Why PIPEDREAM is no ordinary malware

and how it fundamentally changes the threat landscape

Oliver Herterich
Senior Solution Architect
Dragos, Inc.

INTRODUCTION

STAGES OF THE ICS CYBER KILL CHAIN

STAGE 1

Initial survey & access to the enterprise IT environment

Crossing into ICS/OT

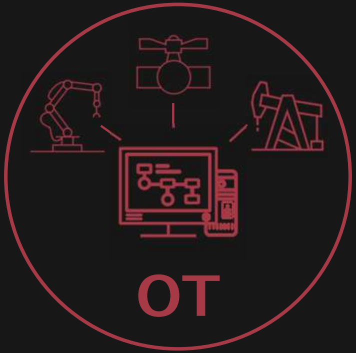
STAGE 2

OT network reconnaissance, penetration, & execution of ICS attacks

Avoid Custom Software & Malware

Emphasize Commodity & System Tools

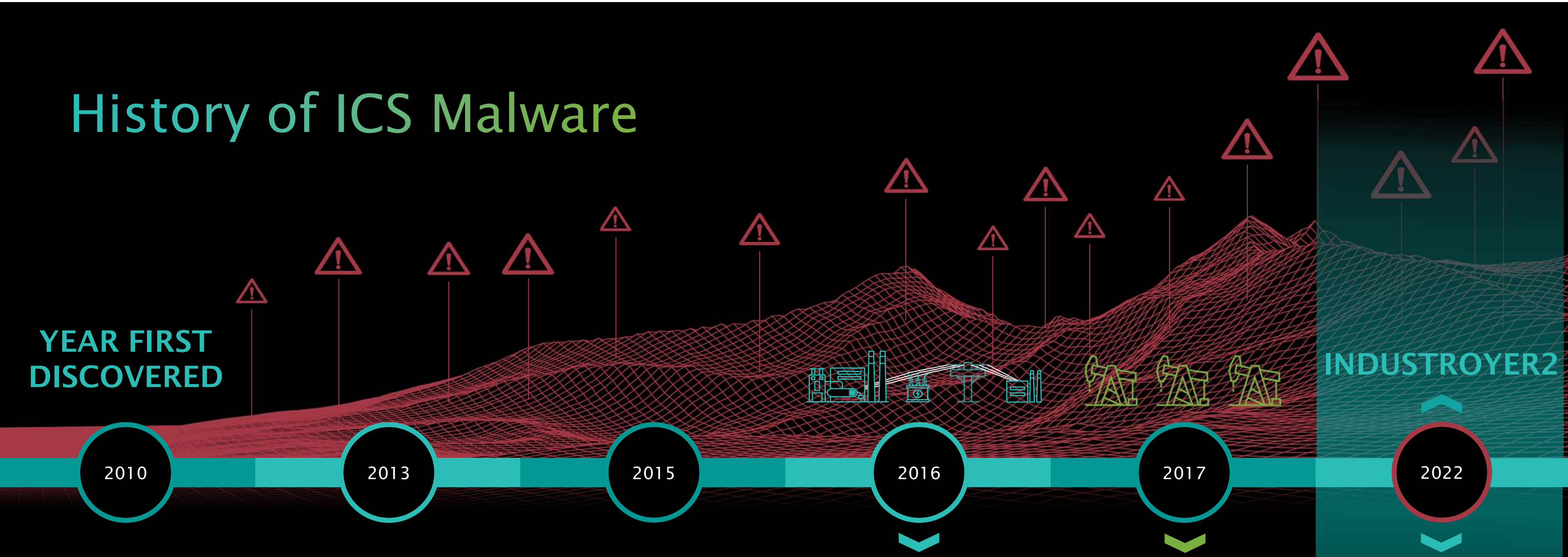
Different systems, network traffic, adversaries, & need to manage vulnerabilities differently



Custom Attack Packages Tailored to a Specific Environment

Limited Ability to Replay or Reuse Attacks

History of ICS Malware



YEAR FIRST DISCOVERED

2010

STUXNET

2013

HAVEX

2015

BLACKENERGY

2016

CRASHOVERRIDE

Effective techniques with little knowledge of protocols used.

IEC101, IEC104, IEC61850/MMS, OPC-DA

2017

TRISIS

Much more in-depth attack.

Understanding of the protocols for reconnaissance and attack.

