OT CYBERSECURITY

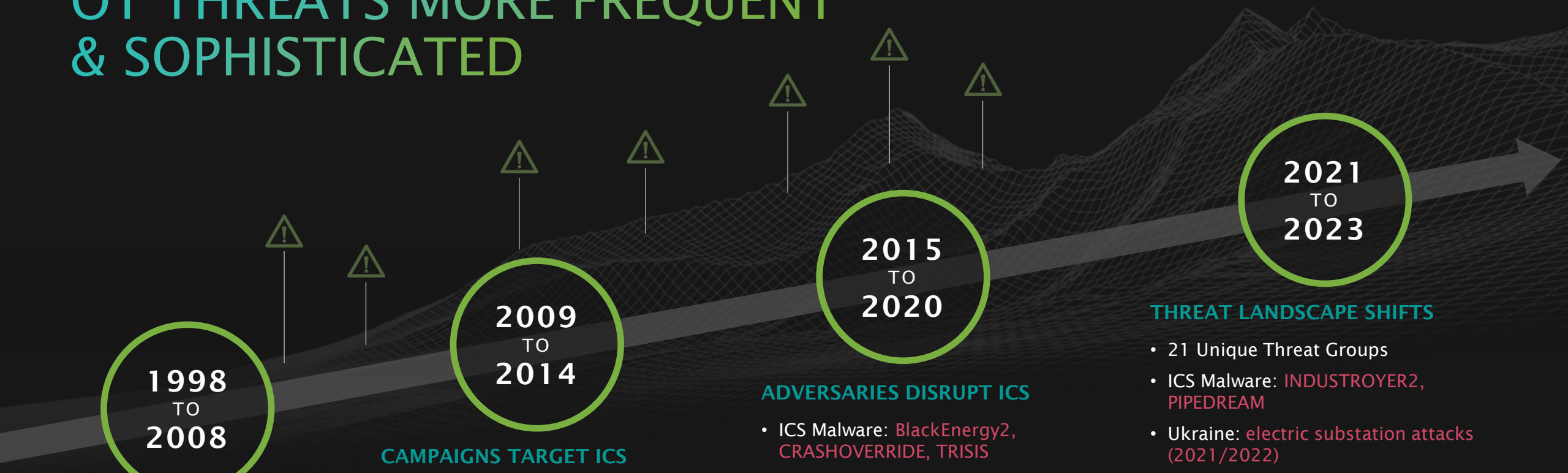
THE 2023 YEAR IN REVIEW

THREAT LANDSCAPE

Bryce Livingston
Senior Adversary Hunter

Conor McLaren
Principal Adversary Hunter

OT THREATS MORE FREQUENT & SOPHISTICATED



1998 TO 2008

LACK OF COLLECTION

- Campaigns: APT1
- ICS Malware: None

2009 TO 2014

CAMPAIGNS TARGET ICS

- ICS Malware: Stuxnet, Havex
- Campaigns: Sandworm, Dragonfly
- Ukraine: Germany: 1st attack cause physical destruction on civilian infrastructure (steel)

2015 TO 2020

ADVERSARIES DISRUPT ICS

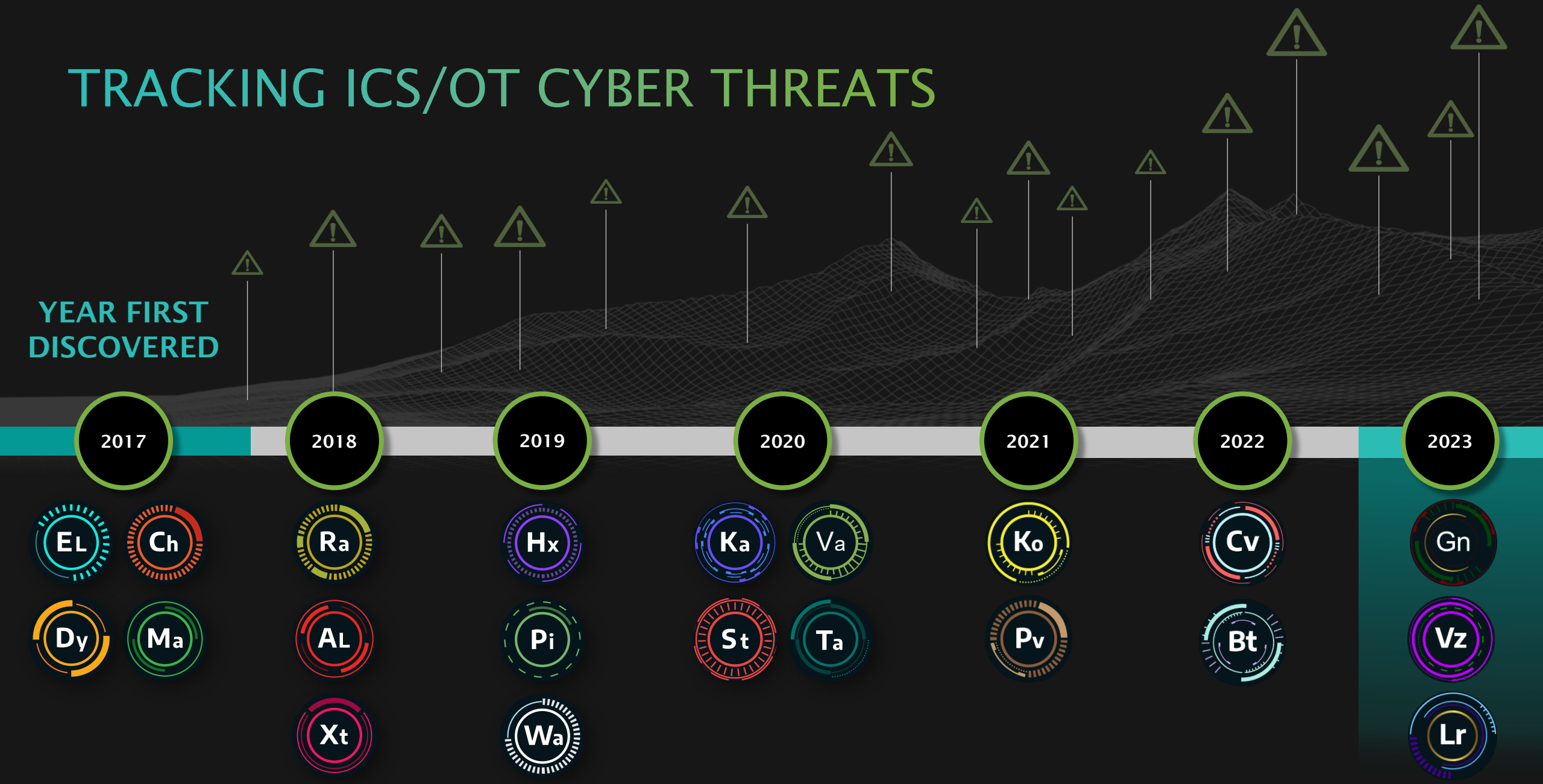
- ICS Malware: BlackEnergy2, CRASHOVERRIDE, TRISIS
- Campaigns: Dragonfly 2.0
- Ukraine: disruption of electric power operations (2015), major electric grid disruption (2016)
- Saudi Arabia: first attack targeting human life (2017)

