STUXNET

The World's First Cyber Weapon

By: Daniel Styles

What was Stuxnet?

- Powerful computer worm – discovered 2010
- Targeted Iranian nuclear enrichment facility in Natanz
- Central goal to disrupt their nuclear program

How Did It Infect?

- Natanz is an air-gapped facility
- Most likely from a USB thumb drive
- Propagated itself through internal network shares

What Did Stuxnet Do?

- Designed to destroy centrifuges used to enrich uranium
- Stuxnet searches the computer for specific Siemen's programmable logic controllers (PLCs)
- Alter the PLC programming causing irregular spinning
- PLC then tells computer it is operating normally

What Vulnerabilities did it Exploit?

- Infected Windows PCs
- Windows Shortcut flaw
- Print Spooler bug
- 2 Privilege Escalation vulnerabilities
- Zero-day flaw in Siemens PLC

How was it detected?

- Stuxnet ended up escaping the Natanz facility
- Office in Iran experiencing unusual reboots and Blue Screens
- The Belarusian, Sergey Ulasen from VirusBlokAda assisted in the malware analysis
- Realized how many zero-days were exploited and shared findings with security community.

Who created Stuxnet?

United States and Israeli intelligence agencies

Probably began development in 2005

If Iran were to develop atomic weapons, Israel would respond

Thus, Operation Olympic Games launched

Looking Forward

“Very few pieces of malware have garnered the same kind of worldwide attention as Stuxnet “ - Jerome Segura

Works Cited

- What is Stuxnet? | Malwarebytes. (2022). Retrieved November 2, 2022, from Malwarebytes website: https://www.malwarebytes.com/stuxnet
- Fruhlinger, J. (2022, August 31). Stuxnet explained: The first known cyberweapon. Retrieved November 2, 2022, from CSO Online website: https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html
- blog/authors/jeromesegura. (2013, November 25). Stuxnet: new light through old windows. Retrieved November 2, 2022, from Malwarebytes website: https://www.malwarebytes.com/blog/news/2013/11/stuxnet-new-light-through-old-windows
- Zetter, K. (2014, November 3). An Unprecedented Look at Stuxnet, the World’s First Digital Weapon. Retrieved November 2, 2022, from WIRED website: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/