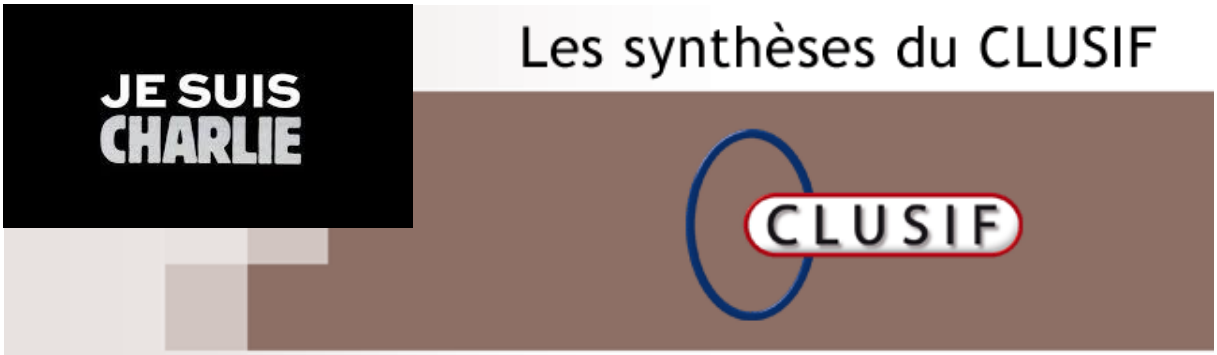


Panorama de la cybercriminalité, année 2014

Pour la quatorzième année consécutive, le CLUSIF (CLUb de la Sécurité de l'Information Français) a dressé un tableau de l'état de la cybercriminalité mondiale. Dévoilé au public et à la presse mercredi 14 janvier 2015, le Panorama 2014 fait la part belle à l'Internet des objets, au rançonnage des individus et des entreprises et aux menaces sur les banques et les moyens de paiement. Un retour d'actualité sur les failles *Heartbleed* et *Shellshock* a, par ailleurs, permis de mieux en comprendre les enjeux. Pour compléter cette rétrospective, l'évolution technique de la menace et la vision qu'en ont les services de polices n'ont pas été oubliées.

Introduction

Lazaro PEJSACHOWICZ - Président du CLUSIF – CNAMTS
Jean-Marc GREMY - Vice-Président du CLUSIF – Cabestan Consultants

L'année 2014 a tenu ses promesses et a donc été, comme toujours, copieuse en évènements. Notre Panorama montre tant les actions malveillantes et criminelles que les faiblesses de nos systèmes et de nos organisations. Il n'y a donc pas de fumée sans feu ; si les attaques peuvent exister, c'est bien que les opportunités persistent côté entreprises. Le CLUSIF appelle donc chacun à améliorer, dans son environnement professionnel, ses pratiques de sécurité. Certes, tous les risques ne peuvent être anticipés, mais les guides techniques du CLUSIF, son Panorama et son enquête sur les menaces informatiques et les pratiques de sécurité (MIPS) sont là pour vous y aider. Une meilleure circulation de l'information entre acteurs publics, privés et associatifs est aussi indispensable. Le CLUSIF l'appelle de ses vœux, car ce n'est que de manières coordonnées que nous pourrons mieux agir pour la sécurité des systèmes d'information.

