DRAGOS

VULNERABILITY BRIEFING

ICS/OT CYBERSECURITY

YEAR IN REVIEW 2022

Logan Carpenter
Vulnerability Researcher
Dragos, Inc.

Nick Cano
Vulnerability Researcher
Dragos, Inc.

AGENDA

1. INTRODUCTIONS
2. MALWARE HEADLINES
3. STATE OF ICS VULNERABILITIES
4. DRAGOS APPROACH
5. TAKEAWAYS & RECOMMENDATIONS

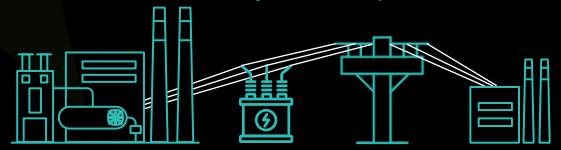
MALWARE HEADLINES

History of ICS Malware

CRASHOVERRIDE

Effective techniques with little knowledge of protocols used.

IEC101, IEC104, IEC61850/MMS, OPC-DA



PIPEDREAM

Combines aspects of CRASHOVERRIDE and TRISIS.

Significant breadth and depth of protocol and controller knowledge.

HAVEX

2010 | 2013 | 2015 | 2016 | 2017 | 2022

STUXNET

BLACKENERGY

TRISIS

Much more in-depth attack.

Understanding of the protocols for reconnaissance and attack.

TRISTATION, TCM, Triconex OS

INDUSTROYER2

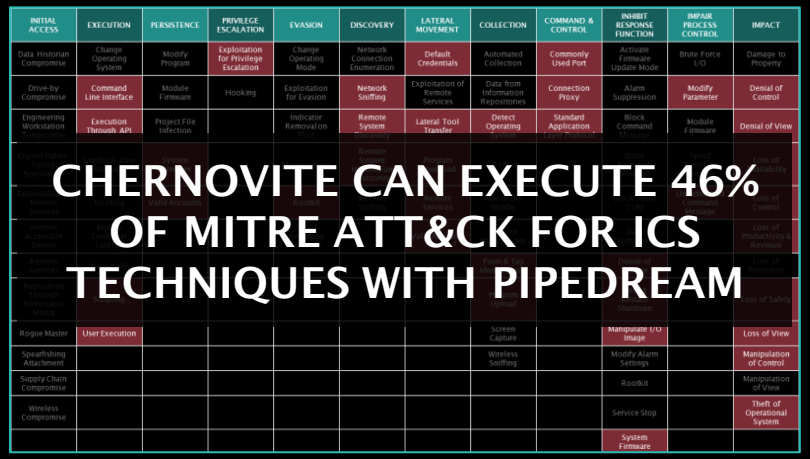
CHERNOVITE'S PIPEDREAM MALWARE

CAPABLE OF DISRUPTIVE & DESTRUCTIVE ICS/OT IMPACT

1st scalable, cross-industry OT attack toolkit

7th ICS/OT targeting malware

Discovered **before** it was employed for destructive purposes



EVILSCHOLAR & BADOMEN

Are extensible – this is rare.

1000s of CODESYS devices across multiple sectors at risk

MOUSEHOLE

Manipulates OPC-UA server nodes & associated devices.

OPC-UA is a widely used communication protocol in ICS/OT

DUSTTUNNEL & LAZYCARGO

Demonstrate that CHERNOVITE can achieve an end-to-end attack.

PIPEDREAM COMPONENTS

EVILSCHOLAR

Designed to discover, access, manipulate, and disable CODESYS devices. Initial targeting of Schneider Electric devices.

BADOMEN

Designed to scan, identify, interact, and manipulate Omron PLCs

MOUSEHOLE

Tool for interacting with OPC UA servers. Designed to read and write node attribute data, enumerate the Server Namespace and associated NodeIds, and brute force credentials.

Windows Components

DUSTTUNNEL

Remote operational implant to perform host reconnaissance and command-and-control.

LAZYCARGO

User-mode Windows executable that drops and exploits a vulnerable ASRock driver to load an unsigned driver.

INITIAL TARGETS

OMRON

NX1P2 Compact Machine Controller
NX-SL3300 Safety Controller
NJ501-1300 Automation Controller
NX-ECC EtherCAT Coupler
NX-EIC202 Ethernet/IP Coupler
NX-ECC203 EtherCAT Coupler
S8VK Power Supply
1S-series Servo Drives

Schneider Electric

TM251 PLC
TM241 PLC
TM221 PLC
TM258 PLC
TM238 PLC
LMC058 Motion Controller
LMC078 Motion Controller

