IOT, Ransomware, ShellShock, Heartbleed au menu du Clusif en 2014

Quelle sont les tendances du **Panorama Cyber-Sécurité retraçant l'année 2014** établi par le **Clusif** ? Quelques mots-clés se distinguent dans le paysage de la sécurité IT : Internet des objets, ransomware, Sony Pictures, Shellshock, Heartbleed, et cryptographie. Plusieurs intervenants ont effectué des focus au nom de ce cercle de spécialistes de la sécurité IT.

Voici les principaux points développés lors de la session de présentation organisée hier après-midi à Paris :

Internet des objets : la sécurité défaillante

Fabien Cozic, enquêteur de droit privé spécialisé en cyber-criminalité, a mis l'accent sur le segment Internet of Things. On l'a vu avec la dernière session du CES à Las Vegas, une vague de produits connectés pour la vie quotidienne va débarquer sur le marché et qui revitaliser le marché de la domotique.

Mais la sécurité IT semble être le maillon faible. La priorité est donnée à la conception technologique des appareils connectés et à leur design. *« Il n'y a pas de prise de conscience globale des problématiques de sécurité »,* constate Fabien Cozic. *« Pas de règles, pas de normes, pas de protocoles secondaires uniformisés… »*, regrette l'expert. Pourtant, début 2014, nous avions assisté à l'émergence du premier « ThingBot » (contraction de « thing et robot ») : une campagne de spam via un botnet dédié aux objets connectés, rapporte nos confrères d'ITespresso.

Le manque de maturité sur le volet de la sécurité IT est susceptible de provoquer des atteintes à la vie privée. Ainsi, la découverte de 73 000 caméras IP (déployés en voie publique, dans les domiciles et entreprises) accessibles via le Web démontrent un manque de rigueur pour assurer la confidentialité.

Néanmoins, des initiatives communes commencent à émerger comme Thread fédérant des acteurs comme Google, Samsung ou ARM : une tentative de déterminer un protocole IP pour réseaux sans fil dans un cadre d'exploitation d'Internet des objets (initiative parallèle au consortium Open Interconnect en faveur de l'interopérabilité des appareils connectés).

D'un point de vue juridique, l'avocate Garance Mathias rappelle que cette dimension de l'Internet des objets « *n'est pas définie dans le droit* » mais qu'elle devrait être prise en compte dans le prochain règlement européen pour la protection des données personnelles (en cours de gestation).

Sony Pictures : cas atypique de ransomware

De son côté, Gérôme Billois, Senior Manager de Solucom, a développé le volet ransomware qui a pris de l'ampleur dans le courant de l'année dernière. Ne serait-ce qu'en raison du dossier Sony Pictures.

Car, à l'origine, il s'agit bien d'une tentative d'extorsion qui a pris des proportions gigantesques : vol massif de données personnelles, de correspondance privée et de secrets industriels, interruption et destruction partielle d'un système d'information d'une entreprise, menaces terroristes associées à la sortie du film The Interview et « cyber-vandalisme » selon les propos du Président des Etats-Unis Brack Obama.

Car cette affaire Sony Pictures s'est transformée en affaire d'Etat susceptible de nuire à la sécurité nationale et la responsabilité de la Corée du Nord est pointée du doigt.

Néanmoins, plusieurs hypothèses cohabitent sur les véritables instigateurs ou commanditaires de l'assaut sur Sony Pictures : pirates russes, employé malveillant, hacktivistes (implication de Lizard Squad ?). On connaîtra probablement le fin mot de l'histoire dans le courant de l'année 2015.

Le préjudice financier pour le groupe japonais victime sera important (« en centaines de millions de dollars »). *« Je n'ai jamais vu une attaque de cette dimension dans une entreprise. On aboutit à une prise d'otage numérique »,* commente Gérôme Billois.

D'autres firmes importantes ont été victimes de ransomware comme Domino's Pizza qui a aussi mal tourné avec la propagation de données personnelles associées à 600 000 clients.

Assiste-t-on à l'émergence de la rançon de masse par voie numérique ? Avec l'usage de cryptlocker du nom d'un malware qui rend inaccessible les données (par chiffrement) et qui permet à des pirates d'exiger une rançon pour récupérer le contrôle.

En juin 2014, l'opération policière Tovar a permis de démanteler le botnet Gameover Zeus, un vecteur de propagande de cryptolocker. La baisse d'intensité de ce type de malware observée juste après ce coup d'éclat n'a été que temporaire…

Failles logicielles : les palmes remises à Shellshock et Heartbleed

Hervé Schauer, expert en sécurité réseau, s'est concentré sur les failles logicielles qui ont ponctué l'année 2014. Sans surprise, les cas Shellshock (faille dans l'usage du shell Bash) et Heartbleed (vulnérabilité dans la bibliothèque de cryptographie open source OpenSSL) ont marqué son esprit.

« Cela faisait des années que l'on n'a pas connu de tels évènements. Tous les acteurs du Net sont concernés », commente Hervé Schauer. Celui-ci s'interroge sur les processus établis relatif au contrôle qualité du code associé aux logiciels libres : quels efforts fournis dans ce sens ? Quelle assurance sur la qualité ?

Il espère que la création du CII (Core Insfrastructure Initiative), regroupant des géants de l'IT pour financer les projets libres, permettra de répondre à cette problématique, tout en rendant les process de développement plus fiables.

