Turian, Software S0647 | MITRE ATT&CK®

Archived: 2026-04-05 17:58:18 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Turian has the ability to use HTTP for its C2.[1]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Turian can use WinRAR to create a password-protected archive for files of interest.[1]

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

Turian can establish persistence by adding Registry Run keys.[1]

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

Turian can create a remote shell and execute commands using cmd.[1]

.004 Command and Scripting Interpreter: Unix Shell

Turian has the ability to use `/bin/sh` to execute commands.[1]

.006 Command and Scripting Interpreter: Python

Turian has the ability to use Python to spawn a Unix shell.[1]

Enterprise T1001 .001 Data Obfuscation: Junk Data

Turian can insert pseudo-random characters into its network encryption setup.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

Turian can store copied files in a specific directory prior to exfiltration.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Turian has the ability to use a XOR decryption key to extract C2 server domains and IP addresses.[1]

Enterprise T1083 File and Directory Discovery

Turian can search for specific files and list directories.[1]

Enterprise T1105 Ingress Tool Transfer

Turian can download additional files and tools from its C2.[1]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Turian can disguise as a legitimate service to blend into normal operations.[1]

Enterprise T1027 Obfuscated Files or Information

Turian can use VMProtect for obfuscation.[1]

Enterprise T1120 Peripheral Device Discovery

Turian can scan for removable media to collect data.[1]

Enterprise T1113 Screen Capture

Turian has the ability to take screenshots.[1]

Enterprise T1082 System Information Discovery

Turian can retrieve system information including OS version, memory usage, local hostname, and system adapter information.[1]

Enterprise T1016 System Network Configuration Discovery

Turian can retrieve the internal IP address of a compromised host.[1]

Enterprise T1033 System Owner/User Discovery

Turian can retrieve usernames.[1]
