# StUXnet

# ABOUT STUXNET

- Computer worm first uncovered in 2010
- Most complex worm of its time
  - Approx. >=5 years to write
- Affected SCADA systems
  - Ex: Nuclear plants, traffic control systems
  - First act of Cyberwarfare

# CAPABILITIES

- Exploited multiple zero-day vulnerabilities
- Could attack Siemens' SCADA control software
- Could autoupdate

# TARGET AND SPREAD

- Target: Programming Logic Controllers (PLCs)
- Likely Vessel:  USB flash drives
    - Believed to be introduced by security personnel, some person/people with access to PLCs

# TARGET AND SPREAD (CONT)

- Copies itself to open file shares
- Windows RPC service
  - Service that allows two computers to communicate
  - Attacked vulnerabilities in it, allowed worm to spread

# TARGET AND SPREAD (CONT)

- Siemens vulnerability
- Default username and password
    - Bug allowed unauthorized login

# AFTERMATH

- Worm had spread to infect large SCADA network
- Shutdown 1,000 centrifuges in Natanz
  - Credited to Stuxnet
- Iranian government announces Cyberweapons Program (2011)

# INVOLVEMENT

- No firm proof of who created Stuxnet
- Rumors
- US involvement
- Israel involvement
- Siemens

# WORK CITED


- https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf
- https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html
- https://nypost.com/2013/05/16/stuxnet-virus-might-have-improved-irans-nuclear-capabilities-report/
- https://www.youtube.com/watch?v=7g0pi4J8auQ
- https://people.carleton.edu/~grossea/aftermath.html#n8