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

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

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

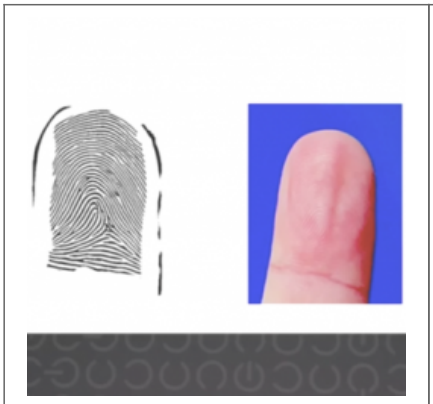
Depuis les révélations d’Edward Snowden sur les pratiques d’espionnage de la NSA et du GHCQ, le réseau anonyme Tor a largement gagné en popularité, ce qui l’a rendu inévitablement le centre des convoitises des agences gouvernementales et la cible de plusieurs attaques.

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

Un hacker parvient à reproduire des empreintes digitales à partir de photos



Un hacker parvient à reproduire des empreintes digitales à partir de photos

Il suffit de prendre la photo des doigts de la personne ciblée avec un appareil photo classique pour récupérer ses empreintes digitales.

On savait déjà quil était possible de récupérer les empreintes digitales d'une personne ayant touché une surface lisse, comme un verre ou un smartphone. Mais un hacker allemand a montré qu'il était possible de voler ces caractéristiques biométriques spécifiques à partir d'une simple photo.
Lors de la 31e convention annuelle (27-30 décembre, Hambourg, Allemagne) du Chaos Computer Club, la plus grande association de hackers européens, un hacker du nom de Jan Krissler, également connu sous le pseudonyme de « Starbug », a expliqué comment reproduire les empreintes digitales d'une personne à partir de simples photos.
Pour sa démonstration, il a copié l'empreinte de la ministre de la Défense allemande, Ursula Von der Leyen.
En effet, il suffit de prendre la photo des doigts de la personne ciblée avec un appareil photo classique pour récupérer ses empreintes digitales. Étant donné que ces empreintes peuvent être utilisées pour l'authentification biométrique, « Starbug » estime que sa démonstration va vraisemblablement obliger « les politiciens à porter des gants lors de leurs apparitions publiques ».
Pour réussir son exploit, Jan Krissler a utilisé le logiciel VeriFinger disponible dans le commerce. Comme source, il est reparti d'un gros plan du pouce de la ministre, pris lors d'une conférence de presse donnée en octobre dernier, plus d'autres photos prises sous des angles différents pour restituer une image complète de l'empreinte digitale.

Si la méthode est aussi facile à réaliser que ce qu'a montré le hacker, elle pourrait remettre en question l'usage des empreintes digitales pour la sécurisation de certains accès. Et dans ce cas, il faut garder ces options de détournement en mémoire. Mais, même si la reproduction des empreintes digitales s'avère viable pour forcer l'accès d'un système, aussi bien un smartphone qu'un lieu très sécurisé, l'exploit accompli par le hacker au 31C3 ne signifie pas pour autant que leur usage est devenu brusquement obsolète.
Les systèmes de sécurité parfaits n'existent pas, et les empreintes digitales ont encore leur place dans la sécurisation des systèmes. Dans un grand nombre de situations, on peut renforcer la sécurité en ajoutant des codes PIN, et il est toujours temps de coupler les solutions biométriques existantes avec des codes ou d'autres protections par mots de passe pour multiplier les niveaux de sécurité.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-un-hacker-parvient-a-reproduire-des-empreintes-digitales-a-partir-de-photos-59753.html
Par Jean Elyan

Les hackers iraniens montent en puissance

Les hackers iraniens montent en puissance

Les pirates informatiques iraniens montent en puissance et ont déjà dérobé des données « hautement sensibles » lors d'attaques contre des gouvernements et des entreprises aux Etats-Unis, en Chine ou en France, affirme aujourd'hui une société américaine de cyber-sécurité. « A mesure que les capacités de l'Iran en matière de cyber-attaque se transforment, la probabilité d'une attaque qui aurait un impact dans le monde réel, à un niveau national ou mondial, augmente très rapidement », met en garde Cylance.

