2025 OT/ICS Cybersecurity Executive Briefing

8th Annual Year in Review

Robert M. Lee
CEO & Co-Founder
Dragos, Inc.

8TH ANNUAL YEAR IN REVIEW

FROM THE 2025 OT/ICS CYBERSECURITY REPORT

Today's geopolitical climate is driving increased concern for cybersecurity in industrial & critical infrastructure

2024 saw the expansion of adversaries, tools, & ransomware events targeting industrial organizations.

SANS 5 ICS Critical Controls provide a path to OT security. We provide guidance within that framework in this discussion.

THREAT GROUP UPDATE: VOLTZITE

VOLTZITE
SINCE 2023

ADVERSARY:
+ Overlap with Volt Typhoon and BRONZE SILHOUETTE

CAPABILITIES:
+ Heavy use of living off the land techniques
+ Slow steady reconnaissance to evade detection
+ Use of Fast Reverse Proxy, multiple web shells

VICTIM:
+ Targets the electric sector across the United States, Guam

INFRASTRUCTURE:
+ Uses internet-facing SOHO networking equipment for communications

ICS IMPACT:
+ Loss of Confidentiality, Theft of Operational Information
+ Espionage and persistent access

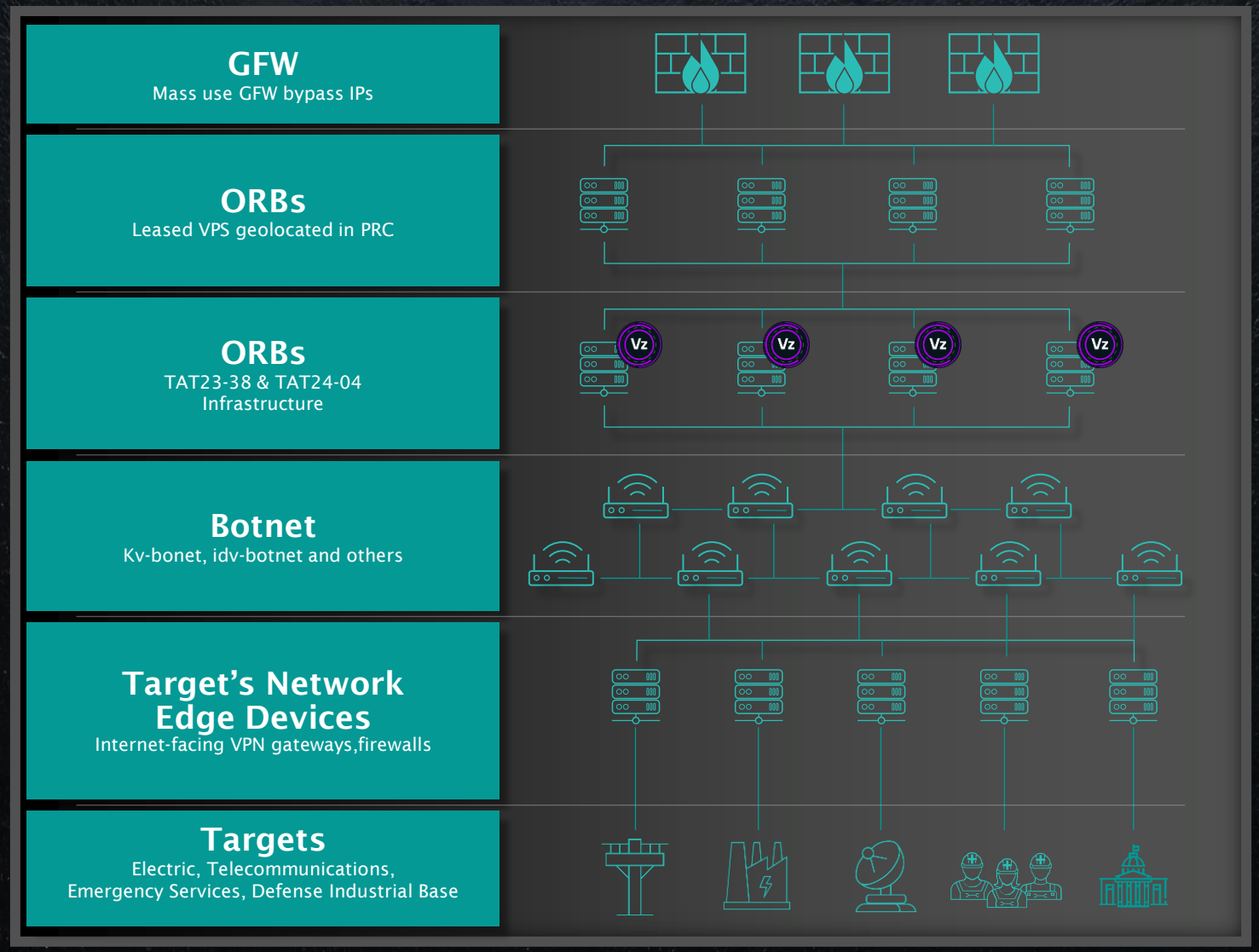
"[Chinese government-linked hackers have burrowed into U.S. critical infrastructure and are waiting] 'for just the right moment to deal a devastating blow.'"