TRISTATION, TCM, Triconex OS

INDUSTROYER2

2022

PIPEDREAM

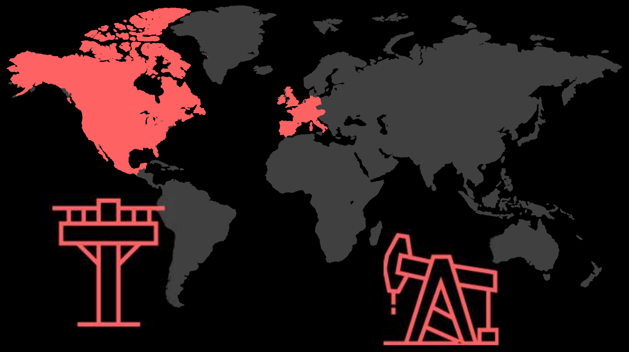
Combines aspects of CRASHOVERRIDE and TRISIS.

Significant breadth and depth of protocol and controller knowledge.

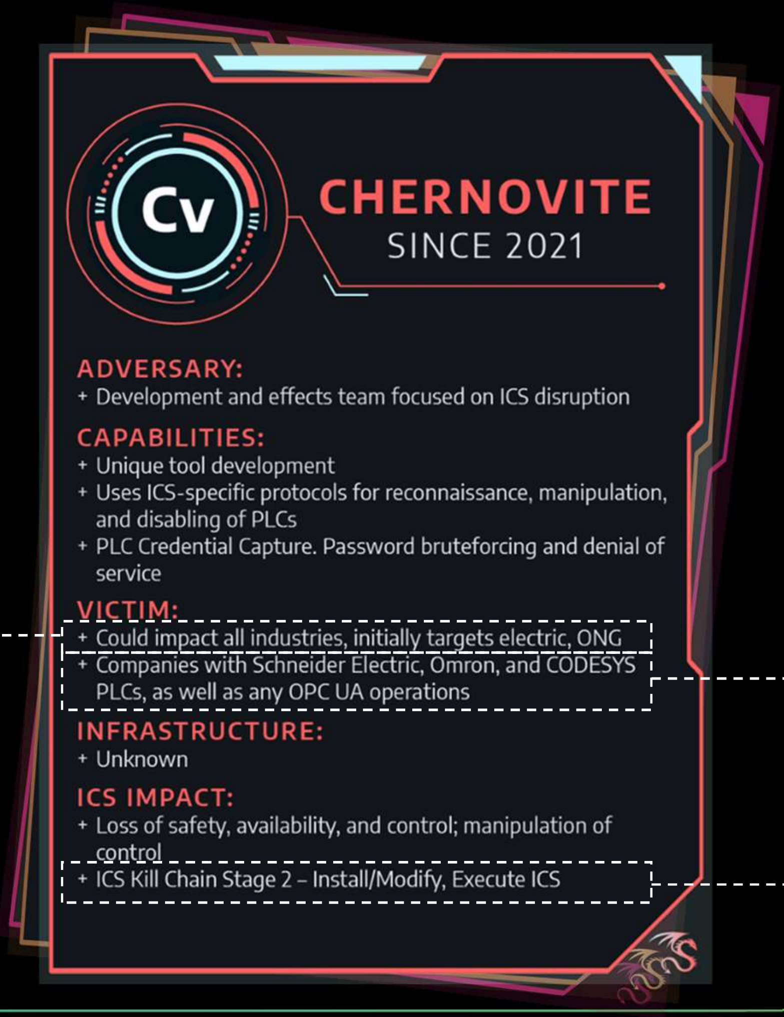
CHERNOVITE:
PIPEDREAM

CHERNOVITE: NEW IN 2022

ICS/OT SYSTEM SPECIALIST



Potential to impact all industries and regions



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

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

Tens of thousands of ICS vendors use CODESYS, Modbus, OPC UA

Capable of Stage 2 of the ICS Cyber Kill Chain

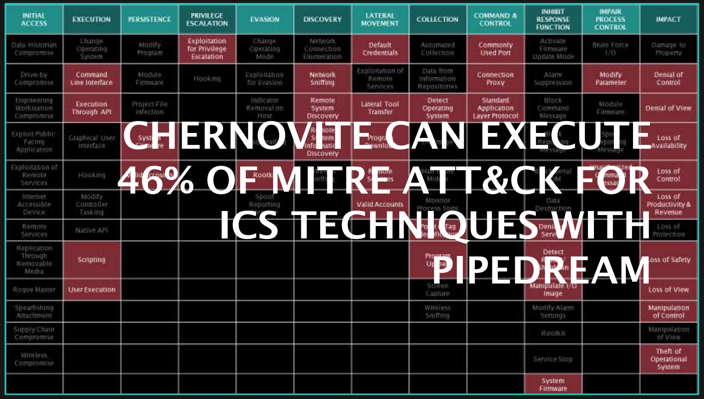
CHERNOVITE'S PIPEDREAM MALWARE

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



INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND & CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
Data Historian Compromise	Change Operating System	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Engineering Workstation Compromise	Execution Through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating