Le ministère de la Défense attaqué par des ‘Anonymous’

Le ministère de la Défense attaqué par des ‘Anonymous’

Le site Web du ministère de la Défense était inaccessible en raison d’une attaque en déni de service revendiquée par un groupe baptisé Anonymous OpGPII. Ils déclarent vouloir venger la mort du militant Rémi Fraisse.

Le site Internet du ministère de la Défense a fait l’objet hier 6 janvier d’une attaque informatique en déni de service, le rendant ainsi inaccessible aux internautes une bonne partie de la journée. « Le Centre d’analyse en lutte informatique défensive (Calid) est sur le coup » indiquait hier un porte-parole du ministère à 20Minutes.
Le DDoS a depuis été revendiqué sur Twitter par les membres d’un groupe se revendiquant d’Anonymous et baptisé « Anonymous OpGPII ». Ces derniers justifient cette attaque informatique par la mort du militant écologiste et opposant au barrage de Sivens, Rémi Fraisse, tué par une grenade des gendarmes le 25 octobre dernier. D’ailleurs pourquoi la Défense et non l’Intérieur dont dépend désormais la gendarmerie ?
« Aujourd’hui, nous commençons une opération pour le venger » déclarent des Anonymous dans un message mis en ligne sur le site Pastebin et repéré par le Figaro. « Pendant trop longtemps, Anonymous est resté à l’écart, nous n’avons pas pris de mesures. Mais maintenant, nous allons le faire » promettent-ils encore.
Un autre membre des Anonymous assurait cependant hier à 20 Minutes que le mouvement (jamais véritablement coordonné) n’était en rien responsable de l’attaque contre le ministère de la Défense. « Cela dit, cela fait des années qu’on leur a fait remarquer que leur site est truffé de failles » soulignait-il aussi.
De quoi permettre de futures attaques ? Une plainte pourrait en tout cas être déposée par le ministère, qui précise par ailleurs que deux adresses IP, liées au déni de service, ont été identifiées et signalées aux autorités.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/le-ministere-de-la-defense-attaque-par-des-anonymous-39812391.htm

---

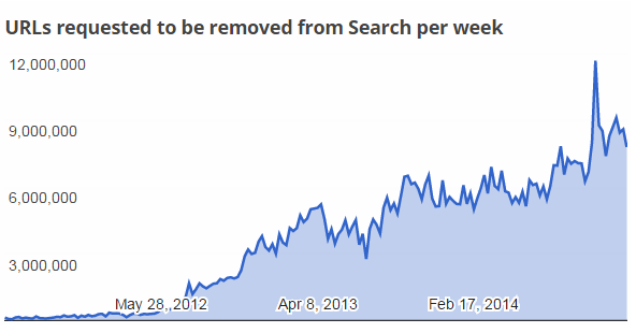
Google a retiré des millions

de pages Web de son moteur en 2014

Piratage, Google a retiré des millions de pages Web de son moteur en 2014

En 2014, Google a reçu plus de 345 millions de demandes de retrait de pages Web de son moteur de recherche au nom du droit d'auteur. C'est 75% de plus qu'en 2012 et cela devrait encore s'accélérer en 2015.

Les grandes organisations d'ayants droit ont à plusieurs reprises reproché à Google de ne pas en faire suffisamment pour lutter contre le téléchargement illégal sur Internet. Le géant s'est pourtant, en matière de déréférencement, montré particulièrement actif en 2014.
Selon les données compilées par Torrent Freak et extraites des rapports de transparence de la firme, Google a reçu l'année passée environ 345 millions de demandes de retrait de pages Web de son moteur de recherche. Des requêtes DMCA dans la grande majorité des cas satisfaites par Google qui procède donc à leur déréférencement.



Moins de 100 millions de demandes en 2012
Et si le nombre de ces demandes est élevé, il est aussi en très forte croissance sur un an, de l'ordre de 75%. La tendance n'est pas nouvelle, même si l'inflation du nombre de demandes de retrait est plus forte ces dernières années.

