SolarWinds : une campagne d'espionnage peut en cacher une autre

Sunburst et Supernova auraient-elles servi des campagnes d'espionnage distinctes, voire différents groupes cybercriminels ? On le supposait… et cela semble se confirmer.

L'une et l'autre de ces *backdoors* ont visé la plate-forme logicielle Orion de SolarWinds. Les alertes se sont jusqu'alors largement concentrées sur la première. Elle résidait dans une DLL vérolée que SolarWinds a distribuée à son insu, au travers de mises à jour d'Orion. Les États-Unis apparaissent comme la principale victime. Ils ont désigné un responsable : la Russie.

Supernova se fondait aussi sur le détournement d'une bibliothèque logicielle. Mais le code malveillant ne résidait pas dans des *updates* d'Orion. Et il n'était pas signé. Ces différences – entre autres – avaient suggéré l'existence d'une deuxième attaque. Pour en trouver l'origine, il semble falloir regarder du côté de la Chine.

> *1. The software flaw (known as SUPERNOVA) exploited by the suspected Chinese group is separate from the one the United States has accused Russian government operatives of using to compromise up to 18,000 SolarWinds customers https://t.co/m2eQQDPvjv*
>
> *— Chris Bing (@Bing_Chris) February 2, 2021*

Parmi les victimes de cette attaque « parallèle » figurerait le National Finance Center. L'agence dépend du département américain de l'Agriculture. Elle affirme gérer paye et RH pour « plus de 160 » organes gouvernementaux dont le FBI, le Trésor et le département d'État.

SolarWinds : au-delà des *backdoors*

SolarWinds a déclaré avoir examiné, avant même le début de l'affaire qui porte aujourd'hui son nom, un cas de piratage potentiel vraisemblablement basé sur Supernova. Il n'avait cependant pas pu en identifier les auteurs. Ce qui lui semble plus clair, c'est la compromission de son Office 365. Des tiers indésirables auraient commencé à y accéder fin 2019. Avec, comme porte d'entrée, un compte de messagerie.

Comment ces tiers possiblement en lien avec Sunburst et/ou Supernova ont-ils pu passer si longtemps sous les radars ? Microsoft a fourni quelques éléments de réponse axés sur le cas Sunburst. En insistant sur le soin apporté à séparer l'exécution de la *backdoor* et du loader Cobalt Strike qu'elle a servi à déployer. L'objectif étant, pour les pirates, d'éviter que la chaîne d'attaque soit mise au jour à la découverte d'un seul de ses maillons.

On continue à découvrir des éléments de cette chaîne. Symantec, par exemple, a récemment attiré l'attention sur un dropper « alternatif ». On connaissait Teardrop, utilisé pour récupérer l'exploit Cobalt Strike. Il y a aussi Raindrop. Il lui ressemble, mais n'est pas livré *via* Sunburst. On le trouve

toutefois sur des réseaux où la *backdoor* est présente.

Sunburst et Supernova n'ont visiblement pas été les seuls supports de ces différentes attaques. Compte tenu du but final (les environnements Office 365), d'autres techniques ont été mises à contribution. Elles gravitent essentiellement autour d'Active Directory. Malwarebytes en a été victime, alors même qu'il n'est pas client de SolarWinds.

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