"atlantico
UN VENT NOUVEAU SUR L'INFO

XAVIER RAUFER - février 2020-3

CYBER-CRIME, *ransomware* : une prolifération hors-contrôle

Toujours plus, des entreprises sont touchées par une nouvelle cybercriminalité, le *ransomware* (logiciels-pirates d'extorsions de rançons). Récents exemples : la méga-entreprise *ISS World* (500 000 salariés dans le monde...) voit les profils de milliers de ses employés "disparaître" ; aux États-Unis, des pipelines entiers de gaz - au cœur du dispositif énergétique de l'Amérique du Nord - doivent fermer, suite à des piratages-rançons.

1. Pouvez-vous expliquer l'ampleur de cette criminalité ? Est-elle en pleine expansion ?

La propagation planétaire du cyber-crime est hors-contrôle. Rien dans le monde numérique n'est à l'abri du piratage. Une exagération ? Hier, le réseau le plus sécurisé au monde, la *Defence Information Systems Agency* (DISA) qui assure les transmissions des militaires américains sur le champ de bataille - et des échanges par téléphone du président Trump - a été piraté et les dossiers personnels de 200 000 de ses usagers - militaires, renseignement hauts fonctionnaires, etc., les plus sensibles du système américain de sécurité - "balancés" sur le web. Si ce réseau est piraté, rien n'est sûr.

Pire encore : A la rentrée 2018, des pirates cyber-mercenaires, requis par le *Government Accountability Office* (Cour des Comptes des États-Unis), reçoivent la mission d'infiltrer les systèmes d'armes *high-tech* et informatisés du Pentagone : missiles nouvelle génération, lanceurs de vecteurs nucléaires, etc. (coût total, 1 600 milliards de dollars...) en un test de vulnérabilité digitale. Nombre de ces systèmes sont mis hors-service ; certains sont contrôlés en temps réel : les pirates y voient travailler les opérateurs militaires. 86 de ces systèmes ultrasecrets sont si mal protégés (mots de passe enfantins) que les pirates maquillent leurs page d'accueil en écran de *flipper*, exigeant 50 cents pour y lancer une nouvelle partie...

Conclusion : si les coups de fil du président des États-Unis et les lanceurs de ses bombes atomiques sont ouverts aux *hackers*, jugez de la sécurité du reste...

2. Que font les autorités face à ce nouveau fléau d'ampleur mondiale ? Est-il possible de traquer ces hackers ?

Fléau d'ampleur mondial, à coup sûr : pour 2020-2025, l'ONU estime que l'insécurité de l'ensemble Internet/data, causera un préjudice mondial de ± 5 200 milliards de dollars. Et pour le rapport 2019 (McAfee+Centre for International Strategic Studies) le cyber-crime a

coûté en 2018 600 milliards de dollars à l'économie globale, 0,8% du produit brut mondial.

Or face à ce péril planétaire, les États et instances internationales (Union Européenne, ONU) lambinent : bavardages... conférences creuses... promesses en l'air. À présent en Europe, la seule Grande-Bretagne a révélé l'état réel de la répression du cyber-crime. Tenez-vous bien : moins de 1% des cybercriminels repérés ont été *inculpés*. Oublions les *condamnés*, au nombre plus infime encore. Pas mieux, voire pire ailleurs en Europe. Décodeur : tout cybercriminel a 99% de chances d'impunité. On risque bien plus en traversant la rue...

L'internet est d'autant plus friable que ses acteurs majeurs les GAFAM (Google, Apple, Facebook, Amazon, Microsoft) sont de culture libertaire et trouvent ces histoires de pirates plutôt rigolotes. Du haut de leurs capitalisations frisant les 1000 milliards de dollars, leurs dirigeants et propriétaires sont aussi bien sûr dans l'impunité totale.

3. Qu'en est-il en France ?

En 2019, le seul *Phishing* (croyant répondre à un mail de sa banque, des Telecom, etc., la victime donne ses données privées à des pirates) a fait quelque deux millions de victimes. Et le piratage contre rançon affecte chaque jour des hôpitaux, municipalités et entreprises de toutes tailles. Exemple : en novembre 2019, la communauté de communes de Nuits-Saint-Georges (Côte d'Or, célèbre pour ses grands crus de Bourgognes) subit une grave cyber-attaque : informatique détruite, écrans noirs.

Zone gendarmerie (France rurale-périurbaine) fin 2018, 67 890 infractions numériques y sont recueillies, + 7% sur 2017. De 2016 à 2017, c'était déjà + 32%. Escroqueries liées à Internet, fraudes à la carte bancaire, cyber-rançons, visant particuliers et entreprises : tout cela figure dans l'intéressant rapport annuel du Service central de renseignement criminel de la gendarmerie.

Côté Police nationale en revanche, rien de tel. Au su de l'auteur, on n'y publie nul rapport annuel avec comptes précis, classement du cyber-crime en type d'infractions, etc. Récemment on lit que "l'intelligence artificielle entretient l'espoir de meilleurs résultats au ministère de l'Intérieur et à la chancellerie".

Bien irénique, tout ça.
Décodeur : à présent, rien de systématique n'y est fait.
Faut-il compter sur les plutôt confus Castaner et Belloubet pour doper leurs ministères en matière de cyber-crime ? Ne rêvons pas. ■