IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review on two dangerous cyber-attacks in the world

[1]Torpunuri Rohit Simha

[1]Student
[1]Department of Computer Science
[1]Vardhaman College of Engineering, Hyderabad, India

Abstract: There is a threat of cyber attacks all over the world. We are highly prone to these cyberattacks every day. It is possible that these cyber tools can be used as weapons and target specific machines on a large scale. They are also called cyberweapons and this phenomenon is called cyberwarfare. In this paper, we discuss about cyberweapons and also explain about a cyberweapon called 'Stuxnet' that has been used to damage Iran's nuclear power plant. We will also discuss about 'Industroyer' which is also a virus that caused a lot of disturbance in Ukraine.

***Index Terms* - Cyberattacks, Stuxnet, Industroyer, cyberweapons.**

Introduction:

A cyberattack is a kind of invasion and an intrusion into the computer to disrupt its infrastructure, networks and devices. These attacks are usually employed by unknown individuals and groups to fulfill certain objectives which could be illegal. By 2022, the amount spent on cybersecurity is forecasted to reach to $133 billion. According to cybint solutions, in 2018, 60% of the business experienced cyberattacks (mainly phishing). The Data breaching which happened in 2019 leaked about 4.1 billion records which indirectly portraits that the data is not protected. By 2020, the estimated number of passwords used by humans and machines would grow upto 300 billion. There are about 715,000 cybersecurity workers employed by US alone. According to sources, there is a cyberattack every 39 seconds and an average of 75 records are stolen every second. There are about 444,259 ransomware attacks that took place in the year 2018.All such attacks could range from hacking of a personal computer to disrupting power of the entire nation. In this paper, we will discuss about some large scale attacks that took place in the world and also describe about the cyber weapon responsible for it. A cyberweapon is a special malware agent that is employed to accomplish certain objectives (parliamentary, military and intelligence). These cyberweapons are used as a substitute of a spy or a soldier for a task. In general cyberweapons could infect, disturb and destroy all the sensitive and critical parts of the country's systems such as electric power supply grids, systems for territory controls, hospitals and government controls, communication networks and defense systems. We are all in cyber era and the cyberwar are fought without any rules. We are not sure how much does a cyberweapon cost or in other words what is the development cost of such cyber weapon. Here is the estimated value provided by Charlie miller.

JOBS	UNITS	COST
Vulnerability analysts	10S,10J	$2.9million
Exploit developers	10S,40E,20J	$7.3million
Bot collectors	50S,10J	$4.15million
Bot maintainers	200S,20J	$12.9million
Operators	50S,10J	$5.4million
Remote personnel	10S,10J	$400,000
Developers	50S,20J	$2.85million
Testers	10S,5J	$800,000
Technical consultants		$2million
System admins		$500,000
Manager	52	$$6.2million

Fig 1: cost estimation for creating a cyber weapon (Charlie miller)(J=junior,S=senior)

Cyberweapons consists of three components: propagation method, payload and exploits. Absence of any one of these would deny the fact that it is a cyber weapon. There are many cyberattacks that happened till the day. It is said that United Nations infected the pipeline control software of Soviet Union. According to REED the pipeline software responsible for running pipelines and valves was programmed to reset pump speeds and valve settings to produce lot of pressure. This led to the larget non-nuclear explosion which could be seen from the space. In 2013 Spamhause experienced the largest DDOS attack in the history. Similarly, there are many cyber-attacks that had an impact on the nation in a large scale. In this paper we shall discuss two of them in detail.

