The R.A.T in the Shell

An analysis of breach into Kudankulam Nuclear Power Plant through the lens of Cyber Kill Chain and the study of Remote Access Trojans and the targeting of critical infrastructures.

Siddharth Balyan, Pradyumn Khanchandani, Monika Arora
(balyan.sid@gmail.com; PradyumnKhanchandani27@gmail.com, monika.a@lucideustech.com)

ABSTRACT

The Lockheed-Martin Cyber Kill Chain is a list of steps followed in a cyber attack. The Kill Chain lists Reconnaissance as the first stage. This is where the attacker gathers information about the target and seeks to find loopholes in the security of the system, a backdoor or an internet facing insecure computer. All of these can be classified into vulnerabilities. The latest breach discovered in NPCIL (Nuclear Power Commission of India Ltd.) is rumoured to have involvement of the Dtrack malware. Dtrack has been under investigation since the summer of 2018 and is a dual-purpose malware. One of its functions being, gathering information on the target system. This comes under the Reconnaissance stage as Dtrack could have been used to find vulnerabilities and backdoors so that more critical systems could be exposed. A later example of the malware in question being used in a different form is when reports of Indian financial institutions being targeted came out and this was the cyber-espionage software in question. Advanced Persistent Threat (APT) cyber crime group called The Lazarus Group based in North Korea also has ties with the spyware in discussion.

KEYWORDS: Kudankulam Nuclear Power Plant, Remote Access Trojans, NPCIL, nuclear plant, Industrial Control Systems, Cyber Kill Chain, Spyware.

1. Introduction

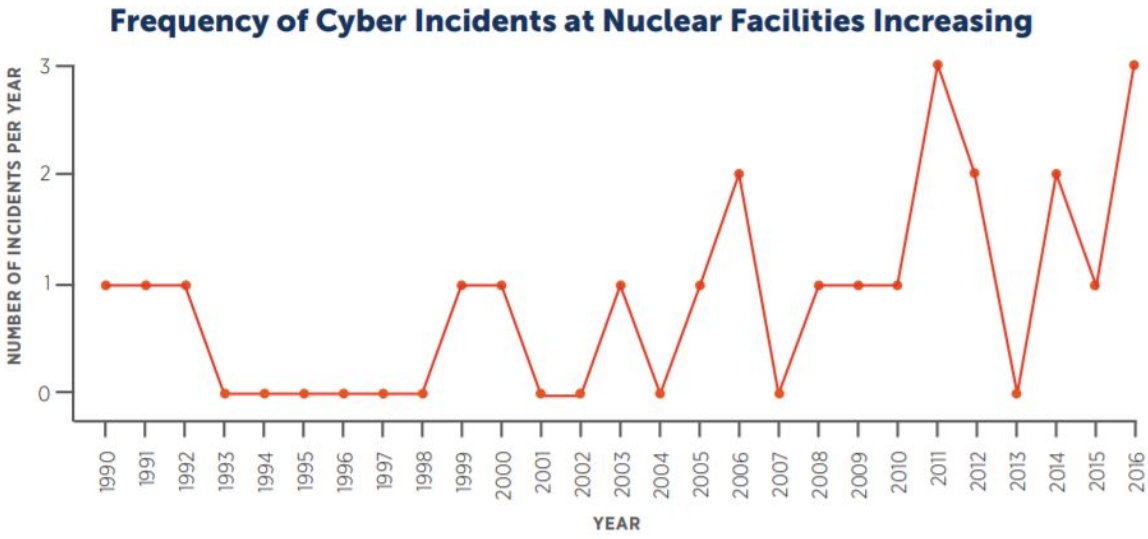

Figure 1: The incidents pictured above represent publicly disclosed cyber incidents at nuclear facilities since 1990. It is possible that more incidents have occured that have not been publicly disclosed or for which details are classified or otherwise unavailable

Cyber attacks on multinational corporations, banks, news agencies and even government websites and services have been making the news these past few years. Fortunately, close to none of these *attacks* have been catastrophic to life or the function of society. That's not to say that cyber attacks don't have the capability to cause harm to life, the public services and infrastructure. Critical infrastructure has been targeted quite often ever since the 90's, with nuclear facilities being hit by cyber attacks upwards of twenty times [1]. A hit to such sensitive facilities is much scarier. A lot of stages go in planning and mounting such an attack.
To properly understand these stages and mount an appropriate defence requires the defender, here, a nuclear facility, to fully understand the importance of cyber security as an important aspect and accelerate development of frameworks and guidelines towards it.

The fact that the threat on important services and facilities is ever so real is proven by the recent breach detected in India's largest nuclear facility in Kudankulam Nuclear Power Plant (KKNP). A lot can be extracted, learnt and analyzed from this recent incident.
A timeline to summarize the sequence of events [2]:

- October 29: A breach detected, NPCIL denies any claims
- October 30: 24 hours later after denying, NPCIL owns up to breach and says only non-essential, administrative workstations were compromised, computers important to the functioning were safe.

- Later, a cyber security researcher responds and says NPCIL and ISRO were warned of the potential hack in September, which is quite a while coming to these things. ISRO says, internal checks were performed.
- VirusTotal, publishes a paper stating that quite a lot of data was compromised.
- Kaspersky article and paper reveals that the malware detected was similar to Dtrack, a remote access trojan (RAT)

This is clear that the attack was against a high value strategic infrastructure and may be an act of cyber espionage. While the system compromised was an administrative one and not an Industrial Control System (ICS), it does not mean that harm was not intended. A look at one of the most researched hacks against the nuclear facility in Natanz, Iran will point to the fact that a cyber espionage like this preludes to something larger with much more malicious intent.
Another interesting clue is that the system was infected with a malware known as Dtrack which has origins tied to North Korean's hacker group, Lazarus. Adding a geo-political twist to such incidents helps put things in perspective and understand what really is going on here.

