# *Stuxnet*

*Cyberwarfare: World's First Cyberweapon*

Aaron Khoo

25th November 2023

COMP3123 – Security Project Fall 2023

# Table of contents

# 1. Introduction

Its widely known that a computer virus, a malware designed to damage, corrupt files, and security system of a computer. Similarly, to a biological virus, it could replicate, spread and infect other computers. However, people don't seem to realize how much impact a virus can do until the first cyberweapon is known, Stuxnet, the virus that put-on alert several countries' secret services. This is the first computer virus that could cause physical destruction on infected devices.

Stuxnet is a computer worm that is discovered in 2010. This worm is so complex and sophisticated that took security experts months to examine it. It was written using several Object Oriented Languages and Procedural Oriented Language. This is the starting point where cyber defense was taken really seriously.

Iranian President Mahmoud Ahmadinejad pays a visit to Natanz's nuclear facility on April 8th, 2008. Photos were taken and published on a public website. Those photos revealed crucial information of the nuclear facility structure that are responsible for the production of uranium.

*Figure 1 shows President Ahmadinejad in Natanz.*

The rapid development of uranium enrichment program raises concerns as it could potentially lead to producing nuclear weapons. It was obvious that Iran's nuclear program doesn't comply with safety measures, and this result in the creation of Stuxnet.

## 2. Initiation

The nuclear facility of Iran is located in Natanz, capital of Iran. To keep their facility safe, they use an air-gapped network. An air-gapped network isolates themselves from any unsecured network such as the public internet, made it impossible for any unauthorized users to the network including data transferring and communication. Any user wouldn't be able to connect to their network remotely unless connecting physically to their computer. Hence, the name "air-gapped" as its protected and isolated by air.

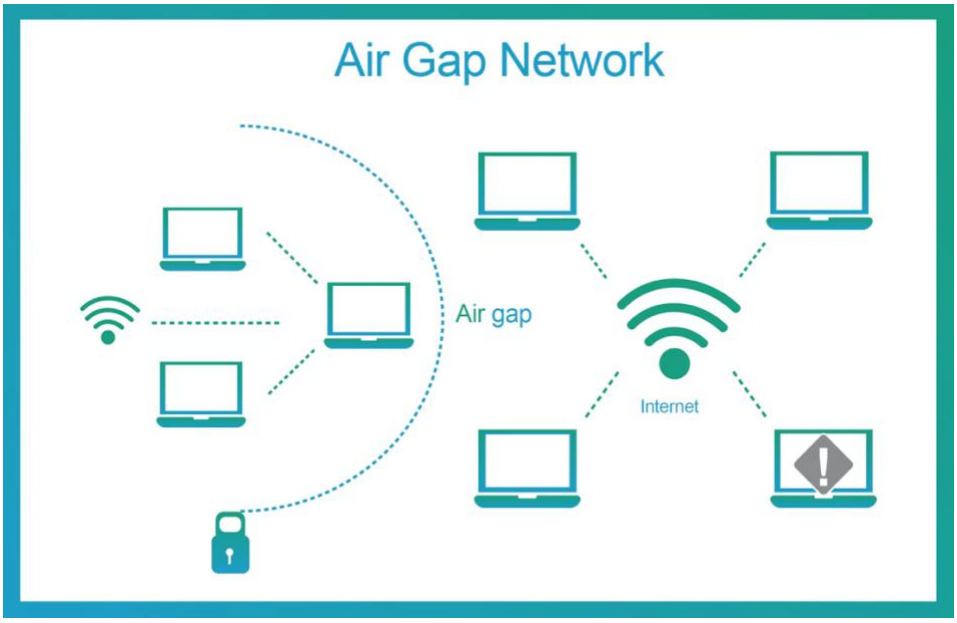


*Figure 2 shows an air-gapped network connection compared to public network connection.*

Since there's no way of intersecting an air-gapped network, they targeted 4 major companies that cooperate with the nuclear facility. "Human Assets" are used to release the worm. Once the worm infected a device, all it needs is to wait for a maintenance agent/engineer to enter the facility and connect the device to the network. Stuxnet could even infect devices that are not connected to the Internet. It could be as easy as plugging in a USB drive into the device, and the virus will begin spreading.

