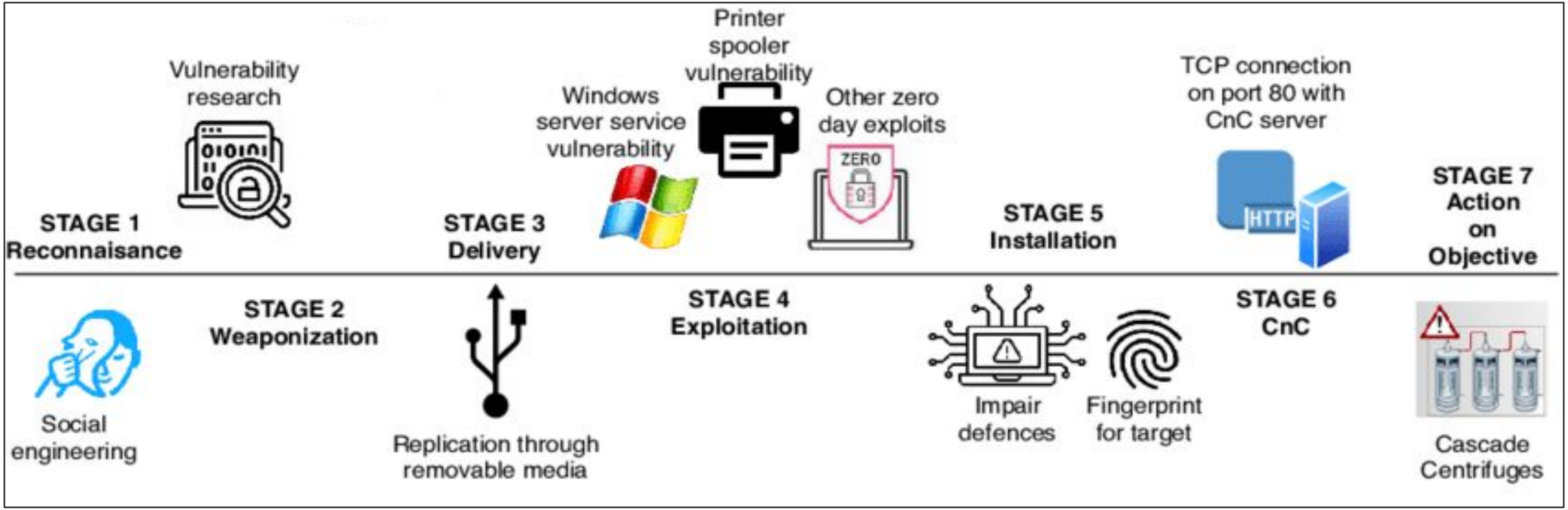
CASE STUDY- STUXNET CYBERATTACK

NEERAJ JAYESH
ELIJAH JOHN

Stuxnet Cyberattack (2009)

- Stuxnet was a highly targeted worm discovered in 2010 that manipulated Siemens PLCs to damage uranium-enrichment centrifuges at Iran's Natanz facility, causing physical degradation of hundreds of machines.

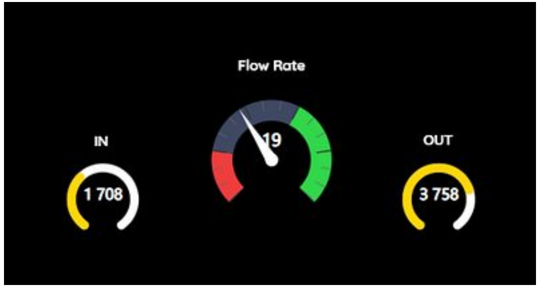


Stuxnet

The worm — **Stuxnet** — secretly spread via **infected USB drives** (because the network was isolated from the internet). It jumped from regular Windows PCs into **industrial control systems**.

Once inside:

- It looked for **specific Siemens PLC models** used in uranium centrifuges.
- When it found them, it **altered the PLC code** to:
  - Randomly **speed up and slow down centrifuge rotors**.
  - While **faking sensor data** so operators saw normal readings.



Five Stages of the Cyberattack

1

Initial Infection

Infected USB drives introduced into air-gapped networks—potentially by unwitting contractors or insiders

2

Network Propagation

Multiple exploits spread malware through Windows networks and removable media with surgical precision

3

Target Identification

Scanning systems for Siemens Step7 software controlling specific PLC configurations at Natanz

4

Payload Delivery

Injecting malicious code into PLCs to manipulate centrifuge speeds—causing catastrophic mechanical failure

5

Concealment

Rootkit technology hides changes and feeds false normal readings to monitoring systems, delaying detection

The Four Zero-Day Vulnerabilities

Stuxnet weaponized four previously unknown exploits—an unprecedented arsenal that demonstrated sophisticated state-level capabilities and meticulous planning.