Polémique, FUD et exagérations ou comment bien décrypter l'actualité *cyber*

Gérôme BILLOIS - Senior Manager – CERT-Solucom

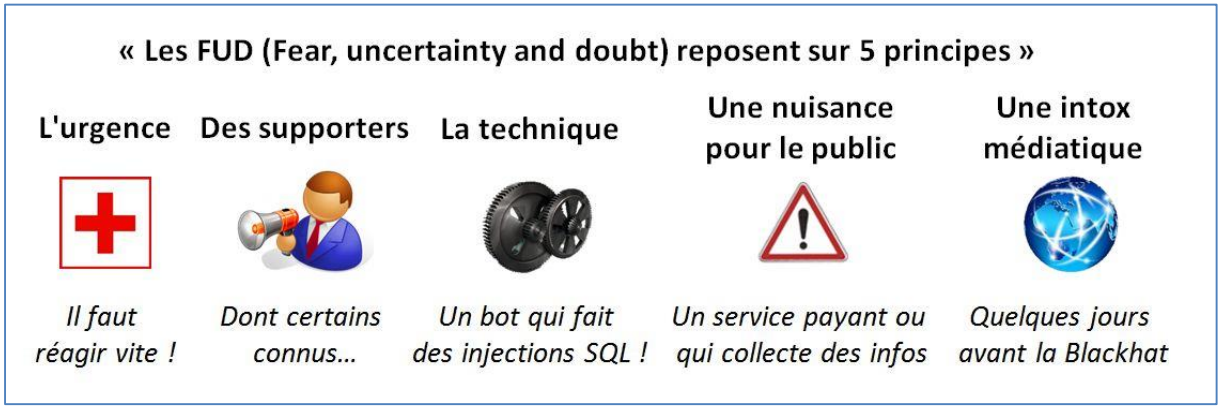
En août dernier, la presse annonce la fuite de plus d'un milliard de mots de passe. L'affaire est dénommée *Cybervor*[1]. Cette information a été lancée, quelques jours plus tôt, par une société américaine, Hold Security. Sur son site, un communiqué insiste sur l'ampleur de l'incident et l'urgence des actions correctives à déployer. La société en profite pour offrir des solutions reposant sur les multiples prestations qu'elle propose[2]. Finalement, l'affaire *Cybervor* s'essouffle et se révèle être l'un des nombreux *FUD* de l'année 2014.

Le *FUD* (*Fear, uncertainty and doubt*) est une technique d'accroche reposant sur cinq principes. L'annonce s'accompagne d'une urgence dans la réponse, de supporters qui la relayent (tels que des experts en sécurité), de détails techniques qui la confortent, d'une offre commerciale (une « nuisance » pour le public qui peut l'inciter à recourir à un service payant pour se protéger). Le tout se produit à un instant propice pour une forte diffusion dans les médias. Avant de s'emballer, le responsable sécurité, comme le journaliste, doit donc évaluer la fiabilité des informations et leur pertinence. Leur origine et les motivations de son annonce sont un

[1] http://www.undernews.fr/hacking-hacktivisme/cybervor-des-pirates-russes-volent-12-milliard-de-mots-de-passe.html
[2] http://www.holdsecurity.com/news/cybervor-breach/

premier critère. Si l'on parle de vols de données, la fraîcheur des informations dérobées, les catégories de personnes concernées et l'origine de la fuite peuvent aussi aider à évaluer le risque. Il est important de sensibiliser les directions quant à l'existence des *FUD*. Même lorsqu'elles sont à l'évidence infondées, ces annonces font perdre un temps précieux de par les investigations techniques qu'elles entrainent pour démontrer leur faible niveau du risque.

Cybervor est loin d'être le seul cas de FUD repéré en 2014 ; on peut encore citer l'annonce de BAE Systems[3], la fuite de données d'ICloud[4] (le *Celebgate)* ou encore de TF1[5]. Cette dernière annonce, bien que réelle, a été surestimée en mettant en avant l'image de la chaine de télévision en lieu et place de son sous-traitant.



L'Internet des objets, nouvelles menaces et opportunités criminelles

Fabien COZIC - Enquêteur de droit privé spécialisé en cybercriminalité

Avec l'Internet des objets (ou *Internet of things – IoT*) les données ne sont plus créées par les internautes mais directement captées par les objets. Elles sont produites par l'environnement et l'activité de ceux qui les possèdent. L'objectif annoncé de ces produits est la simplification du quotidien des utilisateurs. L'objet réagit de façon autonome, influence son propriétaire et diffuse des comptes rendus sur les réseaux. En 2014, le marché a explosé mais la sécurité n'a pas été la priorité des fabricants et des prestataires. Par le passé, les chercheurs en sécurité avaient déjà démontré que des détournements étaient possibles (à Black Hat[6], au CCC, dans le *Labs* de IoActive[7]). Il n'existe pas suffisamment de normes, ni d'unification des protocoles secondaires. Les outils de chiffrement solides demeurent rares. L'Internet des objets est également exposé aux risques inhérents aux *Cloud* et au *BYOD*. Les risques imaginés en 2013 se sont réalisés l'an dernier. Dans cet environnement, le premier *thingbot*[8] (un *botnet* composé d'objets connectés) et le premier ver sont ainsi répertoriés[9]. Aux États-Unis, les cas de prise de contrôle de caméras IP se multiplient[10]. Enfin des moteurs de recherche équivoques dédiés aux objets connectés apparaissent sur la toile (Shodan, GHDB)[11].

