Trisis masterminds have expanded operations to target U.S. industrial firms

By Chris Bing

Published: 2018-05-24 · Archived: 2026-04-05 21:10:14 UTC

A group known for infecting a Saudi petrochemical plant with highly sophisticated industrial control malware has expanded its operations, according to new research, with a former U.S. official telling CyberScoop that companies inside the United States have been breached.

The group behind the malware, which ICS-focused cybersecurity startup Dragos refers to as "Xenotime," has expanded its operations to include attacks on multiple U.S. companies. The malware shows similarities to what's commonly known as Trisis, which was used in an attack last year in Saudi Arabia. While Trisis exploited one particular industrial control system, researchers say a new variant impacts a variety of safety instrumented systems.

The former U.S. official spoke on condition of anonymity to discuss a sensitive, private security alert shared inside government.

Safety instrumented systems, or SIS for short, are hardware and software controls that protect large-scale industrial processes and equipment typically found in nuclear, petrochemical or manufacturing plants. There are few companies who create and manage SIS systems, including but not limited to St. Louis-based Emerson, New Jersey-based Honeywell, and Tokyo-based Yokogawa.

Dragos has declined to name any of the newly affected systems or targeted industrial companies, although a former U.S. official with knowledge of the situation told CyberScoop those impacted operate in the Middle East and United States.

The company has turned over relevant information to the federal government and been in contact with the targeted companies.

It's unclear how Xenotime is able to successfully manufacture and maintain such sophisticated malware.
The Dragos report is largely absent of technical indicators, doesn't state how many new cases exist, where they occurred or how the activity differs from the Saudi Arabia incident.

What is apparent, however, is that a dangerous and imminent threat looms over critical infrastructure providers inside the U.S., said Sergio Caltagirone, Dragos's director of threat intelligence and analytics.

"The reason we put this out there, even though we can't say much, is to let people really know that this threat exists," Caltagirone told CyberScoop. "People need to start thinking about auditing their safety systems. This is a much bigger problem than what we maybe all first thought it was."

Caltagirone said in some of these recent incidents, Xenotime was able to successfully breach the organization's IT systems and move into safety instrumented systems. Another system hop and hackers could have reached actual control processes and caused significant, life-threatening damage.

According to Caltagirone, Xenotime is using phishing emails and so-called "watering hole" websites to hack engineers working at industrial companies. The specific lures are designed to grab the attention of engineers in order to breach their accounts and steal administrative credentials.

After compromising engineers, Xenotime will usually remain hidden for weeks or months, traversing the breached company looking for soft barriers between the IT and operational technology (OT) network.

It's not uncommon for hackers to initially attack an industrial company's IT system in order to gain a foothold for future attacks that are aimed at vital safety systems.

In the Saudi Arabia incident, hackers exploited software vulnerabilities in French energy technology developer Schneider Electric's SIS system in an attempt to cause heavy physical damage. However, a misconfiguration in the malware triggered the safety system, stopping the attack before it could be fully completed. The attack still disrupted operations for several days.

When Trisis first appeared, researchers told CyberScoop the malware was an engineering feat. Months of careful and meticulous research went into understanding how Schneider's system works and what Trisis did to send it into a shutdown mode.

Trisis has yet to be publicly attributed to a known set of actors. The original infection vector for Trisis has never been disclosed. Code overlaps do exist between Xenotime and other advanced persistent threat groups, said Caltagirone. Some of Xenotime's tools date back to 2014.

Over the last year, there have been a few publicly visible incidents focused on the U.S. energy sector. For example, in April, Dallas-based pipeline company Energy Transfer Partners saw a third-party transaction system hit by an attack.

Caltagirone declined to comment on whether any publicly known disruption in the sector is related to Xenotime activity.

The Department of Homeland Security did not respond to a request for comment.

UPDATE, 11:55 a.m. EDT: *Portions of this story have been corrected to reflect that CyberScoop learned of Xenotime's target locations through a former U.S. government official and not through Dragos' public report.*
