MANDIANT

Bad and Evil: Real ICS Security Incidents and Findings from Live ICS Assessments

SANS ICS Asia Pacific Summit 2020

Moath Sakaji

FIREEYE

Presentation Flow

- whoami
- Timeline
- The Triton Case
- Recent Observations
- Questions?

whoami

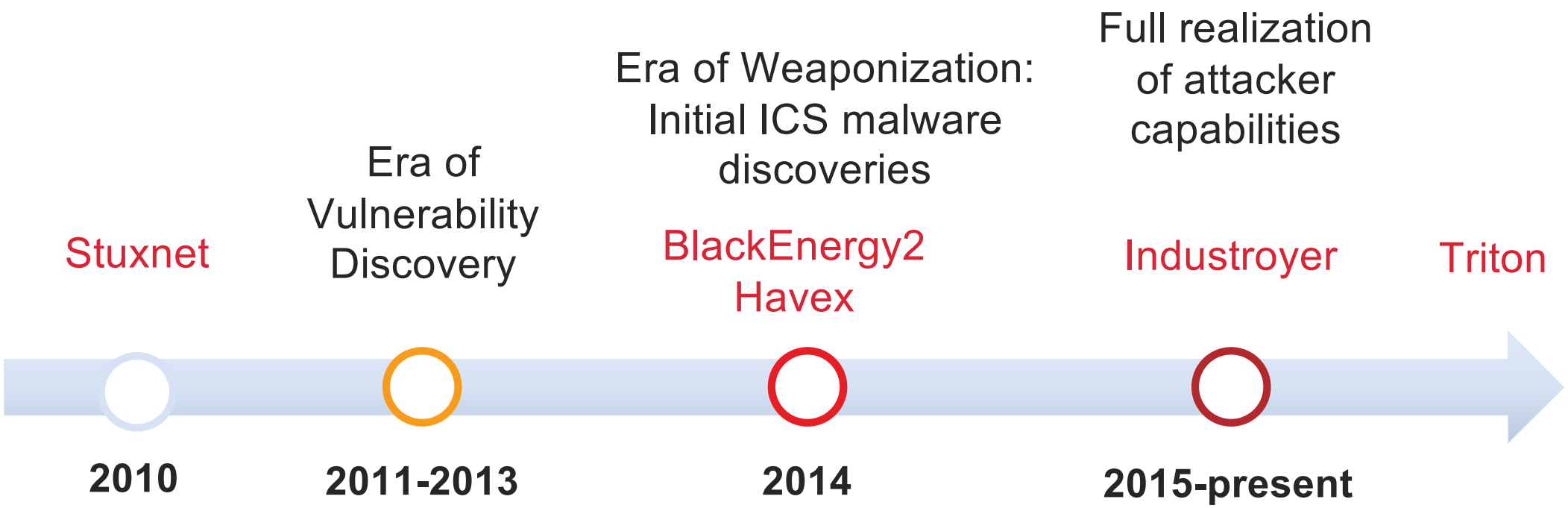
@MoathSakaji

Moath Sakaji

- Moath Sakaji
  - MEA Lead Consultant @Mandiant @FireEye


MANDIANT
Timeline

