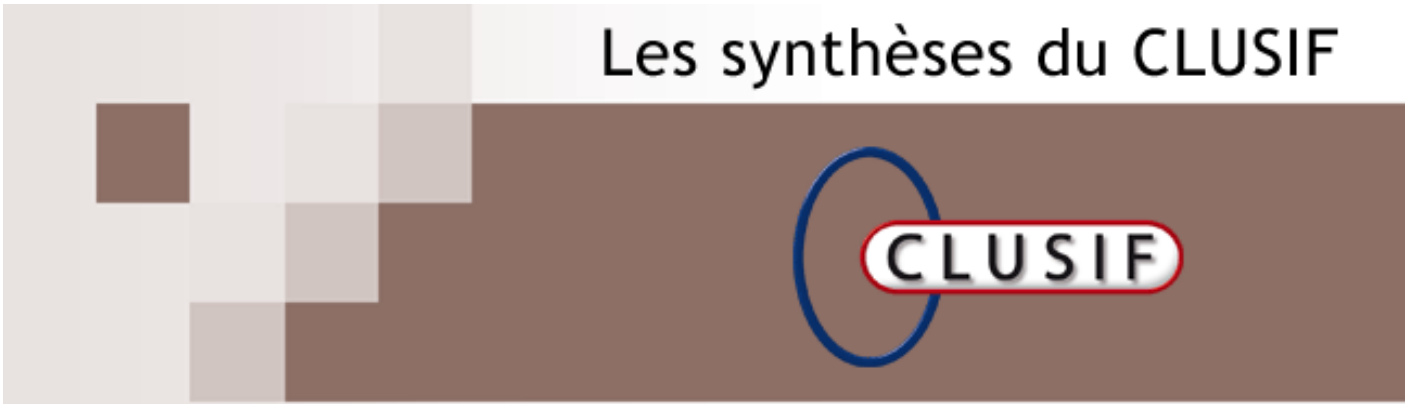

Panorama de la Cybercriminalité – Année 2017 : *Synthèse de la conférence thématique du CLUSIF du 18 janvier 2018*

Le Panorama annuel de la Cybercriminalité du CLUSIF a été dévoilé le 18 janvier 2018. Au cours de cette conférence, les experts du groupe de travail ont présenté un **bilan en matière de** cybercriminalité **mais également en matière d'événements sociétaux** en relation avec la sécurité de l'information. Plusieurs thématiques ont été balayées : les attaques destructives, les attaques *via* des tierces parties, la gestion de crise et ses limites, les vecteurs d'attaques innovants, les enjeux géopolitiques, notamment l'influence sur les élections, les rançons, le Bitcoin, le Darknet. Ce groupe de travail réunit des experts adhérents du CLUSIF mais aussi invités experts.

L'animateur du groupe de travail, Loïc Guézo, a rappelé que le groupe de travail comprend une trentaine de membres qui, sur la base de sources ouvertes, sélectionnent et approfondissent les nouvelles tendances, les événements qui marquent le domaine de la sécurité des systèmes d'information, ceux qui auront des répercussions l'année suivante, en l'occurrence en 2018. Les groupes du CLUSIF qui travaillent sur la sécurité des systèmes industriels et sur l'Internet des objets ont rejoint la liste de ceux qui échangent avec celui du panorama de la cybercriminalité, comme MIPS.