ICS Protocols

CODESYS
Schneider Discovery (NetManage)
Modbus
Omron FINS
OPC UA

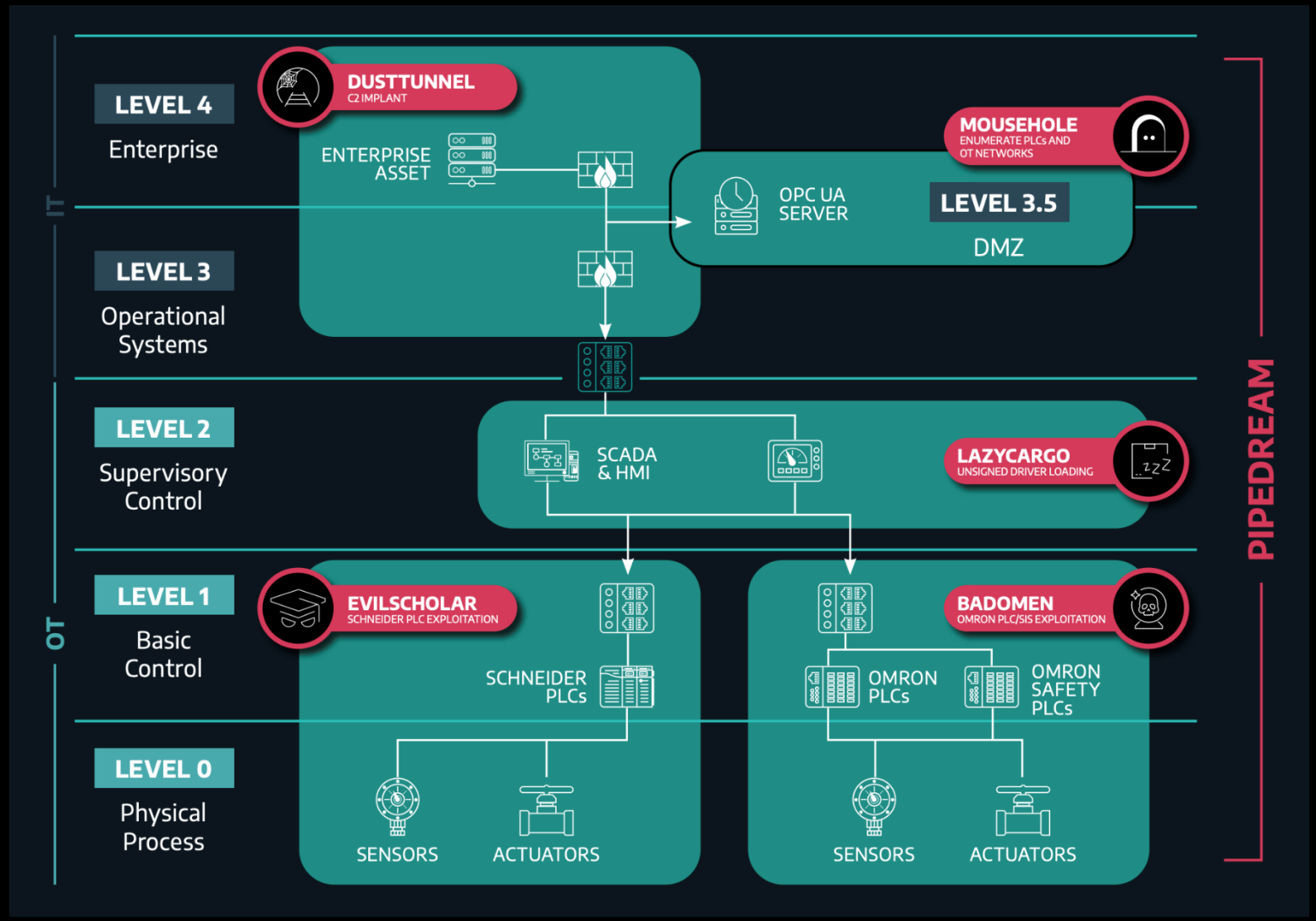
Vulnerabilities, Exposures, and Susceptibilities