En mai 2012, Google recevait moins d'un million de requêtes DMCA par semaine de la part des ayants droit. En 2014, ce rythme a atteint puis dépassé les 6 millions par semaine. Une inflation à laquelle participe largement l'industrie musicale britannique qui au travers de la BPI représente plus de 60 millions des demandes de retrait adressées à Google en 2014, soit 17% du total.
Quant aux domaines les plus ciblés par ces accusations de violation du droit d'auteur, il s'agit, d'après TorrentFreak, de 4shared.com, rapidgator.net et uploaded.net, visés chacun par 5 millions de requêtes.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/piratage-google-a-retire-des-millions-de-pages-web-de-son-moteur-en-2014-39812271.htm

Attaquer des sites internet : Désormais un service comme un autre…

Attaquer des sites internet : Désormais un service comme un autre…

Les hackers de Lizard Squad vendent leurs services pour attaquer les sites

Faites-leur attaquer les sites concurrents
Vous aussi vous trouvez que GamAlive est un site qui mériterait d'être mis hors service ? Vous aussi vous estimez que nous dépassons trop souvent les bornes et que notre irréverence mérite un châtiment digne de ce nom ? Vous aussi vous pensez que nos moqueries répétées contre, au choix, les religions, les défenseurs des animaux, les végétariens, les porteurs de tongs, les racistes, les homophobes, les routiers et les fans de Sexion d'Assaut ne peuvent rester impunies, justement parce que vous êtes un pieux routier végétarien racite et homophobe qui défend les animaux et écoute Sexion d'Assaut dans son camion qu'il conduit avec des tongs ?

Ne cherchez plus et faites tomber le site GamAlive.
En effet, les Lizard Squad, ce groupe de hackers à l'origine des perturbations du PSN et du Xbox Live durant les fêtes de Noël, proposent désormais leurs services contre une modeste rétribution.
Ainsi, pour une somme allant de 6 à 500 dollars, vous pouvez vous offrir leurs services. Des attaques DDoS sont proposées contre les sites de votre choix. Des attaques d'une durée de 100 secondes à 30 000 secondes. Réparties sur plusieurs journées, elles peuvent aller jusqu'à bloquer un site pendant une vingtaine de jours, selon leurs dires.
Actuellement, seuls les bitcoins sont acceptés comme moyen de paiement, mais Paypal devrait prochainement être proposé aux clients intéressés par leurs services, même si on doute que le géant américain du paiement en ligne accepte de blanchir de l'argent issu de la cybercriminalité. Car on vous rappelle, au cas où vous seriez un peu con (comme un routier fan de Sexion d'Assaut qui conduit en tongs), que s'offrir leurs services est un acte illégal et répréhensible.

Et non, nous ne vous donnerons pas l'adresse du site, pour des raisons évidentes et, là aussi, légales.
Lire la suite….

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.gamalive.com/actus/23252-hackers-lizard-squad-services-payants-attaques-ddos-sites-propose.htm
Par Cedric Gasperini

En 2015, la cyberguerre va continuer à changer nos vies…

En 2015, la cyberguerre va continuer à changer nos vies…

En ce début d'année, Industrie & Technologies a repéré pour vous les 15 leviers qui vont booster l'innovation en 2015. Ils ne sont pas tous au même degré de maturité mais tous tireront la créativité et l'inventivité des centres de R&D. Aujourd'hui, la cybersécurité. Un sujet qui sera une préoccupation pour tous les industriels.

Pourquoi il faut la suivre :
Externalisation des données vers le cloud, BYOD et objets connectés, le développement de toutes ces nouvelles technologiques numériques inquiète les spécialistes de la cyber-sécurité. 2015 sera sans aucun doute l'année de la mise en place de dispositifs de défense (et d'attaques) pour permettre aux industriels de se défendre. Fin 2014, Symantec a d'ailleurs listé les principales menaces. Nous vous les présentons ici :

Les moyens de paiements électroniques en ligne de mire
Il est peu probable que des attaques à grande échelle similaires à celles qui ont ciblé les équipements de points de vente aux États-Unis se produisent en Europe. En effet, notre système de carte à puce associé à un code confidentiel ne facilite pas la récupération des données de carte bancaire. Cela dit, ces cartes à puce et à code confidentiel peuvent être subtilisées et utilisées pour effectuer des achats sur Internet. L'adoption grandissante des cartes de paiements sans contact, accompagnée du paiement sans contact via les mobiles, augmentera le risque d'attaques ponctuelles.