Recent History of ICS Security



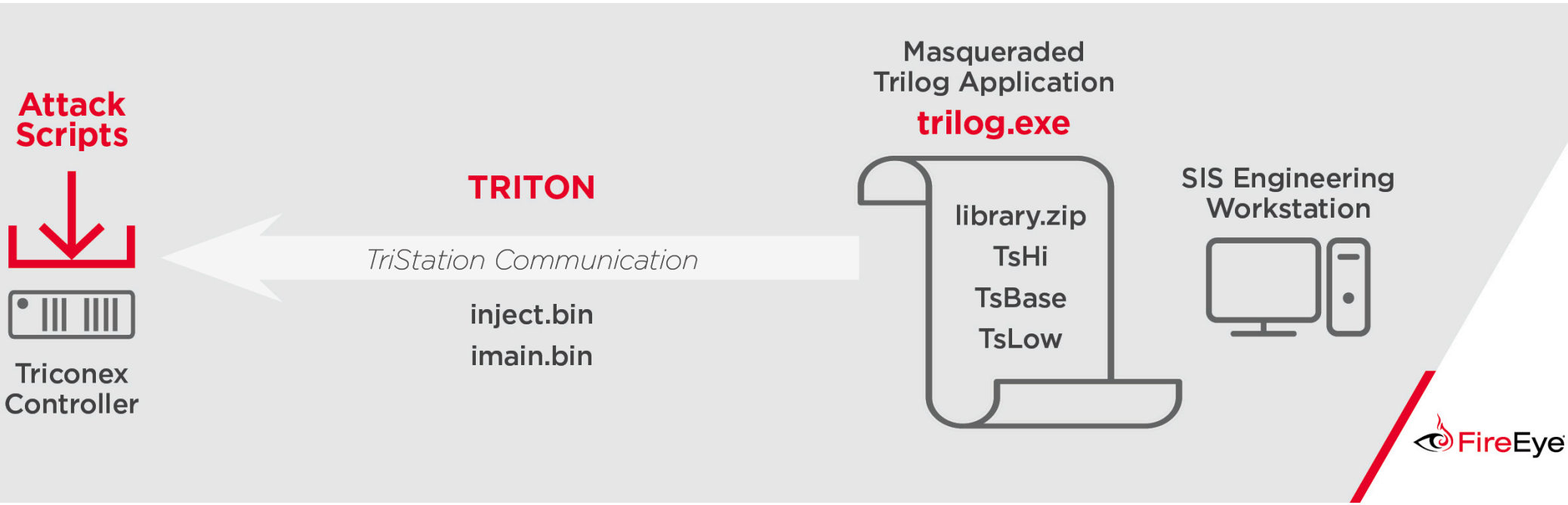
The Triton Case

The Triton Case

- Mandiant responded to an incident at a critical infrastructure organization

- Why it mattered?

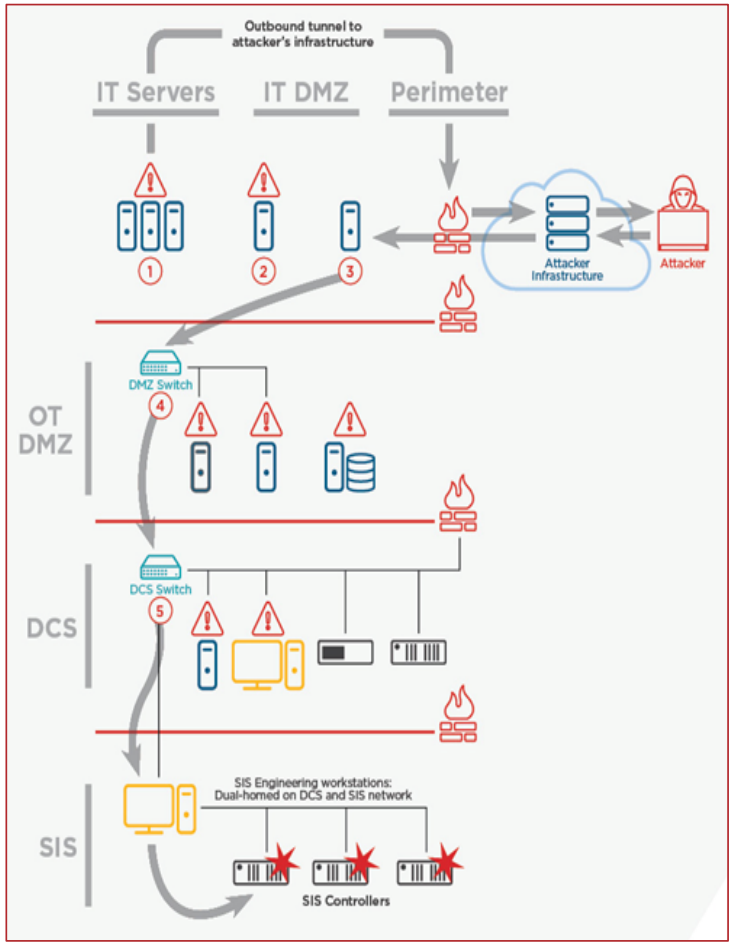
The Triton Case



The Triton Case

IT

The compromise of IT and IT DMZ provided the attacker with remote access, credentials, and recon data needed for their objective



