Hello From the OT Side!

Daniel Kapellmann Zafra
Technical Analysis Manager
danielkapellmann.z@fireeye.com
www.kapell.tech
@Kapellmann

Image generated with imgflip.

What's the Deal With OT?

- IT and ICS are not the same.
- Isolated ICS systems were safer.
- Yet, there is growing integration.
- Operational Technologies (OT).
- Then attack surface grows.

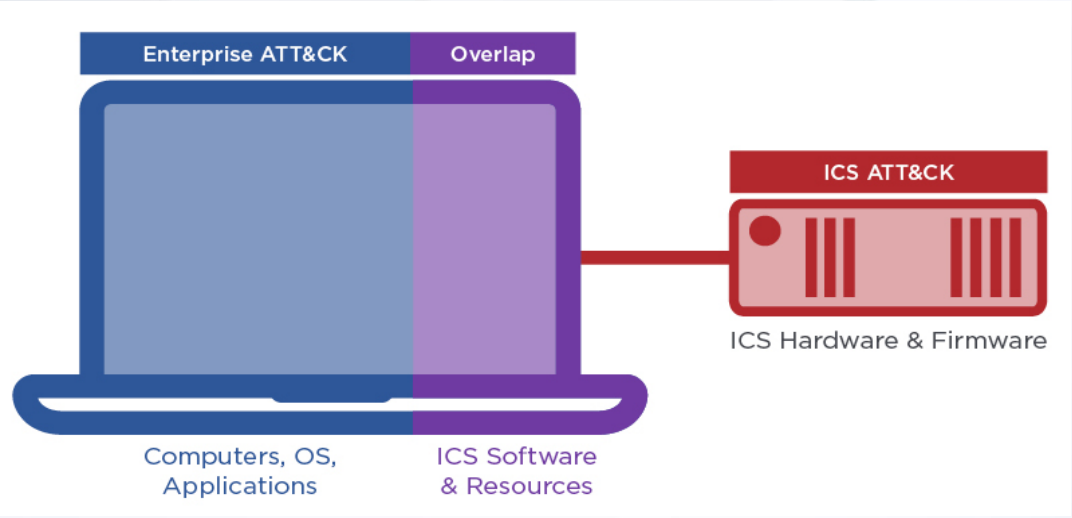
Just Stop Doing It, Duh!

- Why is this happening if it sounds so dangerous?
- Because it works…
- The Industry LOVES IT!

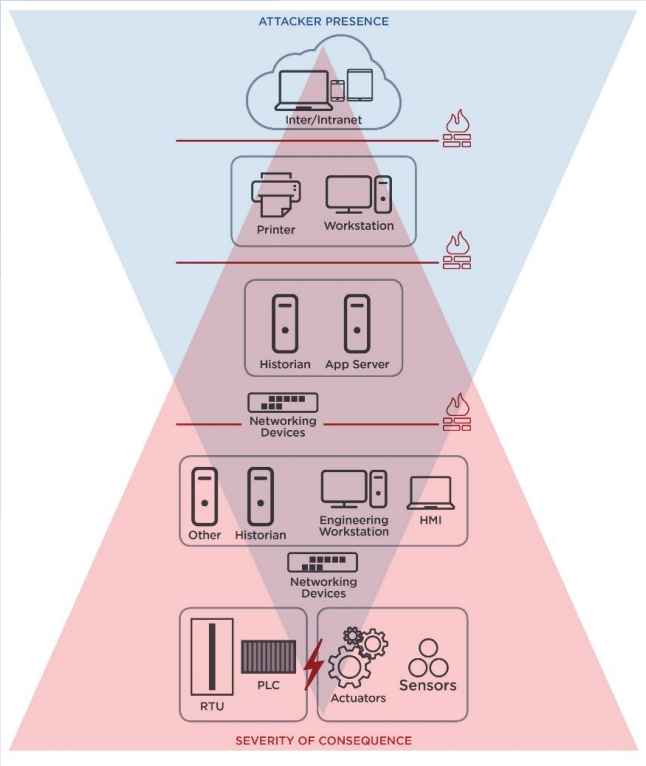
Dangerous by Nadja Robot (CC BY-NC 2.0)

As a Result, We Have an Overlap…

Intermediary Systems: "…computers (servers and workstations) and networks using the **same or similar OS and protocols** as used in IT that serve as an **avenue for impacting physical assets or processes**."