Volt Typhoon has successfully gained access to numerous American companies in telecommunications, energy, water and other critical sectors, with 23 pipeline operators targeted

"The CCP's dangerous actions—China's multi-pronged assault on our national and economic security—make it the defining threat of our generation."

- US FBI Director Christopher Wray

VOLTZITE BOTNET



FUXNET ICS MALWARE

What happened?

In April 2024, the pro-Ukrainian hacktivist persona Blackjack claimed responsibility for a cyberattack on Moskollektor,a Russian organization managing Moscow's municipal infrastructure.

The attack allegedly used a malware called Fuxnet, designed to disrupt sensor operations within Moskollektor's OT monitoring network.

8th
known ICS malware

*Pending Validation

FROSTYGOOP ICS MALWARE

What happened?

In January 2024, during sub-zero temperatures, a cyber attack disrupted the energy supply for central heating in more than 600 apartment buildings in Ukraine.

Dragos discovered FrostyGoop in April 2024.

FrostyGoop interacts directly with industrial control systems (ICS) using Modbus TCP over port 502.

9th
known ICS malware

1st
known Modbus ICS malware that causes effects on ICS devices

46,000
Internet-exposed ICS devices communicating over Modbus TCP

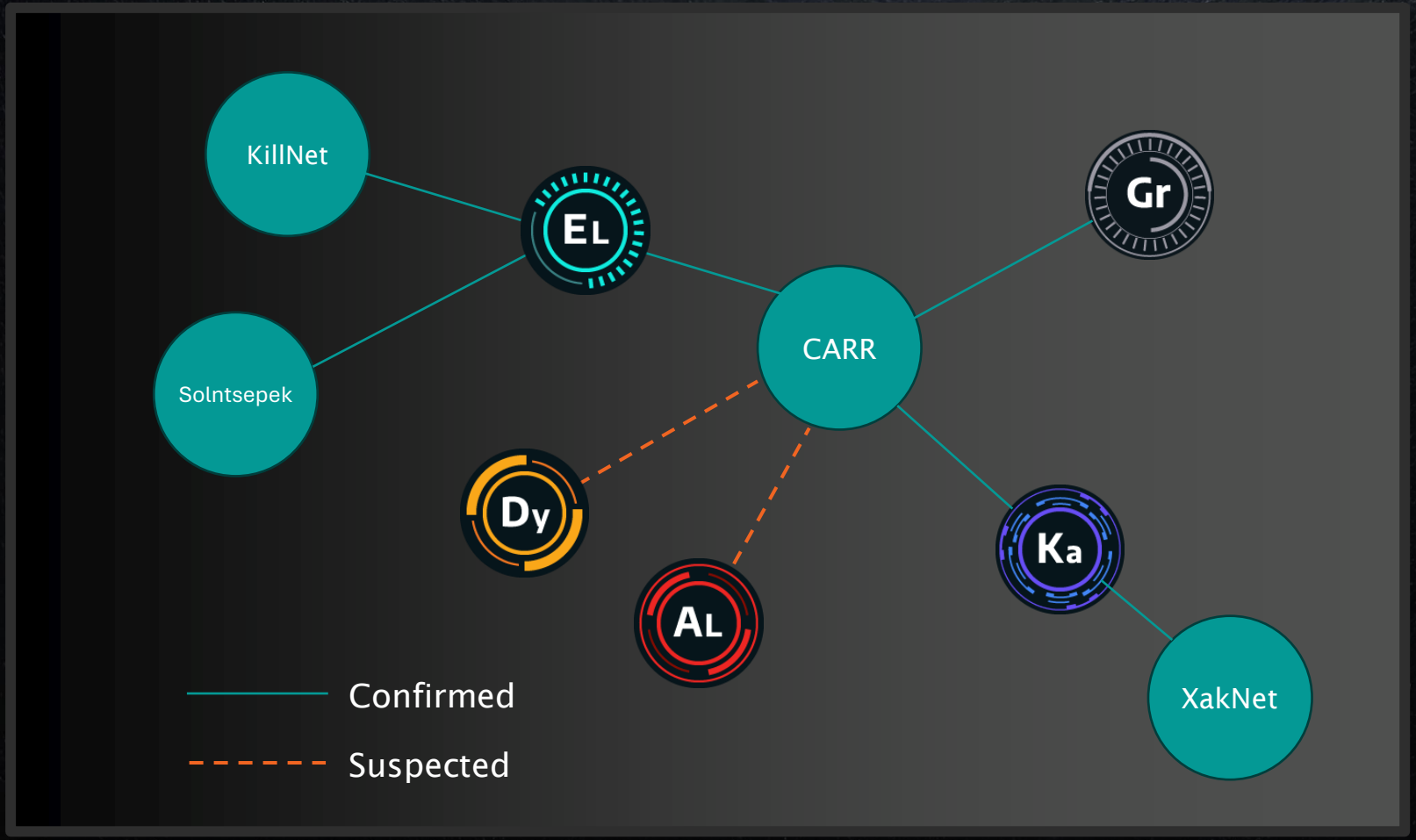
Modbus is used worldwide across industries.