OT DMZ

The compromise OT DMZ was required to act as a pivot point towards the DCS and SIS segments

DCS

The attacker compromised DCS systems

SIS

TRITON was ultimately used to interact with and impact Triconex SIS

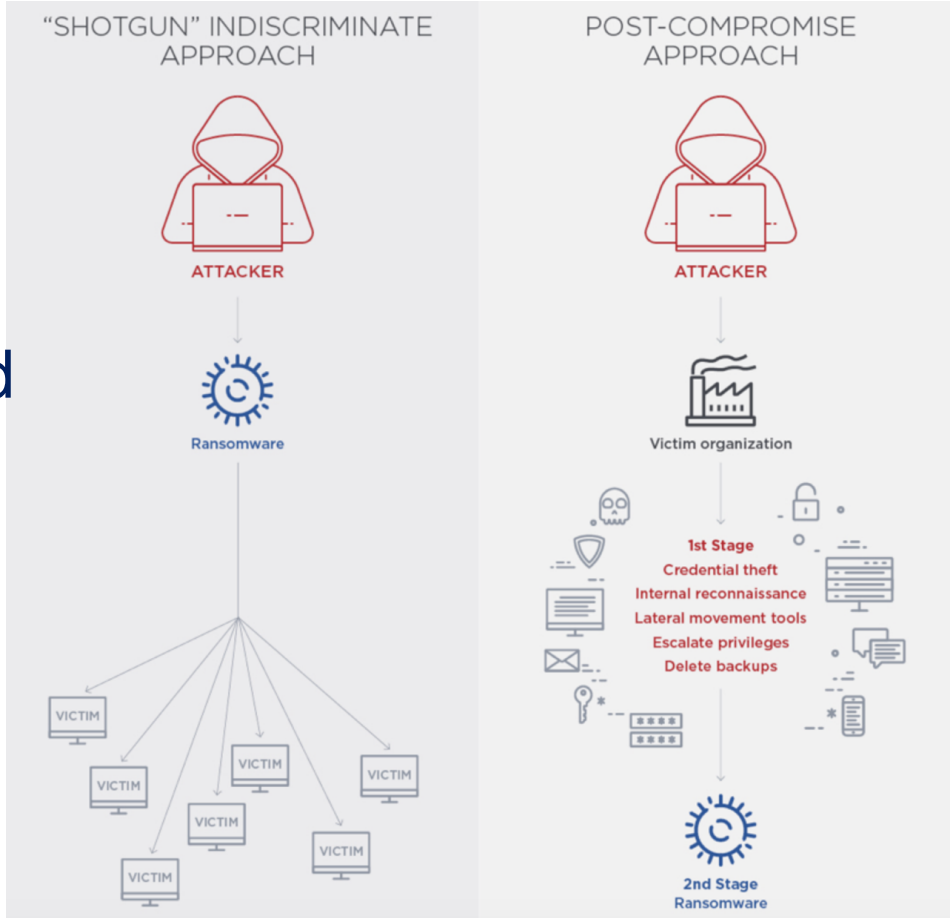
Recent Observations

Findings Still Exist

- Vulnerable infrastructure by nature
- Patterns in findings
- Similarities across multiple clients/ industries

Organized Financial Crime Actors Have Demonstrated an Ability to Disrupt OT Assets

- A trend of financial crime groups interested in OT
- We analyzed the increased trend
- We will look at two sample process kill lists



Kill List 1- kill.bat

- Associated with at least 6 ransomware families
- GE Proficy processes
- Possible loss of historical data

