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

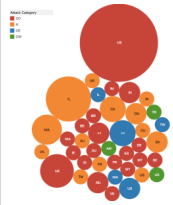
Source : *Conficker : un virus de 8 ans toujours vivace ! –*

ZDNet

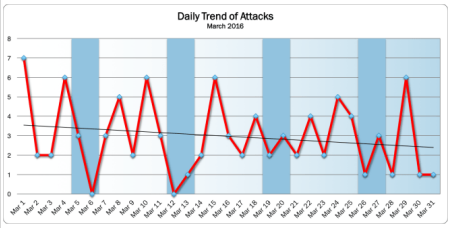
April 2015 Cyber Attacks Statistics – HACKMAGEDDON

	**Météo des cyberattaques de mars 2016**

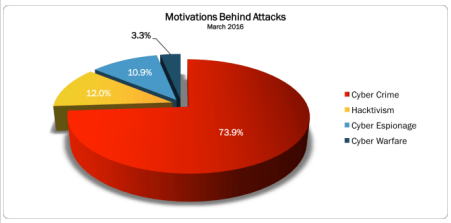
Afin de vous tenir informé de la météo des cyberattaques, nous avons souhaité partager avec vous l'étude récemment parue sur l'état des lieux des cyberattaques pour le mois de mars 2016 .



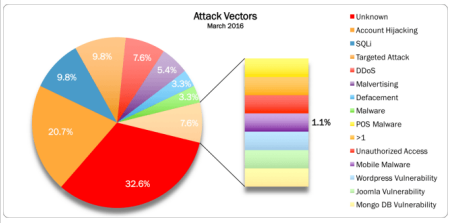
I finally found the time to aggregate the data of the timelines of March (part I and part II) into statistics.
As usual let's start from the **Daily Trend of Attacks**, which shows quite a sustained level of activity throughout the entire month, most of all during the first half.



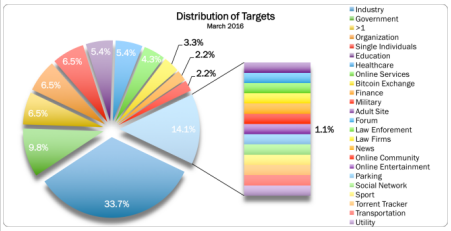
Cyber Crime ranks on top of the **Motivations Behind Attacks** chart with a noticeable 73.9%, a sharp increase compared with 62.7% of February. On the other hand hacktivists seem to have taken a temporary period of vacation in March (maybe due to the beginning of Spring), since Hacktivism reduces its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



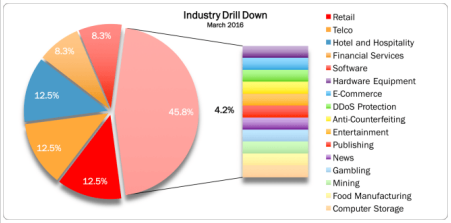
In the 32.6% of the cases the **Attack Vectors** are unknown. Account Hijackings rank at number one among the known attack vectors with 20.7% (was 12%, this growth is the effect of the numerous BEC and tax return scams reported in March). SQLi, an evergreen, confirms its momentum with 9.8% (was 10.7%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

Windows 10 Mobile acceptera l’empreinte digitale comme moyen d’authentification cet été

Windows 10 Mobile acceptera l’empreinte digitale comme moyen d’authentification cet été

La version mobile de Windows 10 gagnera bientôt la compatibilité avec les lecteurs d'empreinte digitale déjà exploités par Android et iOS.

Selon *Engadget*, Microsoft en a fait l'annonce aujourd'hui dans le cadre de la conférence WinHEC. Alors qu'il était déjà possible de déverrouiller son téléphone Windows grâce à la reconnaissance faciale du système, la lecture d'empreinte digitale pourra également être employée.

Pour en bénéficier, il faudra attendre que les fabricants de téléphones Windows ajoutent le lecteur en question.

Ainsi, Windows Hello gagnera cette fonctionnalité dans la mise à jour anniversaire de Windows 10 Mobile dont le déploiement est prévu pour juillet prochain.

Bien entendu, pour en bénéficier, il faudra attendre que les fabricants de téléphones Windows ajoutent le lecteur en question. Pour le moment, seul l'Elite X3 de HP – un téléphone Windows toujours en développement destiné pour le marché des affaires et promettant d'agir comme un ordinateur portable – intègre un lecteur d'empreinte digitale… [Lire la suite]

Réagissez à cet article

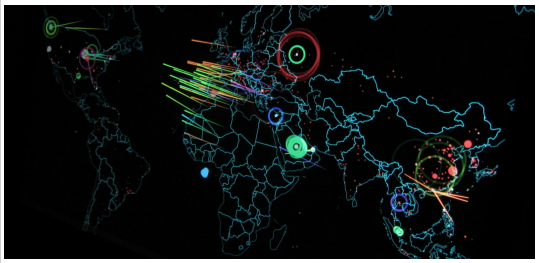
Source : *Windows 10 Mobile acceptera l'empreinte digitale comme moyen d'authentification cet été | Branchez-vous*

Laurent LASALLE

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.

