THE FIRST CYBER WEAPON

STUXNET

Presentation by Charlotte Strobl

For CSCI 405 – Principles of Cybersecurity

C:\Overview

- Understanding Stuxnet
- Worm Structure
  - Propagation Phase
  - Triggering Phase
  - Execution Phase
- Zero Day Exploits
  - Windows Shortcut
  - Print Spooling

PNGarts. (n.d.). World map transparent background PNG [PNG file]. PNGarts. https://www.pngarts.com/explore/108718. Modified by Charlotte Strobl.

C:\Understanding—STUXNET\

Stuxnet is a highly sophisticated computer worm that innovated cyber attacks. It was active from 2007 – 2010 and marked the beginning of cyber warfare (Knapp & Langill, 2015).

> TARGET: Iran's Uranium Enrichment Facilities

> INTENT: Destroy real-world machinery using a computer program

P30Carl. (1941). *Map of Iran* [Map]. GNU Free Documentation License. https://aquarius.geomar.de. Modified by Charlotte Strobl.

C:\Worm-Structure\Phases

Worms follow a four-phase process: dormant, propagation, triggering, and execution.

This is the process that allowed Stuxnet to spread and damage machinery.

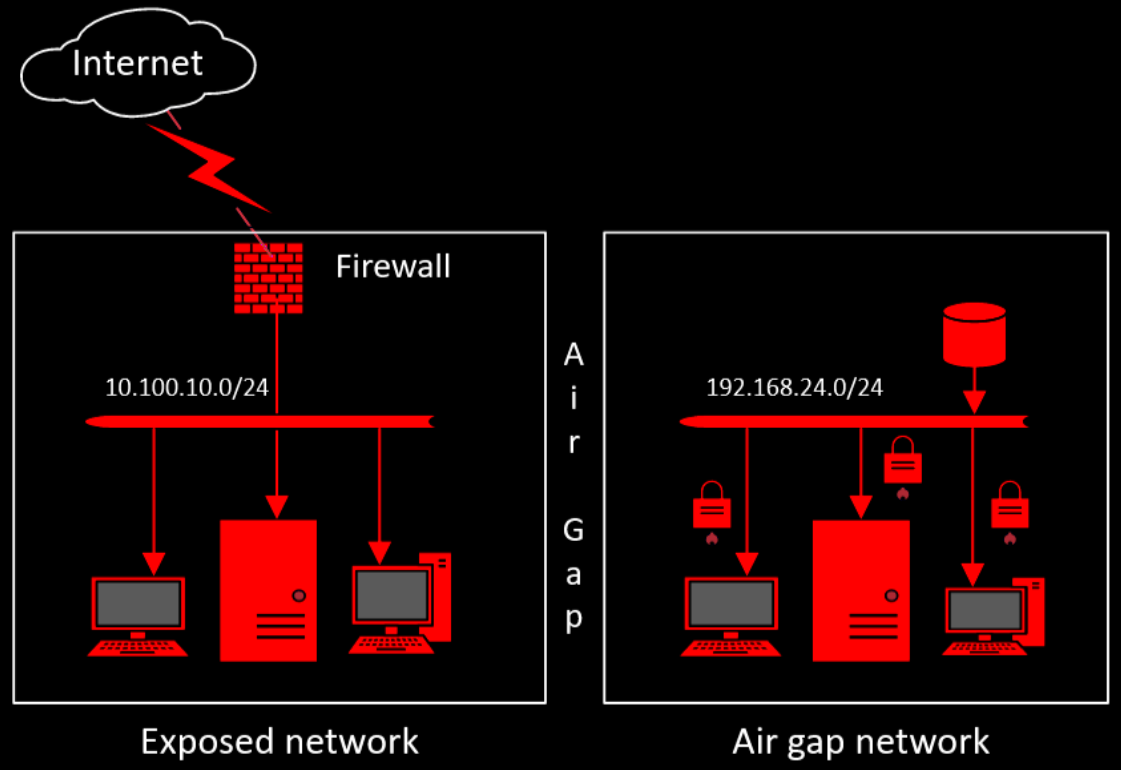
PROPAGATION	TRIGGERING	EXECUTION
Spread & multiply	Activation	Payload delivery

C:\Worm-Structure\Propagation

Most worms spread via the internet, but the Uranium Enrichment Facility had an isolated network (also known as an “air gap” network).

