Sputnik France visé par une cyberattaque

Sputnik France visé par une cyberattaque

Le 25 décembre, une attaque de type DDoS a fait bloquer l'accès au fil d'actualités Sputnik France. Les spécialistes techniques sont en train de régler le problème d'accès au site.

Les attaques par déni de service (Distributed Denial of Service ou DDoS) sont aujourd'hui fréquentes, notamment du fait de la relative simplicité de leur mise en exécution et de leur efficacité contre une cible non préparée. Une attaque DDoS vise à envoyer une multitude de requêtes à un serveur afin de provoquer un déni de service, c'est à dire un arrêt total du service attaqué.

Ce n'est pas la première fois que Sputnik est victime d'une telle attaque. Le 7 décembre dernier, le site de Sputnik Turquie a été attaqué par des pirates informatiques. En octobre 2015, les fils d'actualité de l'agence russe Rossiya Segodnya, et notamment ceux de Sputnik, avaient été bloqués.

Réagissez à cet article

Source : *Sputnik France à nouveau visé par une cyberattaque*

Les juges antiterroristes veulent recourir à des hackers

Les juges antiterroristes veulent recourir à des hackers

Interrogé par les sénateurs, le vice-président chargé de l'instruction à la section antiterroriste du TGI de Paris a demandé que les magistrats puissent recourir à des « experts » (comprendre des hackers) pour installer des mouchards sur les ordinateurs de suspects, puisque l'État ne veut pas fournir ses propres outils utilisés par les services de renseignement.

Interrogé par les sénateurs, le vice-président chargé de l'instruction à la section antiterroriste du TGI de Paris a demandé que les magistrats puissent recourir à des « experts » (comprendre des hackers) pour installer des mouchards sur les ordinateurs de suspects, puisque l'État ne veut pas fournir ses propres outils utilisés par les services de renseignement.
Le Sénat conduisait le 9 décembre dernier différentes auditions à huis clos dans le cadre du Comité de suivi de l'état d'urgence, mis en place pour s'assurer que l'État n'abuse pas des pouvoirs spéciaux confiés à la suite des attentats du 13 novembre 2015, et pour tirer des enseignements sur les pratiques et les obstacles rencontrés par les spécialistes de l'anti-terrorisme. Le Sénat a rendu public le compte-rendu d'audition, qui permet d'en savoir plus sur les attentes des juges.
Les sénateurs ont en effet entendu David Bénichou, le vice-président chargé de l'instruction à la section antiterroriste et atteintes à la sûreté de l'État au tribunal de grande instance de Paris. Celui-ci a vivement critiqué le manque de moyens des juges pour prévenir les actes de terrorisme, en demandant que les magistrats disposent de pouvoirs légaux et de moyens technologiques beaucoup plus proches de ceux dont disposent la police et en particulier les services de renseignement.

Une justice antiterroriste sert-elle à compter les morts ?

Alors que le rôle premier de la police est traditionnellement d'empêcher la commission des infractions, et le rôle de la justice est de les punir, M. Bénichou réfute l'opposition. « Une justice antiterroriste sert-elle à entraver des attentats ou à compter les morts en offrant à leurs auteurs une tribune, et à leur payer un avocat ? », a-t-il lancé. « Nous préférons prévenir les attentats. Pour cela, il nous faut des moyens opérationnels, performants et actualisés ».
Le magistrat a ainsi formulé deux demandes principales. Tout d'abord, il souhaite que les juges puissent saisir les e-mails archivés des suspects dans le cadre d'enquêtes préliminaires, sans que les personnes concernées soient prévenues. Actuellement les juges doivent se contenter de mettre sur écoute les boîtes emails des suspects pour collecter les correspondances reçues ou envoyées à un instant T, mais ils ne peuvent pas collecter ce qui a été émis ou reçu dans le passé (ce qu'a rappelé la cour de cassation le 8 juillet 2015). Le seul moyen d'obtenir copie des e-mails passés est de réaliser une perquisition, ce qui en droit oblige à prévenir le suspect qu'il fait l'objet d'une enquête, et à lui faire assister à la perquisition.
Ensuite, le magistrat demande à pouvoir installer des mouchards informatiques chez les suspects. En théorie cette capacité à capter à distance des données grâce à un dispositif installé localement (clé USB ou autre) ou injecté par une attaque informatique existe déjà en droit, depuis la loi Loppsi de 2011. Elle autorise les juges d'instruction à faire « mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par saisie de caractères ».

