ELECTRUM & KAMACITE

Ten Years of Destruction

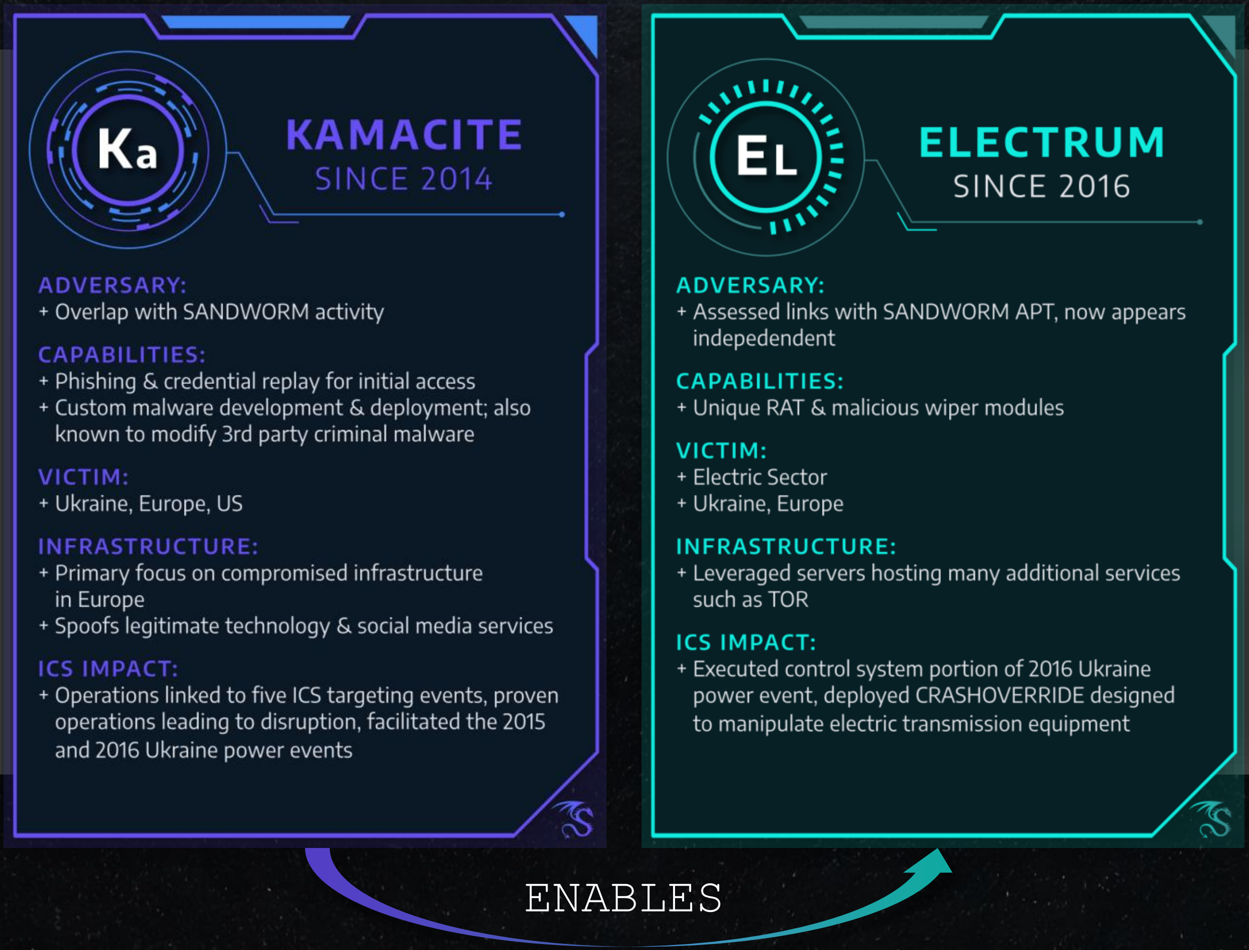
Kyle O'Meara – Director, Adversary Hunting
Bryce Livingston – Principal Adversary Hunter

UPDATE: KAMACITE: & ELECTRUM

A CONTINUED PARTNERSHIP, KAMACITE ENABLES ELECTRUM ICS ATTACKS

KAMACITE

- Initial access provider, focused on IT compromise and post exploitation.
- Uses both bespoke and commodity IT centric malware since 2015.
- Heavy focus on Ukrainian infrastructure since 2022, with activity observed expanding to Europe and US in 2024 and 2025



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

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

- Responsible for destructive or OT specific attacks.
- Conducted first ever known successful attack on electric power operations in 2015
- Demonstrated use of OT-aware malware designed to manipulate ICS.
- Focus on energy grids & communication infrastructure in Ukraine, Poland.

