Ransomwares : des prestataires technologiques en eaux troubles ?

Assureurs et prestataires technologiques, aussi gris les uns que les autres face aux *ransomwares* ? Les premiers en ont pris pour leur grade la semaine passée au Sénat. Dans les grandes lignes, on les a accusés de favoriser le paiement des rançons… et de rendre la France d'autant plus attractive pour les cybercriminels.

Il n'y a pas eu, à cette occasion, de pareilles remarques à propos des seconds. Mais eux aussi semblent susceptibles d'entrer dans un jeu trouble. Certains exploitants de *ransomwares* les y invitent en tout cas. Il en est ainsi de Carbon Spider. Ce collectif avait émergé en 2016. Il s'en prenait à l'origine aux terminaux point de vente. Son périmètre d'action avait commencé à s'élargir au printemps 2020. Possiblement en réponse à la réduction d'activité dans le *retail* avec la pandémie.

À partir du mois d'août, le pilier de cette action fut DarkSide, un *ransomware* qui allait plus tard se distinguer en attaquant notamment les serveurs VMware ESXi. Sur la liste de ses victimes revendiquées figurent plusieurs entreprises françaises. Parmi elles, ECS (intégrateur alsacien), OMV System (usinage de précision ; Savoie) et Wonderbox*.

On trouve ladite liste sur un « site vitrine » qui nécessite une connexion au réseau Tor. Ce mode de communication est devenu classique chez les opérateurs de *ransomwares*. Mais « DarkSide Leaks » a des particularités. Kaspersky en a récemment recensé quelques-unes, pour illustrer le business qu'a construit Carbon Spider.

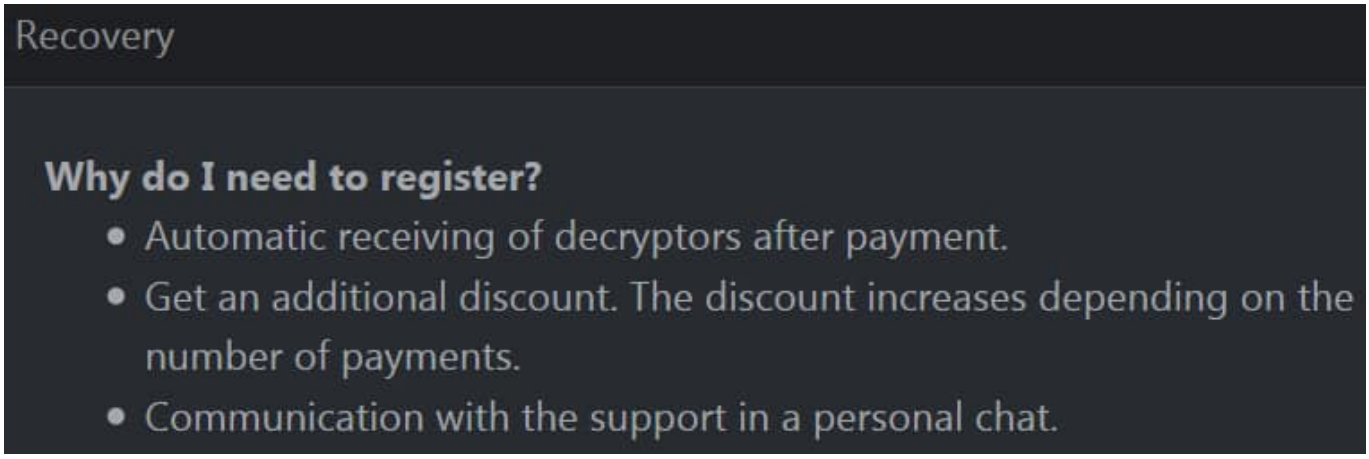
Le site se divise en deux rubriques. La principale consiste en un fil d'annonces, une pour chaque nouvelle victime. L'autre s'intitule « Press Center ». Elle abrite un deuxième fil public d'annonces, mais d'un autre genre. Carbon Spider y déclare par exemple de prétendus « principes éthiques » en vertu desquels il ne s'en prendra pas à certaines entités. Le groupe cybercriminel se félicite aussi d'avoir donné une partie de ses gains à des organisations à but non lucratif.

Des rançons qui ne disent pas leur nom

Pour aller plus loin, par exemple être notifiés par avance des publications de données, les médias sont invités à s'inscrire. Ils ne sont pas les seuls auxquels Carbon Spider fait appel.
Les **prestataires de services de récupération de données** sont aussi dans son collimateur. Les deux derniers messages postés dans le « centre de presse » s'adressent d'ailleurs à eux. Leur contenu est sans équivoque. « Certaines de nos cibles ont besoin d'aide pour déchiffrer et se remettre de nos attaques. Nous cherchons des entreprises que nous pouvons recommander. Nous n'avons pas besoin de coopérer avec vous. [Juste] être sûrs que vous aiderez nos cibles. **Créez un compte chez nous […] et nous prendrons contact avec vous.** »

Il n'est même pas besoin de lire entre les lignes pour comprendre le deal proposé à ces prestataires. Il s'agit d'une combine « à trois temps » :

- Facturer le client pour les services de récupération
- Verser la somme aux cybercriminels
- Recevoir, de la part de ces derniers, les clés de déchiffrement… et une partie de la somme



L'approche est particulièrement intéressante vis-à-vis des établissements publics. On leur interdit peut-être de payer toute rançon, mais pas de recourir à des services de déchiffrement…

** ECS fut le premier des trois à apparaître sur le site de DarkSide. C'était le 19 décembre 2020. Il ne semble pas s'être ensuivi de publication de données. Même chose pour Wonderbox, apparu le 30 janvier. Entre les deux, il y avait eu OMV System (3 janvier)… avec une archive de 33 Go.*