Discussion Questions from the Case Study Related to the Stuxnet Malware

William Slater

CIS 537 - CyberEthics

Bellevue University

Week 3, Written Homework Assignment

Patrick Artz, M.S. - Instructor

December 20, 2011

Discussion Questions from the Case Study Related to the Stuxnet Malware

Summary

During the Summer of 2010, industrial equipment located in facilities that were specialized for the production of nuclear weapons material manufacturing, was attacked by a special type of malware now known as the "Stuxnet worm." This worm was introduced into the IT infrastructure and found its way into the areas where some of the industrial equipment required to nuclear weapons material was being processed. The Stuxnet worm was successful in its mission because with surgical precision, it struck the programmable logic controllers (PLCs) in the industrial equipment it attacked, and rendered the equipment inoperable (Zetter, 2011).

Final expert analysis of the Stuxnet worm indicated that it was well designed to accomplish its mission and that it was most likely the work of highly skilled, knowledgeable agents representing at least one, but most likely two nation-states (Reynolds, 2012).

Initially, the U.S. government wanted to have as many details about the Stuxnet worm as possible classified because of the sensitive nature of the data surrounding the development of such capabilities. But the work of engineers at Symantec and Langner, would ultimately result I the release of some extremely detailed information about how the worm attacked and how it performed the functions for which it was designed (Zetter, 2011), (Langner, 2010).

Though there had been previous malware attacks in industrial facilities, the emergence of the Stuxnet worm onto the international is now foretelling that the newest dimension of the landscape of conflict will include cyberspace and the vulnerable infrastructure components of nation-states (Gelton, 2010).

1) **How is the Stuxnet worm different from previous malware aimed at industrial systems?**

The Stuxnet worm differed from previous malware aimed at industrial systems in the following ways:

A. It was highly specialized: Once it was introduced into an infrastructure, it was programmed to attack the programmable logic controllers that are embedded in centrifuge equipment that was used to purify fissile material used to construct nuclear weapons (Zetter, 2011).
B. The code in the worm was so well designed that it required intimate knowledge of both the IT infrastructures and the industrial equipment control systems that it was designed to attack (Zetter, 2011).
C. The worm was initially introduced via USB drives, indicating a risk that the attacker was using a non-traditional method to start the spread of the worm.
D. The Stuxnet worm attack came at a time that was critical because it halted the Iranian production of nuclear material (Zetter, 2011). Speculation: It would result in helping buy the attackers additional time to plan for other means to thwart this effort.

2) Do you think the Stuxnet worm constitutes cyberwarfare? Why or why not?

Yes. The Stuxnet worm was definitely an act of cyberwarfare. These are the reasons that support that conclusion:

A. The worm was so sophisticated as evidenced by its construction and specialized capabilities, that it was obviously the work of at least one technical people in at least one nation-state and perhaps two (Reynolds, 2012).
B. My guess that those nation-state actors were the United States and Israel, because both countries have the capability to produce cyberweapons as well as a shared motives of wanting to protect Israel and shut down the very capabilities in Iran that the Stuxnet Worm targeted.
C. Cyberwarfare is cheap, comparatively speaking. (See figure 1 below.) Cyberweapons can be developed and deployed for a fraction of the cost of weapon systems such as the U.S. Air Force B-2 Stealth Bomber or the U.S. Air Force F-117A Stealth Fighter-Bomber, and these cyberweapons can be usually deployed, usually in an undetected manner, utilizing the target's infrastructure, without endangering humans on the side of the attacker (Technolytics, 2011). From an economic and from a financial perspective, it makes perfect sense to develop and deploy these cyberweapons if they are proven to be effective.
D. Iran has been very vocal about the development of the capability to create own nuclear weapons and its president, President Akmajinedad has been very adamant about his hatred of Israel and his desire to eliminate its people from the face of the Earth (Zetter, 2011).