System	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Exploit Public-Facing Application	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Exploitation of Remote Services	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Internet Accessible Device	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity & Revenue
Remote Services	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Replication Through Removable Media	Scripting						Program Upload		Device Restart/ Shutdown		Loss of Safety
Rogue Master	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Spearfishing Attachment							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Supply Chain Compromise									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational System
									System Firmware		

CHERNOVITE CAN EXECUTE 46% OF MITRE ATT&CK FOR ICS TECHNIQUES WITH PIPEDREAM

EVILSCHOLAR & BADOMEN are extensible – this is rare.

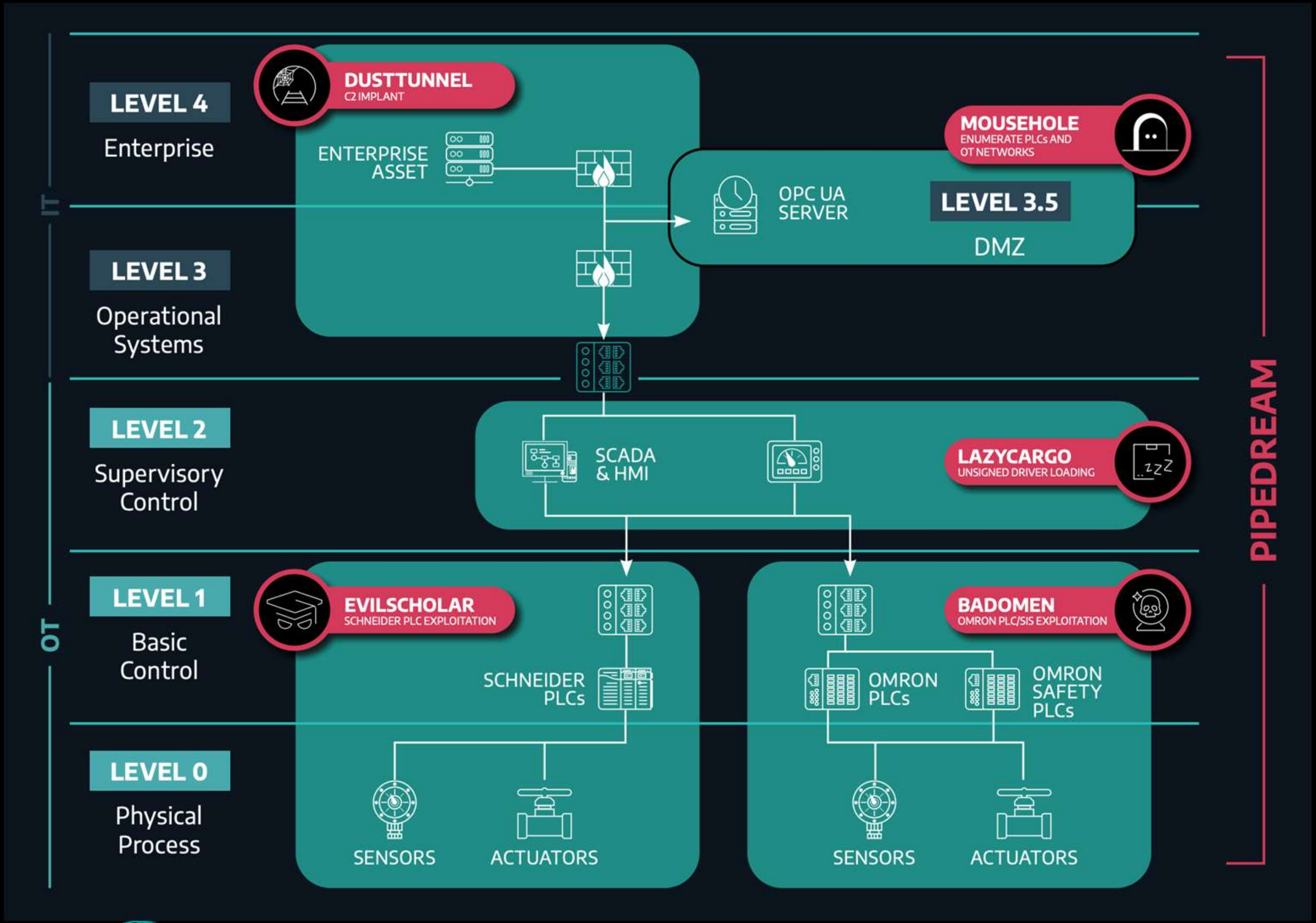
1000s of CODESYS devices across multiple sectors at risk

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.