Les attaques de cyber-espionnage et de cyber-sabotage à prévoir
En 2015, les campagnes de cyber-espionnage et de cyber-sabotage financées par des États, telles que les opérations DragonFly et Turla observées en 2014, ou encore le spyware très récemment analysé et rendu public Regin, constitueront toujours des menaces pour la sécurité des infrastructures nationales et stratégiques dans le monde entier. Face à de telles campagnes visant à soutirer des renseignements et/ou à saboter des opérations, les entreprises et administrations devront revoir leur politique de cyber-sécurité et donner la priorité à la sécurité, qui deviendra un investissement stratégique plutôt que tactique.

Les secteurs publics et privés devront davantage collaborer pour lutter contre la cyber-criminalité
Fortes des différents démantèlements de groupes de cyber-criminels tels que les opérations Gameover Zeus, Cryptolocker ou encore Blackshades menées en 2014, les autorités internationales adoptent une approche plus active et plus agressive vis-à-vis de la cyber-criminalité en renforçant leur collaboration avec l'industrie de la sécurité en ligne. Cette collaboration entre le secteur privé et les forces de police se poursuivra en 2015 afin d'avoir un impact durable et de stopper les cyber-criminels dans leur élan.

De nouvelles réglementations pour les entreprises européennes
À l'heure où l'Europe souhaite appliquer sa nouvelle législation sur la protection des données, la confidentialité et l'utilisation des informations demeureront au centre des préoccupations en 2015. Contraintes de garantir le respect des nouvelles réglementations, mais aussi de suivre le rythme de l'économie mondiale en exploitant leurs énormes volumes de données pour créer de nouveaux services et de trouver d'autres sources de revenu, les entreprises européennes vont devoir relever un certain nombre de défis en 2015.

Les plates-formes open source seront le maillon faible
L'année 2015 apportera son lot de vulnérabilités dans les bases de données open source et les plates-formes de services Web, que les pirates exploiteront en toute impunité. À l'instar de Heartbleed et Shellshock, ces vulnérabilités constituent une cible potentiellement juteuse pour les pirates, le plus gros risque continuant d'être lié aux failles connues; entreprises et particuliers n'appliquent pas toujours les patchs correctifs appropriés.

L'Internet des objets restera l'Internet des vulnérabilités, mais les attaques seront limitées et ponctuelles
«L'Internet des objets» étant essentiellement lié à la génération de données, les cyber-criminels redoubleront d'imagination pour exploiter les failles logicielles des appareils connectés. Seront notamment concernés les technologies portatives, les équipements domestiques connectés, comme les téléviseurs connectés et les routeurs, et les applications automobiles connectées. Cela dit, nous ne devrions pas observer d'attaques à grande échelle sur l'Internet des objets, seulement des attaques ponctuelles.

Les organisations reconnaîtront que le système identifiant/mot de passe classique a ses limites
À une époque où les organisations cherchent des solutions pour prévenir les intrusions et protéger leurs utilisateurs, elles seront heureuses d'apprendre que des alternatives à l'ancien système se profilent à l'horizon. Notamment, l'authentification à deux facteurs, qui n'exige pas seulement une information que seul le véritable propriétaire connaît (mot de passe, etc.), mais aussi une information que lui seul est censé détenir (numéro de téléphone portable, etc.). Toutefois, alors que chaque service commence à prendre ce genre de mesures, le consommateur va devoir de plus en plus composer avec des applications, numéros de téléphone et questions de sécurité multiples (et ce sur différentes plates-formes), risquant ainsi de lui compliquer la tâche.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.industrie-techno.com/en-2015-pas-de-repit-sur-le-front-de-la-cyberguerre.35237

Vie privée, vie professionnelle, sommes-nous tous espionnés ? Reportage Zone Interdite

Vie privée, vie professionnelle, sommes-nous tous espionnés ? Reportage Zone Interdite

Avec le développement de la technologie, le monopole de la surveillance électronique n'est plus réservé à l'Etat : surveiller ses proches ou ses employés est devenu un jeu d'enfant.
Paul et Nicolas, deux maris, se livrent à l'espionnage conjugal. Ils ont installé des logiciels sur les téléphones portables de leurs épouses afin de suivre leurs conversations. Mais le danger vient aussi d'Internet, où les traces laissées sont très difficiles à contrôler. Des salariés ont ainsi été licenciés pour avoir critiqué leur patron sur Facebook. Cette tendance a parfois des conséquences tragiques. Aux Etats-Unis, Tyler Clementi, 18 ans, s'est donné la mort après avoir été filmé par ses colocataires. Au Royaume-Uni, des volontaires scrutent les images des caméras de surveillance pour dénoncer les infractions. Ils sont payés pour chaque alerte donnée.

