Ransomware : Maze est mort, vive Egregor ?

Maze appartiendra-t-il bientôt au passé ? C'est ce que confient certains de ses exploitants.

Leurs témoignages corroborent ce qu'on a pu constater sur le site vitrine du *ransomware*. Le nombre de victimes mises en avant sur la page d'accueil s'est réduit ses dernières semaines. Il ne reste désormais plus que deux entreprises américaines : Platinum Pools (piscines) et Capital Lumber Company (matériaux de construction).

Les 252 autres victimes revendiquées sont passées dans la rubrique « Archive ». Bouygues Construction – touché en janvier – en fait partie. Une vingtaine de Go de données dérobées au groupe français sont disponibles au téléchargement.

Découvert en mai 2019 par un chercheur de Malwarebytes, Maze aura médiatisé cette méthode dite de « double extorsion ». C'est-à-dire l'exfiltration des données avant de les chiffrer, pour engendrer un moyen de pression supplémentaire.

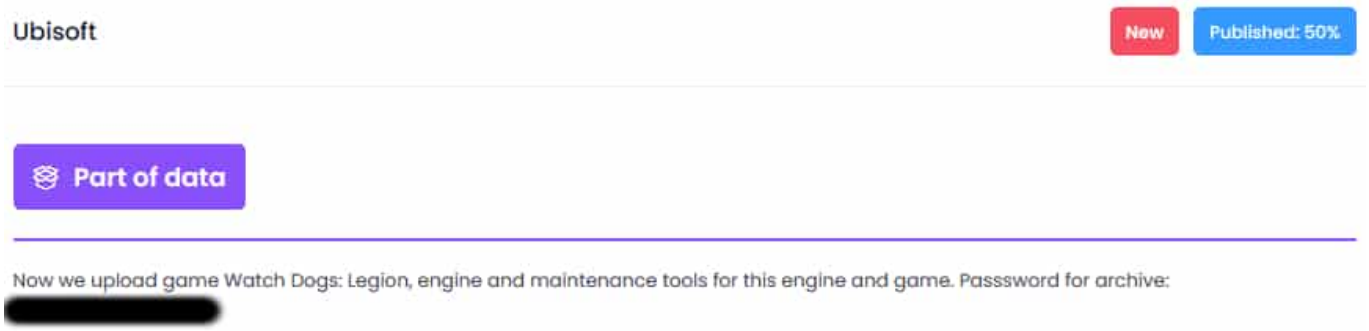
Ses créateurs auront aussi impulsé la constitution d'un « cartel du *ransomware* », en nouant des alliances avec pairs. Notamment les groupes cybercriminels derrière Ragnar Locker et LockBit.

Maze – Egregor : un air de famille

On surveillera l'éventuelle publication des clés de déchiffrement associées à Maze, comme cela s'est passé avec d'autres *ransomwares* arrivés au bout de leur vie. Mais on gardera à l'esprit que cette fin induit un nouveau commencement… vraisemblablement avec Egregor.

Les exploitants de Maze semblent migrer massivement vers ce *ransomware* qui fait figure de descendant direct. Apparemment fondé pour l'essentiel sur le même code, il présente d'autres similitudes, dont les messages de rançon et le nommage des sites destinés au paiement.

Le site vitrine d'Egregor liste pour l'heure une quarantaine de victimes. Deux d'entre elles sont mises en avant sur la page d'accueil, nommées pour « le prix de la faille du mois ». Il s'agit de deux éditeurs de jeux vidéo : l'allemand Crytek et le français Ubisoft. Au menu, nous affirme-t-on, des contrats, des mots de passe, du code source ou encore des infos financières.



> *Egregor actors just published an archive sized more than 500GB for Ubisoft, while saying it's only still 50% of all they have from them.*
> *No idea if it's legit or not, guess some people will verify sooner or later. But if it's not, it would be bad marketing for the actors, so… pic.twitter.com/PBjO4xCaj3*
>
> *— MalwareHunterTeam (@malwrhunterteam) October 28, 2020*

Illustration principale © Sergey Nivens – shutterstock.com