SolarWinds : nouvelle backdoor… et nouvelles victimes

Une porte dérobée peut en cacher une autre. En tout cas chez SolarWinds.

L'éditeur américain est au cœur d'une probable campagne d'espionnage étatique fondée sur le détournement de sa suite Orion. Les alertes se sont jusqu'alors concentrées pour l'essentiel sur une bibliothèque logicielle. Du code malveillant s'y est logé… et SolarWinds l'a distribué à son insu, par le biais de mises à jour d'Orion.

Le code en question active une *backdoor* qu'on connaît aujourd'hui sous deux noms : SunBurst et Solarigate. Mais pourrait-il en exister une autre ? L'analyse des indicateurs de compromis le suggère. On lui a donné le nom de Supernova. Rien n'indique qu'elle sert la même campagne d'espionnage, voire les mêmes cybercriminels.

Same player shoot again ?

Point commun avec SunBurst/Solarigate : l'infection d'une DLL. Mais cette fois-ci, il s'agit de celle qui est censée transmettre le logo personnalisé du client aux composants de la pile Orion qui en font la demande.

Cette transmission implique une API HTTP. Dans la version vérolée de la DLL, on l'a modifiée afin de pouvoir exécuter des programmes .NET dans le contexte de l'hôte. Tout est compilé et exécuté en mémoire, avec le haut niveau de privilèges dont bénéficie le composant infecté. C'est la porte ouverte à l'exécution de code à distance. Non seulement sur Orion, mais aussi potentiellement sur toute fonctionnalité de Windows exposée par le SDK .NET.

> *This is excellent analysis of a webshell!*
> *However, SUPERNOVA & COSMICGALE are unrelated to this intrusion campaign.*
> *You should definitely investigate them separately bc they are interesting – but don't let it distract from the SUNBURST intrusions.*
> *Details: https://t.co/6FA6VlABV3*
>
> *— Nick Carr (@ItsReallyNick) December 17, 2020*

Touchés, mais pas coulés ?

Qu'en est-il des victimes ? Pour le moment, le bilan se porte sur la *backdoor* SunBurst/Solarigate. De plus en plus d'organisations reconnaissent avoir exécuté des versions compromises d'Orion. En première ligne, des groupes technologiques comme Cisco, Microsoft et VMware.

Une seule de ces victimes déclarées a néanmoins admis une exploitation de la porte dérobée : FireEye. L'éditeur américain, à qui on attribue la découverte de la campagne, estime qu'une

cinquantaine de cibles sont dans le même cas. Ses données concordent avec celles de Microsoft, qui estime que l'attaque est allée, chez une quarantaine de ses clients, plus loin que le dépôt de la *backdoor*.

Des listes de victimes présumées ont commencé à apparaître. Elles se fondent sur la rétroingénierie d'un élément : l'URL que tente de joindre la porte dérobée.

Une partie de cette URL est dynamique, au sens où elle dépend de la cible. Elle consiste en 16 caractères aléatoires additionnés d'une chaîne obtenue par encodage du nom de l'Active Directory auquel est connecté le serveur infecté.

Secrets algorithmiques

L'algorithme mis à contribution exploite deux méthodes. Si le nom de l'Active Directory comprend des capitales, il exploite un encodeur base64 assorti d'un alphabet personnalisé (ph2eifo3n5utg1j8d94qrvbmk0sal76c). Sinon, il s'appuie sur une table de substitution.

Cette dernière se présente ainsi : rq3gsalt6u1iyfzop572d49bnx8cvmkewhj. L'algorithme encode chaque caractère en le remplaçant par celui qui se trouve quatre rangs sur sa droite dans ladite table. La règle diffère légèrement pour les caractères spéciaux, encodés notamment avec un 0 préposé.

Pour savoir quelle méthode a été appliquée, un indice : les chaînes encodées en base64 commencent forcément par 00.

Le décodage laisse apparaître des noms d'hôtes plus ou moins explicites. Parmi ceux qui laissent peu de doutes, il y a belkin.com, cisco.com, nvidia.com, amr.corp.intel et us.deloitte.co. À supposer, évidemment, que les données sources (telles celles-ci ou celles-là) soient de confiance.

> *here is the list of more than 4k sub-domain infrastructure including #DGA domain used by #UNC2452 #SolarWinds #backdoor*
> *Link: https://t.co/UL9myJnYbn*
> *cc: @iblametom @TheHackersNews @threatpost*
>
> *— R. Bansal □□□ (@0xrb) December 16, 2020*

SolarWinds : d'une *backdoor* à l'autre

Les cibles supposées sont majoritairement basées en Amérique du Nord. On en trouve toutefois une nombre important en Israël, pays allié des États-Unis. Notamment l'institut Technion, l'université de Haïfa et la chaîne Channel 2.

Le secteur public ne manque pas à l'appel, entre hôpitaux, écoles et municipalités. On sait le gouvernement américain largement touché, mais son homologue australien l'a peut-être aussi été, au moins à travers son ministère de la Santé. Plus proche de nous, on aura noté la présence de

l'Insead (Institut européen d'administration des affaires), qui a ses bases en France.

Quant à savoir lesquelles de ces cibles ont été d'intérêt pour les exploitants de la *backdoor*, on peut tenter d'examiner les commandes que celle-ci reçoit. Parfois, elles ouvrent une autre porte dérobée liée à un autre serveur de commande et de contrôle. Probablement le signe d'une offensive plus approfondie.

À lire en complément, le « fil rouge SolarWinds » de Silicon.fr :

- SolarWinds : ce qu'on sait une semaine après les révélations (article du 21 décembre 2020)
- SolarWinds : les entreprises IT, pivots de la cyberattaque ? (18 décembre)
- SolarWinds : quand des logiciels légitimes servent de *backdoors* (14 décembre)

Illustration principale © Rawpixel.com – Adobe Stock