The ABCs of ICS Threat Activity Groups

August 26, 2020

Sergio Caltagirone
VP Threat Intelligence
Dragos

Dave Bittner
Producer & Host
The CyberWire Podcast

Before we get started…

- The webinar is being recorded
- The recording will be sent out in a few days
- Please submit questions using the Q&A feature
- All attendee phones are muted
- Let’s meet our speakers!

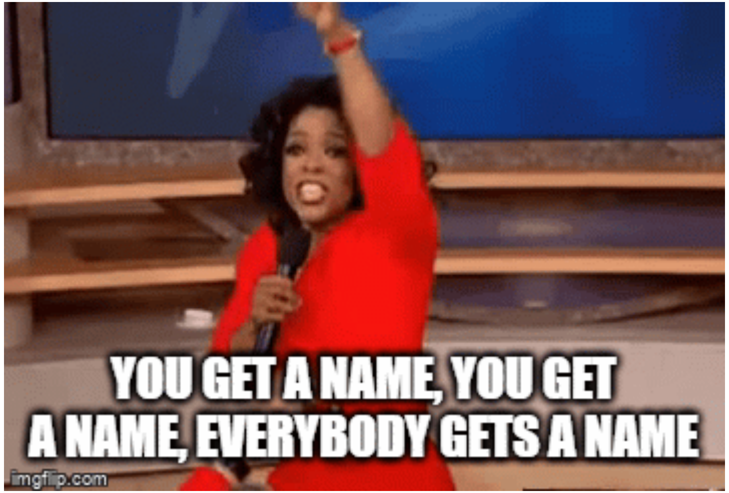
Meet our Speakers

