SUNSPOT, Software S0562 | MITRE ATT&CK®

Archived: 2026-04-05 13:26:56 UTC

Domain	ID		Name	Use
Enterprise	T1134		Access Token Manipulation	SUNSPOT modified its security token to grants itself debugging privileges by adding `SeDebugPrivilege`.[1]
Enterprise	T1565	.001	Data Manipulation: Stored Data Manipulation	SUNSPOT created a copy of the SolarWinds Orion software source file with a `.bk` extension to backup the original content, wrote SUNBURST using the same filename but with a `.tmp` extension, and then moved SUNBURST using `MoveFileEx` to the original filename with a `.cs` extension so it could be compiled within Orion software.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	SUNSPOT decrypts SUNBURST, which was stored in AES128-CBC encrypted blobs.[1]
Enterprise	T1480		Execution Guardrails	SUNSPOT only replaces SolarWinds Orion source code if the MD5 checksums of both the original source code file and backdoored replacement source code match hardcoded values.[1]
		.002	Mutual Exclusion	SUNSPOT creates a mutex using the hard-coded value `{12d61a41-4b74-7610-a4d8-3028d2f56395}` to ensure that only one instance of itself is running.[1]
Enterprise	T1083		File and Directory Discovery	SUNSPOT enumerated the Orion software Visual Studio solution directory path.[1]

Domain	ID		Name	Use
Enterprise	T1070	.004	Indicator Removal: File Deletion	Following the successful injection of SUNBURST, SUNSPOT deleted a temporary file it created named `InventoryManager.bk` after restoring the original SolarWinds Orion source code to the software library.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	SUNSPOT was identified on disk with a filename of `taskhostsvc.exe` and it created an encrypted log file at `C:\Windows\Temp\vmware-vmdmp.log` .[1]
Enterprise	T1106		Native API	SUNSPOT used Windows API functions such as `MoveFileEx` and `NtQueryInformationProcess` as part of the SUNBURST injection process.[1]
Enterprise	T1027		Obfuscated Files or Information	SUNSPOT encrypted log entries it collected with the stream cipher RC4 using a hard-coded key. It also uses AES128-CBC encrypted blobs for SUNBURST source code and data extracted from the SolarWinds Orion <MsBuild.exe process.[1]
Enterprise	T1057		Process Discovery	SUNSPOT monitored running processes for instances of `MsBuild.exe` by hashing the name of each running process and comparing it to the corresponding value `0x53D525` . It also extracted command-line arguments and individual arguments from the running `MsBuild.exe` process to identify the directory path of the Orion software Visual Studio solution.[1]
Enterprise	T1195	.002	Supply Chain Compromise: Compromise Software Supply Chain	SUNSPOT malware was designed and used to insert SUNBURST into software builds of the SolarWinds Orion IT management product.[1]

Source: https://attack.mitre.org/software/S0562/