Recourir à des hackers ou aux services de l'État

Mais dans les faits, comme nous l'avions déjà signalé en 2013, les juges n'ont pas accès aux outils théoriques. Les services de l'Agence nationale de sécurité des systèmes d'information (ANSSI) doivent en effet homologuer les outils mais selon le juge Bénichou, seuls deux outils ont été validés depuis 2011, et pour une raison inconnue, « le ministère de la justice ne les a toujours pas mis à notre disposition ».
« Les services de renseignement monopolisent les outils et ne les mettent pas à notre disposition, par crainte de les voir divulgués. Ils ont pourtant une durée de vie très courte », regrette le magistrat antiterroriste.
David Bénichou demande donc que les juges antiterroristes puissent faire appel à des « experts » extérieurs pour développer de tels outils, c'est-à-dire à des hackers à qui le magistrat passerait commande en fonction des besoins du moment. « Un amendement du Sénat autorisant le juge à commettre un expert pour développer un outil a malheureusement été retiré, le ministre de l'intérieur invoquant la sécurité du système d'information de l'administration », rappelle le juge.

Les services de renseignement monopolisent les outils

Or, « contrairement au contre-espionnage, la lutte contre le terrorisme est avant tout un problème judiciaire : nous avons un besoin opérationnel constant de ces éléments ». « C'est pourquoi je vous suggère de redéposer cet amendement », a-t-il demandé aux sénateurs.
Depuis 2014, la loi autorise potentiellement la police judiciaire à faire appel à des hackers, mais uniquement dans un cadre de perquisitions pour obtenir l'accès à des données chiffrées ou inaccessibles sur le matériel saisi. L'article 57-1 du code de procédure pénale permet en effet aux officiers de la PJ de « requérir toute personne susceptible d'avoir connaissance des mesures appliquées pour protéger les données auxquelles il est permis d'accéder dans le cadre de la perquisition » ou pour « leur remettre les informations permettant d'accéder aux données mentionnées ».
À défaut de pouvoir avoir accès à ces mêmes personnes dans le cadre de mises sur écoute ou de piratage à distance des données, le magistrat souhaite pouvoir recourir aux services du Centre Technique d'Assistance (CTA), qui sert déjà aux magistrats dans les affaires les plus graves, lorsqu'ils doivent déchiffrer un contenu saisi par les enquêteurs. Le CTA met à la disposition de la justice ses analystes et ses supercalculateurs pour décrypter les contenus, sans que la justice ne sache quels moyens techniques ont été utilisés pour obtenir la version en clair.

Réagissez à cet article

Source : *Les juges antiterroristes veulent recourir à des hackers – Politique – Numerama*

La Turquie victime d'une grosse cyberattaque

La Turquie victime d'une grosse cyberattaque

Les serveurs internet turcs subissent depuis lundi une vaste cyberattaque qui a notamment considérablement ralenti les services bancaires, a-t-on annoncé vendredi de source proche du gouvernement turc.

L'organisation non-gouvernementale Nic.tr, chargée d'administrer les adresses des sites internet utilisant le nom de domaine «.tr» qui englobe les ministères, l'armée, les banques et de très nombreux sites commerciaux, a indiqué dans un communiqué sur son site internet que l'offensive émane de «sources organisées» en-dehors de Turquie.
Le ministre des Transports et des Communications Binali Yildirim, cité par les journaux, a évoqué une situation «préoccupante» et demandé que soient renforcées les mesures de sécurité, qui, selon lui, se sont avérées «insuffisantes».

