JÉRÉMY DRON

RANÇONGICIEL : LE VIRUS QUI PARALYSE LES HÔPITAUX FRANÇAIS

Ce mois-ci, Jérémy vous propose un article brûlant d'actualité, sur ces attaques qui touchent les services publics de santé en France depuis la mi-février. Qu'est-ce qu'un rançongiciel ? Comment la France se protège-t-elle ? Un début d'éclaircissement dans cet article....

Depuis un an, les hôpitaux mondiaux se battent face au coronavirus... mais depuis la mi-février, c'est un nouveau type de virus que doivent combattre certains établissements de santé en France: RYUK, c'est le nom donné au virus informatique d'origine de l'Est de l'Europe. Villefranche-sur-Saône, Tarare, et Dax, sont trois centres hospitaliers attaqués par ce virus informatique. C'est une grande partie de leur système informatique qui est paralysé. Les ordinateurs sains sont gardés à l'écart, avec la mise en place de la procédure dite Dégradées. Le personnel n'ayant pas accès aux dossiers médicaux des patients et aux divers appareils d'imagerie et de santé, les opérations ont été déprogrammées, et le services des urgences ont été déviés vers d'autres centres de santé. En fin d'année 2019, c'est le CHU de Rouen qui avait dû faire face à des attaques d'une telle ampleur. Pour cause, selon un rapport de l'Anssi, les hôpitaux sont des cibles privilégiées pour ces attaques, d'autant plus depuis la pandémie. En septembre 2020, les autorités allemandes ont rendu publique le premier décès causé par une attaque informatique.

Un rançongiciel ou ransomware est un logiciel malveillant qui s'introduit d'abord dans le système de la cible. Par la suite, le logiciel commence, peu à peu, à crypter tous les fichiers que détient la machine. La cible a accès uniquement à une note déposée par le pirate, incitant la cible à payer une somme d'argent en crypto monnaie, plus difficile à tracer, afin de récupérer la clef pour décrypter les fichiers. Les pirates adoptent diverses stratégies : soit ils envoient à des milliers de personnes le virus avec une faible rançon, stratégie dite de l'opportuniste ; soit ils ciblent des entreprises ou organismes, en demandant une rançon plus conséquente, stratégie du ciblage. L'ANSSI, l'Agence Nationale de la Sécurité des Systèmes Informatiques, est considérée comme le garde du corps numérique de la France. Le nombre d'interventions de l'ANSSI a été multiplié par quatre en 2020. L'ANSSI déconseille fortement de payer la rançon pour éviter d'alimenter ce genre de pratique. De plus, si vous récupérez la clef de déchiffrement, certains fichiers décryptés seront corrompus. Les autorités semblent impuissantes face à ces attaques qui font de plus en plus de dégâts.