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

```
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
```

Kill List 2- Clop

Associated with CLOP malware

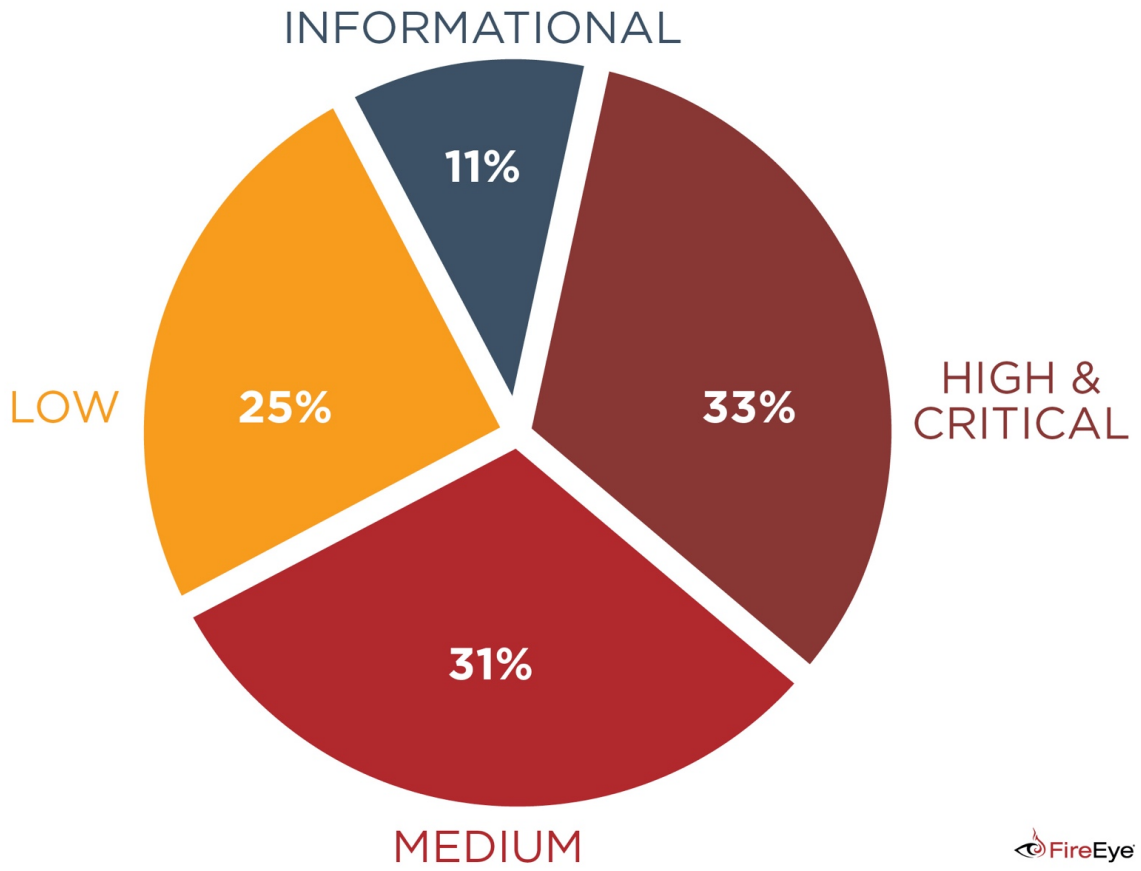
Loss of view/control over the physical processes

```
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
```

Vendor	Product
Siemens	SIMATIC WinCC
Beckhoff	TwinCAT
National Instruments	Data Acquisition Software (DAQ)
Kepware	KEPServer EX
OPC Unified Architecture (OPC-UA)	N/A

Findings Analysis

33% of findings rated high and critical



Critical and High Findings Analysis

HIGH-CRITICAL RISK CATEGORY	DISTRIBUTION
Vulnerabilities, Patches, and Updates	32%
Identity and Access Management	25%
Architecture and Network Segmentation	11%
Encryption and Authentication	8%
Network Management and Monitoring	7%
Insecure Services Enabled	5%
Misconfigurations	5%
Cyber Security Governance and Best Practices	4%
Other	2%