CVE-2020-15368 LAZYCARGO utilizes this CVE to load an unsigned driver

CVE-2019-5106/ CVE-2019-9013 and undisclosed vulns in CODESYS/Schneider

CVE-2022-34151 Hardcoded Creds in Omron devices

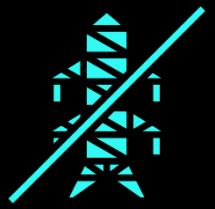
AN EXAMPLE DEPLOYMENT



INDUSTROYER 2

6th Sixth known ICS-specific malware

INDUSTROYER2 is a new variant of CRASHOVERRIDE with fewer capabilities

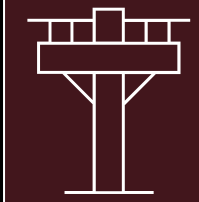


CRASHOVERRIDE caused the Kiev power disruption in December 2016

Developed by ELECTRUM

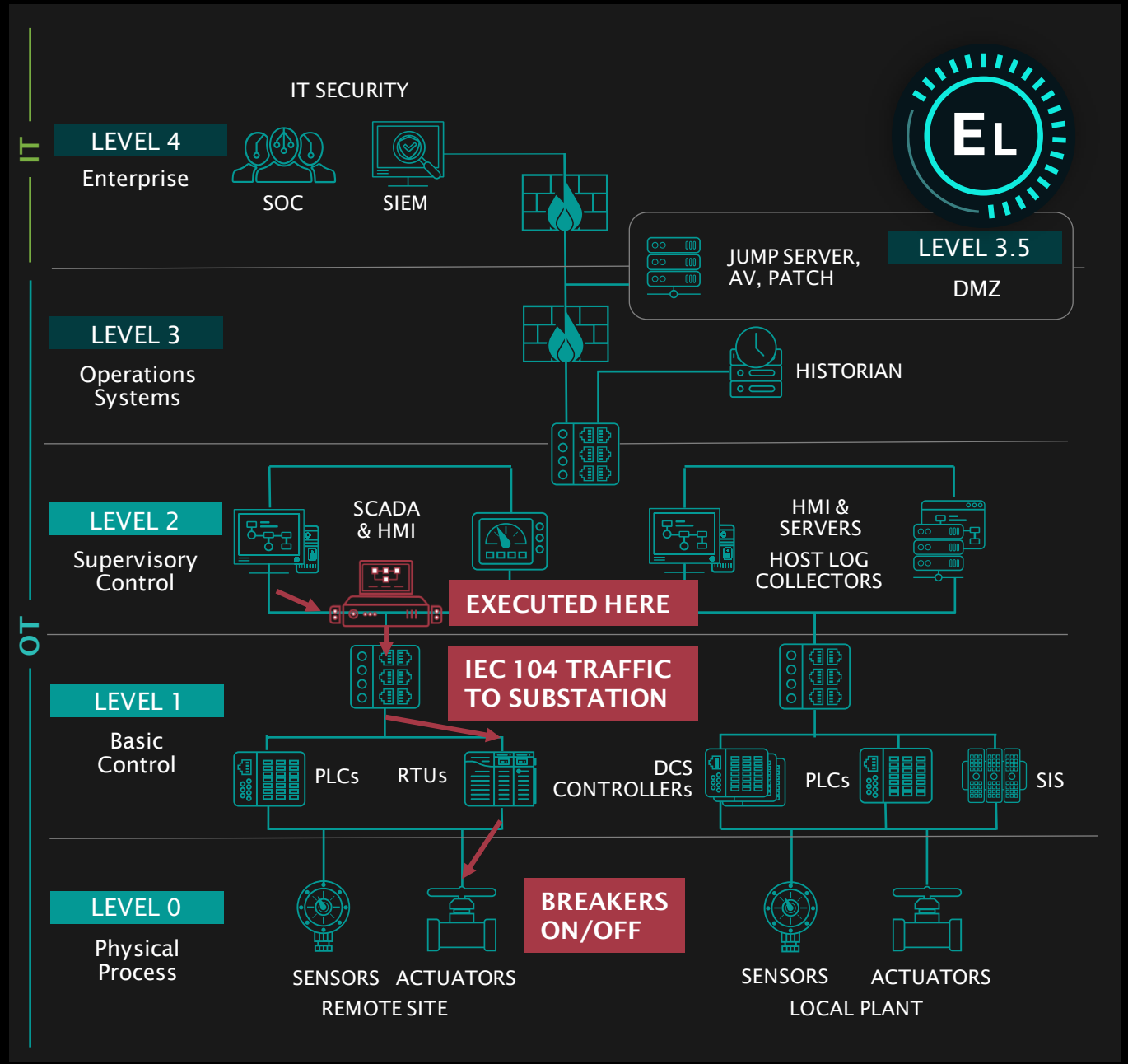
INDUSTROYER 2

- Targeted substations and hardcoded configuration includes 3 IP addresses
- Likely had a detailed understanding of the victim's environment before deploying



IEC 104 IS A TCP/IP NETWORK PROTOCOL COMMONLY USED IN ICS/SCADA ENVIRONMENTS IN THE ELECTRIC SECTOR.

Used for communications between control stations & substations for gathering information, monitoring power, & making control changes across the network.

