Les synthèses du CLUSIF

Panorama de la cybercriminalité, année 2013

Synthèse de la conférence du CLUSIF du 16 janvier 2014.

En 2002, le CLUSIF présentait son premier Panorama de la Cybercriminalité. Cet évènement est très vite devenu incontournable pour tous ceux qui s'intéressent à la sécurité des systèmes d'information, qu'ils soient utilisateurs en entreprises ou collectivités publiques, ou offreurs de solutions ou de services issus de tous les secteurs d'activité de l'économie. Depuis plus de dix ans, cet événement permet d'apprécier les tendances ainsi que l'émergence de nouveaux risques. Il permet de relativiser et de mettre en perspective des incidents qui ont, à tort ou à raison, défrayé la chronique. À partir de 2009, le panorama s'est élargi aux événements accidentels et aux faits de société pouvant induire ou aggraver des actions cybercriminelles. La sélection des sujets est réalisée par un groupe de travail pluriel, constitué d'officiers de police et de gendarmerie, de RSSI et d'offreurs de biens et de services. Les informations utilisées proviennent exclusivement de sources ouvertes.

L'édition 2013 du Panorama s'est focalisée sur six grands sujets. Elle s'est poursuivie avec une table ronde regroupant, autour du Président du CLUSIF, quelques acteurs incontournables de la sécurité.

Démystification ou comment s'affranchir du « PRISM » déformant de l'actualité

Sujet présenté en salle par Gérôme BILLOIS - Senior Manager – CERT-Solucom

Si les révélations d'Edward Snowden ont été au cœur de l'actualité 2013, elles ne doivent pas occulter d'autres événements importants en matière de cybercriminalité. L'année 2013 fut aussi celle du **rapport APT1** de la société Mandiant[1] mettant en lumière un groupe de hackers probablement issu de l'armée chinoise. Ayant pour activité principale le cyber-espionnage, ce groupe a visé 140 entreprises de 20 secteurs d'activité différents. Les moyens alloués étaient importants puisque la masse de données collectées et stockées par le groupe APT1 s'évaluerait en téra octets.

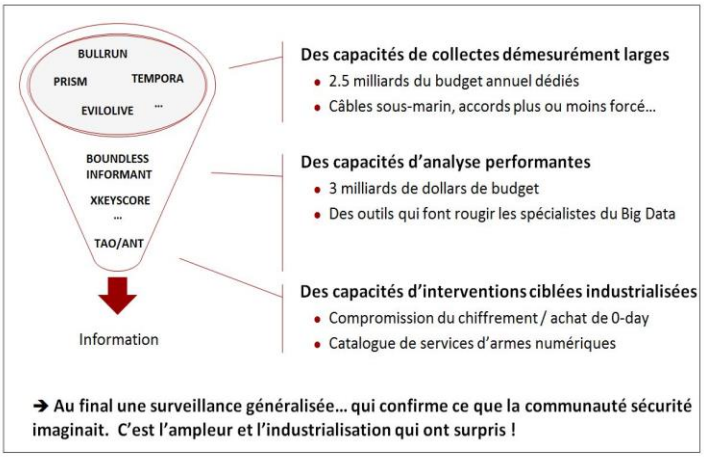

Figure 1: La NSA et Snowden depuis juin : une formidable machine à espionner !

Aux États-Unis, le scandale de la NSA a révélé la mise en œuvre d'un véritable **« entonnoir d'espionnage » industrialisé**. Les capacités de collecte et d'analyse y sont particulièrement élevées et la possibilité de rechercher des informations ciblées impressionne. Mais, cette affaire démontre aussi que

[1] http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

la NSA est vulnérable. À cause d'une traçabilité insuffisante, l'étendue des fuites demeure d'ailleurs une énigme pour ce service. Sa faiblesse provient peut-être du fait des 1000 postes d'administrateur sous-traités. Ainsi, la NSA devrait être réorganisée dans les prochains mois.