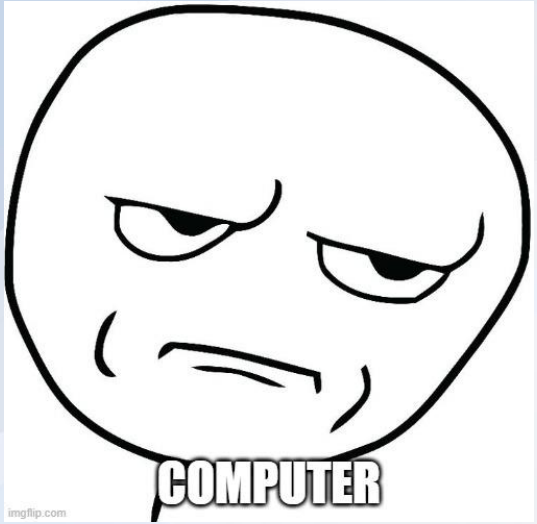


Funnel of Opportunity & Intermediary Systems



- Timeline of the intrusion and proximity to physical world
- As the intrusion progresses, the severity of negative outcomes becomes higher
- Difficult to detect as footprint grows smaller and fewer security tools to defend

Tomato / Tomahto?

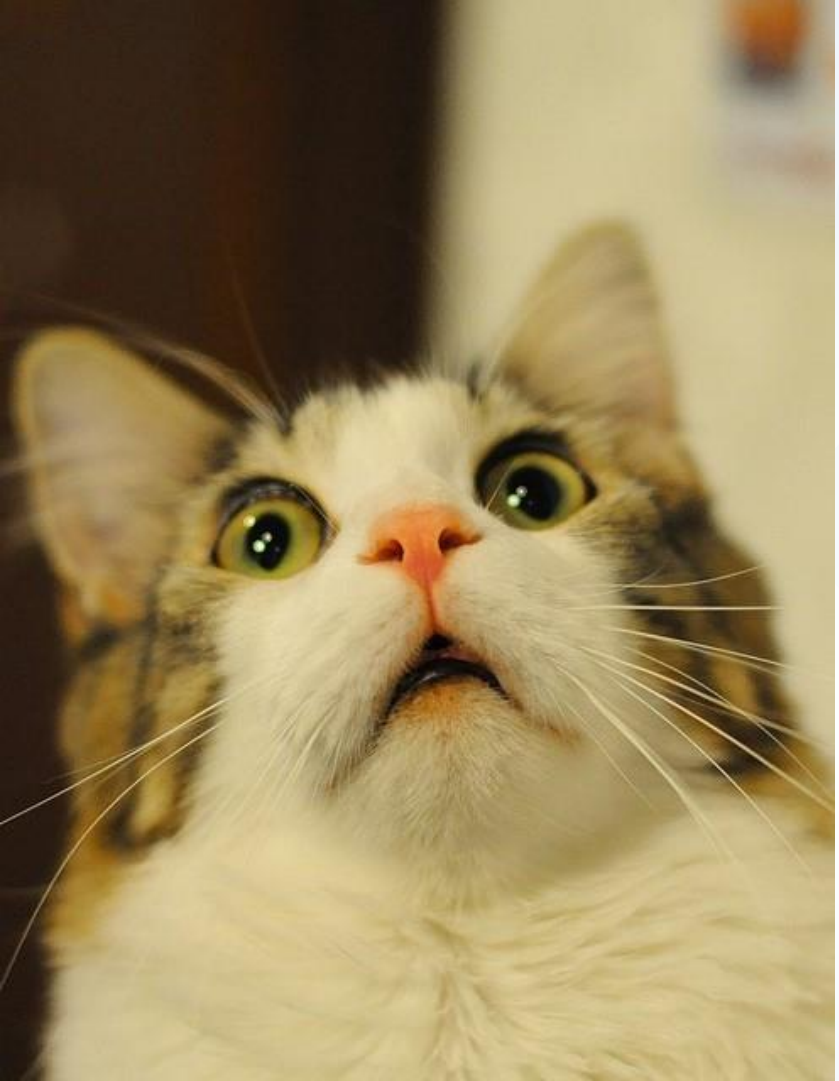


Images generated with imgflip and Flaticon Freepik.