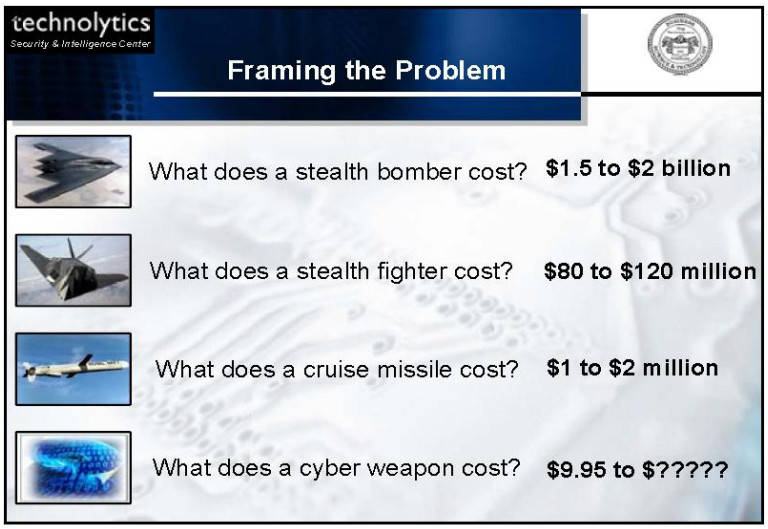

Figure 1 – Comparing the costs of a cyberweapon to other modern weapons (Technolytics, 2011).

3) What types of precautions could be taken to protect critical infrastructure from malware that can take control of and reprogram a SCADA system?

The following steps will help prevent future Stuxnet attacks:

A. Hire knowledgeable people who understand the complexities and vulnerabilities of both modern IT infrastructures and modern industrial control systems, especially those that utilize programmable logical controllers (PLC)s (Langner, 2012).
B. Continually monitor the IT systems and the industrial systems for vulnerabilities and update the security controls (including patches) when vulnerabilities occur (Reynolds, 2012).
C. Proactively scan for and apply the resources to act on the efforts required to mitigate vulnerabilities that are identified (Reynolds, 2012).
D. Conduct frequent security audits that audit everything from written policies, procedures, and guidelines to the proper and secure implementation of security controls in all IT infrastructure components and the industrial systems (Reynolds, 2012).
E. Maintain close relationships with the vendors of all IT equipment and industrial equipment and ensure that information about available software updates is gained, and that the updates are obtained and implemented as quickly as possible (Reynolds, 2012).
F. Ensure that special attention is paid to the areas that form the network perimeters between IT equipment and industrial equipment, so that the industrial equipment with vulnerable PLCs is protected as well as possible, given the known state of vulnerabilities and the security controls that mitigate the treats that can exploit them.

Supplemental Information about the Stuxnet Worm

The diagrams below, shed additional light on how the Stuxnet worm operated. These were developed after careful analysis was done on captured specimens of the worm.

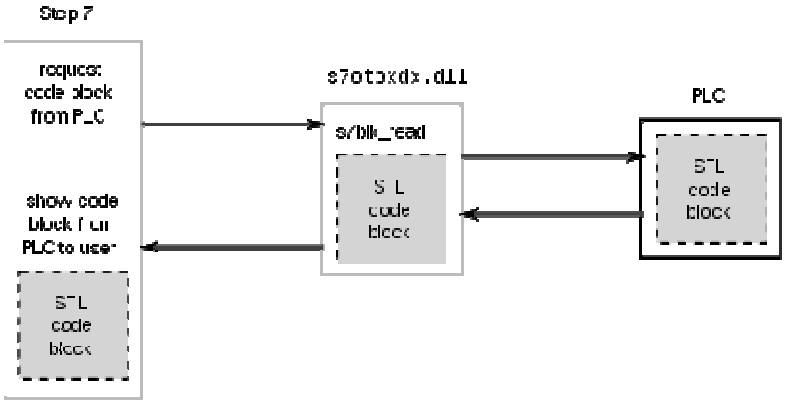

Figure 2 – High level diagram - How the Stuxnet Worm Attacked Programmable Logic Controllers in Industrial Machines (Wikicommons, 2011)

