliquée à la sécurité peinent encore à faire la démonstration de la valeur de leurs solutions. Lors d'échanges, ceux-ci cherchent surtout à se différentier en évoquant l'étendue ou le volume de leurs échantillons de données, le framework analytique utilisé ou encore la technologie analytique employée – apprentissage machine, deep learning, et intelligence artificielle sont là largement mis à contribution. Las, si le cabinet voit là des « facteurs importants et des sujets de discussions divertissants », tous « échouent à constituer un différentiateur majeur » car, pour Avivah Litan et Eric Alhm, « les éditeurs devraient d'abord se concentrer sur la manière dont le recours à l'analytique rend leur technologie meilleure en termes de résultats, de manière mesurable. Par exemple, dans quelle mesure trouver des attaques inconnues est plus efficace en pourcentage avec l'analytique que chercher à trouver un logiciel malveillant inconnu sans ».

Une inéluctable consolidation

Pour autant, les deux analystes ne contestent pas la valeur intrinsèque que l'analytique apporte à la détection de brèches. Mais ils soulignent l'importance des étapes suivant la détection. D'où la convergence anticipée entre acteurs de la détection basée sur l'analytique et de l'orchestration/réaction. Et c'est peut-être là que le SIEM est appelé à jouer une nouvelle carte, pour dépasser des limites bien connues. Dès lors, pour Gartner, les acteurs de détection devaient « soit prévoir de nouer formellement des partenariats avec des acteurs du SIEM […] ou se préparer à reprendre des fonctions clés du SIEM ».

Le cabinet s'attend donc clairement à une consolidation prochaine de systèmes de détection de menaces basés sur les comportements, mais il n'exclue pas l'émergence de solutions de type plateforme dédiées à l'investigation et à la réponse aux incidents. Des solutions sur lesquelles les composant de détection et de réponse viendraient se greffer. Et n'est-ce pas justement ce que cherche à proposer un Phantom Cyber ?

Article de Valéry Marchive

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 : *L'adoption de l'analyse comportementale appelée à s'étendre*

Sensibilisation aux arnaques aux petites annonces

Sensibilisation aux arnaques aux petites annonces

Vous feriez confiance à cet homme ? Sur Internet aussi, soyez vigilants: il arrive que des acheteurs ou vendeurs malhonnêtes essaient de vous arnaquer. Découvrez les bons réflexes sécurité avec PayPal. Acheter et vendre en ligne est simple et sécurisé avec PayPal, 7 millions de Français nous utilisent déjà.

Campagne Paypal France 2016

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

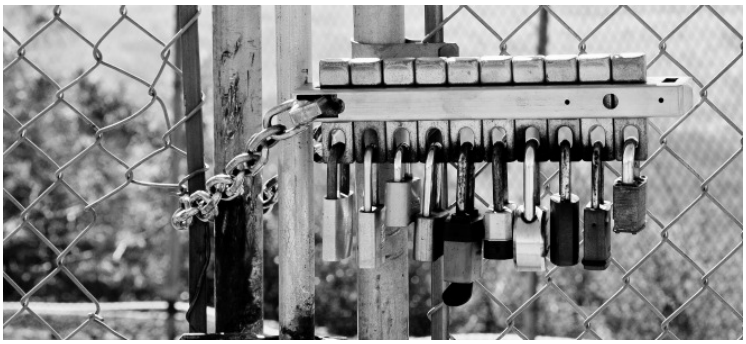
Réagissez à cet article

La sensibilisation des

salariés à la Cybersécurité est essentielle

La sensibilisation des salariés à la Cybersécurité est essentielle

Bonne nouvelle : selon une étude menée par Solucom/Conscio Technologies et relayée par Les Échos, 82% des salariés sont sensibles aux risques informatiques et aux risques de vols d'informations. Mieux, 75% disent en avoir une bonne connaissance…. Des données intéressantes lorsque l'on sait que les failles de sécurité sont le plus souvent le fruit d'une négligence voire d'une malveillance humaine.



Une prise de conscience insuffisante ?

Si 88% des salariés disent être sensibilisés à l'enjeu de sécurité des mots de passe, dans les faits, ils ne sont que 47% à adopter les bonnes pratiques en la matière !
Parfois, les bonnes pratiques en elles-mêmes sont méconnues : 61% des salariés ne savent pas quoi faire à la réception d'un e-mail envoyé sous fausse identité, alors qu'ils sont 72% à se dire *sensibles* à la problématique.
On le voit, il y a un véritable enjeu pour les employeurs et les services IT : **mieux évangéliser, et ce de manière très concrète** pour que les salariés changent leurs comportements.

