# Nightdoor, Software S1147 | MITRE ATT&CK®

Archived: 2026-04-05 14:57:49 UTC

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1071 | | Application Layer Protocol | Nightdoor uses TCP and UDP communication for command and control traffic.[1][2] |
| Enterprise | T1059 | .003 | Command and Scripting Interpreter: Windows Command Shell | Nightdoor creates a cmd.exe shell to send and receive commands from the command and control server via open pipes.[2] |
| Enterprise | T1140 | | Deobfuscate/Decode Files or Information | Nightdoor stores network configuration data in a file XOR encoded with the key value of `0x7A`.[2] |
| Enterprise | T1574 | | Hijack Execution Flow | Nightdoor uses a legitimate executable to load a malicious DLL file for installation.[2] |
| Enterprise | T1070 | .004 | Indicator Removal: File Deletion | Nightdoor can self-delete.[1] |
| Enterprise | T1680 | | Local Storage Discovery | Nightdoor can collect information about disk drives, their total and free space, and file system type.[1] |
| Enterprise | T1057 | | Process Discovery | Nightdoor can collect information on installed applications via Windows registry keys, as well as collecting information on running processes.[1] |

| Domain | ID | | Name | Use |
|---|---|---|---|---|
| Enterprise | T1053 | .005 | Scheduled Task/Job: Scheduled Task | Nightdoor uses scheduled tasks for persistence to load the final malware payload into memory.[2] |
| Enterprise | T1082 | | System Information Discovery | Nightdoor gathers information on the victim system such as CPU and Computer name as well as device drivers.[1] |
| Enterprise | T1016 | | System Network Configuration Discovery | Nightdoor gathers information on victim system network configuration such as MAC addresses.[1] |
| Enterprise | T1033 | | System Owner/User Discovery | Nightdoor gathers information on victim system users and usernames.[1] |
| Enterprise | T1124 | | System Time Discovery | Nightdoor can identify the system local time information.[1] |
| Enterprise | T1497 | .001 | Virtualization/Sandbox Evasion: System Checks | Nightdoor embeds code from the public `al-khaser` project, a repository that works to detect virtual machines, sandboxes, and malware analysis environments.[2] |
| Enterprise | T1102 | | Web Service | Nightdoor can utilize Microsoft OneDrive or Google Drive for command and control purposes.[1][2] |

Source: https://attack.mitre.org/software/S1147