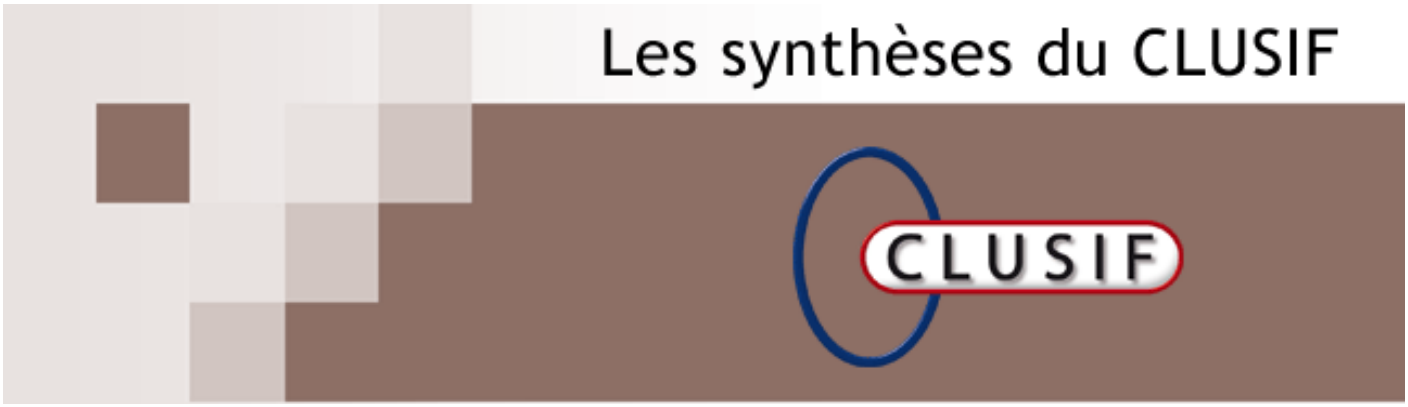

Panorama de la Cybercriminalité – Année 2015

Conférence thématique du CLUSIF du 14 janvier 2016.

Pour la quinzième année consécutive, le CLUSIF (**CLU**b de la **S**écurité de l'**I**nformation **F**rançais) dresse un tableau complet de l'état de la cybercriminalité mondiale.

Dévoilé au public et à la presse ce jeudi 14 janvier 2016, le Panorama 2015 a fait la part belle à l'Internet des objets, à la mobilité, à l'exploitation et au commerce des vulnérabilités ainsi qu'à l'évolution technique et astucieuse de la menace.

Un retour d'actualité sur les terribles évènements de novembre a également permis de mieux comprendre le rôle d'Internet durant cette période et les réponses immédiates des services de l'état dans le domaine cyber.

Pour compléter cette rétrospective l'aspect juridique n'a pas été oublié. Qu'il s'agisse des objets connectés ou du renseignement, les experts du CLUSIF ont montré que bien des choses avaient évolué au cours d'une année intense pour les cybercriminels et ceux qui les poursuivent.

Les interventions de cette année ont porté sur les thèmes suivants :

1. Attaques astucieuses ou comment les cybercriminels nous surprennent
2. 0-days : analyse des marchés noirs des outils d'attaques numériques
3. Cyber-diplomatie : Chine, États-Unis mais pas seulement
4. Jihad numérique : état des lieux, enjeux opérationnels et juridiques
5. Objets connectés : 2015 l'année du piratage des voitures, et demain ?
6. Nos téléphones mobiles : des cibles de premier plan
7. Les conséquences d'une attaque
8. (Malgré tout,) quelques raisons de se réjouir

En conclusion de cette après-midi bien remplie, le ***Préfet Jean-Yves LATOURNERIE***, *Conseiller du Gouvernement, chargé de la lutte contre les cybermenaces*, prend la parole.

Attaques astucieuses ou comment les cybercriminels nous surprennent

Fabien COZIC – Directeur d'enquêtes privées – Red Team

Fabien COZIC débute son intervention par un étonnant constat : « *Tout investi qu'il soit dans la lutte contre le cybercrime, un esprit honnête se doit de reconnaître que l'étude de certaines nouvelles techniques d'attaque lui a fait découvrir une créativité qui parfois confine au génie* ».

