Stuxnet

The First Cyber Weapon Targeting Industrial Control Systems

OT Security Learning Series

Document 410 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Stuxnet, discovered in 2010, is widely considered the first true cyber weapon—malware specifically designed to cause physical damage to industrial equipment. It targeted Iran's nuclear enrichment facility at Natanz, destroying centrifuges while hiding its activities from operators.

Critical

Stuxnet demonstrated that cyber attacks can cause physical destruction of industrial equipment. It fundamentally changed the threat landscape for critical infrastructure worldwide.

1.1 Key Facts

Attribute	Details
Discovery Date	June 2010
Target	Natanz uranium enrichment facility, Iran
Target Systems	Siemens S7-300 PLCs controlling centrifuges
Attack Method	USB propagation, network spreading, PLC manipulation
Physical Impact	Approximately 1,000 centrifuges destroyed
Attribution	Widely attributed to US and Israel (unconfirmed)
Zero-Days Used	4 Windows zero-day vulnerabilities

2 Attack Overview

2.1 Propagation Methods

Stuxnet used multiple methods to spread and reach its target:

1. **USB Drives:** Primary initial infection vector—exploited Windows autorun and LNK file vulnerabilities
2. **Network Shares:** Spread via Windows network shares using multiple vulnerabilities
3. **Print Spooler:** Exploited Windows Print Spooler vulnerability (MS10-061)
4. **Siemens WinCC/Step 7:** Spread through shared project files

Warning

Stuxnet crossed the "air gap" through infected USB drives carried by contractors and employees. Physical isolation alone is not sufficient protection.

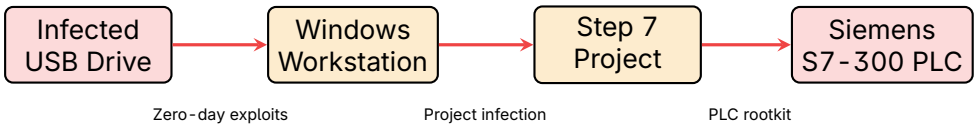

Figure 1: Stuxnet Attack Path

2.2 Target Identification

Stuxnet was highly selective in its targeting:

- Searched for Siemens Step 7 software installations
- Identified specific PLC configurations (S7-315 and S7-417)
- Verified presence of specific frequency converter drives (Vacon and Fararo Paya)
- Checked for drive frequencies between 807–1210 Hz (centrifuge operating range)
- Only activated payload when all conditions matched

Tip

The extreme specificity of Stuxnet's targeting criteria indicates detailed intelligence about the Natanz facility's configuration was available to the attackers.

3 Technical Analysis

3.1 Zero-Day Vulnerabilities

Stuxnet exploited four previously unknown Windows vulnerabilities:

CVE	Component	Description
CVE-2010-2568	Windows Shell	LNK file vulnerability for USB propagation
CVE-2010-2729	Print Spooler	Remote code execution via shared printers
CVE-2010-2772	Windows Server Service	Network propagation vulnerability
CVE-2010-3338	Task Scheduler	Privilege escalation

3.2 PLC Payload

The core payload targeted Siemens S7-300 PLCs:

PLC Attack Mechanism

1. **Infection:** Malicious code injected into Step 7 project files
2. **Rootkit:** PLC rootkit hid modifications from engineering software
3. **Recording:** Captured 21 days of normal centrifuge operation data
4. **Replay:** Played back normal data to operators while attacking
5. **Manipulation:** Varied centrifuge speeds to cause mechanical stress
6. **Destruction:** Centrifuges destroyed through metal fatigue

3.3 Man-in-the-Middle on PLCs

Critical

Stuxnet implemented a man-in-the-middle attack between the HMI/SCADA system and the PLCs. Operators saw normal readings while centrifuges were being destroyed. This "lying to the operator" technique has been replicated in subsequent attacks.

4 Attack Timeline

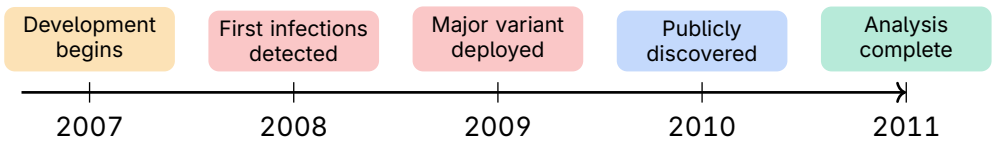

Figure 2: Stuxnet Timeline (2007–2011)

- **2005–2007:** Development phase (estimated)
- **June 2009:** First known variant deployed
- **March 2010:** More aggressive variant released
- **June 2010:** Discovered by VirusBlokAda (Belarus)
- **July 2010:** Siemens acknowledges targeting of their systems
- **September 2010:** Full analysis published by Symantec

5 Impact and Consequences

5.1 Immediate Impact

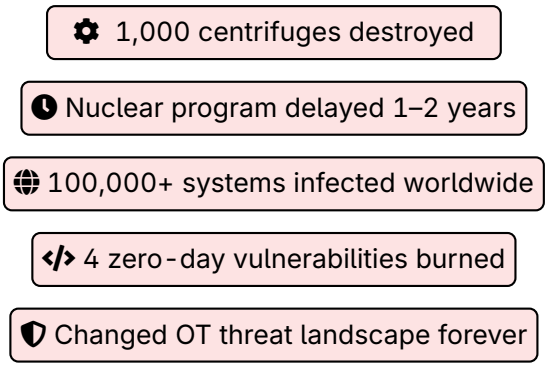

Figure 3: Stuxnet Impact Summary

- Approximately 1,000 IR-1 centrifuges destroyed at Natanz
- Iranian nuclear program delayed by an estimated 1–2 years
- Stuxnet spread beyond intended target to systems worldwide
- Over 100,000 systems infected globally (most not affected by payload)

5.2 Long-Term Consequences

Warning

Stuxnet's legacy extends far beyond its immediate impact:

- Demonstrated feasibility of cyber-physical attacks
- Lowered the barrier for future ICS attacks
- Code and techniques studied and reused by other actors
- Sparked global investment in OT security
- Led to development of ICS-specific security standards

6 Lessons Learned

6.1 Defense Recommendations

Key Point

Key takeaways for OT security:

1. **Air gaps are not absolute:** USB drives and contractor laptops can bridge isolated networks
2. **Monitor PLC integrity:** Detect unauthorized changes to PLC logic
3. **Verify operator displays:** Cross-check HMI data with independent measurements
4. **Control removable media:** Implement strict USB and media policies
5. **Segment networks:** Limit lateral movement within OT environments
6. **Update systems:** Apply security patches where safely possible

6.2 Detection Indicators

Stuxnet could have been detected through:

- Monitoring for unauthorized Step 7 project file modifications
- Detecting anomalous PLC communication patterns
- Identifying unexpected DLL injections in SCADA software
- Monitoring centrifuge performance deviations
- Network traffic analysis for C2 communications

7 Further Reading

Technical Reports

- **Symantec** – W32.Stuxnet Dossier
  https://docs.broadcom.com/docs/security-response-w32-stuxnet-dossier-11-en
- **Langner Communications** – To Kill a Centrifuge
  https://www.langner.com/to-kill-a-centrifuge/
- **ICS-CERT** – Advisory ICSA-10-272-01
  https://www.cisa.gov/news-events/ics-advisories

Books

- Zetter, K. – *Countdown to Zero Day* (Crown, 2014)
- Langner, R. – *Robust Control System Networks* (Momentum Press, 2011)

Documentary

- *Zero Days* (2016) – Documentary by Alex Gibney

Part of the OT Security Learning Series