The inside story of the world’s most dangerous malware

By Blake Sobczak

Published: 2019-03-07 · Archived: 2026-04-05 21:29:01 UTC

On Aug. 4, 2017, at 7:43 p.m., two emergency shutdown systems sprang into action as darkness settled over the sprawling refinery along Saudi Arabia’s Red Sea coast.

The systems brought part of the Petro Rabigh complex offline in a last-gasp effort to prevent a gas release and deadly explosion. But as safety devices took extraordinary steps, control room engineers working the weekend shift spotted nothing out of the ordinary, either on their computer screens or out on the plant floor.

The reasons for the sudden shutdown were still buried under zeros and ones, nestled deep within the code of the compromised Schneider Electric safety equipment.

Investigators soon discovered a dangerous hacking tool that would usher in a new chapter in the global cyber arms race, much like the Stuxnet worm that damaged Iranian nuclear centrifuges at the start of the decade. The discovery of the Triton malware, named for the Triconex line of safety systems it triggered, echoed from the ancient Saudi city of Rabigh to a research institute in Moscow, and from California to Tokyo.

"Worst-case scenario here, you’re dealing with a potential release of toxic hydrogen sulfide gases, a potential for explosions from high pressure, high temperature," said Julian Gutmanis, a cybersecurity contractor who sources say led the Saudi Arabian Oil Co.’s investigation of the Triton intrusion.

"We considered the entire organization to be compromised," Gutmanis said at the S4 cybersecurity conference in Miami earlier this year, where he declined to name the target facility or even identify his employer. "We had a very sophisticated attacker. We knew that the systems, and the integrity of these systems, can no longer be trusted."

Experts say the same hackers behind the Saudi intrusion are probing U.S. petrochemical plants and refineries, positioning themselves for dangerous, even deadly, future strikes. Earlier this year, top U.S. intelligence officials warned that multiple hacking groups, backed by foreign spy agencies, are poised to disrupt American electricity and pipeline networks in the event of war with the United States.

The intrusion in Saudi Arabia stands as the most brazen use of the Triton tool to hijack safety systems and to clear the way for what could have been a lethal attack on a vast industrial complex. If taken to its extreme, the prospect of losing control of a major industrial plant echoes the 2005 BP PLC refinery explosion in Texas City, Texas, which killed 15 people.

At Petro Rabigh, access to digital safety backstops signaled to investigators that a team of hackers had also breached the control system. They could seize the rest of the plant, and the outcome turned on the hackers’ restraint.

Today, the Triton cyber espionage case is still shrouded in secrecy. Some of what's known is buried in the notes of private cybersecurity firms that swooped in to investigate. And its lethal potential is talked about in U.S. security circles and across the energy industry.

The story is told here in previously unreported detail, based on open-source intelligence, non-public documents obtained by E&E News and extensive interviews. Many of the sources would speak only on the condition of anonymity because of the sensitive nature of investigations into an active cyber espionage group.

The poster child

Aerial view of the Petro Rabigh petrochemical and refinery complex. | Sumitomo Chemical Co., Ltd.

Petro Rabigh is a 3,000-acre maze of steel pipes, hulking distillation towers and catalytic reformers, their distinctive, red-and-white caps poking up like toxic candy canes. It is one of the biggest facilities of its kind in the world.

The integrated chemical and refining complex produces more than 5 million tons of petrochemicals a year, from antifreeze to common plastics like polypropylene. It also churns out millions of barrels of refined products annually, including kerosene and gasoline. Situated along the Red Sea, Petro Rabigh has emerged as a major supplier to African, Asian and European markets. The company was launched as a joint venture between the Saudi Arabian Oil Co., the world's biggest oil company — known as Saudi Aramco — and Tokyo-based Sumitomo Chemical.

The facility stands as a poster child for Schneider Electric, one of the world's top suppliers of industrial control equipment. The French company won an operations management contract with Petro Rabigh as it expanded in the late 2000s.

In June 2017, on a Saturday during the Islamic holy month of Ramadan, Schneider Electric product specialists were called in to assess an apparently malfunctioning Triconex unit. The safety device had tripped part of Petro Rabigh offline, but it wasn't clear why. Everything seemed to be working normally.

Triconex equipment is designed to act, not to warn, like a home circuit breaker that trips automatically when outlets are dangerously overloaded. Triconex devices come loaded with a digital road map that allows them to constantly scan for unsafe conditions. If enough devices agree something's wrong, they won't wait for a human go-ahead. They'll simply grind industrial processes to a halt.