KAMACITE

TARGETING THE ELECTRIC SECTOR IN EUROPE, IN PARTICULAR UKRAINE, SINCE 2015

Ka

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

2015/2016	2017	2018	2019/2020	2022	2024/2025
Enables access for ELECTRUM attacks	Intrusions in German electric sector	Uses VPNFilter malware, affecting over 500,000 devices in ~54 countries	Targeting of U.S. electric with Cyclops Blink	Targeting of infrastructure for initial access to electric substation in Ukraine	Targeting industrial supply chains across Europe that help support Ukraine's infrastructure Scanning exposed industrial devices in U.S.

ELECTRUM

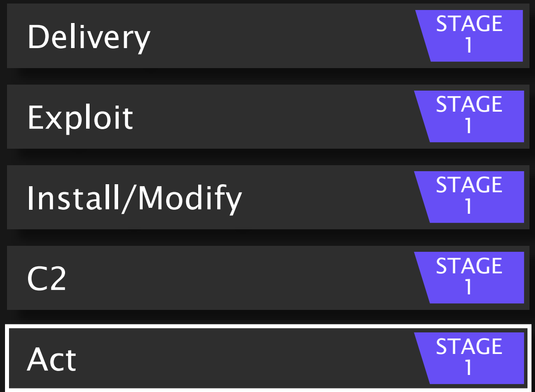
TARGETING THE ELECTRIC SECTOR IN EUROPE, IN PARTICULAR UKRAINE, SINCE 2015

EL

Responsible for multiple disruptive attacks against Ukrainian electric grid since 2015

Consistent focus on critical infrastructure, primarily in Ukraine but also in Europe and US

Demonstrated use of OT-aware malware (Crashoverride, Industroyer2) as well as OT specific LoTL techniques, as well as dozens of wiper malware



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

IN 2015 ELECTRUM SUCCESSFULLY DISRUPTED POWER TO A ¼ MILLION UKRAINIAN CONSUMERS.

IN 2016 ELECTRUM DEPLOYS CRASHOVERRIDE (INDUSTROYER) CAUSING POWER OUTAGE IN KYIV FOR ABOUT 1 HOUR.

