De Sasser à WannaCry, ces menaces qui ont marqué les RSSI

WannaCry ? Pour Loïs Samain, RSSI membre du CESIN, ce ne fut « pas une crise d'entreprise, mais une crise de communauté » qui a engendré « une véritable évolution des dirigeants sur la vision du risque cyber ».

Xavier Leschaeve, d'une quinzaine d'années son aîné, y voit « un énorme rappel » quant à l'existence des vers informatiques, qu'on « avait un peu oubliés ».

Quinze ans, c'est justement le temps qui s'est écoulé depuis que l'intéressé, aujourd'hui RSSI chez Rémy Cointreau, s'est retrouvé confronté à l'un de ces vers : Sasser. Il était alors directeur de la sécurité et du réseau pour la filiale réassurance d'AXA.

« *Ç'a été la première et l'unique vraie crise cyber que j'aie connue*, affirme-t-il. *Il y a eu une vraie prise de conscience quand ces petites bestioles ont commencé à se propager de manière autonome* ».

Sasser était l'une de ces « petites bestioles ». Œuvre d'un jeune Allemand, il exploitait une faille de sécurité dans Windows, au niveau du composant LSASS assurant l'authentification des utilisateurs. Les premières infections sont datées du 30 avril 2004.

Microsoft : incontournable épine

« *Il n'y avait pas de RSSI* [à l'époque], explique Xavier Leschaeve. *Comme je venais du réseau, je m'occupais des* firewalls *et on m'avait donné la casquette 'sécurité'* ».

Il poursuit : « *C'est l'un des événements qui ont fait que la sécurité a vraiment commencé à m'intéresser.* [...] *C'était la première fois que je voyais toute l'informatique d'une entreprise s'arrêter* ». En l'occurrence, un parc de 800 machines perdues en l'espace de 30 secondes.

« *Je me souviens, on était sur le plateau et quelqu'un a dit :* 'Tiens, c'est marrant, mon PC *reboote*.' *Et le gars d'à côté a répondu :* 'Le mien aussi.' *On se retourne et on voit tous les PC qui* rebootent *les uns après les autres* ». Des PC, mais aussi « quasiment tous les serveurs ».

« *C'est à partir de ce moment-là qu'on s'est dit :* 'Quand Microsoft sort un patch, il faut le passer tout de suite' ». L'éditeur avait bien livré un correctif, le 13 avril 2004. La même chose s'est produite avec WannaCry, qui a pu se propager à défaut d'application du patch corrigeant la faille SMB.

« *On a dû graver des dizaines de cédéroms à la chaîne*, reprend le RSSI de Rémy Cointreau. *Il n'y avait pas de clés USB. On a réquisitionné les trois quarts du service informatique (on était une cinquantaine à l'époque) et on a passé pratiquement 24 heures* [...] *à aller de machine en machine* ».

Le choc WannaCry et NotPetya

Le virus n'était pas destructif. La fulgurance de sa propagation sur le port 445 a néanmoins surpris. « *On a commencé à se dire qu'il fallait ségréguer les réseaux, filtrer les protocoles et les partages de répertoires laissés ouverts…* ».

Quant aux coûts induits, Xavier Leschaeve a bien du mal à les estimer, « ne serait-ce que [de par] les cellules de crise déclenchées à gauche, à droite [et] les gens qui ont travaillé le week-end ».

Après l'épisode Sasser, « *on n'a plus reparlé des vers pendant un moment* », affirme-t-il. Jusqu'à ce que WannaCry et NotPetya arrivent. « *Je me souviens d'une réunion il y a deux, trois ans. On disait :* 'Il faut un peu arrêter le côté *firewalls*, ségrégation des réseaux… Des vers, il n'y en a plus.' *L'histoire nous a donné tort* ».