2021 TO 2023

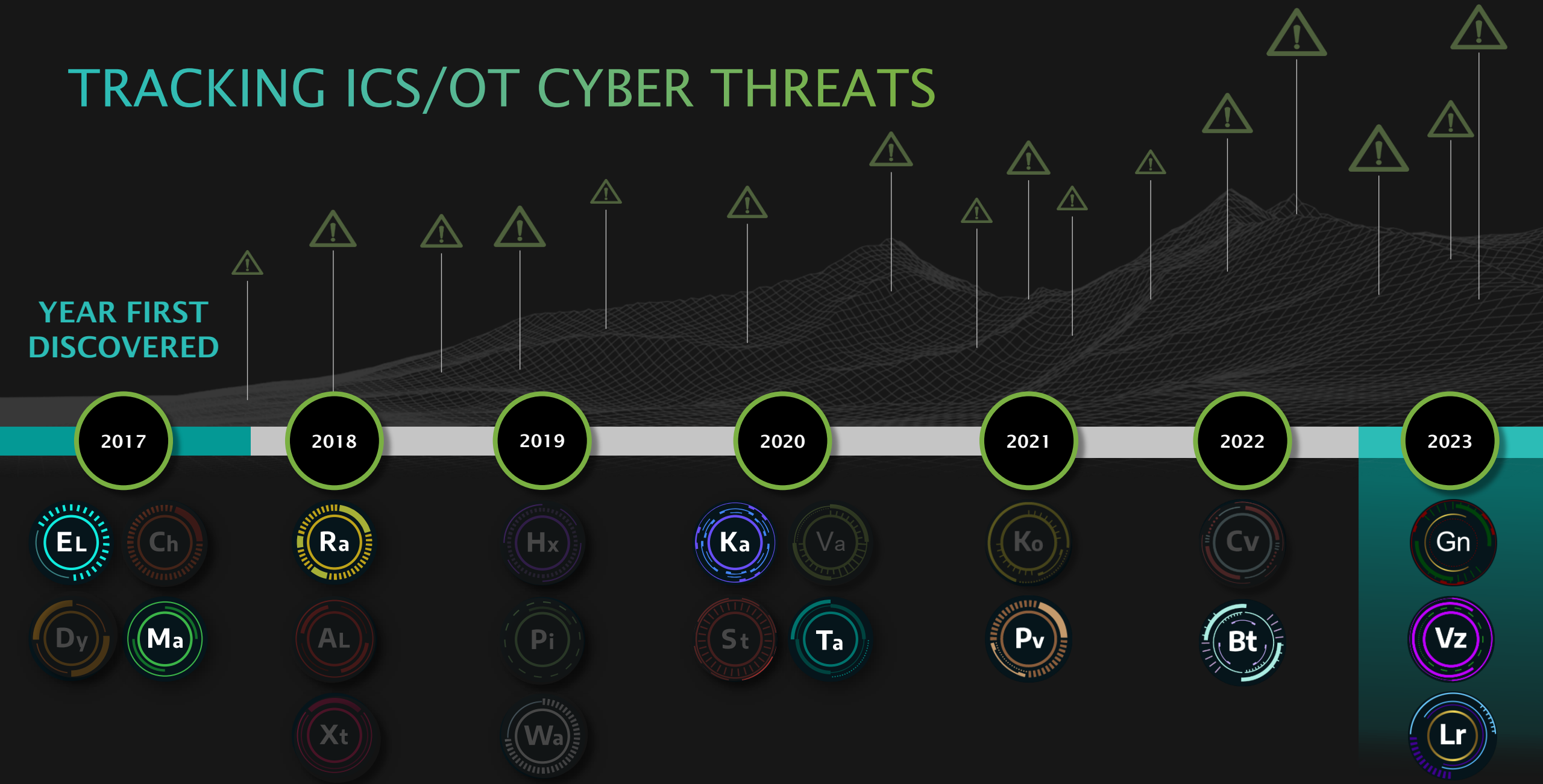
THREAT LANDSCAPE SHIFTS

- 21 Unique Threat Groups
- ICS Malware: INDUSTROYER2, PIPEDREAM
- Ukraine: electric substation attacks (2021/2022)
- Oldsmar, FL: Water Treatment attack
- Hacktivist Attacks: disruption of water utilities in U.S., Europe (2023)
- Ransomware attacks: Colonial Pipeline, JBS Foods, Norsk Hydro, Kojima, Foxconn, Dole, Yanfeng Automotive, Boeing

TRACKING ICS/OT CYBER THREATS



TRACKING ICS/OT CYBER THREATS



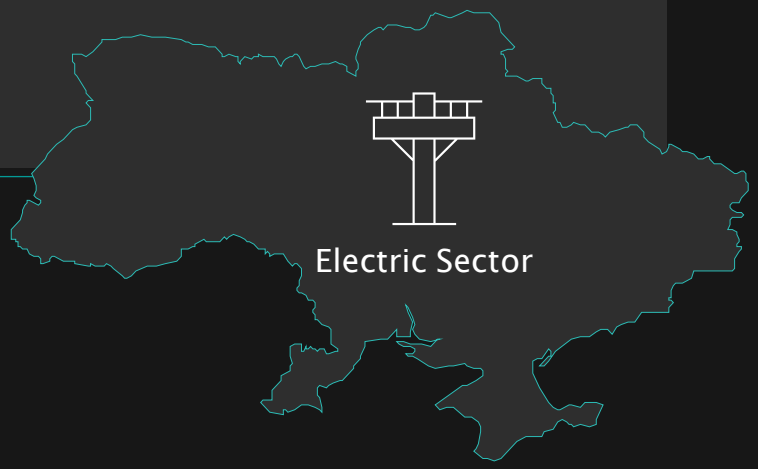
CONFLICT-DRIVEN CYBER ACTIVITY

CYBER

Dedicated, mature threat groups targeting industrial infrastructure networks: ELECTRUM & KAMACITE

Aggressive cyber operations to achieve geopolitical objectives in Ukraine-Russia war

Targeting Ukraine electric sector



KINETIC

THE KYIV INDEPENDENT

NATIONAL, HOT TOPIC, WAR, WAR UPDATE

Ukraine war latest: Power deficit still 'significant' after Russia launches 'more than 1,000 missiles and drones' at Ukrainian energy since October

Share

by Asami Terajima · December 9, 2022 11:42 PM · 2 min read

USA TODAY

Subscribe Sign in

Russian missile attacks on Ukraine power grids cut electricity, heat and water to millions

Ukrainians are living with less electricity since Russia began unleashing missiles to attack power grids around the country, causing blackouts.