2013 a également vu se développer quatre types d'attaques. D'abord la **méthode du « *waterholing* »** (en français, méthode « du point d'eau ») consistant à piéger une page d'un site très visité par la population ciblée. Ce piège permet d'infecter le poste des visiteurs. Cette méthode a notamment été employée pour collecter des informations auprès de la communauté du nucléaire américain en piégeant la page du site du Ministère du travail consacrée aux compensations en cas d'exposition aux radiations[2]. Les **attaques destructives** se sont multipliées. Leur objectif n'était pas le vol de données mais leur suppression définitive (sabotage) ou temporaire (demande de rançon). Côté destruction, l'attaque de Jokra, en Corée du Sud, est un parfait exemple[3]. En mars 2013, elle a impacté 35 000 postes. Côté chantage, citons le « *ransomware* » (« rançongiciel ») CryptoLocker. Le nombre d'**attaques « métiers »** a aussi augmenté en 2013. Elles ont ciblé l'ensemble d'un processus métier comme, par exemple, dans l'affaire du piratage massif de distributeurs de billets où des escrocs ont pu « siphonner » des comptes bancaires dont ils avaient préalablement supprimé la limite de retrait par carte bancaire[4]. Enfin, les hackers ont de plus en plus visé les particuliers avec des **attaques « vie privée »**. Plutôt que de se confronter à la sécurité du système d'information d'entreprises, ils se sont intéressés aux réseaux personnels de communication, souvent moins protégés, de leurs managers (Facebook, email, etc.)[5].

Ainsi, **les méthodes d'attaques n'ont cessé de se diversifier en 2013**, les hackers cherchant désormais à contourner les mesures de sécurité déployées sur les systèmes d'information des organismes. La NSA n'est finalement qu'une menace parmi de nombreuses autres qui doivent toutes être prises en compte au sein du processus de gestion des risques.

Les cybercriminels n'ont pas disparu...

Sujet présenté en salle par Fabien COZIC - Consultant senior en cybercriminalité - CERT-LEXSI et par le Colonel Éric FREYSSINET - Chef de la division de lutte contre la cybercriminalité – Pôle Judiciaire de la Gendarmerie Nationale / STRJD

L'année 2013 a été marquée par de nombreuses arrestations dont celles des créateurs des *malwares* Gozi[6], Zeus/SpyEye[7] et Blackhole[8] ou encore de l'auteur de l'attaque *DDoS* contre SpamHaus[9]. En octobre 2013, Ross Ulbricht *aka* Dread Pirate Roberts, suspecté d'être le créateur et l'administrateur du cybermarché Silk Road a lui aussi été interpelé par les autorités américaines[10]. Le site rouvrait néanmoins un mois plus tard, et même si les deux nouveaux administrateurs présumés furent interpelés à leur tour, le site est toujours actif. Ces arrestations n'ont donc eu qu'un effet limité, démontrant une **professionnalisation** et une **pérennisation** de la cyberdélinquance. Ces marchés se développent. À côté des offres déjà connues (« *crimeware as a service* », « *carding* », « *DDoS as a service* ») de nouveaux services illicites apparaissent. Ainsi, le groupe chinois Hidden Lynx[11] regroupant 50 à 100 spécialistes, offre ses services d'espionnage industriel.

[2] http://www.alienvault.com/open-threat-exchange/blog/us-department-of-labor-website-hacked-and-redirecting-to-malicious-code
[3] http://www.symantec.com/connect/blogs/are-2011-and-2013-south-korean-cyber-attacks-related
[4] http://www.ibtimes.co.uk/cyber-crime-bank-theft-45m-27-countries-466578
[5] http://securityaffairs.co/wordpress/14877/cyber-crime/senior-management-considered-a-primary-target-by-modern-cybercrime.html
[6] http://www.fbi.gov/newyork/press-releases/2013/three-alleged-international-cyber-criminals-responsible-for-creating-and-distributing-virus-that-infected-over-one-million-computers-and-caused-tens-of-millions-of-dollars-in-losses-charged-in-manhattan-federal-court
[7] http://www.infosecurity-magazine.com/view/32239/accused-of-stealing-millions-spyeye-developer-extradited-to-us/
[8] http://krebsonsecurity.com/2013/12/who-is-paunch/
[9] http://www.theguardian.com/technology/2013/may/20/man-accused-breaking-the-internet
[10] http://www.ice.gov/news/releases/1310/131002baltimore.htm
[11] http://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire

Figure 2: L'offre se professionnalise

Les moyens numériques sont exploités par la **criminalité organisée** dite « traditionnelle » poussant ainsi à son **internationalisation**. Les cybercriminels gagnent aussi du terrain dans le monde réel en élargissant leurs domaines d'activité (trafic de stupéfiants, trafic de biens, traite d'êtres humains).

