Lucifer, Software S0532 | MITRE ATT&CK®

Archived: 2026-04-05 14:27:32 UTC

Enterprise T1071 Application Layer Protocol

Lucifer can use the Stratum protocol on port 10001 for communication between the cryptojacking bot and the mining server.[1]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Lucifer can persist by setting Registry key values `HKLM\Software\Microsoft\Windows\CurrentVersion\Run\QQMusic` and `HKCU\Software\Microsoft\Windows\CurrentVersion\Run\QQMusic`.[1]

Enterprise T1110 .001 Brute Force: Password Guessing

Lucifer has attempted to brute force TCP ports 135 (RPC) and 1433 (MSSQL) with the default username or list of usernames and passwords.[1]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Lucifer can issue shell commands to download and execute additional payloads.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Lucifer can decrypt its C2 address upon execution.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Lucifer can perform a decremental-xor encryption on the initial C2 request before sending it over the wire.[1]

Enterprise T1210 Exploitation of Remote Services

Lucifer can exploit multiple vulnerabilities including EternalBlue (CVE-2017-0144) and EternalRomance (CVE-2017-0144).[1]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

Lucifer can clear and remove event logs.[1]

Enterprise T1105 Ingress Tool Transfer

Lucifer can download and execute a replica of itself using certutil.[1]

Enterprise T1570 Lateral Tool Transfer

Lucifer can use certutil for propagation on Windows hosts within intranets.[1]

Enterprise T1498 Network Denial of Service

Lucifer can execute TCP, UDP, and HTTP denial of service (DoS) attacks.[1]

Enterprise T1046 Network Service Discovery

Lucifer can scan for open ports including TCP ports 135 and 1433.[1]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

Lucifer has used UPX packed binaries.[1]

Enterprise T1057 Process Discovery

Lucifer can identify the process that owns remote connections.[1]

Enterprise T1012 Query Registry

Lucifer can check for existing stratum cryptomining information in `HKLM\Software\Microsoft\Windows\CurrentVersion\spreadCpuXmr - %stratum info%`.[1]

Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

Lucifer can infect victims by brute forcing SMB.[1]

Enterprise T1496 .001 Resource Hijacking: Compute Hijacking

Lucifer can use system resources to mine cryptocurrency, dropping XMRig to mine Monero.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Lucifer has established persistence by creating the following scheduled task `schtasks /create /sc minute /mo 1 /tn QQMusic ^ /tr C:Users\%USERPROFILE%\Downloads\spread.exe /F`.[1]

Enterprise T1082 System Information Discovery

Lucifer can collect the computer name, system architecture, default language, and processor frequency of a compromised host.[1]

Enterprise T1016 System Network Configuration Discovery

Lucifer can collect the IP address of a compromised host.[1]

Enterprise T1049 System Network Connections Discovery

Lucifer can identify the IP and port numbers for all remote connections from the compromised host.[1]

Enterprise T1033 System Owner/User Discovery

Lucifer has the ability to identify the username on a compromised host.[1]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

Lucifer can check for specific usernames, computer names, device drivers, DLL's, and virtual devices associated with sandboxed environments and can enter an infinite loop and stop itself if any are detected.[1]

Enterprise T1047 Windows Management Instrumentation

Lucifer can use WMI to log into remote machines for propagation.[1]