Karina Zaiets and Stephen J. Beard USA TODAY

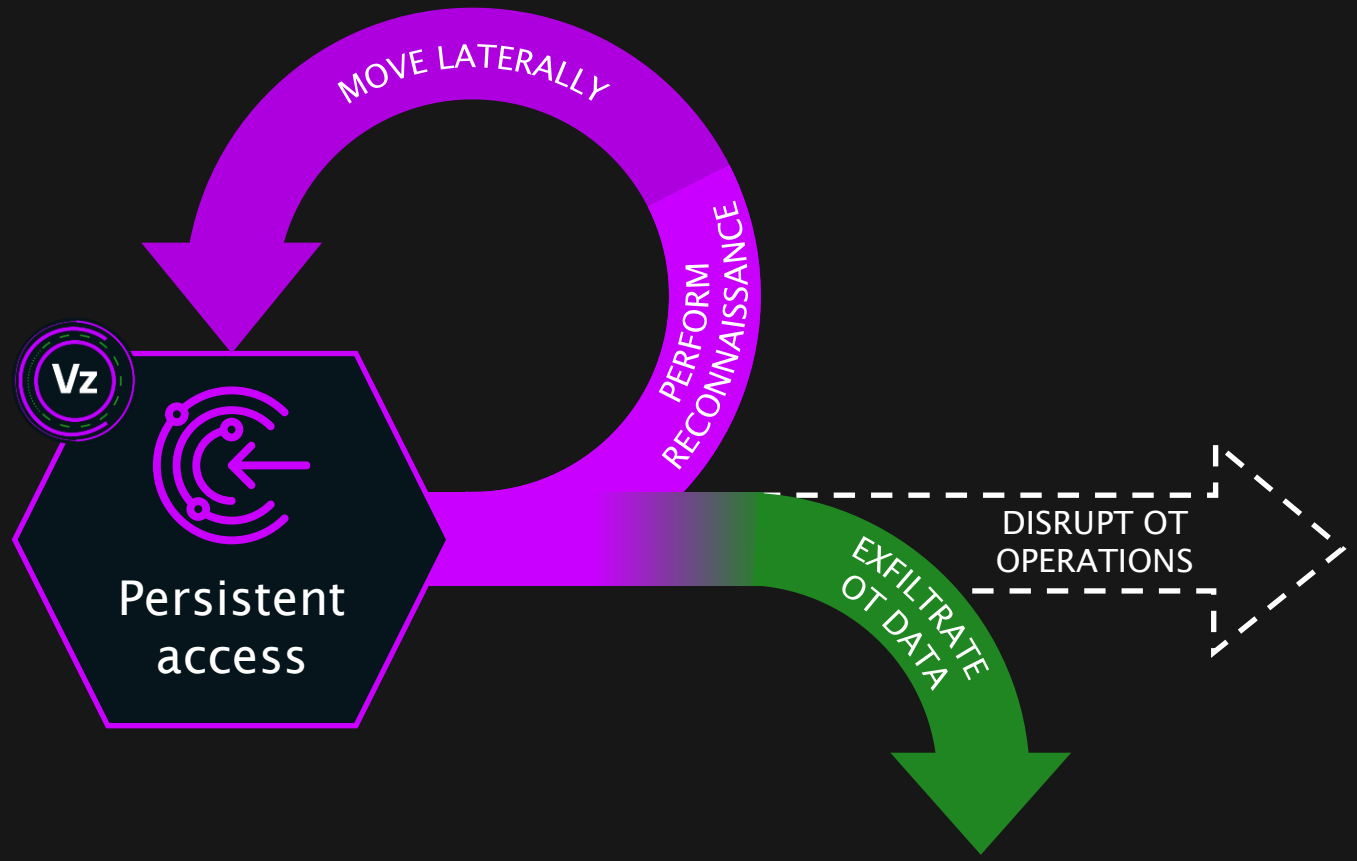
Published 7:30 AM EST Dec. 24, 2022 | Updated 7:30 AM EST Dec. 24, 2022

ESPIONAGE OPERATIONS: IMPLICATIONS FOR ICS/OT

Gain geopolitical advantages: tensions between China & Taiwan, competition with U.S.

VOLTZITE has targeted critical infrastructure entities in Guam, the U.S., Africa since 2021

Actions involving prolonged surveillance and data gathering



TRADITIONAL HACKTIVISM MOTIVATION & TACTICS

FUD

Fear, **U**ncertainty, **D**oubt

Draw attention to geopolitical and social causes.
Influencing perceptions to create a narrative of instability.

DDoS attack

Website defacement

False claims

THE RISE OF CONFLICT-DRIVEN HACKTIVISTS

MOTIVATED BY UKRAINE-RUSSIA WAR

GhostSec
Proukraine
Zarya
Name057(16)
Anonymous Sudan
Killnet
SiegedSec
CyberArmyofRussia_Reborn

MOTIVATED BY ISRAEL-HAMAS CONFLICT

Cyber Av3ngers
ThreatSec
AnonGhost
Predatory Sparrow

ACHIEVING STAGE 2 OF ICS CYBER KILL CHAIN

November

December

Booster station belonging to the Municipal Water Authority of Aliquippa

The Full Pint Beer Brewery in Pittsburgh

Erris, Ireland water scheme

180 residents without running water for 2 days

25 26 27 28 29 30 1

CyberAven3gers posted the following message:

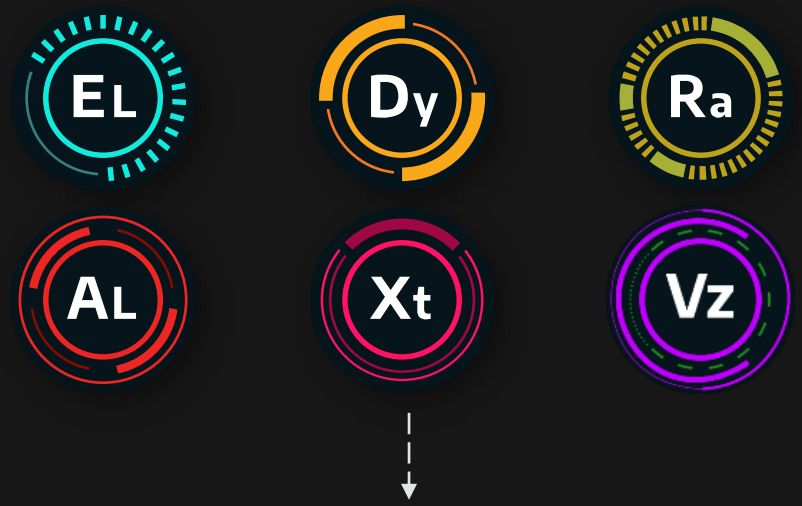
"Every Equipment "Made In Israel" Is CyberAv3ngers Legal Target!"

