



Case Study: Reverse Engineering the Stuxnet Worm

Explore the infamous Stuxnet worm. It was the first known cyberweapon. It targeted Iranian nuclear facilities. This event changed cybersecurity forever.



Introduction: What is Reverse Engineering in Cybersecurity?



Analyzing Malware

Understanding functionality through code analysis.




Identifying Vulnerabilities

Pinpointing weaknesses and attack vectors.



Essential for Defense

Protecting systems from future attacks.



Background: Stuxnet – The First Cyberweapon

Discovery in 2010

Identified by VirusBlokAda.

Targeted SCADA Systems

Sabotaged industrial equipment.

Joint US-Israeli Effort

Believed to be a state-sponsored attack.



Discovery of Stuxnet: How It Was Found in the Wild

1

System Malfunctions

Initial detection in Iran.

2

USB Drive Spread

Key infection vector.

3

Network Propagation

Rapid spread in industrial settings.

4

PLC Errors

Unexplained anomalies observed.

Initial Analysis: Behavior and Anomalies Observed



Complex Malware

Multi-component architecture.



Zero-Day Exploits

Leveraged unknown vulnerabilities.



Stealthy Propagation

Self-replicating and hidden.

MALWARE

Reverse Engineering Techniques Used on Stuxnet

Static Analysis

- Examining code without execution.
- Disassembly with IDA Pro.
- Identifying function calls.

Dynamic Analysis

- Observing behavior during execution.
- Sandboxing system calls.
- Debugging code execution.



Deep Dive: How Stuxnet Targeted Iranian Nuclear Facilities

Targeted PLCs

Manipulated industrial controllers.

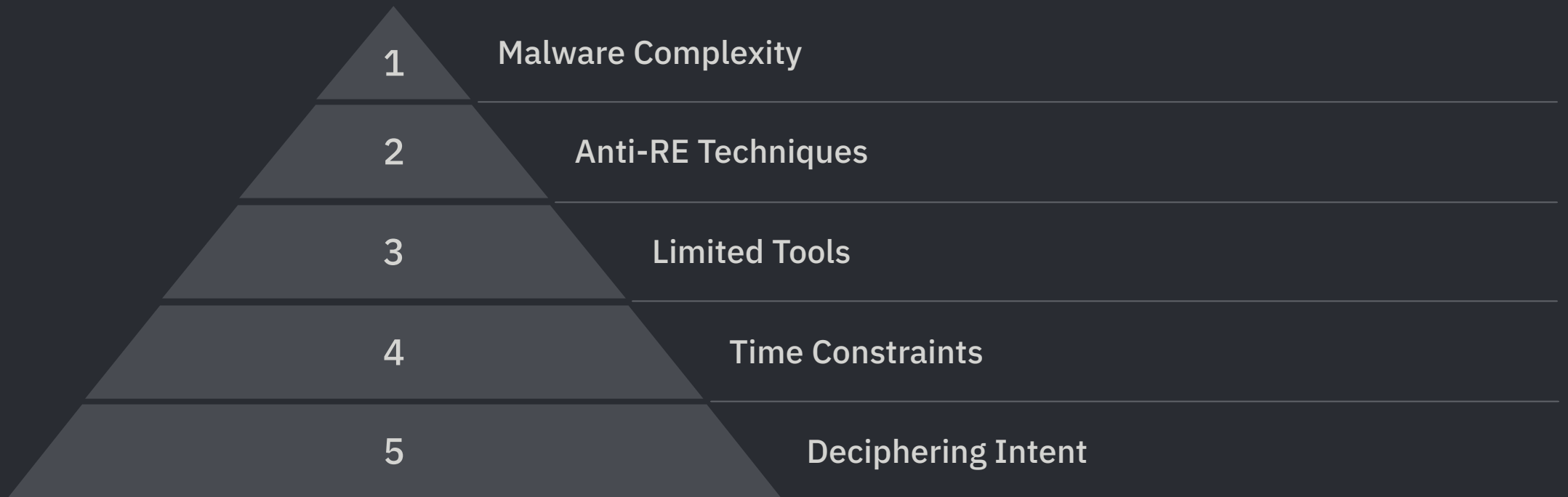
Modified Rotor Speeds

Caused physical damage to centrifuges.

Physical Destruction

Resulted in centrifuge failures.

Challenges Faced in Reverse Engineering Stuxnet





Impact of Stuxnet

2000

Centrifuges Destroyed
Significant physical damage.

1st

Nation-State Cyberweapon
Set a new global precedent.

100%

Awareness Raised
Focused on ICS security.

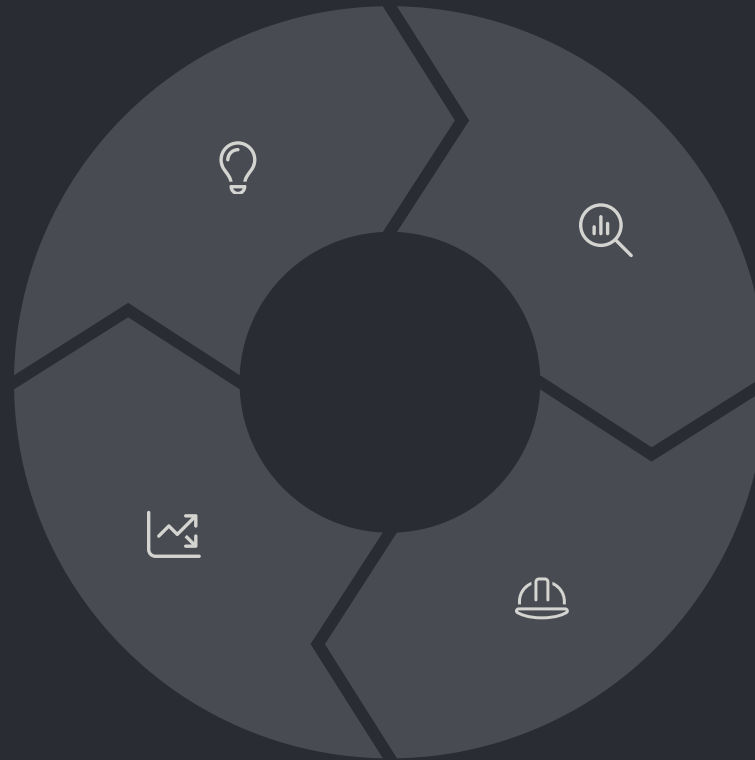
Conclusion

Watershed Moment

Changed cybersecurity forever.

Shape Practices

Lessons learned drive security.



RE is Crucial

Understanding and mitigating threats.

Infrastructure Vulnerabilities

Highlighted critical weaknesses.