Cyberattaque sur Sopra Steria : un bourreau nommé Ryuk ?

Comment réussir sa gestion de crise ? Sopra Steria proposait, la semaine passée, d'échanger sur le sujet avec les visiteurs des Assises de la cybersécurité.

> *[#LesAssises] Les étapes incontournables pour une gestion de crise réussie ? RDV stand 147 aux @Les_Assises ! Jean-Philippe Cassard, Responsable GRC, est présent pour en échanger avec vous. https://t.co/ezLWcfixPm*
>
> *— Sopra Steria Cybersecurity (@SopraSteriaSecu) October 15, 2020*

La sixième plus grosse ESN française n'imaginait pas qu'elle allait se trouver, quelques jours plus tard, mise en situation. Ce jeudi 21 octobre, vers 19 h, elle a émis un court communiqué faisant état d'une cyberattaque à son encontre, détectée la veille au soir.

Pas de confirmation, depuis lors, de la principale piste qu'on évoque : celle de Ryuk. Le FBI le présentait, en mars dernier à la conférence RSA, comme le plus rentable des *ransomwares*. Avec, en l'occurrence, 61 millions de dollars collectés entre février 2018 et octobre 2019.

Ryuk + Zerologon ?

Dans son étude technique, l'ANSSI met en avant la capacité de Ryuk à contourner les solutions antivirales. Elle souligne aussi la tendance de ses exploitants à réaliser une « étude approfondie » de leurs cibles. Et à faire varier le message de rançon en fonction de l'importance accordée aux victimes.

Son rapport « État de la menace rançongiciel » publié en début d'année établit un lien avec FIN6. Ce groupe cybercriminel russophone se spécialisait initialement dans la compromission d'entités du secteur financier et de terminaux en points de vente.
Le document liste des victimes en France : Travel Technologies Interactive et Fleury Michon, mais aussi Bouygues Construction, à travers une filiale canadienne.

Le *trojan* bancaire TrickBot pourrait être l'un des vecteurs de diffusion de Ryuk On trouve en tout cas régulièrement l'un et l'autre sur les machines infectées. Le *phishing* est un autre canal, apparemment en combinaison avec la faille Zerologon.

> *Steria est la seconde plus grande ESN (sous traitant informatique) en France et travaille notamment avec les ministères de la défense, l'intérieur, l'éducation nationale et Bercy.*
>
> *Il va falloir couper quelques accès VPN... https://t.co/dVE2JIgXzF*
>
> *— Cedric Foll (@follc) October 22, 2020*

Illustration principale © danielfoster437 via *Visual hunt / CC BY-NC-SA*