JÉRÉMY DRON

LE RANÇONGICIEL DES HÔPITAUX FRANÇAIS : ON FAIT LE POINT !

Dans cet article d'actualités économiques et juridiques Jérémy revient sur les rançongiciels. Au mois de mars dernier, il vous avait exposé le problème de ces virus informatiques qui paralysaient les services médicaux, mais qu'en est-il aujourd'hui ? Quelle est la situation des hôpitaux ? Comment ces attaques fonctionnent-elles ? Qui se cache derrière celles-ci ?

4'

Rappelez-vous, il y a quelques mois, des hôpitaux français étaient paralysés par un virus informatique appelé rançongiciel. La situation aujourd'hui est loin d'être revenue à la normale. Les médecins utilisent toujours le bon vieux couple papier-stylo pour suivre les patients du mieux qu'ils le peuvent. Pour certains médecins, c'est même plus difficile à gérer que la crise de la Covid-19 elle-même. Les auteurs de cette attaque d'envergure ne sont toujours pas identifiés. Voici une petite piqûre de rappel : un rançongiciel est un logiciel malveillant qui chiffre vos données ce qui les rend tout à fait inutilisables. C'est à ce moment-là que les pirates laissent un petit message, dans un fichier texte parfois caché, à la victime, afin qu'il paie une somme d'argent en bitcoin pour sauver ces données. Par ailleurs, si la victime décide de payer la rançon, ce qui est fortement déconseillé par les autorités, le pirate transmet un logiciel qui est censé déchiffrer les données. Le logiciel bien souvent, bogué et mal conçu ne permet pas de tout récupérer, ainsi certaines données sont tout de même perdues.

Les rançongiciels sont apparus au début des années 1990, envoyés à l'époque par voie postale. C'est en 2010 que le phénomène s'est accentué, les logiciels malveillants étant envoyés par courriel à n'importe qui. Aujourd'hui, les attaques sont plus ciblées, mais les hôpitaux ne sont pas les seuls victimes, les entreprises le sont également. D'après le podcast de nos confrères de le Monde, le célèbre boucher charcutier Fleury Michon a été, lui aussi, victime de ce genre d'attaque. C'est l'ensemble des usines de la firme d'agro-alimentaire qui a été bloqué. Pour certaines entreprises, l'attaque peut représenter jusqu'à 50 millions d'euros de pertes. C'est pourquoi une entreprise qui est restée anonyme a préféré payer la rançon de 28 millions.

Comment se déroule une attaque ? Au début, les ordinateurs ne cessent de s'allumer et de s'éteindre, puis des fonctionnalités ne sont plus exploitables. Souvent, le responsable pense à une attaque interne par un de ses salariés. « Mais ce n'est jamais le cas » affirme Martin Untersinger. Dans ce genre de cas, la priorité est de séparer la partie saine de la partie infectée par le virus, puis trouver comment les pirates ont introduit le réseau. La cellule de crise appelée pour l'occasion occupe les lieux. Personne n'est autorisé à toucher à un des ordinateurs. Il n'est pas rare de voir un post-it avec noté « Ne pas insérer de clé USB », ce fut le cas pour TV5 Monde.

Qui sont ces pirates informatiques qui font trembler de peur ces grands groupes ? Le stéréotype d'une jeune personne isolée est dépassé, de nos jours ces pirates font preuve de professionnalisme dans la cybercriminalité et agissent en groupe organisé. Certains indices comme le fuseau horaire du programme, de morceau de code en cyrillique ou encore des forums russophones laissent à penser qu'ils sont d'origine de l'Europe de l'Est. Mais rien n'est sûr. Leur motivation première est le gain d'argent. Certains pirates avancent comme argument de leurs actes le côté éthique, en renseignant l'entreprise de sa faille de sécurité par exemple. Cette thèse reste à démontrer.