An Example Deployment Scenario



Impact:

- Denial of Control, View
- Loss of Availability, Control, Safety and View
- Manipulation of Control
- Program Download/Upload

MITIGATION &
OT BEST PRACTICES

PROTECTION AGAINST PIPEDREAM

Monitor East-West ICS networks with ICS protocol aware technologies

- Perform network traffic monitoring on East-West communications in addition to North-South (ingress/egress) communications. Look for modifications to PLCs occurring outside of maintenance periods such as changing the logic using native ICS protocols.

Conduct network telemetry analysis

- Look for non-standard workstations or accounts to identify unusual interactions with PLCs.

Network isolation of safety systems

- Monitor safety system networks for new connections or devices and verify all configuration changes comply with change management procedures.

Isolate mission critical skid systems

- Consider implementing hardwired I/O between critical skid systems and distributed control systems I/O in place of direct communications if feasible.

LONG-TERM READINESS

ICS FOCUSED INCIDENT RESPONSE PLAN

Create and update an ICS-focused Incident Response Plan with accompanying SOPs and EOPs for operating with a hampered or degraded control system.

SPARE PARTS & INVENTORY PLAN

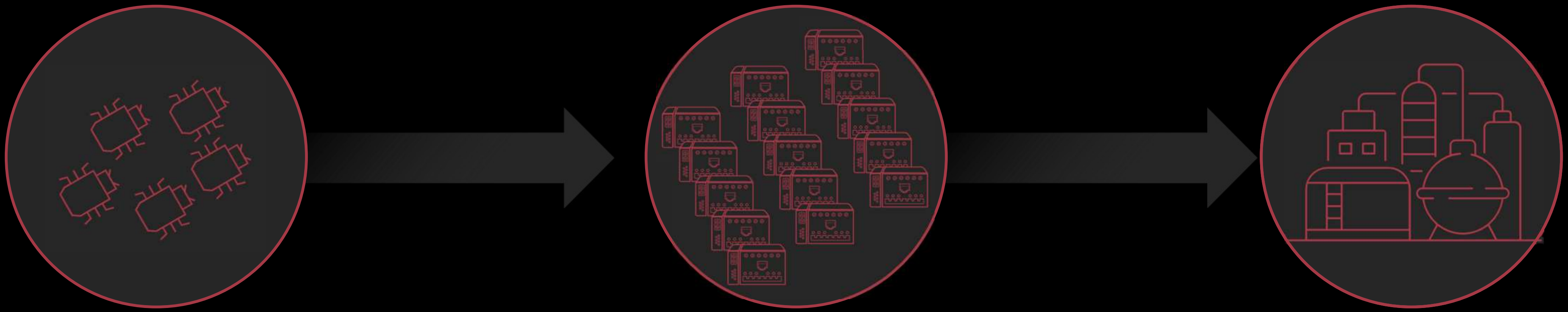
Create and update a spare parts inventory for critical control system components, including hardware, software, firmware, configuration backups, and licensing information. Develop plans and procedures for sourcing and procurement of critical control system components. Consider the implementation of cold backups for rapid replacement of ICS level on devices.

THREAT LANDSCAPE

CHERNOVITE’S PIPEDREAM

EVOLUTION OF ICS/OT MALWARE

FIRST scalable, cross-industry OT attack framework (7TH overall ICS/OT specific)
Discovered before it was employed for destructive purposes.



5 ICS PROTOCOLS ABUSED
FINS, MODBUS, CODESYS, OPC UA, Schneider Electric NetManage

100s VENDORS IMPACTED

1000s DEVICES POTENTIALLY IMPACTED

CAPABLE OF DISRUPTIVE & DESTRUCTIVE ICS CYBER ATTACKS

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.

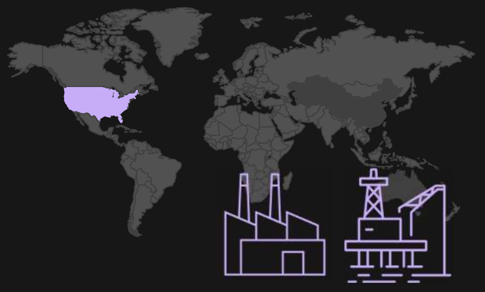
Is skilled in software development.

