The New York Times | https://nyti.ms/2DrztDy

TECHNOLOGY

A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.

By NICOLE PERLROTH and CLIFFORD KRAUSS MARCH 15, 2018

In August, a petrochemical company with a plant in Saudi Arabia was hit by a new kind of cyberassault. The attack was not designed to simply destroy data or shut down the plant, investigators believe. It was meant to sabotage the firm's operations and trigger an explosion.

The attack was a dangerous escalation in international hacking, as faceless enemies demonstrated both the drive and the ability to inflict serious physical damage. And United States government officials, their allies and cybersecurity researchers worry that the culprits could replicate it in other countries, since thousands of industrial plants all over the world rely on the same American-engineered computer systems that were compromised.

Investigators have been tight-lipped about the August attack. They still won't identify the company or the country where it is based and have not identified the culprits.

But the attackers were sophisticated and had plenty of time and resources, an indication that they were most likely supported by a government, according to more than a dozen people, including cybersecurity experts who have looked into the attack and asked not to be identified because of the confidentiality of the continuing investigation.

The only thing that prevented an explosion was a mistake in the attackers' computer code, the investigators said.

The assault was the most alarming in a string of hacking attacks on petrochemical plants in Saudi Arabia. In January 2017, computers went dark at the National Industrialization Company, Tasnee for short, which is one of the few privately owned Saudi petrochemical companies. Computers also crashed 15 miles away at Sadara Chemical Company, a joint venture between the oil and chemical giants Saudi Aramco and Dow Chemical.

Within minutes of the attack at Tasnee, the hard drives inside the company's computers were destroyed and their data wiped clean, replaced with an image of Alan Kurdi, the small Syrian child who drowned off the coast of Turkey during his family's attempt to flee that country's civil war.

The intent of the January attacks, Tasnee officials and researchers at the security company Symantec believe, was to inflict lasting damage on the petrochemical companies and send a political message. Recovery took months.

Energy experts said the August attack could have been an attempt to complicate Crown Prince Mohammed bin Salman's plans to encourage foreign and domestic private investment to diversify the Saudi economy and produce jobs for the country's growing youth population.

"Not only is it an attack on the private sector, which is being touted to help promote growth in the Saudi economy, but it is also focused on the petrochemical sector, which is a core part of the Saudi economy," said Amy Myers Jaffe, an expert on Middle East energy at the Council on Foreign Relations.

Saudi Arabia has cut oil exports in recent years to support global oil prices, a strategy central to its efforts to make a potential public offering of shares of government-controlled Saudi Aramco more attractive to international investors. The kingdom has tried to compensate for its lost revenue by expanding its petrochemical and refining industry.

Some technical details of the attack in August have been previously reported, but this is the first time the earlier attacks on Tasnee and other Saudi petrochemical companies have been reported.

Security analysts at Mandiant, a division of the security firm FireEye, are still investigating what happened in August, with the help of several companies in the United States that investigate cyberattacks on industrial control systems.

A team at Schneider Electric, which made the industrial systems that were targeted, called Triconex safety controllers, is also looking into the attack, the people who spoke to The Times said. So are the National Security Agency, the F.B.I., the Department of Homeland Security and the Pentagon's Defense Advanced Research Projects Agency, which has been supporting research into forensic tools designed to assist hacking investigations.

All of the investigators believe the attack was most likely intended to cause an explosion that would have killed people. In the last few years, explosions at petrochemical plants in China and Mexico — though not triggered by hackers — have killed several employees, injured hundreds and forced evacuations of surrounding communities.

What worries investigators and intelligence analysts the most is that the attackers compromised Schneider's Triconex controllers, which keep equipment operating safely by performing tasks like regulating voltage, pressure and temperatures. Those controllers are used in about 18,000 plants around the world, including nuclear and water treatment facilities, oil and gas refineries, and chemical plants.