Images of compromised Unitronics Vision devices located in North America are shared online

Joint Cybersecurity Advisory warns of IRGC-affiliated actors exploiting PLCs in multiple sectors

LIVING OFF THE LAND (LOTL) ATTACKS

THREAT GROUPS USING LOTL TECHNIQUES

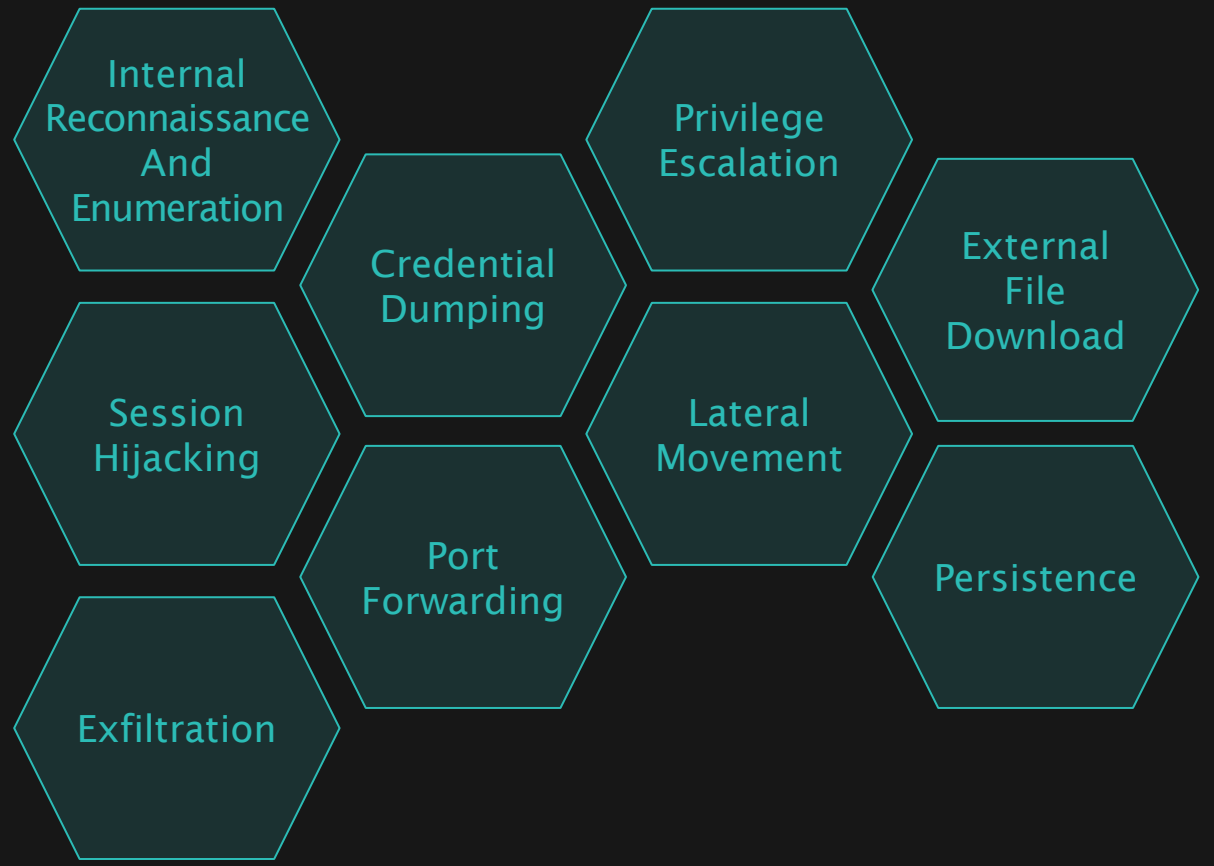


Fileless Attacks Using Tools Native to Victim Environments

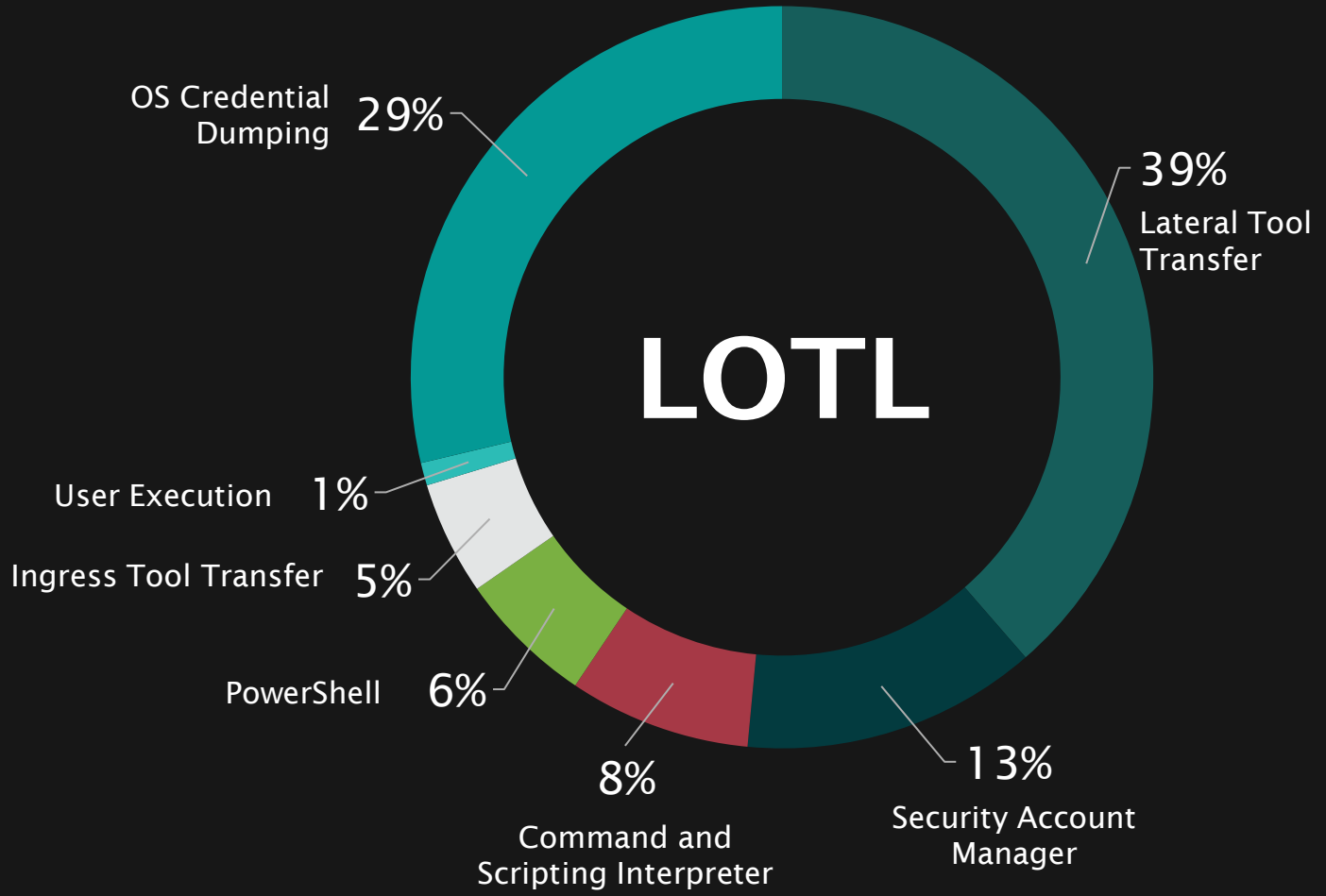
Evade Detection

Persist Longer

RANSOMWARE GROUPS USE LOTL TECHNIQUES TO ESCALATE PRIVILEGES, GAIN PERSISTENCE, & ESTABLISH C2 CHANNELS



LIVING OFF THE LAND (LOTL) TECHNIQUES



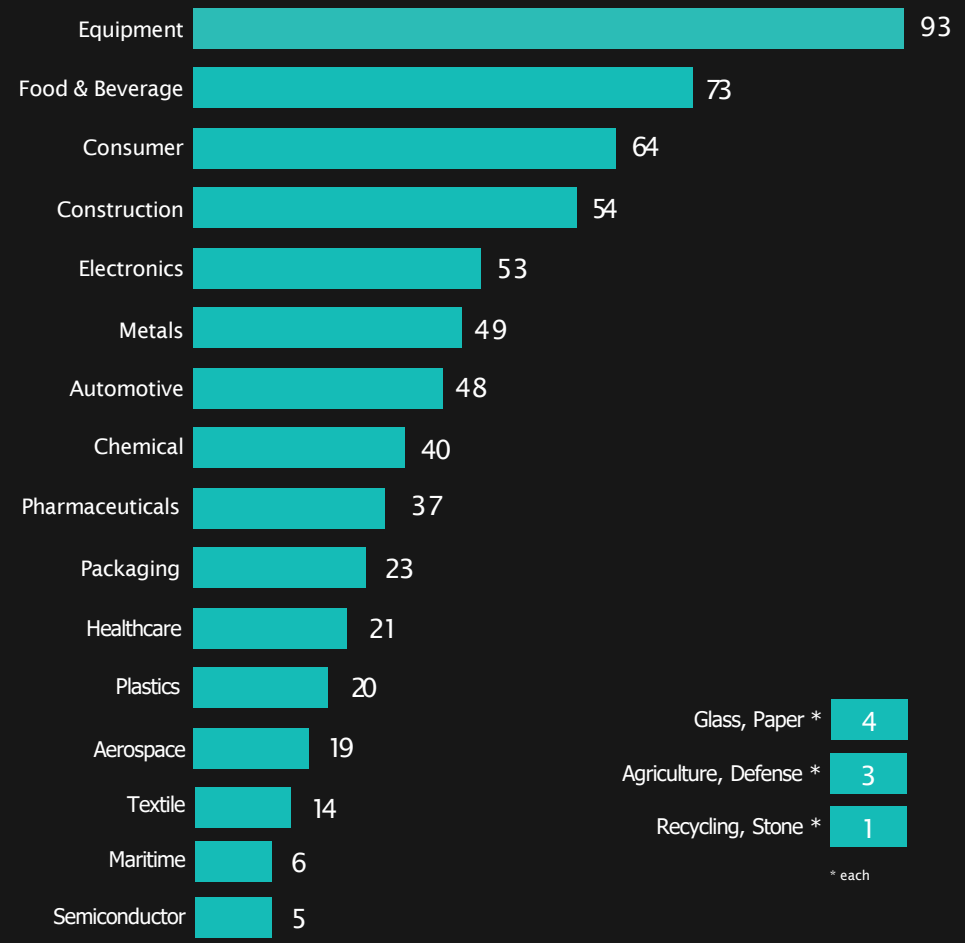