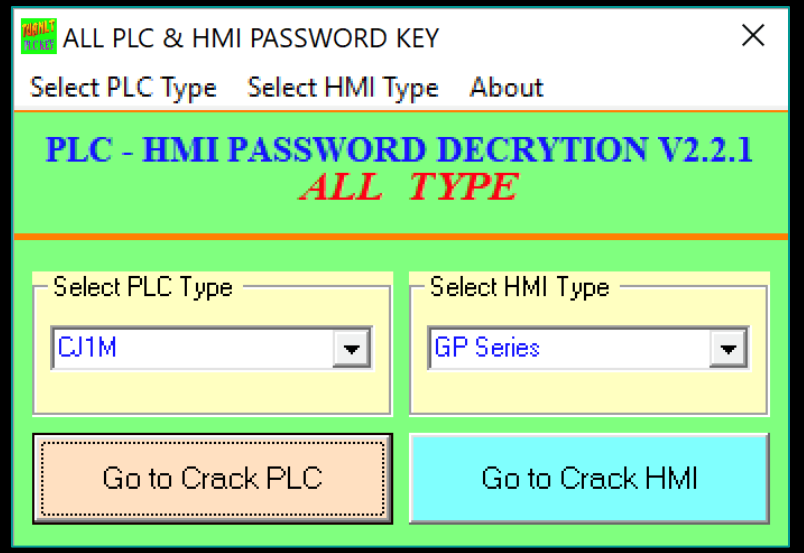


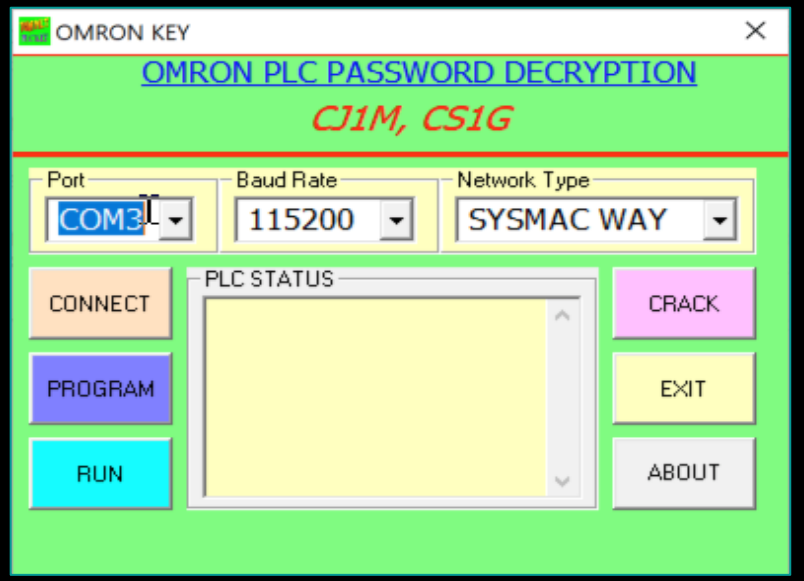
PASSWORD CRACKING SOFTWARE

Ads on social media for: Programmable Logic Controller (PLC), Human-Machine Interface (HMI), and project file password cracking software

One sample on VirusTotal embedded ~44 exploits targeting various systems.

But why would someone download this type of software?



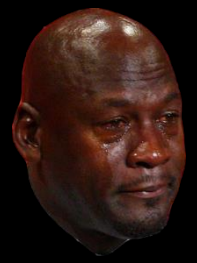


Claimed Product Support

HMIs

Fuji Electric POD UG
Fuji Electric Hakko
Mitsubishi Electric GT 1020 Series
Mitsubishi Electric GOT F930
Mitsubishi Electric GOT F940
Mitsubishi Electric GOT 1055
Pro-Face GP Pro-Face
Weintek
IDEC Corporation HG2S-FF

PLCs



Automation Direct DirectLogic 06
Omron CP1H
Omron C200HX
Omron C200H
Omron CPM2*
Omron CPM1A
Omron CQM1H
Omron CJ1M
Siemens S7-200
Siemens LOGO! 0AB6
Delta Automation DVP, ES, EX, SS2,EC Series
Mitsubishi Electric Q02 Series
Mitsubishi Electric FX Series (3U and 3G)
Allen Bradley MicroLogix 1000
Panasonic NAIS F P0
Fatek FBe and FBs Series
LG K80S
LG K120S
Vigor VB
Vigor VH

Project Files

Siemens S7-200 (*.mwp)
ABB Codesys (*.pro)
Pro-Face GP (*.prw)
Fuji Electric V-SFT

ANALYZING THE ROOT CAUSES

AUTOMATION DIRECT'S DIRECTLOGIC

MITSUBISHI ELECTRIC'S Q SERIES

OMRON'S CJ1M

Protocols Lacking Authentication on Critical Functions

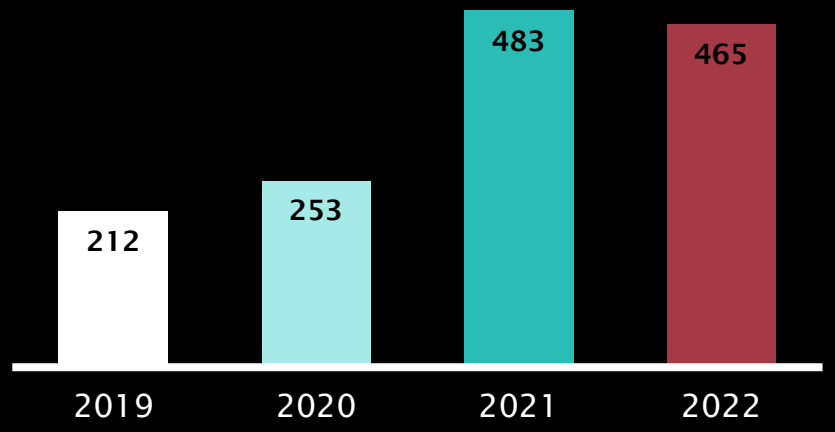
Undocumented Protocol Commands

STATE OF ICS VULNERABILITIES

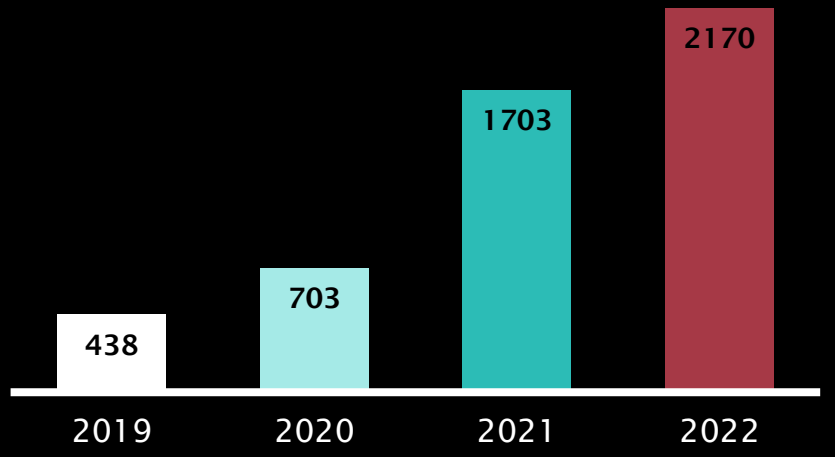
WE LOOKED AT 2170 CVEs IN 2022

THE NUMBER OF VULNERABILITIES KEEPS GROWING YEAR OVER YEAR – THANK YOU CYBERSECURITY RESEARCHERS OF THE WORLD!