TWO NEW DRAGOS THREAT GROUPS

YEAR FIRST DISCOVERED

2017	2018	2019	2020	2021	2022	2023	2024
EL	Ra	Hx	Ka	Ko	Cv	Gn	Bx
Ch	AL	Pi	Va	Pv	Bt	Vz	Gr
Dy	Xt	Wa	St			Lr	
Ma			Ta				

CONVERGENCE OF HACKTIVISM & STATE-SPONSORED THREATS



- Shared Infrastructure
- Intelligence Sharing
- Victim Overlaps

NEW THREAT GROUP: BAUXITE

STAGE 2: ICS ACTIONS AGAINST EASY-TO-ACCESS TARGETS

BAUXITE
SINCE 2023

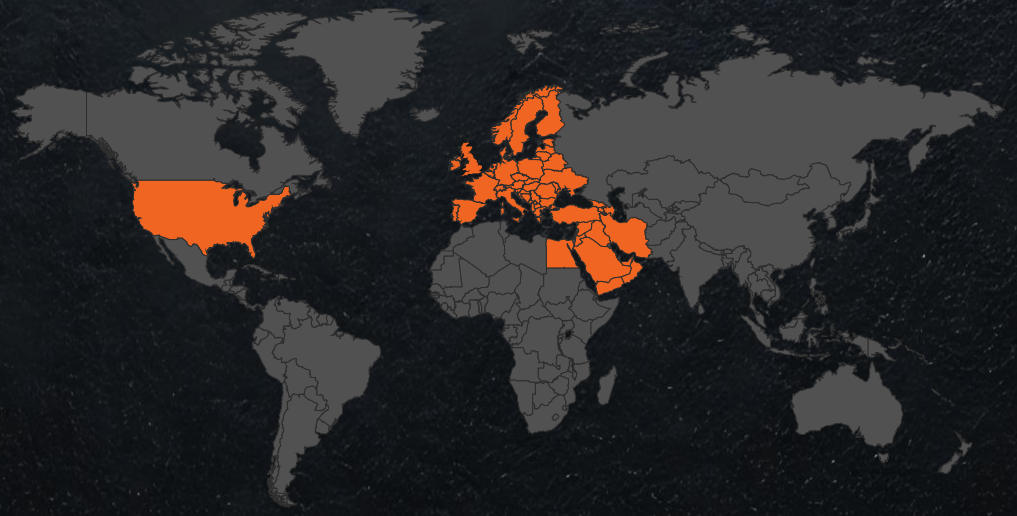
ADVERSARY:
+ Overlaps with CyberAv3ngers