Attaques destructives

Hervé SCHAUER, HSC by Deloitte

Hervé Schauer a exposé l'impact de Wanacry et de NotPetya, deux logiciels malfaisants qui ont fait la une en 2017. « Les deux successeurs de Petya, apparu en 2016 comportaient une nouveauté : un chiffrement de bas niveau, c'est-à-dire l'amorçage du disque par exemple, et non plus simplement les documents », a précisé Hervé Schauer. « En 2017 apparait un nouveau rançongiciel, PetWrap, une profonde amélioration faite à partir de Petya qui est commercialisée en mode "ransomware as a service" où le distributeur partage les bénéfices avec les auteurs ». La diffusion par le groupe de hackers Shadow Brokers d'outils et de failles dérobées à l'Equation Group, le centre cyber-espionnage de haut-niveau de la NSA, va avoir « une forte incidence sur l'avènement d'une nouvelle génération de rançongiciels comme Wanacry et NotPetya », poursuit Hervé Schauer. NotPetya n'est pas un rançongiciel, mais un *wiper* qui efface les données. Plus ciblé que Wanacry, il fera finalement toutefois moins de dégâts.

Dans l'ensemble, Wanacry et NotPetya ont eu des conséquences majeures mais heureusement dans un nombre de sociétés limitées. Elles ont **« permis de sensibiliser et ont constitué un entrainement pour les cellules de crise »**, conclut Hervé Schauer.

Attaques via des tierces parties

Gérôme BILLOIS, Wavestone

Au cours de l'année écoulée, certaines attaques ont été plus sournoises et difficiles à contrer que les rançongiciels.

C'est notamment le cas des attaques *via* tierces parties. « Sans intention de nuire, des fournisseurs majeurs ont été à l'origine de failles de sécurité très importantes. Nous pouvons citer Apple avec les multiples bugs permettant d'accéder à des informations confidentielles, Microsoft avec le gestionnaire de mots de passe dont on pouvait voler… les mots de passe ou encore les fabricants de processeurs, comme Intel, avec les failles Meltdown et Spectre qui donnent accès à des informations confidentielles dans la mémoire des ordinateurs », a expliqué Gérôme Billois.

Ces « *supply chain* attacks » ont toujours existé mais **leur multiplication et leur gravité ont rendu plus complexe le travail des équipes de sécurité**. Gérôme Billois a par exemple cité le cas de la faille dans WPA ou celle de l'Intel management engine. En outre les réponses apportées par les fournisseurs ont parfois été discutables. Apple a par exemple réintroduit une faille précédente dans un deuxième correctif.

2016 a été marquée par des piégeages massifs *via* des éditeurs, comme celui de Ccleaner avec 2,27 millions d'ordinateurs touchés. L'attaque visait en fait 18 grands groupes dont 8 ont été infiltrés, et non pas les particuliers.

Le piégeage des infogérants a également montré **l'inventivité des pirates qui ont ainsi exfiltré des données des clients**. Gérôme Billois a cité quelques exemples, dont CloudHoper, avec une attaque débutée en 2014 et découverte seulement en 2017. « Cette tendance lourde va sans doute se développer en 2018 et l'observation des comportements des ressources autorisées sera un challenge pour 2018 et le futur », a-t-il conclu.

La gestion de crise et ses limites

Erwan BROUDER, BSSI

Bien que l'État règlemente pour protéger au mieux les actifs sensibles, que les entreprises s'organisent avec la mise en place de CERTs, de SOC, d'outils de gestion de crise, Erwan Brouder a rappelé que certaines attaques ont eu des répercussions très importantes pour certaines entreprises qui n'ont pas géré très efficacement des attaques.

Equifax a ainsi déclaré en septembre 2017 un vol de données. Quelque 140 millions de consommateurs ont été touchés (nom, adresse, numéro d'assurance sociale et dans certains cas les numéros des cartes de crédit). Plusieurs erreurs de gestion de la crise se sont accumulées et ont abouti à une très forte baisse du cours d'Equifax et à la démission du PDG. Tout d'abord, les consommateurs n'avaient pas donné leur consentement pour la collecte de certaines données. Le portail mis en place pour les victimes utilisait un certificat auto-signé qui déclenchait un message d'alerte dans le navigateur des visiteurs. En outre, les utilisateurs du service devaient s'engager à renoncer à toute action en justice. Enfin, Bloomberg a révélé que des cadres dirigeants avaient vendu leurs actions de l'entreprise avant l'annonce. **L'effet conjugué a été déplorable.**

Autre société visée par une attaque : Uber. L'annonce d'une fuite de données concernant 57 millions d'utilisateurs dont 600 000 chauffeurs a terni l'image de l'entreprise. D'autant que cette fuite a été dissimulée pendant un an.