Schneider Electric specialists responded quickly to Petro Rabigh's request to investigate. They ran tests on-site and pulled the glitchy shutdown controller back to the lab for more analysis.

They found nothing terribly unusual in June. The plant restarted, and things stayed quiet until August — on the surface.

The Saudis' 'brief outage'

Analysts consider Schneider Electric's response in June a missed opportunity to identify the hackers before the August outage.

Engineers cast a wider net after the more dramatic August event. They found unusual communications beaconing out from the plant's information technology network to its operational workstations, areas normally kept isolated from one another.

Petro Rabigh called in a Saudi Aramco team to investigate, including Gutmanis, a soft-spoken Australian cybersecurity ace. Though Saudi Aramco wasn't responsible for the plant's security, the company's 37.5 percent stake in Petro Rabigh, combined with close management ties, cleared the way for a rapid response. By this point, the plant had entered a "state of panic," as Gutmanis recounted. No one could rule out the possibility that the shutdown was the work of a malicious insider.

Soon, Gutmanis and his responders unearthed the bundle of files that would later be called Triton. The plant was riddled with other malware, too. Nobody knew where it all came from.

A poorly configured firewall gave remote attackers a foothold inside corporate computers, where they were able to pivot to operational technology, the OT networks that housed Schneider Electric's safety systems.

The insider threat theory looked less and less likely. Now, new fears emerged: Could the intruders have left digital time bombs, armed and ready to go off as soon as the hackers lost their connection? Would they try to battle Petro Rabigh's digital defenders, as engineers there tried to cure the infected systems and bring the plant online again?

The plant stayed down for more than a week. While hardly an existential threat to a company that sells more than $9 billion annually, the blip hit the radar of energy industry observers and journalists in the region. In the tightly controlled Saudi mediascape, the financial news outlet Argaam declared on Aug. 14, 2017, that a "brief outage" at Petro Rabigh had been "solved."

'High confidence'

Moscow-based research institute CNIIHM has been accused of developing the tools needed to carry out a sophisticated cyber intrusion into a Saudi petrochemical facility in 2017. | Image capture June 2017 ©2019 Google

The Triton case was far from solved.

Gutmanis and his team urged Petro Rabigh to contract a third party to take a deeper look. Aramco's specialists weren't able to tally the multiple infections or boot out the unknown hackers.

So Petro Rabigh hired U.S. cybersecurity firm FireEye Inc. for the job. The Milpitas, Calif.-based company has deep business ties with the kingdom, including an office in Riyadh. Its flagship defensive software is installed in the Saudi Ministry of Energy, Industry and Mineral Resources and parts of Aramco.

The incident response fell to FireEye subsidiary Mandiant, famed for having tied a series of cyber spying operations back to a Chinese military intelligence agency in 2013. That report cleared the way for U.S. law enforcement officials to bring cyber espionage charges against five People's Liberation Army officers in 2014.

By the time the FireEye investigation began, Triton had already captured the attention of cybersecurity firms tracking the world's most dangerous threats. The job of identifying hackers, then deciding who is privy to that information, has become a parlor game among private investigators, including FireEye, that operate outside the public eye and with very little oversight. As the revolving door spins out of government intelligence agencies, the power and influence of well-heeled cybersecurity firms that arrive on the scene after a major hack is now indistinguishable from the U.S. government's intelligence and security apparatus.

"They have global presence and the ability to collect an enormous amount of information," said Army Gen. Paul Nakasone, head of the National Security Agency and the Defense Department's U.S. Cyber Command, in a military trade publication called *Joint Force Quarterly*. "The products they produce often rival what we see being done by the intelligence community."

On Oct. 23, 2018, FireEye published a version of its non-public analysis that attributed the 2017 Triton hack to a research institute in Moscow. FireEye went public after a German news outlet obtained a copy of the document.

The document laid out ties between the Triton malware and the Central Scientific Research Institute of Chemistry and Mechanics, known by its transliterated Cyrillic acronym, CNIIHM. FireEye had been tracking the group behind the Triton intrusion long enough to link much of its activity back to an internet protocol address — and even a specific individual — at CNIIHM.

Analysts at FireEye assessed that the Russia-owned institute, located along the banks of the Moskva River, "likely possesses the necessary institutional knowledge and personnel to assist in the orchestration and development" of Triton.

FireEye said a number of clues had fed the firm's "high confidence" claim: for one, an IP address registered to the university was used to browse open-source reports on Triton, suggesting an uncommon interest in this kind of malware, according to FireEye.

FireEye tracks the hacking outfit under the name TEMP.Veles.