Stories That Keep OT Awake at Night

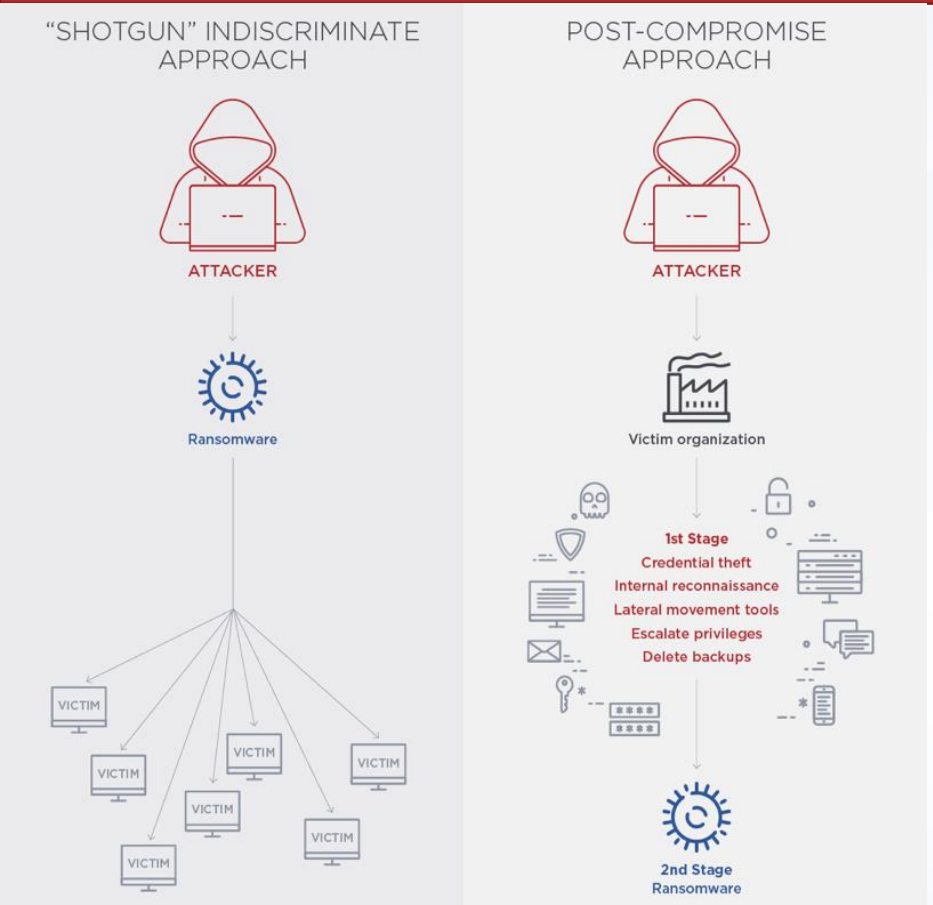
OT Cyber Security Incidents Matrix (OT-CSIO)

ATTACK	SOPHISTICATION	IMPACT				
		Compromise	Data Theft	Degradation	Disruption	Destruction
Targeted	Low	Logging into internet-connected devices (e.g. using Shodan)	Threat actors selling VNC access to SCADA systems	Russian scientists arrested for mining crypto-currencies at Federal Nuclear Center in Sarov		Shamoon
	Medium	TEMP.Isotope Reconnaissance Campaign			Maroochy Shire Sewage Spill and Ukraine 2015 Post-compromise ransomware campaigns (e.g. Megacortex, LockerGoga, or Ryuk)	Ukraine 2015
	High				Ukraine 2016 TRITON Attack	Stuxnet
Non-Targeted	Low	Financially-motivated actor inadvertently accesses internet-connected HMI while conducting mass scanning / brute forcing of RDP/VNC servers		Cryptomining Malware on European Water Utility Portable Executable File Infector Malware Impacting Windows-based OT assets	WannaCry Infection on HMIs	
	Medium					
	High					



