# Mysterious safety-tampering malware infects a second critical infrastructure site

Enlarge / Critical infrastructure sites such as this oil refinery in Port Arthur, Texas, rely on safety systems.

## reader comments

8 with 8 posters participating, including story author

## Share this story

Sixteen months ago, researchers reported an unsettling escalation in hacks targeting power plants, gas refineries, and other types of critical infrastructure. Attackers who may have been working on behalf of a nation caused an operational outage at a critical-infrastructure site after deliberately targeting a system that prevented health- and life-threatening accidents.

There had been compromises of critical infrastructure sites before. What was unprecedented in this attack—and of considerable concern to some researchers and critical infrastructure operators—was the use of an advanced piece of malware that targeted the unidentified site's safety processes. Such safety instrumented systems (SIS) are a combination of hardware and software that many critical infrastructure sites use to prevent unsafe conditions from arising. When gas fuel pressures or reactor temperatures rise to potentially unsafe thresholds, for instance, a SIS will automatically close valves or initiate cooling processes to prevent health- or life-threatening accidents. By focusing on

the site’s SIS, the malware carried the threat of physical destruction that depending on the site and the type of accident had the potential to be serious if not catastrophic. The malware was alternately named Triton and Trisis, because it targeted the Triconex product line made by Schneider Electric. It’s development was ultimately linked to a Russian government-backed research institute.

## Not an isolated incident

Now, researchers at FireEye—the same security firm that discovered Triton and its ties to Russia—say they have uncovered an additional intrusion that used the same malicious software framework against a different critical infrastructure site. As was the case in the first intrusion, the attackers focused most of their resources on the facility’s OT, or operational technology, which are systems for monitoring and managing physical processes and devices.

“After establishing an initial foothold on the corporate network, the Triton actor focused most of their effort on gaining access to the OT network,” FireEye researchers wrote in a report published Wednesday. “They did not exhibit activities commonly associated with espionage, such as using key loggers and screenshot grabbers, browsing files, and/or exfiltrating large amounts of information. Most of the attack tools they used were focused on network reconnaissance, lateral movement, and maintaining presence in the target environment.”

Once the attackers in the new attack gained access to the site’s SIS controllers, they appeared to focus solely on maintaining this control. This focus involved strategically limiting other activities to lessen the chances of being discovered.

The discovery has unearthed a new set of never-before-seen custom tools that shows the attackers have been operational

since as early as 2014. The existence of these tools, and the attacker's demonstrated interest in operational security, lead FireEye researchers to believe there may be others sites beyond the two already known where the Triton attackers were or still are present.

In an email, John Hultquist, FireEye's director of cyber-espionage analysis, wrote:

> *We now know the first incident wasn't isolated. There are others. That is especially disconcerting given the danger associated with this threat, which we still know very little about. Though we've traced this back to the Russian institute we're at a loss for explaining the motive here or whether even this is tied to some other country who might be contracting out with the institute.*
>
> *We are releasing the tools and other information on this actor in the hopes that others will find them and we will all get a better handle on this emerging and disconcerting threat actor. We understand there's some risk that the actor may go to ground. That may have already happened. After we released the blog on attribution in this case, the institute took operational security measures. They took down some of the information on their website and changed their WHOIS.*
>
> *Hopefully, this is a first step in a global hunt for this actor that leads to some answers.*

Wednesday's report omits key details about the additional intrusion. It makes no mention, for example, when the attack occurred, how long it lasted, if it resulted in any unsafe conditions, and whether the malware targeted the same Triconex system as before. A FireEye spokeswoman declined to answer those questions.

The report does include a wealth of technical details about the newly discovered tool set and ways the attackers used them

to remain hidden inside the infected network. The report also contain indicators of compromise that help identify intrusions. FireEye is urging researchers and network defenders to see if the data matches previously seen attacks.

https://arstechnica.com/?p=1488751