Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

Panorama de la Cybercriminalité en 2015 : Attaques sur tous les fronts !

La nouvelle édition du panorama de la cybercriminalité du CLUSIF a fait la démonstration que la crise ne touche pas les pirates informatiques bien au contraire. Ils restent toujours aussi inventifs d'autant que leur terrain de jeu s'accroit grâce à l'introduction des nouvelles technologies dans de plus en plus de domaine entre autre avec les objets connectés. En parallèle, le cyber-terrorisme s'il n'est pas encore avéré au sens d'attaque visant à des détruire des entreprises ou des infrastructures critiques se sert du net pour tisser sa toile en recrutant des futurs terroristes, en menant des actions de communication, voir en servant de support pour monter des opération sur le terrain… cette année riche en actions malveillantes laisse augurer du pire pour 2016…

Après l'introduction par Lazaro Pejsachowicz, le président du CLUSIF qui a présenté les différentes activités de l'association, le panorama a débuté. En introduction il a rappelé que le cyber-crime se porte très bien. En outre, il a annoncé qu'en juin prochain aura lieu la conférence sur les résultats de l'enquête MIPS pour Menaces Informatiques et Pratiques de Sécurité.


Fabien Cozic

Quelques astuces utilisés en 2015

Fabien Cozic, directeur d'enquêtes privées Read Team Investigation, a passé en revue quelques astuces utilisées par les pirates a commencé par la Yes Card qui a exercé ses activités en France et en Belgique. Le pirate était un ingénieur qui avait rajouté une petite puce de la carte bancaire qui permettait de valider les transactions en se substituant à la puce déjà installée.
Un groupe de pirate avait mis en place un système astucieux de déposé et de retrait des sommes. Puis une équipe en République Tchèque puis un second groupe effectuait des transactions aux Etats-Unis puis les annulait et récupérait ainsi de l'argent. Le préjudice se chiffrerait autour de 6 millions d'euros.
XCode Ghost qui a détourné le système de contrôle des applications d'Apple. Les pirates ont utilisé une faille humaine de ce système pour déposer des malwares afin de récupérer des informations
Le malwares Turla a utilisé des APT pour réaliser des écoutes en se servant des liaisons des satellites de communication.
Un malware a été conçu pour prendre le contrôle de la lunette de visé d'un fusil afin de déclencher le tir…
Pour conclure il a cité le détournement d'un jouet en utilisant le système de communication pour ouvrir les portes de garages. Ce malware a contribué à plusieurs cambriolages aux Etats-Unis.


Hervé Schauer

Le 0 Days un business juteux pour les entreprises

Loic Samain du CEIS représenté par Hervé Schauer a présenté l'évolution du business des 0 Days. La palme de l'année revient à un 0 Day sur IOS qui a été récompensé par 1 millions de $. Les systèmes de plateforme de 0 Day existent et se développent. Leurs clients sont tout d'abord les gouvernements qui veulent réaliser des écoutes, mener des attaques… Il a donné quelques exemples de prix comme par exemple 2000$ pour un 0 Day ciblant un site de ecommerce, pour Windows le prix est de 150000$… et pour IOS a atteint 1 million de $.
Le 20 mai 2015 la proposition Wassenaar sur les 0 Day a été publié et elle est déjà adopté par plusieurs pays. Une nouvelle proposition pour amender cette proposition devrait être faite en 2016. Aujourd'hui les primes aux 0 Days explosent avec des prix allant de 2000$ à plusieurs milliers de $. Ainsi, les entreprises de Bug Bounty voient leur valorisation exploser.
Ainsi, Vupen est devenu un grossiste en 0 Day et s'appelle aujourd'hui Zerodium. En janvier 2016 une faille de sécurité a été payée 100 000$ par cette entreprise pour la découverte d'une faille sur flash. Pour Hervé Schauer « 2015 est donc l'année de la professionnalisation de ce marché. »


Loïc Guezo

La cyber-diplomatie commence à émerger

Loïc Guezo, Strategist chez Trend Micro, a expliqué que l'on va vers une cyber-diplomatie avec entre autre la remise en cause de l'ICANN qui est au centre de très grandes manœuvres. On a de nombreux pays qui reconnaissent une capacité offensive sur Internet a commencé par les États-Unis, la Grande Bretagne, la Chine, la Russie et maintenant la France. En 2015, il a rappelé le cas du piratage OPM qui est une sorte de RH des agents des services spéciaux américains avec la récupération très personnel sur l'ensemble des collaborateurs. La Chine a été suspectée d'être l'auteur de ce piratage. Suite à cette accusation plusieurs arrestations ont eu lieu en Chine afin de faire diminuer les tensions entre ces deux pays. Aujourd'hui, le doute persiste sur la nature des personnes arrêtées. Le 31 décembre 2015 les autorités américaines ont ressortie une attaque sur 2009 ciblant Microsoft. Par contre Microsoft n'a pas alerté ces clients. Par ailleurs, la Russie a signé un pacte de non-agression avec la Chine mais ne signifie pas l'arrêt des opérations entre ces deux pays, il y a par contre une convergence de doctrine sur l'Internet autour de l'idée de souveraineté.
Quant à l'Iran et dans une moindre mesure à la Corée du Nord, ils ont été pointés par les Etat-Unis comme deux dangereux pays sources de piratages.
Par ailleurs, il a cité l'Accord Umbrella qui a été noté comme une grande avance en particulier Ui permet de facilité les procédures d'extradition. En France, il faut noter la publication de la Nouvelle Stratégie de la sécurité du numérique. A cette occasion, David Martinon a été nommé Ambassadeur pour la cyber-diplomatie et de l'économie digitale.
La cyber-diplomatie est devenue un élément clé de la vie politique dont l'influence géopolitique prévue dans cette nouvelle stratégie.