FireEye

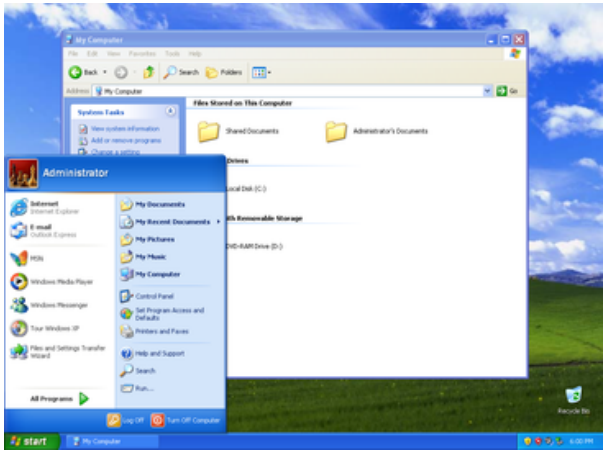
Critical and High Findings Analysis

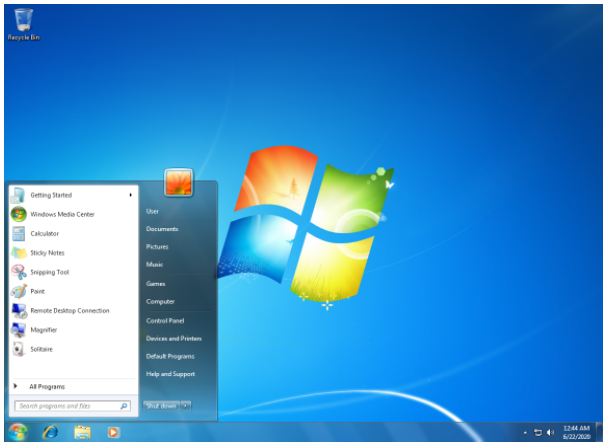
HIGH-CRITICAL RISK CATEGORY	DISTRIBUTION
Vulnerabilities, Patches, and Updates	32%
Identity and Access Management	25%
Architecture and Network Segmentation	11%
Encryption and Authentication	8%
Network Management and Monitoring	7%
Insecure Services Enabled	5%
Misconfigurations	5%
Cyber Security Governance and Best Practices	4%
Other	2%

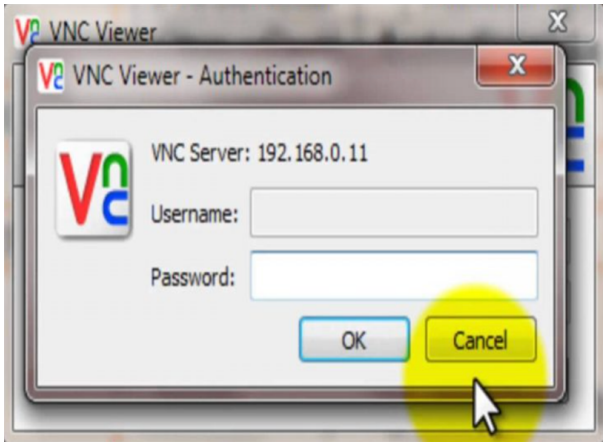
68% of critical and high findings are due to one of these three