RESULTS FROM DRAGOS PROFESSIONAL SERVICES PENETRATION TESTING

RANSOMWARE ATTACKS INCREASED BY 50%

LAST YEAR, THERE WERE 905 RANSOMWARE ATTACKS AGAINST INDUSTRIAL ORGANIZATIONS

RANSOMWARE BY ICS SECTOR

- **638** Manufacturing
- **115** Industrial Control Systems
- **65** Transportation
- **30** Oil & Gas
- **20** Electric
- **13** Mining
- **10** Water
- **10** Renewables
- **2** Government
- **2** Defense



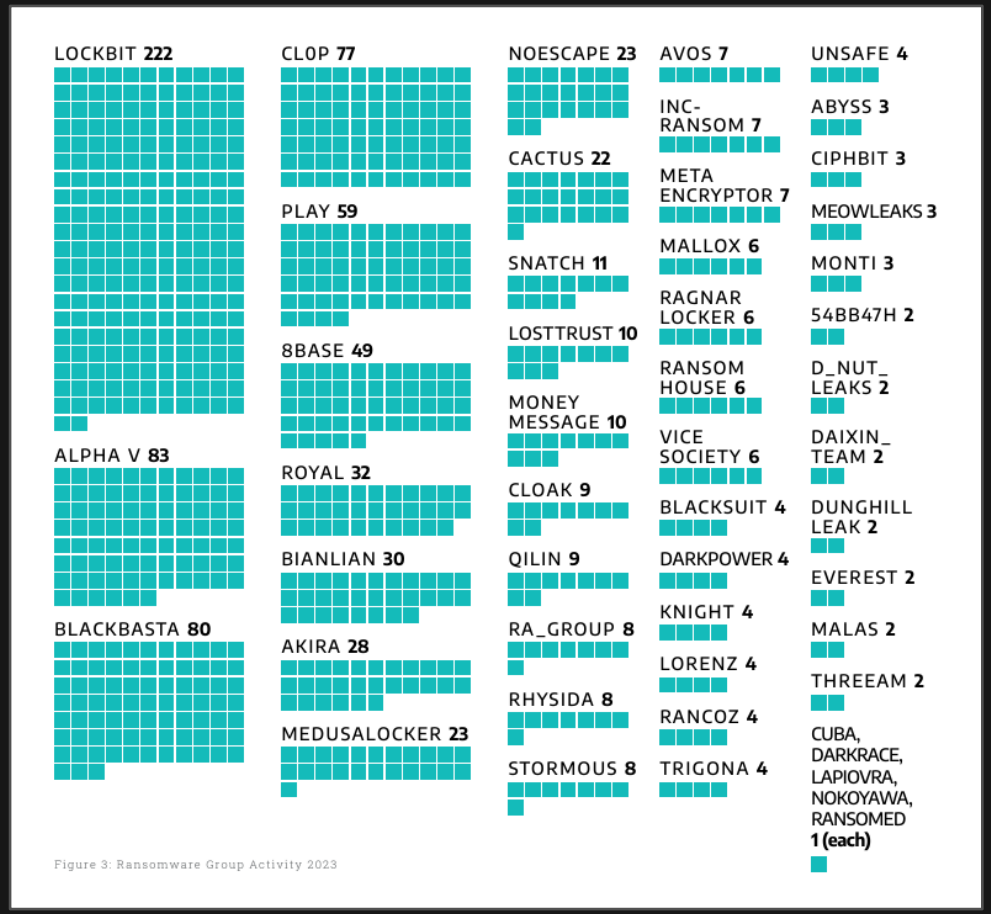
RANSOMWARE SPREADS IN FLAT NETWORKS

28% of customer engagements had findings of segmentation issues or improperly configured firewalls