1

CVE-2010-2568

Windows Shell LNK Vulnerability

Enabled automatic execution via USB drives, bypassing user interaction—the primary infection vector for air-gapped systems

2

CVE-2010-2729

Print Spooler Remote Code Execution

Allowed network propagation and remote control, spreading Stuxnet across connected systems

3

CVE-2010-2743

Task Scheduler Privilege Escalation

Granted elevated system privileges to execute malicious code undetected by security software

4

CVE-2010-2772

Win32k Local Privilege Escalation

Provided kernel-level access for deep system manipulation and persistent rootkit installation

Timeline of the Stuxnet Attack

1

2005: Operation Olympic Games

Development begins as classified US-Israel joint operation targeting Iran's nuclear ambitions

2

2009: Silent Infiltration

First infection at Natanz nuclear facility—operators remain unaware as centrifuges begin failing

3

June 17, 2010: Discovery

Belarusian researcher Sergey Ulasen identifies unprecedented malware complexity

4

2010: Global Spread

Over 200,000 computers infected worldwide, but payload activates only on precise targets

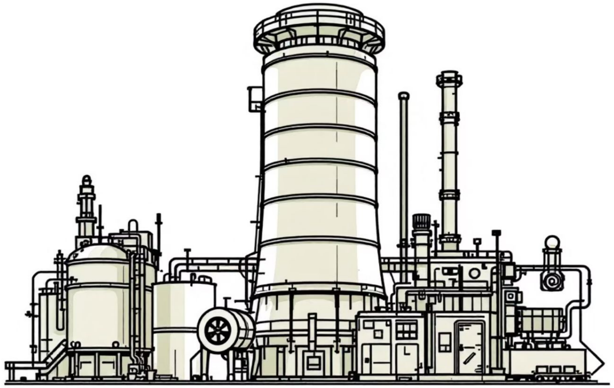
How Stuxnet Sabotaged Iran's Nuclear Program

The Perfect Sabotage

Stuxnet represented the cyberwarfare —a weapon that could reach inside a secure facility and destroy physical equipment without any firing

- Targeted Siemens PLCs controlling uranium enrichment centrifuges
- Manipulated rotor speeds to oscillate erratically between high and low RPMs
- Mechanical stress caused catastrophic centrifuge failures
- Fed false operational data to control rooms, masking the sabotage
- Destroyed approximately 1,000 centrifuges—20% of Iran's capacity

Result: Iran's nuclear program was set back by years, demonstrating cyber capabilities could achieve strategic military objectives.



Infrastructure Damaged by Stuxnet

Natanz Facility

Primary target: uranium enrichment centrifuges physically degraded through controlled manipulation

Equipment Losses

Over 1,000 IR-1 centrifuges destroyed, requiring costly replacements and extensive downtime

Global Exposure

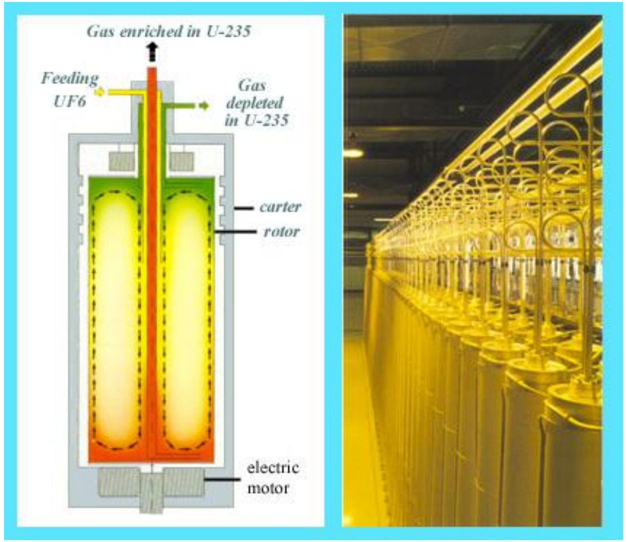
Revealed critical vulnerabilities in industrial control systems protecting infrastructure worldwide

> "Stuxnet demonstrated that cyber attacks could transcend the digital realm and cause tangible, strategic damage to physical infrastructure—a watershed moment in modern warfare."

Nuclear Centrifuges working

Nuclear centrifuges are devices that use high-speed rotation to separate isotopes of uranium

By spinning uranium gas, the heavier isotope (**238 U**) is forced to the outside, while the lighter, more fissile isotope (**235 U**) concentrates towards the center.



Why the Attack Succeeded?

Deep Knowledge of the Target – Stuxnet's creators knew exactly how Iran's Natanz facility worked from the model of Siemens PLCs used, Centrifuge configuration and speed patterns and the software (Step7) engineers used to program them.

Zero-Day Exploits – It used four zero-day vulnerabilities in Windows which were previously unknown.so no antivirus or patch could stop it.

Stealth and Deception –Stuxnet didn't immediately destroy anything. They Hid inside legitimate processes, Altered centrifuge speeds slowly, over time and sent fake normal readings back to operators.

Targeted Payload –It only activated if the right Siemens PLC was present and if the configuration matched **Iran's centrifuge** layout. If those conditions weren't met, it stayed dormant and spread harmlessly.

Lack of OT Security Awareness –In 2009–2010, Systems ran outdated Windows versions, no intrusion detection systems (**IDS**) for OT and Engineers prioritized uptime over security.

THANK YOU