StuxNet: The World’s First Cyber Weapon

Ryan Scott

Grand Canyon University  
Information Security II

Prof. Christine Bakke

**Part 1: Cyber Weapons Development**

**Proof the U.S. was Behind Stuxnet**

Several pieces of evidence suggest that the U.S. was involved in the development and deployment of Stuxnet. The code used in the Iranian nuclear facilities is written in English, and the advanced knowledge of Siemens control systems suggests that the U.S. may have been involved. Additionally, the use of multiple zero-day exploits, which are extremely valuable and are often only known to governments, also indicates that a nation-state is involved, (Andrii Kucheruk, 2017).

**Terms Relating to Stuxnet**

**Worm:** A type of malware that spreads through networks by exploiting vulnerabilities in software.

**Air Gap:** A security measure that physically isolates a computer or network from the internet or other networks to prevent unauthorized access.

**Fire and Forget:** A type of weapon or attack that is launched and operates automatically without further intervention.

**Zero Day Exploit:** A vulnerability in software that is unknown to the software vendor and therefore has no patch or fix available.

**WinCC:** A supervisory control and data acquisition (SCADA) system developed by Siemens that was targeted by Stuxnet.

**PLC:** Programmable logic controllers are industrial computers used to control and automate manufacturing processes, and were targeted by Stuxnet.

**Centrifuge:** A machine used to enrich uranium, which was the specific target of Stuxnet.

**How These Terms Relate to Stuxnet**

As part of its design, Stuxnet targeted industrial control systems, specifically those used in Iranian nuclear facilities. The worm was able to spread through networks and ultimately infect the PLCs responsible for controlling the centrifuges used for uranium enrichment. Due to its zero-day exploits, it was able to bypass security measures and operate automatically without further action, thus making it a “fire and forget” weapon. Siemens' use of the WinCC system was also critical to Stuxnet's success, as it provided a vulnerability for the worm to exploit, (Farwell & Rohozinski, 2011).

**Part 2: A New Type of Warfare**

**Viewpoint 1** – **The U.S. was reckless and provocative**

Contrary to this viewpoint, one might argue that the United States and Israel were legitimately concerned about Iran's nuclear program, and that Stuxnet was a targeted approach to reduce civilian casualties and avoid war. In addition, it may be argued that cyber warfare has already existed for a number of years, and Stuxnet is just one example, (Farwell & Rohozinski, 2011).

**Viewpoint 2** – **The U.S. was precise and restrained**

Contrary to this viewpoint, one might argue that Stuxnet's use will set a dangerous precedent for future cyber warfare. Additionally, they might contend that Stuxnet failed to achieve its intended objectives, since Iran continued to develop its nuclear program despite the disruption caused by the worm, (Farwell & Rohozinski, 2011).

**Stuxnet vs Nuclear Weapons**

Stuxnet and nuclear weapons have some similarities in that they are both weapons of mass destruction that can cause physical injury and death. Nuclear weapons, on the other hand, have a much greater destructive potential and can cause long-term environmental and health impacts. Also, nuclear weapons are subject to international treaties and laws, whereas cyber warfare is an unregulated field that is relatively new, (Farwell & Rohozinski, 2011).

**Arguments About U.S. Using Nuclear Weapons**

Many supporters of the use of nuclear weapons against Japan assert that it was necessary for the war to be ended quickly in order to prevent further casualties from occurring on either side of the war. Additionally, some argue that the bombings ultimately saved more lives than they took, as they prevented the need for a land invasion of Japan. Additionally, some argue that Japan had committed atrocities during the war and deserved to be punished harshly.

There are also those who contend that the bombings were unnecessary and constitute war crimes. They argue that Japan was already on the verge of surrender before the bombings, and that they served as a display of American military strength rather than as a necessary military action. Critics also contend that the bombings resulted in the death of a large number of civilians as well as long-term environmental and health effects.

**Part 3: Malware Analysis**

**How Stuxnet Works**

Stuxnet is a complex computer worm that spreads via removable media and network shares. It targets Windows computers and seeks out Siemens Step7 software, which is used to program industrial control systems. Then, Stuxnet utilizes zero-day exploits to manipulate programmable logic controllers (PLCs) so they can cause damage to centrifuges used to enrich uranium, (Farwell & Rohozinski, 2011).

**Why Stuxnet Wasn’t Effective**

Stuxnet was unable to accomplish its ultimate objective of stopping Iran's nuclear enrichment program, which was the least effective aspect of the attack, (Andrii Kucheruk, 2017). Though the attack was able to severely damage Iran's nuclear infrastructure, it was not sufficient to completely halt the program, despite causing significant damage. By Iran redoubling its efforts and improving the security of its nuclear facilities, the attack may have in fact had the opposite effect. Additionally, Stuxnet's discovery may have led to the development of more sophisticated and resilient defenses against future cyberattacks, (Andrii Kucheruk, 2017).

**Part 4: Consequences and Conclusion**

**How To Handle Cyber Weapons in the Future**

According to the experts in the movie, cyber weapons should be regulated in a similar manner to other types of weapons of mass destruction, including nuclear, biological, and chemical weapons, (Andrii Kucheruk, 2017). In order to determine what constitutes acceptable and unacceptable cyber behavior, establish rules for attribution and accountability, and establish mechanisms for monitoring and enforcing compliance, A global effort should be made to prevent the unchecked proliferation of cyber weapons and to promote responsible behavior in cyberspace, (Andrii Kucheruk, 2017).

**Part 5: Malware Analysis Report**

**What is the goal and target of Stuxnet?**

The goal of Stuxnet is to target and disrupt the centrifuge machines used for uranium enrichment in Iran's nuclear program. ultimately shutting it down.

**How Stuxnet Accomplished its Goals**

A zero-day vulnerability in Windows operating systems enables Stuxnet to copy itself and elevate privileges, and infected USB drives enable it to spread. In order to avoid detection and establish itself as a trusted application, it uses a digital certificate stolen from a legitimate software company. Siemens Step7 software, which is used to program industrial control systems, as well as WinCC, which is used to monitor them, (Falliere et al., 2010). To cause physical damage to centrifuges, Stuxnet modifies the code on the Programmable Logic Controllers (PLCs).

In order to avoid detection and carry out its mission, Stuxnet uses a combination of autonomous management and design. The attack is designed to recognize specific Siemens PLCs and then manipulate the code on them to cause physical damage, (Falliere et al., 2010). It is also designed to spread to other devices and networks in order to ensure maximum reach and effectiveness.

**Infecting Devices Off the Network with Stuxnet**

A PLC device not connected to a network can be infected by Stuxnet by using infected USB drives to transfer data to and from the device. When plugged into a computer, the infected USB drive contains a malicious LNK file that executes the malicious code, (Falliere et al., 2010). Once infected, Stuxnet searches for Siemens software and attacks PLCs connected to the computer. PLCs can still be infected even if they are not connected to a network if an infected USB drive is used to transfer data to or from them, (Falliere et al., 2010).

# 

# References

Andrii Kucheruk. (2017, November 12). *ANONYMOUS - Web Warriors HD Full Documentary - National Geographic* [Video]. YouTube. <https://www.youtube.com/watch?v=gs_pimvLO6I>

Programming w/ Professor Sluiter. (2020, June 9). *Stuxnet Virus: The world’s first cyber weapon* [Video]. YouTube. https://www.youtube.com/watch?v=iKUuuvo\_cSQ

Falliere, N., Murchu, L., & Chien, E. (2010, November). W32.Stuxnet Dossier. *Wired.Com*. <https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf>

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53*(1), 23–40. <https://doi.org/10.1080/00396338.2011.555586>