# Xenotime Threat Group | Dragos

By September 4, 2025 11:25 AM

Archived: 2026-04-05 14:18:08 UTC

XENOTIME is easily the most dangerous threat activity publicly known. It is the only activity group intentionally compromising and disrupting industrial safety instrumented systems, which can lead to scenarios involving loss of life and environmental damage.

Dragos identified several compromises of ICS vendors and manufacturers in 2018 by activity associated with XENOTIME, providing potential supply chain threat opportunities and vendor-enabled access to asset owner and operator ICS networks.

XENOTIME rose to prominence in December 2017 when Dragos and FireEye jointly published details of TRISIS (also known as TRITON, the focus of the MITRE Engenuity ATT&CK® Evaluations for ICS) destructive malware targeting Schneider Electric's Triconex safety instrumented system. The multi-step malware framework caused industrial systems in a Middle Eastern industrial facility to shut down. The incident represented a shift in the capabilities and consequences of ICS malware.

TRISIS was an escalation of the type of attacks historically targeting ICS systems. Targeting a safety system indicates significant damage and loss of human life were either intentional or acceptable goals of the attack, a consequence not seen in previous disruptive attacks such as the 2016 CRASHOVERRIDE malware that caused a power loss in Ukraine.

Note: Industrial safety instrumented systems comprise part of a multi-layer engineered process control framework to protect life and environment. Industrial safety systems are highly redundant and separate controls which override and manage industrial processes if they approach unsafe conditions such as over-pressurization, overspeed, or over-heating. They enable engineers and operators to safely control and possibly shutdown processes before a major incident occurs. They're a critical component of many dangerous industrial environments such as electric power generation and oil and gas processing.

XENOTIME configured TRISIS based on the specifics and functions of the Triconex system within the industrial control (ICS) environment. XENOTIME used credential capture and replay to move between networks, Windows commands, standard command-line tools such as PSExec, and proprietary tools for operations on victim hosts. (Full reports detailing XENOTIME's tool techniques, and procedures are available to Dragos WorldView customers.)

Because the TRISIS malware framework was highly tailored, it would have required specific knowledge of the Triconex's infrastructure and processes within a specific plant. This means it's not easy to scale—however, the malware provides a blueprint of how to target safety instrumented systems. This tradecraft is thus scalable and available to others even if the malware itself changes. Dragos' data indicates XENOTIME remains active. Furthermore, Dragos' analysis of the TRISIS event continues as we recover additional data surrounding the incident.

Dragos assesses with moderate confidence that XENOTIME intends to establish required access and capability to cause a potential, future disruptive—or event. Compromising safety systems provides little value outside of disrupting operations. The group created a custom malware framework and tailormade credential gathering tools, but an apparent misconfiguration prevented the attack from executing properly. As XENOTIME matures, it is less likely that the group will make this mistake in the future.

XENOTIME operates globally, impacting regions far outside of the Middle East, their initial target. Intelligence suggests the group has been active since at least 2014 and is presently operating in multiple facilities targeting safety systems beyond Triconex. This group has no known associations to other activity groups.

---