RANSOMWARE GROUPS — MOVES AND CHANGES

25% OF RANSOMWARE ATTACKS INVOLVE LOCKBIT

ALPHAV + BLACKBASTA ACCOUNT FOR 9% EACH



= 1 RANSOMWARE ATTACK

50 + 28% / 2022
ransomware variants

905 + 49.5% / 2022
ransomware attacks

OT IMPACTS FROM RANSOMWARE ATTACKS

DIRECT

INDIRECT

Preventative/precautionary OT shutdown

Lateral movement and deployment within OT network

ICS process kill list in ransomware (EKANS)

Financial costs of recovery and loss of revenue

Reputational damage

Lateral movement into customer environments

Operational impact for customer base due to loss of availability

Supply chain attack on the customer base

Disclosure of sensitive information via DLS enabling future attacks on customers

IMMEDIATE

LONG-TERM

THREAT GROUPS:
KNOW YOUR ADVERSARIES

VOLTZITE

Heavy use of living off the land (LOTL) techniques. Evades detection with slow, steady reconnaissance.

TARGETS:

Electric Power Generation, Transmission & Distribution, Emergency Services, Telecommunications, Defense Industrial Bases, Satellite Services

INTENT/MOTIVATION:

Espionage & exfiltration, long-term persistent access.

VOLTZITE EXFILTRATION COULD FACILITATE FOLLOW-ON ACTIONS WITH PHYSICAL IMPACTS

KILLCHAIN ANALYSIS

		CAPABILITIES
Delivery	STAGE 01	Exploits internet accessible SOHO routers, uses them as intermediary hops back to ORB
Exploit	STAGE 01	Native Windows command line and PowerShell, Active Directory tools
Install/Modify	STAGE 01	Use of built-in proxy commands, open-source tools, & fast reverse proxy tool (frp
C2	STAGE 01	Initial access by exploiting edge network devices from Cisco, Ivanti, PRTG Network Monitor, Fortinet amongst others
Act	STAGE 01	Stages and exfiltrates sensitive operational data related to OT networks and processes

Overlaps with Volt Typhoon (Microsoft), BRONZE SILHOUETTE (Secureworks), Vanguard Panda (Crowdstrike), UNC3236 (Mandiant)

HUNTING FOR VOLTZITE

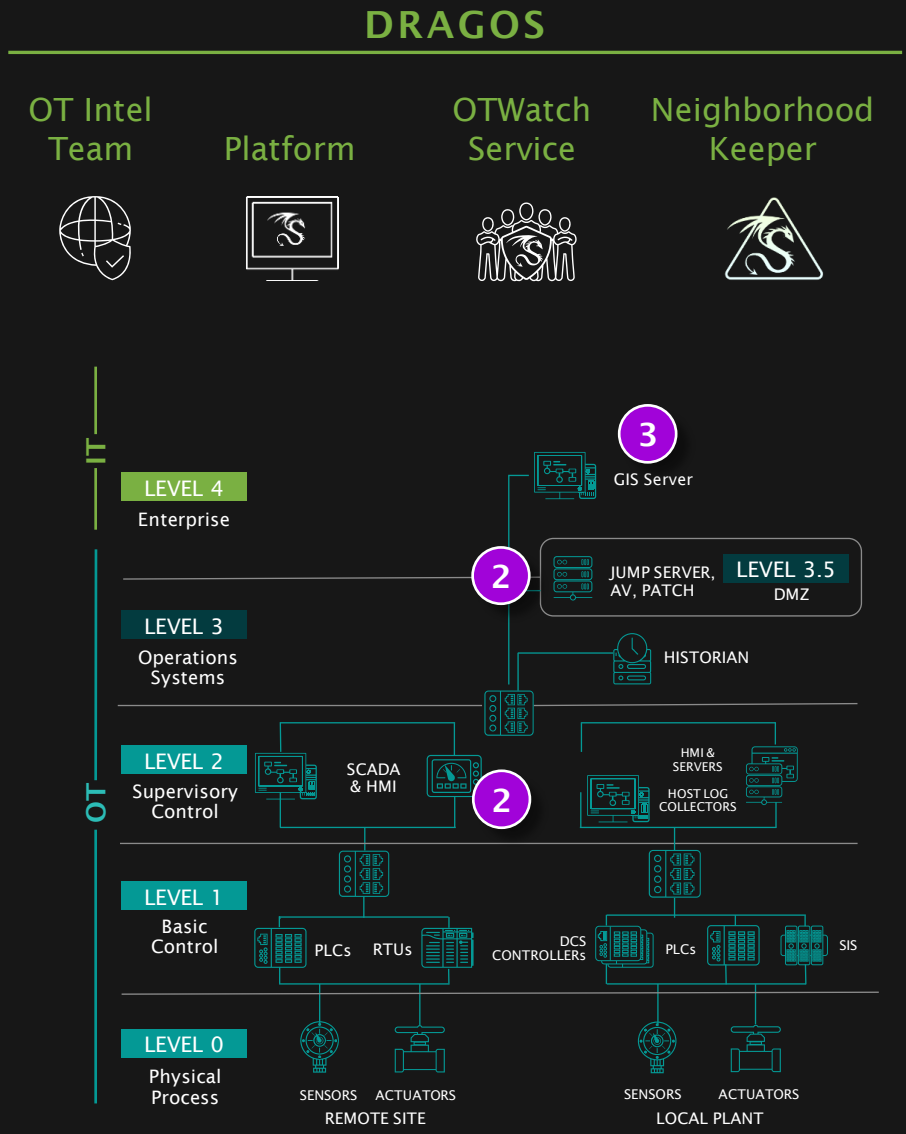
1. Dragos Intelligence VOLTZITE since early 2023 with regular behavioral detections codified in the Dragos Platform

2. New water & electric utility Customer deployed Dragos Platform at Level 3-4 (IT-OT traffic) & Level 2 (OT-OT traffic)

3. OTWatch conducted full hunt; Dragos Platform detected (Server Message Block) SMB traversal maneuvers in IT-OT network traffic

4. OTWatch launches additional hunts across the fleet of subscribed customers; Intel analyzes Platform Neighborhood Keeper participants for indications of VOLTZITE behaviors, anonymously notifies impacted parties