Analysts acknowledged they couldn't rule out that one or more CNIIHM employees acted without the institute's knowledge or approval, but that seemed "less plausible" than the alternative. CNIIHM houses departments with experience in military technology and critical infrastructure.

One of the CNIIHM researchers contributed to Russia's version of *Hacker* magazine and made regular appearances on the international cybersecurity conference circuit, FireEye claimed. Several of the Russian researchers have specialized IT skills, including digital forensics, reverse engineering and knowledge of how to exploit a computer's memory. (Some of the Triton malware's injects embedded themselves in the Schneider Electric device's memory.)

FireEye stopped short of naming a suspected Triton hacker. But it pointed to a unique handle buried deep in a TEMP.Veles tool that had been shared on a Russian social media site, as close to a smoking gun as the analysts were likely to find.

In a separate analysis sent to customers, FireEye noted that entire teams within CNIIHM "were possibly involved" in the Triton hack. "In the case of an intrusion with the mission of executing an attack on ICS processes, it would make sense for multiple teams to be leveraged," FireEye concluded.

FireEye issued caveats in both its customer and public reports: "We do not have specific evidence to prove that CNIIHM did (or did not) develop" the Triton tool itself, with its multiple parts. "We infer that CNIIHM likely maintains the institutional expertise needed to develop and prototype TRITON based on the institute's self-described mission and other public information."

Emails and calls to CNIIHM went unreturned, and three people currently or formerly affiliated with the institute did not respond to requests for comment. A spokeswoman for a partner institution said in a statement that it was not aware of any malicious activity at CNIIHM.

An August nightmare

In mid-August 2017, as the initial investigation ramped up, the Petro Rabigh hackers realized they'd been spotted. They deleted traces of the Triton tool set from engineering workstations at the complex in a belated effort to cover

their tracks.

At least six Triconex controllers had been compromised by the malware, which was built to replace operating code and co-opt the safety equipment during an emergency. The hackers were only able to overwrite devices left in "program" mode.

Circumstances around the August shutdown suggested the attackers didn't mean to trigger the infected devices and set off an investigation, sources said. They meant to maintain persistent access on the machines, waiting for the right moment to strike.

But now that they had been caught, the hackers weren't about to give up access without a fight. When Petro Rabigh's security team changed user passwords and enabled two-factor authentication — a way of adding an extra step for logging into accounts — the hackers were ready. They had already penetrated the corporate network, so they were able to change phone numbers tied to certain accounts in Petro Rabigh contact lists. The updated phone numbers redirected to websites controlled by the hackers, enabling them to capture and use any login codes sent to the devices via text message.

Petro Rabigh was living out any large organization's cyber nightmare: It was squaring off against a highly sophisticated adversary, or perhaps multiple adversaries, that had demonstrated deep knowledge of their target's systems and the ability to shift tactics on a dime.

The attackers had also demonstrated they could pivot to Petro Rabigh's control systems, a rare feat, and from there install a tailor-made tool to cut away a vital safety net.

The hackers apparently had no regard for the potential physical consequences to the petrochemical plant, or to the workers inside it.

An important question remained: Who were they?

The Iranian narrative

As the FireEye specialists rehabilitated Petro Rabigh's systems, they searched for digital breadcrumbs that would later feed into their CNIIHM report.

Evidence emerged that APT34 — APT referring to an "advanced, persistent threat" in cyberspace — had probed Petro Rabigh's networks. The threat group, which private-sector cyber analysts have tied to the Iranian government, is also known as OilRig because it tends to hit energy firms in the Middle East.

On the surface, APT34 looked to be a prime suspect for the Triton malware: Iran, a perennial foe of Saudi Arabia, would have ample motive to target Saudi oil and gas facilities with destructive intent. It wouldn't even be the first time. In 2012, suspected Iranian hackers carried out the infamous Shamoon cyberattack on Saudi Aramco's corporate computers, wiping out files, emails and core operating software in tens of thousands of machines. The Shamoon virus replaced the Windows startup page with an image of a burning American flag.

An intrusion into Petro Rabigh would fit with Iran's reputation as an emerging cyber power. After suffering damage to its nuclear enrichment facilities in Natanz due to the U.S.-deployed Stuxnet worm, the Iranian regime ramped up investment in both defensive and offensive cybersecurity technologies, analysts say. What better way for Tehran to demonstrate its hacking prowess than by striking at Saudi Arabia's oil, gas and chemical sectors?

Plus, Iranian hackers were actively targeting that sector, according to various cybersecurity reports. In July 2017, FireEye competitor CrowdStrike detected a malicious spear-phishing email targeting an employee at an unidentified Middle East petrochemical company. CrowdStrike tracks APT34 as Helix Kitten, a nod to Persian cats.