## 3. Execution

Once Stuxnet successfully gotten into the facility, it didn't execute immediately. Stuxnet was carrying a payload and will only execute its payload once it reached its target destination. A payload contains the core code to be executed. In other words, a payload is the one that causes damage and carries out attacker's objectives. With that being said, the moment the virus is released, it jumps from device to device in search of its target and it won't stop until it reaches its destination.

Stuxnet was searching for a specific system, Programmable Logic Controllers (PLC), a computer used to control, monitor, automated process such as motor speed, conveyors and offers real-time control. The features this computer holds makes it the perfect target to infect.


*Figure 3 Programmable Logic Controller*

## 3.1 Exploits and Vulnerabilities

The PLCs used in the facility are Siemens PLCs and runs on Windows operating systems. Stuxnet used 4 zero-day exploits and 1 Siemens PLC vulnerabilities:

a. Windows LNK Vulnerability (CVE 2010 2568):

A shortcut file created by windows at that time used ".lnk" extension on them. These LNK files are used as "shortcuts" when user tries to open a file. Opening files with LNK extension granted the attackers privileges same for the users, triggering the vulnerability. Upon granting privileges, attacker could execute the malicious code.

b. Window Spooler Vulnerability (CVE 2010 2729):

This vulnerability ( a.k.a print nightmare ) works when printer sharing is enabled, the spooler activities fails to restrict where users have access to. Any authenticated users that are granted access have the privilege to do whatever they pleased. Since the authentication process is not strong, any authenticated users could escalate their privileges and input any files they want. In this way, attacker could create files and execute code consequently, they could potentially made it that whenever a file is open it runs the malicious code.

c. Windows RPC Vulnerability (CVE 2010 2772):

This vulnerability take advantage on hard-coded password that connects to the back-end database. Once obtaining the unencrypted passwords, attackers could gain access to the database easily.

d. Microsoft Security Bulletin Vulnerability (CVE 2010 3889):

This vulnerability allows remote code execution when windows open a faulty request. Once the request bypasses the authentication process, the attackers doesn't need any further authentication the next time attackers wants to run the malicious code.

e. Siemens Vulnerability

This vulnerability allows Stuxnet to gain control over PLCs Step7 software and manipulate almost all kinds of request sent to other device.

## 3.2 Concealment

Upon reaching this system, Stuxnet installed two kernel mode drivers, one for running Stuxnet, another as a rootkit for concealment. Rootkit, a malware once installed in a device, would allow unauthorized access for attackers and gain control of the device while still being hidden from detection. Rootkits are usually installed in hidden or backend mode where users are unable to locate them. For example, kernel mode has the highest privilege among the system, this makes it the perfect place to conceal as user doesn't have direct access to it.

