Stuxnet e Mitre ATT&CK

Mariano Ceccato

mariano.ceccato@univr.it

The worm

- First uncovered in 2010
- The target is supervisory control and data acquisition (SCADA) systems
- Believed the responsible to damage the Iranian nuclear program
  - Campaign against Natanz industrial plant
- History's first field experiment in cyber-physical weapon technology
  - No country officially admitted responsibility

https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

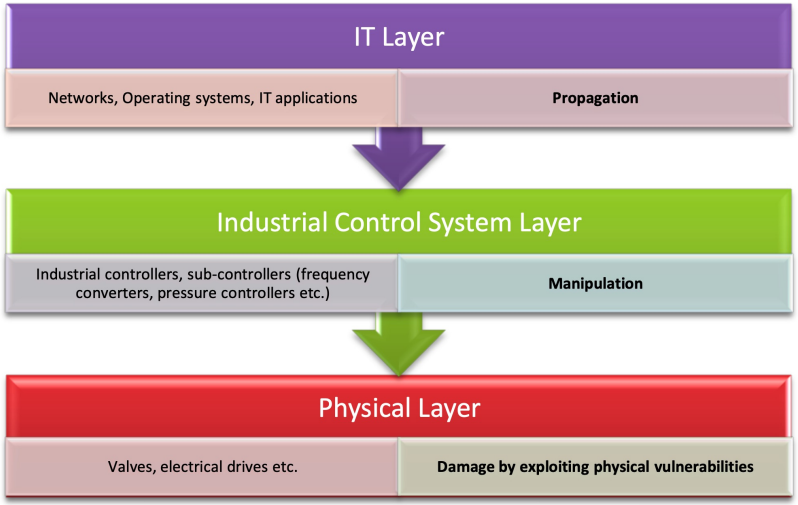
Specific or generic?

- The design features of the plant that was attacked
- Specifically crafted to hit just one singular target that is so different from common critical infrastructure installations
  - Attack was highly specific: only Siemens S7-417 & S7-315 controllers
  - Attack tactics and technology can be generic
    - Roughly 30 nations employ offensive cyber programs, including North Korea, Iran, Syria, and Tunisia

Attack engineering

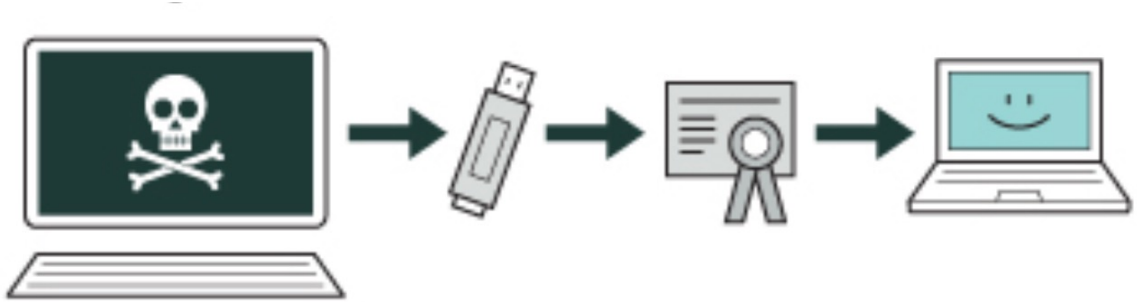
- 3-layer attack: 3 specific vulnerabilities
- Interaction of these layers can be leveraged to create physical destruction by a cyber attack

1. **IT layer:**
   - used to spread the malware
2. **Control system layer**:
   - used to manipulate (but not disrupt) process control
3. **Physical layer:**
   - where the actual damage is created



1 Infection

- Stuxnet enters a system via a USB stick
  - Airgap isolates the plant network: direct access not possible
- It proceeds to infect all the machines running MS Windows
- The worm evades automated detection systems using stolen digital certificates, that shows that it comes from a reliable source



Several vulnerabilities

- The USB stick contains a Windows shortcut (LNK file) to execute code
- Remote procedure call (RPC) to infect other computers in the private network
- Infection of shared printers to spread the worm
- LNK/PIF vulnerability: a file is executed when an icon is viewed (in Windows Explorer).

Spread

Country	Share of infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Other countries	9.2%

2. Search

- Stuxnet checks if a machine is part of the target industrial control system
- The target is an Iranian system of high-speed centrifuges for enriching nuclear fuel
  - Presence of Siemens Step7 software
  - A computer controlling Siemens S7-417 & S7-315 controllers
- In case these 2 conditions are not met, the work becomes dormant

3. Update

- If the system is not the target, Stuxnet does nothing
- It it is, Stuxnet attempts to access the Internet to download a more recent version of itself

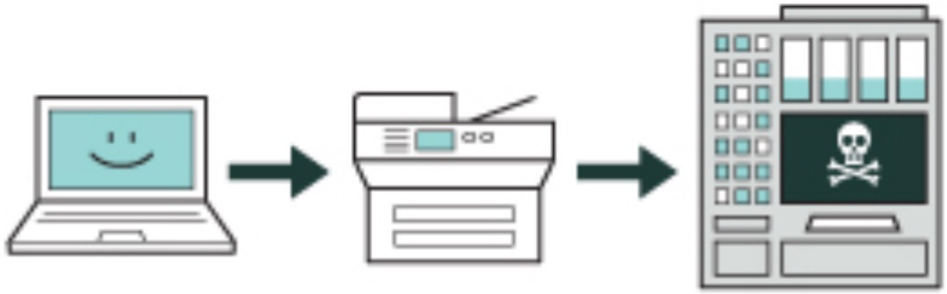
Command and control

- Two C2C servers in Denmark and Malaysia
  - Update in case of internet access
  - Upload data for industrial espionage and for infection monitoring