The malware, Dtrack is a Remote Access Trojan (RAT) which, like Trojan Horses, make their way onto the target computers and give the adversary partial or complete anonymous and administrative control over the system. ATMDtrack is a version which had been targeting Indian Banks and read and stored card details of the customers.
Kaspersky discovered this family of RAT malware related to ATMDtrack and called them Dtrack. The link to the North-Korean hacker group comes when Kaspersky [3] noted similarities to DarkSeoul campaigns attributed to the infamous Lazarus group.

The paper hopes to build up on the topics introduced here in relevant sections. Section two hopes to give a well documented insight on the breach in Kudankulam. Section three hopes to analyse the working of a RAT and give a good understanding of the Dtrack malware family. Section four will like to look at the incident through the Cyber Kill Chain with the context acquired from the previous sections. Using the framework of the CKC, section five hopes to give appropriate comments on the prevention of future cyber incidents and defending future incidents, should they happen.

2. Breach in the Kudankulam Power Plant

India is relatively new to the nuclear race as compared to some of the older, more experienced countries in the nuclear field. On 13th May 1998, a press conference the then PM declared India to be a full fledged nuclear state. The construction of Kudankulam Nuclear Power Plant (KNPP) began on 31st March 2002. It is scheduled to have six reactors built in collaboration with a Russian state company and currently powers the southern states of Tamil Nadu, Karnataka,

Kerala and Puducherry with an output of 2,000 Megawatts. *One more interesting fact is that this facility was a victim of cyber-espionage very recently.*

2.1 The sequence of events

On September 3rd, Cyber security expert Pukhraj Singh informed the National Cyber Security Coordinator Lt. Gen. Rajesh Pant that he believed the systems of critical infrastructure of ISRO and the Kudankulam Power Plant to be compromised. On September 7th, he tweeted, "I just witnessed a casus belli in the Indian cyberspace and it sucks at every level."[4].

On 23rd September, Kaspersky published a report on a malware called Dtrack which was targeted Indian financial institutions and had ties with the North Korean hacker group, Lazarus.

In the evening of the 28th of October, a link to a report on VirusTotal.com emerged pointing to an interesting potential Dtrack breach. Pukhraj Singh said that he didn't discover the intrusion, a third-party did, he merely informed the NCSC. This started to make news and on 29th October, NPCIL released a statement saying that any Cyber attack on the Nuclear Plant Control System is not possible, claiming the system to be air-gapped.

A day later, NPCIL issued a press release saying that a malware was indeed discovered in a NPCIL system on September 4th. The system compromised was said to be an administrative one and not connected to any of the crucial Industrial Control Systems. The standing of all the officials involved is that the compromised system was isolated from the internal networks and everything was handled.

A lot can be studied and analysed from the breach. From the detection and warning stages to the denial stages and the geo-political aspect of the breach, the sub section hopes to look at all the aspects of the incident thoroughly.

3. Targeting of Indian institutions

As stated earlier, targeting of critical and vulnerable public infrastructure is nothing new and this is on the rise throughout the world. To properly and successfully mount an attack of such a large scale like this, meticulous planning, involving Research and Reconnaissance of the target, finding weak points, crafting exploits and delivering the payload takes place.

Important and essential facilities all over the world operated in isolation not too long ago. With the advent of complexity in the facility systems and technology, they have become more reliant on interconnected devices and networks. This has created another facet of risk on these facilities. In this paper's context, the facility in question being a nuclear power plant. The extent of cyber awareness and safe cyber practices are nowhere near the required amounts to deal with the

threats which have been emerging these past two decades against the new aspect of cyber security.

Coming to the Kudankulam Incident, on researching, it was found that the same strain of malware which was reportedly found in the facility had been found on ATMs and other financial institutions [5]. The targeting of essential and dangerous *seems* to be at a high, but experts say that the awareness and the increased focus on these aspects has made a lot of these breaches public. Although it goes without saying that cyber awareness is nowhere near the level it is supposed to be.
One more important link to the breach alarm raised by Pukhraj Singh was that even ISRO was thought to be compromised. A civil space program and a nuclear facility with a breached system does not look good anyway one looks at it [6].
Given the stakes of the infrastructure and the evidence which points to the fact that there is still a lot of work to do to be capable of thwarting cyber attacks against the said infrastructure, they have become a sought after target by a large number of hacker groups. If one takes into the Ukraine Power Grid attack of 2015 as an example, it was noted that Russian hackers were behind the incident. Hence it goes without saying that geo-politics and relations between the countries is an important facet while looking at these incidents.

The largest and the most documented hack into a critical facility which caused disruption was the *Stuxnet* malware in the Natanz facility in Iran. The malware managed to bring the entire facility at a halt and made its way into a special place in history books since 2010. After this there have been multiple cyber attacks and espionages into critical facilities which have shaken the world.
India, being an emerging power and having a large population easily falls into one of the easy targets. This particular case has not been researched or documented enough to clearly state how serious of an attempt this was, but an attempt at spying and espionage usually preludes something even more sinister.

4. A study of Dtrack

Dtrack made the news after the discovery of evidence that it was behind the compromise of a system in KKNPP. Intended to be spying tools, Dtrack and ATMDtrack are strains of Remote Access Trojans and Malware with a wide array of spying tools and as many as 180 different variants. Dtrack samples were found to infect computers in 18 states in India. A fourth of all affected systems were in Maharashtra (24 per cent), followed by Karnataka (18.5 per cent) and Telangana (12 per cent). The other major states where financial institutes were targeted by Dtrack include Tamil Nadu, Delhi, Kerala, and West Bengal [7].

In a blog article, Kaspersky revealed that they had first come across this malware in the summer of 2018 when a different strain of this spyware was found to be infiltrating financial institutions and using spying tools and siphoning card details from ATMs. Talking about the variant of Dtrack discovered on PCs, Konstatin Zykov noted that it had the capabilities of carrying out a variety of functions such as keylogging; retrieving browser history; gathering host IP addresses, information about available networks and active connections; listing all running processes; and listing all files on all available disk volumes. It was also found to have an additional RAT executable, which could give admin privileges to a remote hacker.

