DRAGOS

THREAT LANDSCAPE
ICS/OT CYBERSECURITY
YEAR IN REVIEW 2022

Kent Backman
Principal Adversary Hunter

Josh Hanrahan
Senior Adversary Hunter

Dr. Thomas Winston
Director of Intelligence

AGENDA

1. Introductions
2. CHERNOVITE & BENTONITE
3. Active Threat Groups in 2022
4. Ransomware Trends & Outlook
5. Takeaways & Recommendations

STAGES OF THE ICS CYBER KILL CHAIN

STAGE 1

Initial survey & access to the enterprise IT environment

Crossing into ICS/OT

STAGE 2

OT network reconnaissance, penetration, & execution of ICS attacks

Avoid Custom Software & Malware

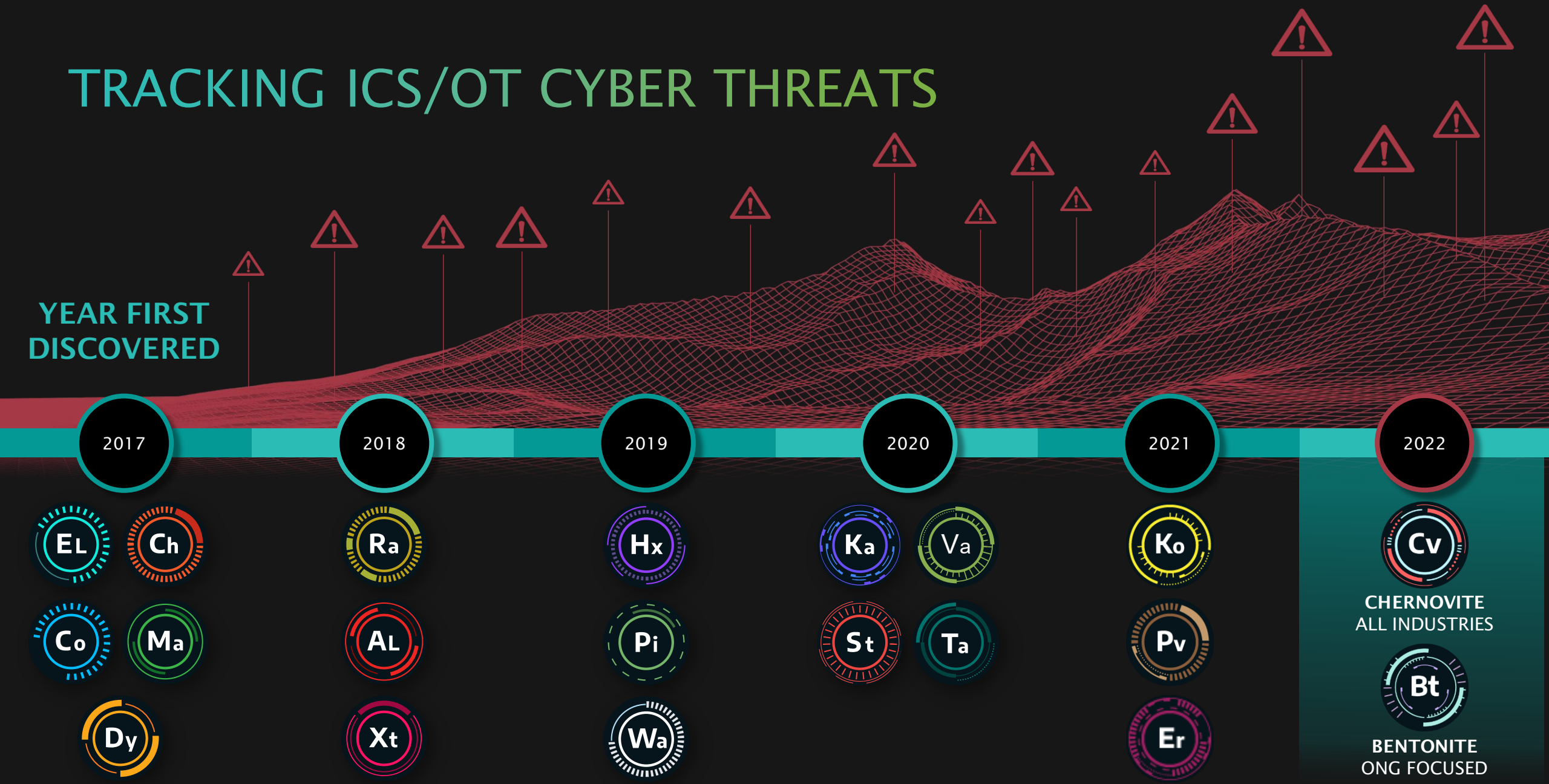
Emphasize Commodity & System Tools

Different systems, network traffic, adversaries, & need to manage vulnerabilities differently

