Avaddon : curieuse fin de parcours pour ce ransomware

Combien de victimes Avaddon a-t-il faites ? À raison d'une clé de déchiffrement pour chacune, près de trois milliers. En tout cas selon l'analyse d'un site spécialisé qui a reçu, vendredi dernier, les clés en question. Et en a vérifié l'authenticité.

> *After sharing the file with Emsisoft's @fwosar and @demonslay335, it was confirmed that the keys are legitimate.*
>
> *BleepingComputer encrypted a VM with a recent sample and was able decrypt the machine using a interim decryptor shared with BleepingComputer by @emsisoft. pic.twitter.com/MYYdiei1KA*
>
> *— BleepingComputer (@BleepinComputer) June 11, 2021*

En toile de fond, la vraisemblable fin de vie d'Avaddon. Une vie qui aura duré à peu près un an, sur le modèle RaaS (*ransomware as a service* = proposé à la location).

Le groupe cybercriminel aux commandes d'Avaddon aura été l'un des pratiquants de la « triple extorsion ». Il a en l'occurrence fourni à ses « affiliés » de quoi mener des attaques DDoS en complément au socle vol + chiffrement de données.

AXA fait partie de ses dernières victimes revendiquées, au niveau de plusieurs filiales asiatiques. En début d'année, la commune française de Marolles-sur-Brie (Val-de-Marne) avait elle aussi été touchée. La demande de rançon n'avait semble-t-il pas donné suite. On avait en tout cas fini par trouver, sur l'un des sites d'Avaddon, des données. Dont certaines à caractère personnel, relatives entre autres à des recrutements d'agents municipaux.

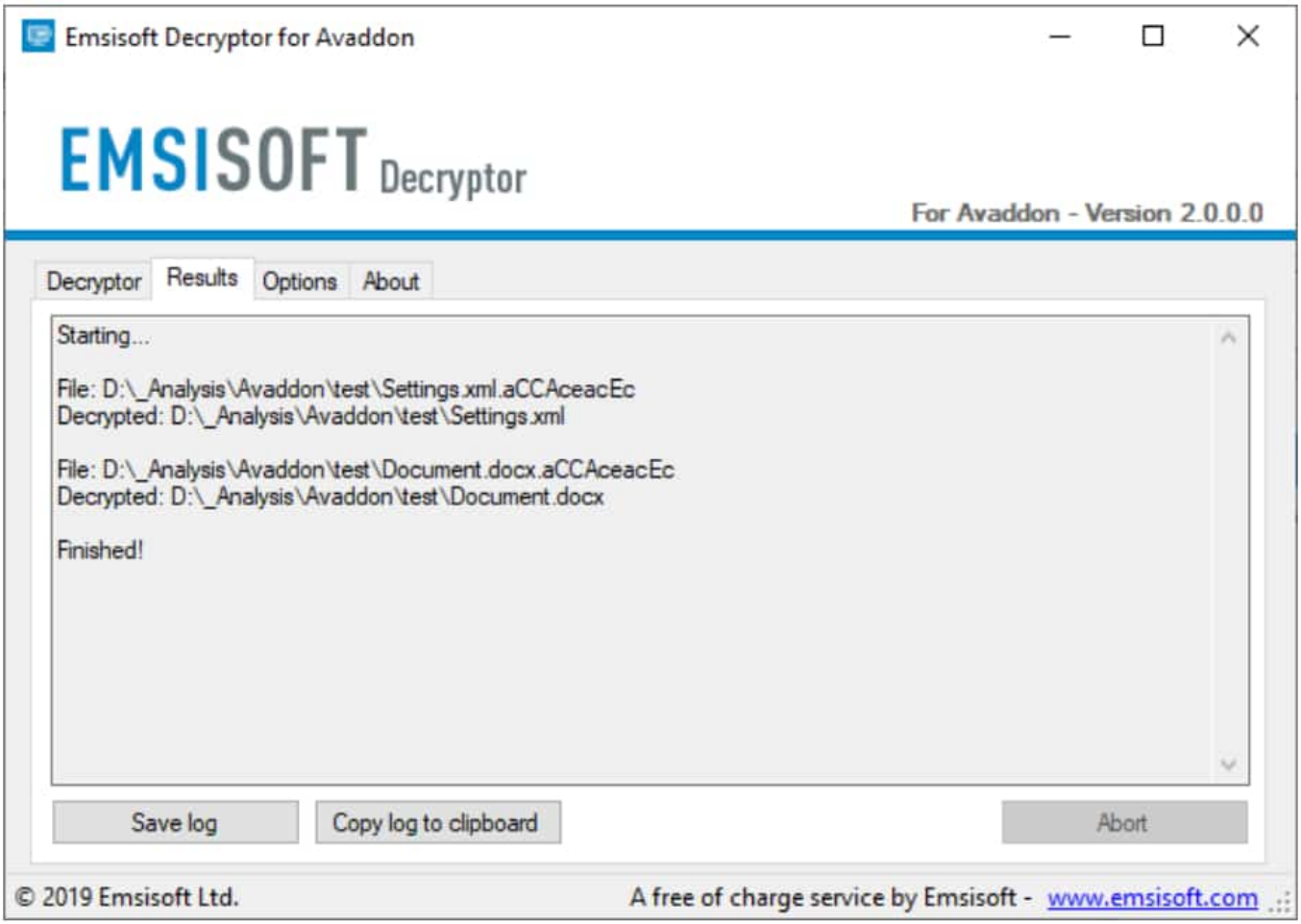
Des « déchiffreurs Avaddon » disponibles