It has now been established that Dtrack is an espionage and a spyware tool, and comes under the Advanced Persistent Threat category which means that it was meant to stay undetected for a long time to gather information quietly. It was also intended to create backdoors in the network and provide remote access to the compromised system. It has been classified as a Remote Access Trojan (RAT) based on its functions and capabilities.

4.1 A study of Remote Access Trojans

Trojan malwares, in simple terms, are malicious programs designed to be useful software for the user. *Remote access* refers to the ability of the malware to listen in on specific TCP/UDP ports, change/create/destroy processes, and give an adversary system remote access to the afflicted system. By giving remote access, the adversary has access to see the filesystem, access the command-line and have administrative privileges. Following shows an example of a RAT in a virtual system in order to convey its working.

There have been quite a number of RAT which were open source and were modified and used for malicious purposes. gh0st RAT is one such example, gh0st v1.0 is still available on GitHub as its harmless. Here we have shown Powershell-RAT developed by the user Viralmaniar from GitHub [2]. It is a python based backdoor that uses Gmail to exfiltrate screenshots and data and is Fully UnDetectable (FUD) by an antivirus. This was demonstrated at BlackHat 2019 [8].
The demonstration below is meant to show the working and processes of RAT and similar Cyber-Espionage software and spyware. It also hopes to shed light on how with some expertise, one can easily modify an existing tool or create even more malicious software.

delScreenShot	28-Aug-19 11:01 P	Windows Batch File	1 KB
delScreenShot	28-Aug-19 11:01 P	Windows PowerS...	1 KB
delScreenShot	28-Aug-19 11:01 P	VBScript Script File	1 KB
Mail	28-Aug-19 11:01 P	Windows Batch File	1 KB
Mail	28-Aug-19 11:01 P	Windows PowerS...	2 KB
Mail	28-Aug-19 11:01 P	VBScript Script File	1 KB
PowershellRAT	24-Nov-19 11:09 A	Python File	5 KB
README	28-Aug-19 11:01 P	MD File	5 KB
Shoot	28-Aug-19 11:01 P	Windows Batch File	1 KB
Shoot	24-Nov-19 11:08 A	Windows PowerS...	1 KB
Shoot	28-Aug-19 11:01 P	VBScript Script File	1 KB

Figure 2: This is a list of the scripts and files used by the RAT

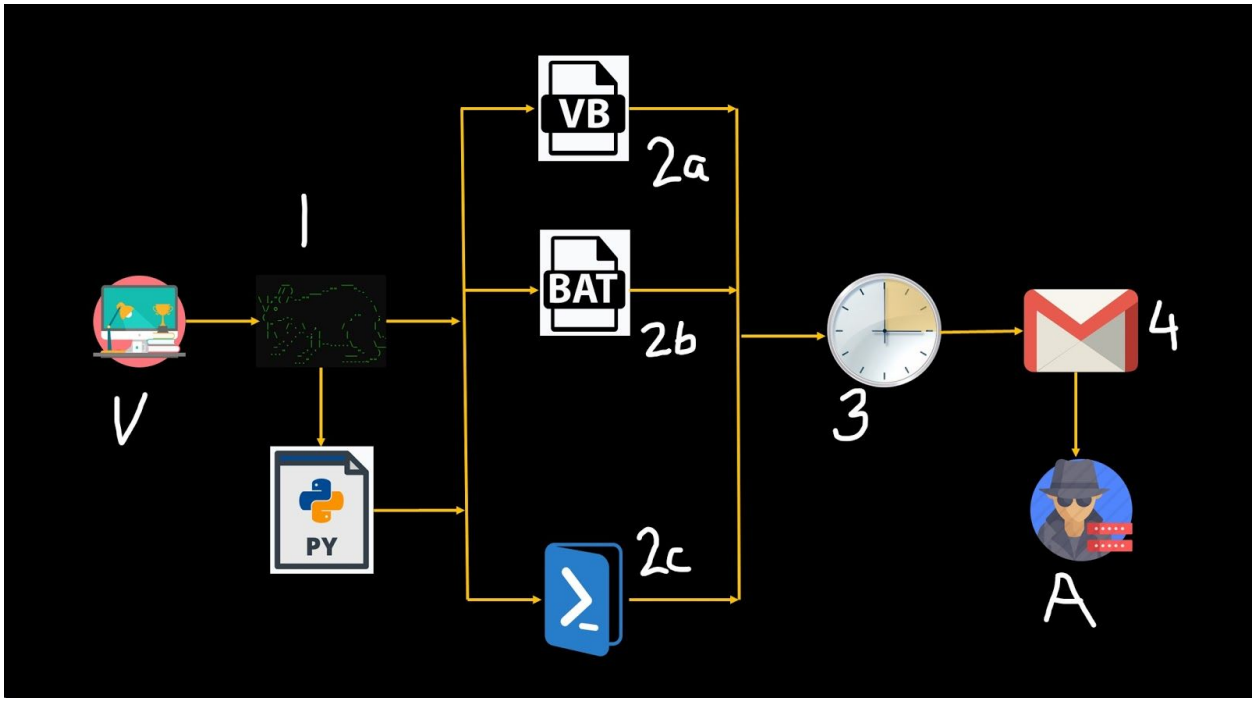

Figure 3: RAT Architecture Diagram

Explanation of the architecture:

- The victim (V) has the RAT(1) installed through a trojan file.
- The RAT consists of a python script which once executed calls upon VBScript(2a) and .bat(2b) and Powershell (2c) scripts.
- Using the task scheduler (3), periodically emails are sent to the Adversary (A) using Gmail (4).