Custom Attack Packages Tailored to a Specific Environment

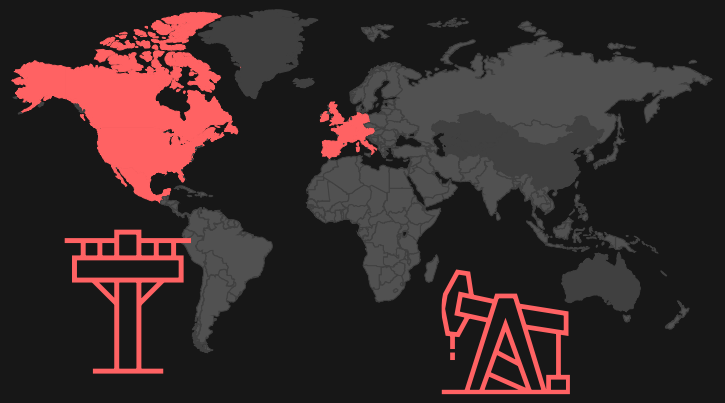
Limited Ability to Replay or Reuse Attacks

TRACKING ICS/OT CYBER THREATS



CHERNOVITE: NEW IN 2022

ICS/OT SYSTEM SPECIALIST



CHERNOVITE
SINCE 2021

ADVERSARY:
+ Development and effects team focused on ICS disruption

CAPABILITIES:
+ Unique tool development
+ Uses ICS-specific protocols for reconnaissance, manipulation, and disabling of PLCs
+ PLC Credential Capture. Password bruteforcing and denial of service

VICTIM:
+ Could impact all industries, initially targets electric, ONG
+ Companies with Schneider Electric, Omron, and CODESYS PLCs, as well as any OPC UA operations

INFRASTRUCTURE:
+ Unknown

ICS IMPACT:
+ Loss of safety, availability, and control; manipulation of control
+ ICS Kill Chain Stage 2 – Install/Modify, Execute ICS

Potential to impact all industries and regions

Hundreds of ICS vendors use CODESYS

Capable of Stage 2 of the ICS Cyber Kill Chain

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

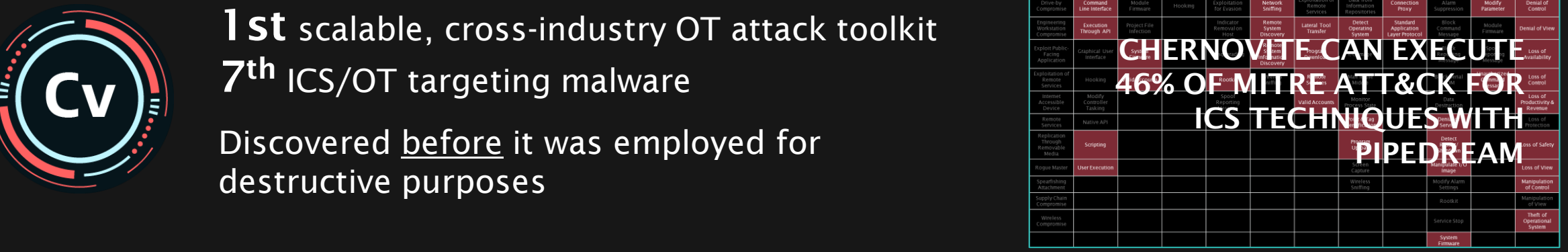
CHERNOVITE'S PIPEDREAM MALWARE

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.

CHERNOVITE ASSESSMENT

IMPLICATIONS OF PIPEDREAM DEVELOPMENT ON CHERNOVITE

The breadth of knowledge required to develop these tools indicates that CHERNOVITE:

Is well versed in ICS protocols & OT network intrusion techniques.

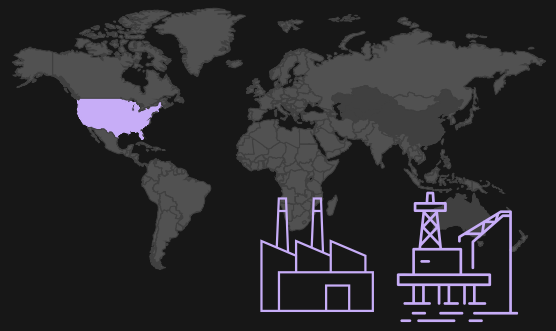
Is skilled in software development.

Is well-funded, with a budget for acquiring devices.

Has knowledge to achieve an impact.

BENTONITE: NEW IN 2022

OPPORTUNISTIC EXPLOITATION



BENTONITE
SINCE 2021

ADVERSARY:
+ Associated with PHOSPHORUS
+ Able to run multiple, concurrent operations

CAPABILITIES:
+ Multi-stage downloaders, victim enumeration, reconnaissance and C2 capabilities
+ Vulnerability exploitation
+ Heavy use of Powershell to facilitate compromise
+ Disruptive Capabilities

VICTIM:
+ Highly Opportunistic
+ U.S. Oil and Gas, Manufacturing
+ State, Local, Tribal and Territorial organizations

INFRASTRUCTURE:
+ Credential harvesting
+ Separate domains for phishing and C2
+ Utilizes Github for delivery, SSH and HTTP for C2

ICS IMPACT:
+ Espionage, Data Exfiltration & IT Compromise
+ Disruptive Effects Possible

Delivery	STAGE 01
Exploit	STAGE 01
Install/Modify	STAGE 01
C2	STAGE 01
Act	STAGE 01