En 2013, le mouvement des Anonymous a perdu de sa force. Les nombreuses arrestations aux États-Unis ont découragé ses sympathisants. Mais l'**hacktivisme** a laissé des traces dans le monde de la cybercriminalité. Les méthodes telles que l'ingénierie sociale ont été reprises et améliorées. Les motivations avancées par les hacktivistes proches des Anonymous sont maintenant reprises par certains hackers à des fins moins honorables. Des sous-groupes plus radicaux tels que la Syrian Electronic Army s'en servent également.

Les ***malwares*** **mobiles** sont en augmentation[12]. Alors que les programmes malfaisants ciblent majoritairement les systèmes d'exploitation Android, des attaques d'un nouveau genre sont apparues (*botnet*, contamination sur PC via la synchronisation, contrôle à distance par la messagerie en ligne, etc.). L'**ingénierie sociale** est très utilisée pour la compromission mobile. Elle permet par exemple de contourner la double authentification et d'installer des programmes malveillants sur les terminaux.

Figure 3: Cryptolocker – un ransomware avec chiffrement RSA 2048 bit !

Les **données bancaires** demeurent aussi très convoitées par les cybercriminels. Les méthodes de piratage de distributeurs automatiques de billets se complexifient. Mais les grandes enseignes sont aussi directement visées. Ainsi, à l'approche des fêtes de Noël, le réseau Target a été victime d'une attaque[13]. Ce sont les données bancaires de plus de 110 millions de personnes qui auraient été dérobées.

L'une des tendances annoncées pour 2014 est l'utilisation croissante des « ***ransomwares*** ». Ces programmes chiffrent les données, verrouillent les postes de travail des utilisateurs puis affichent une demande de rançon et lancent un décompte à l'issue duquel les données seront détruites en l'absence de paiement. Les autorités ont encore peu de visibilité sur ce phénomène. Pour plus de discrétion, les organismes victimes préfèrent parfois payer sans déposer plainte. En effet, avec les dernières versions de CryptoLocker[14], les escrocs restituent les données après paiement (seule solution en l'absence de sauvegarde récente).

[12] http://www.cso.com.au/article/534711/seventy_percent_all_known_mobile_malware_variants_found_2013_kaspersky/
[13] http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores
[14] http://www.pcworld.fr/internet/actualites,ransomware-cryptolocker-aurait-deja-infecte-plus-de-250-000-machines-a-travers-le-monde,544961,1.htm

Le paradis cybercriminel existe-t-il sur terre ? Quelles sont les stratégies des États pour en obtenir la clé ?[15]

Sujet présenté en salle par Diane MULLENEX - Avocat à la Cour – Pinsent Masons LLP

Le coût global des cyberattaques a été estimé à 300 milliards d'euros pour les entreprises en 2013[16]. Avec la délinquance numérique, **la criminalité s'internationalise**. Face à ce phénomène, beaucoup d'entreprises se retrouvent démunies en termes juridiques.

La première difficulté juridique tient aux approches très différentes des dossiers de cyberdélinquance selon les États. Ces différences tiennent aussi bien à la qualification des infractions, aux règles de procédure telles que la recevabilité de la preuve numérique, ou à la compétence juridictionnelle ainsi qu'aux des moyens d'investigation numérique. Ainsi, les entreprises victimes de cyberattaques doivent élaborer une véritable **stratégie judiciaire**.

Avec l'affaire « PRISM », la communauté internationale a pris conscience des risques d'interception des données transitant sur les réseaux. Ainsi, aux États-Unis, de multiples lois permettent à différents services américains de capter de données numériques. Une unité militaire américaine, USCYBERCOM, créée en 2010, est consacrée à la cyberdéfense. Ces dispositifs inquiètent.