Sergio Caltagirone
VP Threat Intelligence
Dragos

Dave Bittner
Producer & Host
The CyberWire Podcast

Threat Group Names are Everywhere

Xt



EL

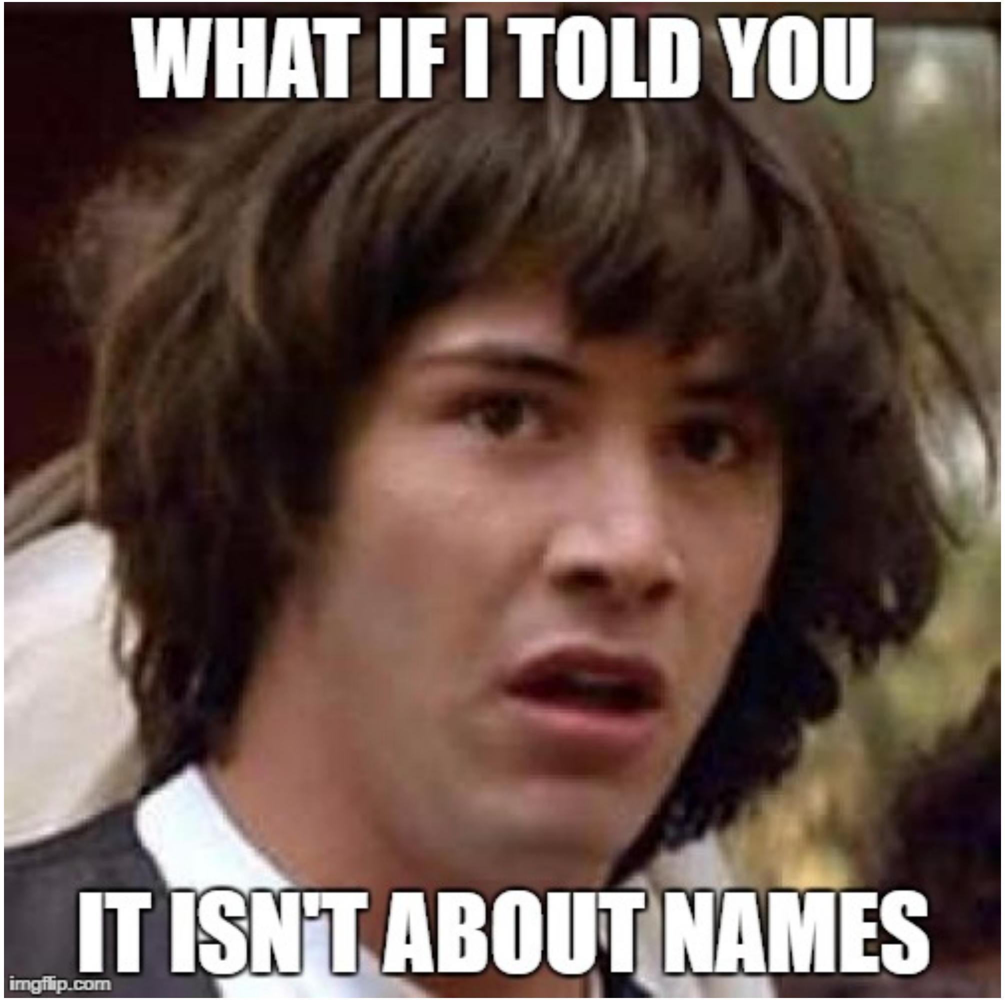
APT34

Dy

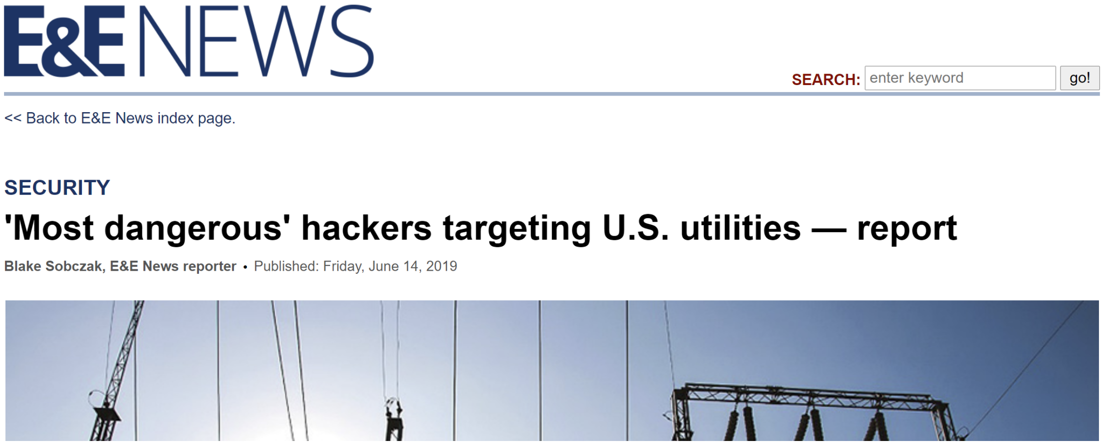
Ma

TRASH PANDAS

APT29


WHAT IF I TOLD YOU
IT ISN'T ABOUT NAMES
imgflip.com

What does this mean?



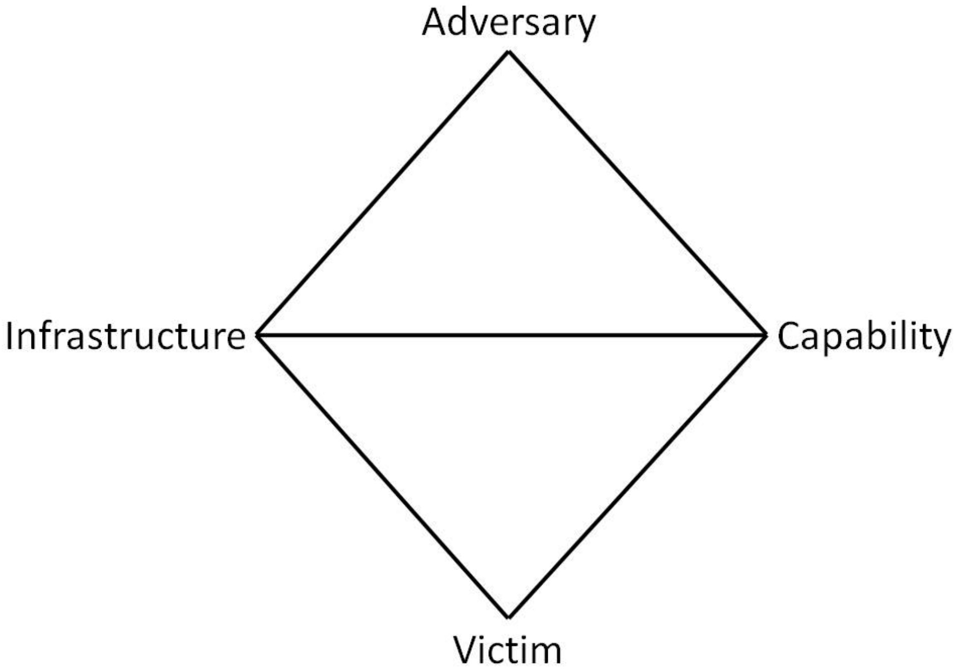
<< Back to E&E News index page.