Advisories by Year

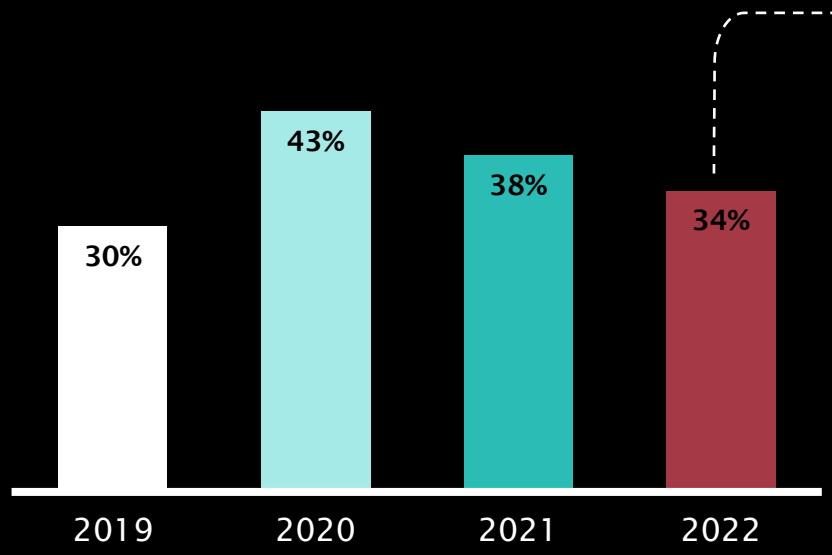


CVEs by Year



THE STATE OF ICS/OT VULNERABILITIES

ERRORS COULD CAUSE ASSET OWNERS AND OPERATORS TO WASTE RESOURCES ON LOW-RISK VULNERABILITIES OVER MORE SEVERE ONES.



Dragos analyzed 465 advisories

34% had incorrect data

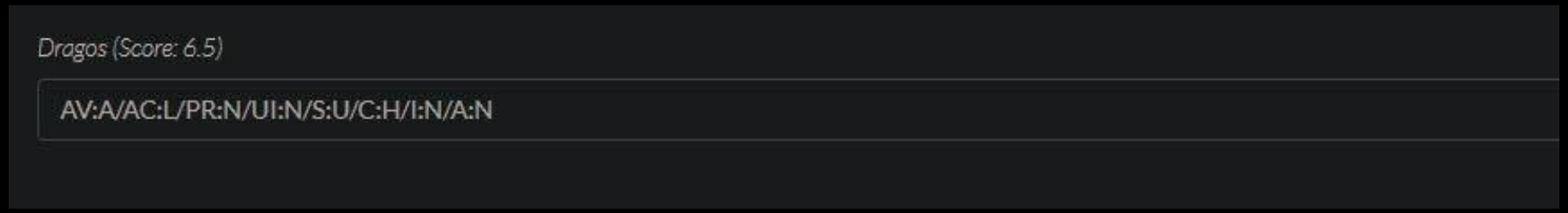
70% Dragos found to be MORE SEVERE than the CVSS score

29% Dragos found to be LESS SEVERE

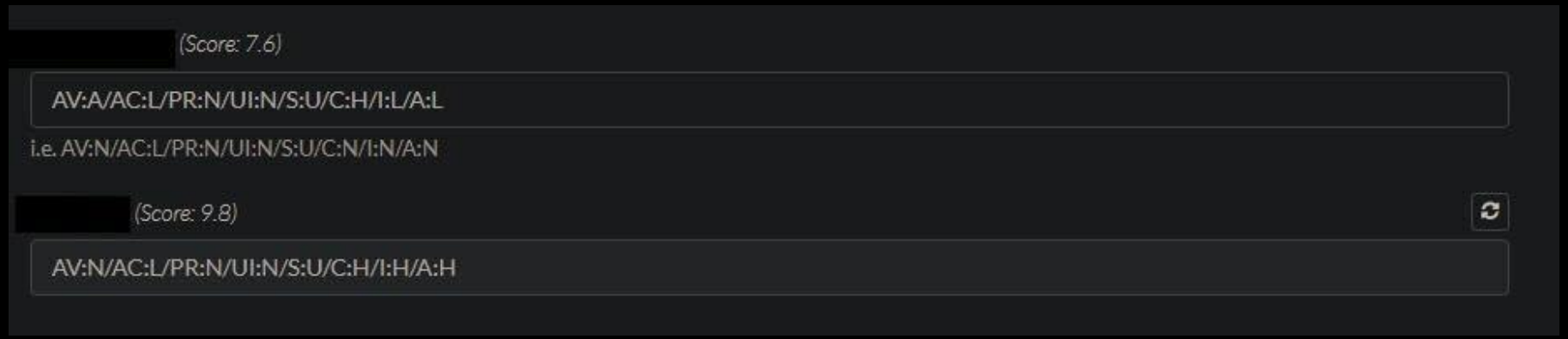
CVSS CORRECTIONS

Information Disclosure: Credential exposure through captured network traffic.

