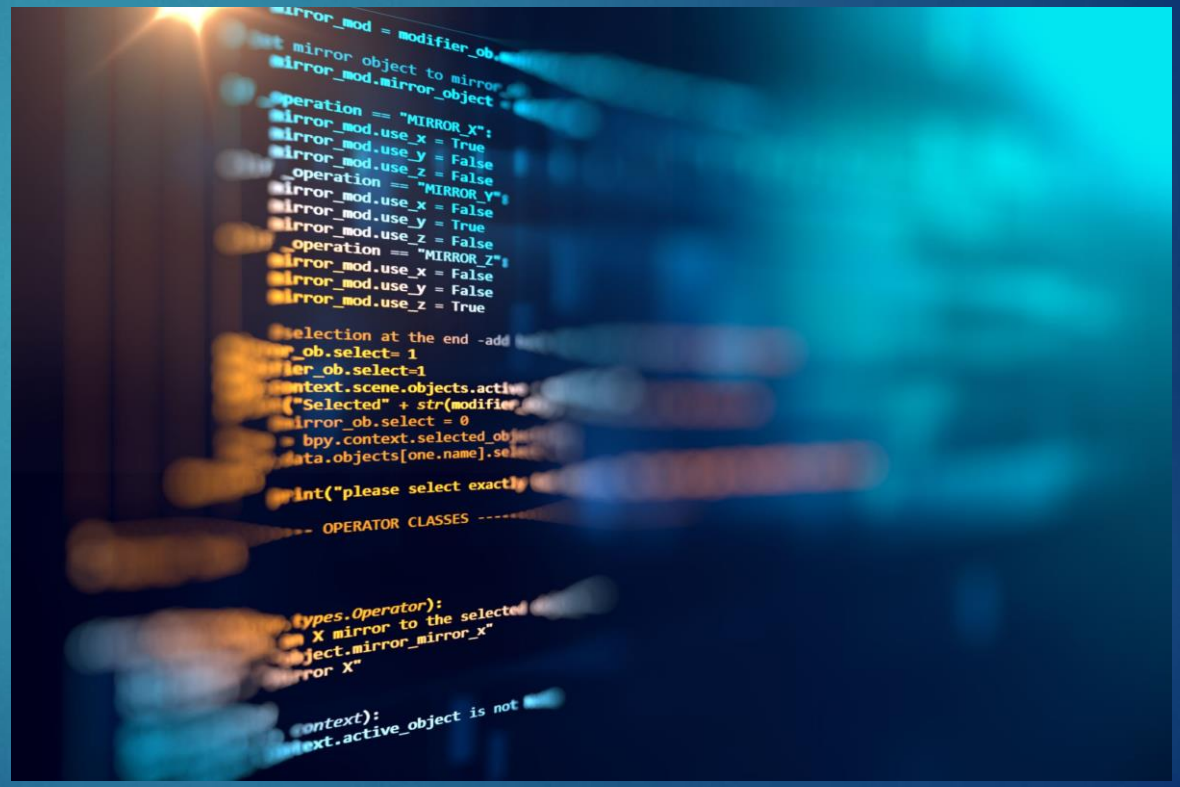
STUXNET

THE WORM THAT PREVENTED WAR

By Zach Weaver

Overview

- 1. What is Stuxnet
- 2. How/why was it created
- 3. How to defend against worms.