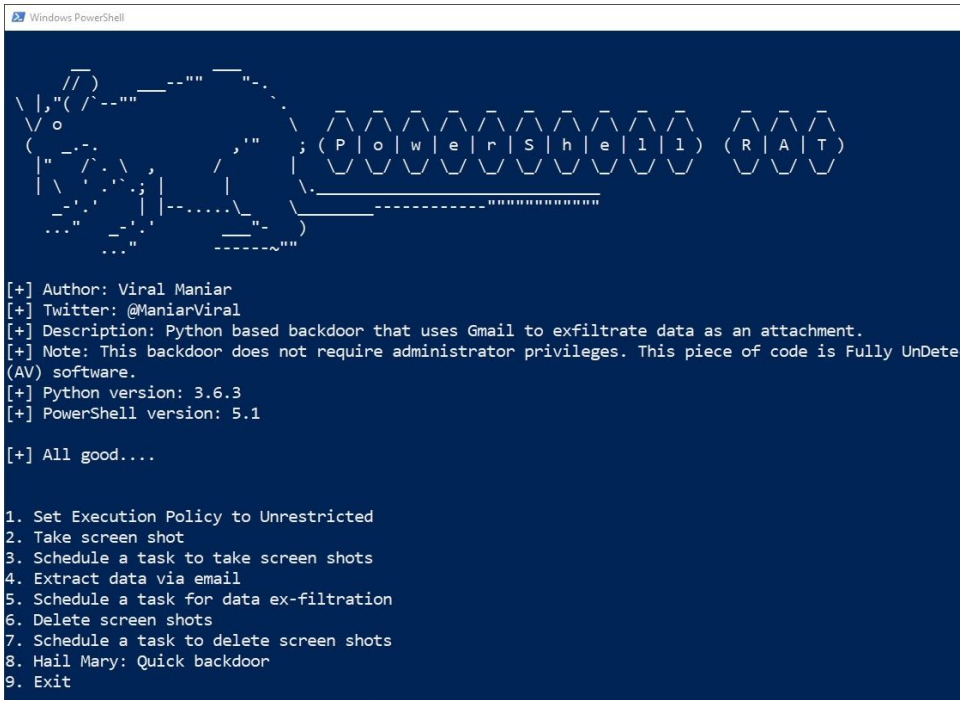

Figure 4: Following shows the different functionalities of the RAT on running the python script. To run Powershell and other scripts, Execution Policy has to be changed.

Figure 5

The Python script has function calls for each feature available, as can be seen above. The functions call a Powershell script written for each specific purpose. The Powershell scripts,

having the escalated privileges due to Unrestricted Execution Policy can make changes in the task scheduler, disable certain processes, enable and start certain processes and more.

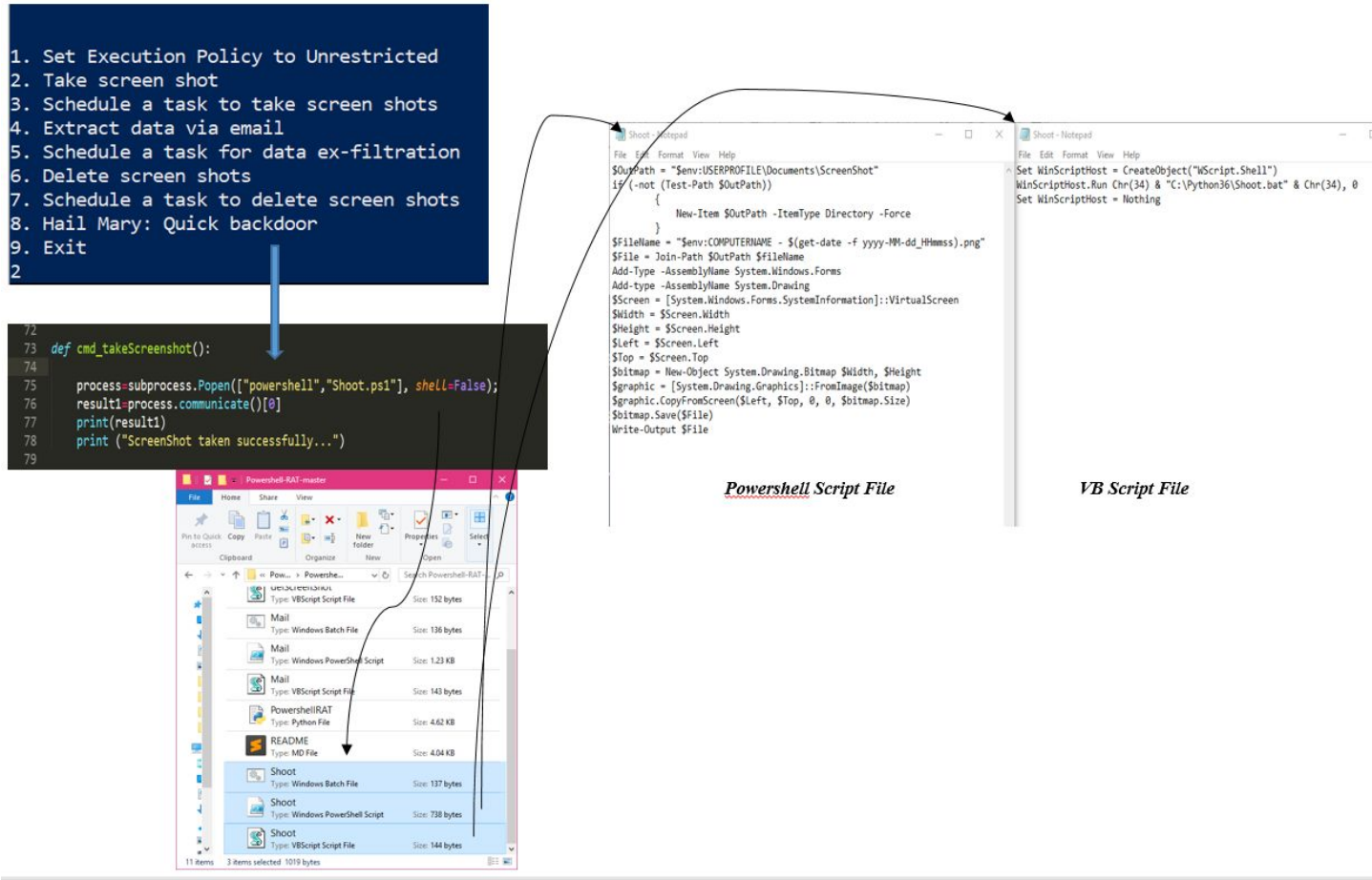

Figure 6

From Figure 6, it can be seen that the Python script calls into action, a Powershell script which then invokes a VBScript. The two script files then perform the task, in this case, taking the screenshot and saving it in a specified folder. In real life purposes, the Python script would be automated, or remotely controlled leading to multiple screenshots of the computer screen leading to exposure of sensitive data.