Quand implication et investissement vont de pair…

Un problème, donc, de communication en interne… Et, aussi, de moyens ? D'après une autre étude mentionnée par Les Échos, deux-tiers des responsables de service informatique considèrent que les budgets alloués par leur entreprise à la cybersécurité sont insuffisants.
=> L'étude, vue par Les Échos

Une formation infdispensable

Formation informatique cybercriminalité : Virus, arnaques et piratages informatiques, risques et solutions pour nos entreprises | Denis JACOPINI

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 : *Cybersécurité : appuyez-vous sur vos salariés ! | Microsoft pour les PME*

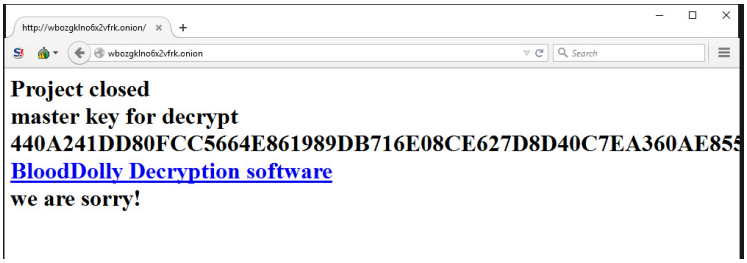
Victime du ransomware TelsaCrypt ? Voici finalement la clé de déchiffrement

Victime du ransomware TelsaCrypt ? Voici finalement la clé de déchiffrement

Les auteurs du ransomware TeslaCrypt ont décidé de réparer leurs méfaits en fournissant gracieusement la clé qui permet aux victimes du logiciel d'extorsion de reprendre le contrôle sur leurs données.

Les maître-chanteurs des temps modernes auraient-ils aussi parfois une conscience, qui se réveille tardivement ? Depuis de nombreux mois, des groupes de délinquants anonymes inondaient des systèmes informatiques d'un ransomware basé sur le framework TeslaCrypt, à l'action hélas désormais bien connue. La victime se retrouvait avec tous ses fichiers et documents personnels chiffrés sur son disque dur, et le seul moyen de les déchiffrer pour y avoir de nouveau accès était de payer une rançon, en suivant les instructions affichées à l'écran. Mais l'auteur (ou les auteurs ?) de TeslaCrypt a décidé de faire amende honorable.

L'éditeur de logiciels de sécurité ESET avait en effet remarqué que les créateurs de TeslaCrypt avaient choisi de mettre fin à leur projet maléfique. Prenant leur audace à deux mains, les ingénieurs du groupe ont donc contacté les créateurs de TeslaCrypt en passant par le service d'assistance intégré au ransomware, et leur ont demandé s'ils accepteraient de publier la « master key » qui permettrait à toutes les victimes de déchiffrer leurs fichiers sans payer un centime.
À leur propre surprise, les pirates ont accepté. La clé est désormais visible sur le site du groupe (accessible uniquement en passant par Tor).



« *Nous sommes désolés* », peut-on lire sur ce site, qui donne également le lien vers un outil de déchiffrement mis au point par BloodDolly, présenté par BleepingComputer comme un « expert de TeslaCrypt ». Il avait déjà proposé un outil gratuit pour déchiffrer les fichiers bloqués par TeslaCrypt 1.0, mais la communication de la clé maître permet désormais à l'outil de déchiffrer y compris TeslaCrypt 3.0 et TeslaCrypt 4.0. ESET a également publié son propre outil gratuit.
L'histoire ne dit pas pourquoi les auteurs du ransomware ont été pris de remords… [Lire la suite]

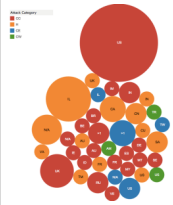
Réagissez à cet article

Source : *Les auteurs du ransomware TelsaCrypt s'excusent et offrent la clé – Tech – Numerama*

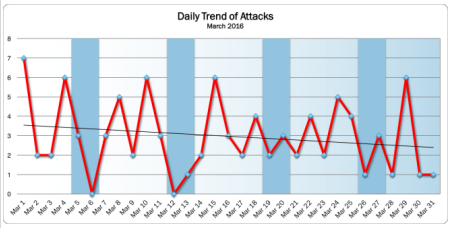
April 2015 Cyber Attacks Statistics – HACKMAGEDDON

Météo des cyberattaques de mars 2016

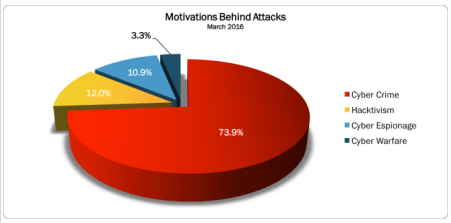
Afin de vous tenir informé de la météo des cyberattaques, nous avons souhaité partager avec vous l'étude récemment parue sur l'état des lieux des cyberattaques pour le mois de mars 2016 .