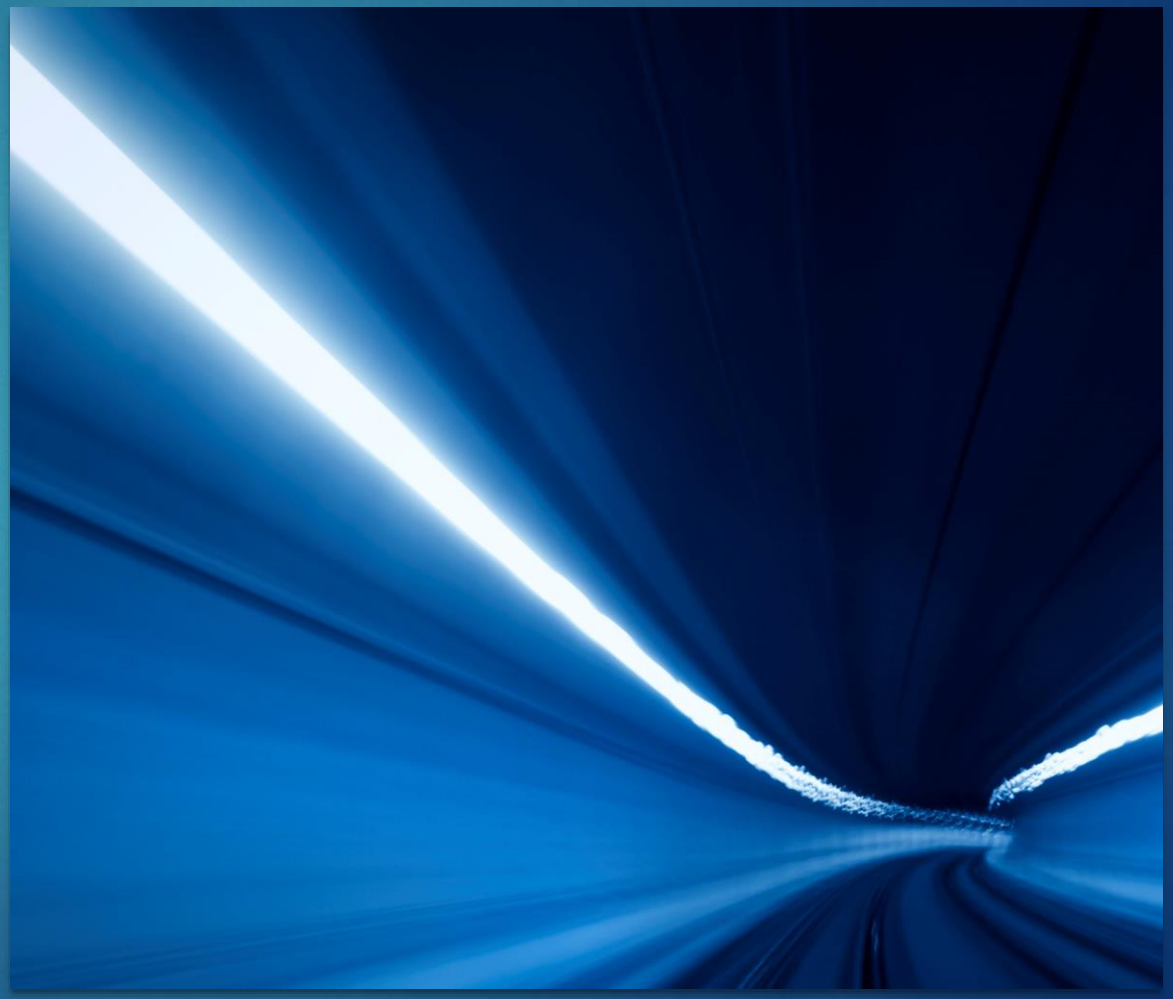
- What is Stuxnet? -

Iranian nuclear centrifuges
Source: https://www.extremetech.com/computing/200898-windows-pcs-vulnerable-to-stuxnet-attack-five-years-after-patches

- Stuxnet was a highly sophisticated worm developed by U.S and Israeli intelligence used to disable an Iranian nuclear program.
- The worm was first discovered publicly in 2010 but many believe it's development began as early as 2005.
- Bush and Obama administrations were worried that Iran was developing nuclear weapons, so the Stuxnet worm was created to prevent regional war between Israel and Iran.
- Speculated to have been written in multiple languages including C, C++, and some other object oriented languages.

