SolarWinds Orion Compromise

Emerging Threat Intelligence Summary

Brent Huston
Security Evangelist & CEO
@lbhuston

MICROSOLVED, INC.

Wide Scale Exploitation Identified

- A back door (“SunBurst”) was illicitly installed into SolarWinds Orion versions 2019.4 to 2020.2.1 HF1 - inclusive

- Allows remote access at admin-level in the product via outbound connections to C2 servers

- Attackers have been actively exploiting the issue across many organizations including sensitive targets

- Product is widely used and stores significant amounts of credentials and proprietary environment data

Known Impacts

- Attackers have been observed using capabilities to empower lateral spread and wide-scale intelligence gathering

- Attackers have been employing significant stealth and opsec, displaying advanced capabilities and targeting network infrastructure as well as systems

- Attackers have been widely leveraging RDP and dropping additional malware and beacon tools as they proceed

- **Data theft has been observed as a part of this campaign**

Investigation & Response

- **If you have an affected version, isolate the system immediately**
- Perform an investigation using the techniques from the articles on the next page
- Change all credentials held in the system, assume all credentials are compromised and handle as such
- Review all egress and system logs for signs of exploitation, as described in the articles on the next page

Sources for More Information

- **Excellent, concise updated information** - https://www.ncsc.gov.uk/guidance/dealing-with-the-solarwinds-orion-compromise
- **FireEye coverage with significant technical details** - https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
- **FireEye GITHub of technical mitigations** - https://github.com/fireeye/sunburst_countermeasures
- **DHS/CISA Directive** - https://cyber.dhs.gov/ed/21-01/
- **SolarWinds Security Advisory** - https://www.solarwinds.com/securityadvisory

Additional Help

- If you need additional assistance including incident response, log analysis or the like, please contact us:
  - (614) 351-1237
  - info@microsolved.com
  - https://microsolved.com/contact
- **If you'd like to discuss specific issues or concerns, please get in touch!**