StruxNet: The World’s First Cyber Weapon

Austin Johns

ITT-306

Professor Kris Peters

3 April 2021

**Part 1 – Discovery**

1. According to the interviews shown in the video “The Truth About Cyber Warfare” the U.S. and Israel were the major actors behind Stuxnet. What evidence was used in this cybercrime/cyber war research to implicate the U.S.?
   1. No resource.
2. Define the following terms and explain how they relate to Stuxnet: Worm, Air Gap, Fire and Forget, Zero Day Exploit, WinCC, PLC, and Centrifuge.
   1. Worm: Struxnet is a worm virus, meaning that it replicates itself to be spread to other computers. Every worm has different purposes to hackers.
   2. Air Gap: Struxnet used an air gap in a network system to sneak into the server’s access.
   3. Fire and Forget: Struxnet used fire and forget to write to a system without any prior transaction between the computer and the target drive. In other words, Struxnet was able to write to the drive without raising any alarm.
   4. Zero Day Exploit: The exploit in this case was the air gap in the network. Through this air gap, Struxnet was able to take advantage of a small opportunity window.
   5. WinCC: This is a type of supervisory control and data acquisition system that was attacked by Struxnet. By attacking this system, Struxnet was able to control the influx of data to manipulate any kind of data-based calculations.
   6. PLC: PLC is a type of worm. In this case, Struxnet is a PLC worm, meaning that the worm was implemented through the network.
   7. Centrifuge: This is an index that includes arbitrary sequences. These sequences can cause a domino effect, meaning that if there is an altercation to this data, changes may cause effect elsewhere in a system. In the case of Struxnet, the centrifuge was located on an engineer’s computer that was infected with the worm.

**Part 2:  A New Type of Warfare**

1. If the United States is the designer and instigator of Stuxnet, there are at least two different viewpoints. For each of the following statements, express the opposing viewpoint’s likely counterarguments:

**Viewpoint 1** – The U.S. was reckless and provocative. The United States was reckless in creating a new category of warfare by releasing Stuxnet. They have crossed the line. Since Stuxnet creates physical damage to its victim, it is similar to dropping a nuclear bomb in WWII. The world has changed for the worse and the US should be blamed for putting us all in greater danger.

Counterarguments:

1. As technology evolves, the United States needs to be at the forefront of advancements, not just to be defensive, but to have a head up on the offensive..
2. The public enemies would have figured out the same thing eventually, so why not be the first?
3. National security has no price. The United States should do anything to protect the country (Radical conservative).
4. The risks of the actions of the United States is justifiable because the safety of the country has no price.
5. The opposing country did us wrong, and they deserve the attack.
6. In any war, whether physical or cyber, there will always be collateral damage (again, radical conservative, not my beliefs.).

Contrary Response: What would a contrary opinion say about this charge?

**Viewpoint 2** – The U.S. was precise and restrained. Iran has declared the destruction of Israel a national priority and sponsored attacks to do so. The U.S. and Israel, in trying to prevent Iran from developing a nuclear weapon, choose to utilize a relatively non-destructive method to disrupt uranium purification. The alternatives to Stuxnet, such as air strikes, special forces, or a ground invasion which would kill people, cause economic damage and political chaos. The U.S. should be *credited,*not criticized, for utilizing a restrained approach in trying to stop a nuclear war.

Counterarguments:

1. There should be more peaceful ways to solve these types of problems.
2. By creating this technology, we have created a new way of war, and this should be protected rather than used.

Contrary Response: What would a contrary opinion say about this charge?

1. How does the use of Stuxnet compare with the use of nuclear weapons? Write a complete answer showing the similarities and differences.
2. What arguments say that U.S. was justified in using nuclear weapons against Japan? What are the criticisms?

**Part 3: Malware Analysis**

1. In a few sentences, summarize the processes of how Stuxnet works. More specific information will be discussed in a later question.
   1. Struxnet is a PLC worm that was directly targeted towards computers that control the machinery that created nuclear weapons for Iran. For Struxnet to work as intended, there are multiple steps that must be completed. To begin, the worm needs to infect the windows system of the host network. This was done using an air gap in the network that connects to an engineer’s computer. Next, the worm was injected into different parts of WinCC, which controls much of the data management of Iran’s nuclear plant. After this, the worm infected the PLC, meaning that the worm took place on the network of the devices being used. By doing this, the network was damaged, the machinery was damaged, and there was farther physical damage.
2. According to the video “The Truth About Cyber Warfare,” explain why the Stuxnet attack was not effective?

**Part 4: Consequences and Conclusion**

Near the end of the movie “The Truth About Cyber Warfare,” the experts comment on weapons treaties that were negotiated in the 20th century. What does the movie suggest for how we handle the use of cyber weapons in the future?

**Part 5 – Malware Analysis Report**

Review the Symantec description of how the Stuxnet virus works in “W32.Stuxnet Dossier.” Then, complete the following:

1. What is the goal and target of Stuxnet?
   1. Machinery that is being used to create nuclear technology in Iran.
2. Explain the techniques used in Stuxnet to accomplish the goals of copying itself, elevating its privileges to admin/root status, delivering its payload, and remaining hidden from view. What specific software, hardware, exploits, autonomous administration and design were used to make this a successful application? Site the specific information found in the “W32. Stuxnet Dossier Report” to support your answers.
   1. In the context of Struxnet, the software copied itself over a network to other computers in the system, and eventually it found the target computer. By elevating administrative status to root status, the worm was able to infect secretly, without any need of approval by the parent device to write to the drive. By creating autonomous systems within the worm that wrote data privately and spread quickly, the software was able to be extremely effective. The effectiveness was fueled by the exploit of vulnerabilities and effectiveness of the intentional changes.
3. Summarize the process by which a PLC device, not connected to a network, can be infected by Stuxnet.
   1. Any PLC device can be infected by Struxnet. Struxnet is injected into a PLC device because Struxnet is designed to reprogram the PLC device. By reprogramming through a 7-step process, Struxnet is able to change the way the PLC functions to use it for its own gain. This gain includes reproduction and spread across a network.