Attaque russe?
Certains médias turcs pensent que cette attaque pourrait provenir de Russie, Moscou et Ankara traversant une grave crise diplomatique depuis qu'un bombardier russe a été abattu par la chasse turque à la frontière syrienne, le 24 novembre.
Selon la presse turque, le groupe de piratage informatique des Anonymous a de son côté déclenché une guerre numérique contre la Turquie et annoncé qu'il continuerait à perpétrer des attaques contre les systèmes informatiques en raison du «soutien de la Turquie au groupe de l'Etat islamique (EI)».

Dans un communiqué, le groupe de pirates informatiques a écrit : «La Turquie soutient Daech en lui achetant du pétrole et en soignant ses combattants (…) Si vous ne cessez pas votre soutien à Daech, nous continuerons à procéder à des cyber-attaques contre la Turquie».

Les experts ont cependant indiqué que pour le moment on ignorait l'origine de cette puissante attaque.

Réagissez à cet article

Source : *20 Minutes Online – La Turquie victime d une cyberattaque massive – Stories*

Hyatt : encore une chaine d’hôtels prise pour cible par un logiciel malveillant

Hyatt : encore une chaine d’hôtels prise pour cible par un logiciel malveillant

La chaine d'hôtels Hyatt vient d'annoncer avoir découvert un logiciel malveillant dans son système de paiement. Il est désormais éradiqué, mais l'étendue des dégâts n'est pas connue. Hyatt n'est que le dernier d'une longue liste d'hôtels dont la sécurité a été mise à mal.

Alors que l'histoire de la porte dérobée dans les pare-feu de Juniper n'est pas encore terminée, une nouvelle affaire de sécurité informatique remonte à la surface. La chaine d'hôtels Hyatt vient en effet d'annoncer officiellement qu'elle a « identifié un logiciel malveillant sur les ordinateurs qui gèrent les systèmes de paiements ».

Le groupe ne donne pas d'informations supplémentaires sur les tenants et aboutissants de cette histoire, pas plus que sur le nombre de clients potentiellement touchés ou sur les données dérobées. Il est simplement demandé aux clients de scruter attentivement leurs relevés bancaires afin de vérifier qu'aucune transaction suspecte n'a été effectuée.

Bien évidemment, Hyatt ajoute avoir pris des mesures pour renforcer sa sécurité informatique (notamment avec l'aide d'une société spécialisée dans ce domaine) et indique que, désormais, ses « clients peuvent utiliser en toute confiance des cartes de paiement dans les hôtels Hyatt dans le monde entier ».
Mais il faut également rappeler que cette brèche dans la sécurité d'un hôtel n'est que la dernière d'une longue série pour 2015. En effet, il y a tout juste un mois, c'était la chaine Hilton qui annonçait avoir découvert un logiciel malveillant dans certains terminaux de paiements. Sur son blog, Krebs dresse une triste liste d'hôtels ayant fait face à une importante brèche dans leur sécurité informatique en 2015 : Starwood, Mandarin Oriental, White Lodgging et Trump Collection.

Réagissez à cet article

Source : *Hyatt : encore une chaine d'hôtels prise pour cible par un logiciel malveillant*

UFC Que Choisir a décidé de porter plainte contre VTech pour son piratage

UFC Que Choisir a décidé de porter plainte contre VTech pour son piratage

---

C’est arrivé, la plainte a été lancée par le groupe UFC Que Choisir contre la société VTech pour une affaire de piratage de jouets. Cette plainte pour « faute intolérable » a été déposée auprès du Tribunal de Grande Instance de Versailles.