Dragos Score Correction



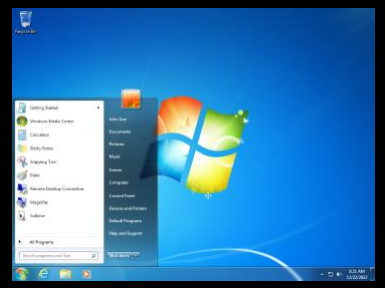
Original Scores Given



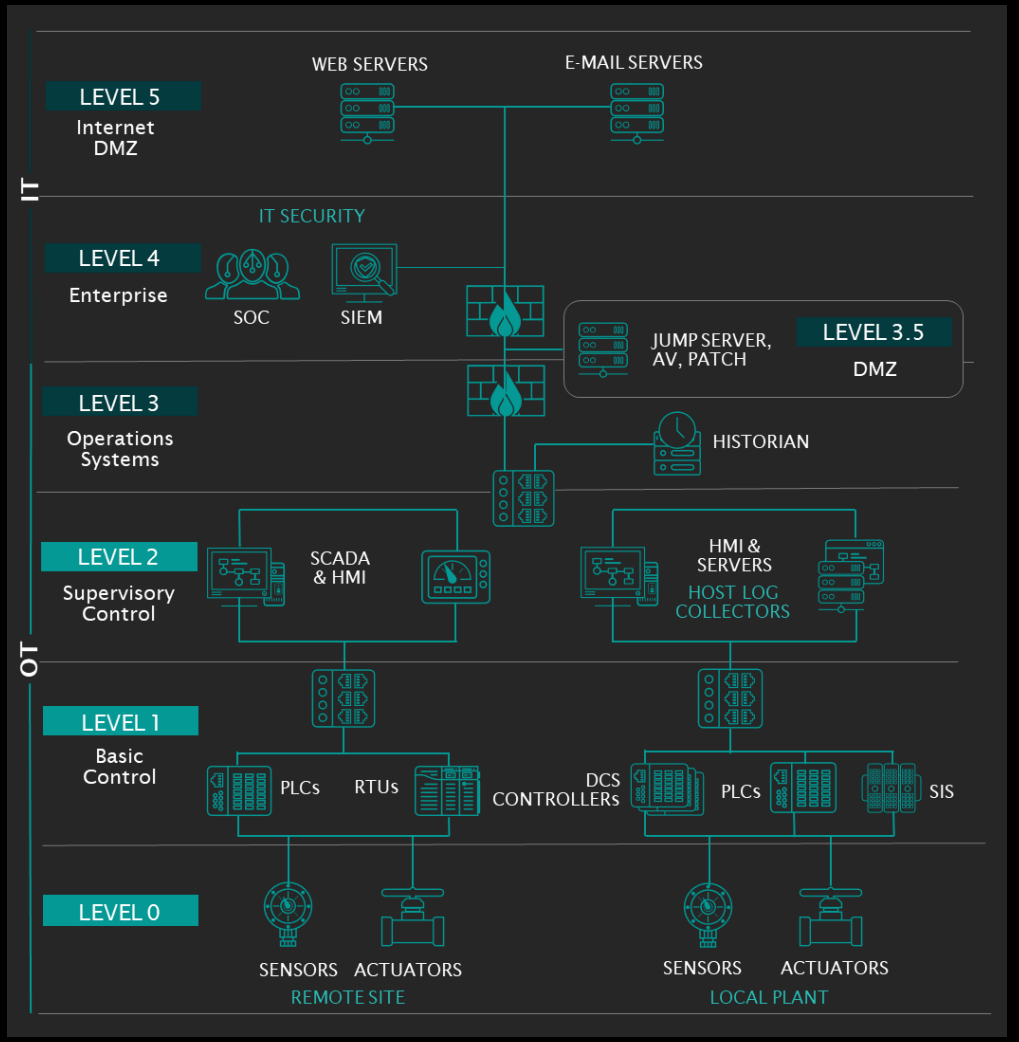
WHERE DO VULNERABILITIES RESIDE?