Selon son rapport, l'opération « Cleaver » menée depuis deux ans par des hackers basés à Téhéran leur a déjà permis de conduire une « importante campagne d'infiltration et de surveillance » dans une longue liste de pays qui compte également Israël, l'Arabie Saoudite, l'Allemagne ou l'Inde. Leurs attaques ont ciblé les gouvernements mais également les entreprises du secteur militaire ou pétrolier ainsi que des infrastructures stratégiques (aéroports, hôpitaux…), énumère la société qui affirme avoir des « preuves » que la sécurité aérienne a été par exemple particulièrement « compromise » en Corée du Sud et au Pakistan.

« Les capacités techniques de l'opération Cleaver évoluent plus vite que toutes les précédentes tentatives iraniennes », assure Cylance, selon qui cette offensive répond aux cyber-attaques subies par Téhéran en provenance d'Israël ou des Etats-Unis et visant son programme nucléaire controversé. L'attaque du virus informatique « Stuxnet », qui avait frappé l'Iran vers 2010-2011, aurait ainsi « ouvert les yeux » des autorités de Téhéran en révélant leur vulnérabilité et les a conduits à « contre-attaquer » en lançant l'opération « Cleaver », explique le rapport, selon qui le soutien du régime à cette offensive ne fait aucun doute.

Plusieurs grandes entreprises américaines, dont Apple ou la banque JPMorgan ont récemment été victimes de cyber-attaques dont l'origine n'a pas été formellement identifiée, suscitant des mises en garde croissantes des autorités.

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

Source : http://www.lefigaro.fr/flash-actu/2014/12/03/97001-20141203FILWWW00452-les-hackers-iraniens-montent-en-puissance.php
Par Gilbert Kallenborn

Arrestation de braqueurs dans la zone ACI au Mali : «Big Brother» est passé par là

Arrestation de braqueurs dans la zone ACI au Mali : «Big Brother» est passé par là

Ils sont de plus en plus jeunes et stupides puisque incapables d'évaluer les risques liés à l'objet de leurs forfaits. Avec la création de la cellule de lutte contre la cybercriminalité, nombre d'entre eux apprennent désormais à leurs dépens que certains actes ne restent jamais impunis.

Les faits remontent au lundi 15 septembre 2014 dans la zone ACI, une cité résidentielle censée pourtant être sous surveillance accrue au regard de ses occupants, pour la plupart, des ressortissants étrangers (missions diplomatiques, organisations internationales, etc.). Mais qu'importe pour les malfrats désormais regaillardis par les nombreuses failles du dispositif sécuritaire dans la capitale et surtout, par des décisions pour le moins controversées des plus hautes autorités de la République.
C'est donc en plein jour, aux environs de 14 heures dans la zone indiquée que trois individus armés ont envahi un magasin de vente de téléphones portables de grandes valeurs et autres accessoirs electroniques dont des clés USB, des chargeurs, des puces, cartes mémoires, etc.
Les deux premiers tinrent la gérante en joue pendant que le troisième dévalisait litteralement la boutique. Ils purent ainsi emporter des appareils d'une valeur marchande de plusieurs dizaines de milliers de nos francs ainsi que la somme de 35.000 F CFA en espèces. Et ils repartirent sans être inquietés. Mission accomplie? Loin s'en fallait !

La victime décida de porter plainte contre X au niveau de la Brigade d'Investigation judiciaire (BIJ) et, naturellement, la nature des objets volés aidant, l'affaire fut confiée à la Cellule de lutte contre la Cybercriminalité dirigée par l'Inspecteur divisionnaire Papa Mambi Keïta surnommé « l'Epervier du Mandé». Commença alors la cyber-traque !