En avril 2014, la prise de contrôle d'un baby-phone terrorise une famille

[3] http://www.cnbc.com/id/101770396
[4] http://www.lexsi-leblog.fr/conseil/sexe-securite-cloud-13-jour-du-celebgate.html
[5] http://www.zataz.com/piratage-tf1-communique-sur-le-vol-de-1-9-million-de-donnees-clients/
[6] http://securityaffairs.co/wordpress/22070/hacking/can-hacking-tools.html
http://www.atlantico.fr/decryptage/voila-comment-hackers-peuvent-prendre-controle-votre-chambre-hotel-et-que-peut-couter-nicolas-arpagian-1673076.html
[7] http://blog.ioactive.com/2014/02/internet-of-threats.html
[8] http://blog.kaspersky.com/beware-the-thingbot/
[9] http://www.welivesecurity.com/2014/10/21/proof-concept-worm-can-attack-network-attached-storage/
[10] http://www.cbsnews.com/news/baby-monitor-hacked-spies-on-texas-child/
[11] http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/

À l'horizon 2015, on peut prédire la multiplication des *thingbot* et des atteintes à la vie privée. Les objets connectés pourraient également devenir de nouveaux outils pour la criminalité dite « classique » et de nouvelles portes d'entrée sur les systèmes d'informations du monde industriel (atteintes SCADA) et de la sphère privée (*ransonware* physiques par la paralysie d'objets domestiques). Mais 2015 pourrait également être l'année des bonnes pratiques si les initiatives en matière d'outils de chiffrement et de normes *IoT* se concrétisent[12].

Objets connectés, le point juridique[13]

Garance MATHIAS - Avocat à la Cour – Cabinet d'Avocats Mathias

Les entreprises et particuliers victimes d'un défaut de sécurité ou d'un dysfonctionnement de leurs objets connectés ne sont pas démunis. L'*IoT* n'est pas une zone de non-droit. Les dispositions légales en vigueur, technologiquement neutres dans leur rédaction, peuvent s'appliquer aux objets connectés. S'agissant de la protection des données personnelles d'abord, les dispositions légales en matière « Informatique en Libertés »[14] sont applicables aux données personnelles captées par les objets connectés. Ainsi, les principes d'information préalable et de consentement exprès des personnes concernées s'appliquent. Les obligations de sécurité de données s'imposent aux responsables de traitement.

De nombreuses dispositions du droit pénal viennent également sanctionner certains comportements illicites où interviennent les objets connectés. C'est notamment le cas des infractions d'usurpation d'identité[15] ou des atteintes aux systèmes de traitements automatisés de données[16]. Enfin, un défaut de sécurité ou un dysfonctionnement d'objets connectés peut engager la responsabilité du prestataire ou du fabricant sur le fondement de la responsabilité personnelle[17] ou du fait des choses[18]. Certaines dispositions législatives spécifiques relatives par exemple à la protection du consommateur ou aux produits défectueux peuvent également couvrir les cas de préjudices résultant d'objets connectés.

Rançons et fraudes aux présidents, des pratiques en pleine explosion

Gérôme BILLOIS - Senior Manager – CERT-Solucom

En 2014, les cas de rançonnage et les fraudes aux présidents ont été nombreux.

Côté rançon, deux catégories se distinguent : l'attaque ciblée et l'attaque de masse. Dans le premier cas, l'affaire *Sony Pictures*[19] a marqué l'année de par ses répercussions sans précédent. L'attaque aurait démarré en février 2014 avec l'extraction de plus de 110 To de données. Le 21 novembre, l'établissement reçoit un courrier électronique de demande de rançon. Le groupe pirate *GOP* menace de publier sur la toile l'ensemble des informations. Sony Pictures refuse de payer.

Le 24 novembre, un *malware* se propage sur l'ensemble des postes de travail Windows et 75% des serveurs de l'organisme. L'activité de l'établissement est paralysée et les collaborateurs sont condamnés à reprendre papiers et crayons. Cette attaque a eu des répercussions sur toutes les dimensions de l'activité de Sony

---

[12] http://www.diplomaticourier.com/news/topics/security/2423-cybersecurity-the-internet-of-things-and-the-role-of-government

[13] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf ; http://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/archives/Forum-debat_7_avril_2014.pdf ; http://www.inhesj.fr/sites/default/files/securite_objets_connectes.pdf

[14] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[15] Art. 226-4-1 du Code pénal