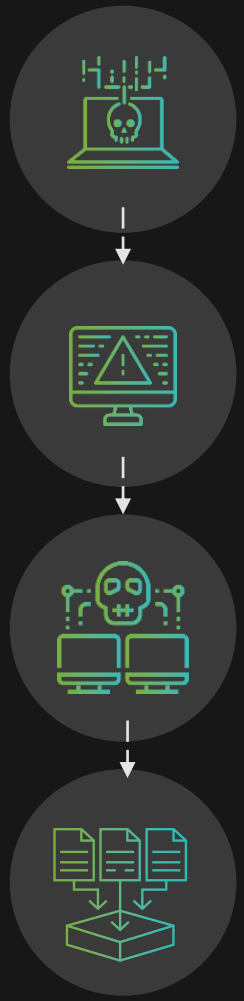
Targets **Oil & Gas, Manufacturing**

Highly opportunistic

Demonstrated **Stage 1** of the ICS Cyber Kill Chain

BENTONITE: OPPORTUNISTIC EXPLOITATION

RECONNAISSANCE & LONG-TERM PERSISTENCE



Exploits vulnerabilities in internet facing assets

Installs initial downloader implant

Implant retrieves malware from adversary Github account

Long-term persistence, reconnaissance, interactive operations

BENTONITE has in the past employed disruptive capabilities

Compromises Maritime ONG, SLLT governments via vulnerabilities in remote access solution

Capable of deploying wiper malware

Capable of ransomware attack

THREAT GROUPS INCREASE ACTIVITY IN 2022

RECON, CAPABILITY BUILDING, & INITIAL ACCESS ACTIVITY ACROSS ALL GLOBAL INDUSTRIAL SECTORS

KOSTOVITE

Targeting Energy
North America, Australia
SINCE 2021

KAMACITE

Many Industrial Sectors Targeted
Ukraine, Europe, U.S.
SINCE 2014

XENOTIME

Targeting Oil & Gas, Electric
Middle East,
North America
SINCE 2014

ELECTRUM

Targeting Electric
Ukraine, Europe
SINCE 20

ERYTHRITE

Multiple Industrial Sectors Targeted
U.S, Canada
SINCE 2021

WASSONITE

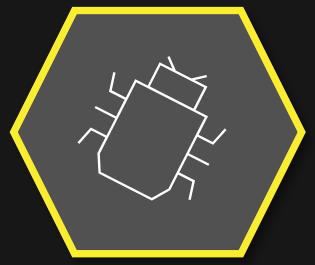
Multiple Industrial Sectors Targeted
South/East Asia,
North America
SINCE 2018

KOSTOVITE

TARGETING ENERGY IN NORTH AMERICA, AUSTRALIA SINCE 2021

Compromise of an energy entity & power generation facilities

Activity of multiple adversaries sharing common infrastructure with KOSTOVITE



KOSTOVITE-linked APT5 was actively exploiting a zero-day in Citrix perimeter access devices

Delivery	STAGE 1
Exploit	STAGE 1
Install/Modify	STAGE 1
C2	STAGE 1
Act	STAGE 1

COMPROMISES INTERNET-EXPOSED REMOTE ACCESS DEVICES

SKILLED LATERAL MOVEMENT & INITIAL ACCESS OPERATIONS INTO ICS/OT

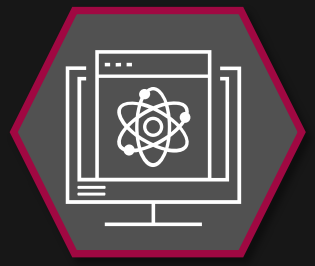
STAGE 2	Develop
STAGE 2	Test
STAGE 2	Deliver
STAGE 2	Install / Modify
STAGE 2	Execute ICS Attack

XENOTIME

TARGETING THE OIL & GAS INDUSTRY IN THE U.S. & EUROPE SINCE 2014

Reconnaissance focused on oil & natural gas (ONG), liquified natural gas (LNG) industries

Heavy use of off-the-shelf tools & open-source information



Currently in the development phase, continues to target downstream & midstream ONG/LNG with a focus on pipeline, maritime, refining

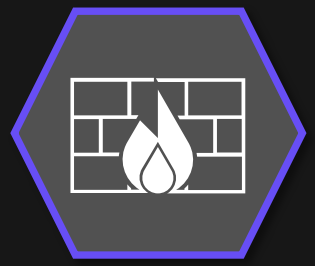
ICS Malware: TRISIS

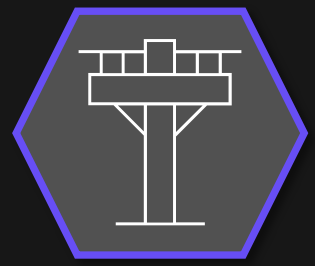
- Delivered in 2017 to an industrial facility in the Middle East by a well funded attack team
- Targeted Safety Instrumented System (SIS) and failed causing a stop in operations
- First malware to specifically target human life

KAMACITE

TARGETING THE ELECTRIC SECTOR IN EUROPE, IN PARTICULAR UKRAINE, SINCE 2014

Victims in **electric, natural gas, rail, aerospace, food & beverage manufacturing & processing, automotive, & U.S. government** communicating with CYCLOPS BLINK

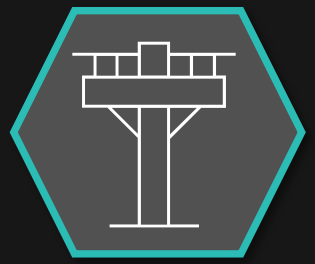




February	March	April	May	June
CYCLOPS BLINK targeting vulnerabilities in small/home office devices	 WatchGuard firewall & router devices  ASUS firewall & router devices	Malware removed from vulnerable firewall devices used for C2 CYCLOPS BLINK operations	Targets another set of routers & IP cameras for initial network access (outside of CYCLOPS BLINK operations)	Communication with the same oblenergo targeted in a 2015 Ukraine cyber attack