Nous ne cesserons jamais de le dire: les objets électroniques sont de véritables traîtres. Ils sont susceptibles de tout révéler sur leurs propres utilisateurs. Et le saviez-vous ? Il est même possible d'ouvrir le micro de certains téléphones à distances. Quant aux puces, cartes mémoires ou clés USB, elles peuvent être également activées de loin. A ce stade, certains commentateurs comparent déjà notre époque à celle décrite par l'auteur de roman de science fiction, Georges Orwell dans «1984» avec le fameux « Big Brother » désormais présent dans la légende contemporainne*.
Naturellement, ces méthodes de surveillance necessitent des équipements adéquats, une collboration accrue des services techniques et surtout, une bonne dose d'intelligence; un aspect de la question qui ne fait nullement défaut au niveau de la cellule de lutte contre la cybercriminalité.

Mettant ainsi toutes ces aptitudes à contribtion, les enquêteurs parvinrent à identifier un nommé Souleymane Doumbia comme utilisateur d'un des objets volés. Il fut interpellé dans les heures qui suivront et sa victime l'identifia formellement comme étant un de ses agresseurs. Il était inutile de nier les faits. Mais comment diantre les enquêteurs sont-ils parvenus jusqu'à lui ? C'est bien la question qu'il se pose encore à l'heure actuelle. Difficile de trouver réponse à cette intérrogation. Et pour cause, « Big Brother » est passé par là. Ses complices, quant eux, attendent à leur tour d'être arrêtés. Une question de jours.

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

Source : http://maliactu.net/mali-arrestation-de-braqueurs-dans-la-zone-aci-big-brother-est-passe-par-la/

2015 sous haute tension en matière de Cybercriminalité

	2015 sous haute tension en matière de Cybercriminalité

Les cybercriminels sont de plus en plus confiants : ils avaient auparavant tendance à attaquer les usagers de services bancaires, voyant en eux le maillon faible de la chaîne de sécurité, mais les experts de Kaspersky Lab anticipent désormais des cyber-attaques ciblées d'envergure sur les banques elles-mêmes. Et les fraudeurs ne s'arrêteront pas là!

Ils devraient tenter le tout pour le tout en essayant de développer de nouveaux malwares capables de retirer du liquide directement depuis les distributeurs. Outre les cyber-crimes financiers, 2015 suscitera probablement encore plus d'inquiétudes quant à la confidentialité et à la sécurité des appareils Apple, et fera resurgir les peurs quant aux appareils connectés ; il s'agira d'empêcher les hackers d'utiliser des outils comme les imprimantes réseau pour pénétrer les réseaux d'entreprises.

1. Quand les cybercriminels s'inspirent des APT
Lors d'une étude récente, nous avons découvert une attaque dans laquelle l'ordinateur d'un comptable a été compromis et utilisé pour effectuer un transfert important avec une institution financière. Cela illustre une tendance intéressante : celle des attaques ciblées contre les banques elles-mêmes.
Nous assistons à une augmentation des incidents provoqués par des malwares dans lesquels les banques sont infiltrées en utilisant des méthodes utilisées dans les APT. Une fois que les pirates ont pénétré les réseaux de la banque, ils volent assez d'informations pour pouvoir voler de l'argent directement à la banque et ce, de plusieurs manières :
• En prenant le contrôle des distributeurs automatiques à distance afin d'obtenir du liquide
• En réalisant des transferts SWIFT depuis plusieurs comptes de clients
• En manipulant les systèmes bancaires en ligne pour réaliser des transferts en arrière-plan
De telles attaques annoncent l'émergence d'une nouvelle tendance qui s'inspire des attaques APT que l'on voit dans le monde cybercriminel.

2. Les groupes se fragmentent, les attaques APT se diversifient
La révélation de l'existence de ces groupes utilisant les APT a mené à l'exposition publique et la condamnation d'un groupe de pirates qui aurait mené des actions de cyber-espionnage contre des entreprises américaines.
Alors que les équipes de recherche continuent d'encourager la découverte de ces groupes ayant recours aux APT, nous nous attendons à des changements en 2015 : les groupes d'APT les plus importants et les plus connus se sépareront en plus petits groupes qui fonctionneront indépendamment les uns des autres. Les attaques deviendront plus répandues et davantage d'entreprises seront touchées car les petits groupes diversifieront leurs attaques. Cela signifie également que les entreprises les plus importantes qui ont déjà été compromises dans le passé par deux ou trois groupes d'APT importants (comme par exemple, 'Comment Crew' et 'Webky') seront la cible d'attaques plus diverses et provenant de plusieurs sources différentes.