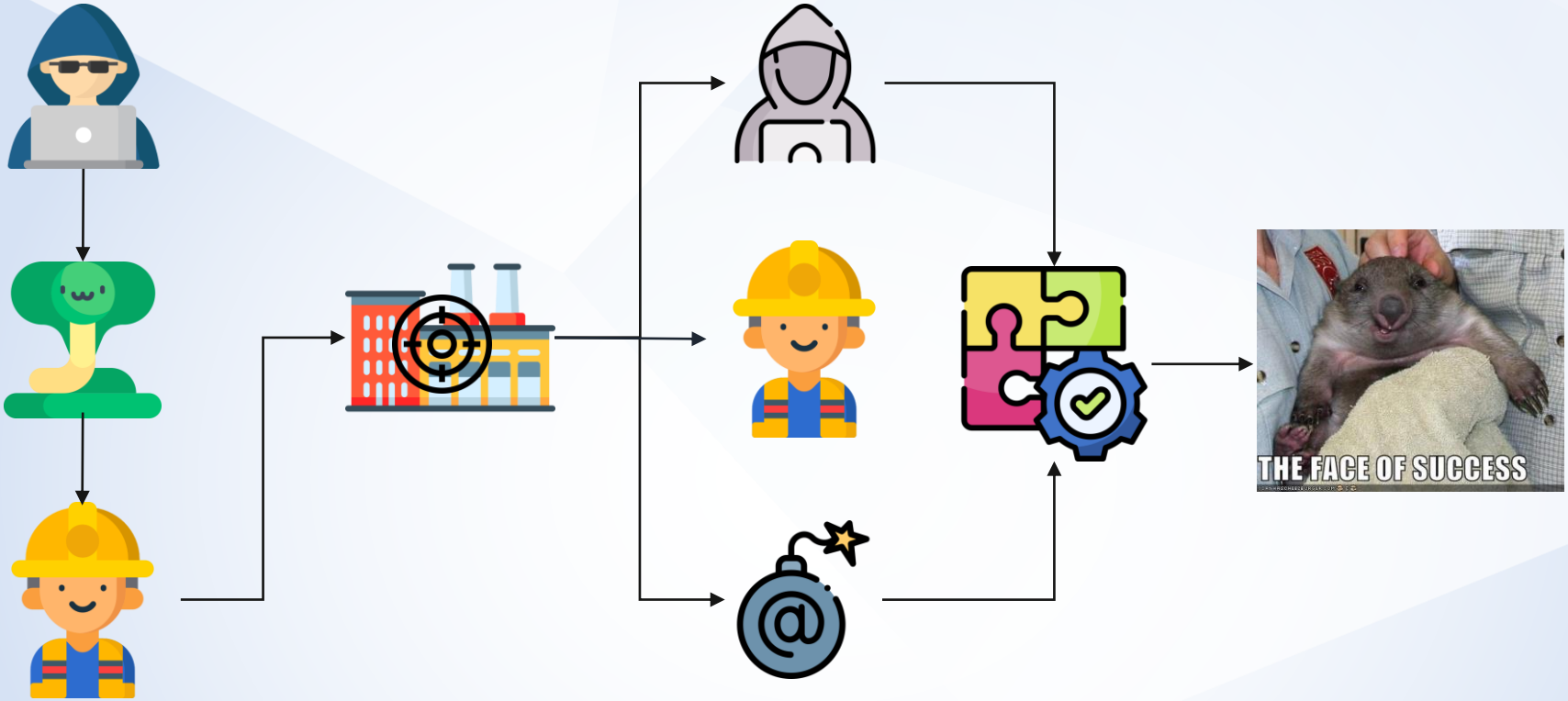
- **Case 1:** Post-Compromise Ransomware
- **Case 2:** TRITON Attack
- **Case 3:** Reconnaissance Campaigns
- **Case 4:** Internet-Connected Assets
- **Case 5:** Portable Executable Infectors

Case 1: Post-Compromise Ransomware



- Increasing ransomware incidents on industrial/critical infrastructure organizations
- Evolution from indiscriminate to post-compromise operations
- If actor can't monetize stolen data, production processes are alternative to profit

Case 1: The Tale of the SNAKE(HOSE)



Icons from Flaticon Freepik, Becris, and Cheezburger.com.