Vie privée vie professionnelle sommes nous tous espionnés 1/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 2/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 3/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 4/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 5/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 6/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Vie privée vie professionnelle sommes nous tous espionnés 7/7.
Reportage diffusé sur M6 dans l'émission Zone Interdite le 10/04/2011.
Disponible sur YouTube en 7 parties.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.programme-tv.net/programme/culture-infos/r8841-zone-interdite/2703356-vie-privee-vie-professionnelle-sommes-nous-tous-espionnes/

Deux millions d’abonnés du site de TF1 piratés

Deux millions d’abonnés du site de TF1 piratés

Les données de deux millions d’abonnés du site de TF1 ont été piratées. Les hackers détiennent les RIB et autres informations sensibles de ces internautes.

Deux millions d’internautes menacés. Les abonnés du site de TF1 regarderont à deux fois avant de s’inscrire sur des plates-formes numériques. Deux millions d’entre eux ont en effet vu leurs données personnelles (RIB, mais aussi toutes les informations qui ont trait à l’identité numérique) piratées par des hackers vendredi. L’information, rapportée par RTL, a été révélée par Damien Bancal, un spécialiste en cybercriminalité qui a découvert ce piratage.

Techniquement, les hackers sont parvenus à attaquer la partie abonnement presse du site de TF1, sur laquelle il est possible de s’abonner à différents journaux. Une plate-forme que la chaîne privée ne gère pas directement, c’est un prestataire commercial externe qui assure son fonctionnement.

Des usurpations d’identités numériques possibles
Selon Damien Bancal, le spécialiste en cyber-criminalité, ce piratage de grande ampleur pourrait permettre aux hackers d’usurper l’identité des personnes inscrites sur le site. Cela pourrait également déboucher sur « une utilisation de ces données pour lancer d’autres escroqueries, aujourd’hui ou plus tard ».
Autre possibilité, cette base de données pourrait être vendue plusieurs milliers ou millions d’euros à d’autres cybercriminels. Les administrateurs du site ont quant à eux déjà corrigé la faille technique dans laquelle se sont engouffrés les pirates.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.europe1.fr/medias/tf1-piratage-de-masse-des-donnees-d-abonnes-2333529

Surveillance des internautes

– La loi valse sous haute discrétion

	Surveillance des internautes – La loi valse sous haute discrétion

Le 24 décembre, Matignon a publié un décret sur une mesure très contestée permettant aux agents de l'État de surveiller le Net français. Habile !C'est un cadeau de Noël dont les internautes et les opérateurs français se seraient bien passés. Le gouvernement a publié mercredi 24 décembre, à la faveur des fêtes de Noël, le décret d'application du très contesté article 20 de la loi de programmation militaire (LPM). Ce texte prévoit un accès très vaste des services de l'État aux télécommunications (téléphone, SMS, Internet, etc.) des Français, et à toutes les informations qui transitent par les réseaux nationaux.
La mesure de surveillance, pudiquement nommée « accès administratif aux données de connexion », avait été votée fin 2013 et entrera en vigueur le 1er janvier 2015. Dénichées par notre excellent confrère Next INpact (http://www.nextinpact.com/news/91534-le-decret-l-article-20-lpm-publie-on-fait-point.htm), qui évoque « un décret qui sent le sapin », ce sont les modalités de sa mise en oeuvre, tout aussi importantes, qui ont été dévoilées pour Noël.
Comme dans de nombreuses démocraties, le spectre terroriste permet au gouvernement de faire passer des mesures très floues et de tirer pleinement parti des systèmes d'information de plus en plus performants afin de surveiller la population.

