Written by Chris Bing
Jan 16, 2018 | CYBERSCOOP

At first, technicians at multinational energy giant Schneider Electric thought they were looking at the everyday software used to manage equipment inside nuclear and petroleum plants around the world. They had no idea that the code carried the most dangerous industrial malware on the planet.

More than four months have passed since a novel, highly sophisticated piece of malware forced an important oil and gas facility in the Middle East to suddenly shut down, but cybersecurity analysts still don't know who wrote the code.

Since last August, multiple teams of researchers in the public and private sectors have been examining what the perpetrators planted inside a nondescript Saudi computer network. It's a rare case involving a computer virus specially engineered to sabotage industrial control systems (ICS) — the gear that keeps factories and refineries running. Manipulating these systems can have a destructive impact far beyond the network.

Today, the incident's magnitude and implications are becoming increasingly clear to the victim, to several foreign governments and to the private sector teams that led incident response. What they all found has been described to CyberScoop as the "next generation of cyberweaponry" — a tool so dangerous that its mere existence significantly intensifies the global digital arms race.

Clues unearthed from September to December suggest that an intricate but slightly misconfigured cyberattack caused the mysterious shutdown. The affected company and the teams investigating the incident still have not publicly revealed where it occurred.

One thing is clear about the code: Dubbed "Triton" or "Trisis," the multi-stage malware framework is unlike anything the security research community has ever seen. It is considered to be just the fifth known variant of ICS-tailored malware. The most recent was "CrashOverride" in Ukraine in 2016, and perhaps the most famous was "Stuxnet" in Iran in 2010.

"Trisis' impact is simple. It is the first piece of malware which can be used remotely to put civilian infrastructure into an unsafe state," explained Sergio Caltagirone, director of threat intelligence with Maryland-based cybersecurity startup Dragos Inc. "When things like this happen, plants get shut down, people can get hurt."

Not only has the case stumped some of the most talented people in cybersecurity forensics, but it also has highlighted the complications and conflicts inherent in investigations that are extremely important to governments but are ultimately controlled by private companies.

While the story behind Trisis is still unfolding — experts on multiple continents are still poring over the malware — CyberScoop has learned more details about what occurred in the last half of 2017. The following account is based on multiple conversations with seven sources with knowledge of the investigation into Trisis. All sources who spoke on the condition of anonymity did so in order to freely discuss sensitive information.

The First Forensics

In late August, employees of an oil and gas plant located in Saudi Arabia quickly noticed when some of its industrial equipment randomly shut down during regular business hours. The quirks eventually forced the entire facility to halt operations, causing immediate financial losses.

The affected company began to inspect workstations connected to some of the faulty industrial equipment. Before long, technicians found an odd computer file named "trilog.exe." It appeared to come from Schneider Electric, which served as a technology supplier for the facility.

engineers to inspect computers in late August. While Aramco was not responsible for the facility's day-to-day operations, the corporation has a stake in the victim's business. Having dealt with the massively destructive Shamoon attack five years prior, Aramco understood the suspicious file would require a thorough inspection.

Sources who spoke with CyberScoop described general details about the victim organization, including its relationship to Aramco, but all declined to provide a company name.

It wasn't long before specialists with Schneider Electric and Aramco realized there was much more to trilog.exe than what met the eye.

Though the file's components appeared at first glance to mimic elements of legitimate Schneider Electric software, further scrutiny indicated that someone from outside the company created the program. Trilog.exe, along with an attached, partner file named Library.zip, carried devastating malware.

Trisis' existence became truly public for the first time on Aug. 29, when components of the code were uploaded to the malware repository VirusTotal by a Saudi Aramco employee, sources told CyberScoop. That post went unnoticed for weeks, though, by outside observers.

In early September, the victim called on Mandiant, a division of U.S. cybersecurity firm FireEye, to provide support. FireEye — which is largely comprised of former U.S. defense, intelligence and law enforcement officials — is one of few U.S. cybersecurity brands to boast a considerable presence in the Middle East, where it operates out of a headquarters in Dubai. FireEye helped in 2012 when the Shamoon attack took 30,000 of Aramco's computers offline and crippled its operations.

This time, Mandiant discovered an even more dangerous cyberweapon, likely developed by a group of government-backed hackers.

Mandiant's researchers would discover that the initial Trisis attack actually had misfired: The plant's unresponsive machines had automatically shut down, entering a fail-safe mode after detecting an anomaly. The attackers had made a configuration mistake.

"The safety systems worked as they were intended to," one source familiar with the early investigation told CyberScoop.

Researchers believe the attackers wanted to use Trisis to cause physical damage, but instead it simply caused the machines to turn off. The jump to a fail-safe mode may have averted catastrophe, as the freeze limited the malware's true potential.