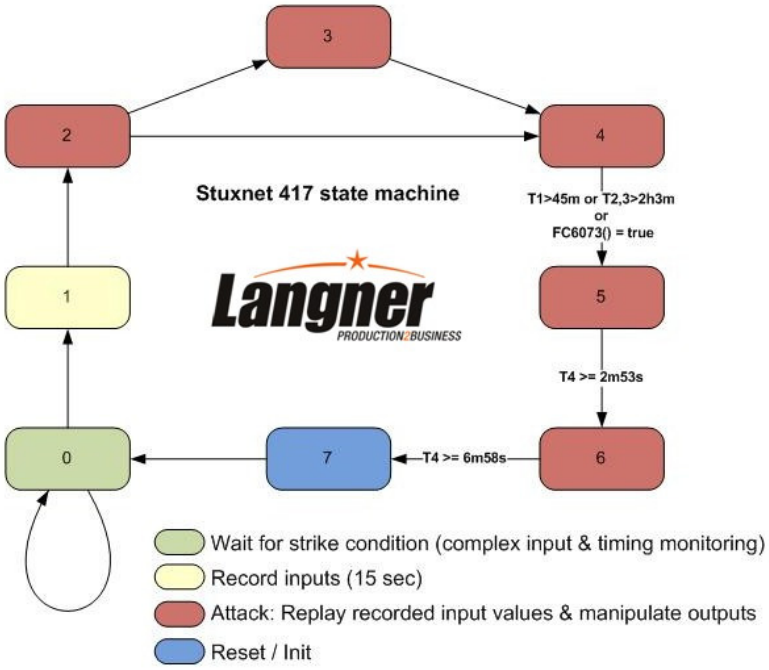

Figure 3 – Stuxnet 417 Finite State Machine (Langner, 2010)

References

Edwards, M. and Stauffer, T. (2008). Control System Security Assessments. A technical paper presented at the 2008 Automation Summit – A Users Conference, in Chicago. Retrieved from http://www.infracritical.com/papers/nstb-2481.pdf on December 20, 2011.

Gjelten, T. (2011). Stuxnet Raises 'Blowback' Risk In Cyberwar. An article published at NPR.org on December 11, 2011.

Retrieved from http://www.npr.org/2011/11/02/141908180/Stuxnet-raises-blowback-risk-in-cyberwar on December 20, 2011.

Gjelten, T. (2011). Security Expert: U.S. 'Leading Force' Behind Stuxnet. An article published at NPR.org on September 26, 2011. Retrieved from http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-Stuxnet on December 20, 2011.

Gjelten, T. (2010). Stuxnet Computer Worm Has Vast Repercussions. An article published at NPR.org on October 1, 2011. Retrieved from http://www.npr.org/templates/story/story.php?storyId=130260413 on December 20, 2011.

Gjelten, T. (2010). Are 'Stuxnet' Worm Attacks Cyberwarfare? An article published at NPR.org on October 1, 2011. Retrieved from

http://www.npr.org/2011/09/26/140789306/security-expert-u-s-leading-force-behind-Stuxnet on December 20, 2011.

Langer, R. (2010). Retrieved from http://www.langner.com/en/blog/page/6/ on December 20, 2011.

Reynolds, G. W. (2012). Ethics in Information Tehnology, 4th edition. Boston, MA: Course Technology.

Technolytics. (2011). Cyber Commander's eHandbook: The Weaponry and Strategies of Digital Conflict. Purchased and downloaded from Amazon.com on April 16, 2011.

Wikipedia Commons. (2011). Stuxnet Diagram. Retrieved from http://en.wikipedia.org/wiki/File:Step7_communicating_with_plc.svg on December 20, 2011.

Zetter, K. (2011). How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History. An article published on July 11, 2011 at Wired.com. Retrieved from http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-Stuxnet/all/1 on December 20, 2011.