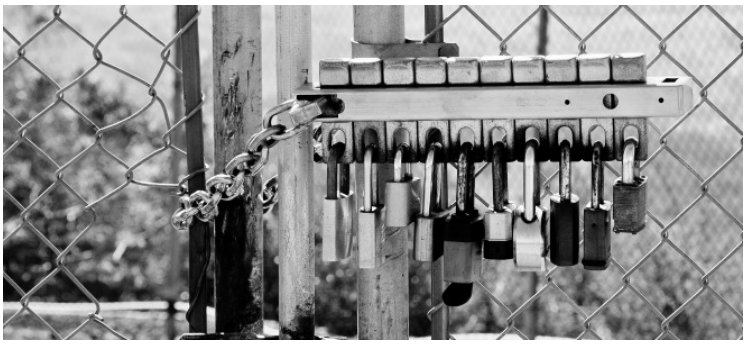
La sensibilisation des salariés à la Cybersécurité est essentielle

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*

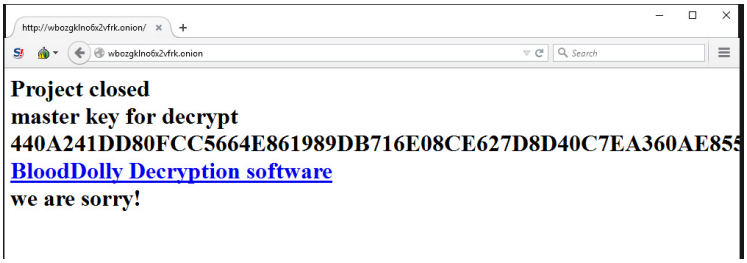
Victime du ransomware TelsaCrypt ? Voici finalement la clé de déchiffrement

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*

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 1000 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 le 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]

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

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

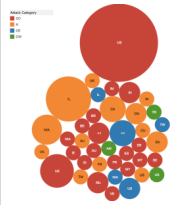
Source : *Conficker : un virus de 8 ans toujours vivace ! –*

ZDNet

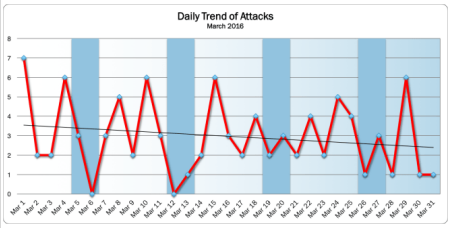
April 2015 Cyber Attacks Statistics – HACKMAGEDDON

	**Météo des cyberattaques de mars 2016**

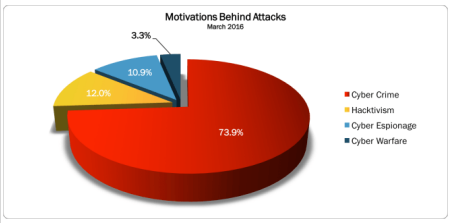
Afin de vous tenir informé de la météo des cyberattaques, nous avons souhaité partager avec vous l'étude récemment parue sur l'état des lieux des cyberattaques pour le mois de mars 2016 .



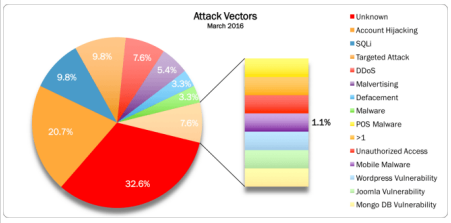
I finally found the time to aggregate the data of the timelines of March (part I and part II) into statistics.
As usual let's start from the **Daily Trend of Attacks**, which shows quite a sustained level of activity throughout the entire month, most of all during the first half.



