Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:05:22 UTC

Tool: Triton

Names	Triton TRITON Trisis TRISIS HatMan
Category	Malware
Type	ICS malware, Reconnaissance, Backdoor, Downloader, Info stealer, Remote command
Description	(FireEye) The TRITON attack tool was built with a number of features, including the ability to read and write programs, read and write individual functions and query the state of the SIS controller. However, only some of these capabilities were leveraged in the trilog.exe sample (e.g. the attacker did not leverage all of TRITON's extensive reconnaissance capabilities). The TRITON malware contained the capability to communicate with Triconex SIS controllers (e.g. send specific commands such as halt or read its memory content) and remotely reprogram them with an attacker-defined payload. The TRITON sample Mandiant analyzed added an attacker-provided program to the execution table of the Triconex controller. This sample left legitimate programs in place, expecting the controller to continue operating without a fault or exception. If the controller failed, TRITON would attempt to return it to a running state. If the controller did not recover within a defined time window, this sample would overwrite the malicious program with invalid data to cover its tracks.
Information	<https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html> <https://www.midnightbluelabs.com/blog/2018/1/16/analyzing-the-triton-industrial-malware> <https://dragos.com/blog/trisis/TRISIS-01.pdf> <https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf> <https://github.com/ICSrepo/TRISIS-TRITON-HATMAN>

	<https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html> <https://blogs.cisco.com/security/how-does-triton-attack-triconex-industrial-safety-systems>
MITRE ATT&CK	<https://attack.mitre.org/software/S0609/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.triton>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Triton

Changed	Name	Country	Observed	
APT groups				
	TEMP.Veles		2014-Mar 2022	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e331cfc5-45c9-4a74-a79f-dac9c622e39f