C’est arrivé, la plainte a été lancée par le groupe UFC Que Choisir contre la société VTech pour une affaire de piratage de jouets.
Cette plainte pour « faute intolérable » a été déposée auprès du Tribunal de Grande Instance de Versailles. En effet, cette association des consommateurs estime que la société VTech met en danger les données de ses clients.

Des serveurs VTech piratés

La plainte déposée par l’association UFC Que Choisir est en rapport avec des serveurs piratés de la société de jouets VTech. En effet pour cette association de consommateurs, les données des clients n’ont pas bénéficier de la meilleure sécurité puisqu’un seul hacker a pu pirater les serveurs. Pas moins de six millions de clients ont vu leurs données totalement violées et notamment sur l’identification de leurs enfants. Sans oublier que VTech ne se serait aperçu de rien jusqu’à que la presse vienne l’interviewer.

Un problème survenu plus précisément aux Etats-Unis

Il faut cependant savoir que ce problème de piratage a d’abord touché les serveurs de la société VTech Américaine. Ce sont les clients des Etats-Unis qui ont été les plus touchés par ce piratage de données, même si la France n’est pas à exclure car elle détient la seconde place. En tout, VTech a sans hésitation confirmé que 868 650 comptes clients ont été piratés en se servant d’applications en ligne mais également de différents services pour accéder aux informations de plus d’un million d’enfants.
Une plainte des plus justifiées car de nombreuses photos d’enfants mais également des adresses et des numéros de téléphone ont été ainsi facilement obtenus par des hackers directement en ligne. VTech va devoir répondre pour cette bavure très grave.

Réagissez à cet article

Source : *Pour cause de piratage UFC Que Choisir a décidé de porter plainte contre VTech*

Bitdefender : Les 5 tendances en cybercriminalité pour 2016

Bitdefender : Les 5 tendances en cybercriminalité pour 2016

Bitdefender publie ses prévisions en matière de sécurité. Dans son rapport, Bitdefender énonce les cinq évolutions notables qui impacteront notre façon de travailler, de jouer et de se sociabiliser sur Internet, au cours de l'année prochaine.

L'année 2016 verra un changement majeur dans la façon dont opèrent les cybercriminels. Le domaine probablement le plus impacté par cette refonte sera celui des PUA, dont l'activité s'est déjà accrue sur des plates-formes telles que Mac OS X et Android.
Suite aux nombreuses fermetures de réseaux de machines zombies et arrestations en 2015, les nouveaux cybercriminels transiteront probablement vers des systèmes de monétisation publicitaire spécifiques aux adwares agressifs, plutôt que de développer de nouvelles souches de malwares. Si pour le moment les botnets constituent toujours une partie importante de l'écosystème de la cybercriminalité, nous assisterons à une augmentation de la sophistication des PUA et des programmes incluant plus de greywares à l'installation.

La publicité sur le Web va également évoluer : étant donné le taux d'adoption ainsi que la popularité des bloqueurs de publicités, les régies publicitaires chercheront à utiliser des mécanismes plus agressifs afin de contourner ces blocages.

Les APT abandonneront le facteur de longévité
Les entreprises et les institutions gouvernementales feront toujours face à des attaques de ce type tout au long de 2016. Cependant, les APT (Advanced Persistent Threats, menaces persistantes avancées) mettront l'accent sur l'obfuscation et la récolte d'informations plutôt que sur la longévité. Les pirates ne s'infiltreront sur le réseau de l'entreprise que quelques jours, voire quelques heures.
Le monde de l'entreprise connaîtra une augmentation des attaques ciblées et des bots fortement obfusqués, avec une courte durée de vie et des mises à jour fréquentes, estime Dragoş Gavriluţ, Chef d'équipe au sein des Laboratoires antimalwares de Bitdefender. La plupart de ces attaques se spécialiseront dans le vol d'informations.
Également, l'évolution latérale de l'infrastructure des fournisseurs de services Cloud ira de pair avec l'avènement d'outils permettant aux pirates de compromettre l'hyperviseur à partir d'une instance virtuelle et de passer d'une machine virtuelle à l'autre. Ce scénario est particulièrement dangereux dans des environnements de « mauvais voisinage », où un tiers mal intentionné serait amené à partager des ressources sur un système physique avec un fournisseur de services ou une entreprise légitimes.