2022 ELECTRUM DEPLOYS INDUSTROYER2 IN ATTEMPT TO DISRUPT POWER AT UKRAINIAN SUBSTATION

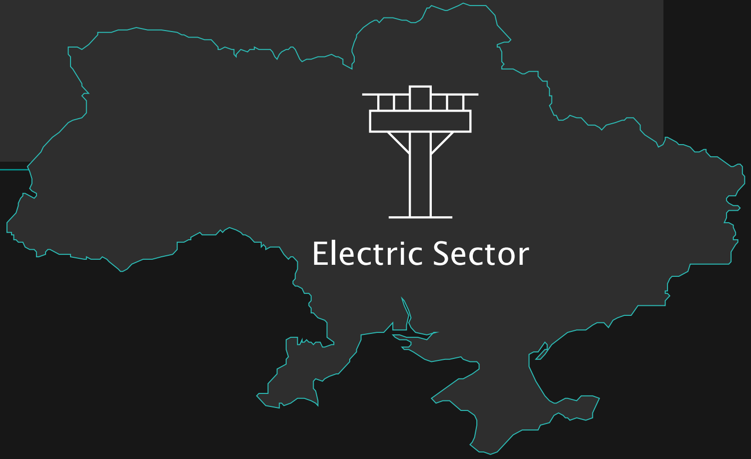
CONFLICT-DRIVEN CYBER ACTIVITY

CYBER

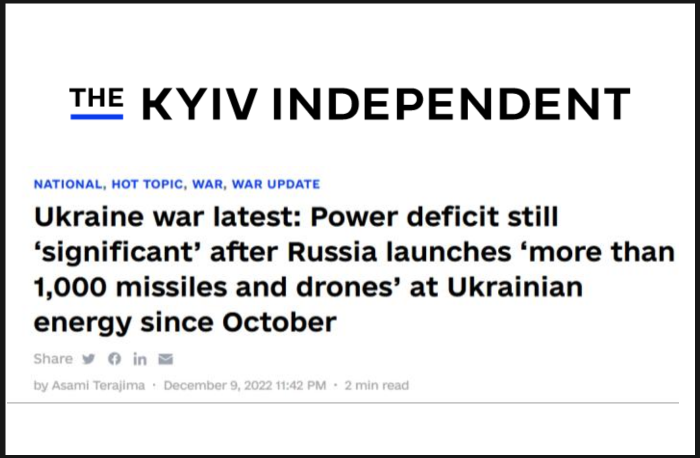
Dedicated, mature threat groups targeting industrial infrastructure networks: ELECTRUM & KAMACITE