But Iranian hackers don't have an extensive track record of breaching complicated industrial control networks.

The Russia connection

Early findings from the FireEye investigation into Triton complicated the Iranian narrative. The hackers had let slip a few clues that pointed toward Moscow, not Tehran.

In fall 2017, there wasn't yet enough evidence to make a confident assessment. And the geopolitical math didn't seem to add up: Relations between Russian President Vladimir Putin and Saudi Crown Prince Mohammed bin Salman were on the upswing that year. Saudi Arabia's King Salman met with Putin in Moscow two months after the Triton infection was discovered, joining what Putin reportedly described as "substantive and meaningful" talks between two of the world's top oil producers.

Some observers raised the prospect that Petro Rabigh could have been a target of convenience, offering a live test bed for Russian hackers to get their feet wet in industrial networks before moving on to their ultimate marks.

An attack on a Saudi petrochemical plant orchestrated out of the Kremlin looks "quite strange," noted Dmitriy Frolovskiy, a Moscow-based political analyst and writer, in an email. "With the current good level of relations

between Putin and MBS, it is dubious that somebody from higher levels of the Kremlin would dare to issue an order to attack an object in [Saudi Arabia]."

In 2017, Saudi Arabia was also exploring an initial public offering of Aramco, a tempting prospect for Russian energy investors. Russian and Saudi companies were already teamed up on exports of liquefied natural gas from new Arctic energy projects. On the other hand, Moscow had been expanding its footprint in petrochemicals. Petro Rabigh's location along the Red Sea gives it easier access to African and European markets, putting it in more direct competition with Russia.

"Moscow was always interested in the Horn of Africa and saw it as a strategic location to affect global trade routes," Frolovskiy pointed out. "It still sees it this way."

Facts on the ground at Petro Rabigh matched up with Russia's playbook, based on U.S. intelligence assessments. By prying into that facility with hacking tools and retaining the ability to disrupt supply routes, Russian hackers could maximize Moscow's options in the event of future conflicts.

Top U.S. officials have warned of analogous Russian efforts to position themselves in U.S. critical infrastructure, keeping their finger off the trigger until some wider dispute called for action.

In a 2016 analysis, then-U.S. Director of National Intelligence James Clapper said Russia was laying the groundwork to bring down the grid or disrupt oil and gas facilities. Clapper's successor in the Trump administration, Dan Coats, offered a more plain-spoken assessment earlier this year:

"Moscow is now staging cyberattack assets to allow it to disrupt or damage U.S. civilian and military infrastructure during a crisis," Coats said.

Name and shame

Early in 2018, the cybersecurity firm Dragos revealed that it had spotted the group behind the Triton malware chasing after other targets. Some of those targets included U.S. facilities, placing the malware in a new and alarming light for the U.S. Department of Homeland Security.

Dragos said the malware had a "game-changing" impact on the defense of large industrial plants. Its analysts added that "any modification" to operating safety systems "represents a significant risk and potential for damage or even loss of life."

DHS placed Triton, which it called HatMan, in the ignominious company of the Stuxnet worm and the CrashOverride malware that disabled a major substation north of Kiev, Ukraine, in late 2016. But the agency added that Triton "surpasses both forerunners with the ability to directly interact with, remotely control, and compromise a safety system — a nearly unprecedented feat."

Yet even at that scale, DHS, Schneider Electric and Dragos declined to name names and identify the bad actors responsible for Triton.

FireEye's decision to name CNIIHM, and link an IP address there to Triton activity, reignited a debate in the information security community about the value of such details.

"As soon as you publish that stuff, you lose the source — it's gone," said Jon DiMaggio, senior threat intelligence analyst at Symantec Corp. "They're going to stop using that infrastructure."

A fount of trackable, malicious activity dating back to 2014 was all but guaranteed to run dry.

"[FireEye] decided that the overall benefit to making the community aware of it outweighed that," DiMaggio noted, adding that he, personally, didn't have a problem with FireEye's decision to publicize the CNIIHM connection. Still, DiMaggio urged private firms in particular to tread lightly when posting information that could cast a cloud over individuals.

"If you get down to naming people and you're wrong, then you really might be causing some issues," he said. "Leave that for governments to do with their indictments."

Katie Nickels, threat intelligence lead for MITRE Corp.'s ATT&CK team, which categorizes malicious cyber tactics, said she sees a use for attribution. "When people say 'attribution,' they mean different things. Some people mean the operator behind the keyboard. Others mean tying activity to a threat group," she said.