Exactly how Trisis arrived on the affected company's network remains an open-ended question. FireEye is aware of what the initial infection vector was — whether, for example, a phishing email or weaponized USB stick is to blame — but has not disclosed those details publicly.

The incident response effort by Mandiant during this investigation included help from analysts spread across two continents, from Alexandria, Virginia, and Dubai to Saudi Arabia.

Stuxnet's Sibling?

Experts say Trisis is able to force a malfunction in the Triconex Safety Instrumented System (SIS), a popular logic controller made by Schneider Electric. These controllers are primarily used to manage physical equipment in nuclear power plants, oil and gas production facilities and paper mills.

One source with knowledge of the investigation described how SIS technology functions after it is infected with Trisis. Physical destruction and loss of life aren't out of the question.

"What these controllers basically do is … let's say you have a turbine or something spinning that's usually supposed to run at about 500 rpm. The controller kind of acts like a safety feature because it will slow down the turbine before redlining at a certain level, say, if it gets up to 700 or 800 rpm, then the controller will react," the source said. "[Trisis] could remotely shutdown a system completely or you could change this redline 'level' so that the equipment would become increasingly unstable until it finally breaks. If equipment breaks, that can mean loss of life."

The way Trisis works echoes Stuxnet, which American spies used to affect the speed of centrifuges as they spun filled with uranium, causing them to eventually break. Some historians consider the Stuxnet operation to have been a success because it derailed Iran's efforts to develop nuclear weapons for some time.

Like Stuxnet, Trisis has the ability to manipulate the expected rotation speed of components as they spin inside a machine.

boobytrap legitimate software downloads; "Blackenergy2," which was used in an elaborate hacking scheme that knocked out Ukraine's electric grid in December 2015; and Crashoverride, which also was used to target multiple Ukrainian power plants companies one year later in December 2016.

"Only three have caused disruptions or destruction to industrial environments and only two have been targeted towards civilian industrial infrastructure," described Robert Lee, CEO and founder of Dragos Inc.

But he and other insiders say Trisis is in a class of its own.

"Trisis is the first ever to specifically target safety instrumented systems and it is the one that gives me the most concern," said Lee, a former Air Force cyberwarfare operator. "CrashOverride was an alarming event for power grid operators and should be taken very seriously, but Trisis specifically targeted a system that is designed to protect human life. To me that is outrageous and infuriating. I expect this will be a watershed moment for the engineering community."

An awkward race for answers

While Mandiant was investigating, analysts with Dragos became aware of Trisis by spotting the aforementioned file on VirusTotal. After diving in, they reached out to the Department of Homeland Security with a warning about the malware's dangerous capabilities. Yet, the initial report shared with the government was far from comprehensive.

Unbeknownst to Dragos, Schneider had also been in contact with DHS, providing the agency with insight into the malware. Once DHS saw the evidence, officials connected Schneider with the Fulton, Maryland-based startup in order to gain a more complete picture of the case — which allowed for further analysis and a private warning to partners.

"We are not able to talk specifics about any of our relationships, but after contacting DHS, Schneider Electric reached out and contacted us," Dragos' Lee said. "When we became aware that Trisis was likely removing safety logic from the controller instead of simply crashing the system, we became increasingly concerned about the situation given the potential for loss-of-life scenarios. We notified the [U.S. government] through the DHS and provided our analysis to them."

Schneider Electric and Dragos' outreach to the government marked an important chapter in the storyline.

The two notices helped update the U.S. government on what transpired without having to badger the victim — a foreign company — for all available evidence. Additionally, they allowed DHS to back off calls for information from Mandiant, which was constrained from speaking about the case due to a nondisclosure agreement with the victim.

"It would not be unusual for DHS or any other research organization to reach out to multiple entities to try to obtain a malware sample," said Marty Edwards, a former director for DHS's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). "This could be an IR [incident response] company, integrator or even the vendor of the equipment that was impacted."

Typically, DHS will relay information about pertinent cyberattacks to U.S. critical infrastructure companies and other partners through ICS-CERT. The National Cybersecurity and Communications Integration Center (NCCIC) is tasked with collecting and analyzing this data before it's sent out.

A DHS spokesperson confirmed the agency had obtained Trisis samples but declined to say how or when this data was acquired.

"Information sharing is a key part of the Department of Homeland Security's important mission to create shared situational awareness of malicious cyber activity," said DHS spokesperson Scott McConnell. "The National Cybersecurity and Communications Integration Center [NCCIC] leverages in-house subject matter expertise as well as strong relationships with researchers and industry to achieve its goal."

During this time frame, the U.S. government was playing catchup, hoping to collect new information but stymied by a lack of information sharing. Prior to reports from private industry, the U.S. government was given notice of the August incident through a intelligence-sharing partnership with the Saudi government. According to one current U.S. official, the Saudi government learned of the incident through Aramco around early September. The Saudis then notified their U.S. counterparts, but passed along little detail due to their own lack of concrete knowledge about what had transpired.