Operation Olympic Games

- Program Under which Stuxnet was developed
- Program took place under Bush and Obama administrations
- Involved many skillful engineers/programmers



- What Happened/How was it Executed?-

- Stuxnet was designed to destroy Iranian nuclear centrifuges

Centrifuges

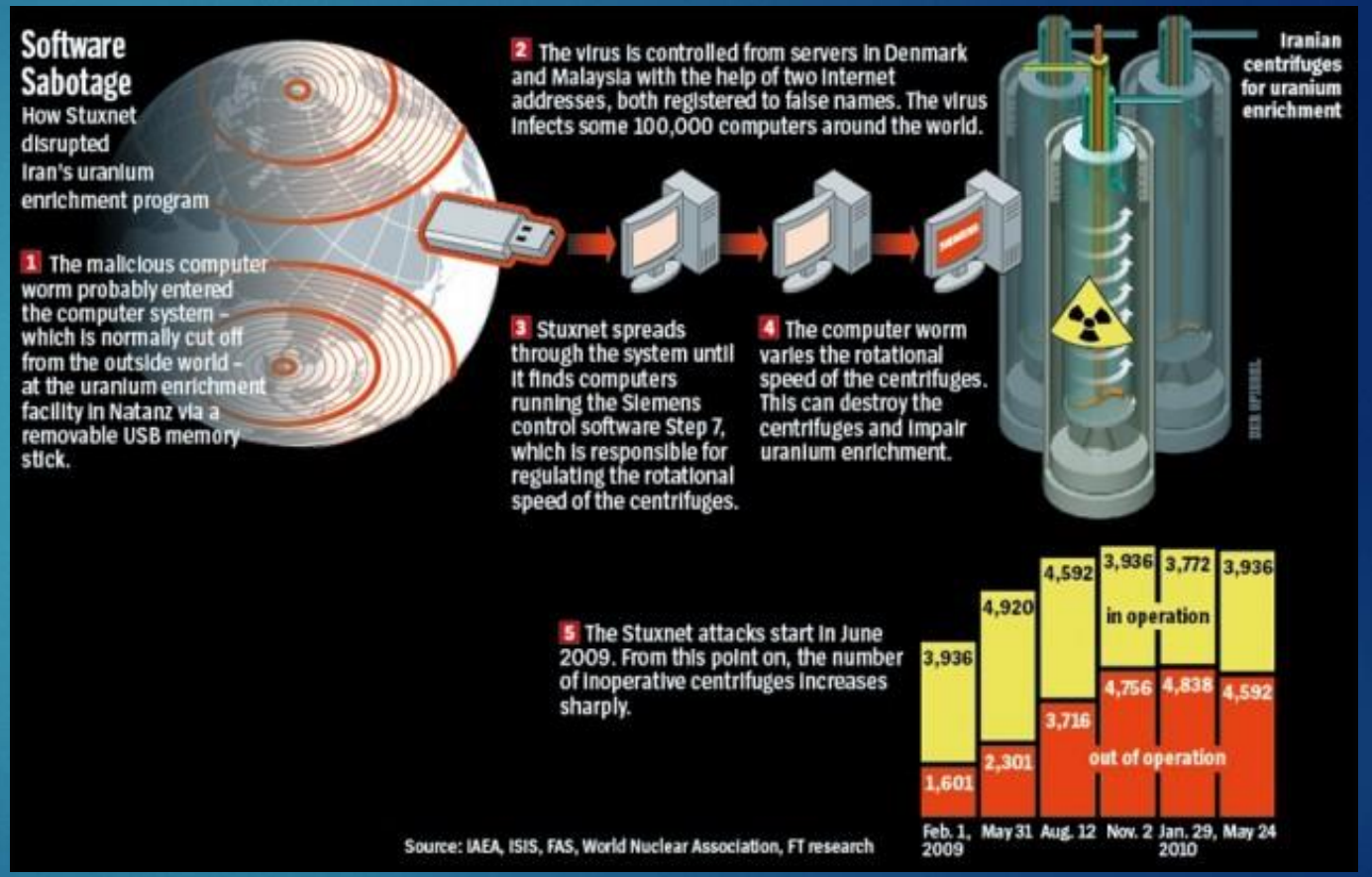
- Primary method of spreading was a USB flash drive
- Unlike Normal worms that just steal information, Stuxnet reeked havoc by causing physical destruction to the machines it impacted
- The worm ultimately effected multiple organizations that supplied machinery to Iranian nuclear programs

Image sources: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Stuxnet Execution

(How Stuxnet Works)

- First, Stuxnet checks to see if target system is connected to any specific PLS's (Programmable Logic Controllers)
- Next, the worm tampers with the PLC's programming.
- While Stuxnet is attacking the system, the PLC tells the computer that nothing is wrong making it hard to pinpoint any problem