Avaddon fait partie des opérateurs de RaaS qui avaient annoncé modifier leurs règles de fonctionnement après l'affaire Colonial Pipeline. Il avait, en particulier, interdit formellement à ses « clients » de s'en prendre au secteur public, à la santé, à l'éducation et aux organisations à but non lucratif.

Ces derniers jours, Avaddon avait accéléré les négociations avec ses victimes. Et était allé jusqu'à accepter des contre-propositions. Le jour même de la publication des clés, il était banni d'un forum cybercriminel de référence, à la suite d'une plainte d'un fournisseur de services DDoS qui s'en était déjà pris au groupe DarkSide.

> *Avaddon banned from the XSS forum.https://t.co/ALUDpAHxlA pic.twitter.com/Dc1xiT3GCe*
>
> *— 3xp0rt (@3xp0rtblog) June 11, 2021*

Emsisoft a publié un « déchiffreur Avaddon » à partir de ces clés. Il en complète un autre, signé Bitdefender et mis à disposition en amont sur le site du projet No More Ransom.



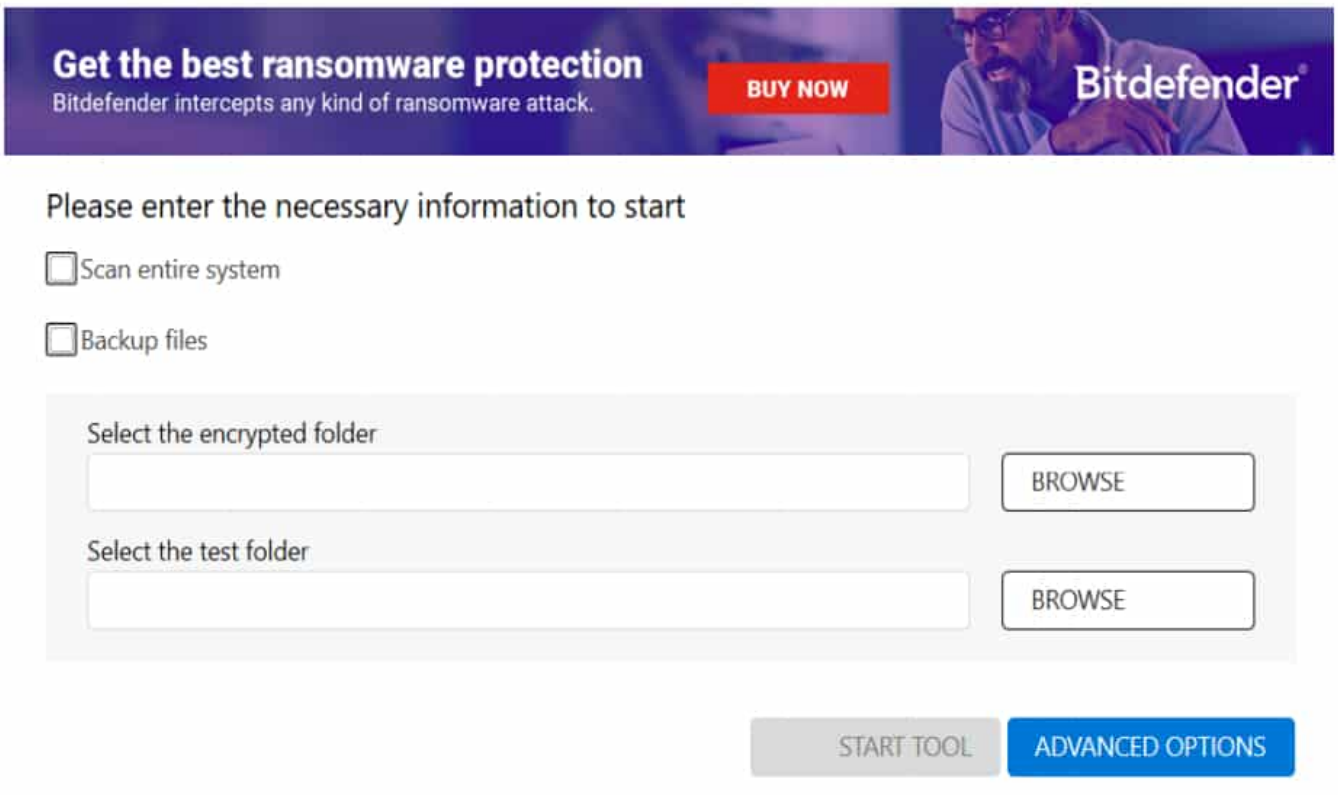


Illustration principale © FLY:D – Unsplash