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

Targeting Ukraine electric sector



KINETIC



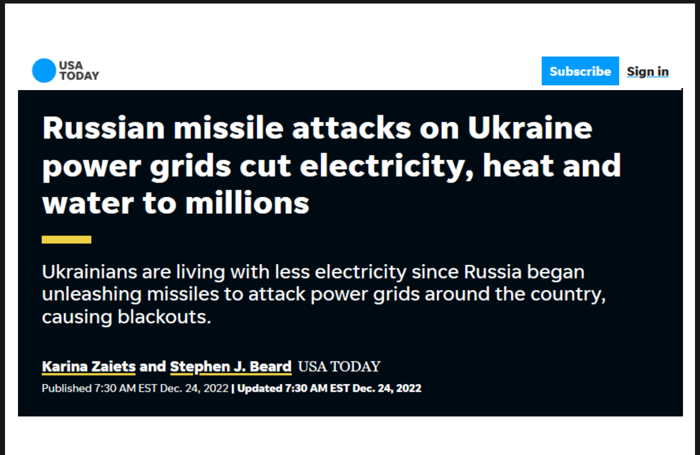
THE KYIV INDEPENDENT

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

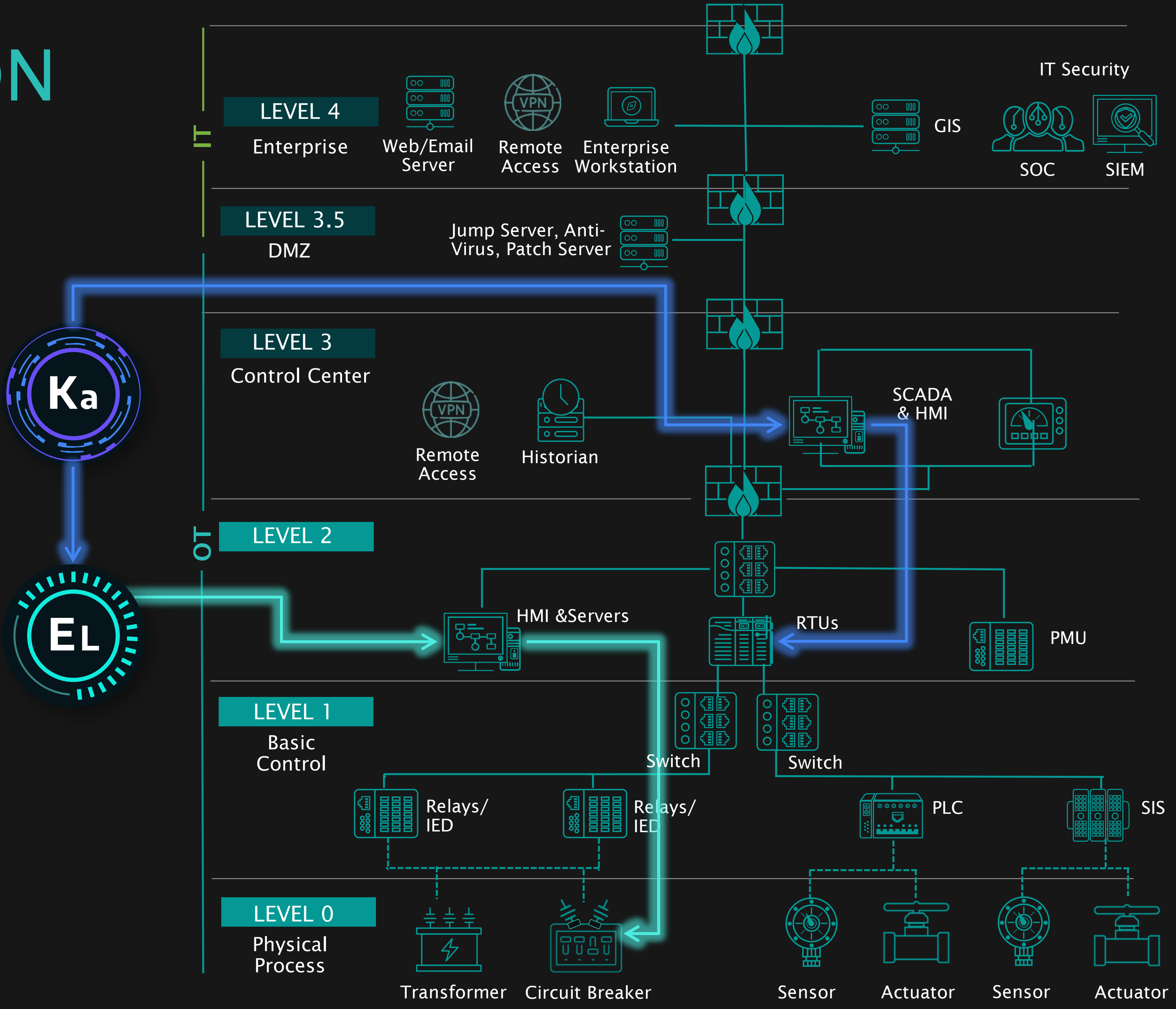
Russian missile attacks on Ukraine power grids cut electricity, heat and water to millions