SECURITY

'Most dangerous' hackers targeting U.S. utilities — report

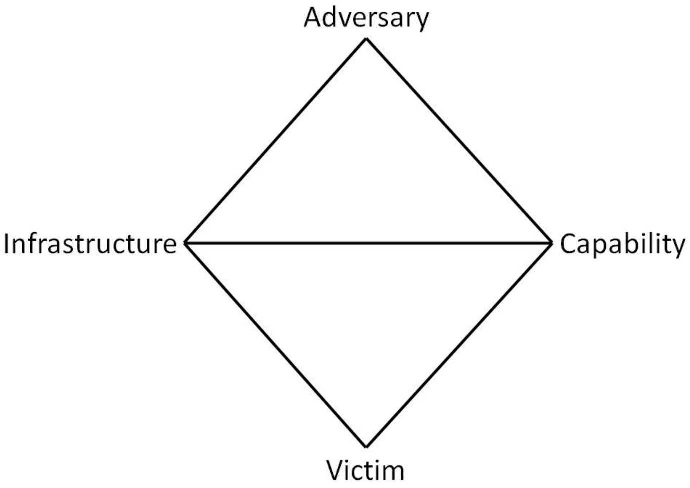
Blake Sobczak, E&E News reporter • Published: Friday, June 14, 2019