Source: https://www.extremetech.com/computing/200898-windows-pcs-vulnerable-to-stuxnet-attack-five-years-after-patches

In the Case of Iran

- Altering the PLCs is what caused the nuclear centrifuges to malfunction by spinning irregularly
- Stuxnet attacked all layers of infrastructure
- Stuxnet exploited a total of 4, zero-day bugs
  - Windows shortcut flow
  - Print spooler bug
  - 2 escalation of privilege vulnerabilities

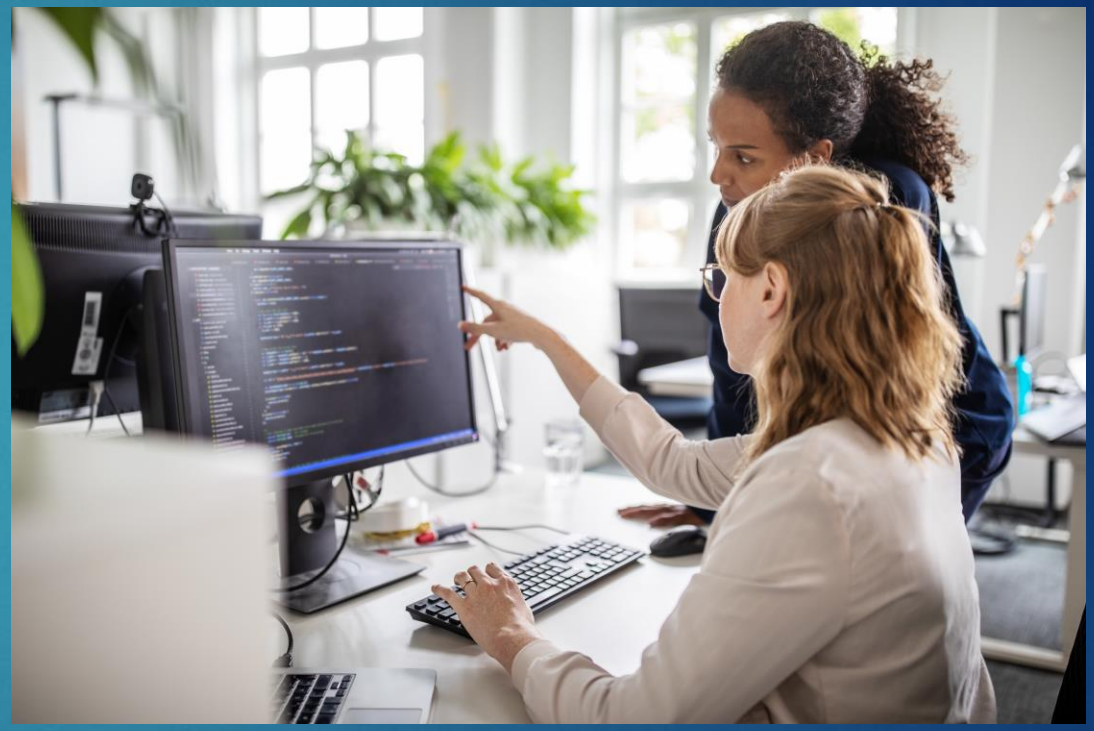
Stuxnet Today

- Even though Stuxnet hasn't completely vanished it's not seen as a major threat today
- Stuxnet was primarily a threat only to its original targets in Iran
- If a normal home computer gets infected with Stuxnet the worst that might happen is random hardware malfunctions like reboots of blue screens of death
- The zero-day vulnerabilities Stuxnet originally used have since been patched

Worm Prevention

- The best way to prevent against worms like Stuxnet is to consciously practice good cyber hygiene.

- Good techniques/practices include:
  - Antivirus Software
  - Refraining from downloading subspinous attachments
  - Refrain from using suspicious external storage devices (USBs, floppy discs, etc.)
  - Keep software up to date
  - Use a firewall to monitor network security



References

https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html

https://www.extremetech.com/computing/200898-windows-pcs-vulnerable-to-stuxnet-attack-five-years-after-patches

https://cyberthreatportal.com/how-to-prevent-computer-worms/