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

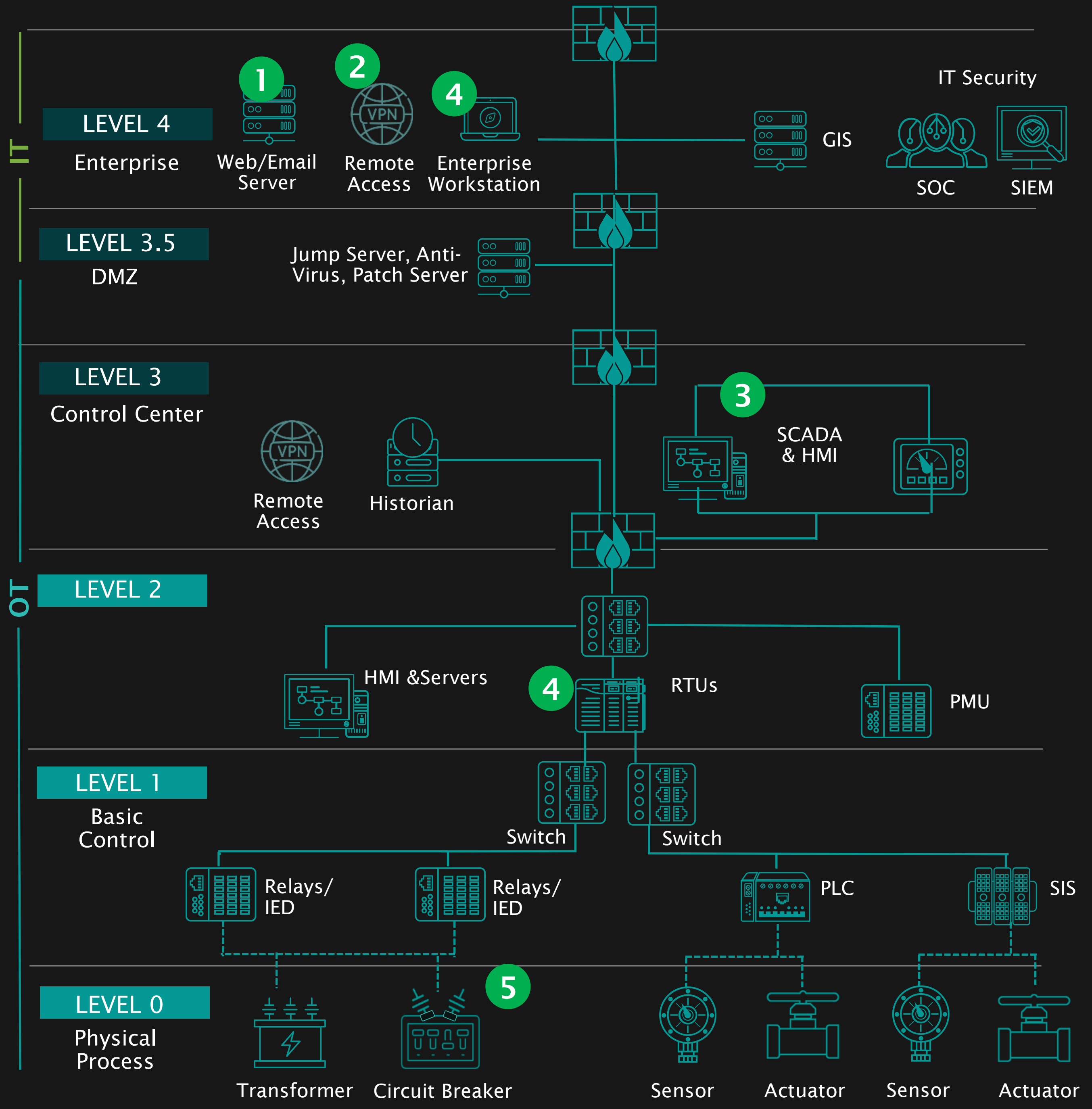
OT INTRUSION LIFECYCLE



2015 ATTACK

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

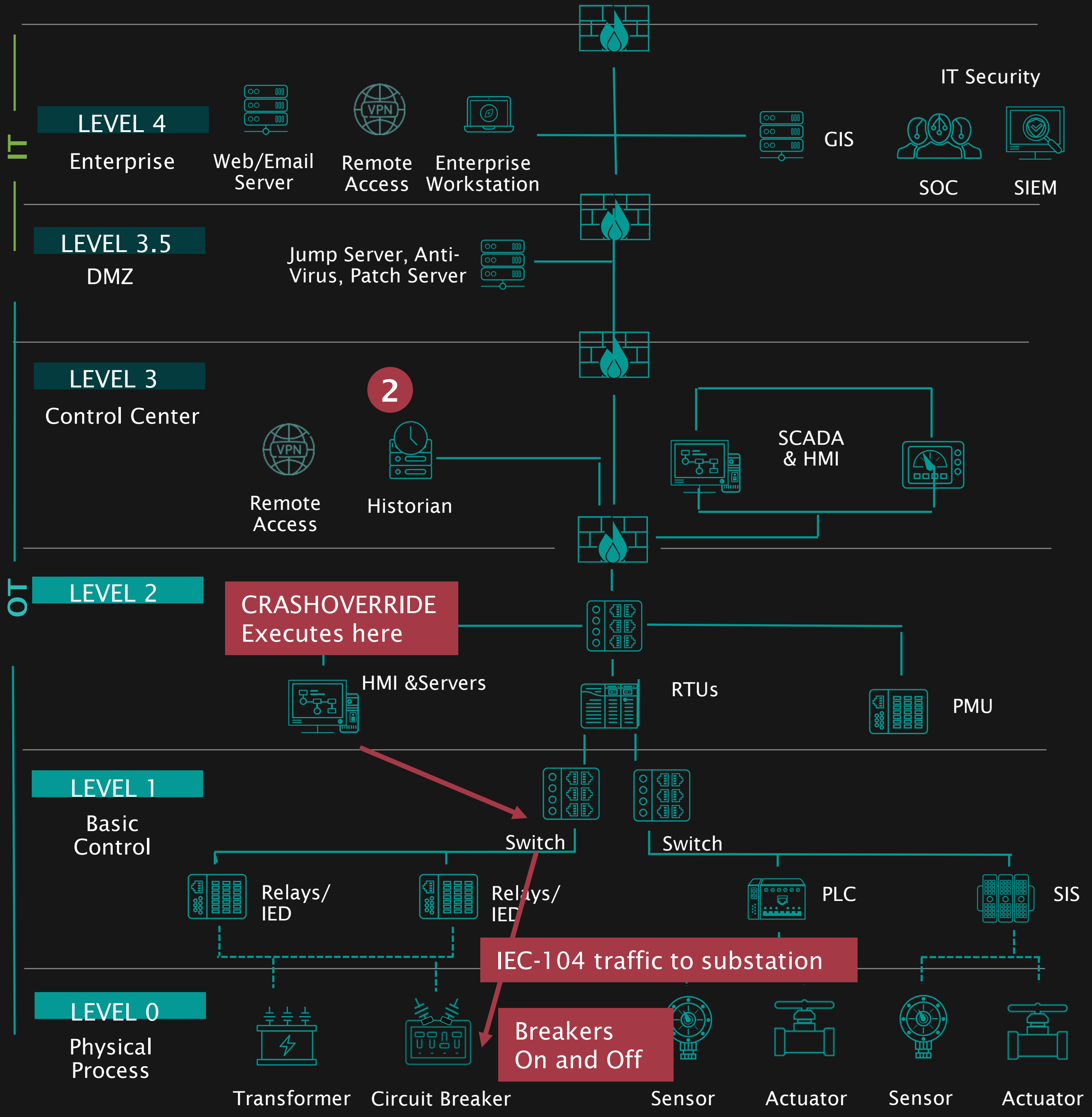
1. Initial access vector was spearphishing.
2. Used compromised, legitimate credentials to access the environment via VPN.
3. Remote access to HMI.
4. Used Killdisk to disable ICS (HMI embedded in RTUs) and corporate network systems.**
5. Remotely operated breakers to disconnect power.



