# REvil : la France ciblée dans l'ombre d'Acer ?

Un *ransomware* peut-il demander 50 millions de dollars à ses victimes ? *A priori*, oui. Acer en témoignera peut-être. Le voilà en tout cas en tête d'affiche sur le « site vitrine » de REvil.

Cette vieille connaissance, qu'on appelle aussi Sodinokibi, fonctionne sur le modèle « par affiliation ». Elle aurait déjà permis à ses commanditaires d'empocher plus de 120 M$.

Acer ne s'en est pas officialisé victime, mais a reconnu des « événements anormaux » sur ses systèmes informatiques.
Pas encore de fichiers publiés, mais des captures d'écran. Elles présentent notamment des listes de clients, d'employés et de comptes bancaires.

Les discussions entre Acer et les assaillants auraient démarré à la mi-mars. Il est question d'un ultimatum au 28 mars. Au-delà, la rançon – exigée en Monero – doublerait, à 100 millions de dollars.

Comment REvil s'est-il infiltré ? L'exploitation de la faille ProxyLogon dans les serveurs Exchange n'est pas à exclure. D'une part, parce que des *logs* dans ce sens ont émergé. De l'autre, parce qu'au moins un *ransomware* s'est déjà engouffré dans cette brèche.

## REvil : une dent contre la France ?

On vient de découvrir, dans un échantillon de REvil, une nouvelle capacité. Le *ransomware* peut forcer le redémarrage de Windows en mode sans échec. Et se faciliter ainsi le chiffrement.

L'une des clés de registre qu'il crée dans ce cadre se nomme « franceisshit ». Littéralement : « La France, c'est de la merde »… Elle permet à Windows de redémarrer normalement une fois le chiffrement accompli.

Une deuxième clé, nommée « AstraZeneca », permet d'assurer que REvil ne s'exécute pas deux fois de suite en mode sans échec. Il est tentant d'y voir un lien avec les tergiversations de la France au sujet de ce vaccin, qu'elle avait un temps suspendu.

> *Not remember seeing these before in REvil ransomware samples.*
> 
> *So basically the actors using REvil now can use it to reboot target machines into safe mode with networking...@demonslay335 @VK_Intel pic.twitter.com/dLk4EirNFO*
>
> — *MalwareHunterTeam (@malwrhunterteam) March 18, 2021*

Acer compte un peu plus de 7 000 employés. En 2020, l'entreprise a dégagé l'équivalent d'environ 8 milliards d'euros de chiffre d'affaires.

*Photo d'illustration © Rawpixel.com – Adobe Stock*