Case 1: Results of Joint Analysis

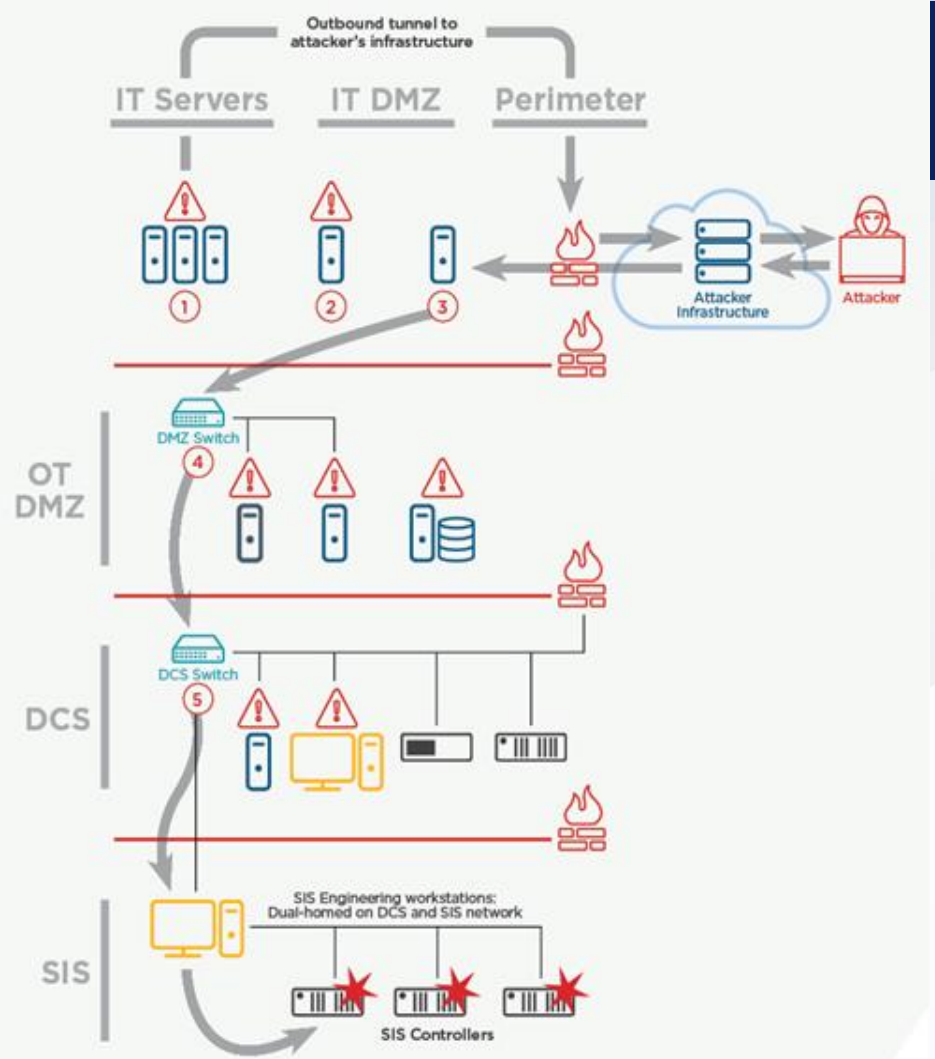
```
taskkill /im proficy administrator.exe /f
taskkill /im ntevl.exe /f
taskkill /im prproficymgr.exe /f
taskkill /im prrds.exe /f
taskkill /im prrouter.exe /f
taskkill /im prconfigmgr.exe /f
taskkill /im prgateway.exe /f
taskkill /im premailengine.exe /f
taskkill /im pralarmmgr.exe /f
taskkill /im prftpengine.exe /f
taskkill /im prcalculationmgr.exe /f
taskkill /im prprintserver.exe /f
taskkill /im prdatabasemgr.exe /f
taskkill /im preventmgr.exe /f
taskkill /im prreader.exe /f
taskkill /im prwriter.exe /f
taskkill /im prsummarymgr.exe /f
taskkill /im prstubber.exe /f
taskkill /im prschedulemgr.exe /f
taskkill /im cdm.exe /f
taskkill /im musnotificationux.exe /f
taskkill /im npmdagent.exe /f
taskkill /im client64.exe /f
taskkill /im keysvc.exe /f
taskkill /im server_eventlog.exe /f
taskkill /im proficyserver.exe /f
taskkill /im server_runtime.exe /f
taskkill /im config_api_service.exe /f
taskkill /im fnplicensingservice.exe /f
taskkill /im workflowresttest.exe /f
taskkill /im proficyclient.exe4 /f
```