Figure 7: Execution Policy set to Unrestricted

On using option 3, a task is scheduled which takes screenshots every 1 minute.

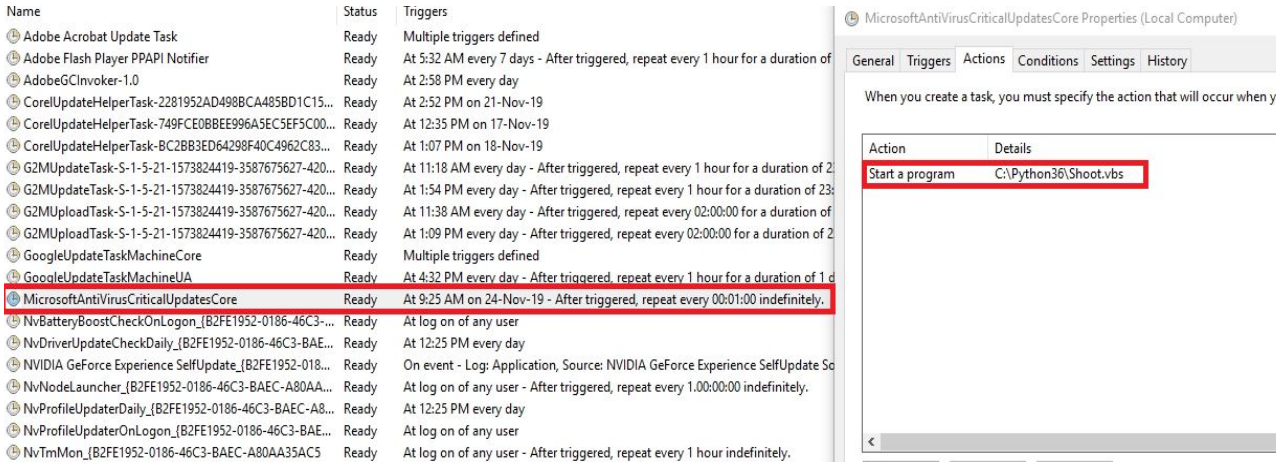

Figure 8: The script Shoot.vbs is the script which captures the screenshots

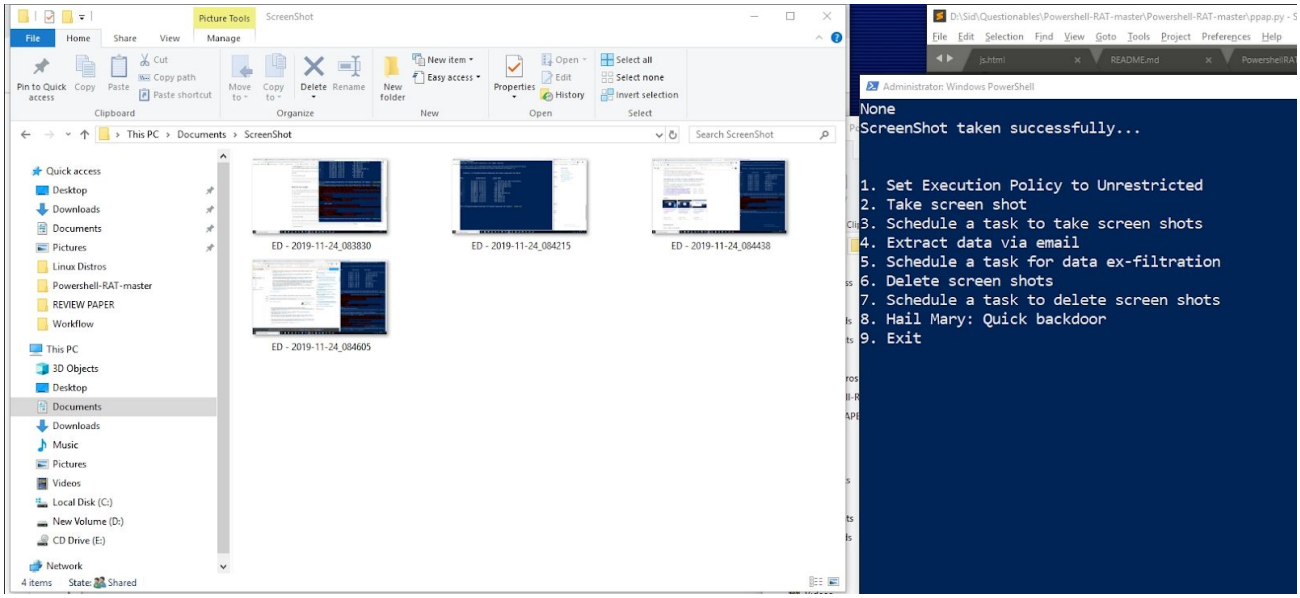

Figure 9: The screenshots are saved automatically in a predetermined directory

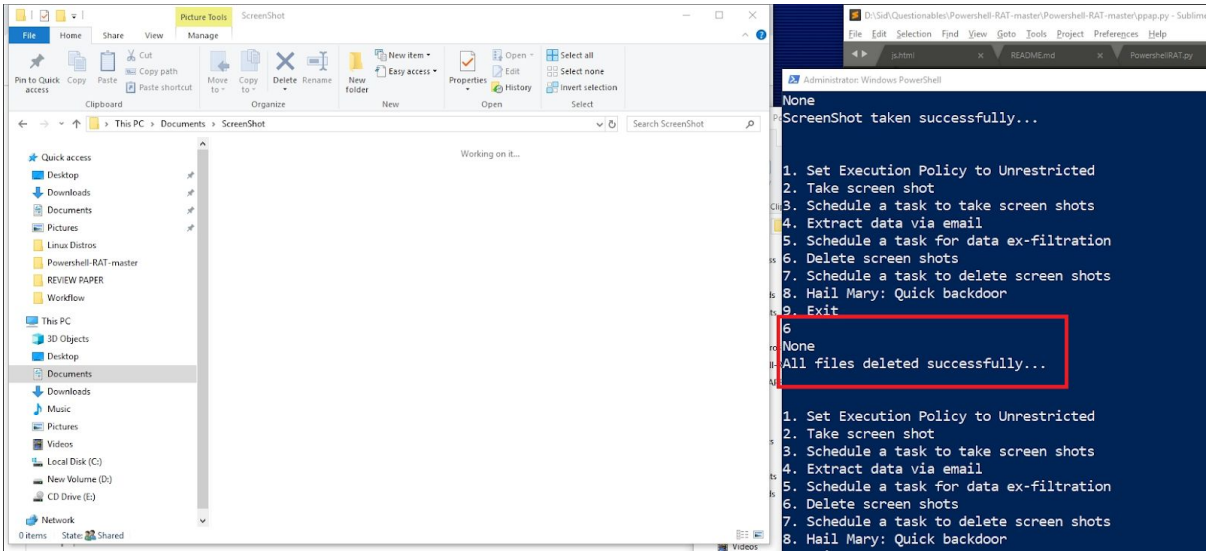

Figure 10: They are also deleted using the 6th option