CAPABILITIES:
+ Uses publicly known exploits
+ Consumes Security Advisories from OT/ICS OEMs
+ Leverages tools built into Kali Linux
+ Linux Backdoor with C2 over MQTT

VICTIM:
+ Global impact, victims in the U.S., Australia, U.K., and Israel

INFRASTRUCTURE:
+ Use/reuse of bulletproof hosting providers & owned infrastructure
+ Different infrastructure for CNA/CNE, Scanning & Research

ICS IMPACT:
+ ICS Cyber Kill Chain Stage 2
+ Denial of Control, Loss of Availability, Loss of Control, Loss of Productivity and Revenue, Loss of View



BAUXITE is capable of modifying ladder logic in PLCs & deploying custom backdoors in ICS equipment. Associated with the manipulation of Unitronics PLCs.

Focused on critical manufacturing, government, and professional services, aviation.

Uses compromised victim infrastructure/identity for operations against other targets.

- Oil & Natural Gas
- Electric
- Water & Wastewater
- Food & Beverage
- Chemical Manufacturing

BAUXITE: STAGE 2 ICS ATTACK

100%
of observed BAUXITE targets were accessible from the internet

100%
of ICS attack activity used SSH for initial access

ICS CYBER KILL CHAIN

INTRUSION

- Reconnaissance — STAGE 01
- Weaponization/Targeting — STAGE 01
- Delivery — STAGE 01
- Exploit — STAGE 01
- Install/Modify — STAGE 01
- C2 — STAGE 01
- Act — STAGE 01

ICS ATTACK

- STAGE 02 Develop
- STAGE 02 Test
- STAGE 02 Deliver
- STAGE 02 Install / Modify
- STAGE 02 Execute ICS Attack

CAPABILITIES

Targets Internet Facing Devices (VPN, Firewalls, PLCs)
Access via brute Force SSH with custom scripts & binaries
Delivers with webpages, SSL, & web pages

Installs malware like IOCONTROL, changes router configs
Establish backdoors with persistent SSH connects
Creates C2 link with Cloudflare infrastructure

STAGE 2
Denial-of-Service (DoS) attacks against PLCs and HMIs, ladder logic manipulation. Potential for wiping firmware on affected devices.

BAUXITE: STAGE 2 ICS ATTACK

45% of OT Watch customers have SSH communicating with publicly routable addresses, and **5%** communicate with external addresses via the PPTP protocol.

INITIATE PROACTIVE THREAT HUNTS TO IDENTIFY UNAUTHORIZED SSH & PPTP COMMUNICATIONS

**(A minor portion of these are untuned environments).*

100%
of observe
BAUXITE
targets we
accessible f
the intern

100%
of ICS attac
activity use
SSH for init
access

lls, PLCs)
ots & binaries

outer configs
nects
e

s and HMIs,
oing

STAGE 02 Execute ICS Attack

NEW THREAT GROUP: GRAPHITE

SPEAR-PHISHING, CREDENTIAL CAPTURE

GRAPHITE
SINCE 2023

ADVERSARY:
+ Overlaps with APT28

CAPABILITIES:
+ Exploitation of multiple zero-day vulnerabilities
+ OCEANMAP, HEADLACE, MASEPIE, STEELHOOK

VICTIM:
+ Critical infrastructure (Energy, Oil & Natural Gas, Logistics)
+ Eastern Europe (Ukraine)
+ West Asia

INFRASTRUCTURE:
+ Use of Compromised SOHO routers, primarily Ubiquiti Edge routers
+ Use of LIS, VPN, VPS

ICS IMPACT:
+ ICS Cyber Kill Chain Stage 1
+ Emphasis on Credential Capture Operations

Near-constant spear-phishing operations using weaponized emails and custom script-based malware. Exploitation of CVE-2023-23397 (Outlook), CVE-2023-38831 (WinRAR).

Oil & gas pipeline operators, logistics, defense suppliers, governments in E. Europe, Turkey, UAE.

Focused on exfiltration & credential capture.

