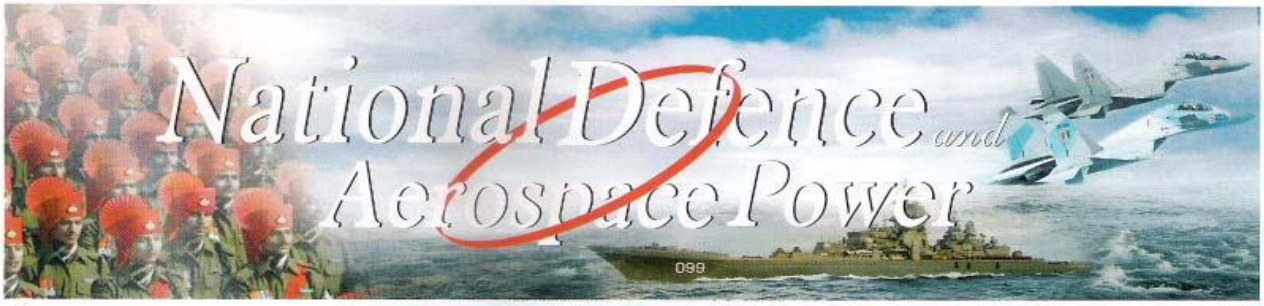

129 / 19 **12 November 2019**

SUPPOSED CYBER ATTACK ON KUDANKULAM NUCLEAR INFRASTRUCTURE - A BENIGN REMINDER OF A POSSIBILE REALITY

Dr. E. Dilipraj

Research Fellow, Centre for Air Power Studies

It all started with the following tweet posted from the twitter handle "@a_tweeter_user" on October 28, 2019:

"Interesting potential DTRACK (CC @Mao_Ware)

Dumps the data mined output via manually mapped share over SMB to RFC1918 address with a statically encoded user/pass:

> net use \\\\10.38.1.35\\C$ su.controller5kk /user:KKNPP\\administrator"

Quoting the above tweet, another twitter user named Mr. Pukhraj Singh with the twitter handle @RungRage made the following tweet on October 28, 2019:

"So, it's public now. Domain controller-level access at Kudankulam Nuclear Power Plant. The government was notified way back. Extremely mission-critical targets were hit."

Posting the tweet was only the delay, as Indian mainstream media as well as social media became frenzy about cybersecurity of the nuclear power plant in Kudankulam. News started spreading since late hours of October 28, 2019 that Kudankulam Nuclear power plant had been a victim of cyber-attack in September 2019 with a malware tool known as 'DTrack' and the perpetrators were alleged to be a hackers group called 'Lazarus' based from North Korea. Earlier news that the second plant in the infrastructure at Kudankulam was temporarily stopped on October 19, 2019 due to technical snag[1], was correlated by the media and the blame for the technical snag was quoted as the alleged cyber-attack.

In order to diffuse the escalating fear psychosis that was being propagated through print, electronic as well as online media regarding the alleged cyber-attack on kudankulam nuclear plant, authorities responsible for the infrastructure released a press release on October 29, 2019. The statement clarified that: *"Any cyber attack on the Nuclear Power Plant Control System is not possible. Presently KKNPP Unit-1&2 are operating at 1000MWe and 600Mwe respectively without any operational or safety concerns"*.[2]

Despite the clarification, the excitement in the media and among the public, related to a possible cyber-attack did not reduce. However, Nuclear Power Corporation of India (NPCIL) made an official statement on October 30, 2019 that *"Identification of malware in NPCIL system is correct. The matter was conveyed by CERT-In [Indian Computer Emergency Response Team] when it was noticed by them on September 4, 2019. The matter was immediately investigated*

by DAE specialists". The statement also clarified that the infected computer belonged to a user who was connected to the internet connected network used only for administrative purposes.[3]

Finally, this clarification from NPCIL helped diffuse the rumours and brought down the fear psychosis from the media headlines as well as from the online platforms across the country. Nevertheless, the incident should be seen as a strong reminder for a possible reality. Though NPCIL and other nuclear infrastructures authorities of the country assure that critical computer systems and networks that operates the power plants are constantly monitored and secluded from outside networks including internet, the past events across the world has cast a dark shadow in the minds of the people which is hard to forget. The reference here is to three important proven cyber-attack cases on Nuclear Power Plants across the world.