François Paget

Le Djiad Numérique : recrutement, endoctrinement…

François Paget a présenté pour sa part le Djiad Numérique. Lors du panorama 2004, il avait été évoqué l'utilisation d'Internet par les terroristes. Aujourd'hui, ils utilisent les réseaux sociaux et adressent plusieurs milliers de Tweet par jour. Daesh offre des conseils pour se dissimuler via par exemple les réseaux Tor, mais aussi Telegram. Ce dernier réseau social est dominant en Russie. Il permet de communiquer de façon chiffrée mais aussi de détruire les messages une fois lus. Les djihadistes se servent aussi du darknet, peut-être de Bitcoins… pour acheter des armes. Sans compter que les réseaux sociaux sont utilisés pour recruter des membres mais ce n'est pas le seul vecteur d'enrolement.
En novembre, les Anonymous se sont réveillés pour attaquer les djihadistes avec des actions parfois intéressantes, mais ils aussi ont réalisé des bévues qui ont parfois ralenties les actions des forces de police, voire aussi en attaquant des sites qui étaient en arabes mais sans aucun lien avec les terroristes.
En janvier dernier, il y a eu des défacements de sites surtout en janvier en particulier par Isis. Par contre, il y en a eu très peu après les attentats de novembre. Durant ces moments tragiques, Google a été particulièrement sollicité. Par contre, les réseaux sociaux ont servi à des élans de solidarité surtout en novembre. En revanche, Facebook a mis parfois beaucoup de temps pour fermer des sites malveillants. Quant à tweeter il a agi un peu plus rapidement, mais a laissé courir de nombreuses rumeurs. En ces périodes, il y eu de nombreuses fausses rumeurs qui ont circulé avec même des chevaux de Troie dissimulés dans certaines images.


Amélie Paget

Vers une limitation des libertés ?

Amélie Paget, consultante juridique SI HCS by Deloitte a fait le point sur les deux nouvelles lois publié en 2015 pour renforcer les pouvoir de l'Etat : la loi sur le renseignement et l'Etat d'urgence. Pour ce qui concerne l'état d'urgence il a été prorogé jusqu'au 26 février 2016. Désormais, lors des perquisitions, les agents peuvent accéder aux données stockées sur les systèmes Informatiques ou l'équipement terminal ou accessible à partir du système initial. En outre, ils auront la possibilité de copier les donner et d'effectuer des saisies en cas d'infraction. Par ailleurs un projet de loi souhaite insérer à notre Constitution, un nouvel article consacré à l'état d'urgence.
En ce qui concerne la Loi sur le renseignement, elle donne des prérogatives pour accéder aux données de connexion en les demandant aux opérateurs, aux FAI et hébergeurs.. Les agents peuvent utiliser des outils de géolocalisation et demander en temps réel aux FAI des information et documents qui transite sur le réseau. Bien sûr toutes ces actions ne peuvent s'effectuer que pour protéger les intérêts fondamentaux de la Nation, notamment pour la prévention du terrorisme. Les agents peuvent collecter des informations en échangeant sur la toile. Quant au chiffrement les opérateurs auront 72 heures pour offrir un système de déchiffrement ou directement les documents en clair.


Gérôme Billois

Objets connectés : la sécurité doit être intégré by design

Gérôme Billois, Manager Sécurité de Solucom a traité des attaques sur les objets connectés en rappelant qu'en juillet dernier deux chercheurs ont pris le contrôle à distance d'une voiture connectée. En fait, les consoles de bords sont connectées à un premier Réseau dit de confort et un second pour la conduite comme celui qui gère le régulateur de vitesse, la boite de vitesse, le volant… En fait, la console de bord est assez facile à pirater et permet de prendre le contrôle de la console de confort. Par contre, la console de sécurité est plus difficile à pirater. Par contre, avec du temps et un peu de chance selon les dires de ces deux chercheurs, la prise de contrôle sur la console de sécurité est faisable. Cette démonstration a eu des impacts médiatiques mais aussi financiers pour les constructeurs avec l'envoi de clés USB aux utilisateurs pour faire des mises à jours, heureusement à ce jour, toujours pas d'attaque sur les voitures… Toutefois il est possible d'envisager la diffusion de ramsowares qui bloqueraient les voitures…
Au delà des voitures, les jouets connectés ont fait l'objet d'attaques plus ou moins amusants avec par exemple Barbie, les téléviseurs… Par contre, d'autres attaques seraient plus graves comme celle sur des pompes à insuline, des fusils, voir des avions…
En fait, en matière de sécurité des objets connectés il y a 4 dimensions à prendre compte : ceux qui les conçoivent, ceux qui les achètent, ceux qui les conseillent et tous ceux qui vont les accueillir en particulier dans les entreprises. Il faut donc réagir en intégrant la sécurité, en protégeant notre vie privée, sans oublier les spécificités de ces objets. Demain, nous allons voir arriver les objets autonomes qui vont demain faire partie de notre quotidien avec par exemple des robots qui vont être mis dans les boutiques Nespresso, à bord des bateaux de Costa Croisières… Cela pose, de nombreuses questions juridiques.