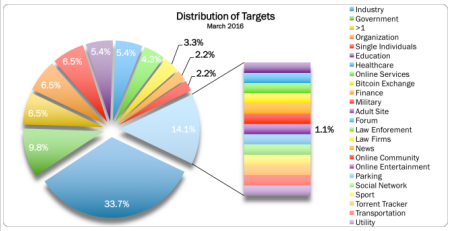
Cyber Crime ranks on top of the **Motivations Behind Attacks** chart with a noticeable 73.9%, a sharp increase compared with 62.7% of February. On the other hand hacktivists seem to have taken a temporary period of vacation in March (maybe due to the beginning of Spring), since Hacktivism reduces its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



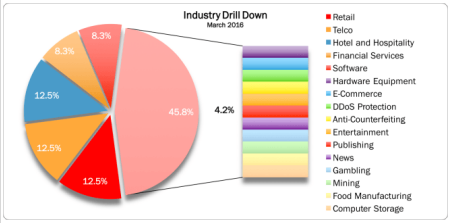
In the 32.6% of the cases the **Attack Vectors** are unknown. Account Hijackings rank at number one among the known attack vectors with 20.7% (was 12%, this growth is the effect of the numerous BEC and tax return scams reported in March). SQLi, an evergreen, confirms its momentum with 9.8% (was 10.7%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

Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage

Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage

---

Lorsque Microsoft a abandonné Windows XP en 2014, on pouvait alors découvrir que 95% des distributeurs de billets de banque tournaient encore sous cette version obsolète de l'OS, devenant ainsi vulnérables au piratage. En 2016, rien n'a changé et les banque comme les constructeurs ne semblent pas décidés à faire le nécessaire.

Lorsque Microsoft a abandonné Windows XP en 2014, la menace de piratage est devenue de plus en plus grande pour les distributeurs de billets. Pourtant, fin 2015, **95% d'entre eux** tournaient encore sous cette version obsolète du système d'exploitation. On dénombre d'ailleurs pas moins de 9000 risques de sécurité sur ces machines. Pourtant les banques semblent s'en laver les mains, pourquoi ?
Comme l'explique Alexey Osipov, ingénieur chez Kaspersky, les constructeurs de distributeurs automatiques ont très peu de concurrents et les banques sont sous contrat avec eux, ils ne font donc pas l'effort de prendre les mesures suffisantes pour sécuriser leurs machines.
Pour Olga Kochetova, également ingénieur chez Kaspersky après avoir travaillé plusieurs années sur le marché des distributeurs bancaires, la réponse est encore plus simple. Ces machines étant désormais trop vieilles pour faire tourner des versions plus récentes et sécurisées de Windows, elles nécessitent donc d'être remplacées, or « **l'investissement serait trop coûteux** ». En outre, ça impliquerait aussi d'embaucher un nouveau personnel mieux formé vis à vis des nouveaux risques de piratage.

Il faut dire que pour un hacker, pirater un distributeur de billet est d'une simplicité enfantine puisqu'il suffit d'acheter une clé sur internet pour se connecter physiquement aux machines. Ils prennent ainsi tout simplement le contrôle du DAB pour lui réclamer la somme qu'ils souhaitent. L'an dernier, une attaque massive baptisée « Carbanak » avait fait perdre plus de **10 millions de dollars** à différentes banques situées un peu partout dans le monde… [Lire la suite]

Réagissez à cet article

Source : *Pourquoi 95% des distributeurs de billets sont encore vulnérables au piratage*

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

Top 10 des arnaques sur Facebook en 2014

Top 10 des arnaques sur Facebook en 2014

Une étude des analystes antivirus Bitdefender révèle que Taylor Swift n'est plus aussi populaire que l'année dernière, lorsqu'une fausse vidéo à son sujet avait permis de répandre massivement un malware sur le réseau social. Chaque année, des millions d'utilisateurs tombent dans les pièges des arnaques diffusées sur Facebook. Voici le classement des 10 arnaques les plus répandues dans le monde, depuis le début de l'année 2014 !

1. **Qui a visité mon profil**– 30.20% (anglais – international)
2. **Changez la couleur de votre Facebook** – 7.38% (anglais – international)
3. **La sextape de Rihanna avec « son » petit-ami**– 4.76% (anglais – international)
4. **Consultez mon nouveau statut pour recevoir gratuitement un T-shirt officiel Facebook** – 4.21% (anglais – international)
5. **Dites au revoir au Facebook bleu**– 2.76% (français)
6. **Produits défilmés. Distribution gratuite**– 2.41% (anglais – international)
7. **Vérifiez si un ami vous a supprimé de sa liste** – 2.27% (anglais – international)
8. **Cliquez ici pour voir le top 10 des profils qui vous harcèlent le plus ! Vous serez étonné d'apprendre que votre ex visite toujours votre profil !** – 1.74% (anglais – international)
9. **Découvre comment voir qui visite ton profil, tu n'es pas au bout de tes surprises !** – 1.55% (espagnol)
10. **Je viens de modifier le thème de mon Facebook. C'est incroyable**– 1.50% (anglais – international)