Les groupes de réflexion sur la **gouvernance de l'Internet** se multiplient. Certains s'interrogent sur la pertinence d'une réglementation, d'autres font un parallèle entre le web et les grands fonds marins déclarés bien commun par l'ONU et placés sous le contrôle d'un organisme intergouvernemental autonome. En Europe, la tendance est à la complémentarité des normes privées et étatiques. La **Convention de Montevideo** sur l'avenir de la coopération pour l'Internet d'octobre 2013 s'inscrit dans ce mouvement de réflexion. Par cette convention, les États invitent notamment à la mondialisation des fonctions de l'IANA et de l'ICANN. À ce jour, l'unique texte international à valeur contraignante reste la **Convention de Budapest** sur la cybercriminalité. Essentiellement ratifiée par des États-membres de l'Union européenne, sa portée reste limitée.

Pour autant, en juillet 2012, le Japon a signé la convention. Cette ratification illustre la récente préoccupation des États d'Asie pour la cybercriminalité. Ainsi, la Chine complète son arsenal pénal en réaction à de nombreuses affaires de racket en ligne et de piratage du jeu World of Warcraft.

Ainsi, la gouvernance de l'Internet pourrait devenir l'enjeu 2014 pour la communauté internationale.

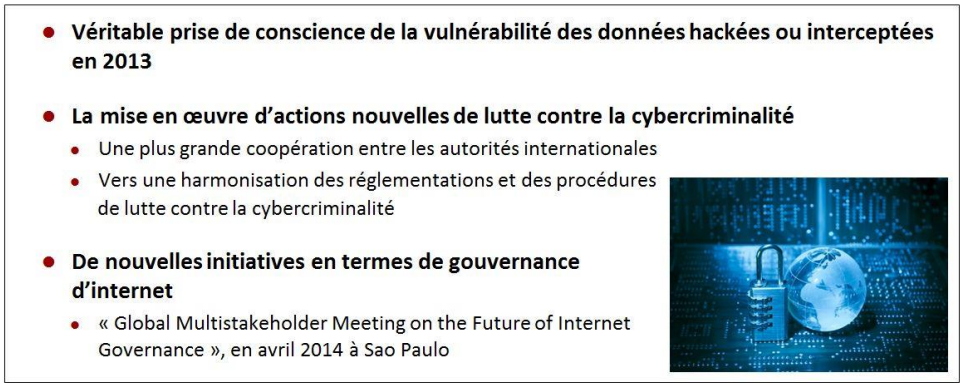

Figure 4: La gouvernance de l'Internet: un enjeu pour 2014 ?

[15] Étude approfondie sur le phénomène de la cybercriminalité et les mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, UNODC, janvier 2013,
http://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_F.pdf
« Le droit pénal face à la cyberdélinquance et à la cybercriminalité », Jacques Francillon, 2012, Revue Lamy droit de l'immatériel
Compétence et accès transfrontalier : quelles solutions ?, 2012,
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2012)3F_transborder_repV27FR.pdf
From nuclear war to Net War : Analogizing Cyber Attacks in International Law, Scott J. Shackelford, 2009,
http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1368&context=bjil

[16] Rapport McAfee/CSIS : http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

2013, l'année des monnaies virtuelles

Sujet présenté en salle par Barbara LOUIS-SIDNEY - Juriste – CEIS et par Garance MATHIAS - Avocat à la Cour – Cabinet d'Avocats Mathias

La fermeture de Liberty Reserve[17] et l'actualité autour du bitcoin ont fait de 2013 l'année de la monnaie virtuelle. Détachée de toute devise, le bitcoin est une **crypto-monnaie** qui pose question. S'il en a les moyens (puissance CPU) chacun peut générer des bitcoins en dehors de tout cadre légal. La monnaie se crée, en effet, par résolution de blocs de calculs. L'anonymat des transactions est réel, mais la « *blockchain* »[18] qui contient un historique horodaté de toutes les transactions permet néanmoins un certain suivi. Même si leurs propriétaires restent inconnus, le parcours de chaque bitcoin peut être tracé.

La **monnaie virtuelle** doit est distinguée de la **monnaie électronique**. Cette dernière, reconnue par les banques centrales, est, en droit français, définie à l'article L.315-1 du Code monétaire et financier[19]. La crypto-monnaie, quant à elle, n'est pas reconnue par la Banque centrale européenne en ce qu'elle est créée et contrôlée par ses seuls développeurs et qu'elle n'est acceptée que par les membres d'une communauté virtuelle spécifique.

