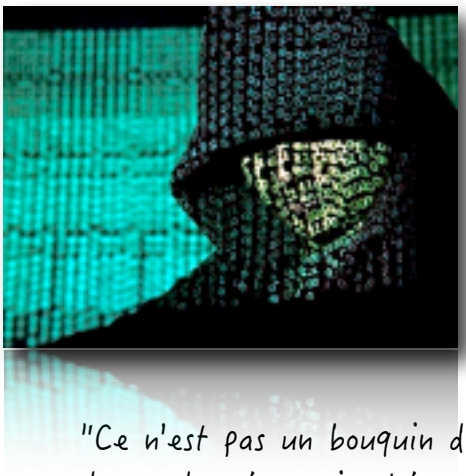
Challenges
High-Tech
Par Vincent Lamigeon
le 17.04.2018

Les "agents dormants cybers", nouvelle menace pour la France

L'Agence nationale de la sécurité des systèmes d'information (Anssi) traque des pirates informatiques de très haut niveau, qui pénètrent et cartographient les réseaux français sans y faire de dégât. L'activation de ces "agents dormants" pourrait avoir des conséquences catastrophiques, prévient l'Anssi.



Kacper Pempel

Dans la salle de conférences de l'hôtel des Invalides, Guillaume Poupard dégaine un livre de poche. "Tension extrême", par Sylvain Fore, une histoire de cyber-attaques qui transforme les objets connectés en armes mortelles.

> "Je n'avais pas lu de polar depuis vingt ans, mais là, sincèrement, ça vaut le coup", insiste le patron de l'Agence nationale de la sécurité des systèmes d'information (Anssi). "Ce n'est pas un bouquin d'anticipation ou de science-fiction. C'est ce qui va nous tomber dessus dans les mois et les années à venir !"

Et de citer le cas, réel celui-ci, d'un casino dont les bases de données ont été piratées... par le biais du thermomètre connecté dans un aquarium.

Discours anxiogène ? Guillaume Poupard le reconnaît volontiers. Il n'en est pas moins nécessaire vu l'augmentation de la menace, assure le patron de l'agence de cybersécurité française.

> "2017 a vu se concrétiser des attaques graves en termes de renseignement, de vol d'informations, avec des attaquants toujours plus forts, toujours plus agiles, et qui ont manifestement des moyens considérables", résume le patron de l'Anssi. "C'est ce que me disent les industriels : le jour où ils découvrent, sur tel ou tel salon, leur prototype présenté par leur concurrent, ils ont un éclair de lucidité. On est dans un domaine où, contrairement à ce qu'on dit souvent, la meilleure défense, c'est la défense."

Infiltration de cyber-attaquants

L'agence de cybersécurité, dont Guillaume Poupard présentait le rapport d'activité 2017, n'a donc pas chômé l'année dernière. Il y a eu le rançongiciel Wannacry, attribué par certains spécialistes au groupe nord-coréen Lazarus Group. Il y a eu le virus NotPetya, qui a touché de nombreuses sociétés

dont Saint-Gobain, qui a chiffré l'impact sur ses comptes à 250 millions d'euros. Il y a aussi eu, grande nouveauté, les tentatives d'influencer l'élection présidentielle française.

> "Un avertissement sans frais", prévient Guillaume Poupard.

La seule solution ? Augmenter le niveau de protection des systèmes, et détecter les attaques au plus tôt, grâce à des sondes

> "capables de les identifier, indique le patron de l'Anssi. "On cherche à exploiter des marqueurs techniques, qui sont des traces d'attaques", explique cet ingénieur de l'armement, spécialiste de la cryptographie.

Le patron de l'Anssi met aussi en garde contre une tendance inquiétante des attaques informatiques récentes.

> "Ce qui nous préoccupe le plus, ce sont ces attaques sur lesquelles on n'a pas les motifs. Ce sont des attaquants de haut niveau, qui prennent pied sur des réseaux sensibles, voire très sensibles, liés à des secteurs d'importance vitale. Ils cartographient ces réseaux, cherchent à comprendre comment ça marche, développent leurs outils. Mais objectivement, je ne sais pas vous dire ce qu'ils préparent."

Ces véritables "agents dormants" cyber, pas si éloignés des agents dormants soviétiques durant la Guerre froide, sont-ils le signe avant-coureur d'opérations de renseignement ou de sabotage ? Mystère.

> "On est probablement face à des acteurs qui préparent des conflits futurs, déclarés ou non déclarés", indique Guillaume Poupard. "C'est extrêmement inquiétant."

Le 4 avril devant l'Association des journalistes de défense, cet ancien de la DGA était encore plus clair :

> "Ils préparent une sorte de boîte à outils, un panel d'options qui pourraient être présentées à leurs autorités. La logique, c'est : "Je place des charges explosives sous le pont de l'Alma au cas où un jour on me demande de faire sauter le pont de l'Alma"".

Les experts de l'Anssi ont déjà trouvé "des preuves" de telles intrusions et "ont tout désamorcé", assurait Guillaume Poupard, cité par l'AFP,

> "même si l'honnêteté me force à admettre que nous ne sommes pas sûrs d'avoir éliminé toutes les métastases".

"Brouillard cyber"

Qui sont ces acteurs ? Sur ce sujet sensible, Guillaume Poupard préfère botter en touche.

> "On n'est pas là pour travailler sur l'attribution, qui est extrêmement complexe et ne peut pas se faire uniquement par les moyens techniques cyber. On travaille sur les modes

opératoires, mais il y a toujours une part de doute, ce qui fait que l'attribution va rester un sujet éminemment politique".

C'est l'art délicat de la cyber-guerre mondiale :

"Il y a donc toujours le risque de se faire manipuler, que certains cherchent à créer ou envenimer des conflits en se faisant passer pour l'un ou pour l'autre, dans cette espèce de brouillard cyber qui est extrêmement difficile à démêler."

Certes, pour réagir, les équipes d'intervention de l'Anssi sont au meilleur niveau, assure Guillaume Poupard.

"Ces pompiers numériques sont reconnus et efficaces. Mais ils ne sont capables de traiter qu'un nombre limité de victimes."

Le patron de l'agence de cybersécurité craint donc le

"scénario catastrophe d'un choc massif, avec beaucoup de victimes en même temps, sur lesquels la priorisation serait difficile".

"Sondes" chez les hébergeurs

L'article 19 de la loi de programmation militaire 2019-2025, en cours d'examen au Parlement, apporte heureusement des armes nouvelles, estime Guillaume Poupard. D'abord,

"autoriser les opérateurs de communication électronique à détecter les attaques, ce qui est aujourd'hui interdit".

Ensuite, autoriser l'Anssi à installer des "sondes de circonstance" chez les hébergeurs, voire les opérateurs, en cas de soupçons de cyber-attaques.

"Aujourd'hui, au moment où je vous parle, on a toute une liste d'adresses IP de serveurs hébergés en France, où on a la quasi-certitude que se logent des attaquants de très haut niveau, parmi les plus hostiles aux intérêts français. Et on n'a pas les moyens réglementaires d'aller voir."

La LPM remédiera à ce manque. Avec un garde-fou substantiel, rappelle assure Guillaume Poupard: les opérations seront soumises au contrôle contrôle de l'Arcep, le gendarme des télécoms.