**Abbreviated destructions TTPs

2016 ATTACK (CRASHOVERRIDE)

1. Accessed duel-homed host between IT and ICS network.
2. Capture credentials from 4 databased servers serving as data historians.
3. Leveraged database access to the SQL Server machines to execute commands via XP_cmdshell, which allows a privileged database user to pawn a command shell on the host
4. Used backdoored Windows Notepad to access compromised systems
5. Impacted ABB-controlled switchgear and circuit breakers



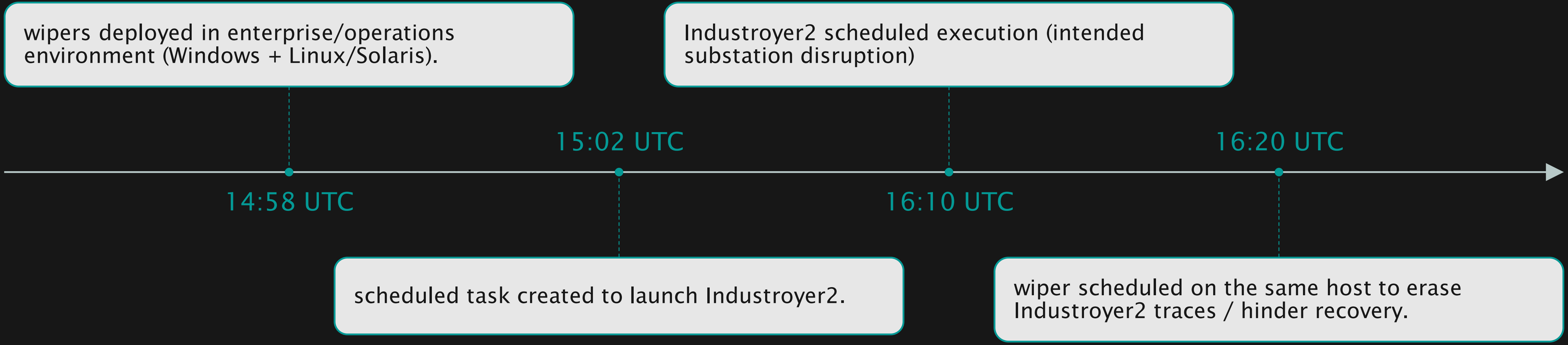
CRASHOVERRIDE Executes here

IEC-104 traffic to substation

Breakers On and Off

April 2022 - INDUSTROYER2

CRASHOVERRIDE	INDUSTROYER2
Modular, multi-protocol payloads	IEC-104 only
Config via separate INI	Config hardcoded (recompile per victim)
Outage achieved (limited duration)	Attempted; impact limited (mitigated)
Malware + ops	Ops choreography (timed tasks + wipers)