3. Un ancien code, de nouvelles vulnérabilités (dangereuses)
De récentes accusations d'altération délibérée et de défaillances accidentelles dans des systèmes de chiffrement (« goto fail ») ainsi que des vulnérabilités critiques dans des logiciels connus (Shellshock, Heartbleed, OpenSSL) ont laissé la communauté dubitative face à ces logiciels non vérifiés. La réaction a donc été de lancer des analyses indépendantes de la clé de ces logiciels ou que des chercheurs en sécurité les dissèquent à la recherche de vulnérabilités critiques (une alternative à l'analyse non officielle). Cela signifie que 2015 sera une autre année remplie de nouvelles vulnérabilités dangereuses qui apparaitront dans des anciens codes, exposant ainsi l'infrastructure Internet à des attaques.

4. Augmentation des attaques contre les distributeurs automatiques et les points de vente
Les attaques contre les distributeurs automatiques semblent avoir explosé cette année avec plusieurs incidents publics et la vive réaction des autorités à travers le monde pour faire face à cette crise. Une des conséquences de ces incidents est la prise de conscience que ces distributeurs automatiques sont très faciles à pirater et les cybercriminels l'ont bien remarqué. Comme la plupart de ces systèmes fonctionnent sous Windows XP et disposent d'une sécurité physique très faible, ils sont très vulnérables par défaut. Et comme les institutions financières disposent d'argent liquide, il est logique que les cybercriminels commencent par là.

En 2015, nous nous attendons à observer une évolution de ces attaques contre les distributeurs automatiques grâce à l'utilisation de techniques d'APT afin d'accéder au système d'information de ces machines. On verra ensuite les pirates compromettre les réseaux des banques et utiliser cet accès pour prendre le contrôle des distributeurs en temps réel.

5. Attaques Mac : des botnets OS X
Malgré les efforts d'Apple pour verrouiller le système d'exploitation Mac, nous continuons d'observer des logiciels malveillants envoyés via des torrents ainsi que des logiciels piratés. La popularité grandissante des appareils Mac OS X fait tourner les têtes dans le monde criminel et rend très intéressante la création de malwares pour cette plateforme. L'écosystème fermé par défaut empêche les malwares d'envahir la plate-forme mais certains utilisateurs choisissent de désactiver les mesures de sécurité Mac OS X surtout ceux qui utilisent des logiciels piratés. Cela signifie que ceux qui cherchent à pirater les systèmes OS X pour diverses raisons savent qu'ils ont juste à cacher leur malware dans un logiciel attirant (certainement en le faisant passer pour un générateur de clé) pour réussir à le diffuser. À cause des idées reçues sur la plateforme OS X, ces systèmes ont peu de chances d'avoir une solution antimalware qui détectera les infections une fois le malware installé : ce dernier passera donc inaperçu pendant très longtemps.

6. Des attaques contre les systèmes de billetterie automatique
Les incidents comme le piratage NFC contre les transports publics chiliens (http://securelist.com/blog/virus-watch/67283/android-nfc-hack-allow-users-to-have-free-rides-in-public-transportation) montre l'intérêt que les criminels ont pour les ressources publiques comme les systèmes de transports publics. Certains pirates ne chercheront même pas à obtenir de l'argent pour ce type d'attaques et seront simplement contents de voyager gratuitement et de partager leur technique avec d'autres. Bien que ces systèmes de billetterie soient vulnérables (la plupart d'entre eux fonctionnent sous Windows XP), dans de nombreuses villes, ils gèrent directement des transactions par carte bancaire. Nous nous attendons donc à voir des attaques plus violentes contre ces systèmes que cela soit pour détourner le système ou voler des données de carte bancaire.

7. Des attaques contre les systèmes de paiement virtuel
La logique veut que les cybercriminels cherchent à gagner de l'argent grâce à leurs attaques de la manière la plus efficace et la plus simple possible. Quoi de mieux que les systèmes de paiement virtuel qui n'en sont encore qu'à leurs débuts ? Nous nous attendons donc à ce que les criminels se jettent sur toutes les opportunités qu'ils trouveront pour exploiter ces systèmes. Qu'il s'agisse d'ingénierie sociale, d'attaques ciblant les appareils des utilisateurs (dans la plupart des cas, les téléphones mobiles), ou de pirater directement des banques, les cybercriminels choisiront les attaques qui pourront leur rapporter de l'argent rapidement et les systèmes de paiement virtuel finiront par en faire les frais.