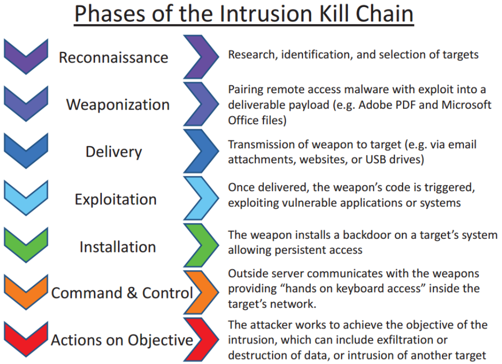
Diamond Model of Intrusion Analysis



Source: diamondmodel.org

Diamond, Kill Chain, ATT&CK



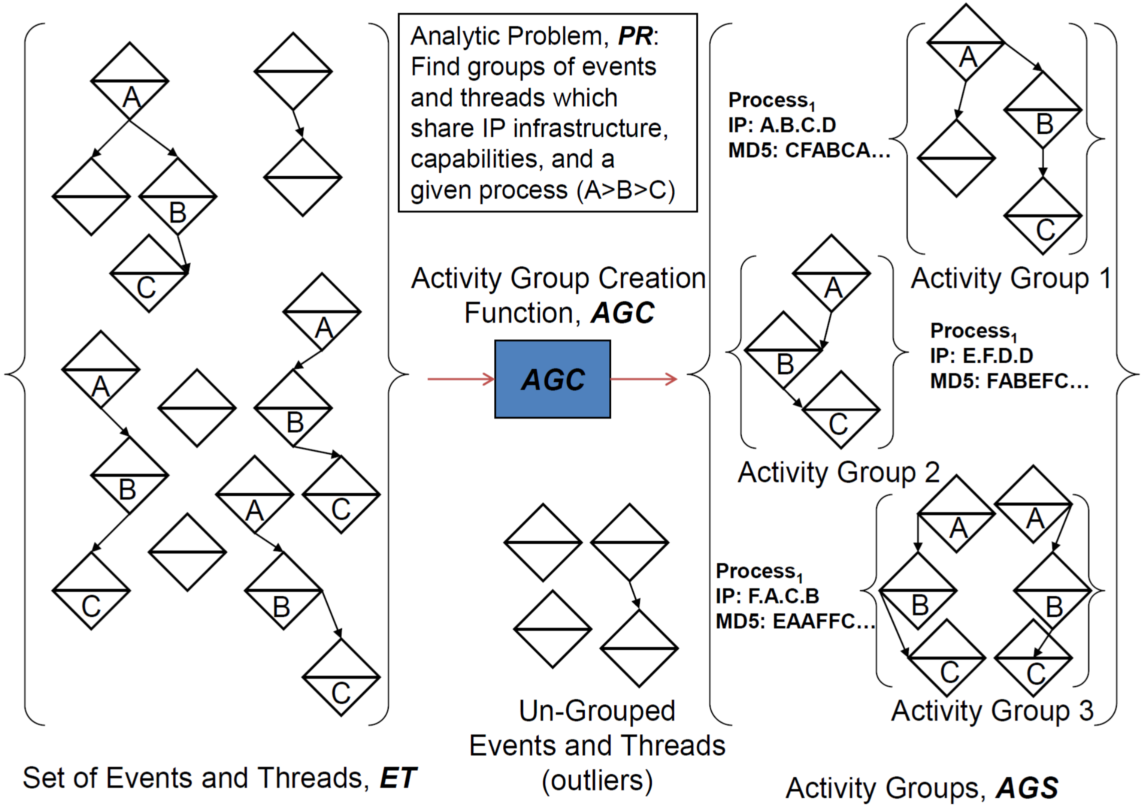


Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command And Control

Activity Groups



Analytic Problem, ***PR***: Find groups of events and threads which share IP infrastructure, capabilities, and a given process (A>B>C)

Activity Group Creation Function, ***AGC***

AGC

Process$_1$
IP: A.B.C.D
MD5: CFABCA…

Activity Group 1

Process$_1$
IP: E.F.D.D
MD5: FABEFC…

Activity Group 2

Process$_1$
IP: F.A.C.B
MD5: EAAFFC…

Activity Group 3

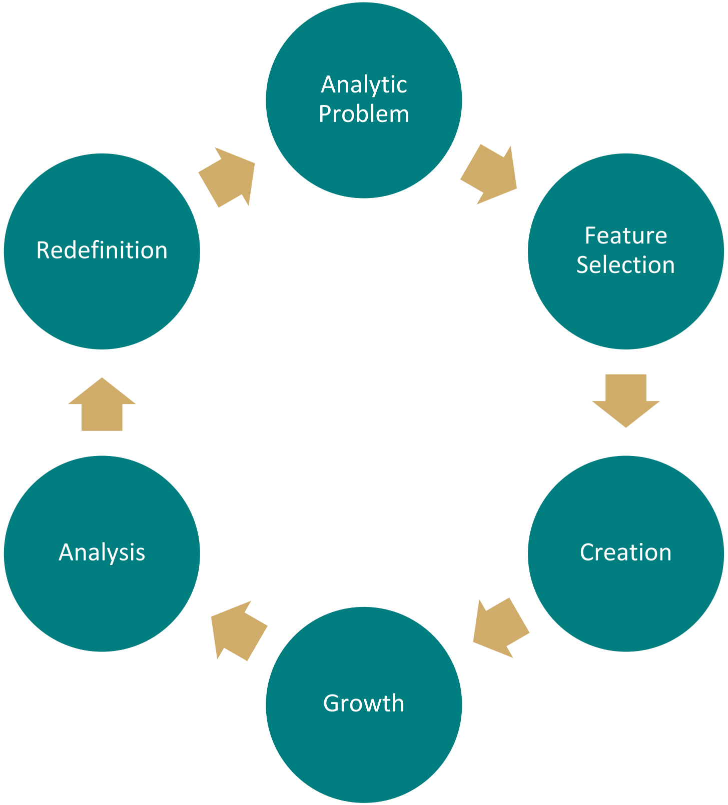
Set of Events and Threads, ***ET***

Un-Grouped Events and Threads (outliers)