Des malwares mobiles de plus en plus sophistiqués
Du côté des particuliers, les types de malware sous Android sont désormais globalement les mêmes que sous Windows. Alors que les rootkits sont en perte de vitesse sur Windows, ils vont probablement devenir monnaie courante sur Android et iOS, car les deux plates-formes sont de plus en plus complexes et offrent une large surface d'attaque, affirme Sorin Dudea, Chef de l'équipe de recherche antimalwares. De nouveaux malwares mobiles, aux comportements similaires à ceux des vers, ou un réseau botnet mobile géant, sont deux autres possibilités envisagées pour l'année prochaine, selon Viorel Canja, Responsable des Laboratoires antimalwares et antispam chez Bitdefender. Ces attaques pourraient être la conséquence de techniques d'ingénierie sociale ou de l'exploitation de vulnérabilités majeures (telles que Stagefright) sur des plates-formes non patchées.

L'Internet des Objets (IOT) et la vie privée
La façon dont nous gérons notre vie privée va aussi changer durant l'année 2016. En effet, les récents vols de données ont contribué à mettre une quantité importante d'informations personnelles en libre accès sur Internet, rendant ainsi le « doxing » (processus de compilation et d'agrégation des informations numériques sur les individus et leurs identités physiques) beaucoup plus facile pour des tiers.
Les objets connectés vont devenir de plus en plus répandus, donc plus attrayants pour les cybercriminels. Compte tenu de leur cycle de développement très court et des limites matérielles et logicielles inhérentes à ce type d'objet, de nombreuses failles de sécurité seront présentes et exploitables par les cybercriminels ; c'est pourquoi la plupart des objets connectés seront compromis en 2016, ajoute Bogdan Dumitru, Directeur des Technologies chez Bitdefender. Également, les réglementations de surveillance de type « Big Brother », que de plus en plus de pays essaient de mettre en place pour contrecarrer le terrorisme, déclencheront des conflits quant à la souveraineté des données et le contrôle de leur mode de chiffrement.

Les ransomwares deviennent multiplateformes
Les ransomwares sont probablement la menace la plus importante pour les internautes depuis 2014 et resteront l'un des plus importants vecteurs de cybercriminalité en 2016. Alors que certains pirates préfèrent l'approche du chiffrement de fichiers, certaines versions plus novatrices se concentreront sur le développement de « l'extortionware » (malware qui bloque les comptes de services en ligne ou expose les données personnelles aux yeux de tous sur Internet).
Les ransomwares visant Linux vont se complexifier et pourraient tirer parti des vulnérabilités connues dans le noyau du système d'exploitation pour pénétrer plus profondément dans le système de fichiers. Les botnets qui forcent les identifiants de connexion pour les systèmes de gestion de contenu pourraient aussi se développer. Ces identifiants pourraient être ensuite utilisés par les opérateurs de ransomwares visant Linux pour automatiser le chiffrement d'une partie importante d'Internet.
Enfin, les ransomwares chiffrant les fichiers s'étendront probablement aux systèmes sous Mac OS X, corrélant ainsi avec les travaux de Rafael Salema Marques et sa mise en garde illustrée autour de son 'proof of concept' malware nommé Mabouia. En effet, si le principe de conception de Mabouia reste pour le moment privé, il pourrait être créé par des cybercriminels enrichissant alors leurs offres orientées MaaS (Malware-As-A-Service).