« **Dans un monde numérique, la confiance devient le capital à sauvegarder** et la bonne préparation des processus de gestion de crise cyber au sein d'une organisation permet de limiter les impacts d'une cyber-attaque en protégeant cette confiance », a souligné Erwan Brouder.

Vecteurs d'attaques innovants

Michaël JACQUES, Inventiva
Franck VEYSSET, Michelin

En 2017, certaines fuites de données ont touché le *cloud computing*, a pour sa part indiqué Michaël Jacques. Les clients

visés ont parfois surpris, comme la NSA et l'armée américaine. Des données stockées sur AWS S3, certaines avec des attributs comme « Top Secret » ou « NOFORN » (No Foreign Nationals) étaient accessibles. Accenture a également été touchée à la suite de l'exposition de plusieurs espaces de stockage AWS S3. Deloitte a pour sa part été victime d'une attaque visant sa messagerie (MS Office 365).

Ces attaques mettent en lumière la problématique de la sécurisation des containers et la non-utilisation de mécanismes de gestion d'identification et d'authentification.

Franck Veysset indique que « comme il fallait s'y attendre, l'Internet des Objets a continué son *expansion* en 2017 – et les menaces déjà identifiées lors du précédent panorama se sont confirmées ». Des botnets (réseau de milliers d'objets compromis) sèment toujours la terreur sur Internet en entrainant des perturbations de type « déni de service distribué ». Franck Veysset alerte tout au long de sa présentation sur le fait que « l'omniprésence des objets connectés nous amène aussi **à nous questionner sur notre dépendance vis-à-vis de ces technologies, sur la protection de notre vie privée, et sur les dérives et usages que peuvent / pourraient en faire les cybercriminels**… »

Toutefois, Franck Veysset qui a relevé un système de gestion très évolué du botnet IoTroop, a précisé que, pour l'instant, en dépit de la taille annoncée de certains botnets, les conséquences visibles restaient faibles. « C'est une épée de Damoclès », a-t-il expliqué.

D'autant que les objets connectés sont de plus en plus nombreux et variés, comme les jouets, les aspirateurs munis de caméras et capables de dresser une cartographie de nos logements, les téléviseurs connectés, les serrures (Garadget et Lockstate) et les outils comme SIRI, Google Home ou Alexa (Amazon), ainsi que les voitures…

Elections et cyber, les enjeux géopolitiques

Loïc GUEZO, Trend Micro

Dans le prolongement des panoramas de 2015 et 2016, la géopolitique mondiale a été largement exposée en 2017 aux influences cyber, a souligné Loïc Guézo. Tout d'abord, 2017 a été marquée par la publication de rapports des services de renseignement américains validant une implication de la Russie dans des tentatives d'interférences sur l'élection présidentielle américaine de 2016 et sur les machines de vote. En 2017, c'est Twitter qui a été pointé du doigt comme outil de manipulation par la Russie.

En France, le parti « En Marche ! » a indiqué avoir fait l'objet d'attaques sur son site Web et de *spear fishing*. L'élection s'est conclue sur un « MacronLeak » « quelques heures avant la période de réserve électorale du second tour ; sans qu'un lien clair de cause à effet soit établi entre ces différentes étapes, sur lesquelles beaucoup de flou, parfois volontaire, persiste », a souligné Loic Guezo. **L'attribution politique reste une problématique centrale dans ces affrontements cyber entre pays.**

Rançon : payer ou ne pas payer ?