[16] Art. 323-1 et suiv. du Code pénal

[17] Art. 1382 du Code civil

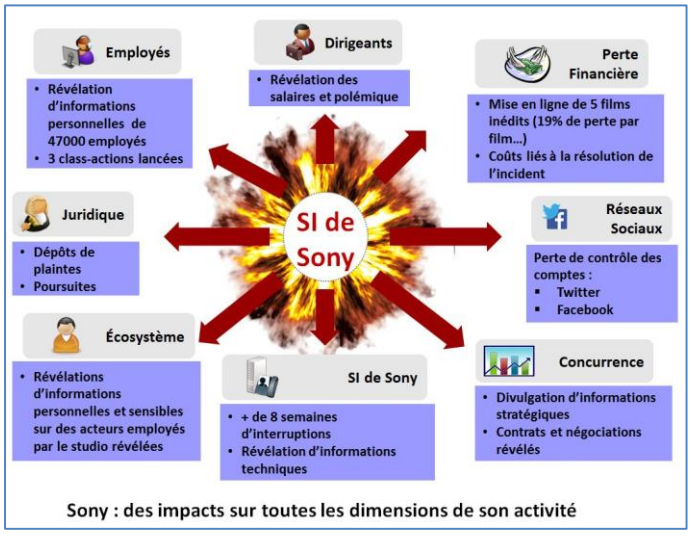
[18] Art. 1384 du Code civil

[19] http://www.theguardian.com/film/2014/dec/18/sony-hack-the-interview-timeline

Pictures. En décembre, s'ajoute la pression psychologique. Le *GOP* menace chacun des membres du comité de direction de la publication du contenu de leur messagerie professionnelle et réclame l'abandon du projet de film *The Interview*. La menace bascule dans le monde réel lorsque les pirates annoncent de possibles attentats sur les salles de cinéma qui diffuseraient le film. L'administration américaine s'en mêle : Barack Obama, accuse la Corée du Nord d'être à l'origine de l'attaque. Finalement, le 25 décembre, le film sort en salle et en ligne sans encombre. En 6 jours, il rapporte 17,8 millions de dollars. Depuis lors, le groupe *GOP* a disparu. L'identité de ses membres et leur origine demeurent inconnues et contradictoires selon les experts.

D'autres cas de rançons ciblées ont émaillé l'année 2014. On peut notamment citer les attaques visant Domino's Pizza[20], Nokia[21], Xbox & PlayStation[22], etc.

Les rançons de masse, quant à elles, ont été médiatisées par l'intermédiaire du *malware Cryptolocker*[23] qui chiffre le contenu des ordinateurs et ne donne la clé pour récupérer les données que contre un paiement. En juin 2014, l'opération *Tovar* a permis de démanteler le *botnet Gameover Zeus*, son principal vecteur de propagation[24]. Quelques mois plus tard, un service de *de-cryptcryptolocker* est proposé en ligne alors que la fin de l'année voit l'apparition de nouvelles variantes du *malware*.



Sony : des impacts sur toutes les dimensions de son activité

Des cas de fraude aux présidents[25] ont aussi fait l'actualité de 2014 (KPMG[26], Michelin[27], etc.). 700 faits ou tentatives ont été recensés entre 2010 et 2014. Plus complexes et plus astucieuses que par le passé, elles peuvent maintenant contenir un aspect *cyber* (attaque combinée *email* / téléphone, usurpation d'identité par *email*, etc.). La sensibilisation des collaborateurs, notamment au risque de *social engineering*, doit se poursuivre et s'amplifier. Et au-delà de la sensibilisation, le renforcement de la traçabilité et des vérifications dans les applicatifs métiers sensibles sont également requis.

L'année des vulnérabilités *(Heartbleed & Shellshock)*

Hervé Schauer – HSC by Deloitte

L'année 2014 a été marquée par la révélation de deux vulnérabilités majeures : *Heartbleed* et *Shellshock*. Très médiatisées, ces vulnérabilités ont touché l'ensemble des utilisateurs de l'Internet. Si ces failles trouvent leur origine dans les programmes de logiciels libres, elles ont des répercussions sur tous les logiciels propriétaires s'appuyant sur les bibliothèques *OpenSSL* pour la première, et *GNU Bash* pour la seconde. L'exploitation de la faille *Heartbleed*, introduite en décembre 2011, permet à un attaquant de lire la mémoire des systèmes disposant des versions *OpenSSL* affectées, de compromettre les clefs privées de chiffrement et de monter des attaques de l'homme du milieu (*MitM, man-in the middle*). Un correctif est apporté par la version *OpenSSL 1.0.1g* en avril 2014[28]. L'introduction de la faille *Shellshock*, quant à elle, remonte à l'année 1989. Son