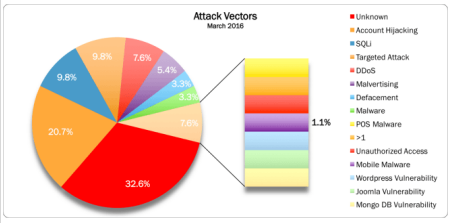
I finally found the time to aggregate the data of the timelines of March (part I and part II) into statistics.
As usual let's start from the **Daily Trend of Attacks**, which shows quite a sustained level of activity throughout the entire month, most of all during the first half.



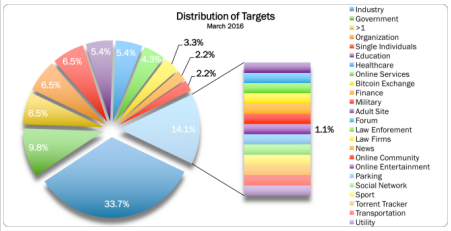
Cyber Crime ranks on top of the **Motivations Behind Attacks** chart with a noticeable 73.9%, a sharp increase compared with 62.7% of February. On the other hand hacktivists seem to have taken a temporary period of vacation in March (maybe due to the beginning of Spring), since Hacktivism reduces its 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.



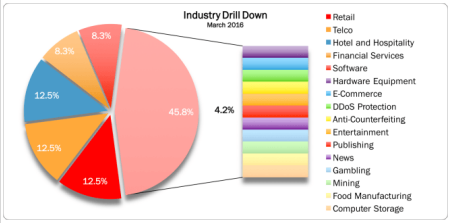
In the 32.6% of the cases the **Attack Vectors** are unknown. Account Hijackings rank at number one among the known attack vectors with 20.7% (was 12%, this growth is the effect of the numerous BEC and tax return scams reported in March). SQLi, an evergreen, confirms its momentum with 9.8% (was 10.7%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

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

Retrouvrer les traces d’une attaque informatique peut s’avérer complexe et coûteuse

---

Selon l'un des principes fondamentaux de la police scientifique, sur une scène de crime, tout contact laisse une trace. Dans l'univers de la cybercriminalité, chercher les traces pour remonter le fil des événements jusqu'à l'auteur de l'attaque, se révèle souvent compliqué.

Lorsqu'un incident survient, il est généralement difficile pour l'entreprise de définir qui a accédé à son système d'information et ce que cette personne – ou groupe de personnes – a fait. La tâche se complique encore un peu plus lorsque cet incident provient d'utilisateurs internes bénéficiant d'un haut niveau de privilèges sur le système – voire même de la personne en charge de prévenir les attaques sur le réseau.
Que l'incident soit le résultat d'une action malveillante d'un utilisateur interne, d'une erreur humaine ou d'une faille, dès lors que l'entreprise n'est pas capable de remonter les informations, elle passe à côté de preuves cruciales, et rend l'enquête beaucoup plus longue et onéreuse.

Le facteur temps : la clé de la réussite
Dans toutes investigations post-incident de sécurité, le temps est un facteur crucial. Pour mener à bien une enquête, il est plus facile, plus précis et généralement moins couteux de conduire une analyse criminalistique, dite forensics, poussée immédiatement, plutôt que plusieurs semaines voire plusieurs mois après l'incident.
L'examen approfondi des logs : remonter les étapes d'une attaque
Lorsqu'une faille est avérée, l'entreprise dépend des logs générés par les terminaux et les applications sur le réseau, pour déterminer la cause initiale et remonter les étapes de l'attaque. En pratique, trier les informations peut prendre des jours – en d'autres termes, cela revient à chercher une aiguille dans une botte de foin.
L'intégrité des logs : le respect du standard des preuves
Si les logs ont été modifiés et qu'ils ne peuvent pas être présentés dans leur format original, l'intégrité des données de logs peut être remise en question lors d'une procédure légale. Les logs doivent respecter le standard légal des preuves, en étant collectés de manière inviolable. A contrario, les logs qui ont été modifiés ou qui n'ont pas été stockés de manière sécurisée, ne seront pas acceptés comme preuve légale dans une cour de justice.
Cependant, même pour les organisations qui ont implémenté des solutions fiables de collecte et de gestion des logs, l'information cruciale peut manquer et ce chainon manquant peut empêcher l'entreprise de reconstituer tout le cheminement de l'incident et ainsi de retrouver la source initiale du problème.