Though NPCIL and other nuclear infrastructures authorities of the country assure that critical computer systems and networks that operates the power plants are constantly monitored and secluded from outside networks including internet, the past events across the world has cast a dark shadow in the minds of the people which is hard to forget.

Davis-Besse v/s Slammer

On January 25, 2003, a computer malware known as 'Slammer' started exploiting the zero-day vulnerability in Microsoft SQL Server. Within a short period the malware had infected thousands of servers across the world and the numbers kept increasing every moment. Although Slammer did not carry any malicious payload that would delete or modify any files from the infected systems, the malware copied itself at a rapid rate which resulted in a huge volume of spurious traffic that consumed bandwidth and clogged several networks. Apart from causing outrage by disabling data-entry terminals at a 911 call centre in Washington, shutting down of 13,000 Bank of America ATMs, causing failure in online ticketing system and kiosks of Continental Airlines resulting in cancellation of several flights, and a nationwide internet outrage lasting half a day in South Korea, the Slammer malware was also successful in entering the computer systems at the Davis-Besse nuclear power plant in Ohio, USA. Although there existed firewalls between the corporate network and the plant network in the infrastructure, a consultant working for the corporate network of First Energy Nuclear, the licensee for Davis-Besse, had created a connection behind the existing firewall to the consultancy's office network. Thus the worm travelled from the consultant's network to the corporate network finally reaching the plant control network and generated huge traffic which clogged the corporate and control networks. As a result, Safety Parameter Display System (SPDS) of the plant became inaccessible for more than four hours and fifty minutes, which caused huge hindrance in the smooth functioning of the plant.[4]

The nuclear power plant escaped without any serious damage only because of the fact that the worm 'Slammer' did not carry any malicious payload; however, the alarming fact remains that the malware was successful in reaching and infecting the nuclear power plant system which was supposed to be air-gapped and stand-alone network from outside networks.

South Korean Nuclear Plant Hack

In mid-December 2014, a twitter account named "president of anti-nuclear reactor group" was found to be uploading sensitive files related to blueprints and manuals of nuclear reactors, air condition and cooling systems, a radiation exposure report, and personal data of employees of the nuclear power plant on a social networking platform.[5] The hacker/s (unclear if it was an individual or a group) had managed to hack and collect internal data of Korea Hydro & Nuclear Power Co (KHNP), the government company that operates all the 23 nuclear power plants in the country; the information was leaked through the social network in stages.

The perpetrators further went to the extent of demanding the authorities to shutdown three nuclear reactors namely Gori-1, Gori-3 and Wolsong-3 starting Christmas. The perpetrators also warned that if their demands are ignored

"residents near the reactors should stay away for the next few months" as they would create chaos with the reactors.[6] However, the authorities did not comply with the perpetrator/s demands for shutting down the reactors and conducted a two day cyber security drill on Dec 22-23, 2014, across the country on all the nuclear power plants to ensure no further leak of information took place. Later in March 2015, after a thorough investigation the South Korean authorities claimed that the perpetrator/s had collected all the information through cyber-attacks which were made between Dec. 9 and 12 by sending 5,986 phishing emails containing malicious codes to 3,571 employees of the nuclear plant operator.[7] Thus, social engineering was the modus operandi used by the perpetrators of this particular attack in order to access sensitive information from critical infrastructure network.