FireEye

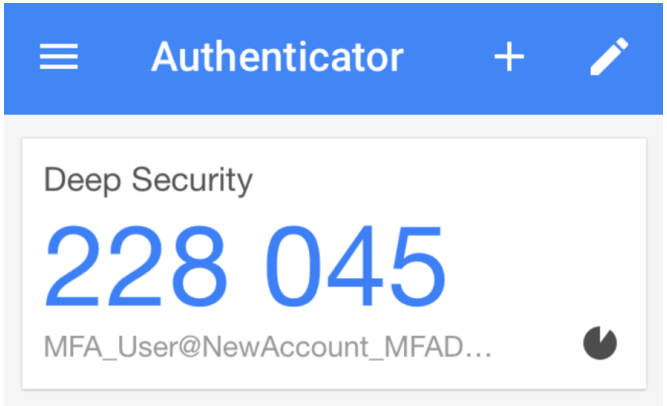
Vulnerabilities, Patches, and Updates

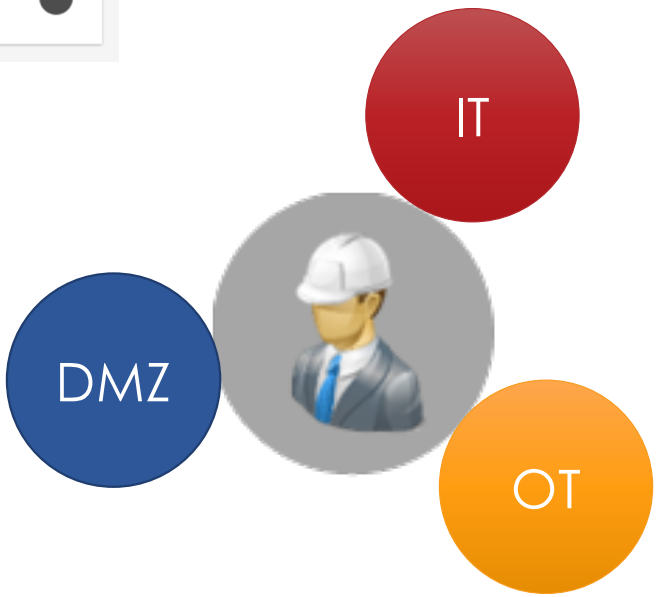




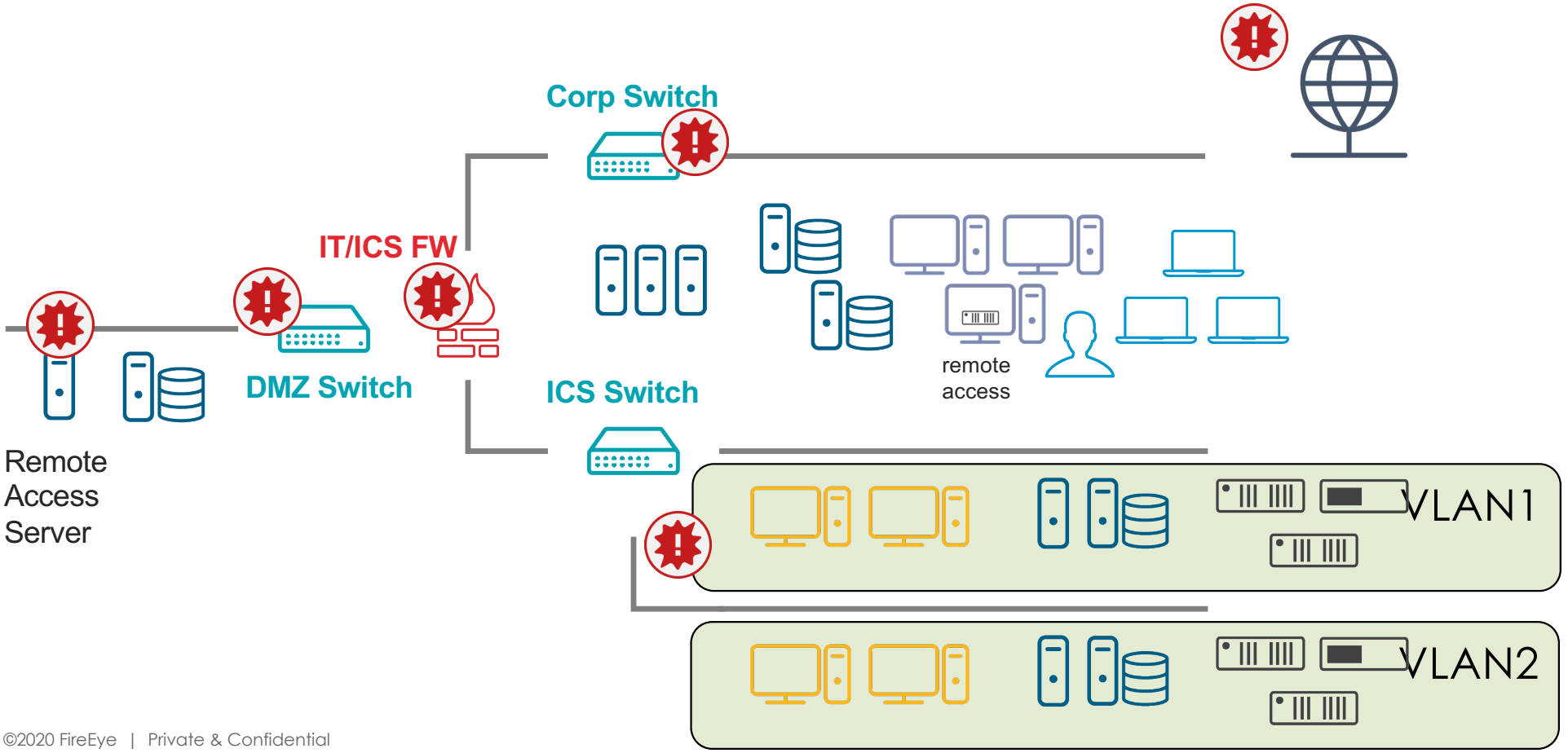


