Triton, Software S1009 | MITRE ATT&CK®

Archived: 2026-04-05 15:47:25 UTC

ICS T0858 Change Operating Mode

Triton has the ability to halt or run a program through the TriStation protocol. TsHi.py contains instances of halt and run functions being executed. [8]

ICS T0885 Commonly Used Port

Triton uses TriStations default UDP port, 1502, to communicate with devices. [8]

ICS T0868 Detect Operating Mode

Triton contains a file named TS_cnames.py which contains default definitions for program state (TS_progstate). Program state is referenced in TsHi.py.[8]

Triton contains a file named TS_cnames.py which contains default definitions for key state (TS_keystate). Key state is referenced in TsHi.py.[8]

ICS T0871 Execution through API

Triton leverages a reconstructed TriStation protocol within its framework to trigger APIs related to program download, program allocation, and program changes. [7]

ICS T0820 Exploitation for Evasion

Triton disables a firmware RAM/ROM consistency check after injects a payload (imain.bin) into the firmware memory region. [3] [9] [4] Triconex systems include continuous means of detection including checksums for firmware and program integrity, memory and memory reference integrity, and configuration. [10]

ICS T0890 Exploitation for Privilege Escalation

Triton leverages a previously-unknown vulnerability affecting Tricon MP3008 firmware versions 10.010.4 allows an insecurely-written system call to be exploited to achieve an arbitrary 2-byte write primitive, which is then used to gain supervisor privileges. [3]

ICS T0874 Hooking

Triton's injector, inject.bin, changes the function pointer of the 'get main processor diagnostic data' TriStation command to the address of imain.bin so that it is executed prior to the normal handler. [7]

ICS T0872 Indicator Removal on Host

Triton would reset the controller to the previous state over TriStation and if this failed it would write a dummy program to memory in what was likely an attempt at anti-forensics. [7]

ICS T0880 Loss of Safety

Triton has the capability to reprogram the SIS logic to allow unsafe conditions to persist or reprogram the SIS to allow an unsafe state while using the DCS to create an unsafe state or hazard. [1]

ICS T0849 Masquerading

Triton's injector, inject.bin, masquerades as a standard compiled PowerPC program for the Tricon. [3]

Triton was configured to masquerade as trilog.exe, which is the Triconex software for analyzing SIS logs.[11]

ICS T0821 Modify Controller Tasking

Triton's argument-setting and inject.bin shellcode are added to the program table on the Tricon so that they are executed by the firmware once each cycle. [3] [7]

ICS T0834 Native API

Triton's imain.bin payload takes commands from the TsHi.ExplReadRam(Ex), TsHi.ExplWriteRam(Ex) and TsHi.ExplExec functions to perform operations on controller memory and registers using syscalls written in PowerPC shellcode. [7]

ICS T0843 Program Download

Triton leveraged the TriStation protocol to download programs onto Triconex Safety Instrumented System. [7]

ICS T0845 Program Upload

Triton calls the SafeAppendProgramMod to transfer its payloads to the Tricon. Part of this call includes preforming a program upload. [8]

ICS T0846 Remote System Discovery

Triton uses a Python script that is capable of detecting Triconex controllers on the network by sending a specific UDP broadcast packet over port 1502. [3]

ICS T0853 Scripting

Triton communicates with Triconex controllers using a custom component framework written entirely in Python. The modules that implement the TriStation communication protocol and other supporting components are found in a separate file -- library.zip -- the main script that employs this functionality is compiled into a standalone py2exe Windows executable -- trilog.exe which includes a Python environment. [3]

ICS T0869 Standard Application Layer Protocol

Triton can communicate with the implant utilizing the TriStation 'get main processor diagnostic data' command and looks for a specifically crafted packet body from which it extracts a command value and its arguments. [7]

ICS T0857 System Firmware

Triton is able to read, write and execute code in memory on the safety controller at an arbitrary address within the devices firmware region. This allows the malware to make changes to the running firmware in memory and modify how the device operates. [3]