Souvent détaillés lors des précédents Panoramas du CLUSIF, les processus de recherche et développement de certaines entreprises criminelles ont de nouveau fait parler d'eux en 2015 avec des attaques par satellite, une modification du cœur de cartes bancaires, des détournements de services de développement d'applications ou encore de jouets électroniques. L'année 2015 a été marquée par la ruse, l'astuce et le hack au sens propre du terme pour détourner la destination première d'un objet ou d'un système afin d'aboutir à une utilisation frauduleuse et rentable.

Bien que ces pratiques du détournement d'infrastructures existantes et légitimes ne soient pas nouvelles, Fabien COZIC n'hésite pas à dire que « *en 2015, les cybercriminels ont mis les bouchées doubles notamment sur le plan technique, et qu'en conséquence, leurs méfaits se sont affichés impunément en une de la presse mondiale et que leurs gains atteignaient des sommets, obligeant au renforcement de dispositifs de sécurité devant, une fois de plus, rattraper leur retard* ».

0-days : analyse des marchés noirs des outils d'attaques numériques

Loïs SAMAIN – Consultant Cybersécurité / Cyberdéfense - CEIS

Le marché des 0-days a évolué durant l'année 2015, aussi bien d'un point législatif que d'un point technique.

On notera tout d'abord que de nouvelles boutiques en ligne sont apparues dans le DarkNet : certaines se sont spécialisées dans le commerce de produits à très haute valeur ajoutée, comme avec *TheRealDeal* qui se focalise sur la vente de codes 0-day et d'exploits. Les prix des 0-days se basent sur une règle du type « *plus le nombre de vulnérabilités est faible, plus le prix augmente.* » Pour une faille 0-day, ils varient entre 500 et 40,000 dollars. Cette année, le record revient à *Zerodium* pour une faille iOS 9.1/9.2b à 1 000 000 dollars.

Au niveau de la législation, le marché des 0-days a aussi évolué cette année. Le Bureau de l'Industrie et de la Sécurité américain (BHS) a proposé une transposition dans la loi américaine de l'évolution de *l'arrangement de Wassenaar* de décembre 2013 : en plus des logiciels d'intrusion et de communication ajoutés dans cette nouvelle version de l'arrangement, les Etats-Unis y ont joint la recherche et l'exploitation de vulnérabilités 0-days. Un fort levé de boucliers de la communauté a poussé la BHS à réfléchir à une nouvelle transposition de *l'arrangement de Wassenaar*, malgré que déjà plus de 30 états américains appliquent cette règle.

Le métier de *Bug Bounty* a aussi évolué cette année dans sa professionnalisation. En plus de nombreuses plateformes (*HackerOne*, *BugCrowd* ou encore *FireBounty*), les primes pour la découverte d'une vulnérabilité ont considérablement augmentés et les sociétés sont de plus en plus hétérogènes. Les récompenses se diversifient aussi, jusqu'à proposer des points Miles pour United Airlines. Enfin, avec l'apparition de *Zerodium*, un nouveau modèle de grossiste est apparu, avec une tarification claire et des primes très élevés pour des demandes très précises.

Cyber-diplomatie : Chine, Etats-Unis mais pas seulement

Loïc GUEZO – Cybersecurity Strategist – Trend Micro Inc.

L'Internet est-il devenu le nouvel espace de confrontation des pouvoirs ?

Loïc GUEZO rappelle en introduction quelques éléments clé sur la structure de gouvernance de l'Internet : « *Depuis sa création en 1998 l'ICANN était par construction sous dominance américaine. Mais les dernières années ont vu cette position très challengée, notamment par la Chine. En 2013* », poursuit-il, « *suite aux premières révélations Snowden sur la surveillance de masse effectuée par la NSA, le monde entier, prenant conscience de sa dépendance d'un Internet gouverné de facto par les Etats-Unis, a exprimé sa perte de confiance dans les systèmes de gouvernance actuels et une volonté forte de les rééquilibrer, au profit de tous, dans le manifeste de Montevideo sur le futur de la coopération Internet* ».

Présentant ensuite l'actualité de l'année sous l'angle des rapports Etats-Unis/Chine, il a souligné la part grandissante des aspects cyber dans toutes les dernières réunions bilatérales diplomatiques de l'année 2015, mais aussi, multilatérale, comme en marge de la COP21 de Paris. Il précise que « *si l'on parle désormais favorablement de cyber-diplomatie, il ne faut pas oublier que le cyber est désormais partie prenante de tous les conflits ou confrontation géopolitique, notamment des attaques ciblées gouvernementales* ».