Identity and Access Management

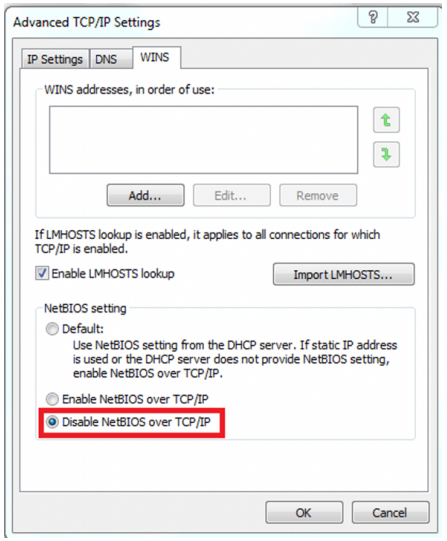


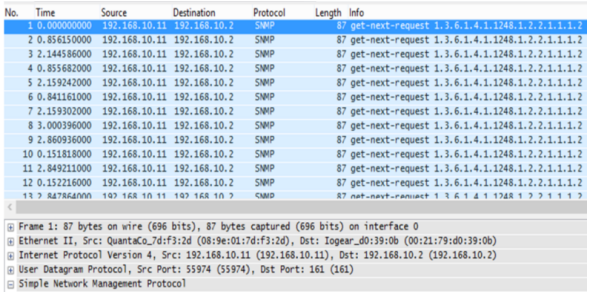


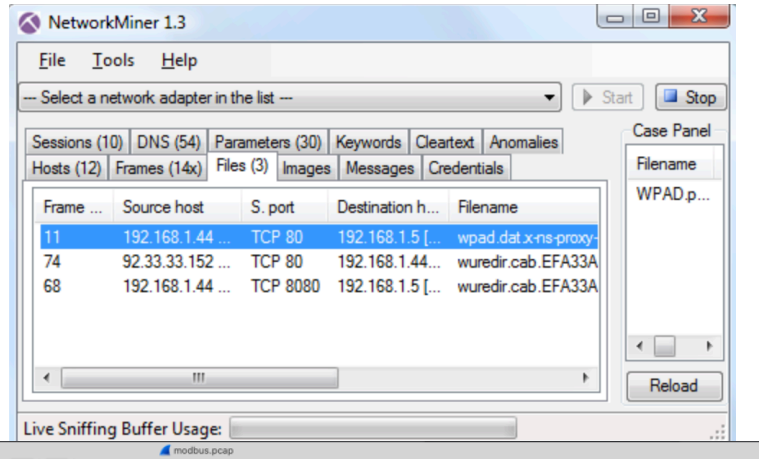