Haro sur les DAB et les grandes enseignes

Dans un volet intitulé « Les nouveaux braqueurs », Christophe Jolivet, Directeur associé de Prosica (conseils en sécurité des systèmes d'information), a effectué un focus sur les assauts menés sur les faiblesses des distributeurs automatiques d'argent.

Car les techniques de skimming – pratique frauduleuse pour pirater et copier des cartes bancaires – se perfectionnent et l'on a observé des tentatives de prises en main de systèmes d'administration des DAB visant à récupérer ou modifier des paramètres de sécurité (comme les seuils de retrait d'argent en liquide par exemple).

En fin d'année, Christophe Jolivet a relevé une faille de sécurité dans le système Certicode, utilisé par la Banque Postale pour réaliser des transactions bancaires mobiles, qui a servi de levier pour une escroquerie. La presse évoque un préjudice estimé à 25 millions d'euros.

De son côté, Loïc Guezo, Evangéliste et directeur Europe du Sud chez Trend Micro, prend le relais pour évoquer des cas de vol massif de données : Home Depot (confirmé en septembre 2014 avec une fuite de 56 millions d'enregistrements entre avril et septembre 2014), Target (qui avait débuté fin 2013, qui a abouti au départ du PDG et qui fait désormais l'objet d'une class action depuis décembre), UPS, Michaels, Goodwill, eBay…

« Il existe des points communs : des alertes données par des tierces parties, des durées d'infraction plus longues, un outillage dédié avec POS malware et RAM scraper. »

Cryptographie : sujet sensible

Philippe Bourgeois, expert securité CERT – IST, a effectué un focus sur les failles associées à la crytographie. *« C'est le sujet numéro un d'un point de vue technique avec la découverte de bugs SLL/TLS. »* Des failles majeures ont été repérées à partir d'un seul composant : GotoFail, CVE 2014 0062 (Linux/Gnu TLS), Heartbleed, Linux Open SSL, Schannel (Microsoft) et Poodle (SSLv3).

« Le niveau d'expertise augmente sur ces sujets (…) La cryptographie est-elle cassée ? Je dirais plutôt qu'elle gagne en maturité », estime Philippe Bourgeois.

Parallèlement, il observe l'apparition d'au moins 15 Avanced Persistent Threats (APT, traduction littérale en français : « menace persistante avancée »), dont Snowglobe et Babar pour la France en mars 2014.

Gendarmerie : essor des click Web kiddies

Au nom de la gendarmerie nationale, le colonel Eric Freyssinet a abordé quelques tendances associées à la cybercriminalité.

Comment mesurer son impact financier en France ? La question reste ouverte. « *Chaque mois, cela représente une perte de 4 millions d'euros pour les entreprises, en prenant en compte les statistiques de la gendarmerie. Sur un an, cela équivaut à un préjudice global de 50 millions d'euros.* » Tout en reconnaissant

que cette vue est partielle mais c'est un indicateur.

Le marché underground est « florissant » avec plateformes de services criminels servant au piratage, à des attaques DDoS ou à pratiquer le doxing (comment exploiter Internet pour pister, traquer ou espionner quelqu'un).

Les tarifs des pratiques cyber-criminelles sont affichés : comptez entre 3 à 5 dollars par heure pour une attaque DDoS. *« Les script kiddies sont plutôt des click Web kiddies qui utilisent ces plateformes »*, constate l'expert en cyber-criminalité rattaché à la gendarmerie.

A partir d'un échantillon portant sur les volumes d'atteintes aux systèmes de traitement automatisé de données (328 cas recensés dans la période août – septembre 2014), il égrène les principaux délits : escroqueries via usurpation d'identité ou via un compte client, atteinte à la vie privée, détournements de compte…

Sur le seul mois d'août, 1750 cas d'infractions économiques et financières sont remontés à la gendarmerie : escroquerie aux petites annonces, usages frauduleux de cartes bancaires, fraudes sur commerce électronique…

Mention spéciale pour l'escroquerie aux faux placements. « *Une faible proportion mais de grosses transactions* » selon le colonel Eric Freyssinet, qui signale le cas d'un particulier ayant placé un montant de 2,2 millions d'euros à un pseudo-intermédiaire financier inconnu via Internet…

Ne pas oublier Scada et les hacktivistes

Pour conclure, François Paget, expert en sécurité IT chez Intel Security – McAfee Labs en charge de la coordination du Panorama Cybercriminalité au nom du CLUSIF, évoque les autres phénomènes qui n'ont pas attiré l'attention cette année mais qui mérite d'être suivi en 2015.

C'est le cas des attaques sur les systèmes industriels SCADA. En Allemagne, un groupe industriel, spécialiste de la production d'acier, a été victime d'un assaut dans ce sens à partir de plateformes SCADA émanant de Siemens.

Autre sujet sous-jacent de l'actualité de la sécurité informatique : le hacktivisme. Moins voyant en 2014, le phénomène s'est amplifié en ce début d'année avec les Anonymous qui partent en guerre contre les réseaux djihad et l'assaut sur un millier de sites Web en France.

« AnonGhost flirte avec des idées terroristes », considère François Paget. Alors qu'une nouvelle vague d'assauts informatiques frappant le Web français est attendue aujourd'hui…

A lire aussi :

Le Top 10 de l'IT de l'année 2014
David Grout, McAfee : « sur la sécurité, les entreprises sont ambivalentes »