[20] http://www.europe1.fr/france/rex-mundi-les-pirates-informatiques-qui-ont-voulu-ranconner-domino-s-pizza-2155193
[21] http://arstechnica.com/tech-policy/2014/06/nokia-paid-millions-in-ransom-to-stop-release-of-signing-key-in-2007/
[22] http://www.lefigaro.fr/flash-eco/2014/12/26/97002-20141226FILWWW00177-playstation-et-xbox-victime-d-une-cyber-attaque.php
[23] http://blog.trendmicro.fr/crypto-locker-un-nouveau-pas-vers-la-professionnalisation-des-cyber-delinquants/
[24] http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/
[25] http://www.cyber-securite.fr/2014/11/02/escroqueries-au-president-les-dessous-dune-fraude-a-250-millions-deuros/
[26] http://acteursdeleconomie.latribune.fr/finance-droit/2014-06-26/kpmg-les-dessous-d-une-escroquerie-record-a-7-6-millions.html
[27] http://www.lesechos.fr/finance-marches/banque-assurances/0203910698411-michelin-victime-de-larnaque-au-president-1060501.php
[28] http://en.wikipedia.org/wiki/Heartbleed

exploitation permet l'exécution de code arbitraire et la mise en œuvre d'attaques par déni de service. La version *bash43-030* intégrant l'ensemble des correctifs a été déployée en octobre 2014[29].

La révélation de ces failles a soulevé des interrogations sur la qualité et la fiabilité des logiciels libres ainsi que sur les moyens mis à disposition des programmeurs de ces logiciels. Dans ce contexte, l'association CII (*Core infrastructure initiative*)[30] regroupant les géants de l'IT a été créée pour financer les projets libres. La répercussion de ces failles a également mis en avant des lacunes dans le contrôle qualité réalisé par les grands acteurs IT exploitant les logiciels libres. Les processus de gestions des incidents ont été mis à l'épreuve. Certains ont révélé leurs dysfonctionnements. Seul point positif, l'expérience acquise lors de la gestion de ces deux failles a, sans conteste, permis aux équipes de gestion de crise d'améliorer leur mode de travail.

Les nouveaux braqueurs

Christophe Jolivet – Directeur associé – Prosica
Loïc Guézo – Directeur & Evangéliste – Trend micro

L'année 2014 a été intense par le nombre d'attaques visant les points de vente, les distributeurs de billets et les applications d'*e-banking*. Avec le *skimming* amovible[31], les distributeurs font face à des attaques toujours plus complexes. Ici, l'attaquant insère son matériel dans le collecteur de cartes pour installer un logiciel espion (*Tyupkin*[32], *Ploutos*[33]). Il revient ensuite pour récupérer les données et désinstaller le programme effaçant ainsi toute trace de l'attaque. Ces programmes sont de plus en plus nombreux. Apparaissent également des attaques plus élaborées visant non seulement les distributeurs mais aussi leurs systèmes d'administration. Il peut s'agir d'attaques multiniveaux. Dans ce cas, la première étape consiste en l'envoi de courriers électroniques piégés aux salariés (*spearphishing*). L'objectif est d'infecter leurs postes de travail pour atteindre ensuite le système d'administration des distributeurs et modifier, par exemple, les seuils de retrait. Parmi les attaques abouties, citons celles du groupe russe *Anunak*[34]. Parfois les distributeurs sont clairement défaillants, ce fut le cas aux Etats-Unis lorsque deux adolescents purent passer en mode privilégié en utilisant un compte par défaut découvert sur une notice disponible sur Internet[35].

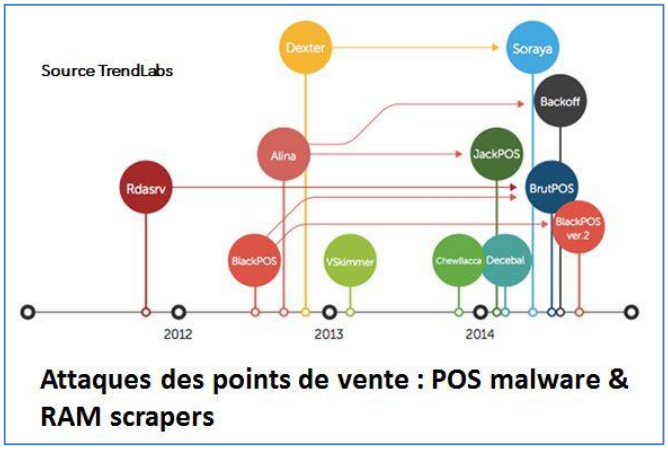
Carte électronique pour skimming amovible