Garance Mathias

Objets connectés : les premiers procès à l'horizon 2016

Garance Mathias en préambule de son intervention explique que nous sommes tous concernés par les objets connectés car nous en avons tous. Le droit à déjà prévu le fait que l'on est responsable de nos objets. Un grand classique du droit est qu'il s'impose à tous les acteurs : le concepteur, l'utilisateur… Par exemple, le Cloud qui relie les objets connectés n'est qu'une externalisation avec toutes les contraintes liées.
Concernant les objets connectés, il faut aussi prendre en compte les analyses d'impacts d'où la nécessité pour les fabricants d'embarquer la sécurité y design. Elle a pris l'exemple de Vtech qui avait fait l'objet d'une plainte par « UFC Que Choisir » du fait de la non-prise en compte de la protection de la vie privée.


Le Colonel Éric Freyssinet

Téléphonie mobile : le protocole SS7 mis à mal…

Le Colonel Éric Freyssinet a évoqué en premier lieu la sécurité des téléphones mobiles. Fin 2014, une conférence lors du CCC a mis en lumière une vulnérabilité dans le protocole SS7 qui permettait de rediriger des communications et d'intercepter des SMS (chiffrés). En ce qui concerne les logiciels malveillants, il y a eu peu de nouveautés. Toutefois, parmi les nouveautés on trouve Pornbroid qui bloque le téléphone sous Android qui est un logiciel assez avancés capable de se relancer une fois désinstallé. Il a aussi cité Xcode qui exploite une vulnérabilité sur IOS.
… et des attaques aux effets collatéraux redoutables
Puis, le Colonel Eric Freyssinet a présenté les conséquences d'une attaque. Il a pris l'exemple de Target dont l'attaque a coûté environ 67 millions de $ avec Visa, la même somme avec MasterCard au final cette attaque devrait coûter environ 100 Millions de $ dont 90 sont pris par son assurance.
L'attaque contre OPM qui ciblait les personnels de l'état américain par la Chine a obligé la CIA a retiré des agents basés en Chine, sans compter la notification à plusieurs millions de personnes.
Hello Kity a aussi été visé par une attaque ciblée pour récupérées données Bancaires des parents.
TV 5 Monde a été une des premières véritables attaques pour détruire une entreprise. Au final l'impact sur le SI a été faible par contre les ventes de publicité se sont effondrées et son budget sécurité a été augmenté de façon conséquente. Son PDG a témoigné dans plusieurs conférences ce qui a un effet plutôt positif.
Ashley Madison est une affaire assez complexe. On a noté quelques retombées tragique comme le suicide d'un pasteur, des démissions, des chantages… De ce fait, la CNIL a demandé aux sites de rencontre français de renforcer leur sécurité.
Pour finir, il a recommandé de prévenir les risques, être capable de décréter la survenance d'un incident et être en mesure de maitriser leur impact.
François Paget a pour sa part rappelé que les forces de police rencontrent quelques succès en arrêtant des cybercriminels partout dans le monde.

Jean-Yves Latournerie

Nous passons à lutte anti-terroriste 2.0

La conclusion a été assurée par le cyber-préfet Jean-Yves Latournerie qui a félicité les intervenants et les organisateurs de ce panorama. Selon lui, il n'y a pas à ce jour d'actions en cyber-terrorisme à proprement parler. Par contre, le cyber joue un rôle très important dans la radicalisation, le recrutement et le passage à l'acte. Dans ces périodes tragiques, on apprend vite et on est en train de passer dans la lutte antiterroriste 2.0. Dans ce cadre le panorama du CLUSIF est important afin de mieux comprendre la nature de la menace de façon systémique et analytique et pouvoir ainsi anticiper les développements des actions terroristes. Il s'est félicité de voir le travail entre les forces de police et les entreprises privées se renforcer en particulier avec les principaux acteurs d l'Internet. Il note de réel progrès opérationnel entre janvier et novembre dernier. En effet, un travail méthodologique a été effectué entre ces deux périodes qui porte ces fruits aujourd'hui.
Il a conclu son intervention en rappelant que même s'il a quelques arrestations, le crime pour le moment sort le plus souvent des confrontations avec les forces de polices, toutefois, il semble que tous les acteurs d'Internet sont de plus en plus sensibiliser à ces attaques ce qui donne des espoirs pour améliorer cette situation.

Réagissez à cet article

Source : *Panorama 2015 de la Cybercriminalité du CLUSIF : Attaques sur tous les fronts ! – Global Security Mag Online*