MUNESCO

Forum: GC5- Communication and Information

Issue: Reforming cyber security policies with a special emphasize on open source viruses such as stuxnet

Student Officer: Derin Karzan

Position: Deputy Chair

Introduction

From the time that technology entered in people's life so has the negative sides of technology. Firstly it started with basic systems but within the progress of technological devices and especially computers, the negative sides referred to as computer worms and viruses progressed proportional with it. Because of the progressing viruses and computer worms the concept of Cyber Security was created.

However, whether cyber security present or not viruses and computer worms have not stopped. For example the creation of Stuxnet.

Definition of Key Terms

Cyber Security: Computer, network, program, and data protection techniques against unauthorized access or exploitation.

Stuxnet: Stuxnet is a highly mature computer worm that uses many previously unknown Windows security vulnerabilities to infect and spread computers.

Computer Worm: Self-replicating malware to propagate itself to uninfected computers.

Virus: Designed to spread from the host to the host and has the ability to replicate itself. Similarly, computer viruses can not spread and spread without programming like a file or document, such as the inability of viruses to replicate without a host cell.

Flame: A very sophisticated, malicious program that uses many organizations in many countries actively as a cyber weapon.

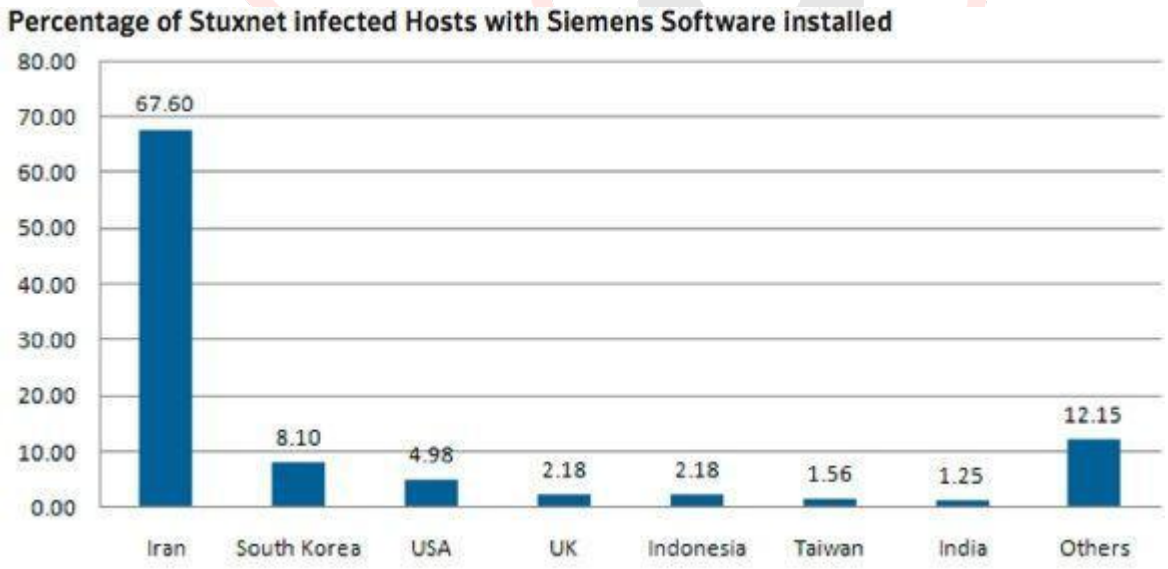
Gauss: Gauss was cut from the same side with Flame malware spreading to Iran and the Middle East earlier this year, and reminiscent of the infamous Stuxnet worm.

Computer Firewall: A firewall is a system designed to avoid unjustified access to or from a private network.

Background Information

Stuxnet is the world's first accepted cyber weapon, designed to find and destroy a physical target autonomously. As the researchers began to notice the magnitude of the program in which they had fragmented their pieces, the world of security overtook the storm of discovery. Previously, attacks and exploits had predictable goals: information or profit was an unmatched feature of Stuxnet, the sole thought to cripple the physical infrastructure, and used techniques that were never seen before to do it. There are amounts of evidences to suggest that the targeted systems are Iranian uranium enrichment cascades in the Natanz compound, but the virus appears to lack about 1,000 centrifuges (which is critical for Iran's uranium enrichment process), but the gap. Thus, when Stuxnet did not meet Iran's ultimate goal of stopping its nuclear program, researchers were quick to observe that not seeing the end of the Stuxnet-based code.