[29] http://spin.atomicobject.com/2014/10/16/shellshock-cves-patches-updates/
[30] http://www.linuxfoundation.org/news-media/announcements/2014/05/core-infrastructure-initiative-announces-new-backers
[31] http://krebsonsecurity.com/2014/05/thieves-planted-malware-to-hack-atms/
[32] https://securelist.com/blog/research/66988/tyupkin-manipulating-atm-machines-with-malware/
[33] http://www.symantec.com/connect/blogs/backdoorploutus-reloaded-ploutus-leaves-mexico
[34] http://www.group-ib.com/files/Anunak_APT_against_financial_institutions.pdf
[35] http://www.cbc.ca/newsblogs/yourcommunity/2014/06/winnipeg-atm-hacked-by-14-year-olds-using-manual-found-online.html

En 2014, les cyber-braqueurs ont aussi ciblé les systèmes d'information des établissements financiers. JPMorgan fut l'une de leurs victimes avec 83 millions de comptes clients divulgués, mais sans les données bancaires[36].

Les clients sont également la cible de ces braquages avec, là aussi, des attaques multi-niveaux pour outrepasser la double authentification : piégeage de l'ordinateur, redirection vers des sites miroirs, incitation au téléchargement d'un second programme sur le smartphone, obtention du mot de passe unique et réalisation du virement frauduleux. En novembre 2014, une dizaine de personnes est placée en garde à vue. Elles sont soupçonnées d'avoir effectué des virements frauduleux réalisés notamment grâce à l'usurpation des codes envoyés sur les *smartphones* de clients de la Banque Postale (Certicode)[37].

Notons enfin que, les pirates visent de plus en plus les points de vente. On se souvient de l'affaire *Target* fin 2013 et de ses suites l'année suivante[38]. En 2014, ces attaques ont été nombreuses. On peut citer les cas de Home Depot[39], UPS[40], Michaels[41] et Goodwill[42]. Pour ce dernier, l'origine de l'attaque se trouve être un opérateur de terminaux dont Goodwill, notamment, était partenaire. Ce sont les données bancaires de 900 000 cartes qui ont alors été dérobées. Les programmes malveillants utilisés sont des *POS malware* et *RAM scraper*. Ces derniers interceptent par exemple les données inscrites sur la piste magnétique des cartes bancaires lorsque celles-ci passent en clair en mémoire au moment du paiement sur le terminal. Au cours du premier semestre de l'année 2014, un minimum de six nouvelles versions persistantes de *POS malware* ont été repérées.



Attaques des points de vente : POS malware & RAM scrapers

Évolution technique de la menace

Philippe Bourgeois – Expert Sécurité au CERT-IST

L'année 2014 a démontré que le risque d'attaque technique augmentait. Citant le cas de l'*APT DarkHotel*[43] (utilisation du réseau Wi-Fi d'un hôtel pour cibler un *VIP*) ou celui des douchettes code barre *ZombieZero*[44], on constate que des attaques jusqu'alors hypothétiques sont devenues réelles.