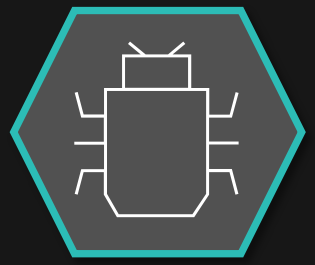
ELECTRUM

TARGETING THE ELECTRIC SECTOR IN EUROPE, IN PARTICULAR UKRAINE, SINCE 2016



In April 2022, ESET reports malware is uncovered at a Ukrainian utility provider

INDUSTROYER2 overlaps with CRASHOVERRIDE, with fewer components



Wiper malware is deployed with INDUSTROYER2: CADDYWIPER, ORCSHRED, SOLOSHRED, & AWFULSHRED

Delivery	STAGE 1
Exploit	STAGE 1
Install/Modify	STAGE 1
C2	STAGE 1
Act	STAGE 1

2016 ELECTRUM ATTACK CAUSED A POWER OUTAGE IN KYIV FOR ABOUT 1 HOUR.

KAMACITE FACILITATED INITIAL ACCESS INTO OT NETWORK.

CRASHOVERRIDE WAS DEPLOYED BY **ELECTRUM** DISRUPT POWER TO A ¼ MILLION UKRAINE HOMES.

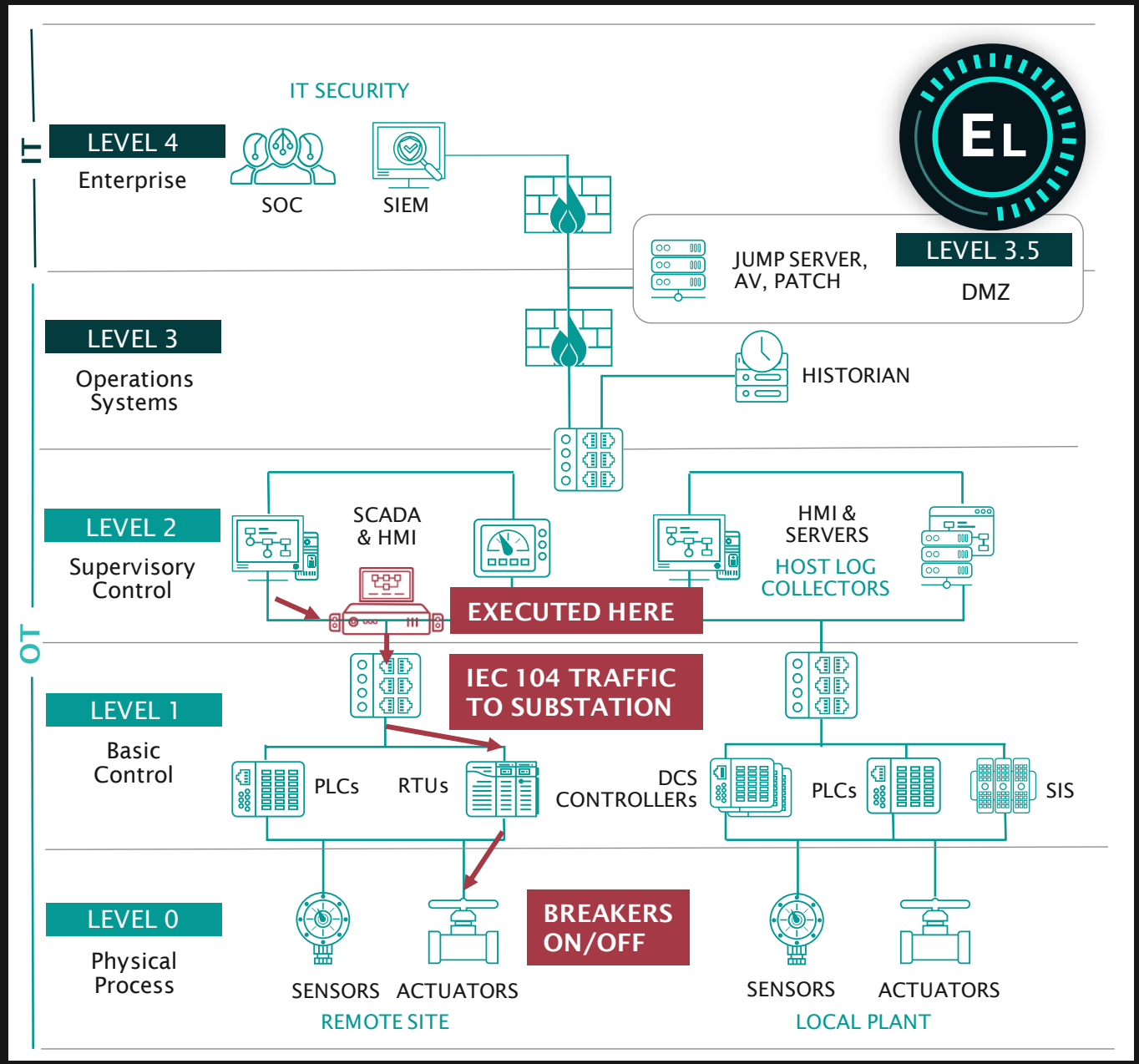
STAGE 2	Develop
STAGE 2	Test
STAGE 2	Deliver
STAGE 2	Install / Modify
STAGE 2	Execute ICS Attack

ELECTRUM INDUSTROYER 2

- Targeted substations and hardcoded configuration includes 3 IP addresses
- ELECTRUM 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.