> ENTRY ALTERNATIVES:

- > Infected USB
- > Compromised Employee Laptop
- > Social Engineering



Speculos. (2023). Air gap network topology [mage]. Wikimedia Commons. https://commons.wikimedia.org/w/index.php?curid=138639069 Modified by Charlotte Strobl

C:\Worm-Structure\Triggering

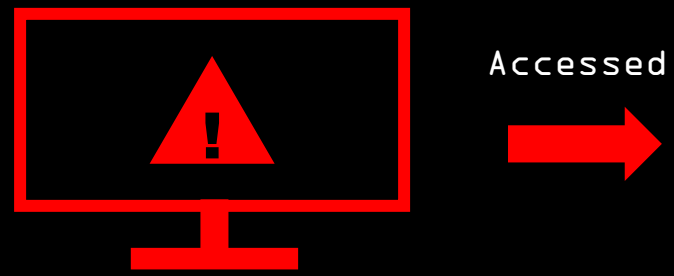
In the triggering phase, Stuxnet looked for:

> WIN-CC:

- > Machine Operating System
- > Managed Industrial Process

> Siemen's Step 7:

- > Software for Programmable Logic Controllers (operates centrifuges)



Infected Device

Accessed

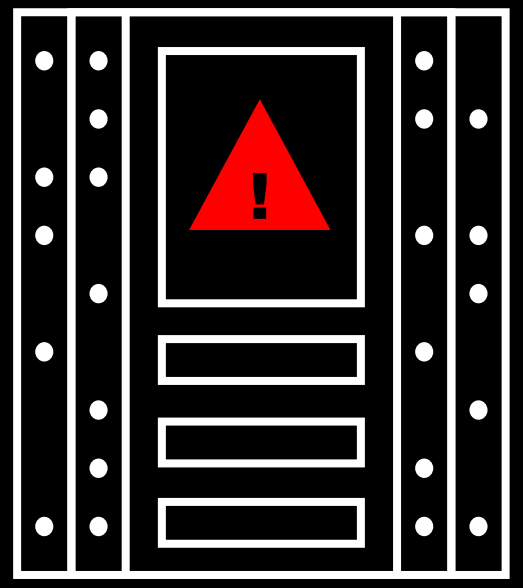
Programmable Logic Controller

C:\Worm-Structure\Execution

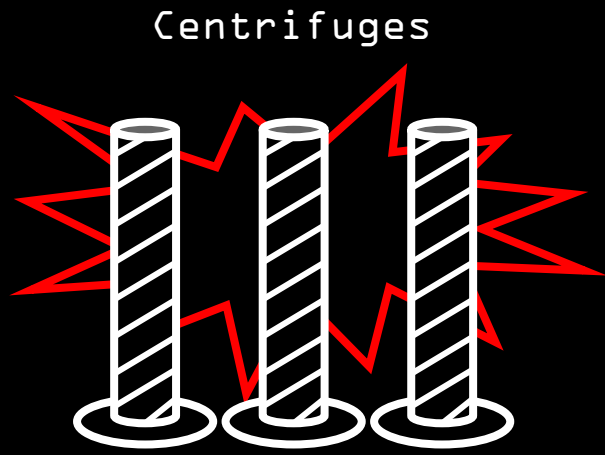
In the execution phase, the worm delivers the payload, meaning the main function or purpose of the virus is carried out.

