Source : www.idsa.in Date : 2021-05-21

GROWING CYBER RISKS TO ENERGY INFRASTRUCTURE

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

More from the author

The US fuel pipeline operator, Colonial Pipeline, was hit by a cyber-attack on May 9 which led to the shutdown of supplies in states like Washington, Baltimore and Atlanta. Colonial Pipeline supplies nearly half of the US East Coast's fuel supply. The company took parts of their systems offline soon after the attack to contain the threat. The cyber-attack on the Colonial Pipeline network involved ransomware. The Federal Bureau of Investigation (FBI) on May 10 confirmed that the 'DarkSide' group of hackers was responsible for the attack.1

The cyber-attack on Colonial Pipeline led to fuel shortages and panic buying in the south-eastern United States. Around 2.5 million barrels per day of supplies, comprising gasoline, diesel and jet fuel, was affected following the attack. Oil prices rose with the price of Brent crude rising to $69 per barrel the following week, a 1.5 per cent rise.2 US gasoline futures jumped more than 3 per cent to $2.217 a gallon, the highest since May 2018.3

While analysts pointed out that a prolonged shutdown of operations could lead to a further hike in fuel prices, Colonial Pipeline on May 15 announced that it had returned to its normal operations and was focussed on the safe and efficient restoration of its pipeline system.

The FBI has been investigating the DarkSide group since last October, after repetitive attacks on organisations using the same modus operandi.4 Reports notes that at least 90 utilities were impacted, including companies like Brookfield, OneDigital and Gyrodata, among others.5

DarkSide brazenly maintains a list of all the companies it has hacked and the information on the data it has stolen, openly on its website on the dark web. The group of hackers had released a new software in March that can encrypt data even faster. The hackers work with 'access brokers' – cyber-criminal gangs who steal and sell personal data to the highest bidders on the dark web.6

Research by a London-based cybersecurity firm, Digital Shadows, has shown that the DarkSide group avoids attacking companies in Russia or in post-Soviet states like Ukraine, Belarus and Georgia.7 According to cybersecurity firm Cybereason, DarkSide is likely based in a Russian-speaking country as its software avoids encrypting any computer systems where the language is set as Russian.

US President Joe Biden has vowed to raise the issue of the pipeline cyber-attack with President Vladimir Putin, although there is no evidence of state involvement.8 In April, the Biden administration imposed new sanctions on Russia specifically targeting technology companies after it publicly identified the Russian Foreign Intelligence Service as the perpetrator of the 2020 SolarWinds attack. The SolarWinds cyberattack impacted both government agencies like the Pentagon and private companies.9

Biden signed an executive order (EO) on May 13 to encourage improvements in digital security standards across the private sector and better equip federal agencies with cybersecurity tools.10 The EO states that steps to prevent, detect, assess, and remedy cyber incidents are essential to ensure national and economic security. It also calls for Public Private Partnership to adapt to the

continuously changing cyber threat environment.

As per latest reports meanwhile, Colonial Pipelines paid a ransom amount of nearly $5 million to the hackers in cryptocurrency.[11] Even as the hackers provided the decrypting tool for restoration of the networks after the payment, the company had to reportedly use its own backups since the decrypting tool was too slow. The FBI stated that paying ransom encourages cyber criminals to repeat their crimes on other organisations or more likely on the same organisation.[12]

This incident has once again exposed the vulnerable nature of critical infrastructure to cyber-attacks. Given the geographically dispersed energy infrastructure, successful cyber-attacks on it have cascading, negative effects. Increased digitisation in recent times, undertaken to smoothen the complex operational and organisational requirements, have paradoxically opened up more opportunities for cyber criminals.

The various components used to monitor the flow of gases through the pipelines, for instance, like pressure sensors, valves, thermostats and pumps, are mostly controlled by centralised computers systems. Interconnected systems and networks are vulnerable to malicious attacks and in turn can affect the functioning of the pipelines.[13]

According to a report by Siemens, 18 per cent of the global utilities sector use high technology like AI and big data analysis.[14] Colonial Pipeline, for instance, also uses high technology inspection robots, controlled digitally, that check for anomalies if any. Such assets increase the number of potential entry points through which malicious attacks can take place.

In February 2021, an attempt was made by a hacker in Florida to tamper with the chemical levels in the drinking water supply of the city. The hacker had gained access to the water system through the control system of the water treatment plant using a remote access program. The hacker then tried to increase the levels of sodium hydroxide to dangerous levels. The attack was detected by a supervisor monitoring the computer system who reversed the chemical levels as soon the hack was detected, averting a crisis.[15]

Data theft and ransomware are some of the most typical threats faced by the utilities in the critical infrastructure sector. Such attacks result in loss of productivity, revenue and disruption of utility services. The Spanish electric utility, Iberdola, Brazilian oil company, Petrobras, among others have been victims of ransomware in the past causing major disruptions in their services.

Ransomware poses risks to critical infrastructure beyond the energy infrastructure. In 2020, over 500 incidents of ransomware attacks in the US on healthcare facilities, for instance, were detected.[16] These attacks took advantage of the prevailing pandemic situation, which makes victims more prone to extortion. The source of a ransomware attack is the hardest to trace since cyber criminals use automated attack tools and further demand the extortion amount in cryptocurrencies.

Cyber-related risks to the energy sector can be minimised by strategic intelligence gathering on potential threat actors, weaving of cyber security strategies into corporate decisions, industry-wide collaboration and sharing of intelligence data, investments in cybersecurity controls as well as periodic review of cybersecurity program budgets. Basic cyber security hygiene like multi-factor authentication, ready-to-implement response plans, and up-to-date backup systems can minimise the impact of cyber-attacks on critical infrastructure.

Views expressed are of the author and do not necessarily reflect the views of the Manohar Parrikar IDSA or of the Government of India.

END