SolarWinds kompromittert

SUNBURST malware

Oppsummering av saken

- Fireeye meldte 13. desember at de har oppdaget en global inbruddskampanje.
- De oppdaget et "supply chain attack" som har laget trojaner i SolarWinds Orion programvare for å distribuere malware kalt SUNBURST
- Angrepet benytter forskjellige teknikker for å unngå deteksjon og skjule aktiviteten, men det finnes også mulighet til å oppdage dette.
- Fireeye har frigitt signaturer for å oppdage angrepet på egen GitHub side

Eksterne referanser og informasjon

Fireeye:
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Solarwinds:
https://www.solarwinds.com/securityadvisory

Netsecurity anbefaler:

1. Isoler Solarwinds installasjonen fra internett
2. Les og sett dere inn i overnevnte informasjon
3. For å verifisere at dere er utsatt
4. Sjekk filene SolarWinds.Orion.Core.BusinessLayer.dll og netsetupsvc.dll i en oppdatert antivirus-løsning, eventuelt bruk Virustotal, her https://www.virustotal.com/gui/home/upload, eller verifiser hash-sum mot kjente indikatorlister.
5. Dersom mulig:
    a. sjekk om det har gått DNS trafikk til domenene nevnt i Fireeye informasjonen, listet under avsnittet "DGA and Blocklists"
    b. At dere har fått DNS svar som matcher rangen oppgitt under avsnitte "Network Command and Control (C2)", svar som matcher har vil ha terminert malwaren
6. Bytt passord på alle kontoer som har tilgang inn mot Solarwinds server
7. Følg med på Solarwinds sider og oppdatert til versjon som inkludere fiks, tenativt update H2 som har ETA 15/12.

Dersom dere ønsker bistand fra Netsecurity til enten å sjekke dette, eller til å verifisere at dere ikke er utsatt for videre kompromittering, eller for generell sjekk av infrastrukturen eller annet, så ber vi dere ta kontakt!