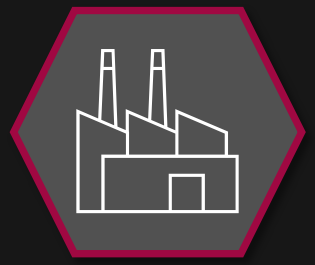


ERYTHRITE

TARGETING MULTIPLE INDUSTRIAL SECTORS IN THE U.S. & CANADA SINCE 2021

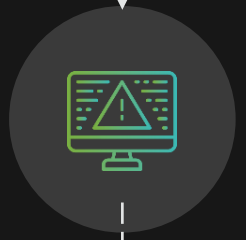
High volume of activity, focus on data & credentials

Hundreds of thousands of vulnerable, otherwise legitimate websites are abused

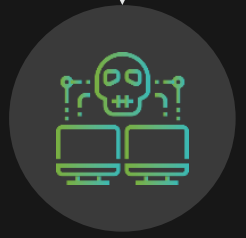


Compromised the OT network of a manufacturer, electrical utility IT network, food & beverage, automotive, oil & gas sectors

Uses adaptable search engine optimization (SEO) poisoning



Deploys custom, rapidly refreshed malware



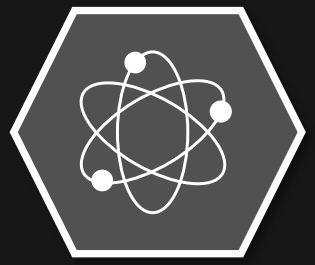
Credential stealing and remote access

WASSONITE

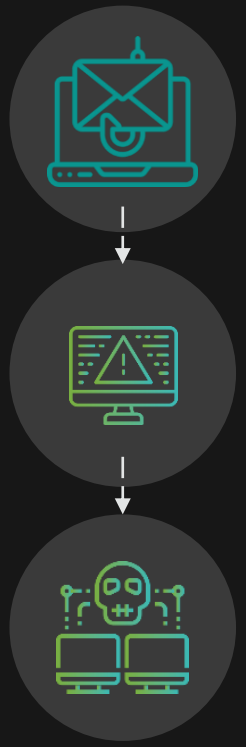
TARGETING ADVANCED INDUSTRIAL SECTORS IN SOUTH/EAST ASIA SINCE 2018

Focuses on South/East Asia, some North American entities compromised

Targeted modifications - hard-coded credentials, non-public IP addresses



In October 2022, Dragos analyzed WASSONITE's nuclear-energy themed spear phishing lures



Customized spearphishing lures for specific industries & organizations

Deployment of customized variants of AppleSeed backdoor RAT

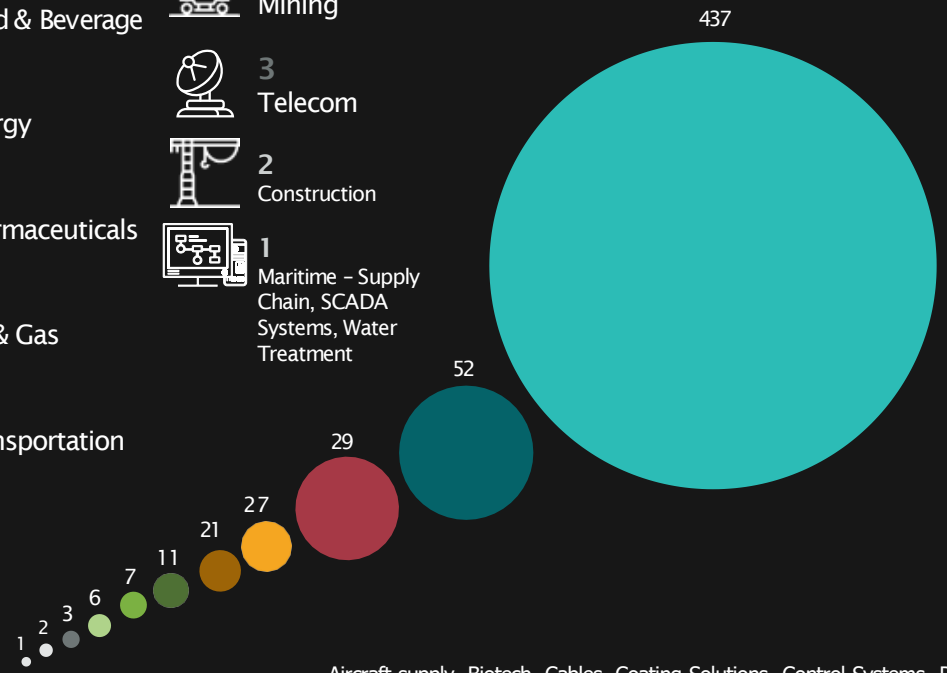
Takes screenshots, logs keystrokes, collects files, executes commands

