DÉBATS • SÉCURITÉ INFORMATIQUE

« Traitons le cybercrime organisé à l'instar du terrorisme »

TRIBUNE

Collectif

Le projet de loi d'orientation et de programmation du ministère de l'intérieur (Lopmi), actuellement débattu au Parlement, aura l'effet paradoxal d'inciter les cybercriminels à frapper la France, déplorent les spécialistes du renseignement Bernard Barbier, Jean-Louis Gergorin et Edouard Guillaud, dans une tribune au « Monde ».

Publié aujourd'hui à 05h00, mis à jour à 05h00 | Lecture 4 min.

Le 21 août, le centre hospitalier de Corbeil-Essonnes (Essonne) a subi une cyberattaque par rançongiciel bloquant son système informatique. Le groupe criminel russe Lockbit l'a revendiquée, le 12 septembre, en réclamant une rançon de 10 millions de dollars (10 millions d'euros) pour obtenir une clé de déblocage et éviter la publication des données dérobées. En l'absence de paiement, des documents médicaux personnels ont été rendus publics sur le dark Net *[l'Internet clandestin, non indexé par les moteurs de recherche, accessible seulement avec des navigateurs spécifiques]*.

Le processus technique de cette cyberattaque réussie utilise des failles techniques classiques au sein du système d'information de l'hôpital. Son directeur général a annoncé que le coût pour contrer la cyberattaque s'élève déjà à plus de 2 millions d'euros et que la reconstruction pour sécuriser le système d'information coûtera plus de 5 millions d'euros.

Ces cyberattaques s'inscrivent dans une longue suite d'agressions d'hôpitaux par rançongiciel, de l'attaque initiale du CHU de Rouen en novembre 2020 à celle de la maternité des Bluets par le groupe russophone Vice Society le 9 octobre. Cette multiplication des attaques contre le système de santé intrigue, car les entités publiques ne paient jamais de rançon. La même observation s'applique aux attaques contre les collectivités locales. Pour élucider ce mystère, il suffit de rappeler ce qu'est l'écosystème des rançongiciels.

Ils signent leurs méfaits

Les entités faîtières de cet écosystème sont des groupes criminels mus par le gain, très majoritairement établis dans des pays autoritaires (principalement Russie, Chine, Corée du Nord, Iran) et donc soumis à une tutelle de fait des services de sécurité de ces pays. Ces groupes d'une part conçoivent et maintiennent les « maliciels » *[programmes malveillants]* de pénétration et de blocage des systèmes d'information ciblés et les outils de collecte et de blanchiment des rançons payées en cryptomonnaies, et d'autre part supervisent des affiliés.

Lire aussi : Cyberattaque contre l'hôpital de Corbeil-Essonnes : ce que l'on sait sur les données diffusées

Depuis environ cinq ans, les groupes russes, qui jusqu'alors protégeaient leur identité, sont apparus publiquement de plus en plus souvent : REvil, Conti, et désormais Lockbit ont pris l'habitude de signer leurs méfaits. Cette nouvelle communication s'explique par le contexte géopolitique. Les dirigeants russes considèrent que depuis la révolution ukrainienne de Maïdan en février 2014, attribuée par eux aux manipulations des Etats-Unis, la Russie est confrontée à une tentative occidentale de déstabiliser son régime. Depuis lors, la Russie se considère comme opposée à « l'Occident global », dans une confrontation hybride qui se caractérise par un mélange d'opérations militaires et d'actions déstabilisatrices non directement létales : cyberattaques et guerre informationnelle, sabotages d'infrastructures critiques de communication ou énergétiques.

Lire aussi : Derrière les attaques aux rançongiciels, un cercle très fermé et vénal de cybercriminels

Les démocraties occidentales ont longtemps ignoré ce caractère hybride des cyberattaques et ont réagi uniquement par des efforts de défense et de résilience *[faire face à l'attaque et assurer la continuité de l'activité]* et par les mécanismes classiques policiers et judiciaires, qui sont inefficaces face à des Etats abritant les groupes de cybercriminels. L'attaque paralysant Colonial Pipeline, un des plus grands opérateurs de gazoducs américains, en mai 2021, a servi de révélateur pour les Etats-Unis.