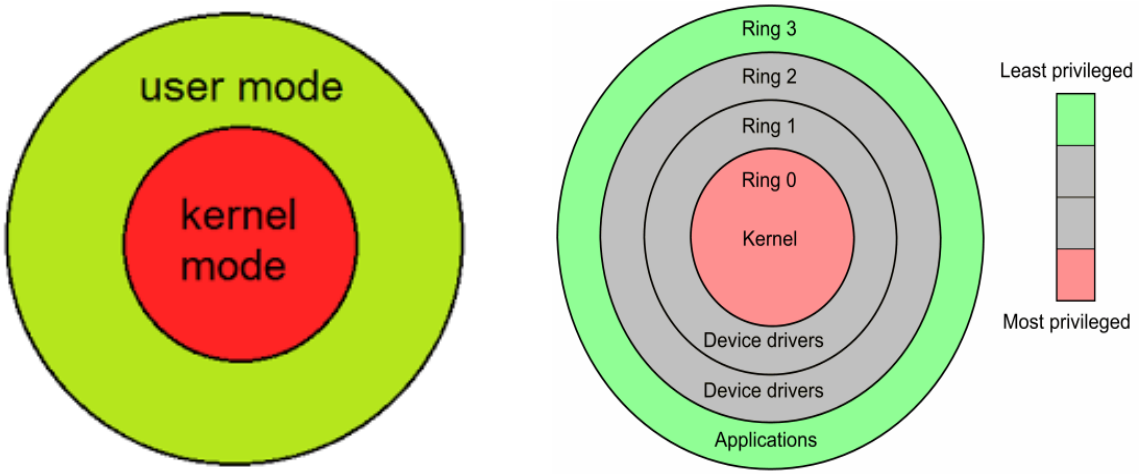


*Figure 4 shows user/kernel mode and levels of privileges*

Not only did it hide itself, Stuxnet is able to manipulate requests sent to devices. This is made possible when Stuxnet infect Step7 projects, a programming software used to control PLCs, it inputted malicious code and gain control of these devices.

Stuxnet also installed two drivers files known as Mrxcls,sys and Mrxnet.sys:

a. Mrxcls.sys

   This file contains malicious code that gain control over the core operation of PLCs, this allow all manipulation of the PLCs machine.

b. Mrxnet.sys

   While Mrxcls.sys focus on control, Mrxnet.sys focus on filtering request sent. It was known as this files act as a system filter driver.

Both drivers' installation goes unnoticed, this is because both drivers are signed by Realtek Semiconductor Corporation. They used stolen digital certificates to avoid suspicion.

This is the core part of concealment as it responsible for updating the centrifuges condition to the display screens that are monitored by nuclear scientists.

## 3.3 Attack

It’s important to know that centrifugal motors have a certain rpm limit within which they can operate safely. The code inputted into the PLCs consist of 3 attack phases. First phase being manipulating the speed of the motors to rotate at very high speed. Second phase being manipulating the speed of the motors to rotate at very low speed. Third phase was known to never executed. All attack phases are made to cause explosion of the centrifuges in the facility.

At the meantime, when the motors are manipulated to spin at very high or very low speed, the statistical data displayed on the monitoring device are also altered to past data that are shown a few weeks ago. This fools the nuclear scientist and the engineers that everything is working as intended.

Centrifuges explosions happen from time to time, and scientist struggles to identify any faults in their centrifuges system. One thing worth mentioning, PLCs are built with safety precautions that runs a safe shutdown, Stuxnet can manipulate that safety precaution and interrupts the safe shutdown, causing it to explode. Stuxnet is also capable to schedule different attacks to prevent continuous explosion and suspicion. This causes several scientists got fired as they’re blamed for the centrifuges explosion.

Stuxnet have all the logic, steps, deciding factor and execution steps all programmed in it. Making damage almost one fifth of Iran’s total centrifuges. Nobody is able to figure it out what’s happening for several years.

Stuxnet is the first cyberweapon to be known, having complex structure, multiple languages written in it, logic, deciding factor and execution steps all programmed in it

# 4 Risk associated.

Once Stuxnet is released, there's no way it can be retrieved. The creators want a way to be able to monitor and track its progress. Since Natanz uses an air-gapped network, it would be useless to have a Command-and-Control Servers (CC servers). A CC server are servers that allow an attacker to communicate with the malware. This way an attacker receives feedback and send commands to the malware.