WannaCry n'a pas touché Rémy Cointreau directement, mais « par ricochet », notamment au niveau de fournisseurs de bouteilles en verre. Une issue plus heureuse que pour Saint-Gobain, dont l'ancien patron enchaîne aujourd'hui les conférences pour mettre ses confrères au parfum.

Lorsqu'il s'adresse au top management sur ce sujet, Xavier Leschaeve « montre toujours quelques gros titres de journaux » qui « [remettent] les choses dans le contexte » et permettent de mesurer les conséquences de telles attaques. Il refuse toutefois se montrer trop anxiogène, faisant « écho avant l'heure » au message que l'ANSSI a fait passer lors des Assises de la sécurité.

Les malware attaquent l'industrie

Loïs Samain partage cette approche de « sensibilisation positive ». « *Mon boulot, c'est 60 à 70 % de communication*, explique-t-il. *Le plus important, c'est qu'on ait des éléments à apporter aux métiers* […] *et qu'eux aussi se rendent compte des choses* ».

Reflet de ses fonctions actuelles, le RSSI se montre plus marqué par des attaques qui ont touché des SI industriels. À commencer par Stuxnet.

Le virus, découvert en 2010 et attribué au tandem USA – Israël, a frappé des centrales iraniennes d'enrichissement d'uranium. « *C'était la première démonstration au grand public d'une attaque sur le système industriel*, déclare Loïs Samain. *Ces systèmes, c'est un peu comme 'L'IoT d'avant' : ils sont partout autour de nous, mais on ne se rendait pas vraiment compte de la criticité* [qu'ils] *pouvaient avoir* ».

Autre opération à l'avoir marqué : celle qui a mis à mal, fin 2015, le réseau électrique en Ukraine. Fondée sur le *malware* BlackEnergy, elle s'est assortie d'un déni de service téléphonique [TDoS, ndlr] destiné à empêcher les clients d'appeler leurs fournisseurs.

Prise de conscience… et de recul

« *À la base, le* malware *se trouvait sur un SI de gestion* [avec un e-mail comme vecteur de diffusion, ndlr]*, mais il a réussi à rebondir jusqu'au SI industriel* », précise Loïs Samain.

Et de poursuivre sur le cas Triton. On considère qu'il s'agit du premier *malware* à avoir été activé pour cibler spécifiquement un système de contrôle industriel (il existait une variante de Stuxnet, restée en sommeil).
Ces systèmes de sécurité sont censés prévenir les dommages matériels et humains. Triton a permis d'en prendre le contrôle. En tout cas, dans au moins un cas avéré qu'on pressent être l'entreprise pétrochimique saoudienne Aramco. L'attaque n'est pas allée à son terme, mais le niveau d'intrusion était tel qu'un arrêt de la production pouvait être envisagé.

« *On se rend compte que même ces petits verrous peuvent être attaqués*, résume Loïs Samain. *C'est très lié à l'évolution de nos SI* […]*, de plus en plus interconnectés* ».

Plus que d'interconnexion, le « botnet IoT » Mirai tire parti de l'hyperconnexion. Il a permis d'exploiter des objets connectés par milliers pour engendrer des dénis de services qui ont notamment touché OVH.

Pour des raisons de coût ou de consommation de batterie, ces objets connectés « sont malheureusement peu protégés par certains fabricants », déplore Loïs Samain. On les contrôle d'autant moins qu'ils sont vendus en marque blanche. Et on se retrouve avec des « munitions […] au chaud […] qui n'attendent plus que l'activation ».

Avec WannaCry, la prise de conscience est allée au-delà des RSSI. « [Les collaborateurs] *voient que Saint-Gobain est arrêté, que Renault est arrêté, etc., se posent des questions, viennent nous voir* ». L'attaque contre TV5Monde survenue quelques mois en amont a pesé dans la balance, estime Loïs Samain.

Pour les RSSI, WannaCry fut aussi le déclencheur d'une prise de… recul vis-à-vis du discours des éditeurs de solutions de sécurité, glisse-t-il.