THE INDIA FORUM
A JOURNAL-MAGAZINE ON CONTEMPORARY ISSUES

January 7, 2020

# The Computer Infection of Kudankulam and its Implications

**By: M V Ramana,Lauren J. Borja**

*The October 2019 cyberattack on a computer system at the Kudankulam nuclear power plant points to new pathways to severe accidents that can result in widespread radioactive fallout. Attempts to lower this risk would further increase the cost of nuclear power.*

On October 28, 2019 a computer security analyst tweeted that computer hackers had gained "Domain controller-level access at Kudankulam Nuclear Power Plant" (KKNPP) in Tamil Nadu. KKNPP has two operational nuclear reactors that had been connected to the electric grid in October 2013 and August 2016. The tweet was based on an information drop on the Dtrack virus at VirusTotal, which is an online repository of malware code. A version of the Dtrack virus found on the VirusTotal website included credentials specific to KKNPP's internal network, indicating that Dtrack had infected computers inside the nuclear power plant.

Nuclear energy is a unique source of electricity. One of its peculiarities is its capacity to suffer severe accidents that can spread hazardous radioactive contamination across thousands or even tens of thousands of square kilometres requiring evacuation of populations for decades or centuries. To avoid such accidents,the construction of nuclear power plants requires vast quantities of concrete and steel, exacting manufacturing standards, and layers upon layers of control systems at nuclear plants.

> The realization that hackers might be able to infect the computers in a nuclear power plant, potentially affecting the physical operation of the nuclear reactors themselves, is another safety vulnerability that had initially not been fathomed.

Despite such measures, there have been a number of accidents, of both small and large magnitude, since the beginning of the nuclear age. Each accident typically exposes a new vulnerability and often these accidents occur through pathways that were not conceived of by plant designers. The realization that hackers might be able to infect the computers in a nuclear power plant, potentially affecting the physical operation of the nuclear reactors themselves, is another safety vulnerability that had initially not been fathomed.

In addition to the technical aspects of accidents at nuclear power plants, the nature of organizations that operate hazardous technologies can affect both the likelihood and severity of accidents. Scholars who study safety in hazardous technologies have identified three characteristics of organizations that help to mitigate accidents, all of which involve how organizational leaders behave. These include placing a high priority on safety in design and operations; setting and maintaining safety standards and practices; and learning from failures. The little that is known of how the Nuclear Power Corporation of India has responded to the malware infection at KNPP suggests that organizational leaders did not meet these requirements adequately, especially the last one.

## What Happened

The Dtrack virus was well known in the computer security business. The prominent cybersecurity firm Kaspersky had reported that initial versions, called ATMDtrack, had been used to steal card data from Indian ATMs. Dtrack is the broader variant, which has been used to infiltrate Indian financial institutions and research centres. The malware uses a remote administration tool that would allow a remote party to gain full control over an infected device. Specifically, the most successful version of Dtrack "is able to list available files and running processes, key logging, browser history and host IP addresses," according to a description provided by Kaspersky. These functions indicate that the primary goal of the Dtrack virus is to spy on or steal information from its victim.

Based on similarities to a previous malware attack in South Korea, Kaspersky attributed Dtrack to the Lazarus hacking group. Lazarus attacks have occurred in many different countries and have included the infamous WannaCry and Sony Breach. Kaspersky has connected activity from Lazarus to IP addresses in North Korea; however, the cybersecurity firm acknowledges that this may be a 'false flag' operation intended to obfuscate the cyber criminal's true location.

> [T]he October 2019 attack was more sophisticated than initially thought, and potentially targeted at retrieving information specifically from KKNPP.

In the KKNPP attack, the file dump from the Dtrack virus suggests that the hackers only had access to the internal information technology (IT) network of the plant. This network contains information pertaining to the organizational aspects of the plant corresponding to tasks associated with management or payroll. While valuable information, such as personal information on employees or business practices, still exists on IT networks, they are not considered as critical as operational technology (OT) networks. OT networks control industrial processes; at KKNPP the OT networks would control the management and safety of the plant's nuclear reactors.

More recent coverage and investigation by additional cybersecurity researchers found that the Dtrack variant at KNPP included credentials specific to the KNPP networks coded directly into the virus itself. This indicates that the October 2019 attack was more sophisticated than initially thought, and potentially targeted at retrieving information specifically from KKNPP.

The targeted nature of the malware version found on KKNPP computers suggests that this might actually be a second version of the virus, created from information gathered during an initial infection. By coding in information specific to KNPP networks, hackers might have tried to make the second round of malware more lethal. There is precedent for hackers using a persistent presence on a network to successively unleash more complex and devastating attacks: one example was the devastating cyberattacks in 2015 and 2016 on the Ukraine power grid.

> [I]t still does not seem likely that the KKNPP attack was intended to cause direct damage. The hackers might have been just targeting information about the plant.