5. Intel works with detection engineering to develop high-fidelity detections for Platform deployed via Knowledge Packs



GANANITE

INITIAL ACCESS, ESPIONAGE, DATA EXFILTRATION

GANANITE
SINCE 2022

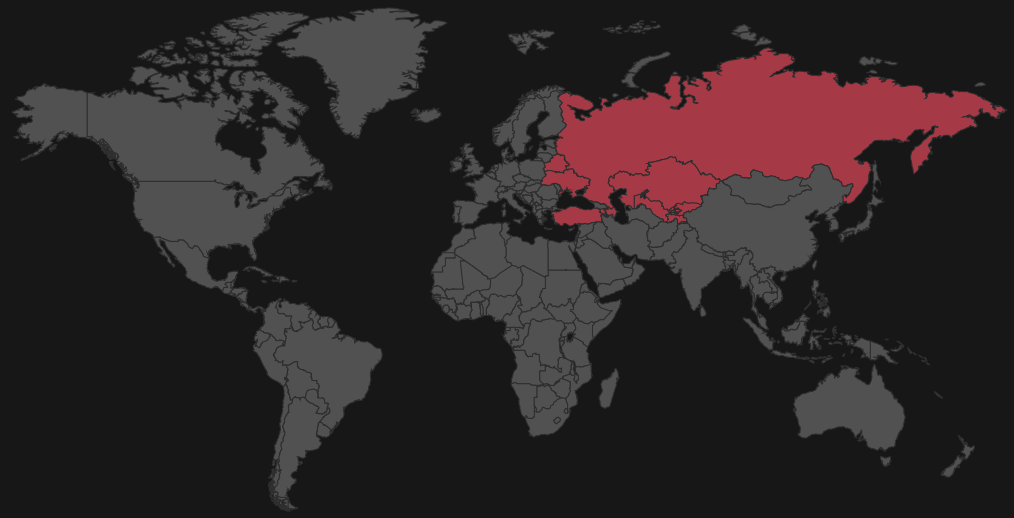
ADVERSARY:
+ Overlap with YORO TROOPER, TOMIRIS, STURGEON PHISHER

CAPABILITIES:
+ Uses multiple remote access trojans (RATs) & public proofs of concept exploits
+ Credential phishing via lookalike domains to obtain credentials

VICTIM:
+ Targets Commonwealth of Independent States & Central Asia
+ Focus on Oil & Gas, Logistics, Transportation, and Government entities

INFRASTRUCTURE:
+ Frequent use of VPNs and anonymizing infrastructure
+ Uses telegram bot for data exfiltration

ICS IMPACT:
+ Loss of convention confidentiality, Theft of operations information
+ Espionage, exfiltration, initial access, data theft



Oil & Gas

Transportation

Logistics, Government

Focused on data exfiltration and establishing initial access.

GANANITE poses a threat to ICS entities with poor network segmentation because initial access to IT environments may present an easy pivot into OT.

GANANITE may hand off access to operators with ICS skillsets.

LAURIONITE

TARGETING CRITICAL MANUFACTURING, INTELLECTUAL PROPERTY

LAURIONITE
SINCE 2023

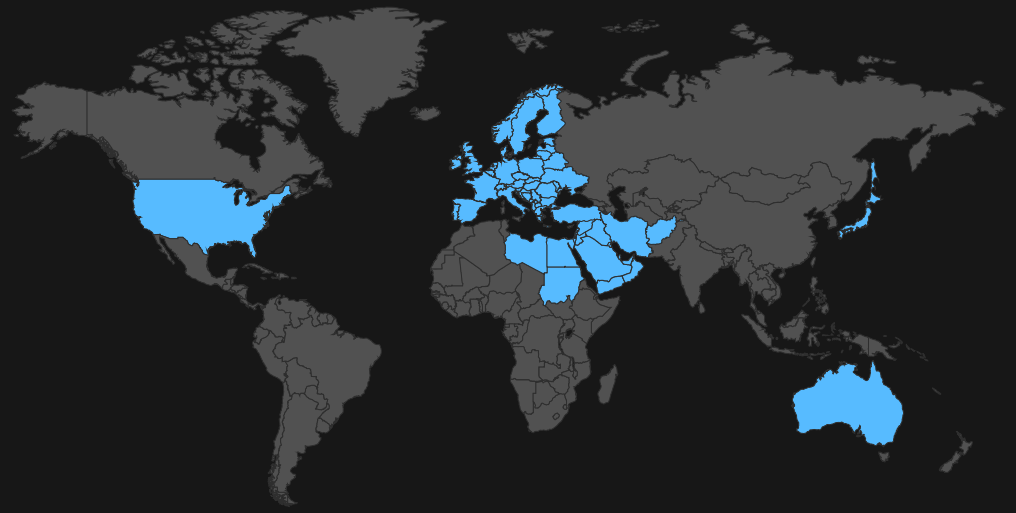
ADVERSARY:
+ No known associations
+ Refined operational trade craft, technical competence

CAPABILITIES:
+ Uses web shells, SlipIt delivery tool, open-source security tools
+ Public proof of concepts for initial access

VICTIM:
+ Internet facing assets with oracle E-Business iSupplier
+ Targets multiple industries and organizations, including aviation, automotive, manufacturing, and government

INFRASTRUCTURE:
+ Create domain masquerades to appear as victims' identities
+ Performs offensive operations against other targets from victim infrastructure

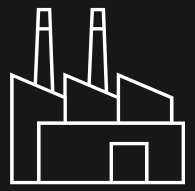
ICS IMPACT:
+ Loss of confidentiality, theft of operational information
+ Espionage and persistent access



Wide-ranging campaign targeting organizations with Oracle E-Business Suite with iSupplier on external assets.

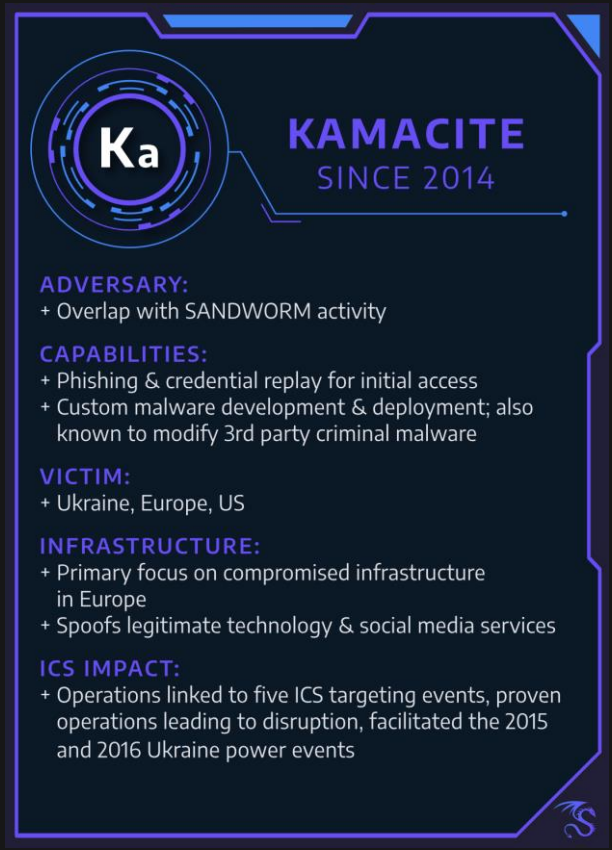
Focused on critical manufacturing, government, and professional services, aviation.

