Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:31:37 UTC

APT group: TEMP.Veles

Names	TEMP.Veles *(FireEye)* Xenotime *(Dragos)* ATK 91 *(Thales)* G0088 *(MITRE)*	
Country	Russia	
Sponsor	State-sponsored, Central Scientific Research Institute of Chemistry and Mechanics	
Motivation	Sabotage and destruction	
First seen	2014	
Description	TEMP.Veles is a Russia-based threat group that has targeted critical infrastructure. The group has been observed utilizing TRITON, a malware framework designed to manipulate industrial safety systems.	
Observed	Sectors: Critical infrastructure, Energy, Manufacturing, Oil and gas. Countries: Saudi Arabia, USA and others.	
Tools used	Cryptcat, Mimikatz, NetExec, PsExec, SecHack, Triton, Wii.	
Operations performed	2014	TRISIS malware <https://dragos.com/resource/trisis-analyzing-safety-system-targeting-malware/>
	2017	TRITON malware <https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html> <https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html>
	Feb 2019	The most dangerous threat to ICS has new targets in its sights. Dragos identified the Xenotime activity group expanded its targeting beyond oil and gas to the electric utility sector. This expansion to a new vertical illustrates a trend that will likely continue for other ICS-targeting adversaries. <https://dragos.com/blog/industry-news/threat-proliferation-in-ics-

		cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/>
Counter operations	Oct 2020	US Treasury sanctions Russian research institute behind Triton malware <https://www.zdnet.com/article/us-treasury-sanctions-russian-research-institute-behind-triton-malware/>
	Mar 2022	DOJ unseals indictments of four Russian gov't officials for cyberattacks on energy companies <https://therecord.media/doj-unseals-indictments-of-four-russian-govt-officials-for-cyberattacks-on-energy-companies/>
Information	<https://dragos.com/resource/xenotime/> <https://www.fireeye.com/blog/threat-research/2019/04/triton-actor-ttp-profile-custom-attack-tools-detections.html> <https://ics-cert.us-cert.gov/sites/default/files/documents/MAR-17-352-01%20HatMan%E2%80%94Safety%20System%20Targeted%20Malware_S508C.pdf> <https://www.cisa.gov/uscert/ncas/alerts/aa22-083a>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0088/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=ea108a02-eb3a-4e08-be7b-bd164fc5c220