Réagissez à cet article

Source : *Bitdefender : Les 5 tendances en cybercriminalité pour 2016 – Global Security Mag Online*

Vaincre les attaques DoS/DDoS

en temps réel

Vaincre les attaques DoS/DDoS en temps réel

La vulnérabilité des serveurs DNS des fournisseurs de services vis-à-vis des attaques DoS/DDoS est bien réelle et s'intensifie à un rythme effréné, mettant ainsi en péril l'expérience utilisateur des clients ainsi que la réputation des fournisseurs de services.

Les techniques actuelles visent à arrêter les attaques en dotant le site du fournisseur de matériel supplémentaire ou en identifiant le coupable caché dans le logiciel malveillant sur le site du client. Cependant, ces deux méthodes sont onéreuses et ne permettent de résoudre le problème que partiellement. La nouvelle approche consiste à intégrer la protection contre les attaques DoS/DDoS directement dans un serveur cache DNS à haute fiabilité et à contrecarrer l'attaque en temps réel au moment où elle pénètre dans l'infrastructure, la désamorçant avant même qu'elle n'affecte les performances ou le service.
Lire la suite…

Réagissez à cet article

Source : *InfoBlox*

Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi – metronews

Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi – metronews

Plus de 2 millions de personnes doivent recevoir ces jours-ci une prime de Noël de la part de la Caf et Pôle emploi. Des escrocs profitent de l'occasion pour envoyer de faux mail provenant soi-disant de ces organismes. Objectif : vous soutirer des données personnelles.

La prime de Noël est versée à partir de ce mercredi 16 décembre 2015. La période parfaite pour des cyber-escrocs de tenter de vous soutirer des informations personnelles en se faisant passer pour des administrations ou des grands organismes. Leur objectif : usurper votre identité voire se servir sur vos comptes bancaires.

La police nationale alerte en effet sur les faux mails prétendument envoyés par la Caf ou Pôle emploi, qui sont chargés de verser cette aide à plus de 2 millions de bénéficiaires. Cette technique est appelée phishing, ou hameçonnage. Pour mieux la reconnaître et donc ne pas tomber dans le piège, voici en quoi elle consiste et comment réagir :

Logos qui semblent vrais ⇒ Vous recevez un courrier électronique qui reprend les intitulés, les couleurs et les logos bien connus pour ne pas éveiller vos soupçons.

Liens vers des sites piégés ⇒ Ce mail mail comporte un lien ou une pièce jointe. En cliquant dessus, vous êtes redirigé sur un site piégé qui vous invite à saisir des données personnelles (login, mot de passe, numéro de compte client, coordonnées bancaires…) soi-disant pour confirmation ou une vérification.

Fautes d'orthographe ⇒ Ne cliquez pas si vous avez un doute. Un indice : ces faux messages comportent souvent des fautes d'orthographe. Sachez également qu'aucun opérateur ou organisme ne vous demande de venir vérifier sur leur site des informations confidentielles en vous les faisant retaper en ligne. Vous pouvez si vous le souhaitez signaler l'email douteux **ici** sur la plateforme Pharos.

Réagissez à cet article

Source : *Arnaque prime de Noël : attention aux faux mails de la Caf et Pôle emploi – metronews*

Un pirate soupçonné du piratage de VTech arrêté

Un pirate soupçonné du piratage de VTech arrêté

Un jeune homme de 21 ans soupçonné d'être à l'origine du piratage des 6,4 millions de comptes d'enfants et 4,9 millions de comptes d'adultes, clients du fabricant de jouets VTech a été interpellé par la police britannique.