Despite this unsettling revelation, it still does not seem likely that the KKNPP attack was intended to cause direct damage. The hackers might have been just targeting information about the plant. What might motivate such information gathering expeditions? The reason is that if a hacker, either an individual or a group, were to be interested in causing serious damage to some nuclear installation, the biggest challenge might be obtaining the technical information about the design of the facility. We know that in the case of the Stuxnet attack that was launched by US and Israeli intelligence services to attempt to sabotage Iran's uranium enrichment program, there is reason to think that the espionage component was perhaps the most expensive aspect of the entire operation. (Ralph Langner, the person who gets the most credit for deciphering the Stuxnet attack has estimated that the development of Stuxnet may have cost "around ten million dollars".) Malware, such as the Dtrack virus, aimed at gathering information, might be a way to reduce the cost of complex cyberattacks.

## Three Difficult Conundrums

Cyber security should be a concern at nuclear power facilities worldwide, and the infection at KKNPP is one more indication that these types of cyberattacks are possible. Many other security researchers have sounded a similar warning. Two recent reports,one from the UK-based Chatham House and one from the US-based Nuclear Threat Initiative, have identified multiple computer security concerns specific to nuclear power plants. The Chatham House report identifies the nearsightedness of the plant operators: "nuclear plant personnel may not realize the full extent of this cyber vulnerability," in part due to a "pervading myth that nuclear facilities are 'air-gapped'– or completely isolated from the public internet – and that this protects them from cyberattack. Yet not only can air-gaps be breached with nothing more than a flash drive (as in the case of Stuxnet), but the commercial benefits of internet connectivity mean that nuclear facilities may now have virtual private networks and other connections installed, sometimes undocumented or forgotten by contractors and other legitimate third-party operators[1]."

> [O]ne cannot even try to avoid cyberattacks without forgoing the benefits that come with network or internet connectivity.

Let us unpack that a little. First, the term commercial benefits refers to the fact that while connecting a computer system to the internet poses risks, it also provides benefits. An obvious one is operational convenience. Someone working on that computer might need to copy some information or download a piece of software that is needed to carry out a task or report to a supervisor. Connecting to a larger network also allows technicians elsewhere, such as maintenance personnel, to work on the system without having to physically come into the nuclear power plant. This is the first conundrum: one cannot even try to avoid cyberattacks without forgoing the benefits that come with network or internet connectivity. For nuclear power plants that require extensive use of computers and similar equipment, the operational cost of not being connected to the larger network could be considerable.

Second, the role of employees is important. The phenomenon where employees who either knowingly or unknowingly threaten the security or safety of the organization they work in is referred to as the "insider" threat. Many of the examples presented in the Chatham House report were either caused by an employee or contractor who was authorized to act on the internal plant control system. For the most part, these contractors or employees might well have had no malicious intentions. But nevertheless their actions do result in adverse consequences. The conundrum here is that nuclear power plants or other infrastructural organizations must have employees, so the risk from insiders cannot be eliminated.

Further, bringing in contractors or third-party operators further increases the number of people with "inside" access to a system. Furthermore, these outside employees, while they may have technical expertise in a subsystem, may have less familiarity with the nuclear plant as a whole. This is illustrated in an example from 2008 at the Hatch nuclear power plant in the United States. In March of that year, the industrial control system failed when a contractor restarted a computer to install an update on the IT network of the plant. The restart of the IT network, which is supposed to be separate from the OT network that controls the nuclear reactors, caused a zero value to be entered into the control system data. A safety system misinterpreted this zero value as an insufficient cooling water and automatically shut down the reactor. The contractor was aware that the computer would need to be restarted, but not that it could potentially shut down the nuclear reactor. The reactor was out of commission for 48 hours and the company had to purchase electricity from another provider to make up its power supply obligations. This cost the company 5 million US dollars. Had the problem occurred at a different period, when the electricity grid is already stretched, there could have been blackouts.

> In most realistic circumstances, there can be no guarantee that the computer systems at nuclear power facilities can be kept completely safe from attacks.

The third conundrum arises from the almost inevitable conflicts between organizational priorities. It is clear that timely updates to plant computer systems is an important priority, but this can negatively impact operations. As everyone with a computer or smart phone should know, installing software updates of different kinds in a timely fashion is generally considered good for avoiding virus attacks and malware and so on. At Hatch, there may well have been some vulnerability that arises from leaving the system unpatched. But installing the update had a detrimental effect on the control system of the plant and thus its operations.

Likewise, there are conflicts between what is good for business and what is better for security. Having access to the internal control network of a nuclear power plant might be important from a business perspective. Creating this connection, however, also creates a security vulnerability. Since 2008, many companies recognized the problems with this connectivity and attempted to build separate networks. But the problem is far from fixed, as the NotPetya malware attack in 2017 revealed. While the virus primarily targeted IT networks, its impact was felt in OT networks around the world, such as in the radiation monitoring systems at the Chernobyl nuclear power plant.

One definition of the word conundrum is that it is a problem with no good solutions. That is definitely the case with cyberattacks on complex facilities like nuclear power plants. In most realistic circumstances, there can be no guarantee that the computer systems at nuclear power facilities can be kept completely safe from attacks.