- Oil & Natural Gas
- Electric
- Defense Suppliers
- Government

GRAPHITE: STAGE 1 INTRUSION

ICS CYBER KILL CHAIN - INTRUSION

Reconnaissance	STAGE 1	ID email addresses & vulnerable Outlook clients of critical infrastructure organizations.
Weaponization	STAGE 1	Spear-phish with malicious attachments (HEADLACE, MASEPIE, OCEANMAP, WinRAR, Outlook UNC path attacks)
Targeting	STAGE 1	AND/OR link to webpages hosting malware
Delivery	STAGE 1	Deploys custom backdoors (HEADLACE, OCEANMAP, MASEPIE). Modifies registry & startup folders. Establishes persistence.
Exploit	STAGE 1	Leverages Outlook & WINRAR CVEs to steal NTLM hashes, execute scripts.
Install/Modify	STAGE 1	
C2	STAGE 1	C2 uses HTTP, webhook communications, IMAP email drafts, & encrypted channels for remote execution & exfiltration
Act	STAGE 1	Exfiltrates credentials, executes remote commands, & logs keystrokes.

OT Watch Identified that **14%** of customers communicate with external addresses via IMAP protocol

UPDATE: KAMACITE: & ELECTRUM

A CONTINUED PARTNERSHIP, KAMACITE ENABLES ELECTRUM ICS ATTACKS

KAMACITE

- Persistent intrusions into Ukraine critical infrastructure, including energy & telecom networks.
- New Kapeka malware used to exfiltrate data and maintain persistent access.
- Activity observed expanding to European oil & gas sectors, using SSH brute-force techniques.

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

ENABLES

ELECTRUM
SINCE 2016

ADVERSARY:
+ Assessed links with SANDWORM APT, now appears indepedendent

CAPABILITIES:
+ Unique RAT & malicious wiper modules

VICTIM:
+ Electric Sector
+ Ukraine, Europe

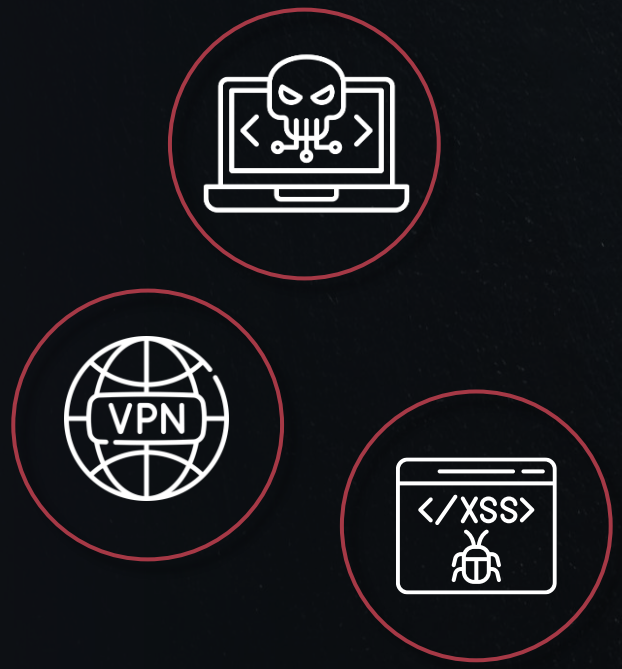
INFRASTRUCTURE:
+ Leveraged servers hosting many additional services such as TOR

ICS IMPACT:
+ Executed control system portion of 2016 Ukraine power event, deployed CRASHOVERRIDE designed to manipulate electric transmission equipment

ELECTRUM

- Key player in the Kyivstar telecom attack (March 2024), disrupting telecommunication & critical infrastructure communication systems.
- Focus on energy grids & communication infrastructure in Ukraine, Poland.
- Increased use of OT-aware malware designed to manipulate ICS.

TACTICS, TOOLS, & PROCEDURES



New ICS Malware
is increasingly emerging; lack of visibility in OT conceals the full scope of attacks

Internet-accessible OT devices
key attack path, highlighting need for simple changes to create more defensible architectures

Remote Access
adversaries routinely exploit VPNs, SSH, default credentials, & third-party remote access.

Lateral Spread After Compromise
adversaries use LOTL techniques, native tools, ICS protocols to evade detection.

NEW OT/ICS SPECIFIC MALWARE

FUXNET
8th known ICS malware*

Malware Targeting sensors used in Industrial Operations

Frosty Goop
9th known ICS malware

Dragos discovered FrostyGoop in April 2024. interacts directly with industrial control systems (ICS) using Modbus

*Pending Validation

CASE STUDY: KURTLAR MALWARE

Dragos identifies new malware

1 Kurtlar Malware Discovery

Dragos OT Cyber Threat Intelligence
Discovers the Kurtlar malware sample.