Network Segmentation and Segregation

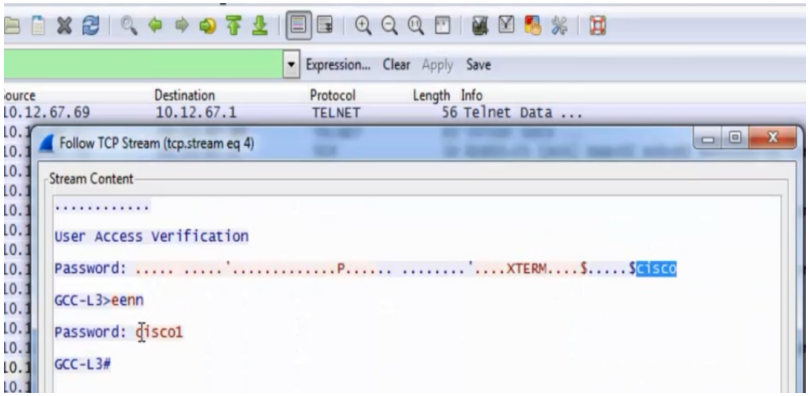


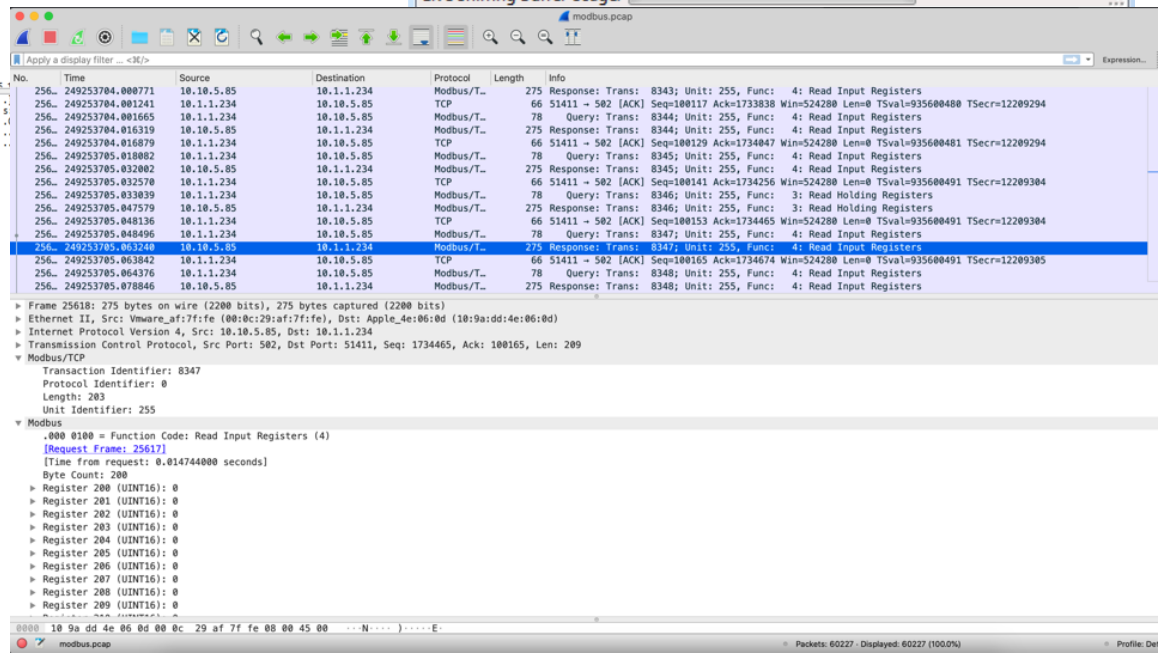
Insecure Services Enabled/ Used












MANDIANT
The End