DoppelPaymer, LockerGoga, Maze, MegaCortex, Nefilim and SNAKEHOSE

```
000600C8  CCESERVER.EXE
00060190  CCPROJECTMGR.EXE
00060258  SIEMENS.INFORMATIONSERVER.DISCOVERSERVICEINSTALLER.EXE
00060320  SIEMENS.INFORMATIONSERVER.ISREADY.PLUGINSERVICE.EXE
000603E8  SIEMENS.INFORMATIONSERVER.SCHEDULER.EXE
000604B0  OPCUASERVERWINCC.EXE
00060578  S7ASYSVX.EXE
00060640  SCORECFG.EXE
00060708  SSERVCFG.EXE
000607D0  SIMNETPNPMAN.EXE
00060898  S7WNRMSX.EXE
00060960  SIM9SYNC.EXE
00060A28  S7WNSMSX.EXE
00060AF0  CCCAPHSERVER.E
00060BB8  CCDBUTILS.EXE
```

CLOP Sample

Case 2: TRITON Attack



- **Corporate & IT DMZ:** remote access, credentials, and recon data
- **OT DMZ:** pivot towards the DCS and SIS
- **DCS:** reach the SIS controllers
- **SIS:** Attacker objective

Case 2: TRITON Tools

- Leveraged custom tools to avoid anti-virus detection and at a critical intrusion phases
- Exploited intermediary systems throughout the entire attack lifecycle.
- Only last step differed from other incidents.