"As a defender, do I care if it's North Korea or Russia, or another country? I'm not convinced," Nickels said. "But I think at a minimum, there is value in tracking it back to a group or campaign."

FireEye declined to comment beyond the public version of its Triton analysis.

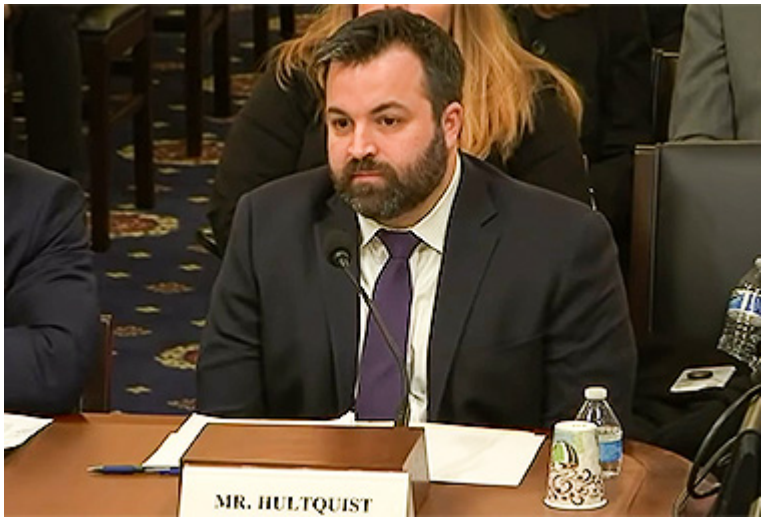
The FBI has declined to comment on whether it is investigating CNIIHM or people affiliated with the institute, citing agency protocol.

'Preparing for an attack'

The shutdown at Petro Rabigh one and a half years ago stands as the most recent known example of a cyber disruption to a major industrial safety and control system.

On Dec. 14, 2017, FireEye published its first Triton analysis for public consumption and offered a vague account of the August shutdown at Petro Rabigh, identified only as a "critical infrastructure organization."

"We believe the activity is consistent with a nation state preparing for an attack," FireEye experts concluded.



> John Hultquist, director of intelligence analysis at U.S. cybersecurity firm FireEye, testified before the House Homeland Security Committee on Feb. 26. FireEye and other private cybersecurity firms have emerged as significant sources of intelligence about hackers that target U.S. infrastructure. | House Committee on Homeland Security

Schneider Electric investigators carried out their own Triton investigation in parallel with Aramco and FireEye. What they found was a highly customized set of tools that could start from a Windows-based engineering workstation and dig all the way into the device memory of a Tricon 3008 v10.3 controller, taking advantage of a previously unknown vulnerability or "zero day" in the device along the way.

"This attack, this situation, has all the hallmarks of a nation-state attack," said Andrew Kling, the director of cybersecurity and architecture at Schneider Electric, at the 2018 S4 conference in Miami.

Kling described the attackers as having "unlimited resources," sophisticated skills and plenty of time to map out their intrusion. Yet the malware had limitations, including glitches that ultimately led to its discovery and removal. At its core, Triton carried a remote access Trojan, or RAT, a tool that gave hackers the ability to read and write code on the infected safety systems. It was tailored to the specific model and firmware version installed at Petro Rabigh.

Outing a suspect

The hackers behind the 2017 attack remain active, and the intruders' ultimate goal isn't known, according to multiple sources and cybersecurity firms. They've moved on to hitting vendors of industrial equipment, often using "off-the-shelf" tools that are widely used.

E&E News reached out to several individuals affiliated with CNIIHM, including one who apparently updated a personal website the day after the FireEye report went live last October.

FireEye has withheld additional evidence contributing to its "high confidence" report, and it declined to comment on the identity of one or more individuals its analysts linked to Triton activity.

Still, it's possible to draw a line from the clues FireEye dropped to at least two specific individuals. One researcher affiliated with the Russian institute has been publicly active in cybersecurity circles since 2011, as noted in the FireEye report, and E&E News confirmed that he contributed to the Russian-language *Hacker* magazine.

That person declined comment, citing a non-disclosure agreement with his employer. But a North America-based cybersecurity researcher who had worked on a project with this Russian national said nothing seemed out of the ordinary.

"He likes to do security research and present the results to the community, just like many aspiring youngish and talented researchers out there, from what I see," his collaborator said.

"But we never talked about our professional sides at all," the collaborator said. "And I never know what he or anyone does, behaves and thinks outside of what I see."