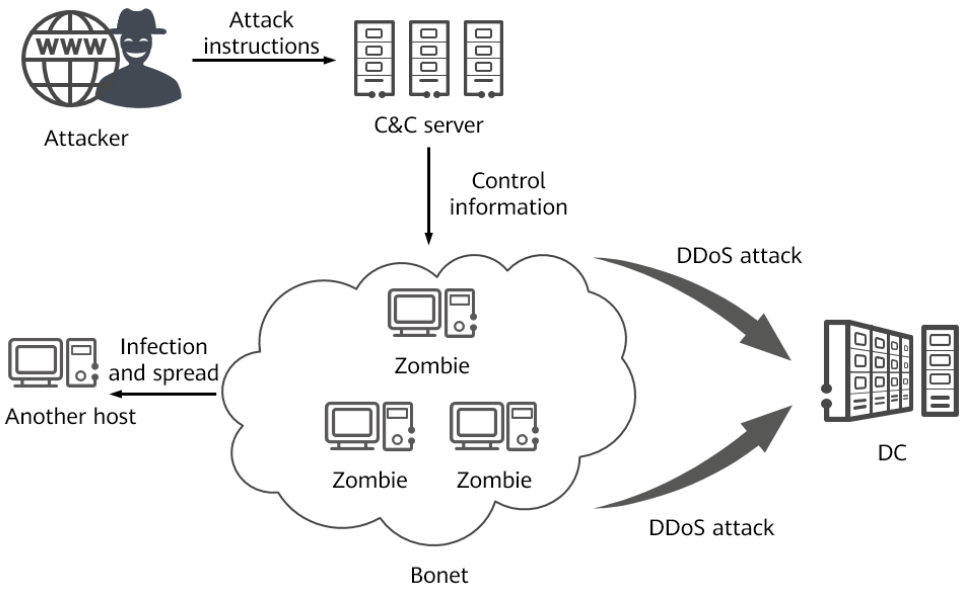


*Table 1 shows attacker gain control of botnet and remotely control it to execute actions.*

This raises questions about why Stuxnet have a CC server. The creators have foreseen this issue and implement a CC server in Stuxnet. Instead of monitoring and tracking how Stuxnet is doing, they bring newer version to Natanz for Stuxnet to update itself. They used "human asset" to deliver the newer version to Natanz. Every new version can make Stuxnet operate differently, it could make it more aggressive and more destructive. Having a CC servers made this possible.

Other reasons why Stuxnet have a CC server:

a. Kill Switch

This act as a detonator to destroy evidence and avoid unwanted attention to the creators.

b. Version Control

This allow Stuxnet to update to its latest version, allowing creators to control what Stuxnet should do next.

c. Tracking

Allows creators to make future decision on what it should do next.

## 5 Discovery

Stuxnet was originally made to target Iran enrichment uranium facility. Its purpose is to limit the rapid development of nuclear weapons in Iran. Due to the nature of worm's viruses, it infected a significant number of computers in Iran including their neighbour countries. The creators weren't satisfied with the results, they tried modifying the code and causing it to be more aggressive. This aggression led to Stuxnet started infecting device outside Natanz. Over 20,000 devices are infected in Iran alone, a significant amount of device are also infected in Iran's neighbouring countries.

It was an antivirus company that brought Stuxnet to light. On a regular day, a cybersecurity engineer notice something unusual about his laptop, constantly rebooting. Initially, they thought it has something to do with fault power supply or Windows bug update, but even restarting windows, the issue is still there. One thing led to another, security expert found there's a file that wasn't supposed to be in there, and it was almost all of the devices have similar issue have the same file installed. After thorough investigation, they're able to locate the origin of the virus.

## 6 Mitigation

The unprecedented of technology raised concerns on cyber security for every technology there is. A hacker once said, “Every device can be hacked”. It’s crucial to have tight security when it comes to protecting sensitive information and any business companies.

In my opinion, have tight security on authentication, authorization and proper security checks or monitoring procedure are the most crucial aspects in cybersecurity. Think of a house protecting someone inside, attackers have many ways of entering your house. A friend who is sick got his virus spread (Worm virus), giving presents that serves other purpose (Trojan horse), a robber acting they’re hurt and asked for your help (Adware), a group of people rushing through your place (botnets) and many more.

- Layering security
    - Firewall

      Firewall monitors and records all incoming and outgoing traffic based on a set of conditions; incoming traffic will have to pass all conditions for it go through. Adding more tighter conditions to prevent possible penetration attack.