RANSOMWARE ATTACKS INCREASED BY 87%

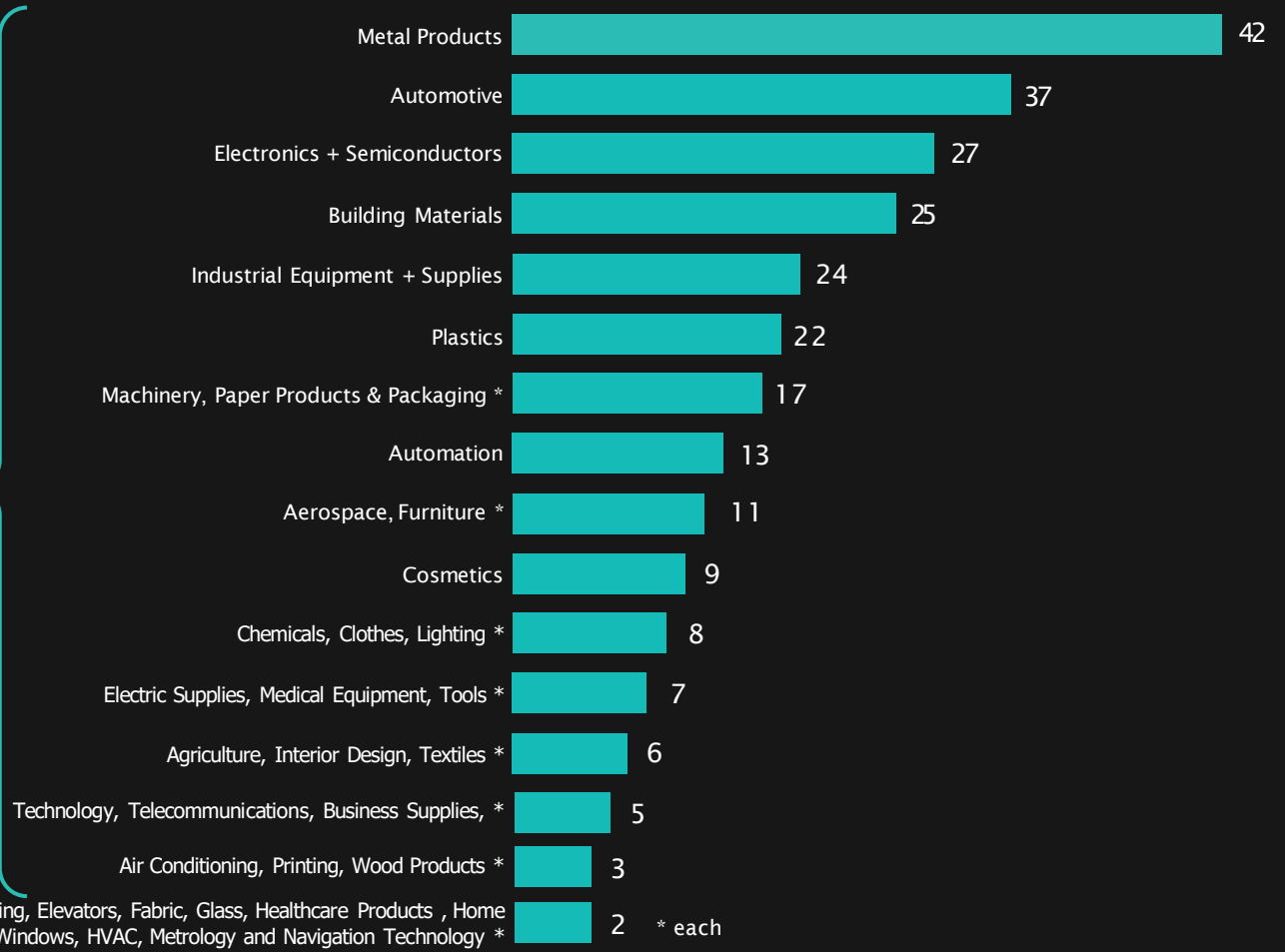
MANUFACTURING TARGETED IN 72% OF 2022 INCIDENTS

Ransomware by ICS Sector

- **437** Manufacturing
- **52** Food & Beverage
- **29** Energy
- **27** Pharmaceuticals
- **21** Oil & Gas
- **11** Transportation
- **7** Engineering, Utilities
- **6** Mining
- **3** Telecom
- **2** Construction
- **1** Maritime – Supply Chain, SCADA Systems, Water Treatment

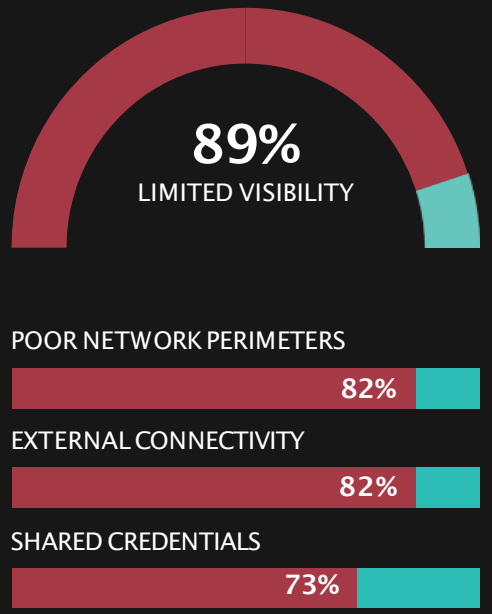


Ransomware by Manufacturing Subsector



RANSOMWARE USE CASE: MANUFACTURING

RANSOMWARE IS ONE OF THE TOP FINANCIAL & OPERATIONAL CYBER RISKS TO THE MANUFACTURING INDUSTRY



MANUFACTURING SECTOR IS OFTEN THE LEAST MATURE IN THEIR OT SECURITY DEFENSES

Kojima

February 2022
Plant operations were suspended for several days.