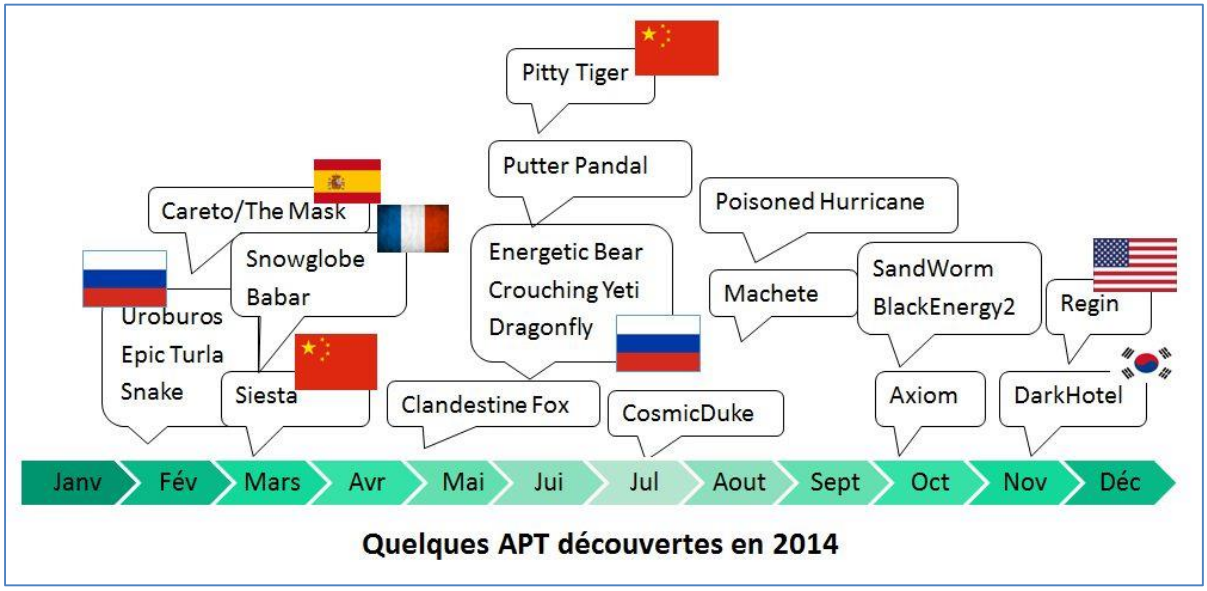
L'un des domaines techniques les plus actifs en 2014 fut la cryptographie. Ainsi, à la faille *Haertbleed* s'ajoute le bug *GoToFail*[45], *Schannel*[46] ou encore *Poodle*[47]. Au-delà de ces failles, les outils de cryptologie furent aussi attaqués. Citons en 2014 les attaques de dé-anonymisation visant *TOR*[48], et l'utilisation du *Trojan Citadel* pour obtenir la clé des coffres-forts *Keepass* ou *Password Safe*[49]. Ces attaques inquiètent. Le chiffrement étant

[36] http://www.reuters.com/article/2014/10/03/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141003
[37] http://www.linformaticien.com/actualites/id/34732/une-faille-dans-certicode-coute-tres-cher-a-la-banque-postale.aspx
[38] http://cdn.arstechnica.net/wp-content/uploads/2014/12/document4.pdf
[39] https://corporate.homedepot.com/MediaCenter/Pages/Statement1.aspx
[40] http://www.infosecurity-magazine.com/news/ups-unaware-of-pos-malware-for/
[41] http://www.observeit.com/blog/2014/12/11/throwback-thursday-michaels-pos-hacked/
[42] http://krebsonsecurity.com/2014/09/breach-at-goodwill-vendor-lasted-18-months/
[43] http://www.wired.com/2014/11/darkhotel-malware/
[44] http://trapx.com/news/press/trapx-discovers-zombie-zero-advanced-persistent-malware/
[45] https://nakedsecurity.sophos.com/2014/02/24/anatomy-of-a-goto-fail-apples-ssl-bug-explained-plus-an-unofficial-patch/
[46] http://www.zdnet.com/article/microsoft-reissues-fixed-schannel-update/
[47] https://www.openssl.org/~bodo/ssl-poodle.pdf
[48] https://blog.torproject.org/blog/being-targeted-nsa
[49] http://arstechnica.com/security/2014/11/citadel-attackers-aim-to-steal-victims-master-passwords/

l'un des piliers de la sécurité des communications et du passage dans le nuage. On notera aussi l'arrêt de *TrueCrypt*[50] en mai et les rumeurs qui en découlent.

Sur le plan expérimental, des chercheurs ont mis en avant la possibilité d'attaquer les systèmes isolés (ou *air-gapped*) par le biais de programmes reposant sur une communication par ultra-sons (démonstration au SSTIC-2014 de M. Ricordel et M. Capillon[51]), par signaux lumineux (théorie *Scangate*[52]) ou signaux FM (théorie *AirHopper*[53]).

Notons aussi le nombre important d'*APT* sur l'année. Plus de 15 de ces attaques ont été relatées par la presse. Ce chiffre est certainement inférieur à la réalité. Quant aux victimes, les États ne sont plus les seules ciblent des attaques complexes. Des entreprises et même parfois des individus sont maintenant visés.



Quelques APT découvertes en 2014

La cybercriminalité, des deux côtés de la rivière

Colonel Éric FREYSSINET - Chef du Centre de lutte Contre les Criminalités Numériques (C3N), Gendarmerie nationale

Chaque année, la presse présente des chiffres en hausse quant au coût que représente la cybercriminalité pour les États. Mais qu'en est-il de la fiabilité de ces annonces ? Sait-on évaluer l'impact de la cyber-délinquance en France ? La première difficulté consiste, pour l'entreprise victime d'une cyber-attaque, à évaluer son préjudice. Ensuite, le montant du préjudice revendiqué devant les juridictions diffère souvent de celui finalement reconnu par les tribunaux. Aux vues des plaintes reçues par la Gendarmerie Nationale, le montant total des préjudices déclarés atteint, en moyenne, 4 millions d'euros par mois.