ANATOMY OF STUXNET:

Stuxnet is a computer worm which was discovered in 2010. Stuxnet is designed to target SCADA systems which were responsible for operations in the nuclear power plant of Iran. Although there are certain conspiracies that this cyber weapon was created with collaboration of the US and Israel to stop the nuclear program of Iran, But there is no solid proof for that. Stuxnet has three components a worm, a link file and a rootkit. The Share of computer infected by Stuxnet in Iran was about 58.85%.Stuxnet is designed in certain way to fulfil its purpose step by step:

1. Stuxnet is injected in a windows system using a USB pretending that it has a reliable digital certificate.
2. This virus then checks weather the given machine is a part of targeted industrial control system
3. If the system isn't the targeted one it leaves it. but if it is the one that it is searching for it downloads the latest version of itself.
4. The worm compromises over the target system and then takes complete control.
5. Finally, by taking control it makes the centrifuges spin in an abnormal way thereby damaging them. Also, it hides its presence by providing false feedback to the outside controllers.

Stuxnet was injected into the network using a USB. Its work was to first find simens step 7 software that controls PLC (programme logic control). Stuxnet not only infected Iran's nuclear power plant but also infected many other countries. The following table shows the share of computers of the countries infected by Stuxnet.

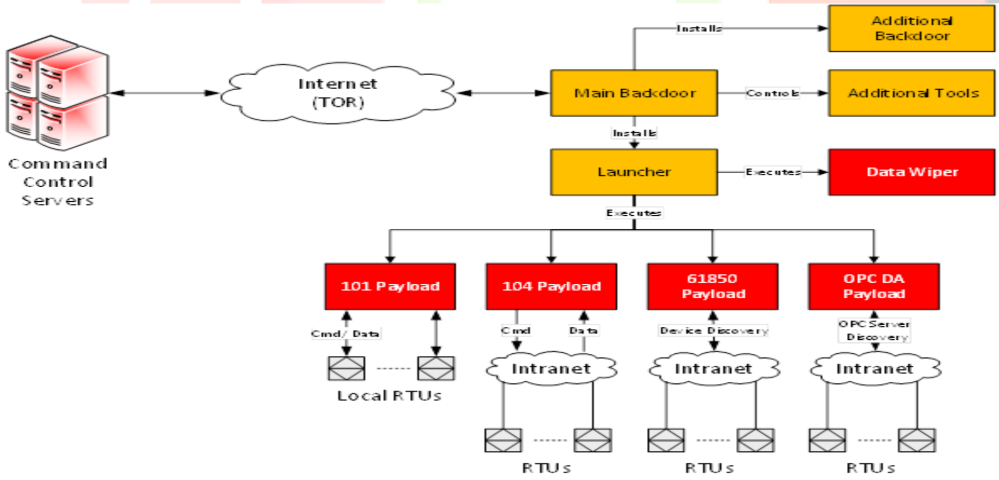
Country	Percentage of infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
United states	1.56%
Pakistan	1.28%

Fig 1: Share of computers of the countries infected by Stuxnet.

According to a report, it was planned to create disturbance even in North Korea's nuclear power plant. But, due to extreme security and secrecy it was impossible for the virus to be introduced in its power plant. Stuxnet damaged about one-fifth of Iran's centrifuges. It was estimated that the cost of making Stuxnet was just $1 million US dollars although it could cost way more. Stuxnet created a huge impact in Iranian society and politics by making it look weak and prone to any problem as its infrastructures were not strong enough to protect their systems with such cyber-attacks. Similarly like Stuxnet there was another type of cyberattack that happened in Ukraine.

ANATOMY OF INDUSTROYER:

Industoyer (crashoverride) is a cyber weapon which was used to disrupt Ukraine's power grid on December 17, 2016. This virus consists of a main backdoor, an additional backdoor, a launcher component, four payload components andata wipER



.