Autres : 41.22%

Alors que Taylor Swift quitte le Top 10, **Rihanna reste la star la plus utilisée en tant qu'« appât »** par les scammers pour répandre un malware via Facebook.
L'arnaque des billets "gratuits" pour Disneyland sort aussi du classement alors qu'en juillet dernier, elle surclassait l'arnaque « Je peux vérifier qui regarde mon profil » qui avait fait des dizaines de milliers de victimes. Le scam « **Qui a visité mon profil » conserve quant à lui sa 1ère place**, représentant presque un tiers de la part totale des arnaques sur Facebook (30.20%).
Les arnaques du type « changez la couleur de votre Facebook » se sont internationalisées et représentent dorénavant **7,38 % de la part totale des scams sur Facebook** (vs 4.16% en 2013).

Les mêmes arnaques Facebook fonctionnent toujours

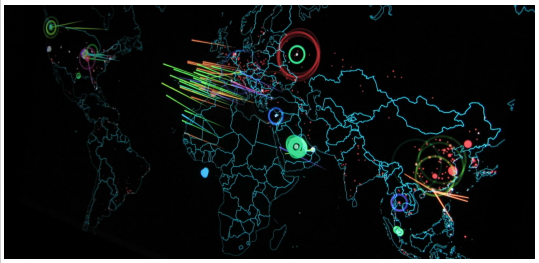
« Pourquoi les utilisateurs veulent-ils toujours savoir qui a jeté un coup d'œil à leur profil, malgré tous les avertissements de sécurité à ce sujet ? » déclare Catalin Cosoi, Responsable de la Stratégie de sécurité chez Bitdefender. *« Ils pensent certainement qu'il s'agit de vraies applications… C'est ce que l'on appelle de l'ingénierie sociale, et elle atteint alors son plus haut niveau – un jeu psychologique entre le cybercriminel et sa victime. Les appâts ont changé avec le temps – harceleurs, voyeurs, admirateurs, petites amies trop attachées et ex qui vous hantent, mais la raison pour laquelle ces arnaques fonctionnent est simple : la nature humaine. »*
Une offre de **T-shirts Facebook gratuits** fait son entrée dans le Top 10 (4.21 %). Les fans intéressés par des vêtements à l'effigie de la marque américaine se retrouvent à remplir de **fausses études ou à installer des add-ons malveillants** qui exploitent leurs données personnelles.
L'autre nouveauté de ce classement concerne des arnaques qui piègent les utilisateurs avec des **cadeaux publicitaires défilmés** (2,41 %).
Au cours de ces deux dernières années, les **arnaques sur Facebook se sont multipliées** en même temps que la plate-forme de réseau social s'est développée. L'étude Bitdefender montre aussi une augmentation du nombre d'arnaques via des **vidéos virales qui utilisent de façon abusive les *"Like"*** Facebook et les options de partage. L'année passée, les sites frauduleux utilisant le **likejacking** (détournement de « *J'aime*«), **clickjacking** (détournement de liens) et **YouTube** ont proliféré en anglais mais aussi en allemand, chinois et en italien.
Pour éviter d'être détectés plus facilement, les scammers peuvent utiliser des caractères spéciaux et numéros dans la description de leur fausse application. Une **variante populaire du scam « Top profil visiteurs »** attire de nouvelles victimes avec ce message : *"Check 0ut n0w wh0 viewed ur profile"*.
Cette étude se base sur les données issues de l'outil Safego de Bitdefender, l'application Facebook gratuite qui scanne les timelines et alerte les utilisateurs en cas de posts malveillants et frauduleux. Pour plus d'informations sur la protection de vos comptes utilisateurs de médias sociaux, vous pouvez consulter le guide de sécurité de Bitdefender à ce sujet… [Lire la suite]

Source : *Fausses sextapes et arnaques diverses : le top 10 des scams en 2014 sur Facebook*

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 ?*