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

Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016

Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016

La 8e édition du IT-Forum (Forum des décideurs et acteurs des Technologies de l'Information) se déroulera les 2 et 3 juin prochain à Abidjan.

IT FORUM 8ème EDITION

Des conférences seront animées en plénières par des spécialistes, des Experts-Consultants et des Universitaires. Ce sera le lieu de faire des exposés, de partager des expériences, de former et d'informer les participants.
Les enjeux de la transformation numérique et plus globalement de l'appropriation des nouvelles technologies modifient considérablement notre mode de vie. La sécurisation des données et des dispositifs de paiement comporte des failles qu'il comporte d'améliorer pour apporter la confiance nécessaire au climat des affaires.
De nombreuses études viennent conforter ce constat et tendent à démontrer le potentiel de croissance du secteur.
En Côte d'Ivoire, les transactions mobiles s'élèvent à 15 milliards de FCFA par jour soit 22,5 millions d'Euros.
Des montants qui donnent le vertige et qui poussent les sites marchands notamment les opérateurs de télécommunications à prendre des mesures de sécurité de plus en plus importantes… mais qui montrent aussi rapidement leurs limites !
Au fil des années, la Côte d'Ivoire s'est imposée comme l'un des leaders naturels dans le domaine des transactions mobiles en Afrique.
En insistant sur la priorité à donner à la protection des données et des transactions (mobile banking, eCommerce),
Devenu un rendez-vous incontournable depuis une décennie, l'IT Forum s'impose aujourd'hui comme l'une des
rencontres les plus importantes.
QUAND
Jeudi 2 juin 2016 à 08:00 – Vendredi 3 juin 2016 à 18:00 (Heure : Côte d'Ivoire) – Ajouter au calendrier
LIEU
Maison de l'entreprise – CGECI (Confédération Générale des Entreprises de Côte d'Ivoire – Patronat ivoirien), Avenue Lamblin, Abidjan, Lagunes, Côte d'Ivoire, Abidjan, Plateau, Cote d'Ivoire –
PROGRAMME
http://www.ciomag-event.com/8eme-edition-it-forum-cote-d-ivoire

---

Réagissez à cet article

Sources :

IT-Forum 2016 – 8e édition du Forum des décideurs et acteurs des Technologies de l'Information

http://it-forum.ci

https://www.eventbrite.fr/e/inscription-it-forum-2016-8eme-edition-24951266911

Combien vous coûterait le piratage de vos données ?

Combien vous coûterait le piratage de vos données ?

Un consommateur français sur trois reconnaît que sa loyauté envers une marque diminue après qu'une attaque informatique a porté atteinte aux données qu'il lui avait confié.

Souvent préparées de longues dates, les attaques informatiques qui frappent les entreprises laissent des traces longtemps après.
Publiée aujourd'hui, une étude internationale menée par Vanson Bourne, pour l'éditeur de logiciels de cybersécurité FireEye, souligne que les conséquences de tels épisodes entament la performance commerciale de la société victime, au-delà des dégâts informatiques des premiers jours. « *La sécurité des systèmes d'information a un réel impact sur la confiance des consommateurs* », affirme Yogi Chandiramani, directeur des ventes en Europe pour FireEye.
« *En France, l'attaque qui a touché TV5 Monde en avril 2015 et les vols de données chez Orange en 2014 ont particulièrement marqué les esprits* », poursuit-il. 34 % des consommateurs français reconnaissent que leur loyauté en tant que client actuel ou potentiel d'une marque diminue après qu'une entreprise a laissé fuiter des données, pointe le questionnaire en ligne envoyé à 1.000 d'entre eux. Un argument de plus pour ceux qui voient les efforts de cyber-sécurité comme un argument de compétitivité .
L'atteinte à leurs données personnelles refroidit particulièrement les ardeurs à l'achat des consommateurs. Quand le vol de données est connu, plus de trois Français sur quatre déclarent qu'ils stopperaient leurs emplettes de produits ou services fournis par la victime, surtout si la faute vient de l'équipe dirigeante – ils sont plus conciliants s'il s'agit de l'erreur humaine d'un subordonné. La tendance se confirme au fil des années. D'après l'étude, 61 % des Français déclarent avoir pris en considération la sécurité de leurs données lors de leurs achats en 2015. Ils n'étaient que 53% dans cet état d'esprit en 2014…

Après une cyber-attaque, la transparence prime

A cette perte de chiffre d'affaires potentiel s'ajoute le risque de poursuite en justice. La moitié des Français déclarent qu'ils engageraient des poursuites contre l'entreprise cyber-attaquée qui n'a pas su protéger leurs données personnelles, volées ou utilisées à des fins criminelles. Aux Etats-Unis, Target et Sony Picture s ont été attaqués en Justice par des procédures de class action, le premier par ses clients, le second par ses salariés.
Dès lors, la tentation peut être grande pour une entreprise de garder secret le fait que son système d'information ait été vulnérable à des cyber-criminels. Ce serait pourtant aggraver le mal qui surviendra au moment où, inévitablement à l'heure d'Internet, l'information ressortira.
« *Les consommateurs pointent les négligences des entreprises mais attendent surtout d'elles de la transparence, 93 % d'entre eux souhaitent être prévenus dans les 24h quand leurs données sont exposées* », prévient Yogi Chandiramani.