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

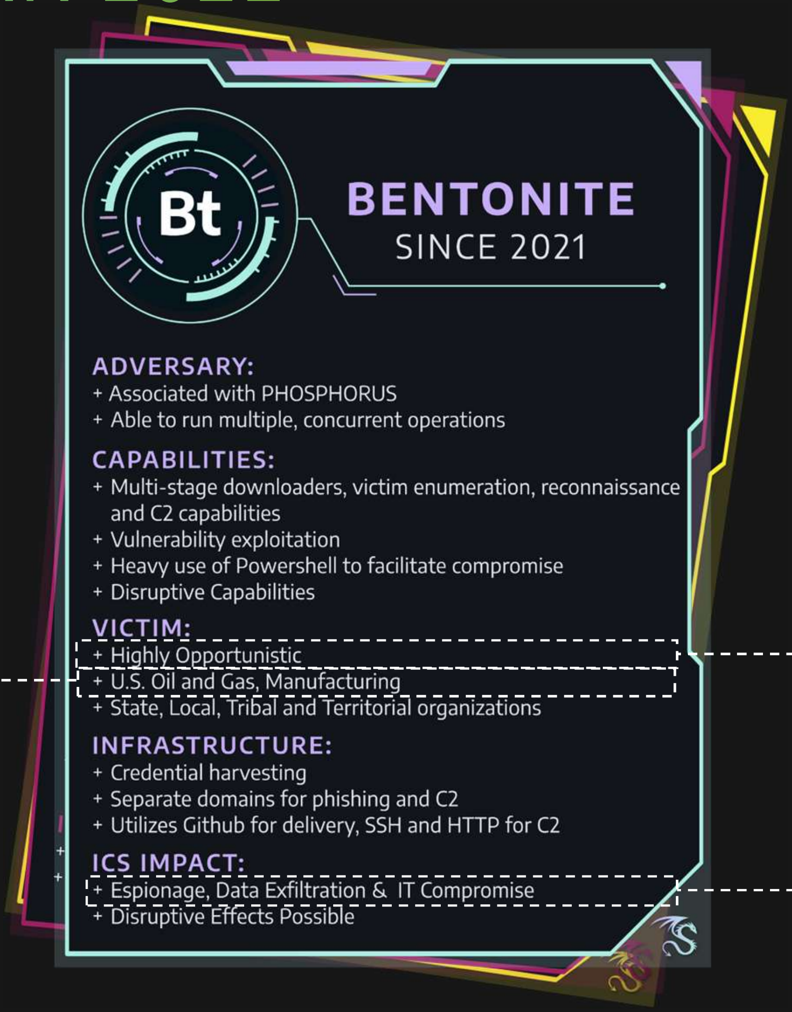
Has knowledge to achieve an impact.

BENTONITE: NEW IN 2022

OPPORTUNISTIC EXPLOITATION



Targets **Oil & Gas, Manufacturing**



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

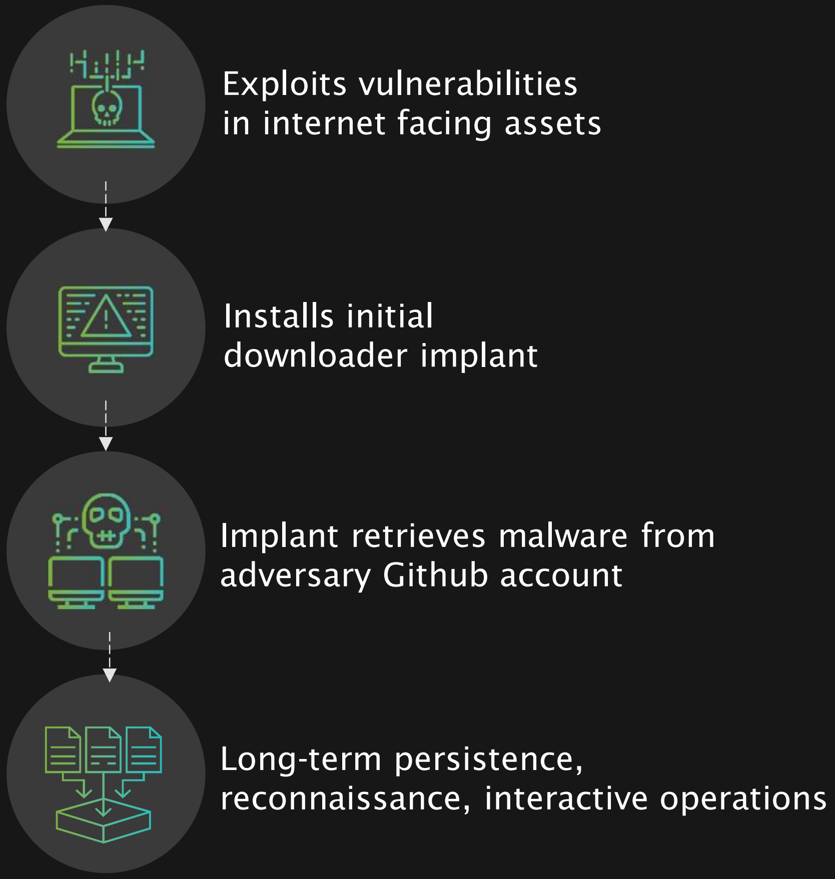
Delivery	STAGE 01
Exploit	STAGE 01
Install/Modify	STAGE 01
C2	STAGE 01
Act	STAGE 01