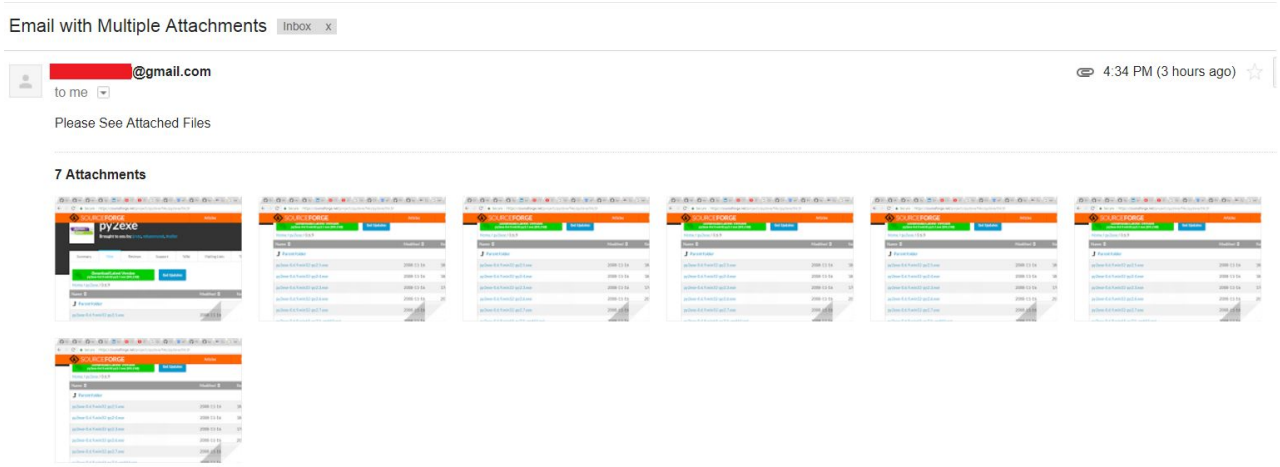

Figure 11: The screenshots in an email

The option 8, is used as a Hail Mary if anything goes wrong and creates multiple processes using Task Scheduler and deletes all the screenshots.

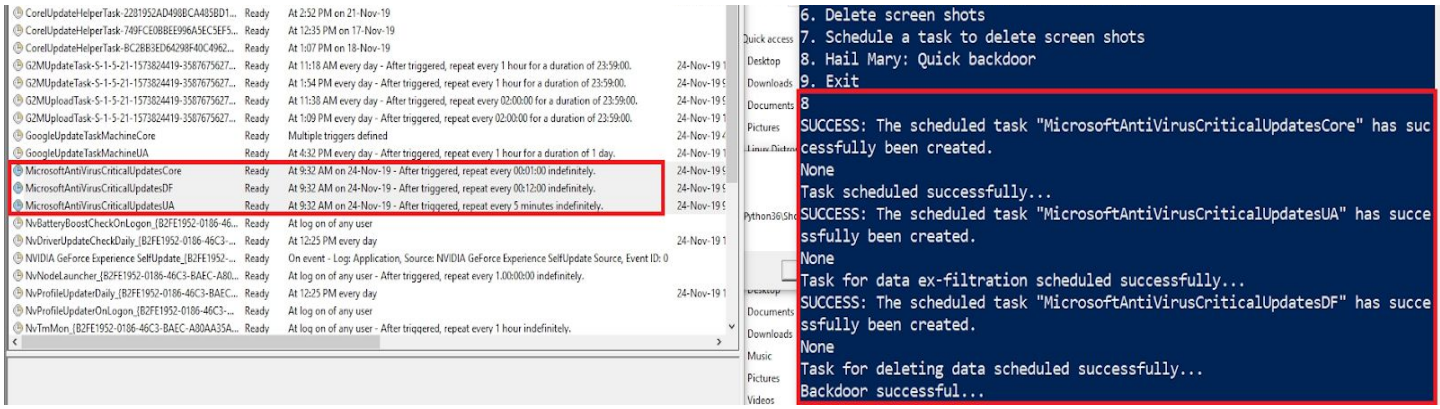

Figure 12

Thus, the script can successfully change admin settings, take screenshots, and email the screenshots periodically while deleting them while being FUD.

