SolarWinds : la chaîne d'attaque se dessine

Jusqu'où va la chaîne SolarWinds ? Un mois s'est écoulé depuis la révélation de cette campagne d'espionnage XXL… et on continue d'en découvrir des maillons.

Le logiciel de gestion informatique Orion – qu'édite l'entreprise américaine SolarWinds – apparaît toujours comme le centre névralgique. On y a trouvé plusieurs *backdoors* injectées dans des mises à jour.

Voici qu'émergent des informations à propos du *malware* qui aurait permis la mise en place d'une de ces *backdoors*. CrowdStrike lui donne le nom de **Sunspot**. Son analyse se fonde sur un échantillon compilé le 20 février 2020. Soit précisément la date à laquelle SolarWinds situe le début du déploiement sur des serveurs de développement d'Orion.

Sunspot serait resté sur ces serveurs jusqu'au 4 juin 2020. Pendant tout ce temps, il a exécuté, en boucle (à intervalle d'une seconde), une routine destinée, dans les grandes lignes, à :

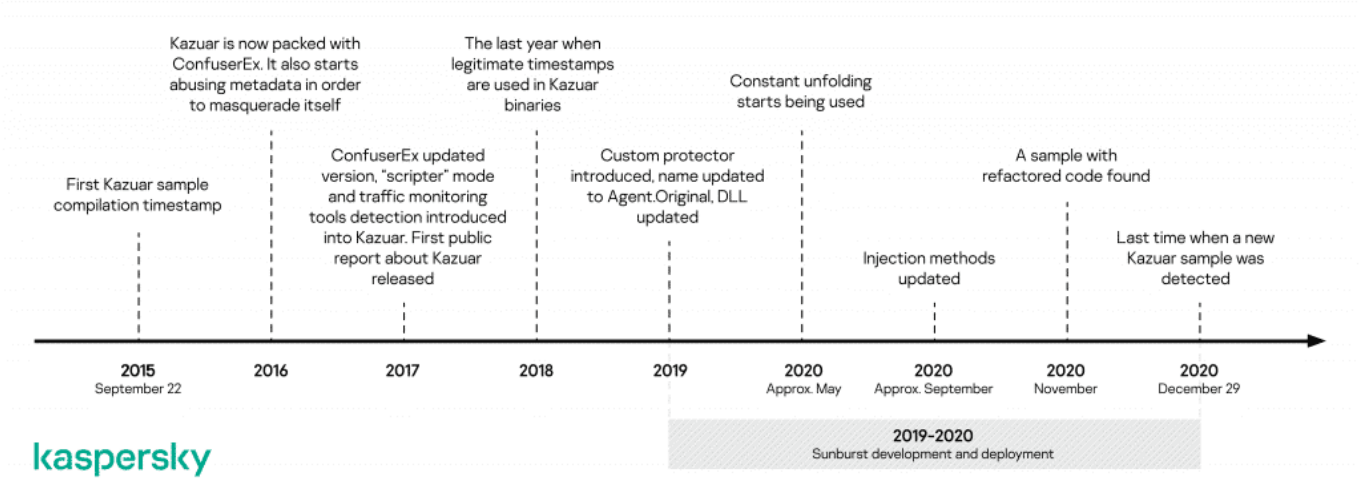
- détecter les instances de MSBuild.exe (composant de Visual Studio) ;
- repérer celles qui compilaient Orion ;
- modifier, dans le répertoire de compilation, le fichier InventoryManager.cs en y intégrant le code malveillant.

La démarche a impliqué plusieurs garde-fous (hashs, mutex, directives pragma…) pour minimiser les chances de voir remonter des alertes. Le code malveillant lui-même était chiffré (en AES128-CBC), comme les *logs* (RC4).

Kazuar et SolarLeaks

Du côté de Kaspersky, on établit un parallèle avec Kazuar. Depuis 2017, on a connaissance de cette *backdoor* souvent attribuée à Turla, groupe cybercriminel russe qui aurait ciblé, entre autres, des administrations publiques en Autriche et en Arménie.
Parmi les ressemblances avec Sunspot, on notera trois algorithmes, qui assurent respectivement :

- La création des identifiants uniques des victimes
- La gestion des délais de connexion avec le serveur de commande et de contrôle
- Le hachage de certains fichiers



Microsoft et FireEye ont tous deux reconnu faire partie des victimes… et avoir constaté des accès indésirables au code source de certains de leurs produits.
L'un et l'autre se retrouvent en vitrine sur un site « SolarLeaks » qui prétend proposer à la vente une partie du code source en question. Prix affichés : 600 000 $ pour le pack Microsoft (2,6 Go) et 50 000 $ pour le pack FireEye (39 Mo). SolarWinds aussi figure sur la liste, avec un lot à 250 000 $. Même sort pour Cisco (500 000 $), qui a réagi. Le groupe américain appelle à la méfiance et assure n'avoir aucune preuve qu'on lui ait dérobé des données.

Illustration principale © Rawpixel.com – stock.adobe.com