Kurtlar captures credentials in internet-exposed, poorly-secured industrial devices running VNC servers for targeted IP addresses.

2 Internet-exposed VNC Servers

TAT24-76
claims use of Kurtlar malware to compromise internet-exposed VNC servers.

The group advertises VNC access to HMI and SCADA devices.

3 Victim Notification & Threat Analytics

Dragos OT-CERT
alerts affected organizations.

OT Watch
identified 9% of participants with VNC communicating with external addresses.
Deploys daily threat hunts,

Detections added to Dragos Platform

BEST PRACTICES THREAT MANAGEMENT

Disconnect devices from the Internet (CC#2)
Place behind a firewall

Create proper access control policies (CC#2 & 4)
Restrict VNC access, especially on targeted ports, & ensure weak credentials are changed

Continuously validate access control (CC#3)
Evaluate access & segmentation policies, monitor activity on network

CASE STUDY: KURTLAR MALWARE

Dragos identifies new malware

46% service engagements included findings of lack full visibility across OT networks

Traditional IT tools miss ICS specific threats

YOU CAN'T SECURE WHAT YOU CAN'T SEE.
OT-NATIVE MONITORING IS ESSENTIAL.

RACTICES
REAT
GEMENT

devices from the
#2)
a firewall

er access control
#2 & 4)
access, especially
ports, & ensure
tials are changed

y validate access
#3)
ss &
n policies,
ity on network

RANSOMWARE ATTACKS BY SECTOR

RANSOMWARE ATTACKS INCREASED BY 87% IN 2024

RANSOMWARE BY ICS SECTOR

BASED ON PUBLIC THREAT INTEL SOURCES

- **1171** Manufacturing
- **177** Industrial Control Systems
- **176** Transportation
- **44** Oil & Gas
- **41** Communications
- **30** Electric
- **20** Government
- **12** Water
- **11** Mining
- **7** Renewables
- **4** Data Centers

TOTAL: 1693 INCIDENTS

Ransomware Insights From Dragos Incident Response Cases

25% Involved full shutdown

75% Involved disruption to operations to some degree

WHAT CAN GO WRONG: RANSOMWARE

HOW TO FIX IT

- Patch VPN vulnerabilities, enforce MFA
- Restrict admin privileges, monitor access
- Implement strict IT/OT segmentation
- Deploy OT-native threat & anomaly detection
- Conduct TTX, establish offline backups

PRACTICAL RISK MITIGATION IN ICS/OT

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

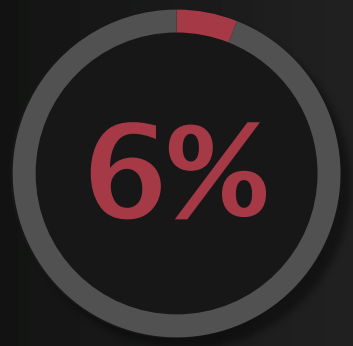
74%
Advisories with a patch

26%
Advisories with no patch when announced

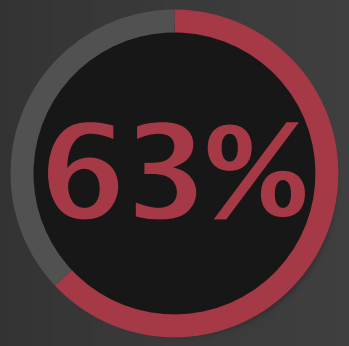
47%
DRAGOS PROVIDED ALTERNATE MITIGATIONS FOR ADVISORIES MISSING BOTH A PATCH & MITIGATIONS