- NDS records will redirect data to try and disable the malware

4. Compromise

- The worm compromises the target system's logic controller
- "Zero days" vulnerabilities are exploited: software weaknesses that have not been identified by security experts



Compromise steps

- Stuxnet infects project files belonging to Siemens WinCC/PCS 7 SCADA control software (Siemens Step 7)
  - SCADA: Supervisory Control And Data Acquisition
  - It subverts a key communication library of WinCC
  - Intercepts communications between the WinCC software (Windows) and the target Siemens PLC devices
  - Install itself on PLC devices unnoticed
  - Subsequently mask its presence from WinCC if the control software attempts to read an infected block of memory from the PLC system.

5. Control

- Stuxnet spies on the operations of the target system
- Gathered information are used take control of the centrifuges, to spin them to failure

Man in the middle

- Input and output signals are passed from the electrical peripherals to the legitimate program logic and vice versa by attack code that has positioned itself “in the middle”.
- Legitimate control logic is executed only as long as malicious code permits it to do so
- Essentially a rootkit for PLCs.

6. Deceive and destroy

- Stuxnet provides false feedback to outside controllers
- They would not know what is going wrong until it is too late
  - Speed reading of centrifuges seems fine on the dashboard


KEANU REEVES DENNIS HOPPER SANDRA BULLOCK
GET READY FOR RUSH HOUR.
SPEED
JUNE 10

Replay legitimate sensor readings

- Sensor values are recorded for a period of 21 seconds
- These 21 seconds are replayed in a constant loop during the execution of the attack
  - These data are shown on SCADA screens in the control room
    - Human operator in the control room
    - Software implemented alarm routine
- Legitimate code continues to execute but receives fake input values, and any output (actuator) manipulations of legitimate control logic no longer have effect

First attack: over-pressurize centrifuges

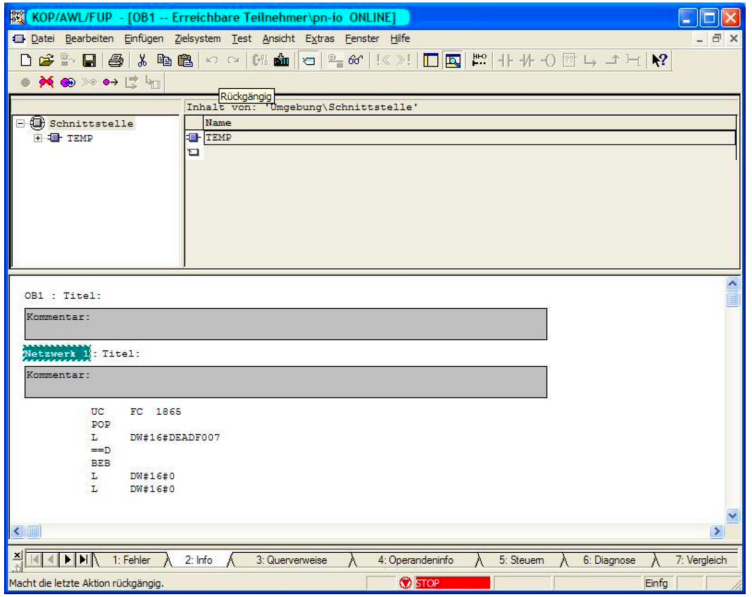
- De-calibration of the pressure sensors
  - Responsible of translating pressure into an analog output signal
- The pressure controller then acts accordingly by never opening the stage exhaust valves
  - actual pressure keeps rising
- Emergency safety controls
  - The same tactic used for the exhaust valves and the additional pressure transducers.

Second attack: over-speed centrifuges

- Centrifuge Drive System (CDS) that controls rotor speeds
- Attack operates periodically: once per month
- Attack: changing rotor speeds
  - Normal operating speed of the IR-1 centrifuge is 63,000 rpm
  - Stuxnet increases speed by 30% to 84,600 rpm for 15 minutes
    - Avoid in catastrophic damage
    - Good chance of creating damage (cause the rotor to vibrate and create resonance)

SCADA dashboard

- It displays the exact speed values from the time before the attack sequence executes
- The SCADA software gets its information from memory in the controller, not by directly talking to the engine



Cover

- Potentially simultaneous destruction of hundreds of centrifuges per infected controller
- The malware would have been detected fairly easily by engineers in post-mortem analysis
- Great care to avoid catastrophic damage
- Real objective: increase rotor stress, thereby causing rotors to break early, but not necessarily during the attack run

Maximizing damage

- Simultaneous catastrophic destruction of all operating centrifuges would not have set back the Iranian nuclear program longer enough
  - Plenty of centrifuges in stock for replacing a massive destructive event

- Pakistan managed to go from zero to successful production within just 2 years
- The same effort took Iran over 10 years

- Stuxnet started as nuclear counter-proliferation and ended up to open the door to cyber weapon technology proliferation that is much more difficult to control

References

- Ralph Langner “To Kill a Centrifuge. A Technical Analysis of What Stuxnet’s Creators Tried to Achieve” The Langner Group, November 2013
- Kushner, David. "The real story of stuxnet." ieee Spectrum 50.3 (2013): 48-53.
- Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." White paper, Symantec Corp., Security Response 5.6 (2011): 29.