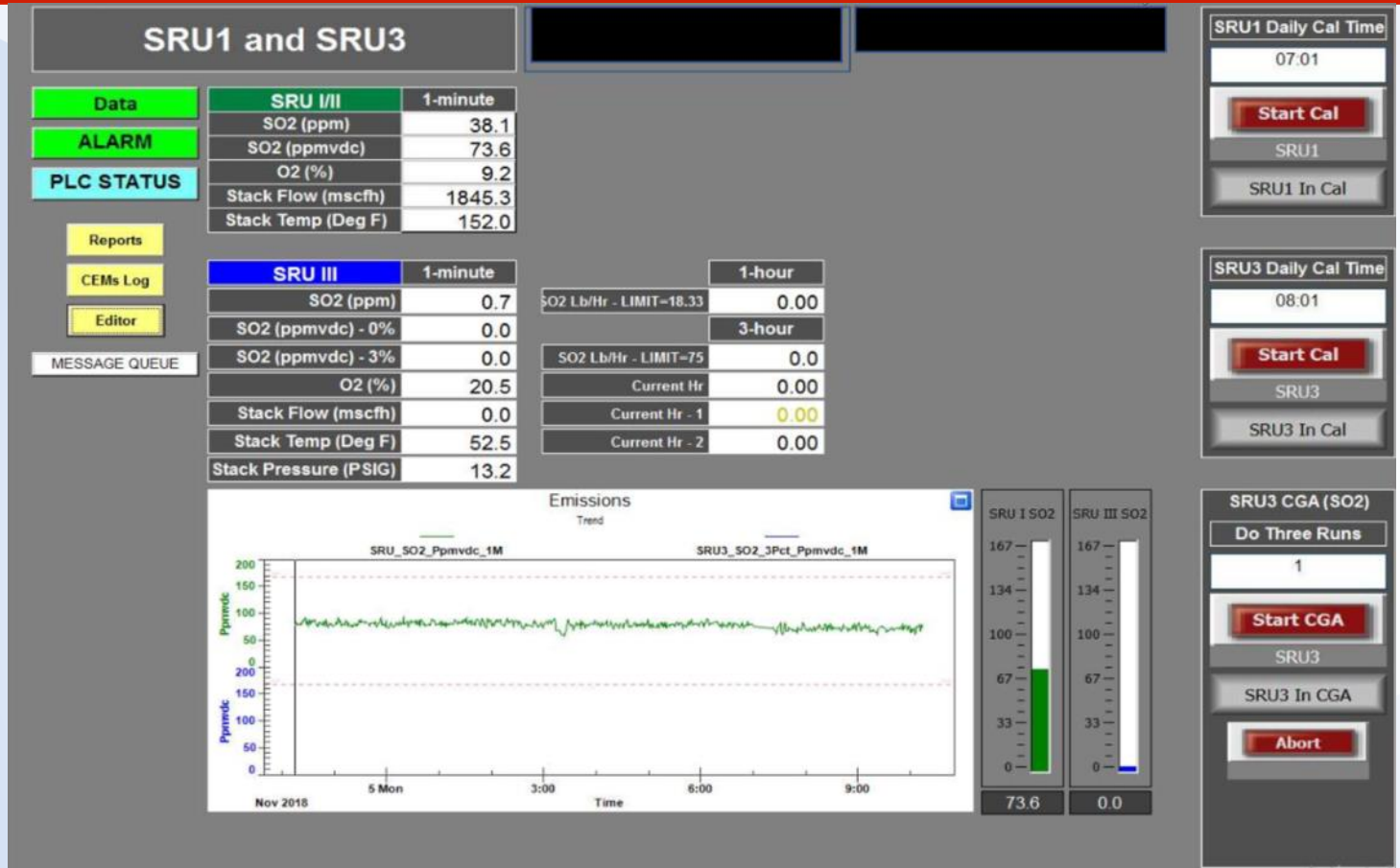
TOOL	COMPONENTS	PURPOSE	ATTACK LIFECYCLE STAGE						
			Initial Compromise	Establish Foothold	Escalate Privileges	Internal Reconnaissance	Move Laterally	Maintain Presence	Complete Mission
SecHack	KB77846376.exe	Credential harvesting			X	X			
	KB77846376.exe.x64								
NetExec	NetExec.exe	Remote command execution							
	runsvc.exe	NetExec runner					X		
Cryptcat-based backdoor	cryptcat.exe cryptsvc.exe svchostpla.exe	Backdoor							
	compattelprerunner.exe	C&C domain name generator		X					
	ProgramDataUpdater.xml	Scheduled task file (persistence mechanism)							
PLINK-based backdoor	napupdatedb.exe	Backdoor		X				X	
Bitvise-based backdoor	alg.exe userinit.exe csrss.exe	Backdoor							
	tquery.dll txflog.dll cryptopp.dll DEFAULT DEFAULT.BAK	Backdoor components					X	X	
OpenSSH-based backdoor	spl32.exe WinSAT.exe csrss.exe	Backdoor							
	clusapi.dll PolicMan.dll verifier2.dll misc.mof setup.ini	Backdoor components					X	X	
WebShell	logoff.aspx	Modified legitimate Outlook Web Access Component							
	flogon.js	Modified legitimate Outlook Web Access Component				X		X	
	ftpexts.tlb	Output file containing credentials harvested by logoff.aspx							

Case 3: Filtering the Noise - Recon

Reconnaissance Campaigns

CASE	DESCRIPTION	DETERMINATION OF OT SCOPE
TEMP.Isotope 2017 [13]	Cluster of threat activity targeting energy and other critical infrastructure sectors leveraging spear-phishing and strategic watering holes.	• Spear phishing directed at engineers • Watering holes on strategic industry sites • Uncovered activity accessing HMIs and other process-related information
APT33 2019 [14]	Password-spraying attacks across thousands of organizations.	• Dozens of industrial equipment and software firms targeted (among other victims)
WildPressure 2020 [15]	Malicious campaign distributing Milum trojan across victims in the Middle East.	• At least some targets were related to the industrial sector