> PAYLOAD FUNCTIONS:

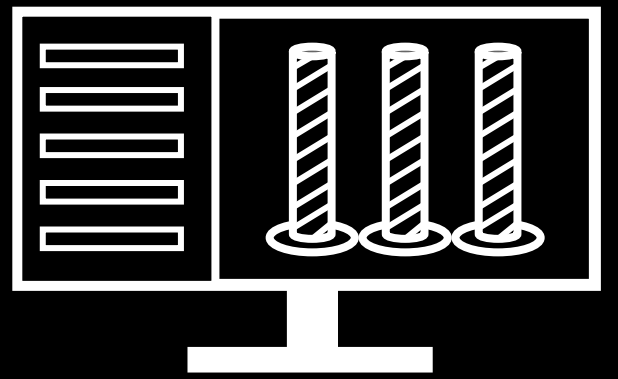
- > Alter centrifuge code to spin out of control
- > Feed artificial data to the Industrial Control System



Programmable Logic Controller



Centrifuges



Industrial Control System

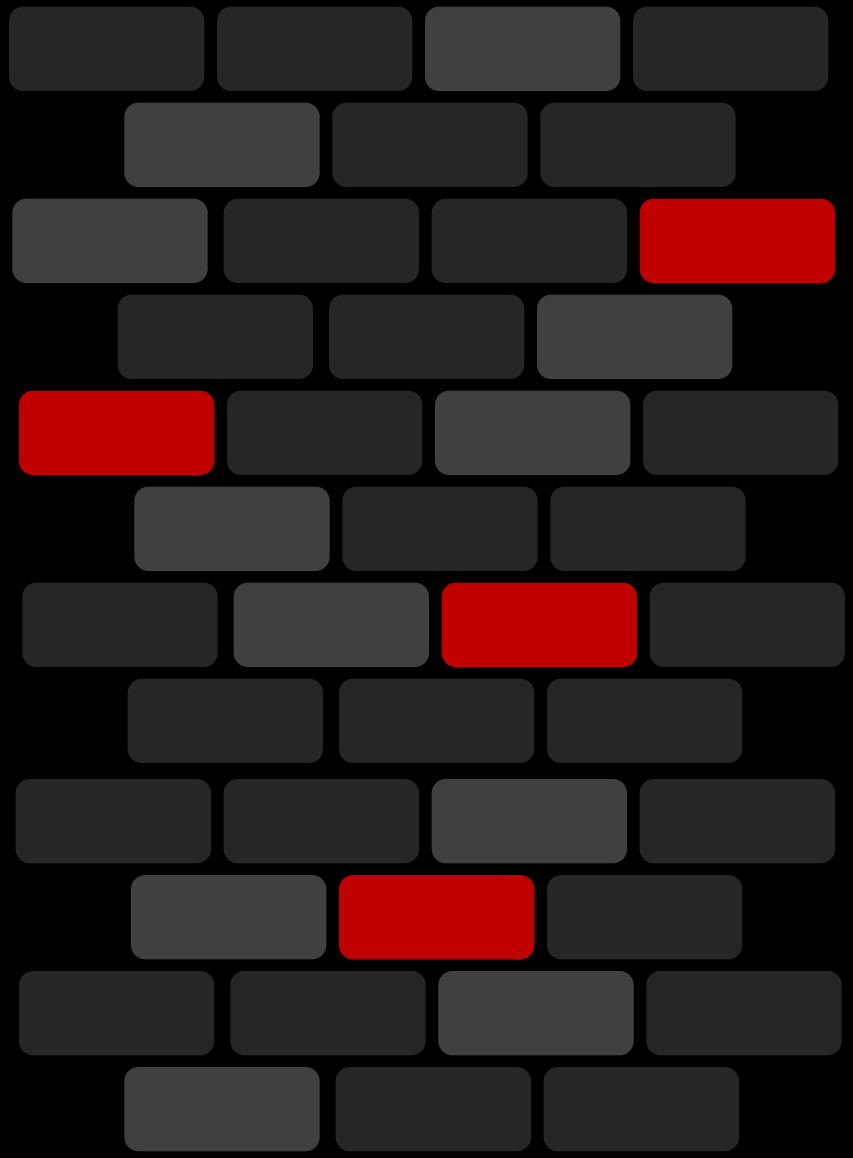
C:\Zero-Day\Exploits

Zero Days are vulnerabilities unknown to developers.

It is undetectable against antivirus software since its signature is unknown (IBM, 2024).

They cannot patch or defend against an attack they are not aware of.

Stuxnet used 4 Zero Days, two of which being a Windows shortcut vulnerability and Print Spooling.