Qui chapeaute le système ?
Le décret du 24 décembre présente « le groupement interministériel de contrôle […], un service du Premier ministre chargé des interceptions de sécurité et de l'accès administratif aux données de connexion ». Ce groupement est chargé de centraliser les demandes des agents et de les transmettre aux opérateurs concernés, en les épurant de toute information sensible.
En effet, si les services de l'État doivent justifier leurs requêtes auprès du Premier ministre (qui nomme une « personnalité qualifiée »), il est hors de question de transmettre ces explications aux opérateurs. Les fournisseurs d'accès ne sauront même pas de quel service ou ministère émane une demande, ni à quelle date elle a été formulée.

Quelles données sont concernées ?
Sans surprise, le décret se réfère à l'article 20 de la LPM, sans vraiment le préciser. Peuvent donc être interceptés les « informations ou documents traités ou conservés par les réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications ».
On notera l'utilisation de la formule « y compris », qui n'est aucunement exhaustive : difficile de faire plus vaste.

Un contrôle démocratique insignifiant
Face aux critiques sur l'intrusion dans la vie privée, le gouvernement invoque la Commission nationale de contrôle des interceptions de sécurité (CNCIS), un organe très joli sur le papier mais qui n'a jusqu'à présent pas été doté d'un réel pouvoir. Cette commission « dispose d'un accès permanent aux traitements automatisés », et « l'autorité ayant approuvé une demande de recueil d'informations ou de documents fournit à la commission tous les éclaircissements que celle-ci sollicite », promet le décret, plein de bons sentiments.

Néanmoins, la CNCIS **n'a toujours pas le pouvoir de sanction et ne peut même pas alerter la justice en cas de manquement sur un dossier couvert par le secret de la défense nationale**. Habile…

Par ailleurs, le gouvernement se protège en supprimant ses archives en un temps record. Si l'on peut saluer la suppression des informations et des fichiers recueillis au bout de trois ans, on ne peut être que surpris par le fait que les registres mentionnant qui a autorisé telle ou telle surveillance soient eux aussi « automatiquement effacés » après trois ans. Le seul contrôle démocratique possible lorsqu'on jongle avec le secret défense, celui qui s'effectue a posteriori, est donc rendu impossible, pour la CNCIS comme pour la justice.

À quel prix ?
« Les coûts supportés par les opérateurs pour la transmission des informations ou des documents font l'objet d'un remboursement par l'État », précise le décret. Pas un mot sur la grille tarifaire qui sera appliquée, car ils seront définis par les ministères concernés.

Qui peut demander les informations ?
Trois ministères sont habilités à émettre des demandes. Le décret détaille le nombre impressionnant de services pour lesquels les vannes du Web français sont ouvertes :

– Au ministère de l'Intérieur : la Direction générale de la sécurité intérieure (DGSI), la Direction générale de la police nationale (unité de coordination de la lutte antiterroriste, Direction centrale de la police judiciaire, Direction centrale de la sécurité publique, Direction centrale de la police aux frontières), la Direction générale de la gendarmerie nationale (sous-direction de la police judiciaire ; sous-direction de l'anticipation opérationnelle ; service technique de recherches judiciaires et de documentation ; sections de recherches), la préfecture de police (Direction du renseignement ; direction régionale de la police judiciaire ; service transversal d'agglomération des événements ; cellule de suivi du plan de lutte contre les bandes ; sûreté régionale des transports ; sûretés territoriales).

– Au ministère de la Défense : la Direction générale de la sécurité extérieure (DGSE), la Direction de la protection et de la sécurité de la défense, la Direction du renseignement militaire.

– Au ministère des Finances et des Comptes publics : la Direction nationale du renseignement et des enquêtes douanières, le service de traitement du renseignement et d'action contre les circuits financiers clandestins.

Dans tous ces services, seuls les agents et officiers « dûment habilités » par leur directeur pourront réclamer des informations, assure le décret.

Des perspectives inquiétantes
La loi de programmation militaire a mis en place un outil de surveillance de la population française qui aurait fait pâlir d'envie les pires dictateurs de l'histoire. Si nous sommes très loin d'un régime totalitaire en France, il n'est pas exclu que des leaders extrémistes disent demain merci au gouvernement Valls pour leur avoir fourni un tel outil clé en main.

