Egregor : le ransomware frappé en plein cœur ?

Egregor, bientôt démantelé ? Rien d'officiel à ce sujet, mais des signaux de plus en plus forts. L'un des derniers en date : une opération que la police judiciaire française aurait menée la semaine passée avec son homologue ukrainienne*. À la clé, l'arrestation, sur place, d'individus possiblement liés à l'activité de ce *ransomware*.

Les enquêteurs auraient réussi à remonter la piste des rançons, payées en bitcoins. Ils auraient orchestré leur coup de filet vendredi.
Depuis ce jour-là, le site « vitrine » d'Egregor est inaccessible. Cette perturbation n'est cependant pas une première. On avait déjà pu constater des indisponibilités prolongées. À tel point que les cybercriminels avaient fini par afficher, à l'occasion d'un énième retour vers la mi-janvier, le message « Malgré vos espoirs, nous sommes à nouveau avec vous ».

Des perturbations, il y en a aussi eu plus récemment. Fin janvier en l'occurrence, à l'heure où une opération internationale mettait à mal un autre *ransomware* : NetWalker. Au-delà du site « vitrine », l'interface de dialogue avec les victimes d'Egregor semble avoir été inaccessible à ce moment-là. Quasiment en parallèle, une autre opération – impliquant également arrestations en Ukraine – portait un coup à l'un de ses vecteurs de diffusion : le botnet Emotet.

Egregor : 200 victimes revendiquées

Découvert en mai 2019 par un chercheur de Malwarebytes, Egregor présente des caractéristiques qui l'inscrivent dans la lignée de Maze. Il aura médiatisé la méthode dite de « double extorsion ». En d'autres termes, l'exfiltration des données avant de les chiffrer, pour engendrer un moyen de pression supplémentaire. Ses créateurs auraient par ailleurs impulsé la constitution d'un « cartel du *ransomware* », en nouant des alliances avec des pairs. Notamment le groupe connu sous le nom de LockBit.

Le CERT-FR lui a dédié un rapport, publié mi-décembre. Il recensait alors 69 organisations victimes. Un volume qui a triplé depuis. En tout cas si on en croit la liste qui figurait sur le « site vitrine » avant son extinction.

Egregor aura fait des victimes de marque en France. Parmi elles, l'éditeur de jeux vidéo Ubisoft et le groupe Ouest-France, touchés respectivement en octobre et en novembre 2020.
On l'aura vu user d'une technique notable chez l'entreprise de distribution chilienne Cencosud : imprimer des demandes de rançon aux caisses de certains magasins.

** En novembre, des affiliés d'un* ransomware *concurrent (REvil/Sodinokibi) avaient affirmé avoir identifié les exploitants d'Egregor. Qu'ils aient guidé les forces de l'ordre n'est pas à exclure.*

> *Heard about the Maze-FSB connection for a while now.*
>
> *REvil operators aren't the only ones who are saying it.*

> *Wonder if they're jealous because the Maze gang can pull off so many brazen and reckless attacks while everybody else has to be on their tiptoes https://t.co/FNd3FIUFm6*
>
> *— Catalin Cimpanu (@campuscodi) November 30, 2020*

Photo d'illustration © Rawpixel.com – stock.adobe.com