Le cas récent de piratage de l'Office de Gestion du Personnel américain (OPM), rendu public en juillet 2015 et attribué par les Etats-Unis à la Chine, a servi de fil rouge à cette démonstration. « *Face à l'ampleur d'un piratage, qui concerne les données personnelles de plus de 20 millions d'agents du gouvernement américain, dont des entretiens classifiés pour l'obtention de postes sensibles liés à la sécurité nationale, ou des relevés d'empreintes digitales - ce qui est inédit - les Etats-Unis et la Chine se sont retrouvés autour d'une table pour négocier et sortir par le haut en annonçant avoir trouvé un terrain d'entente : arrestations de hackers en Chine, définition de lignes de bonne conduite sur le commerce… en termes très diplomatiques* ».

Loïc GUEZO présente ensuite les positions respectives d'autres pays, dont les approches sont différentes (Russie, Iran, Corée du Nord) et conclut par la position française indiquant que le 19 octobre dernier, concomitamment à l'annonce de la Nouvelle Stratégie Nationale pour la Sécurité du Numérique, nous avions appris la nomination de M. David Martinon, en qualité d'ambassadeur pour la cyber-diplomatie et l'économie numérique.

Jihad numérique : état des lieux, enjeux opérationnels et juridiques

François PAGET – Secrétaire Général Adjoint du CLUSIF et animateur du groupe « Panorama »

Deux représentants de la Sous-Direction de Lutte contre la Cybercriminalité / Division de l'anticipation et de l'analyse – Ministère de l'Intérieur

Amélie PAGET – Consultante Juridique SI – HSC by Deloitte

En marge des attentats de 2015, Internet et les réseaux sociaux ont joué un rôle différent et plus important que par le passé. Ces dernières années, a expliqué Francois PAGET, « *la toile était connue comme une plateforme de communication et de propagande pour des groupes terroristes qui découvraient, sur le tard, les nouvelles technologies* ».

Parallèlement à l'essor de Twitter et de Facebook et au détriment des forums de discussion, Daesh a, selon lui, changé la donne en s'entourant de spécialistes des médias, de la vidéo et parfois du renseignement. « *Ceux-ci connaissent maintenant le Darknet et ses boutiques* », ajoute-t-il. Au-delà de la propagande, ils diffusent des conseils avisés en matière de communication et de chiffrement. Ils poussent leurs sympathisants à se tourner vers de nouvelles plateformes d'échanges telles que Telegram. Le discours reste simpliste et fédérateur et la mise en relation est parfois facilitée par les modules de suggestion d'amis qu'offrent toutes ces applications.

A l'occasion de cette triste actualité, le délai de réaction face à des contributions à éliminer a parfois été critiqué. Avec le mouvement Anonymous, la riposte est aussi passée par Internet. Elle a connu son lot habituel d'approximations et de bévues allant parfois même, le craint Francois PAGET, « *jusqu'à compliquer le travail des services de renseignement* ». Les réseaux sociaux ont aussi permis, dans l'urgence, l'essor d'inattendus élans de solidarité (#PorteOuverte). « *Certains y verront peut-être une*

arrière-pensée mercantile, mais le contrôle d'absence de danger (bouton Safety check), puis le filtre tricolore en solidarité avec notre pays, ont été généralement très appréciés ».

Il y a bien sûr eu des rumeurs et des fausses alertes, mais la présence constante des forces de sécurité sur ces mêmes réseaux sociaux en a minimisé l'impact. Force est donc de constater qu'Internet joue, dans le domaine du terrorisme, un rôle important. Il n'est cependant jamais seul dans les trajectoires de radicalisation : « *consulter un site djihadiste ne fait généralement pas de vous un djihadiste* » indique Francois PAGET, « *il peut être un facteur de renforcement de la radicalisation, mais des rencontres et des interactions sociales au sein du monde réel seront généralement nécessaire avant le passage à l'acte* ».

* * * *

Pour les représentants de la Direction Centrale de la Police Judiciaire, les attentats de janvier et novembre 2015 ont consacré les nouvelles formes de terrorisme dans leur accompagnement et leur contextualisation via Internet. Les terroristes utilisent désormais activement les moyens de communication modernes, notamment les principes du marketing viral, pour toucher leur cœur de cible de la façon la plus large et la plus efficace possible.