Les comptes à privilèges : une cible fructueuse pour les cybercriminels
En ciblant les administrateurs du réseau et autres comptes à privilèges qui disposent de droits d'accès étendus, voire sans aucune restriction au système d'information, aux bases de données, et aux couches applicatives, les cybercriminels s'octroient le pouvoir de détruire, de manipuler ou de voler les données les plus sensibles de l'entreprise (financières, clients, personnelles, etc.).

L'analyse comportementale : un rempart nouveau pour les entreprises
Les nouvelles approches de sécurité basées sur la surveillance des utilisateurs et l'analyse comportementale permettent aux entreprises d'analyser l'activité de chacun des utilisateurs, et notamment les événements malveillants, dans l'intégralité du réseau étendu.
Ces nouvelles technologies permettent aux entreprises de tracer et de visualiser l'activité des utilisateurs en temps réel pour comprendre ce qu'il se passe sur leur réseau. Si l'entreprise est victime d'une coupure informatique imprévue, d'une fuite de données ou encore d'une manipulation malveillante de base de données, les circonstances de l'événement sont immédiatement disponibles dans le journal d'audit, et la cause de l'incident peut être identifiée rapidement.
Ces journaux d'audit, lorsqu'ils sont horodatés, chiffrés et signés, fournissent non seulement des preuves recevables légalement dans le cadre d'une procédure judiciaire, mais ils assurent à l'entreprise la possibilité d'identifier la cause d'un incident grâce à l'analyse des données de logs.
Lorsque ces journaux sont complétés par de l'analyse comportementale, cela offre à l'entreprise une capacité à mener des investigations forensics beaucoup plus rapidement et à moindre coût, tout en répondant pro activement aux dernières menaces en temps réel… [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 Liberté) ;
- 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

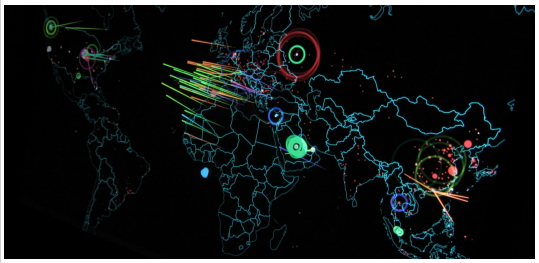
Réagissez à cet article

Source : *Recouvrer les traces d'une attaque informatique : l'investigation peut s'avérer complexe et coûteuse – JDN*

A quoi doit-on s'attendre en matière de cybersécurité à l'horizon 2020 ?

A quoi doit-on s'attendre en matière de cybersécurité à l'horizon 2020 ?

A l'heure où les objets connectés continuent de se déployer et où les piratages de données personnelles ou professionnelles se multiplient, quel avenir peut-on envisager en termes de cybersécurité ? Un groupe de chercheurs a élaboré plusieurs scénarios.



Le Centre pour la cybersécurité à long terme, un groupe de chercheurs pluridisciplinaires de l'Université de Berkeley en Californie, s'est questionné sur ce possible avenir en fonction de divers paramètres (déploiement de l'IoT, avancées technologiques, initiatives politiques, etc.). Et selon eux, plusieurs scénarios émergent :

• The New Normal décrit un monde où les cyberattaques à grande ou petite échelle seront, en 2020, autant légion que personnelles, dépassant les pouvoirs publics par leur nombre et leur ampleur, et encombrant les cours de justice de dossiers liés à la criminalité digitale – une sorte de « Far West 2.0 » dans lequel les utilisateurs n'hésiteraient pas à se rendre justice par eux-mêmes ;

• Omega conte, quant à lui, le futur de l'analyse prédictive : bien au-delà des études démographiques, la nouvelle génération d'algorithmes pourrait cibler plus étroitement les caractéristiques et préférences d'un individu donné, ce qui pourrait introduire un débat des plus clivants, à la frontière du philosophique et du politique, sur la manipulation comportementale ;

• Sensorium, enfin, dépeint l'évolution du *quantified self* jusqu'à faire d'Internet un vaste système de « lecteurs d'émotions », comme le souligne The Conversation, touchant du doigt les aspects les plus intimes de la psychologie humaine. Au risque que les données des applications de *quantified self* émotionnelles puissent être « retournées » contre leurs utilisateurs.

Plus d'informations et plus de scénarios ici.

Réagissez à cet article

Source : *Quel avenir pour la cybersécurité à l'horizon 2020 ?*