Case 4: Internet-Exposed Assets



Case 5: Portable Executable Infectors

File Name	Function	MD5	PE Infecting Malware Family
CCAlgIAlarmDataCollector.exe	HMI Alarm Logger	3eaa5863a3c6cc2c01585ebb727f5b0f	Sality
RsActivityLogServ.exe	HMI Activity Logger	b925509bcc00ffb4ced0302cdd9a9e1f	Tank
EventViewer.exe	Physical Security Alarm Viewer	e63ad3c1b5df66a0c432e6bfbb7e1591	Sality
4004be11be1736a92dd2fbe5de9a8725.virus	OPC Server	4004be11be1736a92dd2fbe5de9a8725	Sality
s7otbxsx.exe	STEP7 Communication	3fb51613fa61a768272dd6c379e3b11e	Parite

Shared Challenges

- **Case 1:** Stop financial actors
- **Case 2:** Detect targeted OT activity
- **Case 3:** Reduce noise
- **Case 4:** Avoid critical asset exposure
- **Case 5:** Stop malware propagation

Image from Daniel Kapellmann.

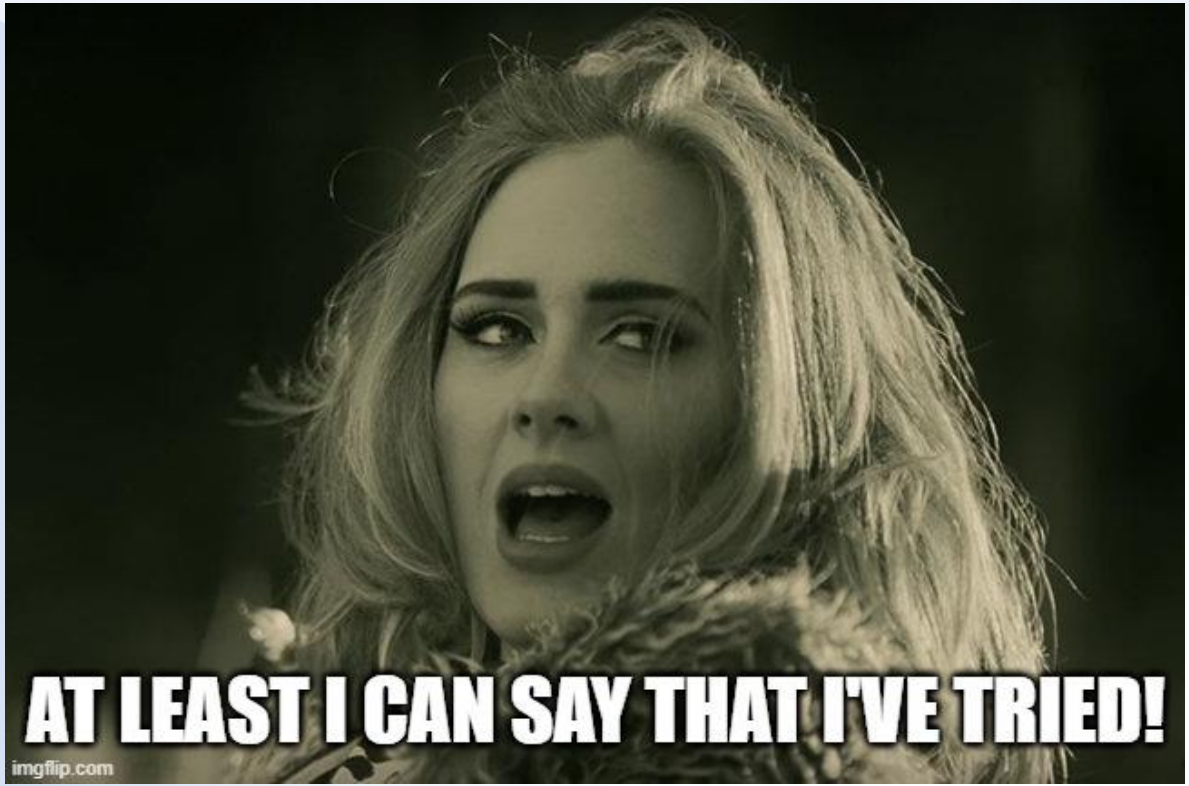


Image generated with imgflip.

Questions?

Daniel Kapellmann Zafra
Technical Analysis Manager
danielkapellmann.z@fireeye.com
www.kapell.tech
@Kapellmann