Iran v/s Stuxnet

In 2008, the centrifuges in Natanz Nuclear facility in Iran began to face unprecedented crashes. These breakdowns, which seemed to be like minor random accidents, continued till spring 2010 and the engineers in the facility were clueless about the reason for those crashes. In Spring 2010, the situation in Natanz facility began to deteriorate further when the centrifuges in the facility started to function in a haphazard manner, followed by more frequent and high intensity breakdowns thus affecting the whole nuclear programme of Iran. During this period, the engineers struggled to decipher the reason behind the disruptions in the facility which was later discovered by Symantec, a cybersecurity products manufacturing company, to be a highly sophisticated computer worm that had affected the controller systems or Supervisory Control and Data Acquisition (SCADA) systems in the facility.[8] This computer worm was named as STUXNET, thus becoming the first computer programme to be used as a cyber-weapon.

It was generally reported across all media that Stuxnet was the result of joint effort by US and Israeli intelligence agencies - NSA and Unit 8200 respectively, which was developed under a covert cyber program codenamed Olympic Games in order to sabotage Iran's nuclear program. The engineers at NSA and Israeli Unit 8200 initially wrote a 'beacon' computer programme that could map the functioning of Natanz facility and introduced it into the facility possibly with the aid of an unsuspecting insider. The 'beacon' program collected and transmitted information related to the facility's computer configurations and more such sensitive information to the agencies. Using the collected data, the engineers again wrote another complex 'worm' programme with the ability to disrupt the facility and introduced this programme into the computers of the facility through different unknown methods. The worm programme took control of many centrifuges in the facility and made them run either too fast or too slow; at times the centrifuges even exploded, thereby disrupting the nuclear programme of Iran.

Apart from being categorized as the first cyber-weapon tool, the Stuxnet episode had two other distinct features. First, this malware was the first known precision cyber weapon specifically built for a particular purpose. Second, unlike the other cases where malware spread from internet to the protected internal network, the Stuxnet case was the different. The various versions of the Stuxnet were injected into the sensitive networks of the Nantanz nuclear plant through different precisely targeted methods[9] and successfully carried out the sabotage job for several years. However in a later stage, due to a programming error in one version of stuxnet, the malware accidently copied itself from the protected network into a laptop of another Iranian scientist who worked in the facility. When the scientist connected the same laptop to internet outside the facility, the worm spread itself to other parts of the world through internet and this is when the world community took notice of such a malicious cyber-weapon.

Shadow of Reality

In the recent case of Kudankulam nuclear power plant, although one can attribute the hyper-reactions and fear mongering spread in mainstream as well as online media to ignorance and lack of technical understanding, the genuine concern of the country's population related to security against cyber –attacks of the nuclear facilities cannot be ignored. It has been identified by the cybersecurity community that possible

methods of cyber-attack on a nuclear infrastructure would include methods such as:

- Exploiting an insider (insider threat),
- Social engineering method and
- Supply chain contamination method.

These methods can be effectively used to conduct a number of cyber attacks like Denial of service/ Distributed Denial of Service attacks, Botnet attacks, SQL injection, viruses, worms, Trojans, ransomware attacks, etc.

Also, it is generally claimed that the computer resources in critical infrastructures like nuclear power plants would be in isolation from other networks even within the campus and they would not be connected to internet, therefore cyber-attacks on these air-gapped systems is highly impossible. The statement released by the authorities of Kudankulam Nuclear Power Plant as well as from NPCIL also highlighted the same rhetoric of air-gapped critical systems where cyber-attacks are impossible. While the aspect of isolation remains true to certain high sensitive computer resources probably inside the plant, the fact remains that the precisely targeted attacks are specifically customized in order to overcome this aspect of isolation, like in the case of Suxnet. Moreover with the current sophistication in hacking techniques, isolating a system or a network alone is not enough for securing the same as many new methods have emerged, especially for hacking into isolated/ air-gapped systems. Some of the recently developed cyber-attack methods on an air-gapped computer resource are:

It is generally claimed that the computer resources in critical infrastructures like nuclear power plants would be in isolation from other networks even within the campus and they would not be connected to internet, therefore cyber-attacks on these air-gapped systems is highly impossible.