A cette évolution répond un changement similaire dans la lutte contre le terrorisme : l'anti-terrorisme 2.0 a fait son apparition. En janvier, les signalements effectués par des citoyens sur la plateforme PHAROS (http://internet-signalement.gouv.fr) ont été multipliés par 10 par rapport à la normale. Au-delà de l'expression d'une émotion, ils avaient aussi pour but de lutter activement contre le terrorisme en signalant aux autorités des contenus annonçant des attentats à venir ou relevant de l'apologie.

Cette tendance s'est amplifiée en novembre 2015 : la qualité policière des informations envoyées a très fortement progressé avec une proportion beaucoup plus importante de signalements pertinents donnant lieu à procédure judiciaire. La réponse des autorités n'est pas en reste : la coopération entre les services antiterroristes et de lutte contre la cybercriminalité est toujours plus importante. Les unités judiciaires cyber sont co-saisies pour apporter leur soutien tandis que les unités techniques fournissent leur expertise aux groupes d'enquêtes durant les perquisitions. La DCPJ affirme donc sans détour, que tant du côté des forces de l'ordre, que du grand public, la lutte antiterroriste 2.0 est en marche.

* * * *

En troisième partie de cette intervention, Amélie PAGET aborde l'aspect juridique de la question. Au cours de ces quinze dernières années, rappelle-t-elle, l'arsenal judiciaire dédié à la répression du terrorisme n'a cessé de se renforcer. L'année 2015 a été dédiée aux pouvoirs de police administrative et, réaction politique aux évènements de 2015, les textes consacrés à la prévention du terrorisme se sont multipliés. Ces projets et propositions de loi très médiatisés ont fait l'objet de critiques multiples. Entrant dans le cœur du sujet, Amélie PAGET présente les dispositions consacrées à la surveillance des communications électroniques et les textes définitivement adoptés.

Il s'agit d'abord de la loi du 24 juillet 2015 relative au renseignement. Elle permet aux services de renseignement d'accéder aux données de connexion, d'intercepter les correspondances électroniques et d'échanger sur les réseaux sociaux. Ces prérogatives sont renforcées lorsqu'elles sont justifiées par la prévention du terrorisme.

En second lieu, le régime des interceptions administratives des communications émises ou reçues à l'étranger, censuré par le Conseil constitutionnel, a fait l'objet d'un texte isolé : la loi du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales.

Suite aux attentats de novembre dernier, l'état d'urgence a été déclaré puis prorogé pour une durée de trois mois par la loi du 20 novembre 2015. Les dispositions de la loi de 1955 ont été complétées afin, notamment, d'ajouter des pouvoirs d'investigation numérique aux prérogatives de police administratives. Ainsi, dans le cadre de l'état d'urgence, les forces de l'ordre peuvent accéder aux systèmes informatiques et copier les données accessibles depuis les équipements se trouvant sur les lieux d'une perquisition. Le Ministre de l'Intérieur peut également ordonner l'interruption d'un service de communication en ligne faisant l'apologie ou provoquant à la commission d'actes terroristes.

En conclusion, Amélie PAGET a enfin évoqué les projets annoncés pour 2016 telle que le projet de loi constitutionnelle pour la protection de la Nation, la proposition de loi renforçant la lutte contre le crime organisé et son financement, l'efficacité et les garanties de la procédure pénale ou encore le droit au chiffrement.

Objets connectés : 2015 l'année du piratage des voitures, et demain ?

Gérôme BILLOIS – Senior Manager – CERT-Solucom

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

2015 aura vu le premier piratage d'une voiture de série permettant de désactiver ses freins ou encore d'éteindre son moteur à distance pendant qu'elle roule. Heureusement, ce piratage a été réalisé par des chercheurs en sécurité sans intention de nuire. « *Cette démonstration montre la vulnérabilité des véhicules qui sont aujourd'hui des objets connectés comme les autres mais où les conséquences d'une attaque peuvent être beaucoup plus grave* » analyse Gérôme BILLOIS, expert en cybersécurité au cabinet Solucom. L'année dernière a vu la multiplication des cas d'attaques réussies sur des objets connectés divers et variés tels que des poupées, des fusils de *snipers*, des babyphones, ou encore des pompes à insuline.