Highly opportunistic

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

BENTONITE: OPPORTUNISTIC EXPLOITATION

RECONNAISSANCE & LONG-TERM PERSISTENCE

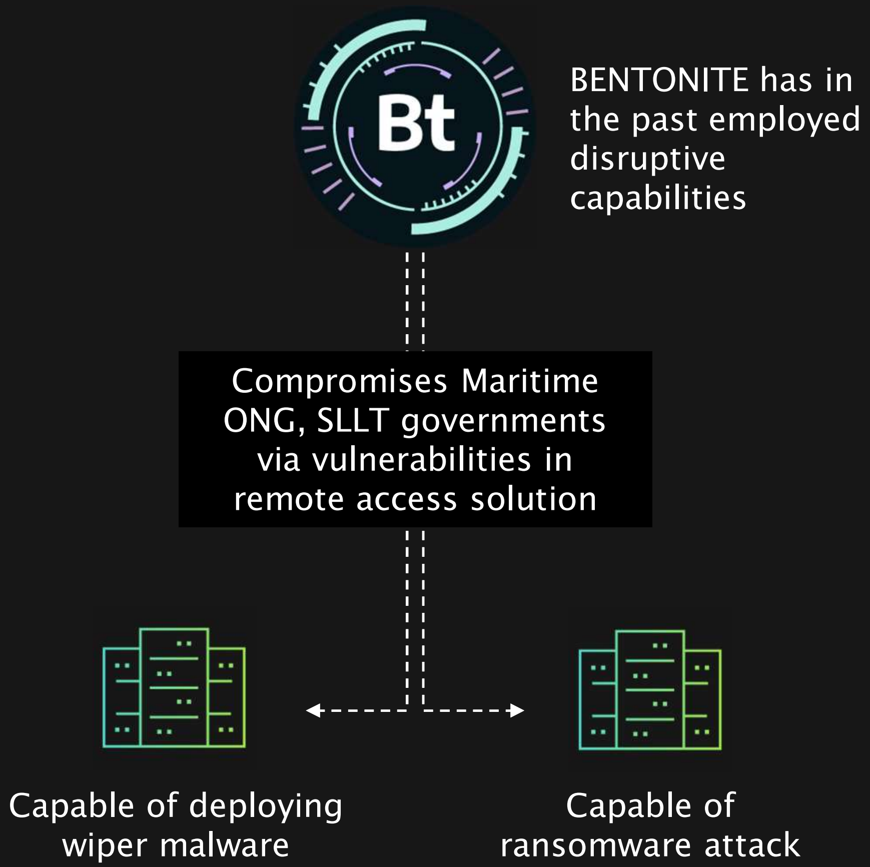


Exploits vulnerabilities in internet facing assets

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

ELECTRUM

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

EL

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.