For U.S. officials, the desire to be informed came from an understanding that Trisis could be potentially dangerous to U.S. critical infrastructure. The Triconex SIS product is deployed across the U.S. in thousands of industrial plants.

"Most people don't see ICS-CERT as this global, independent body for good, you know," a former U.S. official described. "What you need to understand is that in other parts of the world, [ICS-CERT] is understood as 'the Americans' ... and not everyone wants to share their embarrassing secrets with the U.S. government."

In late November, FireEye eventually provided sparse details about Trisis to DHS ahead of publishing a blog post about the malware on Dec. 14. Dragos published its own limited research the same day.

"While we can't comment on the details of the investigation, we continue to study [Trisis] to improve our technical understanding and derive intelligence value," said Dan Scali, a senior manager for Mandiant's ICS security consulting practice. "We coordinated with the vendor and USG prior to publishing our blog post. We have shared our detections with the industry to help asset owners improve defenses."

On Dec. 18, NCCIC issued a Malware Analysis Report about Trisis, presenting a "worst case scenario" about the virus' capabilities, intended for industrial control system operators. NCCIC is currently in the process of conducting additional analysis.

An alarming enigma

Sources with access to Trisis samples say the malware is immensely difficult to analyze. The complete file library was built with five different coding languages, and can only be fully understood if it's tested on the same industrial equipment that it was designed to specifically target.

Even inside the National Security Agency — where the government's very best cybersecurity analysts are tasked with collecting foreign intelligence and defending the Pentagon from cyberattacks — Trisis has stumped analysts, sources say.

The Office of the Director of National Intelligence (ODNI) and NSA declined to comment for this story.

"The reports that have been published so far are all accurate and based on analysis of the malware, but this is not a simple capability to truly deep dive on," said Lee. "It requires buying the physical Triconex system and leveraging against it to understand exactly what is occurring. There may not be new revelations but adding nuance to the specifics that we already know can help better enable the security community."

One source estimated that it would take upwards of a year for a professional malware development team to engineer something on par with Trisis. The same source said Trisis was once likely worth "millions of dollars" because of all the intricately designed features included in its code.

"When you really look at [Trisis], you realize just how much research, development and testing must have gone into this thing," said the source. 'The fact that everyone knows about [Trisis] must be maddening for its creator … they totally got burned … It's worth so much less now."

Technical indicators hidden within Trisis' computer code show that it was in development since at least June 2016. The malware was then reassembled for an attack on Aug. 15, based on a private technical report provided to CyberScoop.

Though progress has been slow, FireEye and Dragos analysts are still analyzing the malware. Additionally, sources say that DHS and NSA also continue to study it.

A mystery unsolved

Although FireEye and Dragos pinned Trisis on a nation-state, further analysis has provided little conclusive evidence for either company to be precise in its attribution. A variety of different coding indicators within Trisis have never been seen before or used by any known hacking group, leaving analysts without a roadmap.

Within the U.S. government, teams of contractors and intelligence officials familiar with the matter spent November debating whether a nation-state was alone responsible for Trisis, or the malware was possibly a collaborative effort where one country created it and then handed it off to another government. In this scenario, insiders theorized a partnership between Russia and Iran.

However, these internal assessments were based on flimsy evidence and categorized as "low-confidence."

"We all left the room frustrated without a good answer," said one source familiar with the conversations. "That just goes to show you how difficult this is to understand."

Four days after the initial FireEye blog post about Trisis, Foreign Policy reported that Saudi Aramco was infected with Trisis, with the article pointing a guarded finger at attackers backed by Iran. Multiple sources familiar with Trisis criticized the conclusion reached in the article.

sources said.

The seemingly insurmountable challenge of accurately attributing Trisis underscores one of the harsh but quiet truths understood in Washington: The U.S. government's current attribution capabilities lag far behind where they need to be. This reality has only become more obvious with the Trisis case. It's an incident where everyone is deeply committed to finding an answer, but no one has been able to provide one.

An Aramco spokesperson provided CyberScoop with a carefully worded statement about Foreign Policy's story and the incident itself: "Saudi Aramco corporate and plants networks were not part of any cyber security attack or breach."

An Aramco spokesperson did not respond to additional questions concerning a Trisis infection at a partner organization.

-In this Story-

analysis, BlackEnergy, breach, CrashOverride, Department of Homeland Security, DHS, Dragos, energy sector, FireEye, hacker, Havex, ICS, ICS-CERT, malware, Mandiant, NCCIC, NSA, ODNI, research, Saudi Arabia, SCADA, Schneider Electric, Stuxnet, Trisis, Triton

RELATED NEWS

GOVERNMENT

DOJ unseals charges...

by **Sean Lyngaas** • 2 days ago