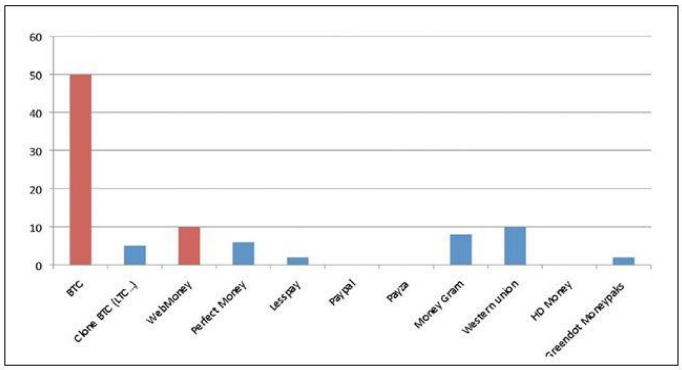

Figure 5: Bitcoin, la monnaie préférée des cybercriminels (rapport CEIS)

Aujourd'hui, le bitcoin est d'abord utilisé sur les marchés parallèles. Sur 55 forums et *shops* pris en exemples, 50 acceptent les bitcoins. Pour 10 d'entre eux, le bitcoin est soit la seule monnaie acceptée, soit la monnaie privilégiée. La plupart, déçue de Perfect Money, encourage vivement son usage. 50 ne mentionnent pas Perfect Money, dont 5 qui refusent catégoriquement cette e-monnaie[20].

Ainsi, la crypto-monnaie a été au cœur de nombreux cas de criminalité organisée en 2013. Associée à des services de blanchiment et des intermédiaires dits « de confiance », cette monnaie permet des transactions anonymes en brouillant la « *blockchain* ». Mais de nouvelles crypto-monnaies apparaissent. Citons par exemple Zerocoin[21] qui se présente aujourd'hui comme un bitcoin anonyme et sécurisé.

Face à ce phénomène, les États entament une réflexion. La **réglementation** de cette monnaie pourrait renforcer le cadre législatif de lutte contre la cybercriminalité. Le 13 août 2013, les États-Unis, sans aller jusqu'à reconnaître le bitcoin, ont accordé une licence qui permet à la plate-forme MT.GOX de traiter cette monnaie et de réaliser des transferts de fond, le tout surveillé au titre de la lutte contre le blanchiment et le financement du terrorisme. De son côté, la Banque de France refuse aujourd'hui toute reconnaissance du bitcoin. D'autres défendent l'idée d'une **autorégulation** avec le développement de bonnes pratiques visant à renforcer la confiance des utilisateurs.

[17] http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR/Liberty%20Reserve,%20et%20al.%20Indictment%20-%20Redacted.pdf
[18] https://fr.bitcoin.it/wiki/Block_chain
[19] http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=6F863450DF2598A58EE4DDFDCD9F528F.tpdjo11v_3?idArticle=LEGIARTI000027007558&cidTexte=LEGITEXT000006072026&dateTexte=20140118
[20] Statistiques issues du rapport « *Monnaies Virtuelles et Cybercriminalité – Etat des lieux et perspectives* » du CEIS.
[21] http://zerocoin.org/

Le droit à l'épreuve de la cybercriminalité. Quel arsenal juridique pour la France et l'Europe ?

Sujet présenté en salle par Garance MATHIAS - Avocat à la Cour – Cabinet d'Avocats Mathias

L'année 2013 a été riche en projets tant en droit européen que français. Ainsi, le 11 janvier 2013, l'Union Européenne a mis en place le **Centre européen de lutte contre la cybercriminalité** (EC3)[22]. Quelques jours plus tard, elle érigeait la lutte contre la cybercriminalité au rang des priorités de l'organisation[23].

Deux textes européens ont été adoptés cette année. C'est d'abord le règlement technique consacré à la procédure de **notification des violations de données personnelles** obligatoire pour les opérateurs[24]. En droit interne, ce texte s'est traduit par l'élaboration d'une téléprocédure accessible sur le site de la CNIL. La directive relative aux **attaques contre les systèmes d'information**[25] a également été adoptée. Elle devra être transposée par chaque État-membre d'ici 2015.