AGCO
Your Agriculture Company

May 2022
Likely a precautionary shutdown of their IT networks impacted ICS/OT operations.

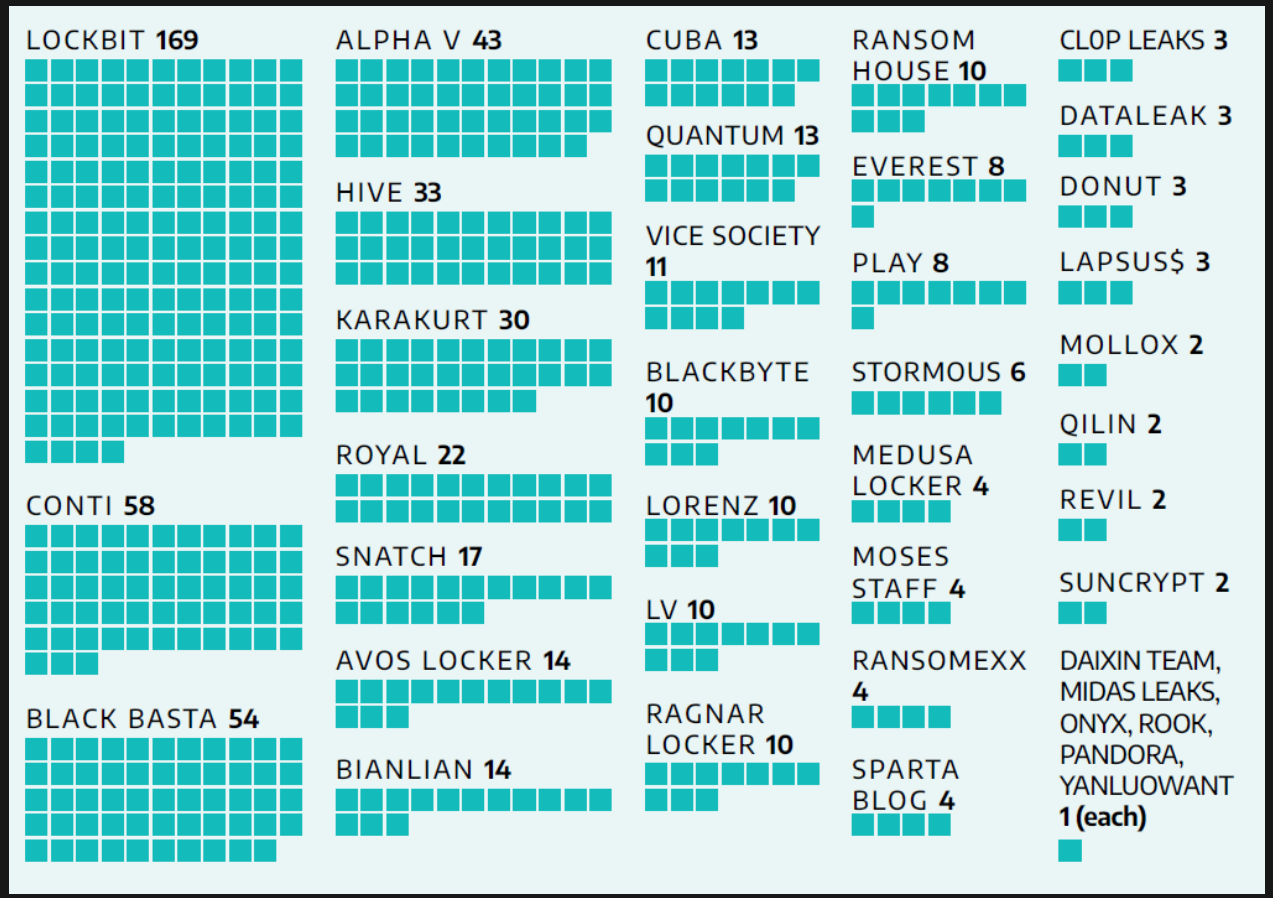
FOXCONN

May 2022
Compromised data included electric system topology info.

