Homework 3: Analyzing the Stuxnet Worm

1. What vulnerability did the worm use to spread?

Stuxnet spread by exploiting multiple zero-day vulnerabilities in Microsoft Windows. One of the key vulnerabilities was in the Windows Print Spooler service, which allowed it to move from one system to another via USB drives and network shares, making it difficult to detect and stop.

2. Did the worm target specific countries?

Yes, Stuxnet was primarily designed to target Iran. Its main goal was to disturb Iran's nuclear program, particularly the centrifuges used for uranium enrichment. Although the worm did spread to other countries, its damaging effects were most severe in Iran.

3. Did the worm target specific systems? If so, how?

Stuxnet specifically targeted Siemens industrial control systems, which are critical in managing industrial processes. It infected the Siemens Step7 software, used to program PLCs (Programmable Logic Controllers). Once inside, Stuxnet altered the PLC code, causing the centrifuges to spin at dangerous speeds, leading to physical damage, while simultaneously hiding these changes from operators.

4. What other infamous worms did you find in your research?

Conficker (2008): Conficker was a highly aggressive worm that spread by taking advantage of a security flaw in Windows. It formed a massive network of infected computers, known as a botnet, which attackers used for harmful activities like sending spam and launching cyberattacks. Despite efforts to eliminate it, Conficker remains an ongoing threat.

Mydoom (2004): Mydoom quickly became the fastest spreading email worm in history, according to NordVPN. It spread by tricking people into opening an infected email attachment, which then forwarded itself to all the contacts in the victim’s email list. Additionally, it opened a backdoor, allowing hackers to remotely control the computer. causing widespread internet disruptions and significant financial damage.

ILOVEYOU (2000): The ILOVEYOU worm spread through an email titled "I Love You," enticing people to open the attachment. Once opened, it overwrote files on the victim’s computer and sent itself to everyone in the email address book. The worm spread fast impacting many computers and causing financial damages.

Works Cited

* The Guardian. *Stuxnet worm heralds a new era of global cyberwar*. <https://www.theguardian.com/technology/2010/sep/30/stuxnet-worm-new-era-global-cyberwar>
* NordVPN. Stuxnet explained — the worm that went nuclear

<https://nordvpn.com/blog/stuxnet-virus/#:~:text=Stuxnet%20was%20the%20first%20virus,due%20to%20its%20aggressive%20nature>.

* W32.Stuxnet Dossier Version 1.4 (February 2011) <https://docs.broadcom.com/doc/security-response-w32-stuxnet-dossier-11-en>
* What is the Conficker worm.

<https://www.cybereason.com/blog/what-is-the-conficker-worm>

<https://www.ccdcoe.org/uploads/2018/10/Kaska2012_ConfickerConsiderationsInLawAndLegalPolicy.pdf>

* Conficker: Considerations in Law and Legal Policy.

<https://www.ccdcoe.org/uploads/2018/10/Kaska2012_ConfickerConsiderationsInLawAndLegalPolicy.pdf>

* ILOVEYOU virus

<https://www.techtarget.com/searchsecurity/definition/ILOVEYOU-virus>

* I love you’: How a badly-coded computer virus caused billions in damage and exposed vulnerabilities which remain 20 years on.

<https://www.cnn.com/2020/05/01/tech/iloveyou-virus-computer-security-intl-hnk/index.html>

* The MyDoom worm: history, technical details, and defense

<https://nordvpn.com/blog/mydoom-virus/?srsltid=AfmBOoq_233ZkzAMhCRfCB7F35VYIHwYSgBq8vhmXzKz4BxbPt3b3bRx>