Pour info :
Décret n° 2014-1576 du 24 décembre 2014 relatif à l'accès administratif aux données de connexion
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000029958091&dateTexte&categorieLien=id

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/le-cadeau-de-noel-du-gouvernement-aux-internautes-la-surveillance-26-12-2014-1892495_506.php
Par GUERRIC PONCET

La NSA pourrait avoir eut accès aux appels, messages, fichiers, vidéos échangés sur Skype, d'aprè

La NSA pourrait avoir eut accès aux appels, messages, fichiers, vidéos échangés sur Skype, d'après de récents documents

Newly published NSA documents show agency could grab all Skype traffic

A National Security Agency document published this week by the German news magazine Der Spiegel from the trove provided by former NSA contractor Edward Snowden shows that the agency had full access to voice, video, text messaging, and file sharing from targeted individuals over Microsoft's Skype service. The access, mandated by a Foreign Intelligence Surveillance Court warrant, was part of the NSA's PRISM program and allowed "sustained Skype collection" in real time from specific users identified by their Skype user names. The nature of the Skype data collection was spelled out in an NSA document dated August 2012 entitled "User's Guide for PRISM Skype Collection." The document details how to "task" the capture of voice communications from Skype by NSA's NUCLEON system, which allows for text searches against captured voice communications. It also discusses how to find text chat and other data sent between clients in NSA's PINWALE "digital network intelligence" database. The full capture of voice traffic began in February of 2011 for "Skype in" and "Skype out" calls—calls between a Skype user and a land line or cellphone through a gateway to the public switched telephone network (PSTN), captured through warranted taps into Microsoft's gateways. But in July of 2011, the NSA added the capability of capturing peer-to-peer Skype communications—meaning that the NSA gained the ability to capture peer-to-peer traffic and decrypt it using keys provided by Microsoft through the PRISM warrant request. The NSA was then able to "task" any Skype traffic that passed over networks it monitored or by exploitation of a targeted user's system. "NSA receives Skype collection via prism when one of the peers is a (FISA Amendments Act Section 702) tasked target," the Skype collection guide stated. Because Skype has no central servers, the guide explained, for multiparty calls, "Skype creates a mesh-network, where users are connected together through multiple peer-to-peer links. Instant Messages sent to this group of meshed participants can be routed through any participant." If any participant in a chat was monitored, the NSA could capture all of the IM traffic in the shared chat. Initially, NSA analysts had to piece together voice communications between peers because they were carried over separate streams, but a service added by August of 2012 by the NSA's Cryptanalysis and Exploitation Services (CES) automatically stitched both audio streams of a conversation together. As of 2012, however, analysts still had to search for associated video from a call session to match it up with audio in a tool called the Digital Network Intelligence Presenter (DNIP).
Après cette lecture, quel est votre avis ? Cliquez et laissez-nous un commentaire… Source : http://arstechnica.com/tech-policy/2014/12/newly-published-nsa-documents-show-agency-could-grab-all-skype-traffic/

Le groupe de Cybercriminels Rex Mundi fait chanter les sociétés belges

Le groupe de Cybercriminels Rex Mundi fait chanter les sociétés belges

Rex Mundi, le “roi du monde” en latin , un groupe de cybercriminels, est passé à l’action à la nouvelle année en republiant sur le Net des informations, parfois privées, sur des milliers de Belges.

Ces informations proviennent de treize sociétés ou filiales belges piratées au cours des derniers mois, dont Numéricable, Mensura, Domino’s Pizza, Thomas Cook, Finalease Car Credit, Buy Way et d’autres sociétés spécialisées dans l’intérim comme Tobasco et Z-Staffing.
L’information a été publiée sur le blog d’un expert en piratage, Len Lavens, puis relayée par “De Tijd”. “Ce qui prouve ce que j’ai déjà dit à la télévision : une fois sur le Web, toujours sur le Web”, a commenté l’expert.
Le piratage de ces sociétés n’est pas un fait nouveau, mais la diffusion des informations est, dans, certains cas, nouvelle. Les données ont été publiées sur la plateforme Tor, haut lieu de l’échange anonyme de données (NdlR, voir article ci-contre).
“Pour nous, cette affaire date de janvier 2013”, souligne Alain De Deken, de la société de crédit Buy Way. “Ils ont eu accès à des gens qui avaient fait une demande de crédit personnel sur Internet. Il s’agissait de 545 demandes. On a repéré la fuite, et elle a été colmatée.”
Buy Way affirme que les données volées n’ont qu’une valeur commerciale. Rex Mundi, qui s’inspire par sa devise des Templiers, a tenté de faire chanter la société, contre 20 000 euros, en menaçant de publier les données sur le Net, “mais on n’a pas donné suite”.
Rex Mundi opère depuis 2012 et a déjà à son actif plusieurs sociétés belges dont Dexia et Voo. Dans ce dernier cas, le pirate affirmait avoir saisi des données de près d’un demi-million de clients du câblodistributeur. La société a déposé plainte et assuré que ses clients n’avaient subi aucun préjudice. Pressée de questions par la RTBF, elle n’a ni démenti ni confirmé qu’elle avait payé une rançon pour sortir d’affaire. “Des entreprises ont payé. Je crois que c’est une erreur. Car le maître chanteur peut revenir”, juge Olivier Bogaert, de la Computer Crime Unit de la police fédérale.
A l’égard de Domino’s Pizza, une rançon de 30 000 euros avait été réclamée. La société a refusé, et ses informations ont été publiées sur le Net.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lalibre.be/economie/actualite/cybercriminalite-rex-mundi-fait-chanter-les-societes-belges-54a6e9b7357028b5e9d01b6d
Par Christophe Lamfalussy & P.V.C.