Ka

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

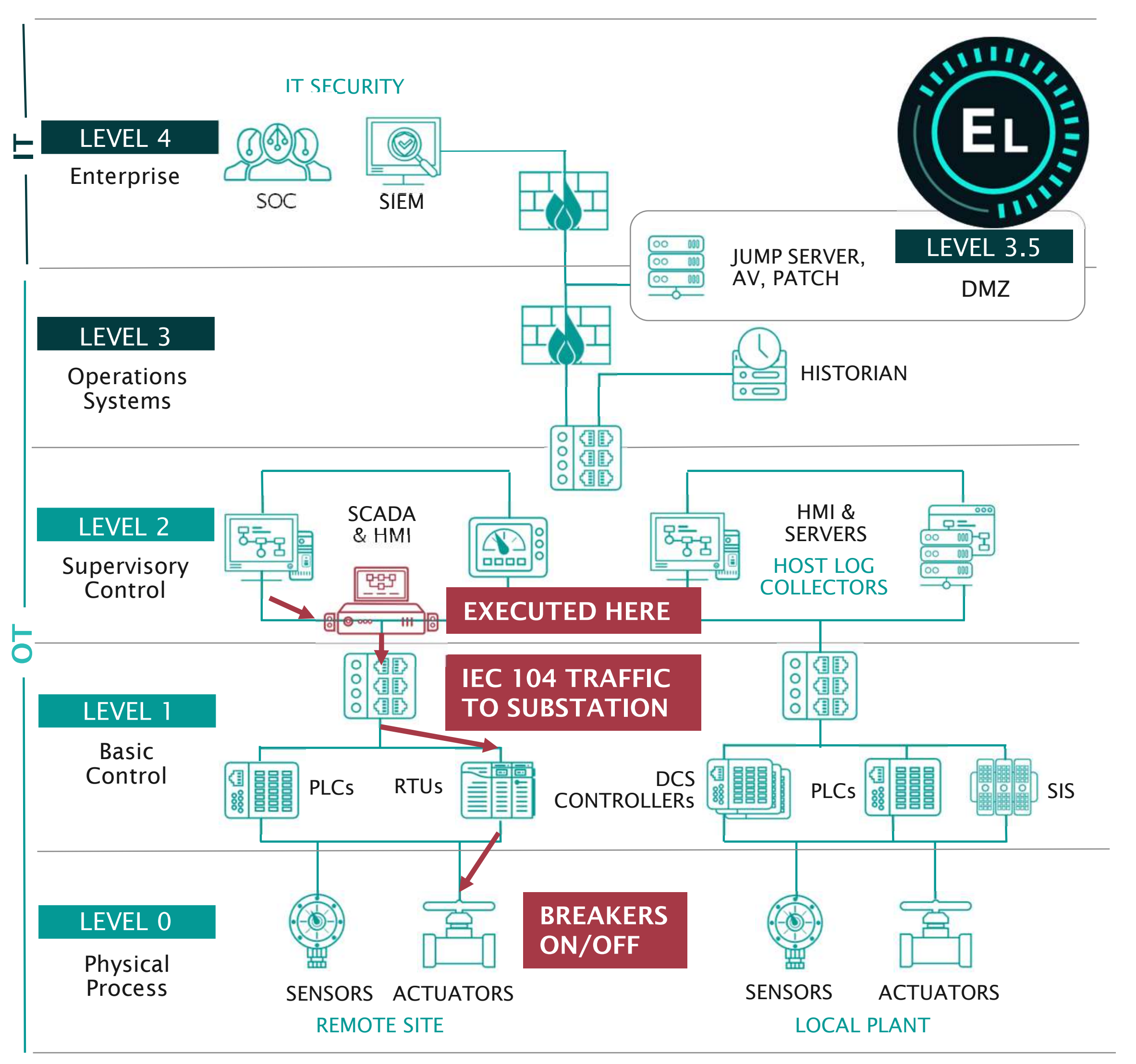
- STAGE 2 — **Develop**
- STAGE 2 — Test
- STAGE 2 — Deliver
- STAGE 2 — Install / Modify
- STAGE 2 — Execute ICS Attack

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.



IT

OT

LEVEL 4
Enterprise

IT SECURITY

SOC

SIEM

JUMP SERVER,
AV, PATCH

LEVEL 3.5
DMZ

LEVEL 3
Operations
Systems

HISTORIAN

LEVEL 2
Supervisory
Control

SCADA
& HMI

HMI &
SERVERS

HOST LOG
COLLECTORS

EXECUTED HERE

LEVEL 1
Basic
Control

IEC 104 TRAFFIC
TO SUBSTATION

PLCs

RTUs

DCS
CONTROLLERs

PLCs

SIS

LEVEL 0
Physical
Process

SENSORS

ACTUATORS

BREAKERS
ON/OFF

SENSORS

ACTUATORS

REMOTE SITE

LOCAL PLANT

THREAT GROUPS INCREASE ACTIVITY IN 2022

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

Ko

KOSTOVITE

Dragos observed a possible link to multiple adversaries sharing common infrastructure with KOSTOVITE, with reports of exploitation of vulnerabilities by linked APT5.