Désormais, les attaques par rançongiciels sont considérées comme une menace contre la sécurité nationale américaine et légitiment des ripostes précoces contre les agresseurs : l'ensemble des infrastructures numériques du groupe russe REvil a ainsi été mis à bas en octobre 2021 par une opération officieusement confirmée par le CyberCom du Pentagone. Le Royaume-Uni rejoint cette ligne en décembre 2021, en mettant les groupes criminels transnationaux parmi les cibles possibles des ripostes de la National Cyber Force.

Remboursement des rançons

La France, comme ses partenaires de l'UE, continue de ne répondre à la cybercriminalité que par une politique fondée principalement sur la résilience. Cette stratégie annoncée par le président Macron le 18 février 2021, alors que deux hôpitaux venaient d'être durement frappés par des attaques par rançongiciels, est mise en œuvre efficacement. Cependant elle ne supprime en rien l'incitation des cybercriminels à frapper des cibles européennes résultant de l'absence du risque de riposte dure. Le projet de loi d'orientation et de programmation du ministère de l'intérieur (Lopmi), actuellement soumis au Parlement, ajoute une deuxième incitation à frapper la France.

Il légitime le remboursement par les assurances des rançons payées, à la condition de déclarer l'attaque et de porter plainte dans un court délai. Cette disposition non seulement n'aura aucun effet sur les attaques de type guerre hybride, mais enverra un signal désastreux aux hackeurs : pourquoi se priveraient-ils d'attaquer de nouveau, puisque le marché est inépuisable ?

La motivation de cette disposition est évidemment de protéger les entreprises de taille intermédiaire (ETI) et les petites et moyennes entreprises (PME) dont la survie est mise en danger par un blocage prolongé de leur système informatique. Ce risque est une réalité. Mais la disposition de la Lopmi, qui ne prévoit aucune limitation de taille pour les bénéficiaires, peut par son mécanisme retarder les nécessaires investissements de durcissement de la protection numérique des entreprises. Elle devrait au minimum limiter son champ d'application aux PME et ETI et imposer à l'entreprise qui demande à

profiter de ces dispositions un plan d'action volontariste pour en durcir *[sécuriser]* le système d'information et prévoir régulièrement des audits de sécurité.

Capacité souveraine

Au niveau de l'Etat, il faudrait d'une part, créer une incitation fiscale afin de permettre aux PME-ETI d'investir dans la cybersécurité, et d'autre part, défendre sa propre souveraineté numérique en infligeant des dégâts et des coûts significatifs aux entités qui la violent constamment en lançant des attaques par rançongiciels.

Voir notre dossier : Attaques aux rançongiciels : la déferlante

Traitons le cybercrime organisé à l'instar du terrorisme : à la fois dans le cadre pénal et par des instruments spécifiques de sécurité nationale et de défense en appliquant l'article L2321-2 du code de la défense qui autorise l'attaque contre les infrastructures des groupes de cybercriminels.

Le gouvernement français doit profiter de la prochaine loi de programmation militaire pour annoncer publiquement qu'il se réserve la possibilité de neutraliser les systèmes d'information qui s'attaquent à des services publics ou à des entreprises critiques. A cette fin, il est fondamental d'investir massivement dans une capacité souveraine et autonome d'attribution des cyberattaques.

En l'absence d'une telle volonté, non seulement les cybercorsaires attaquant actuellement la France accentueront leurs raids, mais ils seront rejoints par ceux d'autres pays autoritaires souhaitant l'affaiblir.

¶ **Bernard Barbier,** ancien directeur technique de la DGSE, ancien directeur du Laboratoire d'électronique et de technologies de l'information (LETI) et membre de l'Académie des technologies ; **Jean-Louis Gergorin,** chargé de cours à Sciences Po, ancien chef du Centre d'analyse et de prévision du Quai d'Orsay ; **Edouard Guillaud,** amiral et ancien chef d'état-major des armées.

Collectif

Services