SUNBURST, Software S0559 | MITRE ATT&CK®

Archived: 2026-04-05 18:38:42 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

SUNBURST communicated via HTTP GET or HTTP POST requests to third party servers for C2.[3]

.004 Application Layer Protocol: DNS

SUNBURST used DNS for C2 traffic designed to mimic normal SolarWinds API communications.[3]

Enterprise T1059 .005 Command and Scripting Interpreter: Visual Basic

SUNBURST used VBScripts to initiate the execution of payloads.[2]

Enterprise T1132 .001 Data Encoding: Standard Encoding

SUNBURST used Base64 encoding in its C2 traffic.[3]

Enterprise T1005 Data from Local System

SUNBURST collected information from a compromised host.[4][3]

Enterprise T1001 .001 Data Obfuscation: Junk Data

SUNBURST added junk bytes to its C2 over HTTP.[3]

.002 Data Obfuscation: Steganography

SUNBURST C2 data attempted to appear as benign XML related to .NET assemblies or as a faux JSON blob.[3][5][6]

.003 Data Obfuscation: Protocol or Service Impersonation

SUNBURST masqueraded its network traffic as the Orion Improvement Program (OIP) protocol.[3]

Enterprise T1568 Dynamic Resolution

SUNBURST dynamically resolved C2 infrastructure for randomly-generated subdomains within a parent domain.[3]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

SUNBURST encrypted C2 traffic using a single-byte-XOR cipher.[3]

Enterprise T1546 .012 Event Triggered Execution: Image File Execution Options Injection

SUNBURST created an Image File Execution Options (IFEO) Debugger registry value for the process `dllhost.exe` to trigger the installation of Cobalt Strike.[2]

Enterprise T1083 File and Directory Discovery

SUNBURST had commands to enumerate files and directories.[3][4]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

SUNBURST attempted to disable software security services following checks against a FNV-1a + XOR hashed hardcoded blocklist.[5]

Enterprise T1070 Indicator Removal

SUNBURST removed HTTP proxy registry values to clean up traces of execution.[2]

.004 File Deletion

SUNBURST had a command to delete files.[3][4]

.007 Clear Network Connection History and Configurations

SUNBURST also removed the firewall rules it created during execution.[2]

.009 Clear Persistence

SUNBURST removed IFEO registry values to clean up traces of persistence.[2]

Enterprise T1105 Ingress Tool Transfer

SUNBURST delivered different payloads, including TEARDROP in at least one instance.[3]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

SUNBURST created VBScripts that were named after existing services or folders to blend into legitimate activities.[2]

Enterprise T1112 Modify Registry

SUNBURST had commands that allow an attacker to write or delete registry keys, and was observed stopping services by setting their `HKLM\SYSTEM\CurrentControlSet\services\[service_name]\Start` registry entries to value 4.[3][4] It also deleted previously-created Image File Execution Options (IFEO) Debugger registry values and registry keys related to HTTP proxy to clean up traces of its activity.[2]

Enterprise T1027 Obfuscated Files or Information

SUNBURST obfuscated collected system information using a FNV-1a + XOR algorithm.[3]

.005 Indicator Removal from Tools

SUNBURST source code used generic variable names and pre-obfuscated strings, and was likely sanitized of developer comments before being added to SUNSPOT.[7]

.015 Compression

SUNBURST strings were compressed and encoded in Base64.[4]

Enterprise T1057 Process Discovery

SUNBURST collected a list of process names that were hashed using a FNV-1a + XOR algorithm to check against similarly-hashed hardcoded blocklists.[3]

Enterprise T1012 Query Registry

SUNBURST collected the registry value `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid` from compromised hosts.[3]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

SUNBURST checked for a variety of antivirus/endpoint detection agents prior to execution.[4][5]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

SUNBURST was digitally signed by SolarWinds from March - May 2020.[3]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

SUNBURST used Rundll32 to execute payloads.[2]

Enterprise T1082 System Information Discovery

SUNBURST collected hostname and OS version.[3][4]

Enterprise T1016 System Network Configuration Discovery

SUNBURST collected all network interface MAC addresses that are up and not loopback devices, as well as IP address, DHCP configuration, and domain information.[3]

Enterprise T1033 System Owner/User Discovery

SUNBURST collected the username from a compromised host.[3][4]

Enterprise T1007 System Service Discovery

SUNBURST collected a list of service names that were hashed using a FNV-1a + XOR algorithm to check against similarly-hashed hardcoded blocklists.[3]

Enterprise T1124 System Time Discovery

SUNBURST collected device `UPTIME`.[3][4]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

SUNBURST checked the domain name of the compromised host to verify it was running in a real environment.[4]

.003 Virtualization/Sandbox Evasion: Time Based Checks

SUNBURST remained dormant after initial access for a period of up to two weeks.[3]

Enterprise T1047 Windows Management Instrumentation

SUNBURST used the WMI query `Select * From Win32_SystemDriver` to retrieve a driver listing.[3]