Variants of Stuxnet usually appeared in the form of discovery, but other variables such as Gaussian and Flame emerged even after Stuxnet broke up in 2012. Even more disturbing is the list of potential destinations where Stuxnet's source code can be found easily. The public and private infrastructure is one of the goals that Stuxnet could initially cripple a nation if technologically connected, electricity networks, communications networks and public facilities, if an entrepreneurial group or individual were to determine their intentions to rebuild Stuxnet. The cyber battlefield itself is a consequence of Stuxnet (many of the earlier efforts fall into the "Intelligence" category) and in the post-Stuxnet era, nations (especially Iran) are collecting groups of hackers and the programmers.



Cyber security

In today's digital world, computers have become the main way for most people to communicate with each other and interact with each other. Whether connected via email or social networks, a world without

a PC has quickly become unthinkable. Business transactions, storage of personal information, transmission of confidential information, and a number of other information flows occur through computer networks. While technology has made the world a smaller space, it has also caused problems with data security or cyber security issues.

Cyber security protects systems, networks and programs from digital attacks. These attacks are usually aimed at accessing, altering or destroying sensitive information; Forced withdrawal from users; or disrupt normal business processes. Implementing effective cyber security measures is a particularly challenging issue today; because there are more devices than humans and the attackers are becoming more innovative.

Cyber security approach has multiple layers of protection between computers, networks, programs, or data that want to protect security. In an organization, people, processes and technology must complement each other in order to create an effective defense against cyber attacks.

Timeline of Major Events

Date	**Event**
2005	Oldest known version of Stuxnet
July, 2009	Serious Natanz nuclear incident, Iran's Atomic Energy Authority resigned for unknown reasons
March, 2010	2nd version of Stuxnet created
November, 2010	Iran learns they were hit by the virus Stuxnet
2012	Stuxnet self-destructed

Major Countries and Organizations Involved

Iran

Stuxnet attacked five times to Iran organizations. Symantec's researchers described malware as a targeted attack on five networks in Iran.According to the companies, organizations were hit in five separate attacks during 2009 and 2010. Three of these organizations were targeted once, one was twice, and the other three times.

United States of America

The Stuxnet computer worm, which destroyed the centrifuges in Iran's Natanz uranium enrichment area, was only one element of a larger US counter-offensive plan to target Iran's air defenses, communications systems and key parts of the electrical network.

Israel

Stuxnet, a computer virus was developed, claimed by Israel and the United States. Years ago Israel and the United States of America made a joint to bomb Iran's nuclear program.

Previous Attempts to Solve the Issue

Iran

Iran insisted that Stuxnet had infected personal computers of employees at the Bushehr nuclear power plant, but that the bomb was not infecting the working systems involved in the nuclear program and that the program had not been harmed. Officials did not mention whether or not any viruses in the Natanz nuclear facility were infected. Natanz is trying to enrich uranium, which can be used to produce weapons. For this reason, various computer security experts believed that Stuxnet was a possible target.

Possible Solutions

- Access and password control
- Isolate command and control networks from public networks which are accessible by everyone
- Ensuring anti-virus software is up to date
- Utilizing firewalls to secure networks
- Examine internet downloads

Useful Links For Further Research

http://bhconsulting.ie/computer-security-threats-solutions/

https://usa.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

https://www.wired.com/2010/11/stuxnet-sabotage-centrifuges/

https://cybersecurityventures.com/cybersecurity-associations/

https://www.backgroundcheck.org/what-you-should-know-about-cyber-security/

Bibliography

"The Four Amigos: Stuxnet, Flame, Gauss and DuQu." *Concise Courses*, 11 Sept. 2017, www.concise-courses.com/stuxnet-flame-gauss-duqu/.

Kelley, Michael B. "The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought." *Business Insider*, Business Insider, 20 Nov. 2013, www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

Erik Eckel in 10 Things, June 19, 2009, 4:28 AM PST. "10 Ways to Avoid Viruses and Spyware." *TechRepublic*, www.techrepublic.com/blog/10-things/10-ways-to-avoid-viruses-and-spyware/.

"'Israel's Rash Behavior Blew Operation to Sabotage Iran's Computers'." *The Jerusalem Post | JPost.com*, 16 Feb. 2016,

www.jpost.com/Middle-East/Iran/Israels-rash-behavior-blew-operation-to-sabotage-Irans-computers-US-officials-say-444970.

Dan Goodin - Feb 17, 2016 1:26 am UTC. "Massive US-Planned Cyberattack against Iran Went Well beyond Stuxnet." *Ars Technica*, 16 Feb. 2016,

arstechnica.com/tech-policy/2016/02/massive-us-planned-cyberattack-against-iran-went-well-beyond-stuxnet.

Fruhlinger, Josh. "What Is Stuxnet, Who Created It and How Does It Work?" *CSO Online*, CSO, 22 Aug. 2017,

www.csoonline.com/article/3218104/malware/what-is-stuxnet-who-created-it-and-how-does-it-work.html.