## Inadequate response from plant operators and government

All of these vulnerabilities can be ameliorated or intensified by the organization that controls the hazardous technology under question. One way that organizations can make things worse is to think that there is no danger. The safety theorist James Reason once wrote that one of the many paradoxes about safety is that "if an organization is convinced that it has achieved a safe culture, it almost certainly has not". This has, unfortunately, been the case with the Nuclear Power Corporation of India Limited (NPCIL).

The Chatham House report mentioned earlier described a similar phenomenon in nuclear power plant operators—the false belief that an air-gap was sufficient protection for their computer systems.

Belief in that myth was on full display on October 29, 2019, the same day as the initial tweet, when NPCIL issued a press release on behalf of the KKNPP plant:

```
Some false information is being propagated on the social medial platform, electronic and
print media with reference to the cyber attack on Kudankulam Nuclear Power Plant. This is to
clarify that the Kudankulam Nuclear Power Project (KKNPP) and other Indian Nuclear Power
```

> Plants Control Systems are stand alone and not connected to outside cyber network and Internet. Any Cyber attack on the nuclear Power Plant Control System is not possible.

While the press release did not explicitly deny a malware infection, it dismissed public concern over cybersecurity at the plant.

Within a day, however, the NPCIL issued a second press release confirming the presence of malware:

> Identification of malware in NPCIL system is correct. The matter was conveyed by CERT-In when it was noticed by them on September 4, 2019. The matter was immediately investigated by DAE specialists. The investigation revealed that the infected PC belonged to a user who was connected in the internet connected network used for administrative purposes. This is isolated from the critical internal network. The networks are being continuously monitored. Investigation also confirms that the plant systems are not affected.

While it is possible that both of the press releases are true, the initial press release is misleading. And while the second press release admits malware infection, it affirms earlier statements that control systems were not affected. Requiring this nuanced reading of the press release, however, makes it seem like NPCIL was not being forthcoming with information about this security threat.

Despite not containing any falsehoods about the infection itself, from what is known publicly now there was one glaring falsehood in the first press release: the claim that it is not possible to carry out a cyberattack on a system that is not connected to outside networks or the Internet.

> [A] computer virus can have a physical effect on a system that is not connected to the internet.

Why do we say that this claim is false? This is because air-gapped networks can be infected in many ways, most obviously when an employee connects an infected device, such as a PC or USB drive, to the isolated network. This is what appears to have happened at Natanz, the uranium enrichment plant in Iran, where a spy recruited by the Netherlands is reported to have installed the Stuxnet virus. That virus operates by infecting computers that are used to control centrifuges that are used to enrich uranium. The computer does not need to be connected to the internet. If this computer is infected, the virus causes the centrifuges to spin faster than designed, which results in their destruction. Thus, a computer virus can have a physical effect on a system that is not connected to the internet.

Furthermore, as our discussion of security conundrums illustrated, establishing and maintaining this separation is operationally challenging. In some instances, the systems are not separated at all and the “air-gap” may exist only in the minds of plant operators.

## Implications

There are two major implications that flow from the attack on Kudankulam’s computer systems. The first has to do with the potential for severe accidents at nuclear power plants. Cyberattacks can create a further pathway for accidents. Even if the attacks themselves might not cause, say, the meltdown of the core, by potentially disabling safety systems or causing other problems, such as loss of electric power at the plant, these attacks could set the stage for a meltdown if it is combined with some other challenge to the plant’s safety systems, for example a severe storm or an earthquake.

The second implication has to do with one other peculiarity of nuclear power, besides its propensity for severe accidents. Unlike most other sources, the cost of building nuclear plants has increased rather than declined with more experience. This is most evident in the US and France, which are the two countries with the most number of nuclear plants. Under very specific conditions and among small subsets of these plants, there have been slight declines, but the overall trend is unambiguously one of cost appreciation. Analysts have termed this a case of negative learning.

> Should NPCIL address it [the cyber vulnerability] by instituting new safety measures … this would typically drive up the cost of building and maintaining these nuclear plants.

The observed increases in cost have to do with the peculiar characteristic that we started with: the potential for severe accidents at nuclear plants. A substantial part of the cost of building nuclear plants comes from the need to avoid such accidents. The inclusion of safety measures, often designed to deal with new vulnerabilities discovered by examining the record at all nuclear plants, does drive up the cost. Of course, these costs might be only a very small fraction of the already astronomical costs of nuclear power plants, but they

serve to increase the bill. The cyberattack on Kudankulam is an example of a new vulnerability.

Should NPCIL address it by instituting new safety measures at not just that reactor but also other nuclear power plants, those would typically drive up the cost of building and maintaining these nuclear plants. That, in turn, would make electricity from these plants even more expensive than it already is.

**Footnotes:**

1 A Virtual Private Network or VPN is a connection that uses a public connection, like the Internet, to link two previously disconnected computer networks. The public network used to establish this connection, however, does not have to be the Internet. For a nuclear power plant, it is possible that the IT and OT networks could be connected via VPN, but still remain isolated from the broader Internet. This would allow employees to access control room operations while at their desk inside the facility. The Chatham House report, which was compiled after meeting with many nuclear industry professionals, suggests that the public network used was indeed the internet—especially if "contractors," who are less likely to be on-site than plant employees, set up the VPNs.