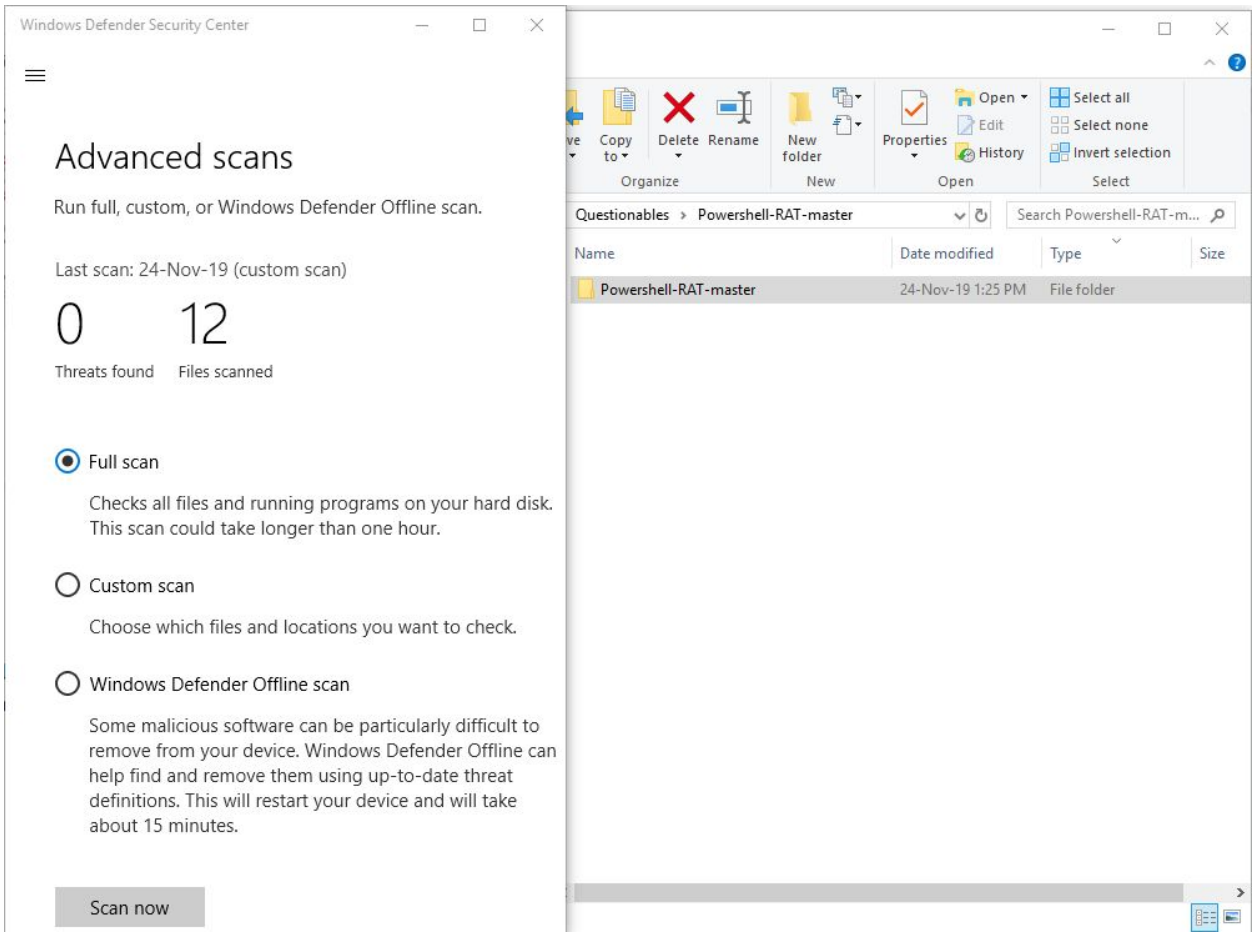

Figure 13: As it can be noted here, the RAT is not detected as a threat by Windows Defender

5. Cyber Kill Chain

A kill chain is a term originally used by the military to define the steps an enemy uses to attack a target. Due to the new arena of cyber defence and attack, Lockheed-Martin, AT&T and some other companies came out with various Cyber Kill Chain models. Lockheed-Martin's cyber kill chain is widely used and accepted. While looking at cyber security, the human side is as important as the technical side. Humans are very easily targeted and are many times the weakest link in the chain of security, as they are predictable and prone to manipulation. Many experts have claimed that the Lockheed-Martin Kill Chain takes this into account as well.

The Kill Chain has 7 stages which an adversary follows to break into a system of networks.

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation

- Command and Control
- Actions on Objectives

The Industrial Control System (ICS) of Kudankulam Power Plant was not breached, if it had been, then that would have been a much more serious issue for the country and the world.

5.1 Kudankulam Power Plant Cyber Kill Chain

This subsection looks at the breach through cyber kill chain. One important thing is that the kill chain can be applied differently, in two ways, in this case. One where the target is compromising the entire plant, and another where the target is gaining command and control over the administrative system and using it to gather information for the former option.

Here we look at the end goal being the compromisation of the power plant:

1. Reconnaissance

It has been established that Dtrack, which was discovered in an admin system was being used for reconnaissance purposes. This is stage one of the kill chain and one of the most important, time consuming and crucial stages.

As one leans more into cyber security, it becomes clear that no system is impenetrable. A secure system is one which is just hard enough to hack that the adversary doesn't do it or doesn't know how to do it. Reconnaissance reveals all of this and much more.

To enter the system, information is gathered passively, and plans are made and it is decided what systems are to be targeted etc. The spywares and remote access trojans are prepared and through various ways delivered to the system for active info gathering.