15% LEVEL 3.5, 4, & 5

63% LEVEL 2 & 3

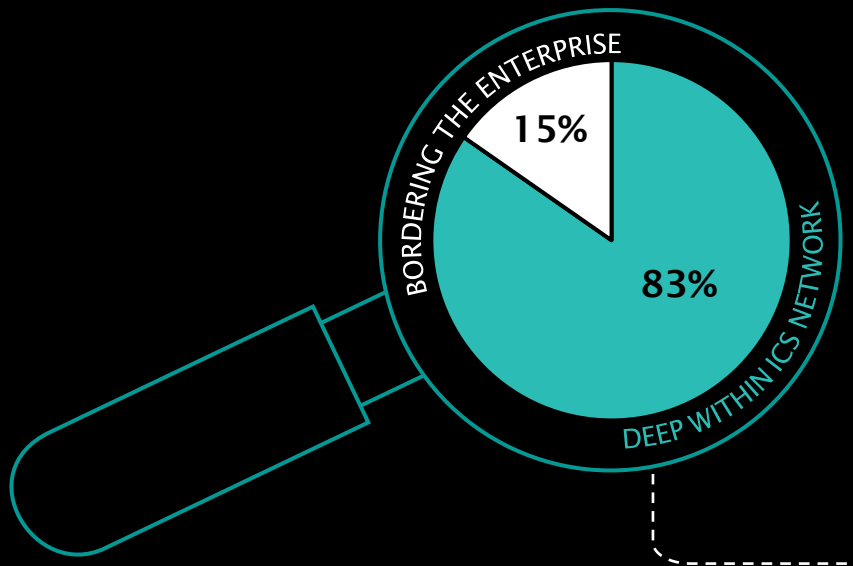


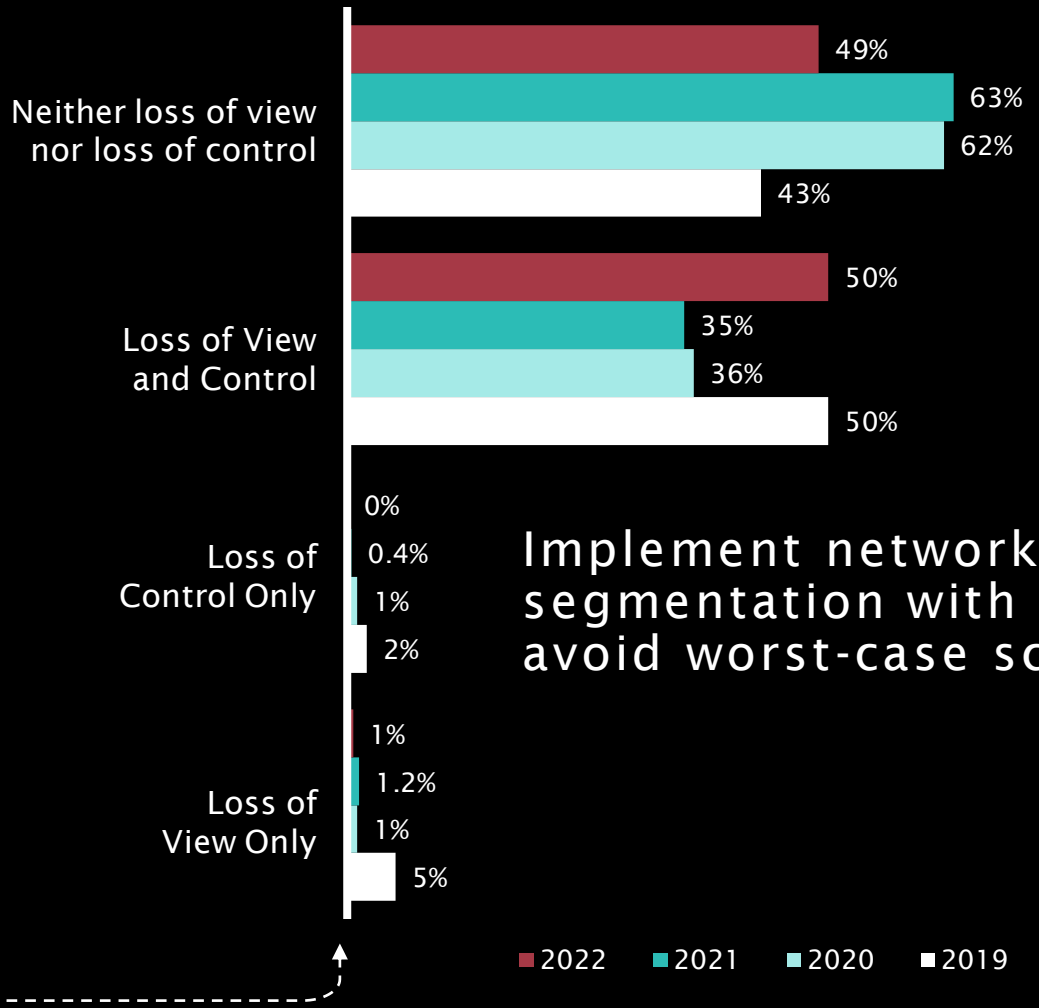
9% LEVEL 0 & 1



OT IMPACTS

ADVERSARIES NEED INITIAL ACCESS TO OT NETWORKS TO COMPROMISE VULNERABILITIES DEEP WITHIN THE ICS NETWORK





Implement network segmentation with MFA to avoid worst-case scenarios

PRACTICAL RISK MITIGATION IN ICS/OT

PATCHING CAN BE IMPRACTICAL IN ICS/OT DUE TO SAFETY & PRODUCTION REQUIREMENTS, ALTERNATIVE MITIGATION IS KEY

70%

Advisories with a patch

30%

Advisories with no patch when announced

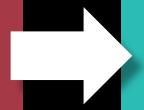
77%

CONTAIN NO PRACTICAL MITIGATION FROM THE VENDOR OR CNA

CONSEQUENCE-BASED VULNERABILITY MANAGEMENT

FOCUS REMEDIATION EFFORTS ON VULNERABILITIES WITH OPERATIONAL IMPACT OR KNOWN TO BE ACTIVELY TARGETED BY ADVERSARIES.