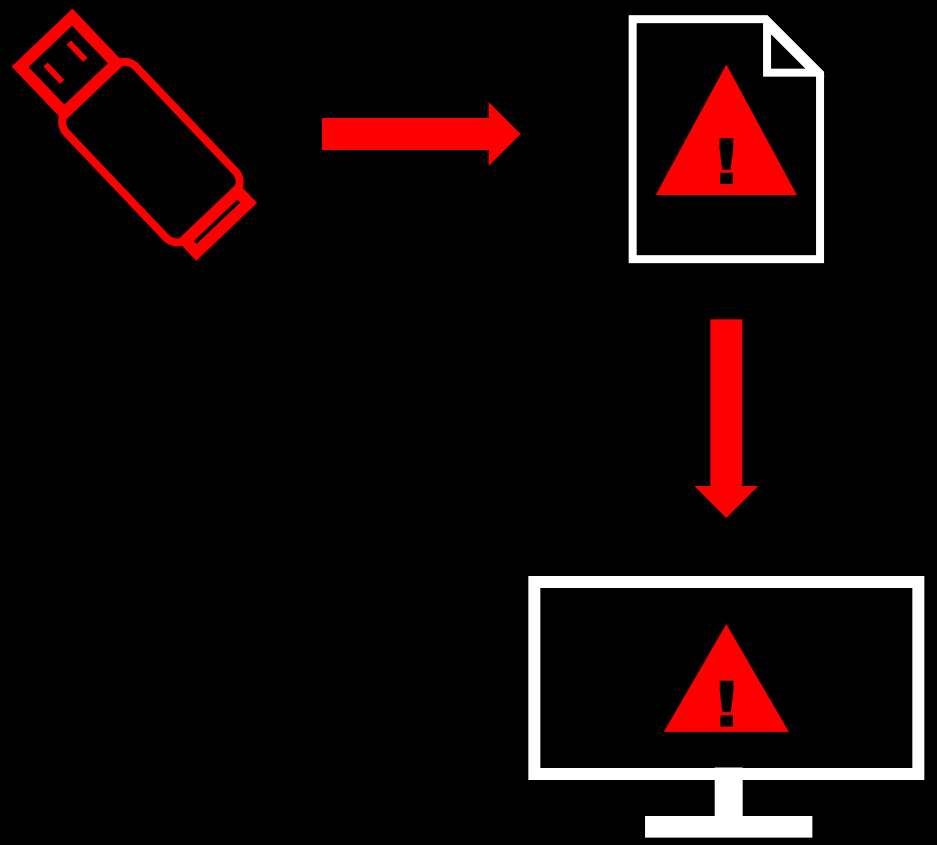


C:\Zero-Day\Windows-Shortcut

Vulnerability in Windows Shell Could Allow Remote Code Execution

> MS10-046

- > Viewing an icon could allow for remote code execution (Microsoft Security Bulletin, 2010)
- > If exploited could give a hacker the same user rights as the local user (Microsoft Security Bulletin, 2010)