Through passive information gathering, it is gathered whether the target is a viable one or not, and then through active information gathering technical details about the system are revealed. Here, it is safe to say that Dtrack was put in place as a part of reconnaissance. Finding and mapping out the different users, details about the network, administration and the systems, all of this would be the function of the malware, in this *active information gathering*. Fortunately, Dtrack was discovered and hopefully, the cyber defences of the plant have improved.

However, let's try to explore the possibility that Dtrack was not found, and the later stages were also reached for the sake of this paper.

2. Weaponization

Here the knowledge gained in stage one is put to use specifically to develop and test a meaningful attack against the ICS, in this case the adversary have to have a fair knowledge of how the power plant works. Then, simple interactions with the ICS applications can be a significant risk.

First the attack is developed and tested on identically configured systems and then finalized. Then and only then is this process complete and thus the malware to be used it decided.

3. Delivery

A spear-phishing attack against an employee is the most common way of delivering the exploit and attack code onto the system. To prevent this from happening so easily, critical systems and the ICS are kept air-gapped, that means these systems are physically isolated from the internet and internet connected devices. However, air gaps have been crossed through various interesting ways in the past.

4. Exploitation and Installation

The attack is let to run on the system and it is ensured that the anti virus don't come into play. Various packages to give control and prevent anyone from finding the malware out are put in place.

It is well known that though air-gapped, ICS are not very secure by themselves. Various factors contribute to this, from basic negligence to the fact that there is no streamlined way to keep these systems updates and secure to the latest standards. Moreover, many of the ICS technology used is pretty old comparatively and thus easy to exploit

5. Command & Control

The systems are then controlled remotely by the adversary remotely.

6. ***Actions on objectives***

Once the system is fully compromised and the network is penetrated, then the adversary, knowing the knowledge of how the plant works and the functions of the ICS can cause slight changes in the working.

A very good example of this is the Stuxnet malware which targeted the Natanza facility in Iran. Stuxnet changed the spinning speed of the Uranium rods during the enrichment process which left the machinery useless and also wasted the Uranium. In our context, something similar could be possible, as a nuclear power plant works in an extremely calculated and delicate way, changing some configuration which is not noticeable to us could cause severe damage.

6. Mitigation and Prevention

Critical attacks like these can have disastrous effects on the world economy and lifestyle of people. Hence, facilities and organizations need to be more secure to prevent such attacks from taking place as these could lead to sensitive data being exposed.Measures need to be taken to ensure the security and privacy of such places. These measures could be classified into 2 categories:
Digital and Physical.

- Digital
    - Checking authenticity of suspicious emails.
    - Ensuring the digital ports that are not in use remain closed.
    - Checking systems regularly for malicious files.
    - Keeping the system clean from unnecessary and sideloaded applications.
    - Installing the latest security patches by updating.
- Physical
    - Ensuring the security of the facility/organization by checking who goes in and comes out and their credibility.
    - By not using Pen Drives found in parking lots,cafeteria's on their systems as they gain access to the network by running malicious scripts without the knowledge of the user,these are also known as Rubber Duckies.
    - Making sure that the servers rooms and physical databases are kept secure and no stranger has access to them.

Once installed, a RAT will allow the attacker to watch,listen,record your screen and even alter your personal files.The severity and seriousness of these attacks can be reduced by catching the malwares in your system in its early stages. A system might be affected with a Remote Access Trojan if it's facing unusually slow internet connection,there are unknown processes running in the background,personal files are being modified and removed without the users knowledge and unknown programs are being installed to your system without your permission.
Such attacks can be avoided in the first place by following some basic security steps to make your system secure. These steps include keeping your security software and operating systems up to date with the latest versions so as to help them search your computer for the latest type of viruses,malwares and vulnerabilities. Regularly backing up your data to not lose crucial information in case of an attack and ensuring that the system's firewall is active to monitor and keep in check of illegal traffic in your network. Downloading applications and softwares only from trusted sources so as to reduce the chances of trojans and malwares inside them. Cover your webcam when not in use as one might never know when their system might get compromised and watch the user using their webcam. Avoid clicking of links and opening attachments from spam and suspicious emails from untrusted senders and sources as they might be an attempt to phish out credential and personal information out of the user. Keeping your web browser updated

and configured to alert you whenever a website is trying to download an application in your system or creating a process.

Consider the worst case scenario of a system getting infected with a Remote Access Trojan and what steps should one take further.

If a system is infected with a RAT it can basically be controlled by you and the attacker simultaneously,as the attacker has Remote Access on your device.A user wouldn't notice a RAT as an attacker would only access the system when you are not using it so as to avoid detection.

If a user has a RAT on his system he needs to disconnect his device from the network so as to prevent the malware from spreading to other systems in the network.Install a security software from a trustworthy source and run a full system scan to remove threats found out by the software. Once the user is sure that the RAT has been removed,he needs to change his passwords for his online accounts and check his banking activity.He needs to report any unusual transactions as needed to the bank and law enforcement authorities.The user needs to learn how to protect his system from future infections and avoid data loss.

REFERENCES

1. Outpacing Cyber Threats Alexandra Van Dine | Michael Assante | Page Stoutland, Ph.D. Priorities for Cybersecurity at Nuclear Facilities: https://media.nti.org/documents/NTI_CyberThreats__FINAL.pdf
2. Kudankulam Cyber Attack Did Happen, Says NPCIL A Day After Denial: https://www.thequint.com/news/india/kudankulam-nuclear-power-plant-malware-attack-correct-confirms-npcil
3. Hello! My name is Dtrack: https://securelist.com/my-name-is-dtrack/93338/
4. https://twitter.com/RungRage/status/1188853620541775872
5. https://threatpost.com/north-korea-atm-espionage-malware-dtrack/148602/
6. https://www.orfonline.org/expert-speak/cyber-attack-against-knppp-and-isro-the-threat-comes-home-57700/
7. https://www.freepressjournal.in/india/dtrack-malware-detected-in-18-states-maharashtra-tops-kaspersky
8. https://github.com/Viralmaniar/Powershell-RAT