Côté projets, plusieurs propositions ont été présentées par la Commission européenne en 2013. Elles portent sur la **sécurité des réseaux de l'information**[26], la **protection du secret d'affaire**[27] ou encore la **signature et l'identité numérique**[28]. Le **paquet sur la protection des données personnelles**[29], quant à lui, a été adopté par la Commission LIBE. Il est actuellement soumis aux gouvernements. L'Union souhaiterait une adoption en 2014 mais ce délai semble compromis. Ce projet divise plus que jamais les acteurs du secteur du numérique.

Figure 6: Que retenir du paquet sur la protection des données personnelles et de la loi de programmation militaire ?

[22] Commission Européenne, Communiqué de presse sur la création de l'EC3, 9 janvier 2013
[23] Communication de la Commission européenne en date du 7 février 2013
[24] Règlement n°611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques
[25] Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil
[26] Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union , http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_fr.pdf
[27] Proposition de directive du Parlement européen et du Conseil sur la protection des savoir-faire et des informations commerciales non divulgués contre l'obtention, l'utilisation et la divulgation illicites
[28] Proposition de Règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur
[29] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ; Proposition de directive sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et libre circulation de ces données

En France, l'actualité a été marquée par le **Livre sur la défense et la sécurité nationale** faisant de la cybersécurité un enjeu national. Mais c'est surtout la **loi de programmation militaire**[30] qui animé les débats de cette fin d'année 2013. Son article 20 autorise et encadre l'interception administrative des données de connexion. Mais sa rédaction particulièrement floue fait l'objet de nombreuses critiques permettant d'envisager des questions prioritaires de constitutionnalité ou une révision du texte dans les années à venir.

Nous aurions aussi aimé vous parler…

Sujet présenté en salle par Gérôme BILLOIS - Senior Manager – CERT-Solucom

L'actualité 2013 ayant été très riche, plusieurs sujets intéressants n'ont pas pu, faute de temps, être développés lors de ce panorama. Ce fut d'abord le cas pour les **accidents informatiques**, première cause des incidents de sécurité. 2013 a connu quelques cas amusants. Dans l'espace, et suite à un problème de mise à jour, la station spatiale internationale a perdu le contact avec la Terre (à l'exception de la Russie) pendant 6 heures[31]. Sur Terre, un centre de données Facebook s'est retrouvé à l'arrêt suite à des problèmes d'humidité. Les contrôles de température totalement déréglés ont fini par causer un phénomène de condensation si impressionnant que les personnes présentes eurent l'impression qu'une averse s'était déclenchée dans la pièce[32].

2013 fut aussi l'année des **objets connectés**. Très prisés des consommateurs, ils attirent aussi les hackers. Ainsi, des webcams et autres équipements privés furent piratés afin de filmer en permanence ou d'envoyer les données à un tiers[33]. Il a été démontré que les lunettes connectées (du type Google Glass) pouvaient être victimes d'attaques similaires[34]. Les incidents de sécurité sur ces objets peuvent aussi mener à l'irréparable. Le système d'accélération défectueux d'un véhicule automobile a causé plusieurs accidents mortels. Suite à ces événements, le constructeur a été condamné.

Plusieurs cas d'**usurpations d'identité sur les réseaux sociaux** ont diverti la toile. Le compte twitter de l'enseigne BurgerKing a été rhabillé en McDonald[35]. Un tweet sur le compte de la société Jeep a annoncé son rachat par Cadillac[36]. Force est de constater que ces nouveaux espaces tendent à devenir des moyens de communication officiels, et ce, malgré leur vulnérabilité. Leur sécurisation doit donc devenir une préoccupation en 2014.

Enfin, le CLUSIF aurait aussi aimé aborder plus longuement les **attaques touchant les mobiles**. Les *malwares* ciblant ces plateformes se perfectionnent. Ainsi, Obad.a est l'un des *malwares* sur système Android les plus sophistiqués connu à ce jour[37]. Les attaques par « *social engineering* » se développent également ; elles sont préparées en fonction du public ciblé. C'est ainsi que le programme Chuli.a a piégé des activistes tibétains en prenant la forme d'un message comportant en pièce jointe, des informations liées à une fausse conférence à Genève[38]. Une fois la pièce jointe ouverte, le *malware* pouvait récupérer l'ensemble du carnet d'adresses de l'utilisateur, ses SMS et l'historique de ses appels. Les mobiles non Android n'ont pas été épargnés en 2013. Une démonstration menée à la conférence BlackHat a montré une attaque physique utilisant de faux chargeurs et visant les iPhone/iPad[39].

