Forum: Sécurité

Topic: Cyberattaque géante

Subject: Re: Cyberattaque géante

Publié par: Tof81

Contribution le : 23/12/2020 23:58:34

Citation :

tignothe a écrit:
Bonsoir,

Citation :
Wulifk

mais rien ne dis que le malware utilisé ne soit pas par la suite déployé plus généralement.

Le malware dont il est question s'appelle « Sunburst » . C'est un cheval de Troie qui a été introduit dans les mises à jour d'« Orion » un logiciel proposé par la société « SolarWind ».

C'est déjà une performance d'avoir été capable de pénétrer les serveurs d' « Orion » pour introduire Sunburst dans ses mises à jour.

Moi la question que je me pose c'est pourquoi aucun antivirus n'a été capable de repérer ce cheval de Troie qui ouvre « une porte dérobée » au sein du réseau des entreprises ciblée ? 18 000 clients (connus) visés, pas un seul antivirus n'a bronché !

Conclusion (rapide) à quoi servent-ils ? Inquiétant quand même !
Il y a toujours un temps de latence avant la riposte des antivirus, mais cela n'explique pas tout !
J'ai pas réussi à trouver quel(s) étai(en)t l'(es) OS incriminé(s) ?