Tout ceci montre que la cybersécurité est encore trop souvent négligée dans les phases de conception et de tests de ces objets. « *Les cas médiatiques majeurs de 2015 commencent doucement à faire réagir les acteurs fabriquant ces objets, mais les sécuriser n'est pas simple et il faut disposer des compétences pour le faire* » complète Gérôme BILLOIS, « *et attention il ne faut pas sécuriser ces objets comme si c'étaient de simples ordinateurs, nous avons par exemple vu des voitures qui exigent d'être mise à jour et qui pendant ce temps ne peuvent pas rouler! C'est quelque chose qui n'est pas acceptable par le grand public* ». Il faut donc repenser en profondeur la sécurité des objets connectés, dans toutes leurs dimensions. Et c'est aujourd'hui une nécessité car les objets connectés laissent deviner un futur rempli d'objets autonomes (voitures, robots…) qui agiront en fonction de leur algorithme.

Abordant alors l'aspect juridique, Garance MATHIAS, appuie cette affirmation, indiquant que « *se pose alors, au-delà des questions techniques, des questions juridiques où la notion de responsabilité devra se réinviter. C'est un débat de fond qui doit être ouvert alors même que les principaux sujets liés aux objets connectés ne sont pas encore totalement instruit.*» En effet, les objets connectés collectent beaucoup de données sur nous et sur nos habitudes. Ils vont ensuite les stocker dans des systèmes informatiques bien nébuleux. Et Garance MATHIAS de conclure : « *le risque juridique doit être analysé et traité en profondeur pour éviter de potentiels poursuites, et ce pas uniquement en cas d'incidents. Les fabricants sont naturellement concernés, mais des sociétés de renoms qui recommandent certains objets à leurs clients peuvent aussi être potentiellement inquiétés, elles ont tout intérêt à effectuer des vérifications en profondeur avant de communiquer sur des partenariats.*»

Nos téléphones mobiles : des cibles de premier plan

Colonel Eric FREYSSINET – Ministère de l'Intérieur/Cybermenaces

Les plates-formes de téléphonie mobile - les réseaux comme les terminaux - restent une cible privilégiée des cyberdélinquants. Et ceux-ci continuent d'innover. Eric Freyssinet a évoqué plusieurs exemples de ces innovations, qu'il s'agisse de nouvelles formes de rançongiciels, du contournement des outils de développement ou encore de l'exploitation avancée des protocoles qui sont au cœur des communications mobiles comme la signalisation SS7.

Pour Eric FREYSSINET, il faut rester attentif à ces évolutions, car les terminaux mobiles sont une cible de plus en plus intéressante pour les délinquants, même si cela reste un univers où l'utilisateur et ses données sont relativement bien protégés grâce aux nombreuses fonctions de sécurité intégrées. Et au final, comme souvent, c'est l'utilisateur qui se révèle vulnérable en commettant la plupart des erreurs qui s'avèreront ensuite fatales à la sécurité de ses usages mobiles.

Les conséquences d'une attaque

Colonel Eric FREYSSINET – Ministère de l'Intérieur/Cybermenaces

Dans ce second sujet, et au travers des suites de plusieurs attaques importantes qui ont fait l'actualité des deux dernières années, Eric FREYSSINET évoque les conséquences qu'elles ont pu avoir, sur les entreprises ciblées et éventuellement sur les utilisateurs

finaux de leurs services. Parfois, comme dans l'attaque qui a frappé l'entreprise américaine Target, les conséquences les plus importantes se font jour plus d'un an après l'attaque.

Pour Eric FREYSSINET, le cas de la plate-forme de rencontres amoureuses Ashley Madison est intéressant en ce que l'objectif des cyberdélinquants était apparemment avant tout de nuire à l'entreprise alors que c'est peut-être surtout les utilisateurs finaux qui ont le plus pâti de la situation, avec parfois des conséquences dramatiques.

En conclusion, Eric FREYSSINET a rappelle la nécessité de prévenir et se préparer aux conséquences de ces attaques, c'est-à-dire être conscient des risques, mettre en œuvre les moyens de s'en prémunir et se préparer à gérer l'incident et d'en maîtriser les conséquences, y compris pour les tiers.

(Malgré tout,) quelques raisons de se réjouir

François PAGET – Secrétaire Général Adjoint du CLUSIF et animateur du groupe « Panorama »

Autour du monde, tout au long de l'année 2015, les services de police, parfois aidés par des entreprises privées, ont pu mettre un terme à diverses actions délictueuses aboutissant parfois à l'arrestation de ceux qui les menaient. Un cours diaporama en a listé, mois par mois, les plus emblématiques.