S'agissant des infractions, le Pôle judiciaire de la gendarmerie nationale a mené une analyse sur

[50] http://linuxfr.org/news/resume-de-l-affaire-truecrypt
[51] http://www.hsc-news.com/archives/2014/000120.html (=== Les rumps ! ===)
[52] https://uptodatecybersecurity.wordpress.com/2014/10/19/scangate-yes-its-a-thing-week-8/
[53] http://threatpost.com/airhopper-program-decodes-radio-signals-to-steal-from-air-gapped-computers/109155

une « photographie » de ce qui lui était remonté[54]. Il relève ainsi chaque mois 2600 cas en moyenne de délinquance liée à l'Internet dont 1700 sont économiques et financiers. Les escroqueries représentent près de 80% des procédures d'enquête en matière de cybercriminalité. 43% des escroqueries visant les particuliers sont celles véhiculées par les petites annonces en ligne. 22% sont des escroqueries aux moyens de paiement dont la majorité consiste en l'utilisation de la carte bancaire de la victime pour réaliser des achats. A ces pratiques s'ajoutent l'usurpation d'identité (7,62%), le recrutement de mules (5%), le chantage (5%) ou encore l'escroquerie aux sentiments (4%). Les escroqueries visant les entreprises, même si elles sont beaucoup moins nombreuses, ont augmenté en 2014. Elles représentent 2% des plaintes relatives aux cyber-escroquerie enregistrées. Les principales méthodes utilisées sont les faux placements et les virements frauduleux.

La plupart de ces escroqueries pourraient être évitées par une sensibilisation des victimes quant à l'existence de ces pratiques. Ainsi, la Gendarmerie, en collaboration avec le CECyF, *Paypal* et Signal Spam ont publié une brochure d'informations : *« Comment se protéger des arnaques aux petites annonces – Conseils et liens pratiques »* disponible sur Internet.

D'un Panorama à l'autre (conclusion)

François Paget – Chercheurs de menaces – Intel Security/McAfee Labs

Depuis maintenant 14 ans le CLUSIF attire l'attention du public sur l'émergence de nouvelles menaces. Bien des années après leurs annonces, nombre d'entre elles n'ont pas disparu. Même si le Panorama 2014 n'a pas parlé cette année du *phishing*, de l'hacktivisme, de l'informatique industrielle et des monnaies virtuelles, ces thématiques sont toujours d'actualité. L'hacktivisme se durcit ; on défend moins la liberté d'expression, mais on flirte plus avec des idées terroristes (groupe *AnonGh0st*). Les attaques visant l'informatique industrielle continuent ; en Allemagne un site de production d'acier a subi d'importants dommages[55]. En France, l'OCLCTIC a démantelé une plateforme d'échange de *Bitcoins*[56]. Enfin il est à redouter que les tristes évènements de ces derniers jours ouvrent la porte à de nouvelles thématiques qui impacteront notre panorama 2015 telles que l'utilisation d'Internet comme soutien au terrorisme et les nouvelles évolutions de la législation en ce domaine[57].

Membres du CLUSIF, retrouvez les vidéos de cette conférence et les supports des interventions sur le web CLUSIF
http://www.clusif.fr/

Le Club de la Sécurité de l'Information Français est un club professionnel, constitué en association indépendante, ouvert à toute entreprise ou collectivité. Il accueille des utilisateurs et des offreurs issus de tous les secteurs d'activité de l'économie. Sa finalité est d'agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques. Il entend ainsi sensibiliser tous les acteurs en intégrant une dimension transversale dans ses groupes de réflexion : management des risques, droit, intelligence économique...
De nombreux groupes de travail se réunissent régulièrement pour traiter de thématiques variées en fonction de l'actualité et des besoins des membres.
Le CLUSIF a des relais régionaux, les CLUSIR et des partenaires européens, les CLUSI.
Contacts :
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

[54] http://fr.calameo.com/read/0027192922937f04188cf?page=110
[55] http://www.bbc.com/news/technology-30575104 /
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.html
[56] http://www.franceinfo.fr/actu/justice/article/la-gendarmerie-dementele-un-trafic-de-bitcoin-528703
[57] http://www.mirror.co.uk/news/technology-science/technology/charlie-hebdo-now-islamic-hackers-4963425