# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:59:57 UTC



## Tool: SUNSPOT

| | |
|---|---|
| Names | SUNSPOT |
| Category | Malware |
| Type | Rootkit |
| Description | (CrowdStrike) SUNSPOT is StellarParticle's malware used to insert the SUNBURST backdoor into software builds of the SolarWinds Orion IT management product. SUNSPOT monitors running processes for those involved in compilation of the Orion product and replaces one of the source files to include the SUNBURST backdoor code. Several safeguards were added to SUNSPOT to avoid the Orion builds from failing, potentially alerting developers to the adversary's presence. |
| Information | <https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/> |
| MITRE ATT&CK | <https://attack.mitre.org/software/S0562/> |

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

### All groups using tool SUNSPOT

| Changed | Name | Country | Observed | |
|---|---|---|---|---|
| **APT groups** | | | | |
| | APT 29, Cozy Bear, The Dukes | | 2008-Feb 2025 | |

*1 group listed (1 APT, 0 other, 0 unknown)*