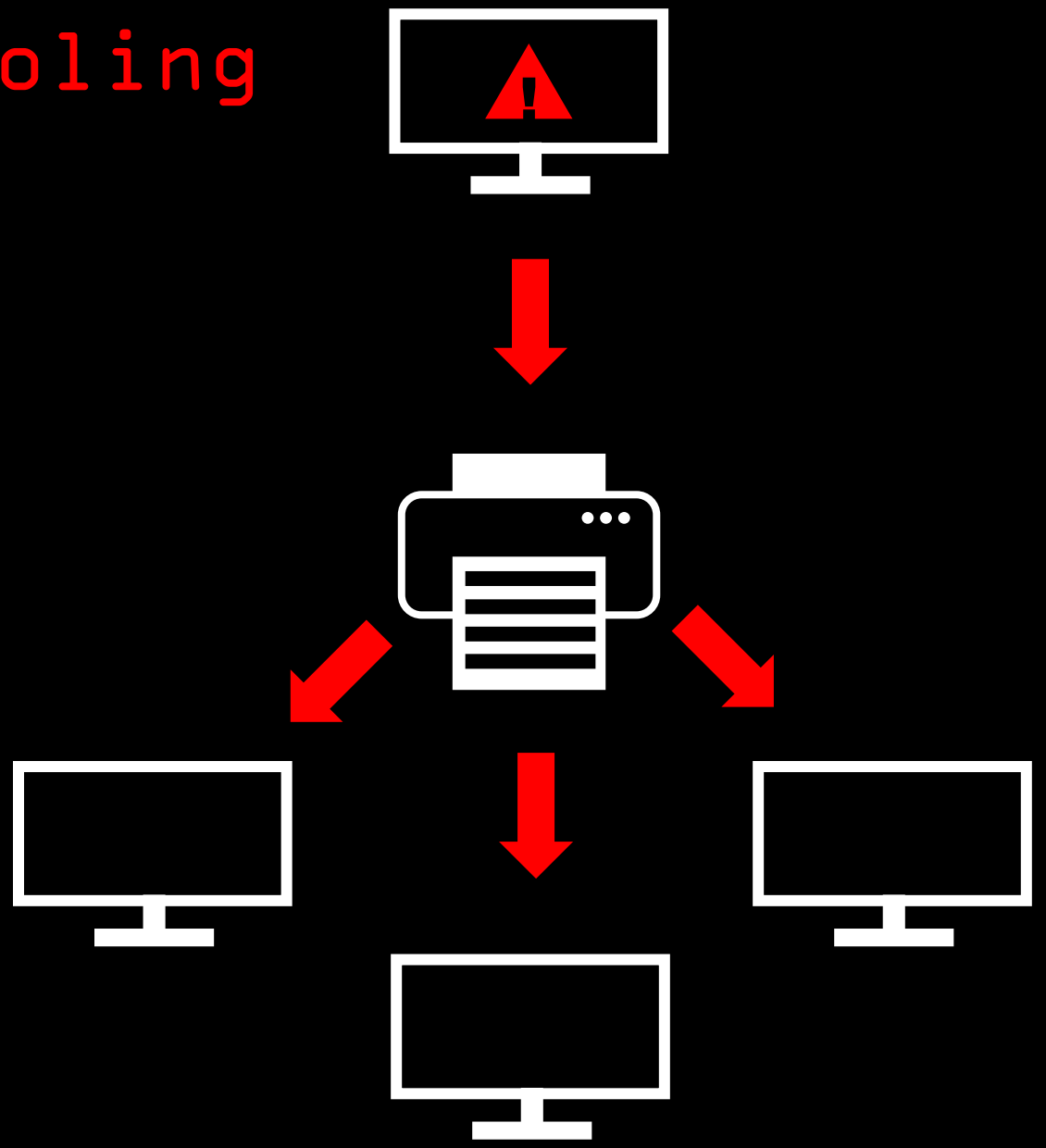
C:\Zero-Day\Print-Spooling

Vulnerability in Print Spooler Service Could Allow Remote Code Execution

> MS10-061

  > A print request could allow for remote code execution (Microsoft Security Bulletin, 2010)

  > This could give access to other devices connected to the printer



C:\Summary

- Understanding Stuxnet
- Worm Structure
  - Propagation Phase
  - Triggering Phase
  - Execution Phase
- Zero Day Exploits
  - Windows Shortcut
  - Print Spooling

PNGarts. (n.d.). World map transparent background PNG [PNG file]. PNGarts. https://www.pngarts.com/explore/108718. Modified by Charlotte Strobl.

D:\References

Knapp, E. D., & Langill, J. T. (2015). Hacking Industrial Control Systems. *Industrial Network Security*, 171–207. https://doi.org/10.1016/b978-0-12-420114-9.00007-1

Kushner, D. (2024, May 24). *The real story of stuxnet*. IEEE Spectrum. https://spectrum.ieee.org/the-real-story-of-stuxnet

IBM. (2024, September 11). *What is a zero-day exploit?*. IBM. https://www.ibm.com/topics/zero-day

Microsoft Security Bulletin. (2010, September 14). *Microsoft Security bulletin MS10-061 - critical*. Microsoft Learn. https://learn.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-061