Ongoing Analysis of SolarWinds Impacts

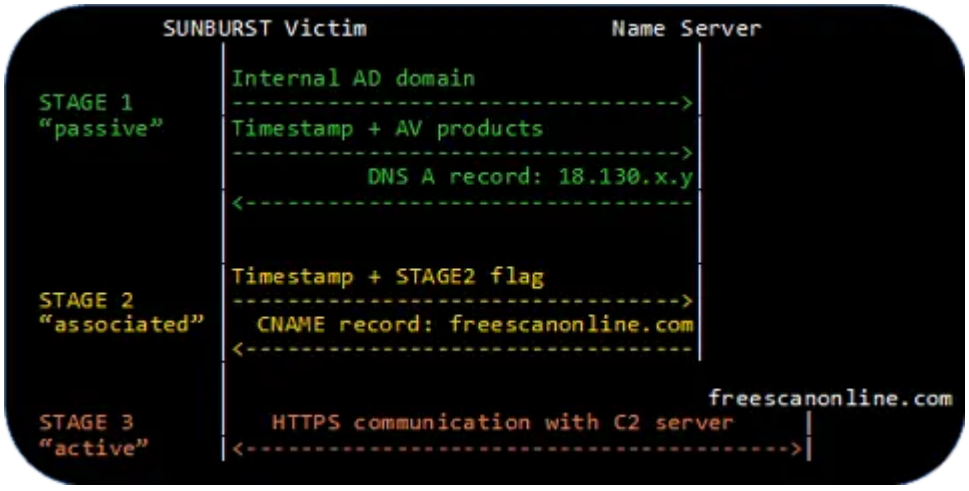
By Rami Mizrahi

Published: 2021-01-26 · Archived: 2026-04-05 21:24:07 UTC

If you are following the latest updates on the SolarWinds attack, you may have seen that hq.fidelis is now included in the growing list of domains known to have been targeted by the attackers. While hq.fidelis is not conclusively Fidelis Security, it certainly could be associated with us and something we needed to investigate further. In this blog, we, Fidelis TRT team, will provide you with the latest information we have on this as well as our efforts to date to investigate and determine if there has been any impact to our networks and data.

To date we have not turned up any evidence that the SolarWinds compromise has impacted our networks; although, our analysis continues. In the spirit of openness and the trust we have with our customers, partners, and the greater security community, we are providing a detailed account of our investigation and will continue to update it here.

On Monday, 1/25, security research firm NETRESEC AB published a list of 23 domains containing the "STAGE2" flag in SUNBURST's DNS beacons[1]. The "STAGE 2" flag identifies domains that were singled out as interesting targets by the threat actors, and "hq.fidelis" was included in that list. The diagram below indicates the three stages of the SUNBURST attack sequence as identified by FireEye.



Ref: NETRESEC Blog

Following the FireEye/SolarWinds disclosure in December, we initiated an internal review of Fidelis networks under the assumption that we too could have been a target. We do not use SolarWinds Orion software for management of our corporate systems; however, the nature of our work requires us to test all kinds of software for compatibility with our products and we wanted to rule out use of SolarWinds software anywhere within our networks. Using Fidelis Endpoint, we were able to determine that we had installed an evaluation copy of the trojanized SolarWinds Orion software on one of our machines in May 2020 as part of a software evaluation and as a result, we continued to dig deeper. The software installation was traced to a machine configured as a test system, isolated from our core network, and infrequently powered on.

Our initial review also included analysis of Fidelis Network metadata and various system logs using threat indicators provided by the Fidelis Threat Research Team (TRT) as well as threat indicators and analysis tools published by others. One of those tools was NETRESEC's Sunburst Domain Decoder Tool[2] that filters and decodes passive DNS (pDNS) records associated with the SUNBURST "STAGE 1" callout domain (avsvmcloud). Using the pDNS sources available at the time, we did not identify the "hq.fidelis" domain in pDNS records associated with SUNBURST.

On Friday evening (1/23), we identified an additional source of pDNS information and using the Sunburst Domain Decoder Tool were able to confirm that a machine on hq.fidelis domain had communicated with the SUNBURST callout "STAGE 1" domain and hq.fidelis was flagged by the attackers as a domain of interest and worth targeting. From analysis of the pDNS records we were able to identify a four-day period in May where the machine on our network communicated with the malware's "STAGE 1" infrastructure (avsvmcloud). Analysis of pDNS records also indicated that the malware set the "STAGE 2" flag within the DNS transaction indicating that we were a target of interest to the attacker. We, however, have not been able to identify any follow-on pDNS or DNS transactions that provide a CNAME for the malware's "STAGE 3" C2 infrastructure (we would certainly appreciate any pointers to this information from the security researcher community if they have additional information to offer). The absence of DNS records that provide a CNAME for the "STAGE 3" command and control would indicate that the malware on our system may not have received a CNAME required for it to communicate with the "STAGE 3" C2 infrastructure.

Our current belief, subject to change given additional information, is that the test and evaluation machine where this software was installed was sufficiently isolated and powered up too infrequently for the attacker to take it to the next stage of the attack.

Though we have not identified any evidence to date that the SolarWinds compromise has impacted our networks, we will continue to investigate potential impacts using our own tooling much like we recommend our customers do. While we are not happy about being targeted by the attackers behind the SolarWinds, FireEye, Microsoft, and Malwarebytes attacks, we think this is a good learning opportunity both for our own internal team (i.e., drink your own champagne and practice your incident response plan), as well as the security community on the best practices to apply to an advanced adversary attack like "SUNBURST". To this end we will publish best practices for identifying whether your enterprise may be under attack from an adversary like the one behind the SolarWinds attack as well as our findings.

References

1. ^https://www.netresec.com/?page=Blog&month=2021-01&post=Twenty-three-SUNBURST-Targets-Identified
2. ^https://www.netresec.com/?page=Blog&month=2021-01&post=Finding-Targeted-SUNBURST-Victims-with-pDNS
