"atlantico
UN VENT NOUVEAU SUR L'INFO

Xavier Raufer - mai 2021 - 3

Cyber Pearl-Harbor aux États-Unis : et de deux

Colonial pipeline : pour la distribution de carburants, la veine jugulaire de la côte Est des États-Unis ; la mère des infrastructures critiques du pays. Du golfe du Mexique, au port texan de Houston à celui de New York, ce réseau de pipe-lines de près de 9 000 km. (avec ses embranchements) est le dispositif de distribution d'énergie majeur de l'hémisphère occidental. Essence, diesel, kérosène : 45% de ce que l'Est du pays utilise passe par ses tuyaux. Sans arrêt depuis 60 ans, il transporte *par jour* 460 millions de litres de carburants divers. Et l'aire immense qu'il couvre ne compte nulle alternative pour le transport de carburants.

Or au fil des années, l'industrie des pipe-lines est devenue hyper-connectée - et plus s'accroît la connectivité, plus le piratage est aisé. Cela, les hackers de *DARKSIDE* l'ont bien vu. Qu'est-ce que ce cyber-gang ? Washington n'a pas idée. Le président Biden a "des raisons de penser" que "les pirates opèrent depuis la Russie". Le FBI est moins sûr : "Russie ou Europe orientale" dit un de ses experts. Encore et toujours, l'intraitable problème de l'attribution de toute attaque numérique.

Où qu'ils soit, *Darkside* a d'abord explosé les défenses de *Colonial Pipeline*, puis capturé et encrypté 100 gigabytes de ses données ; enfin, exigé une rançon. Question cruciale : ces pirates ont-ils "kidnappé" les données administratives de Colonial Pipeline (e-mails... fichier de personnels... facturation...) ou - bien pire - ses serveurs industriels (assurant la marche du réseau, sa surveillance, etc.) ? L'entreprise réalise lors du drame qu'elle "ne comprend pas bien" la logique de sa propre informatique et réagit selon le dicton texan "Boucler l'écurie à clé quand le cheval a été volé". Elle ferme, presque six jours, son réseau entier, puis paie (avoue-t-elle) 4,4 millions de dollars de rançon en *Bitcoins*. Peut-être plus par des voies indirectes ; après quoi - surprise ! - *Darkside* disparaît : ses sites du *Darket* s'évaporent, ses "portefeuilles" numériques de *Bitcoins* sont vidés.

Le drame s'amorce. Certes, maintes cyber-attaques furent simulées sur des réseaux sensibles au fil des ans ; mais l'Amérique réalise vite que, dans la vraie vie, un tel piratage est mille fois pire.

- Washington craint le sabotage d'autres réseaux fragiles : eau, électricité, gaz domestique ; ce d'autant que l'économie reprend à peine : si *Colonial Pipeline* reste clos plus d'une semaine, les transports publics de la côte Est risquent la paralysie ; pétrochimie, raffineries, etc., des usines fermeront faute de pouvoir stocker leurs produits.

- Automobilistes, camionneurs, livreurs, etc. paniquent : réaction en chaîne, dans 12 États de la façade Est, 10 000 sations-services sont vite à sec. Devant les autres, des queues d'une heure et plus de clients énervés, remplissant de nuit des jerrycans par dizaines. Effet de dominos, la panique monte du Texas à New York. Le prix de l'essence triple parfois (de 3 à 9 dollars le gallon de 4,6 litres). Un témoin effaré décrit "le premier quart d'heure d'un film-catastrophe". Un autre gémit "on se croirait en Éthiopie".

Le gouvernement "commence à prendre des mesures". Pas simple dans un pays fédéral ET libéral, où les grands groupes et l'appareil d'État vivent sur deux planètes différentes ; où 85% des infrastructures critiques sont aux mains de sociétés privées qui (*lobbying* aidant) n'en font qu'à leur tête pour la sécurité - *cyber* inclus. Situation que les gouvernements fédéraux tolèrent (subissent ?) depuis des décennies. Là-dessus, le cauchemar de l'internet-des-objets, qui transforme une à une toutes les cyber-architectures en passoires...

Résultat : cinq jours après le début du piratage, *Colonial Pipeline* n'a pas parlé à l'agence fédérale dédiée (*CISA, Cybersécurity and Infrastructure Security Agency*).

Fortune faite, *Darkside* donne certes à sa victime des clés de décryptage, mais cet interminable processus ralentit encore le retour du pipeline à la normale.

La suite ? *Darkside* n'est qu'un *cybergang* parmi d'autres ; récemment des entreprises petites et grandes sont attaquées par centaines dans le monde. Les États aussi : la sécurité sociale irlandaise (*Health Service Executive*) est ainsi quasi-paralysée par "le pire des piratages de l'histoire du pays".

Le gouvernement français se veut conscient de ce gravissime problème, mais comme toujours, se protège d'abord lui-même - ce qui est bien - sans trop contrôler ce qu'il advient au-delà, hormis quelques infrastructures et entreprises critiques.

Or aujourd'hui, Internet-des-objets aidant, tout sous-traitant même lointain donne accès au cœur même de forteresses numériques naguère imprenables. Une réalité si inquiétante que ces experts en informatique pour plateaux télévisés qui d'usage, badinent en mode "ça aurait pu être pire", gardent à présent un silence effrayé. ■