RANSOMWARE GROUPS – MOVES AND CHANGES

LOCKBIT 2.0 + LOCKBIT 3.0 ACCOUNTED FOR 28% OF RANSOMWARE ATTACKS

CONTI SHUT DOWN OPERATIONS IN MAY



39 groups accounted for

605 ransomware attacks

■ = 1 RANSOMWARE ATTACK

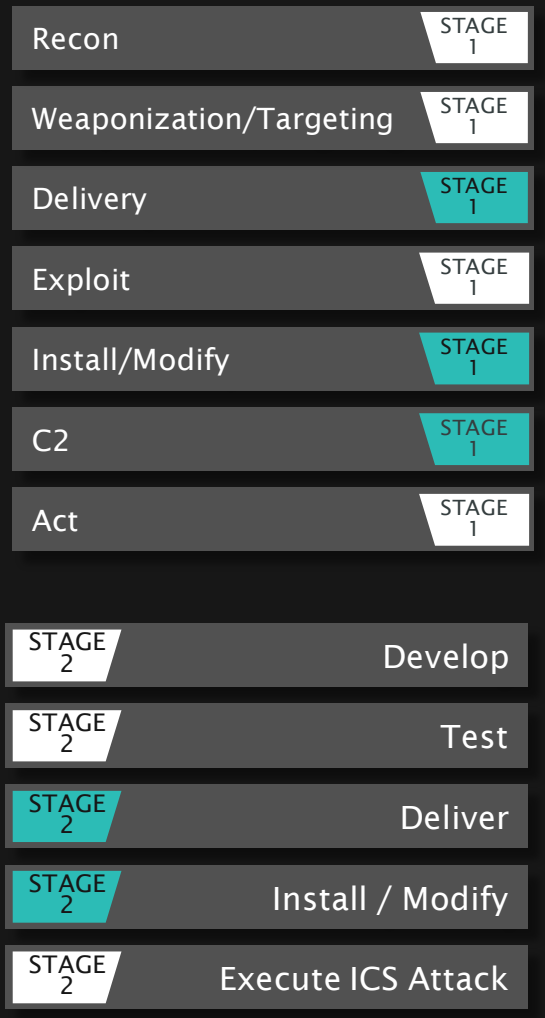
RANSOMWARE ADVERSARY CASE STUDY: BLACK BASTA

ARE BLACK BASTA ICS/OT EXPERTS?

Black Basta continues to cause ransomware attacks on industrial infrastructure in 2023:

- Appears exclusive; no recruiting for outside affiliates
- Advanced techniques, including email thread hijacking, EDR evasion, & privilege escalation
- Heritage of links to FIN7, Conti, BlackMatter, Darkside
- Well honed, rapid exfiltration & lock cycle

RANSOMWARE ADVERSARY CASE STUDY: BLACK BASTA



- Heritage of links to FIN7, Conti, BlackMatter, and Darkside (of Colonial Pipeline infamy)
- Appears exclusive; no recruiting for outside affiliates
- Advanced techniques, including email thread hijacking, EDR evasion, and operationalized privilege escalation
- Honed rapid exfiltration and lock cycle
- Took a break Christmas Eve 2022, did not go back to work until February 2023
- Are Black Basta a gang of OT and ICS experts?
- Black Basta continues its disruption causing attacks into 2023

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

- BENTONITE has exhibited Stage 1 capability and has shown evidence of OT data exfiltration from ONG & Manufacturing targets
- Manufacturing is the standout ransomware sector by a large margin
- All manufacturing organizations should factor in ransomware threats to their threat models

FIVE CRITICAL CONTROLS

CRITICAL CONTROLS FOR EFFECTIVE OT CYBERSECURITY

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

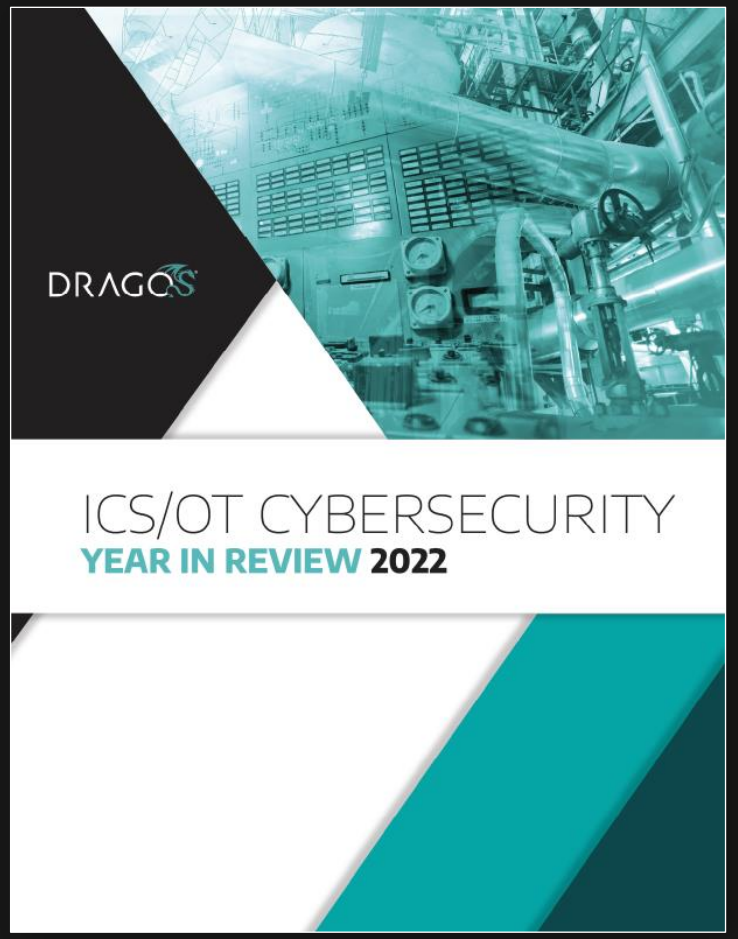
Join us again!

April 18th

Vulnerability Briefing

May 16th

Lessons Learned From the Frontlines



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