MATCH DE LA SEMAINE
ECONOMIE

Santé

LA MENACE DES CYBERATTAQUES

Le secteur sanitaire, particulièrement vulnérable, a été ciblé pendant la pandémie de Covid-19.

Par **Anne-Sophie Lechevallier**
@aslechevallier

Le scénario était écrit et les cibles mobilisées dans toute l'Europe. Cet exercice bisannuel de simulation de cyberattaque, auquel participent les 27 Etats membres, devait pour la première fois impliquer les acteurs de la santé... Il était programmé pour juin, jusqu'à ce que la pandémie oblige à le repousser. Avant même l'émergence du coronavirus, ce secteur concentrait déjà un nombre croissant de cyberattaques. Plus d'une centaine en Europe l'an dernier sur les 450 d'importance recensées contre des entités fournissant un service majeur. En France, sur les 69 incidents relatifs à des attaques par « rançongiciels » traités par l'Agence nationale de la sécurité des systèmes d'information (Anssi) en 2019, 18 concernent la santé, ce qui en fait le secteur le plus touché.

Si les groupes de pirates s'attaquent de plus en plus aux structures sanitaires, c'est que leur pouvoir de nuisance y est immense tant les hôpitaux sont devenus dépendants de leur système d'information pour leurs activités administratives et médicales. Ils peuvent ainsi espérer des gains financiers importants. La « menace informatique la plus préoccupante » selon l'Anssi, tous secteurs confondus, est le rançongiciel. Les criminels, après avoir obtenu les droits d'administrateur d'un réseau, chiffrent les documents et exigent des rançons. Or les fragilités des systèmes hospitaliers sont innombrables, des objets numériques des patients aux appareils médicaux connectés. « Ce secteur est sous-doté en équipement informatique et en personnel, ajoute le professeur Antoine Flahault, directeur de l'Institut de santé globale. Si on le compare au secteur bancaire, les budgets consacrés à la cybersécurité sont bien inférieurs. »

Et pas de trêve durant le confinement. Le 22 mars, l'Assistance publique-Hôpitaux de Paris subissait une attaque rapidement contrée. En Espagne, des employés du secteur sanitaire ont été ciblés par une campagne d'e-mails contenant des rançongiciels. Le 10 mai, l'hôpital San Raffaele de Milan était à son tour visé... « Dans le monde, nous estimons que 30 % des cyberattaques du Covid-19 ont concerné le secteur de la santé, l'OMS y compris, indique Steve Purser, à l'agence européenne Enisa. Du point de vue de la cybersécurité, il n'y a pas eu de crise, malgré les tentatives d'exploiter la situation. » En France, aucun problème majeur ne serait à déplorer. « Nous avons comptabilisé une centaine de signalements de divers incidents au premier semestre, ce qui correspond à la fréquence habituelle », assure Philippe Loudenot, chargé de la sécurité des systèmes d'information des ministères sociaux. Mais les pirates ne sont peut-être pas tous passés à l'action, l'intervalle entre le moment où ils s'introduisent dans un système et celui où ils le paralysent pouvant durer des mois.

LA CYBERMALVEILLANCE A MÊME DES CONSÉQUENCES DIPLOMATIQUES

A l'échelle européenne, la menace a été jugée assez dangereuse pour que le sujet prenne une tournure diplomatique. Après un communiqué du haut représentant pour les affaires étrangères Josep Borrell, la présidente de la Commission, Ursula von der Leyen, a déclaré au terme d'un sommet UE-Chine le 22 juin : « Nous avons vu des cyberattaques contre des hôpitaux et des centres informatiques dédiés. [...] Nous avons clairement indiqué que cela ne pouvait être toléré. » De mémoire bruxelloise, c'est une première. Un pas aussi franchi par les Etats-Unis en mai. Le FBI a accusé des acteurs affiliés au régime chinois de s'intéresser aux entités chargées de la recherche de vaccins et de traitements contre le Covid-19. ■

Le Covid-19, motif d'arnaques en série

Les cybercriminels savent jouer sur les pénuries. A peine les premiers cas d'infection au Covid-19 étaient-ils recensés qu'ils créaient de faux domaines pour vendre du gel et des masques, envoyaient de fausses newsletters et lançaient des campagnes d'hameçonnage mentionnant le coronavirus. De pures escroqueries, qui ne visaient qu'à récupérer données postales et coordonnées bancaires de particuliers. Jérôme Notin, directeur général de Cybermalveillance.gouv.fr, explique : « Si les techniques ne sont en général pas nouvelles, les modes opératoires ont été mis aux couleurs du coronavirus. » Pendant la première semaine de confinement, les demandes d'assistance au service cybermalveillance ont bondi de 400 %, et de 50 % sur toute sa durée. La fréquentation de cette plateforme a été multipliée par 10, avec plus de 20 000 visiteurs uniques par jour. A.S.L.