La cybercriminalité décryptée : objets détournés, élections perturbées et Blockchain dépouillée

Hier, le Clusif (Club de la sécurité de l'information français) dévoilait son 15ème panorama de la cybercriminalité, une analyse des principaux événements de 2016 en matière de cybersécurité. Une année qui aura vu le sujet faire les gros titres, avec une recrudescence des attaques spectaculaires. Pour le colonel Emmanuel Germain, directeur général adjoint de l'Anssi (ci-contre), le second semestre 2016 marque d'ailleurs une accélération des attaques aboutissant à une alerte de l'Agence nationale de la sécurité des systèmes d'information : « *depuis cet été, nous constatons un doublement des incidents qui nous parviennent. Nous sommes passés de 2 à 4 incidents avérés par semaine en moyenne. Et cette tendance va se poursuivre avec le développement du cyberespace, porté par l'IoT* ».

Des objets connectés qui ont montré leur capacité de nuisance en 2016, avec ces botnets constitués à partir d'objets insuffisamment sécurisés pour lancer des attaques par déni de service (DDoS) très puissantes. « *On atteint des volumes d'attaques qui avaient été théorisés, mais jamais démontrés jusqu'alors* », explique Fabien Cozic, de la société Arca Conseil. En tête de gondole, les attaques contre le blog de Brian Krebs (655 Gbit/s enregistrés), OVH (1,1 Tbit/s) et surtout le prestataire DNS américain Dyn (1,2 Tbit/s), une attaque qui a plongé tout un pan d'Internet dans le noir pendant plusieurs heures. « *En réalité, on pense que cette dernière a pu atteindre 1,5 à 1,6 Tbit/s* », précise Fabien Cozic, qui rappelle également le DDoS visant le Libéria, un pays qui présente la particularité d'être desservi en connexion via un unique câble sous-marin. Une infrastructure critique que les pirates ont évidemment prise pour cible.

Tesla et les faux points d'accès Wifi

Et les dangers des objets connectés ne se limitent pas à ces détournements d'usage, en vue de créer de vastes réseaux de machines zombies. Hervé Schauer, le fondateur du cabinet HSC, rappelle les multiples failles présentes sur des automobiles de plus en plus bourrées d'électronique. A commencer par les systèmes d'ouverture des portes à distance insuffisamment robustes, une vulnérabilité qui a entraîné une multiplication des vols par « mouse jacking » (autrement dit, à la souris). Mais les failles les plus graves touchent à la sécurité même des véhicules connectés. « *Sur Shodan (un moteur de recherche d'objets connectés, NDLR), on trouve des centaines de véhicules connectés sans authentification*, explique Hervé Schauer. *Qui plus est, dans bien des cas, l'absence de contrôle d'intégrité des mises à jour logicielles arrivant via la connexion de la voiture permet d'envisager des prises de contrôle à distance.* » Celle dont a été victime la Jeep Cherokee a évidemment

fait le tour du Web. Mais le cas n'est pas isolé, assure l'expert qui signale notamment l'attaque contre les Tesla, via de faux points d'accès WiFi fournissant une mise à jour logicielle permettant de prendre le contrôle des voitures californiennes.

L'autre grand événement de l'année 2016, c'est évidemment la pollution de la campagne électorale américaine par des piratages et des révélations d'informations confidentielles qui ont embarrassé le camp démocrate. Des événements qui se sont étalés entre juin 2016 (la révélation du piratage du DNC, le comité national démocrate) et les premiers jours de janvier 2017 (des développements futurs n'étant d'ailleurs pas à exclure). « *On peut parler de cyber guerre froide, toutes les grandes annonces de l'administration américaine pointant la Russie* », dit Loïc Guézo, expert en cybersécurité de Trend Micro pour l'Europe du Sud. Et ce dernier de relever quelques éléments intéressants. Comme le fait que l'enquête ait été conduite non pas par le FBI (qui est intervenu dans un second temps), mais par une société privée (Crowdstrike). Ou comme le fait que « *les premiers signes avant-coureur de l'attaque au sein du DNC n'ont pas été pris en compte. Toute la gestion opérationnelle a été laissée sur les épaules d'un technicien, qui a commis une erreur aboutissant à la compromission des e-mails de John Podesta (le directeur de la campagne d'Hillary Clinton, NDLR)* », reprend Loïc Guézo.

Blockchain : l'attaque 51 %

Moins médiatisés, mais tout aussi spectaculaires, les piratages de la Blockchain – le buzzword incontournable de 2016 – ont également émaillé l'année qui vient de s'écouler. Car si la technologie de stockage et de traitement de données décentralisée et fonctionnant sans autorité de contrôle est, par principe, « *incorruptible du fait des mécanismes de chiffrement auxquels elle fait appel* », elle a dévoilé trois grandes faiblesses au cours de l'année, résume Gérôme Billois, senior manager en gestion des risques et sécurité chez Wavestone. La première d'entre elles réside dans les éléments périphériques à la technologie elle-même ; « *les PC des utilisateurs, les services Web présentent des vulnérabilités qui peuvent être exploitées pour, par exemple, dérober des clefs.* » C'est par exemple une faiblesse de ce type qui a été mise à profit dans la mésaventure qu'a connue la plate-forme d'échange Bitfinex. L'attaque sur une API a permis à des cybercriminels de dérober quelque 70 M$ en 3 heures.

Deuxième faiblesse mise en lumière : l'attaque dite 51 %. « *L'objectif des assaillants est de prendre le contrôle de plus de 50 % du réseau* », résume Gérôme Billois, qui signale qu'un groupe de pirates (51crew) s'est même spécialisé dans cette technique. Leur attaque contre la Blockchain Krypton, au cours de laquelle les assaillants sont parvenus à créer une chaîne de blocs alternative et à remplacer la plateforme légitime après avoir lancé des DDoS contre les membres de ce réseau, a ainsi montré la faisabilité de ce type de manipulation. « *Des attaques qui restaient théoriques deviennent réelles. La seule limite de ce type d'attaques ? Elles nécessitent une grosse puissance de calcul. A ce titre, les réseaux bien établis comme le Bitcoin paraissent encore à l'abri* », commente Gérôme Billois. D'ailleurs, en septembre dernier, Krypton étudiait le passage de la Blockchain Ethereum, technologie qu'il avait choisie au départ, à la plate-forme Bitcoin.

« *Code is law* »… sauf exception

Mais l'événement majeur de 2016 touchant à la Blockchain reste la découverte d'un bug dans la plateforme Ethereum. Un bug dont le fonds d'investissement participatif The DAO a fait les frais, en juin dernier. Via l'exploitation d'un appel récursif, rendu possible par un code de mauvaise qualité, des pirates ont réussi à détourner plusieurs dizaines de millions de ce fonds qui avait réussi à en réunir 150 en quelques semaines. Un épisode qui a poussé la communauté The DAO de créer un « hard fork » le 20 juillet, permettant aux participants lésés de récupérer leurs investissements. Une manœuvre qui a suscité bien des débats dans une communauté qui faisait jusqu'alors sienne la devise du juriste Lawrence Lessig, « *code is law* » (le code est la loi). Un principe qui interdit, normalement, toute modification a posteriori des règles du jeu inscrites dans le code.

A lire aussi :

Spora : le ransomware qui chiffre hors connexion et qui se pique de marketing

Hacking de Moscou contre les Etats-Unis ? Les experts ne sont pas convaincus

Après les ransomwares, la prochaine menace est le ransomworm

Crédit Photo : Eugène Sergueev-Shutterstock