Des changements dans quelques mois ?

Le règlement européen sur la protection des données, qui devrait s'appliquer en France d'ici 2018, prévoit d'imposer aux sociétés de notifier les autorités, voir leurs clients, de toutes atteintes sur les données personnelles des citoyens européens dans les 72h après la découverte du problème.
A noter :
L'attaque particulièrement destructrice qui a touché TV5Monde en 2015 devrait coûter près de 10 millions d'euros sur trois ans, uniquement en réparation informatique… [Lire la suite]

Réagissez à cet article

Source : *Cyber-attaque : les coûts d'après, Cybersécurité – Les Echos Business*

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ?

Aux États-Unis, une affaire judiciaire pose la question du droit que peuvent avoir les autorités judiciaires à contraindre un suspect à débloquer son iPhone avec le capteur Touch ID qui permet d'accéder au contenu du téléphone avec les empreintes digitales.

La question s'est certainement déjà posée dans les commissariats et dans les bureaux des juges d'instruction, et elle devrait devenir plus pressant encore dans les années à venir : alors qu'un suspect peut toujours prétendre avoir oublié son mot de passe, ou refuser de répondre, les enquêteurs peuvent-ils contraindre un individu à débloquer son téléphone lorsque celui-ci est déblocable avec une simple empreinte digitale ?
Le débat sera tranché aux États-Unis par un tribunal de Los Angeles. Le Los Angeles Times rapporte en effet qu'un juge a délivré un mandat de perquisition à des policiers, qui leur donne le pouvoir de contraindre physiquement la petite amie d'un membre d'un gang arménien à mettre son doigt sur le capteur Touch ID de son iPhone, pour en débloquer le contenu.

Le mandat signé 45 minutes après son placement en détention provisoire a été mis en œuvre dans les heures qui ont suivi. Le temps était très court, peut-être en raison de l'urgence du dossier lui-même, mais aussi car l'iPhone dispose d'une sécurité qui fait qu'au bout de 48 heures sans être débloqué, il n'est plus possible d'utiliser l'empreinte digitale pour accéder aux données. Mais l'admissibilité des preuves ainsi collectées reste sujette à caution et fait l'objet d'un débat entre juristes.

EN MONTRANT QUE VOUS AVEZ OUVERT LE TÉLÉPHONE, VOUS DÉMONTREZ QUE VOUS AVEZ CONTRÔLE SUR LUI
Certains considèrent qu'obliger un individu à placer son doigt sur le capteur d'empreintes digitales de son iPhone pour y gagner l'accès revient à forcer cette personne à fournir elle-même les éléments de sa propre incrimination, ce qui est contraire à la Constitution américaine et aux traités internationaux de protection des droits de l'homme. « En montrant que vous avez ouvert le téléphone, vous montrez que vous avez contrôle sur lui », estime ainsi Susan Brenner, une professeur de droit de l'Université de Dayton. Le capteur Touch ID ne sert pas uniquement à débloquer le téléphone, mais aussi à le déchiffrer, en fournissant une clé qui joue le rôle d'authentifiant du contenu.
D'autres estiment qu'il s'agit ni plus ou moins que la même chose qu'une perquisition à domicile réalisée en utilisant la clé portée sur lui par le suspect, ce qui est chose courante et ne fait pas l'objet de protestations. Ils n'y voient pas non plus de violation du droit de garder le silence, puisque le suspect ne parle pas en ne faisant que poser son doigt sur un capteur.

ET EN FRANCE ?
Pour le moment, le sujet n'est pas venu sur la scène législative en France. Mais il pourrait y venir par analogie avec d'autres techniques d'identification biométrique.
En matière de recherche d'empreintes digitales ou de prélèvement de cheveux pour comparaison, l'article 55-1 du code de procédure pénale punit d'un an de prison et 15 000 euros d'amende « le refus, par une personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une infraction, de se soumettre aux opérations de prélèvement ». De même en matière de prélèvements ADN, le code de procédure pénale autorise les policiers à exiger qu'un prélèvement biologique soit effectué sur un suspect, et « le fait de refuser de se soumettre au prélèvement biologique est puni d'un an d'emprisonnement et 30 000 euros d'amende ».
Sans loi spécifique, les policiers peuvent aussi tenter de se reposer sur les dispositions anti-chiffrement du code pénal, puisque l'empreinte digitale sert de clé. L'article 434-15-2 du code pénal punit de 3 ans de prison et 45 000 euros d'amende le fait, « pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en oeuvre, sur les réquisitions de ces autorités ». Mais à notre connaissance, elle n'a jamais été appliquée pour forcer un suspect à fournir lui-même ses clés de chiffrement, ce qui serait potentiellement contraire aux conventions de protection des droits de l'homme… [Lire la suite]

Réagissez à cet article

Source : *La police peut-elle obliger un suspect à débloquer son iPhone avec son doigt ? – Politique – Numerama*