14:58 UTC — wipers deployed in enterprise/operations environment (Windows + Linux/Solaris).

15:02 UTC — scheduled task created to launch Industroyer2.

16:10 UTC — Industroyer2 scheduled execution (intended substation disruption)

16:20 UTC — wiper scheduled on the same host to erase Industroyer2 traces / hinder recovery.

October 2022 MICROSCADA COMPROMISE

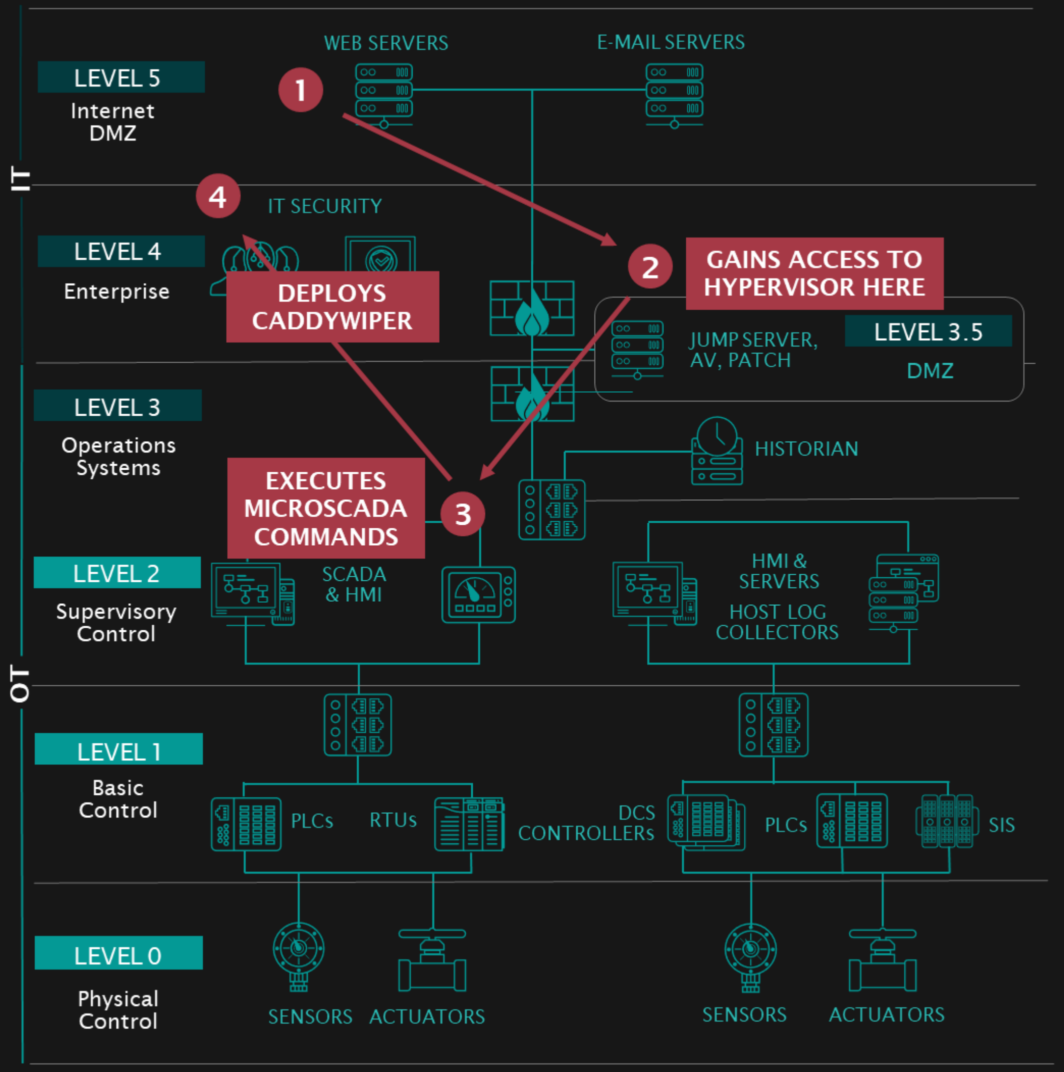
MICROSCADA IS DEPLOYED IN MORE THAN 10,000 SUBSTATIONS AND MONITORS ELECTRIC SUPPLY FOR MORE THAN 10% OF THE WORLD'S POPULATION.