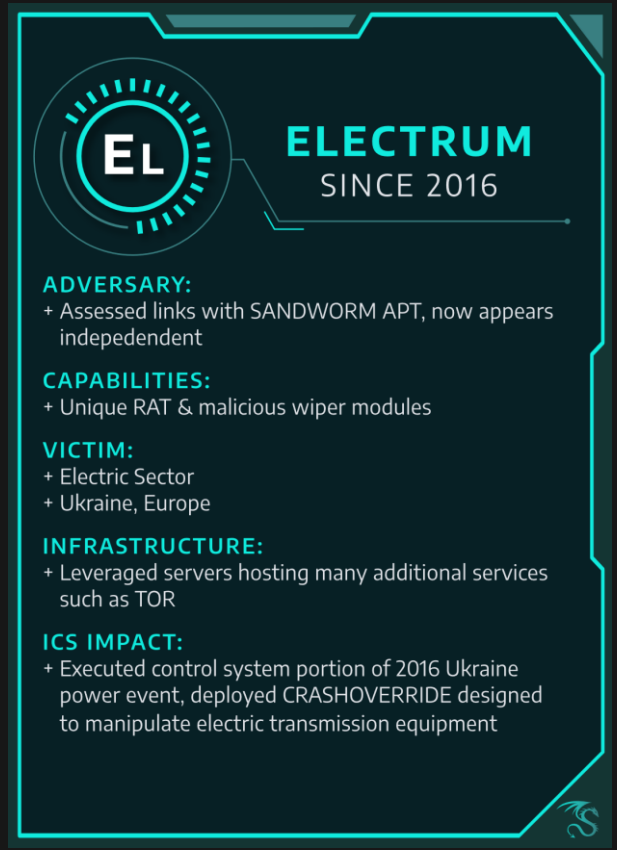
Uses compromised victim infrastructure/identity for operations against other targets.



KAMACITE & ELECTRUM

CONTINUED FOCUS ON UKRAINE… BUT FOR HOW LONG?





KAMACITE

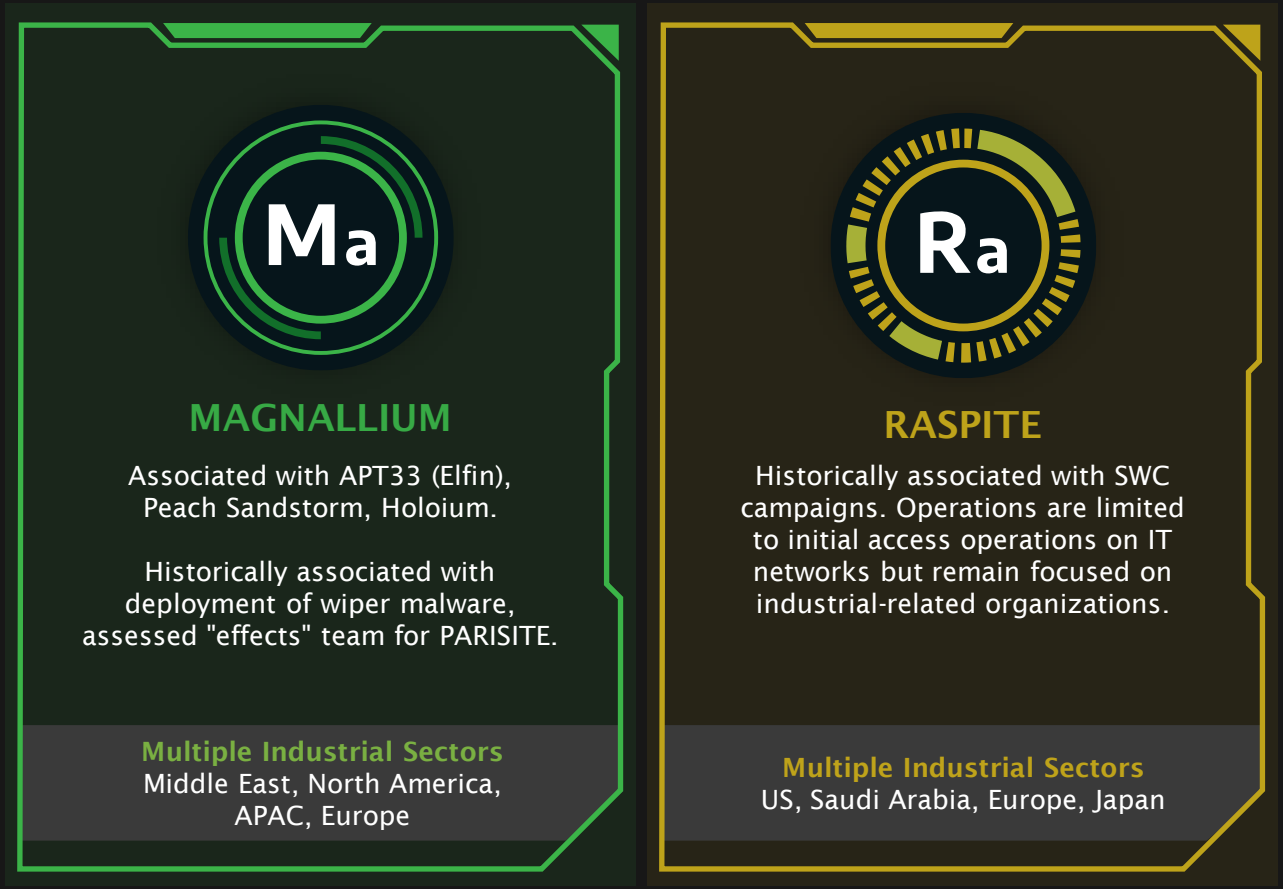
- KAMACITE continues initial access operations focused primarily on Ukrainian entities using commodity or criminal malware (DCRat)
- Increasing focus on telecommunications

ELECTRUM

- Conducted 3rd disruptive attack against electric power operations in Ukraine in Oct 2022
- Used hacktivist persona for operational concealment in impactful destructive attack on Ukrainian telecom Kyivstar in January 2023
- Continuous deployment of wiper malware targeted at Ukrainian organizations

OTHER ACTIVE THREAT GROUPS IN 2023

REMERGENCE AFTER PERIOD OF DORMANCY



RASPITE

- RASPITE observed conducting SMB scanning activity against Electric, Energy, Food and Beverage, Government, Finance, and Education/University sectors globally.
- Continued focus on initial access operations against industrial entities across the U.S, Europe, and the Middle East.

MAGNALLIUM

- MAGNALLIUM observed conducting password spraying campaign in mid 2023.
- Targeted industrial infrastructure and defense organizations, a global mining entity, and a range of ICS and ICS adjacent entities.

RECOMMENDATIONS

SANS

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

ENHANCE YOUR OT THREAT PREPAREDNESS.

Download the Report:
dragos.com/year-in-review