Targeting Energy
North America, Australia

Ka

KAMACITE

Victims in multiple sectors are observed communicating with KAMACITE Cyclops Blink C2 infrastructure. Cyclops Blink malware is removed from firewall devices.

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

Xt

XENOTIME

Dragos observed reconnaissance and research activity focused on oil and gas entities in the U.S.

Targeting Oil & Gas, Electric
Middle East,
North America

EL

ELECTRUM

INDUSTROYER2 malware and a set of wiper malware is discovered at a Ukraine energy provider.

Targeting Electric
Ukraine, Europe

Er

ERYTHRITE

Continued targeting of industrial organizations with SEO poisoning techniques and custom, rapidly deployed malware.

Multiple Industrial Sectors Targeted
U.S, Canada

Wa

WASSONITE

Dragos observed ongoing deployment of nuclear energy themed spear phishing lures to deliver backdoor malware.

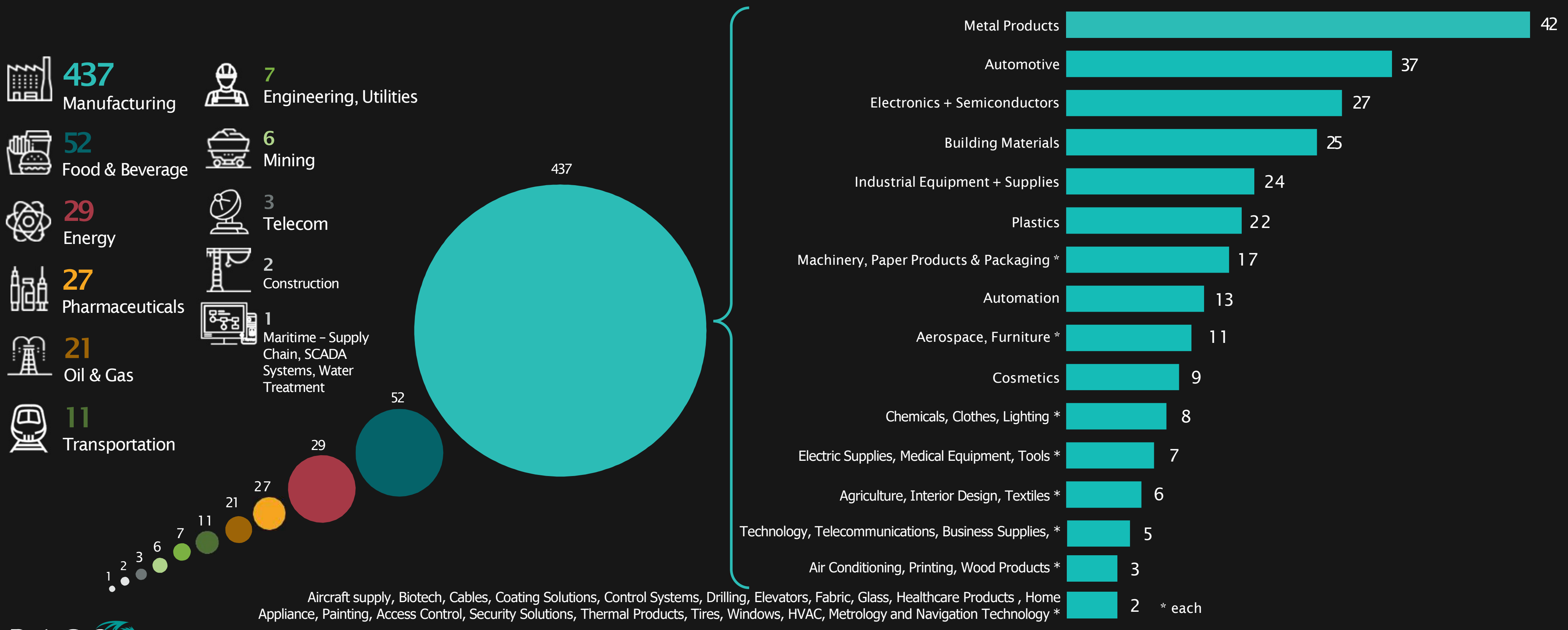
Multiple Industrial Sectors Targeted
South/East Asia,
North America

RANSOMWARE ATTACKS INCREASED BY 87%

MANUFACTURING TARGETED IN 72% OF 2022 INCIDENTS

Ransomware by ICS Sector

Ransomware by Manufacturing Subsector



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 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

KEY TAKEAWAYS

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

THANK YOU