Tor sous la menace d’une attaque en mesure de corrompre l’anonymat des utilisateurs, les serveurs Directory Authorities dans le viseur

Tor sous la menace d’une attaque en mesure de corrompre l’anonymat des utilisateurs, les serveurs

Depuis les révélations d’Edward Snowden sur les pratiques d’espionnage de la NSA et du GHCQ, le réseau anonyme Tor a largement gagné en popularité, ce qui l’a rendu inévitablement le centre des convoitises des agences gouvernementales et la cible de plusieurs attaques.

C’est dans ce contexte que le directeur du projet Tor – Roger Dingledine – a annoncé que le réseau anonyme serait sous la menace d’une attaque informatique ou d’une procédure judiciaire dans les prochains jours.
Dans son billet de blog, Dingledine a tenu à rassurer les utilisateurs que des dispositifs techniques ont été pris pour assurer l’anonymat des utilisateurs, alors qu’ils seront notifiés en cas d’attaques dans les plus brefs délais via le blog et le compte Twitter du projet. De plus, la redondance de l’infrastructure du réseau devrait permettre le fonctionnement de Tor même en cas d’attaque selon le même responsable.
Toutefois, des réserves peuvent être émises quant à la capacité de Tor à résister à cette menace, en effet ladite attaque/procédure cible principalement les serveurs DA (Directory Authorities) via une attaque de type DDoS ou encore par la saisie des serveurs physiques, hors ces derniers qui sont au nombre limité de 10, jouent un rôle crucial dans l’anonymat du réseau, en mettant à disposition des utilisateurs une liste de relais potentiels qui seront par la suite utilisés pour débuter toute communication.
Ainsi, la perturbation du bon fonctionnement des serveurs DA devrait impacter le réseau, pire encore ces serveurs sont aussi responsables de la validation de la liste des relais utilisables, validation qui se fait chaque heure par l’aval de la majorité (au moins 5 serveurs), dès lors le contrôle d’au moins 5 serveurs DA permettrait à l’attaquant de réorienter le trafic vers des relais non sécurisés et déjà sous son emprise, ce qui pourrait signer le coup d’arrêt temporaire de tout le réseau Tor.
À noter aussi que les serveurs DA sont les premiers à être contactés par les utilisateurs, de ce fait leurs adresses IP sont inscrites en dur dans le code du client, ce qui limite le champ d’action et de riposte des responsables du projet.
Quant à la cause d’une telle entreprise, les spéculations vont bon train, allant même à affirmer que cela est relatif au récent piratage de Sony, même si aucune information n’a filtrée lors de l’annonce officielle.
Finalement, le mystère reste entier et les risques sont accrus pour les utilisateurs, ce qui laisse place à la vigilance et à la prudence comme étant les seules consignes en vigueur.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Sources :
http://www.developpez.com/actu/79522/Tor-sous-la-menace-d-une-attaque-en-mesure-de-corrompre-l-anonymat-des-utilisateurs-les-serveurs-Directory-Authorities-dans-le-viseur/
https://blog.torproject.org/blog/possible-upcoming-attempts-disable-tor-network
par Arsene Newman