Garance MATHIAS, Avocats Mathias
Luc VIGNANCOUR, Marsh

Garance Mathias et Luc Vignancour, ont pour leur part évoqué la problématique des rançongiciels. Après un rappel des définitions juridiques (chantage, escroquerie, recel, etc.), Garance Mathias a évoqué les conséquences liées au paiement ou non une rançon, sur l'entreprise. Tous deux ont rappelé **l'importance du dépôt de plainte** qui place l'entreprise dans le rôle de la victime et ouvre la voie à une indemnisation. Luc Vignancour a évoqué les assurances

cyber qui permettent de couvrir les risques liés aux attaques et les conséquences variées qui peuvent être couvertes par de tels contrats.

Bitcoin & Co : l'envol des prix attire les cybercriminels

Gérôme BILLOIS, Wavestone

Autre sujet repéré par le groupe de travail du Panorama de la Cybercriminalité en 2018, les crypto-monnaies dont l'envolée des cours a attiré les cybercriminels. Gérôme Billois, a évoqué les attaques contre des places d'échange, des opérations de mise sur le marché mais aussi les porte-monnaie électroniques des particuliers. « Aucun maillon de l'écosystème des crypto-monnaies n'est à l'abri, les cybercriminels cherchent la moindre faille pour voler ces monnaies », a-t-il précisé. Si ces technologies sont solides, c'est l'environnement qui l'est moins. Gérôme Billois a ainsi rappelé la modification de l'adresse Bitcoin sur une page Web qui avait permis de détourner des sommes très conséquentes.

Ils ont été arrêtés : le Darknet mais pas que…

Frédéric FRAISSE, Ministère de l'Intérieur, DCPJ/D2A

Frédéric Fraisse, du ministère de l'Intérieur a fait un tour d'horizon des affaires (et des arrestations) liées au Darkweb, comme les places de marché Alphabay et Hansa. Les forces de l'ordre ont adapté leurs méthodes. Elles ont renforcé la coopération internationale et le rôle de coordination des grandes agences telles qu'Europol, Eurojust et Interpol. « Contrairement à ce qu'il est communément entendu, il n'est pas d'espace de l'Internet (darknet, deepnet) où les forces de l'ordre ne puissent agir », a-t-il précisé. Pour sa part, Jérôme Notin, directeur général du GIP ACYMA, a évoqué les missions de Cybermalveillance.gouv.fr : l'assistance aux victimes, la prévention et la sensibilisation et la création d'un observatoire de la menace numérique.

La conférence s'est terminée sur une série de questions de la salle aux intervenants. L'une d'elles a porté sur la possibilité de qualifier d'acte de guerre une attaque massive dans le domaine cyber. La nomination du général Olivier Bonnet de Paillerets qui fait partie de l'état-major unifié toutes armes, montre que la question se pose et aux Etats-Unis, la doctrine est désormais claire, une attaque Cyber peut engendrer une réponse physique. La problématique de l'attribution entre ici en compte et des actes cyber peuvent constituer un engrenage supplémentaire.

La possibilité d'une attaque massive, notamment par déni de service sur les réseaux mobiles a également été abordée. Même si cela n'a pas encore été le cas, ce n'est pas impossible, ont estimé les intervenants.

Pour retrouver toutes les présentations et vidéos en ligne :
https://clusif.fr/conferences/panorama-de-cybercriminalite-annee-2017/

A propos du Club de la Sécurité de l'Information Français (CLUSIF)

Le CLUSIF est un club professionnel constitué en association indépendante (Association Loi 1901). Ouvert à toutes les entreprises et collectivités, ce club rassemble des Offreurs et des Utilisateurs issus de tous les secteurs de l'économie. L'objectif principal du CLUSIF est de favoriser les échanges d'idées et les retours d'expériences par des groupes de travail, des publications et des conférences thématiques. Les sujets abordés, en relation avec la sécurité de l'information, varient en fonction de l'actualité et des besoins des 650 membres de l'association.

CONTACT
Luména DULUC, déléguée générale – lumena.duluc@clusif.fr / 06 21 04 86 02