"atlantico
UN VENT NOUVEAU SUR L'INFO

XAVIER RAUFER - avril 2020-3

MARSEILLE : quand un virus *(biologique)* en cache un autre *(numérique)*

Depuis la nuit des temps, les catastrophes, désastres et calamités frappant l'humanité ; naturels (séismes, tsunamis) ; humains (guerres) ; affectaient forcément le monde physique, pour la parfaite raison que c'était le seul. Or depuis vingt ans désormais - les criminologues, étudiant les deux univers, le savent trop bien - les pannes géantes, le crime, l'espionnage, le sabotage, etc., touchent toujours plus le cybermonde. Ils ont en commun les ravages de terribles virus : COVID-19 (registre biologique) et virus-pirates (numérique).

Exemple : la grave et méconnue cyber-attaque ayant dévasté, la nuit du vendredi 13 (!) mars, les serveurs de Marseille (ville, communauté urbaine et alentours). Attaque dont les effets locaux sont toujours sévères, quarante jours plus tard.

On comprend que cette ravageuse attaque soit restée inaperçue : assommés, les Français et leurs dirigeants, bientôt confinés, voient leur monde ambiant - le philosophe Martin Heidegger dit "ce qui va de soi pour les masses" ; et du directoire du néo-monde, "le cercle bien arrêté des dispositifs qui organisent la situation de puissance de l'homme" - s'évanouir sous leurs yeux - sans savoir du tout jusqu'à quand. Mais la gravité de l'attaque vaut qu'on s'arrête à Marseille.

La ville d'abord : 2e métropole de France, l'une des vingt premières de l'Union européenne, 12 000 fonctionnaires ; 200 pour son seul service informatique, qui est énorme : 1 300 serveurs, 6 000 ordinateurs, 450 applications-métiers, etc. Frappée tout autant, la métropole Aix-Marseille, 8 000 agents, en charge des cruciales directions de la voirie, des tunnels, des ordures ménagères, de l'eau, etc.

Or dans la nuit du 13 mars, une attaque "massive et minutieusement préparée" de pirates encrypte 90% du dispositif - dès lors perdu pour ses utilisateurs. Seul, un ingénieur arrachant au réflexe une prise de courant du mur, empêche l'écran noir total et définitif. L'essentiel des serveurs paralysés : la vie sociale par voie informatique est soudain bloquée dans la métropole de 1,8 million d'habitants.

Quand débute une crise sanitaire inouïe, 48 heures avant le confinement, sont ainsi inaccessibles :

- l'état-civil, plus d'enregistrement des naissances et décès (la crise du COVID-19 débute !)
- les services d'appel du public,
- le planning et service des payes de tous les fonctionnaires,

- les listes électorales (la nuit du vote du 1e tour des municipales),
- la liste des enfants inscrits en crèche ou à l'école primaire à la prochaine rentrée,
- les factures à payer par la mairie à ses prestataires,
- les fichiers des permis de construire en cours et des immeubles en péril (à Marseille !),
- les concessions disponibles dans les cimetières.
- la police municipale n'archive plus les mains-courantes ou procès-verbaux (confinement !).

Le 18 avril, la mairie avoue "on est loin d'en être sortis" : il faut "purger" et relancer à la main, un par un, les 1 300 serveurs. Un mois pour rétablir l'application du seul état-civil ; deux mois minimum pour reconstruite un système opérationnel.

Pour Marseille, l'attaque est un d'autant pire désastre que - erreur confondante - les sauvegardes des fichiers cryptés, elles aussi largement perdues, étaient conservées... sur le même réseau que les serveurs eux-mêmes.

Que s'est-il passé ? "Mespinoza-Pysa" virus-pirate servant à rançonner des villes et entreprises, est connu depuis octobre 2018. Dès juillet 2019, l'entreprise de transferts de fonds *Moneygram* reste longtemps paralysée, suite à une sauvage attaque de Mespinoza-Pysa. Dès le 16 décembre 2019, le site spécialisé *Malware-Warrior* avertit ainsi : "Pysa-Ransomware (logiciel-rançonneur) pénètre dans le PC, inaperçu de l'utilisateur, puis encrypte ses fichiers avec un algorithme complexe qui les rend totalement inutilisables. Pysa-Ransomware crypte précisément les fichiers les plus importants pour l'usager : photos, audio, archives et documents de bureau, etc.". Conclusion claire : " Supprimez immédiatement Pysa-Ransomware".

Avant l'attaque sur Marseille et malgré ses efforts, l'auteur n'a pas trouvé trace d'une alerte à de possibles victimes, dont les grandes villes. Le 18 mars - cinq jours après le piratage, l'Agence nationale en charge, l'ANSSI, réagit (CERT FR-2020-CTI 002) ; elle a "récemment été informée d'attaques informatiques visant notamment des collectivités territoriales françaises... Des analyses sont en cours". Pour l'ANSSI toujours, qui "se veut rassurante", "ce phénomène n'est pas nouveau". Suit un simple rappel des mesures de sécurité - sans nulle précision sur d'analogues attaques perpétrées en 2020.

Côté officiel, 40 jours après le ciblage de Marseille, rien de pertinent n'est paru sur qui fut son initiateur, ni comment - et surtout, pourquoi, l'attaque. Même flou du côté des sites experts en cyber-malveillance : tous ont attendu le 19 mars pour publier le communiqué de l'ANSSI, sans autres précisions.

Sans cruauté exagérée, rappelons enfin que l'avertissement rétrospectif est un ressort majeur du cinéma comique : "Attention cher ami, le plafond est bas"... Pour la victime déjà au sol, à demi-assommée, l'annonce est-elle bien utile ?

*** Toutes précisions et sources disponibles sur demande. ■