    - Multi-factor authentication

      As the name suggests, the layering technique authenticate users twice. This authentication uses multiple accounts to verify the user making it more secure.

    - Web content filtering

      A method that monitors and blocks access to certain websites according to a pre-set rule. This practice is a must have for organization and businesses to prevent people who don’t have authorization to access certain places.

    - Managed detection and response

      This is a service provided by a third-party member that monitors and improving the structure of your security network.

- Application security
    - Encryption

    A way of rearranging data and changing how the data is shown and stored. Cryptography is the science behind encryption. The encrypted data are always unreadable by the human naked eye, it requires a specialized decryption to get the data. This is done to protect sensitive information and private data.

    - Static application security

    A method practiced to examine the application source and its vulnerabilities. This reduce the risk of any cyberattacks and detect vulnerabilities earlier.

- Network security
    - Remote Access VPN

    Remote Access Virtual Private Network allows user to connect to a network with a private connection. Think of a main big road entering a building, and a tunnel who can only fit one car going in the building at the back. Remote Access VPN is the tunnel created for a private connection. Since its private, all traffic and request sent are all encrypted. This benefits applications that are geo-blocked and also enhanced privacy.

    - Sandboxing

    A technique used to separate process in an isolated environment and experiment anything there. It works by creating a container, a virtual machine, and test everything in that container. A container is completely isolated from a operating system. Think of container as in two disk, one for MacOS, another one for WinOS.

    - Network segmentation

    A technique that divides a computer network into smaller network, similar to trees growing branches. This method is used widely as each network separated have their own security control and firewalls. This allows better access control.

## 7. Conclusion

Stuxnet was discovered in 2010, assuming it development started during 2005, that was more than 10 years ago. In the modern days, it's safe to say there'll be more powerful and capable malware out there. Such sophisticated malware would require a nation resource to build it. If Stuxnet wasn't discovered, it could potentially deal greater damage and people wouldn't know about it. It's the first cyberweapon publicly known to have such capabilities to create physical destruction. Stuxnet's success serve as a wakeup call to the world on what a malware is capable of, at the same time, Stuxnet existence inspired cyber criminals to develop their own version of malware which potentially led to an outburst of illegal cyber activities in the future.

Ever since Iran encounter with Stuxnet, they have significantly strengthened their cyber defences. They invested a ton in improving their cyber defences. They even built their nuclear facility so deep underground that any air strikes wouldn't destroy it. Besides, Iran also cooperates with other countries who share similar concerns in cyber dominance.

Stuxnet marks a historic event in cybersecurity history, a pivotal point in making cyberattacks more popular and shaping the evolution of global cybersecurity strategies.

References


1. Stuxnet attackers used 4 windows zero-day exploit

https://www.zdnet.com/article/stuxnet-attackers-used-4-windows-zero-day-exploits/

2. Microsoft .LNK Vulnerability

https://www.cisa.gov/news-events/alerts/2010/07/16/microsoft-windows-lnk-vulnerability#:~:text=By%20convincing%20a%20user%20to,sufficient%20to%20trigger%20the%20vulnerability.

3. Windows Spooler Vulnerability (CVE 2010 2729)

https://www.papercut.com/blog/print_basics/windows-print-nightmare-explained/

4. Windows RPC Vulnerability (CVE 2010 2772)

https://www.akamai.com/blog/security/critical-remote-code-execution-vulnerabilities-windows-rpc-runtime

5. Microsoft Security Bulletin

https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-027

6. Serious security holes found in Siemens control system targeted by Stuxnet

https://arstechnica.com/information-technology/2011/08/serious-security-holes-found-in-siemens-control-systems-targeted-by-stuxnet/

7. What is Cybersecurity

https://www.comptia.org/content/articles/what-is-cybersecurity

8. Types of Cybersecurity

https://www.sailpoint.com/identity-library/five-types-of-cybersecurity/