Suite au piratage des données personnelles de 11,3 millions de comptes clients du fabricant de jouet VTech, le plus grand vol de données concernant des enfants, la police anglaise indique avoir procédé à l'arrestation d'un jeune homme de 21 ans, soupçonné d'être à l'origine du délit. L'unité de cybercriminalité régionale du sud-est du Royaume-Uni a en effet indiqué dans un communiqué de presse ce mardi qu'elle avait arrêté un homme dans la ville de Bracknell, soupçonné d'avoir accédé sans autorisation aux serveurs et aux données de VTech. La ville, située à l'ouest de Londres, est un vivier pour les entreprises de haute technologie.
« Nous en sommes encore aux premiers stades de l'enquête et il y a encore beaucoup de travail à faire », indique Craig Jones, chef de l'unité de cybercriminalité régionale. Plusieurs équipements informatiques ont été saisis par la police.
Basée à Hong Kong, la société VTech est spécialisée dans les jeux ludo-éducatifs et propose depuis plusieurs années des tablettes tactiles adaptées aux enfants. Début décembre, elle avait été obligée de révéler que les données personnelles stockées dans les comptes de 6,4 millions d'enfants et 4,9 millions adultes avaient été copiées. Près de la moitié des victimes vivent en Europe.

Réagissez à cet article
Source : http://www.lemondeinformatique.fr/actualites/lire-la-police-britannique-a-arrete-le-hacker-presume-des-clients-vtech-63293.html

12% des attaques DDoS menées

par des concurrents

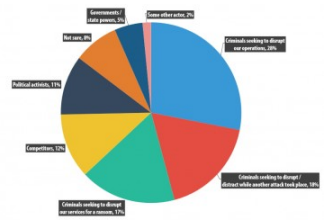
	12% des attaques DDoS menées par des concurrents

Selon Kaspersky, la volonté de nuire à un concurrent serait à l'origine de plus d'une attaque DDoS sur dix dans le monde.

Demande de rançon, tentative d'arrêt de l'activité, distraction pour opérer une pénétration du réseau… Kaspersky s'est notamment penché sur les motivations qui poussent les cybercriminels à lancer des attaques DDoS (Distributed Denial of Service) contre des entreprises.
L'éditeur de sécurité a mandaté le cabinet B2B International pour y voir plus clair dans ces motivations. Non pas en demandant aux responsables des attaques eux-mêmes mais à leur victimes. Soit auprès des responsables IT et dirigeants de plus de 5 500 entreprises de toutes tailles de 26 pays dans le monde.
Selon l'étude, il ressort que près de la moitié (48 %) des victimes d'une attaque par déni de service déclarent connaître les motivations, voire les identités, de leurs assaillants ou commanditaires. Sur cet ensemble, 12% des entreprises pensent que les attaques viennent de concurrents directs qui recourent éventuellement aux services d'organisations « spécialisées » dans ce genre d'opérations. Un chiffre qui monte à 38% dans le secteur des industries de services.

5% d'attaques gouvernementales

« Les attaques DDoS ne sont plus seulement l'œuvre de cyber-criminels qui cherchent à arrêter les opérations d'une entreprise, commente Evgeny Vigovsky, responsable de la division DDoS Protection chez Kaspersky. Les entreprises sont de plus en plus méfiantes les unes des autres et il y a une réelle préoccupation pour de nombreuses entreprises – y compris les petites et moyennes – d'être touchées par les tactiques sournoises de leurs concurrents, qui commissionnent des attaques DDoS directement contre eux, endommageant leurs opérations et leur réputation. »
Autre perception, 18% des attaques seraient menées pour focaliser les équipes IT afin de mener des tentatives de pénétration du réseau en parallèle. Un chiffre proche des 17% des répondants qui déclarent que les DDoS s'accompagnent de demandes de rançons, notamment auprès des fabricants et des acteurs de l'industrie des télécoms qui s'en disent victimes à hauteur de 27% chacun. 11% seraient visés par des activistes politiques et 5% proviendrait d'agressions étatiques/gouvernementales. Mais la majorité des attaques serait menée par des criminels qui chercheraient simplement à interrompre l'activité de l'entreprise. A des fins purement gratuites ?
On en doute…



Réagissez à cet article
Source : http://www.silicon.fr/12-des-attaques-ddos-menees-par-des-concurrents-133929.html