SolarWinds : de nouvelles armes du crime mises au jour

Dark Halo, Nobelium, SolarStorm, StellarParticle, UNC2452… Autant de noms qu'on a attribués à un même groupe cybercriminel. En l'occurrence, celui à l'origine de la méga-campagne d'espionnage révélée voilà bientôt quatre mois.

Le premier vecteur mis au jour avait été une *backdoor* glissée dans des *updates* d'un logiciel de supervision IT made in SolarWinds. Depuis, on découvre régulièrement d'autres outils qui ont – ou semblent avoir – alimenté l'opération. Parmi eux, certains servent à établir une persistance sur des réseaux préalablement compromis. Microsoft en a étudié trois. Il les a baptisés GoldMax, GoldFinder et Sibot.

D'après les échantillons examinés, ces *malwares* ont frappé essentiellement à l'été 2020. GoldFinder apparaît comme le moins complexe. Écrit en Go, il a vraisemblablement servi à identifier, sur des réseaux compromis, les points potentiels de détection de l'activité malveillante. Ce en suivant la route de requêtes HTTP adressées à un serveur donné.

SolarWinds : la pointe de l'iceberg

Également codé en Go, GoldMax a assuré sa persistance par le biais d'une tâche planifiée. Dans l'ensemble des cas étudiés, cette tâche portait le nom d'un logiciel existant dans l'environnement infecté. Elle pointait vers un dossier du même nom contenant un exécutable… du même nom : l'implant en lui-même.

GoldMax sécurise la connexion avec ses serveurs de commande et de contrôle (C2) grâce à des clés de session. Ces serveurs sont souvent accessibles *via* des noms de domaines acquis auprès de revendeurs. L'ancien enregistrement Whois étant conservé, ils paraissent d'autant moins suspects.
L'implant présente aussi des capacités de masquage du trafic. Il utilise notamment les en-têtes de cookies pour transmettre des informations au C2 et recevoir des instructions. Il peut aussi intercaler, dans son flux, des requêtes vers des URL légitimes.

L'implant embarque des informations de configuration. Mais à la première exécution, il les copie, encodées en Base64, dans un fichier .tmp. Cela facilite leur mise à jour ultérieure par l'intermédiaire du C2.

Deux *backdoors* pour le prix d'une ?

FireEye – à l'origine des premières révélations sur SolarWinds – fait état d'une *backdoor* qui ressemble beaucoup à GoldMax : Sunshuttle. Une entité « basée aux États-Unis » l'aurait téléversée en août 2020 sur un dépôt public de *malwares*. Elle reprend les fonctionnalités de masquage du trafic et le principe des clés de session. Mais pas la mise en place d'une tâche planifiée. Comme GoldMax, sa première action est de vérifier l'existence d'une adresse MAC codée en dur (et, le cas échéant, de stopper son activité). Il semble que ce soit celle de l'interface réseau virtuelle de la

sandbox Windows.

Sibot, lui, embarque bien un mécanisme de persistance par planification. Mais pas dans toutes ses variantes, au nombre de trois selon Microsoft. L'implant se fait passer pour une tâche Windows. Soit il télécharge directement une charge utile, soit il s'appuie sur un script stocké dans le registre ou sur le disque et éventuellement exécuté par une tâche planifiée.

Le charge utile en question prend la forme d'une bibliothèque. Elle vient prendre place dans le dossier des pilotes et, renommée en .sys, s'exécute *via* rundll32. L'empreinte sur la machine infectée est réduite, les mises à jour de la DLL se faisant côté serveur.

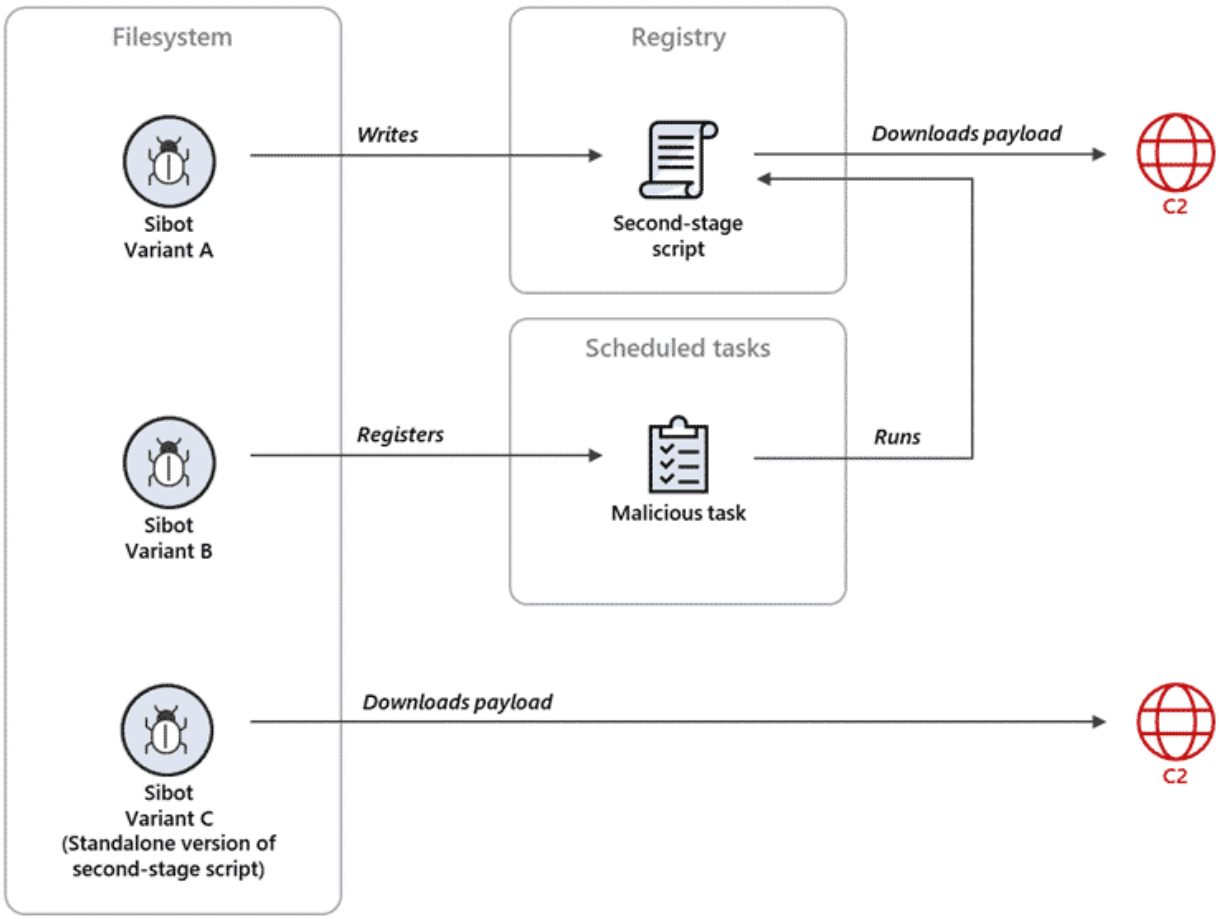

Illustration principale © Rawpixel.com – stock.adobe.com
Images du corps d'article © Microsoft