RISK-BASED VULNERABILITY MANAGEMENT

ONLY SOME VULNERABILITIES NEED IMMEDIATE ACTION

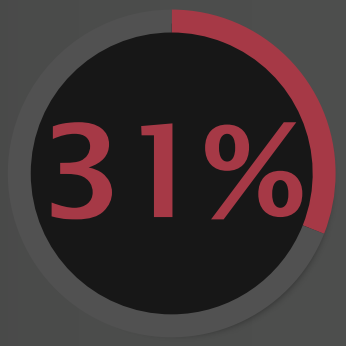


of ICS/OT vulnerabilities needed to be addressed



are network exploitable with no direct operational impact

These need to be addressed



pose a possible threat but rarely require action

They likely never need to be addressed

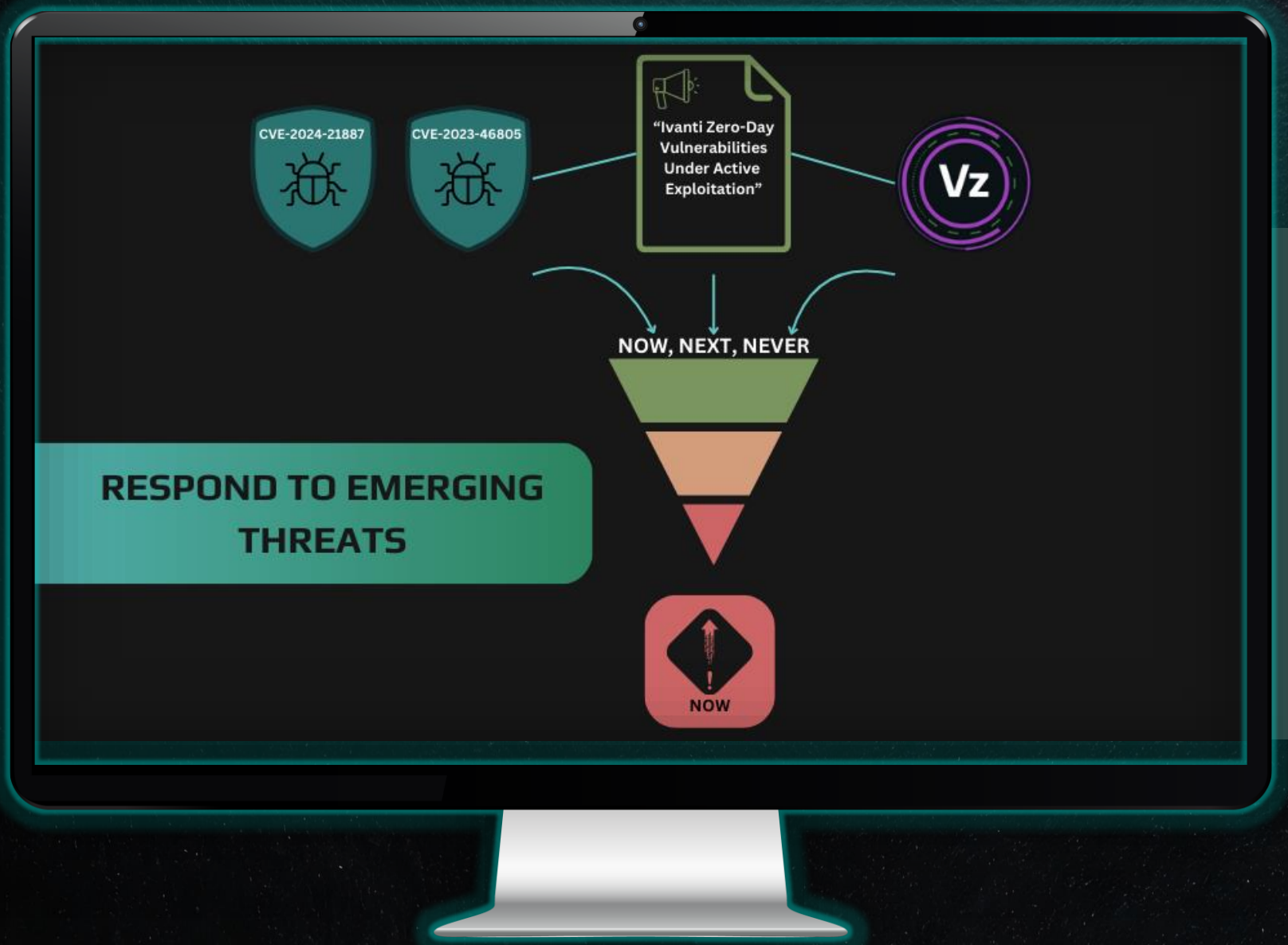
NOW

NEXT

Mitigate through network monitoring, segmentation & MFA

NEVER

Monitor these for signs of exploitation



RISK-BASED VULNERABILITY MANAGEMENT

ONLY SOME VULNERABILITIES NEED IMMEDIATE ACTION

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

Q&A

QUESTIONS AND ANSWERS