Ransomwares : qu'est-ce que la « triple extorsion » ?

Dans l'univers des *ransomwares*, qu'est-ce que la « triple extorsion » ? On a vu émerger le terme il y a quelques semaines, essentiellement en référence à l'ajout du DDoS dans l'arsenal de groupes cybercriminels. Notamment Avaddon et REvil. Ils s'engageaient à fournir ce service à leurs « affiliés » en complément au socle dit de « double extorsion », à savoir vol + chiffrement de données.

REvil, entre autres, ne s'est pas arrêté là dans l'extension de ses prestations. Il a aussi enrichi son catalogue de moyens de pression avec les appels téléphoniques. À deux destinataires. D'un côté, les partenaires commerciaux des victimes. De l'autre, les médias.

> *#Malware #Ransomware #REvil*
>
> *REvil Ransomware launched a service for contact to news media, companies for the best pressure at no cost, and DDoS (L3, L7) as a paid service.*
>
> *Also, they reminded about developing support for VM ESXi and a polymorphic engine for windows. pic.twitter.com/MahKROK161*
>
> *— 3xp0rt (@3xp0rtblog) March 6, 2021*

Chez Check Point, on mentionne autant le DDoS que les appels téléphoniques. Mais on considère que le véritable marqueur de la « triple extorsion » est ailleurs. En l'occurrence, dans le fait de **demander des rançons à des victimes collatérales**. En première ligne, celles dont on a récupéré des données.

Les micro-rançons de Vastaamo

Pour illustrer son propos, l'éditeur américain cite le cas Vastaamo. Cette entreprise exploite un réseau de cliniques en Finlande. En octobre 2020, on a appris qu'elle avait subi une cyberattaque. La chronologie des événements reste incertaine (la première intrusion pourrait remonter à 2019, voire à 2018). L'ampleur est plus claire : on a dérobé les données de l'essentiel du personnel… et d'environ 36 000 patients.

Le 24 octobre, ces victimes ont commencé à recevoir des e-mails. Voire, pour quelques-uns, des lettres et/ou des coups de téléphone. Motif : une demande de rançon, à hauteur de quelques centaines d'euros et à payer en bitcoins. Quelques-uns auraient effectué la démarche, sous la menace de voir leurs données publiées.

Ce qui s'est joué autour de cette date laisse beaucoup d'hypothèses ouvertes. La tentative d'extorsion des patients semble être intervenue dans un second temps. Les cybercriminels ont peut-être changé de stratégie face à la résistance de la clinique, invitée à régler 40 bitcoins. Mais l'implication d'une tierce partie n'est pas exclure. En particulier du fait d'un curieux fichier de 10 Go

publié à la veille de l'envoi des e-mails. Accompagnant un échantillon de données relatives à 300 patients, il avait rapidement disparu de la circulation. A-t-il pu contenir l'intégralité de la base des patients et ainsi donner une arme potentiellement fatale à qui aurait pu le récupérer ?

Un événement similaire dans la forme mais de moindre ampleur était survenu en 2019 dans un centre américain de chirurgie faciale.

> *I'm aware of only one other patient blackmail case that would be even remotely similar: the Center for Facial Restoration incident in Florida in 2019. This was a different medical area and had a smaller number of victims, but the basic idea was the same. https://t.co/9OPJnAL7We*
>
> *— @mikko (@mikko) October 25, 2020*

Illustration principale © Nmedia – Fotolia