Ces craintes peuvent également s'appliquer à Apple Pay qui utilise la NFC (Near Field Communications) pour gérer les transactions sans fil des utilisateurs.

8. Apple Pay
De précédentes attaques se sont concentrées sur les systèmes de paiement NFC mais, grâce à son adoption limitée, ces attaques n'ont pas rapporté beaucoup. Apple Pay va certainement changer cela. L'enthousiasme pour ce nouveau système de paiement va faire exploser l'adoption de ce système et cela attirera bien évidemment les cybercriminels qui chercheront à intercepter ces transactions. Le design d'Apple se concentre principalement sur la sécurité (avec par exemple, la virtualisation des données de transaction) mais nous sommes très curieux de voir comment les pirates exploiteront les fonctionnalités de ce système.

9. Compromettre l'Internet des objets
Les attaques contre l'Internet des objets (ou objets connectés) se sont limitées aux prototypes et aux avertissements (parfois exagérés) annonçant que les smart TV et les réfrigérateurs seront ciblés par les pirates pour créer des Botnets ou lancer des attaques malveillantes.
Alors que de plus en plus d'appareils connectés sont disponibles, nous nous attendons à observer un débat plus important sur la sécurité et la confidentialité, surtout parmi les entreprises de ce secteur. En 2015, on verra certainement des attaques contre des imprimantes connectées en réseau et autres appareils connectés qui aideront les pirates expérimentés à s'infiltrer dans les réseaux corporatifs. Nous nous attendons à ce que les appareils de l'Internet des objets fassent partie de l'arsenal des groupes utilisant les APT, surtout si l'on considère que la connectivité est désormais introduite aux procédés industriels ainsi qu'aux procédés de fabrication.

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

Source : http://www.economiematin.fr/news-2015-attaque-hacker-piratage-criminel-brulez
Par Nicolas Brulez

Copier les données de son entreprise pour son propre compte, c’est risqué !

Copier les données de son entreprise pour son propre compte, c’est risqué !

Fin octobre, la Cour de cassation a rejeté le pourvoi d’un salarié qui avait été condamné en appel pour avoir copié pour son propre compte plus de 300 documents confidentiels de l’entreprise qu’il quittait pour un concurrent.

Les documents étaient protégés par une charte de confidentialité signée par tous les salariés, dont le plaignant, onze ans plus tôt. Après 16 années passées dans la société, l’homme avait informé son employeur, un cabinet de courtage d’assurance, de son intention de démissionner de son emploi de chargé de clientèle en vue de rejoindre un autre cabinet de courtage. Un élément contextuel de nature qui permet également de mieux comprendre les décisions de première instance et d’appel.
Il avait ensuite extrait des données de son poste de travail à l’aide de « treize supports externes » et « en expédiant de son poste professionnel et à destination de sa messagerie électronique privée une multitude de fichiers numériques confidentiels ».

Fond documentaire personnel ?
Il avait admis suite à cela vouloir alimenter un fonds documentaire personnel, mentionnant qu’une partie des données copiées avaient été produites par lui même. Le plaignant également avait reproché à la Cour d’appel de ne pas avoir pris en compte le fait que les informations détournées n’avaient pas été diffusées auprès de tiers. Ces arguments ont été jugés irrecevables.
Dans son arrêt, la Cour de cassation a estimé que l’abus de confiance était caractérisé puisque « le prévenu a[vait], en connaissance de cause, détourné en les démultipliant, pour son usage personnel, au préjudice de son employeur des fichiers informatiques ».
Au terme des différentes procédures, le plaignant à été condamné à verser 12 500 euros à la partie adverse.

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

Source : http://www.zdnet.fr/actualites/justice-copier-des-donnees-du-si-pour-sa-pomme-c-est-risque-39810871.htm