1 **JUNE 2022 -** ELECTRUM deployed a web shell to persistently access the electric substation's internet-facing web servers. Initial compromise vector is unknown.

2 **JULY 2022 –** ELECTRUM deployed a custom TCP tunneling tool, and the Systemd service unit was utilized to maintain persistence.

3 **OCTOBER 10, 2022 – S**tayed dormant before using a set of custom tools to execute MicroSCADA commands on the OT network.

4 **OCTOBER 12, 2022 -** ELECTRUM deployed a new version of **CaddyWiper** using group policy objects (GPO) and scheduled tasks only in the IT environment.



COMPROMISED VERSION OF MICROSCADA CONSIDERED EOL & NO LONGER SUPPORTED.

WHAT HAVE WE LEARNED

- ✓ Access Matters More than Tooling
- ✓ ELECTRUM adapts to the environment, not vice versa
- ✓ OT disruption does not require exotic malware
- ✓ End-of-life systems increase risk
- ✓ Disruption is an outcome, not a phase

PARALLEL CAMPAIGNS BEYOND OT

Destructive IT Operations

Sustained use of wiper malware since 2022
At least 14 distinct IT-focused wiper familes

Targets extend beyond utilities
ISPs, telecom, media, government, satellite infrastructure

Spillover into OT-adjacent environments
Acidrain (Viasat) and AcidPour capable of impacting embedded and OT-adjacent devices

IT disruption is not collateral: it is an intentional parallel effort

Personas & Obfuscation

Repeated use of hacktivist personas
Solntsepek, KillNet, CyberArmyofRussia_Reborn

Used to obfuscate attribution
Enables plausible deniability and narrative control

Often paired with destructive operations
Telecom, ISPs, media, and national infrastructure

Attribution confusion is a feature, not a side effect

KAMACITE 2024/2025

WHY THIS MATTERS BEYOND UKRAINE

- **Late 2024 - early 2025: KAMACITE conducted a sustained campaign targeting industrial supply chains across Europe**
  - Energy, water, heat, and industrial automation vendors
- **Targeting extended beyond Ukraine**
  - European industrial suppliers and trusted third parties
  - Organizations with downstream reach into critical infrastructure
- **Focused on access, not immediate disruption**
  - Spear phishing, reconnaissance, and persistence
  - Multi-day, native-language social engineering with technical staff
- **Intent: enable downstream ICS/OT compromise**
  - Vendors and integrators supporting hundreds of operational sites
  - Creates cascading risk across regions and sectors

KAMACITE U.S. Reconnaissance Campaign

From March 2025 to July 2025, Dragos observed consistent scanning from KAMACITE-controlled infrastructure to exposed industrial devices in the US

Smart HMIs

SE Altivar Process ATV600

Accuenergy AXM

SW Airlink Gateways

STRATEGIC ASSESSMENT

ELECTRUM and KAMACITE represent a durable operational model, persistent for at least a decade, not a single campaign	Initial access and effects are functionally separated, but tightly coordinated
Disruptive cyber operations against critical infrastructure are now normalized	Feasibility was established in 2015; subsequent operations refined tradecraft, timing, and scale
Future activity will be shaped by geopolitical conditions, not technical constraints	Capability exists independent of conflict phase or geography
Industrial supply chains and exposed OT assets are increasingly part of the attack surface	Access does not require direct targeting of asset owners
Geography is not a reliable risk boundary	Recent activity demonstrates preparation beyond Ukraine and Europe