PLC-Blaster, Software S1006 | MITRE ATT&CK®

Archived: 2026-04-05 16:41:27 UTC

Domain	ID	Name	Use
ICS	T0858	Change Operating Mode	PLC-Blaster stops the execution of the user program on the target to enable the transfer of its own code. The worm then copies itself to the target and subsequently starts the target PLC again. [1]
ICS	T0814	Denial of Service	The execution on the PLC can be stopped by violating the cycle time limit. The PLC-Blaster implements an endless loop triggering an error condition within the PLC with the impact of a DoS. [1]
ICS	T0835	Manipulate I/O Image	PLC-Blaster may manipulate any outputs of the PLC. Using the POU POKE any value within the process image may be modified. [1]
ICS	T0821	Modify Controller Tasking	PLC-Blaster's code is stored in OB9999. The original code on the target is untouched. The OB is automatically detected by the PLC and executed. [1]
ICS	T0889	Modify Program	PLC-Blaster copies itself to various Program Organization Units (POU) on the target device. The POUs include the Data Block, Function, and Function Block. [1]
ICS	T0834	Native API	PLC-Blaster uses the system function blocks TCON and TDISCON to initiate and destroy TCP connections to arbitrary systems. Buffers may be sent and received on these connections with TRCV und TSEND system function blocks. [1]
ICS	T0843	Program Download	PLC-Blaster utilizes the PLC communication and management API to load executable Program Organization Units. [1]

Domain	ID	Name	Use
ICS	T0846	Remote System Discovery	PLC-Blaster scans the network to find other Siemens S7 PLC devices to infect. It locates these devices by checking for a service listening on TCP port 102. [1]

Source: https://attack.mitre.org/software/S1006