"If attackers developed a technique against Schneider equipment in Saudi Arabia, they could very well deploy the same technique here in the United States," said James A. Lewis, a cybersecurity expert at the Center for Strategic and International Studies, a Washington think tank.

The Triconex system was believed to be a "lock and key operation." In other words, the safety controllers could be tweaked or dismantled only with physical contact.

So how did the hackers get in? Investigators found an odd digital file in a computer at an engineering workstation that looked like a legitimate part of the Schneider controllers but was designed to sabotage the system. Investigators will not say how it got there, but they do not believe it was an inside job. This was the first time these systems were sabotaged remotely.

The only thing that prevented significant damage was a bug in the attackers' computer code that inadvertently shut down the plant's production systems.

Investigators believe that the hackers have probably fixed their mistake by now, and that it is only a matter of time before they deploy the same technique against another industrial control system. A different group could also use those tools for its own attack.

The August attack was also a significant step up from earlier attacks in Saudi Arabia. Starting on Nov. 17, 2016, computer screens at a number of Saudi government computers went dark and their hard drives were erased, according to researchers at Symantec, which investigated the attacks.

Two weeks later, the same attackers hit other Saudi targets with the same computer virus. On Jan. 23, 2017, they struck again, at Tasnee and other petrochemical firms, deploying a computer virus known as Shamoon, after a word embedded in its code.

The Shamoon virus first surfaced five years earlier at Saudi Aramco, wiping out tens of thousands of computers and replacing the data with a partial image of a burning American flag. Leon E. Panetta, the United States defense secretary at the time, said the attack could be a harbinger.

"An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches," he said.

Government officials and cybersecurity experts in Saudi Arabia and the United States attributed the 2012 Shamoon attack to Iranian hackers.

"Another attacker could have adopted that code" for the January 2017 attacks, said Vikram Thakur, a senior researcher at Symantec, "but our analysis showed the likelihood it was the same perpetrator was pretty high."

The attack in August was not a Shamoon attack. It was much more dangerous.

Investigators believe a nation-state was responsible because there was no obvious profit motive, even though the attack would have required significant financial resources. And the computer code had not been seen in any earlier assaults. Every hacking tool had been custom built.

The attackers not only had to figure out how to get into that system, they had to understand its design well enough to know the layout of the facility — what pipes went where and which valves to turn in order to trigger an explosion.

Investigators believe someone would have had to buy the same version of the Triconex safety system to figure out how it worked. The components, investigators said, could be purchased for $40,000 on eBay.

The attack has also shown the challenge of attributing with unquestionable evidence an attack to one country.

Security experts said Iran, China, Russia the United States and Israel had the technical sophistication to launch such attacks. But most of those countries had no motivation to do so. China and Russia are increasingly making energy deals with Saudi Arabia, and Israel and the United States have moved to cooperate with the kingdom against Iran.

That leaves Iran, which experts said had a growing military hacking program, although the Iranian government has denied any involvement in such attacks.

Tensions between Iran and Saudi Arabia have steadily escalated in recent years, and the conflict has drifted online.

United States officials and security analysts blamed Iranian hackers for a spate of attacks on American banks in 2012 and more recent espionage attacks on the airline industry. Iranian hackers were blamed for the 2012 Aramco attack and are also the leading suspects in the more recent Shamoon attacks.

The August attack was far more sophisticated than any previous attack originating from Iran, Mr. Thakur of Symantec said, but there is a chance Iran could have improved its hacking abilities or worked with another country, like Russia or North Korea.

Tasnee said in an email that it had hired experts from Symantec and IBM to study the attack against it. The company said it had also “completely overhauled our security standards” and started using new tools to prevent attacks.

“Being a global business,” the company said, “we believe that cybersecurity is a concern wherever you are in the world.”

Follow Nicole Perlroth and Clifford Krauss on Twitter: @nicoleperlroth *and* @ckrausss.

A version of this article appears in print on March 16, 2018, on Page B1 of the New York edition with the headline: How Hackers Lit a Fuse.
