

# **Case Study: Stuxnet**

## Case Study: Stuxnet

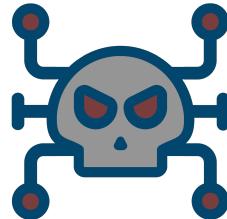
View as it was **analyzed**

View as an **incident response analyst**

- ◆ How would it have been **discovered?**
- ◆ What would you see?
- ◆ What can you **infer from the investigation?**



# **Stuxnet: The First Cyberweapon**



**0-day exploits** are extremely valuable and extremely rare  
**Stuxnet used 5 of them:**

### **Against Windows:**

- ◆ LNK file exploit to spread between USB media
- ◆ Print spooler exploit to spread on a local network
- ◆ Keyboard handler exploit to escalate privileges
- ◆ Task scheduler exploit also used to escalate privileges

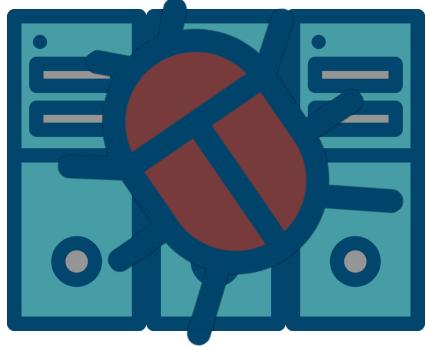
### **Against Siemens Programmable Logic Controller (PLC):**

- ◆ static password hardcoded into controller

## Other Peculiarities

- ◆ Auto-update mechanism
- ◆ Two different, valid code certificates.  
Both apparently stolen.
- ◆ No internet use
- ◆ Would spread, but take no action, unless the system drove a Siemens PLC with one of two specific cards in it, driving at least 33 centrifuges at specific spin rates.  
Indicates the author had a specific lab in mind as a target and intimate knowledge of the target configuration.





Actions

# Incidence Response Perspective



Network behavior



Antivirus signatures



Logging of new executables  
or libraries

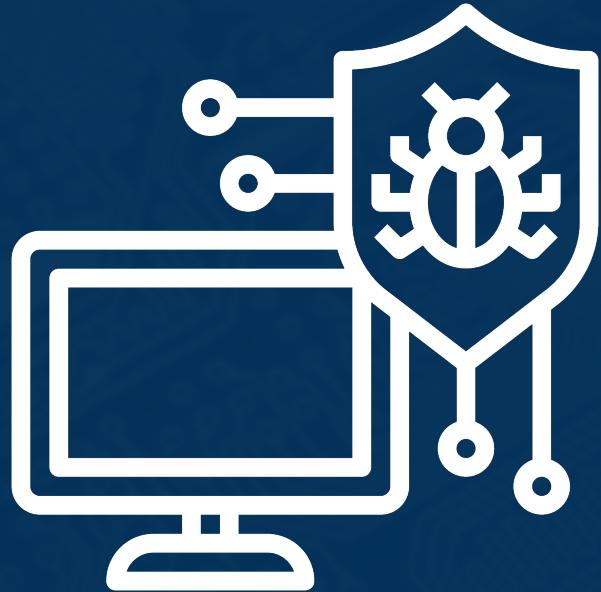


Installations of unsigned  
binaries

Things You Would Not Have Seen

## What Is Your First Sign of an Incident?

- ◆ If you're really lucky, **unusual behavior of a client**
- ◆ **Application whitelisting**, maybe
- ◆ An unusual number of centrifuges failing
- ◆ **Your AV company** finally finds it





## What is Hunt Teaming?

**Advanced security operations** function attempting to find a compromise by **manually searching for it**

### Methods of hunt teaming:

- ◆ Attack systems and see how to find the attack
- ◆ Model usage patterns and investigate departure from normal (may have found updates to Stuxnet)
- ◆ Assume a compromise and try to find it



## What is Hunt Teaming?



### Tooling

- ◆ Log management
- ◆ Endpoint detection and response

## How Would a Hunt Team Identify Stuxnet?

- ◆ New DNS query for update traffic
- ◆ Executing a tmp file
- ◆ Unusual executables in memory