[30] Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale

[31] http://www.v3.co.uk/v3-uk/the-frontline-blog/2249029/nasa-briefly-loses-contact-with-international-space-station

[32] http://www.theregister.co.uk/2013/06/08/facebook_cloud_versus_cloud/

[33] http://readwrite.com/2013/11/13/hacking-the-connected-home-when-your-house-watches-you

[34] http://www.atlantico.fr/atlantico-light/google-glass-hacker-jay-freeman-deja-jailbreakees-715000.html

[35] http://mashable.com/2013/02/18/burger-king-twitter-account-hacked/

[36] http://gizmodo.com/5985353/exclusive-the-burger-king-and-jeep-hacker-is-probably-this-dj-from-new-england

[37] http://www.securelist.com/en/blog/8106/The_most_sophisticated_Android_Trojan

[38] http://blogs.mcafee.com/mcafee-labs/targeted-attacks-the-next-step-in-mobile-malware

[39] https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-Slides.pdf

Table ronde

Éric FREYSSINET - Chef de la division de lutte contre la cybercriminalité – Pôle judiciaire de la Gendarmerie Nationale \STRJD, Lazaro PEJSACHOWICZ - Président du CLUSIF – Chargé de mission auprès de la communauté des SSI – CNAMTS, Hervé SCHAUER - Dirigeant le cabinet de consulting éponyme, Olivier GUERIN (animateur de la table ronde) - Chargé de mission – CLUSIF

En septembre dernier, la presse américaine publiait de nouvelles révélations d'Edward Snowden selon lesquelles la NSA aurait développé un programme décryptant les flux SSL. Cette information a-t-elle un impact dans le domaine de la SSI ? Selon Hervé Schauer, les conséquences d'une telle révélation doivent être relativisées. Le générateur aléatoire suspecté de « piégeage » n'est pas utilisé dans les implémentations courantes de SSL. En effet, depuis plusieurs années, la NSA est suspectée d'avoir cassé l'algorithme RC4. Ainsi, le protocole TLS est à privilégier. Correctement configuré, il assure une confidentialité renforcée. Enfin, dans le cadre d'une analyse de risques, la probabilité qu'un service étatique vienne s'intéresser aux informations du système d'information doit être évaluée. Pour la majorité des organismes, cette probabilité se révèle être minime. Nous n'avons pas d'informations précises sur un cassage de SSL.

Plusieurs traités internationaux organisent la coopération des autorités judiciaires. En pratique, cette coopération est-elle efficace face à la cybercriminalité ? Pour Eric Freyssinet, la mise en place d'une coopération transnationale entre services de police ou de gendarmerie progresse, elle n'en demeure pas moins longue et périlleuse. Les quelques arrestations menées dans les pays de l'Est laissent entrevoir un changement de stratégie dans la lutte contre la cybercriminalité internationale. Autres points positifs, les communautés internationales et européennes développent leur arsenal juridique pour améliorer cette coopération. Au sein de l'Union Européenne le mandat d'arrêt européen en est une parfaite illustration. À l'international, un centre d'innovation et d'échange de compétences rattaché à Interpol s'installe à Singapour. En France, un rapport du groupe de travail interministériel consacré à la cybercriminalité sera remis d'ici février 2014.

À compter du 8 avril 2014, Microsoft n'assurera plus le support ni les mises à jour de Windows XP. Quelles sont les conséquences pour la SSI ? Pour Lazaro Pejsachowicz, cette annonce va induire un coût important pour certains organismes en 2014. Une bonne évaluation des risques devrait permettre une migration progressive et ainsi, une meilleure gestion des coûts. De telles décisions d'éditeurs rappellent que l'utilisation de systèmes d'exploitation du type Windows XP s'avère problématique lorsqu'ils sont installés sur des équipements pilotant des processus industriels.

http://www.clusif.fr
11 rue de Mogador - 75009 Paris
Tél : 01 53 25 08 80 ; Fax : 01 53 25 08 88
Secrétariat : secretariat@clusif.fr