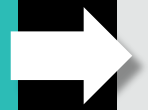
ONLY 2%
OF ICS/OT VULNERABILITIES NEED TO BE ADDRESSED
NOW



68% of vulnerabilities
are network exploitable with some having limited operational impact

Address these
NEXT

Mitigate through network monitoring, segmentation & MFA



30% of vulnerabilities
pose a possible threat but rarely require action

They likely NEVER need to be addressed

Monitor these for signs of exploitation

DRAGOS APPROACH TO VULNERABILITY ANALYSIS & MANAGEMENT

OUR PRIMARY RESPONSIBILITY

How Dragos Vulnerability Team Assists OT Vulnerability Management

We focus our analysis on OT impacts

We help asset owners decide what's important

We work with vendors

WE WORK WITH VENDORS

- When we find vulns, we work patiently and closely with vendors for responsible disclosure
- If we have questions about the details of a vendor's advisory, we will reach out for more detail
- OT vendors are still working through the growing pains of vuln management
- We partner with vendors to eliminate friction in these processes

FOCUS ANALYSIS ON OT IMPACTS

- Often, advisories will lack critical information that could help defenders understand and mitigate the issues
  - Alternative mitigations
  - Port numbers and services used
  - Entry points used for exploitation
- What are the OT-specific impacts?
- Is the advisory accurate?

PRIORITIZING VULNERABILITIES

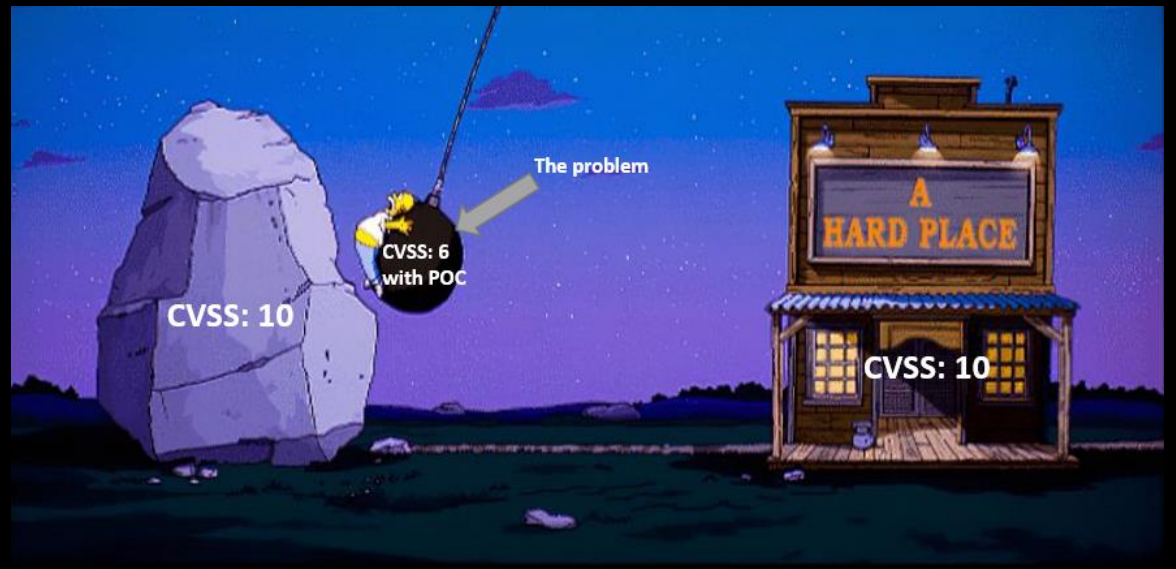
We help asset owners decide what's important

All vulns are not created equal.

CVSS scores were not designed for OT.

We take into consideration:

- Severity
- OT impacts
- Ease of exploitation
- Events in the wild
- & much more



TAKEWAYS & RECOMMENDATIONS

TAKEAWAY & RECOMMENDATIONS

PIPEDREAM brings forward a new extensible and modular OT focused malware framework that advances attack philosophies first showcased with CRASHOVERRIDE and TRISIS

CHERNOVITE presents a concerning threat to all ICS organizations

Dragos tracked threat groups continue to target ICS entities with both old and new capabilities

TAKEAWAY & RECOMMENDATIONS

Downloading password cracking software is a bad idea

All vulns aren't created equal and patching isn't always the right solution

Dragos vuln management insights and recommendations are best in class

RECOMMENDATIONS

SANS

5

THE FIVE ICS CYBER SECURITY CRITICAL CONTROLS

01
ICS Incident Response Plan

02
Defensible Architecture

03
ICS Network Monitoring Visibility

04
Secure Remote Access

05
Risk-based Vulnerability Management

QUESTIONS AND ANSWERS

THANK YOU

Want to reach us? intel@dragos.com

To download a copy of the
2022 Year In Review Report, visit:
www.dragos.com/year-in-review/