Lecture 11

dinsdag 20 december 2022 10:36

Triton targets Schneider Electric Triconex

attacks target Saudi Aramco oil

SIS (safety instrumented systems) → bring system from unsafe state back into safe state

→ industrial facilities can be dangerous places

↓

minimize risk by applying several protection layers

risk → may still be too much

layers fail → accidents happen

conditions violated → bring back to safe state

completely separated from process control system

logic solver programmed with system integrity functions

SIS failure can be prevented with redundancy

attacks:

1. Cause plant shutdown
   introduces notable change in safety system
   - 1.1 create operational uncertainty
   - 1.2 trip safety 'fail-states' i.e. cause system to shut itself down, e.g. by changing threshold value
2. put plant into unsafe physical state
   requires much more knowledge of system
   long preparation required

network segmentation:

- air-gap / isolation
- interfaced SIS → point-to-point connection between SIS controller and process controller
- integrated SIS (2 zones) → firewall, but direct communication between devices (higher attack surface)
- integrated SIS (1 zone) → everything online, process workstation = SIS workstation

attack:

1. compromise control system
2. compromise SIS network
3. deploy Triton framework

Phase 1: watering hole websites to target industrial employees and get foothold

execution by scheduled tasks

WMI implant for remote execution

image file execution options injection — program can be debugged with 'some program' → malware

abuse of VPN

persistence by scheduled tasks

plant web shells on Exchange server

Thinstall for packaging malware (portable software packages)

timestomping, tool & log cleanup

malware from Microsoft Corporation

custom e.g. Open SSH binaries

Mimikatz — dump credentials from memory

RDP, modified PsExec

staging of exfiltrated directories

C2: SSH, dynDNS from afraid.org

C2 ports include 443, 8531 (→ microsoft update)

Shellcode:

- stage 1: verify + prepare memory
- stage 2: override handling function
- stage 3: backdoor; bypass key switch
- stage 4: ???

found due to memory consistency check

↓

shutdown when inconsistency found

mitigation:

- connect only necessary networks
- only switch to program mode when necessary
- code signing

monitoring / detection:

- configuration analytics (device + config (e.g. program mode))
- network analytics (e.g. traffic spikes)
- threat indicators — e.g. known threats
- threat behavior — log operations which might indicate a threat