- Air Hopper – Technology to hack information using FM Radio signals
- BitWhisper – Hacking air-gapped computers using heat
- GSMem - Hacking Air-Gapped Computer using low-end Mobile Phone
- DiskFilteration – Data extraction from Air-Gapped computer via Covert Hard Drive Noise
- LED-it-Go: Data Leak from air-gapped computers via Hard Drive LED

Apart from these techniques, there are numerous other methods that are either operational or under development which increase the threat vector to air-gapped critical computer resources especially in the case of nuclear installations. Apart from these, every air-gapped network would need to be updated from time-to-time both in terms of hardware and software which would require data transfer and equipment movement. This is where the method of supply chain contamination could be employed for precision targeted cyber-attacks on a nuclear infrastructure.

Therefore, given the pace at which technology is leapfrogging ahead against the speed in which security mechanisms are implemented in critical infrastructures of the country, incidents like the cyber-attack on Kudankulam nuclear power plant should act as reminders to the authorities responsible about a possible successful cyber-attack and the need to ensure and upgrade the defences. More importantly, the government should take up the responsibility of creating general awareness about the existing layers of cyber security in these critical infrastructures among the general public, without going into the details, in order to avoid unnecessary hyper-reactions and fear mongering in future.

With the current sophistication in hacking techniques, isolating a system or a network alone is not enough for securing the same as many new methods have emerged, especially for hacking into isolated/ air-gapped systems.

India cannot afford to be a victim of a cyber-attack on its critical infrastructures that will destabilize the country's development. Therefore, securing these critical infrastructures should

remain a job-in-progress forever, with regular upgrades, audits and reviews along with the usage of indigenously developed resources both in physical as well as virtual realm.

Notes

[1]"Second nuclear power plant at Tamil Nadu's Kudankulam stops operation", *The Statesman*, October 19, 2019, https://www. thestatesman. com/technology/second-nuclear- plant-tamil-nadus-kudankulam-stops-operation-02811948.html.Accessed on November 02, 2019.

[2] Press Release from Kudankulam Nuclear Power Project, October 29, 2019.

[3] "NPCIL admits malware attack at Kudankulam Nuclear Power Plant", *The Hindu*, October 30, 2019, https://www.thehindu.com/news/national/npcil-acknowledges-computer-breach-at-kudankulam-nuclear-power-plant/article29834644.ece. Accessed on November 02, 2019.

[4] Brent Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack",*Strategic Insights*, Volume 10, Issue 1, Spring 2011.

[5] "S Korea nuclear firm to hold cyber-attack drills after hack", BBC, December 22, 2015, http://www.bbc.com/news/world-asia-30572575. Accessed on May 08, 2016.

[6] "S. Korea nuclear plant hack: 3 reactors demanded closed by Christmas",*RT*, December 22, 2014, https://www.rt.com/news/216599-korea-nuclear-plant-hacked/.Accessed on November 02, 2019.

[7] Ju-Min Park and Meeyoung Cho, "South Korea blames North Korea for December hack on nuclear operator", *Reuters*, March 17, 2015,

http://www. reuters. com/article/us -nuclear-southkorea-northkorea-idUSKBN0MD0GR20150317.A ccessed on November 02, 2019.

[8] "How a secret cyber war program worked", *New York Times*, June 01, 2012, inhttp://www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html?ref= middleeast. Accessed on November 03, 2019.

[9] One of the various methods used to inject Stuxnet was to insert a contaminated USB onto the laptop of a Iranian Nuclear scientist in a conference abroad.

Centre for Air Power Studies

The Centre for Air Power Studies (CAPS) is an independent, non-profit think tank that undertakes and promotes policy related research, study and discussion on defence and military issues, trends, and development in air power and space for civil and military purposes, as also related issues of national security. The Centre is headed by Air Marshal K.K Nohwar, PVSM VM (Retd).

Centre for Air Power Studies
P-284, Arjan Path, Subroto Park, New Delhi 110010
Tel: +91 11 25699130/32, Fax: +91 11 25682533

Editor: Dr Shalini Chawla e-mail: shaluchawla@yahoo.com