Fig 2 components of Industroyer

This virus is capable of controlling electricity substation switches and circuit breakers. For doing that it uses all industrial communications protocols which are used in power supply, infrastructure, and transportation control system. Cybersecurity firm Dragos named the malware "Crashoverride ". Many researchers say it can automate mass power outages, it includes flexibly swappable components that could allow it to adapt in any electrical environment, it can be easily reused and launched simultaneously to infect and disrupt multiple targets. Researchers also say that the blackout that occurred in Ukraine (1hour) was just a sample as the blackout time could increase. This malware targets the Siemens spirotee digital relay. When the malware finishes its job, it erases its presence by overriding a large number of critical files on the disk of the infected machine and changing the image path thereby not allowing the system to reboot. It attacks based on security weaknesses. It contains DOS tool in it that exploits the CVE-2015 5374 vulnerability in Siemens SIPROJECT devices and render target. The 2016 attack on Ukraine's power grid deprived part of its capital, Kiev of power for an hour. Andrew Clarke said "We are not talking about stealing information or pictures from a cloud storage location. This is about taking control over the power grid. It actually means that a hospital could loose power during a surgery or traffic lights would stop working which would lead to accidents". The Ukraine government blames Russia for this but Russia denies to take responsibility for it. The adaptable features portrait that the malware not only can cause threat to Ukraine's power grids but also to power grids of many nations including America and china. No one clearly know how it infected the system, but, once the windows machines are infected the virus maps out control system and finds the target equipment. It has the potential to record all the network logs and send it back to the operators which would allow them to understand and learn the functions and procedures of the control systems. Both crashoveride and stuxnet are considered to be written by very intelligent people as its code is very complex and highly robust. It is also believed that this is done for a particular objective which could be testing or damaging the economy and power of other nations.

SUMMARIZING AND COMPARING STUXNET AND INDUSTROYER:

STUXNET	INDUSTROYER
• Damaged the centrifuges in Iran which caused disturbance in Iran's nuclear program.	• It is also referred as crashoverride.It was responsible for the black out that occurred in capital of Ukraine
• Stuxnet consists of three main components • A worm • Link file • Rootkit	• Industroyer consists of • main backdoor • additional backdoor • launcher component • four payload components • data wiper
• It was designed to target Siemens industrial control systems and contains specialized malware payload that targets supervisory control data acquisition.	• It targets Siemens pirotee digital relayand it also contains payloads that are very flexible and adaptable
• Stuxnet was original written in c, c++ and other object oriented languages.	• 4. Industroyer was written in many different languages mainly c++.
• The core purpose of this virus sabotaging the high frequency convertor drives used by uranium enrichment facility.	• 5. The purpose was to attack the power grids of the station.
• 6. It contained a time stamp long before the attack. It entered into a system using USB flash drives	• It also contains activation time stamp of Dec 17 2016 which was the date of power outage.

CONCLUSION:

These two viruses have impacted the two nations on a large scale. The cyberweapons proved their power through these two case studies. There might be stronger and more complex weapons which are unused and unknown to us. Although cyber security companies are trying to build a complex and robust infrastructure for such type of attacks, we are not sure that these security walls are enough. Stuxnet almost infected 200,000 computers and crashoveride successfully could shut down the power supply for an hour. We do not know how many cyberweapons exist in the world. All we know is they exist and are being created secretly using very intelligent and professional people in the world. Cyber security is very important concept in today's world and is going to be the priority of every individual as all of them are associated with this digital world and their data is being completely recorded.

REFERENCES:

1. Stevens, Tim. (2017). Cyberweapons: an emerging global governance architecture. Palgrave Communications. 3. 10.1057/palcomms.2016.102.

2. Baezner, Marie & Robin, Patrice. (2018). Stuxnet.

3. Denning, Dorothy. (2012). Stuxnet: What Has Changed?. Future Internet. 4. 672-687. 10.3390/fi4030672.

4. Stevens, Tim. (2017). Cyberweapons: power and the governance of the invisible. International Politics. 10.1057/s41311-017-0088-y.

5. Bendovschi, Andreea. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance. 28. 24-31. 10.1016/S2212-5671(15)01077-1.

6. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

7. https://www.zdnet.com/article/industroyer-an-in-depth-look-at-the-culprit-behind-ukraines-power-grid-blackout/

8. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

9. https://cyber-peace.org/wp-content/uploads/2017/06/Industroyer_-Biggest-threat-to-industrial-control-systems-since-Stuxnet.pdf

10. https://www.cybintsolutions.com/cyber-security-facts-stats/