Activity Groups, ***AGS***

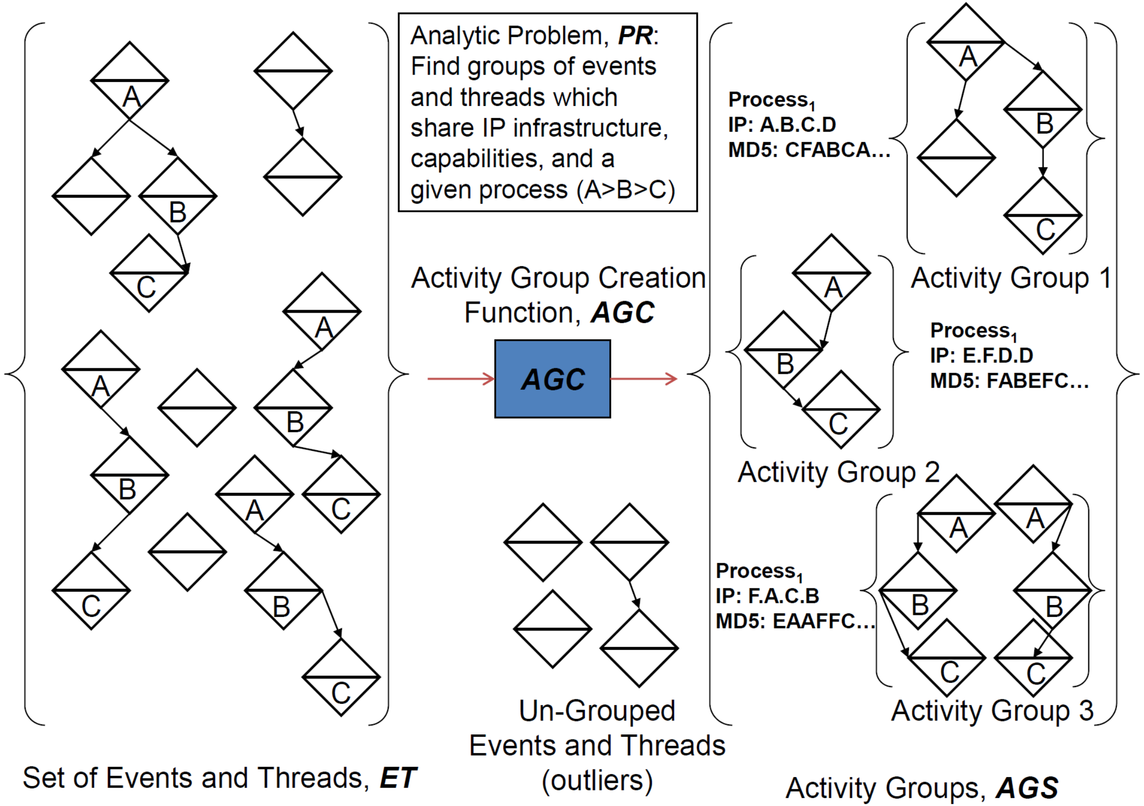
Source: diamondmodel.org

Activity Group Lifecycle



Source: diamondmodel.org

Activity Groups



Analytic Problem, ***PR***: Find groups of events and threads which share IP infrastructure, capabilities, and a given process (A>B>C)

Source: diamondmodel.org

Behavior, Behavior, Behavior

Detection

Detect classes of threats

Detect behaviors, not things

Have 100s of detections, not millions

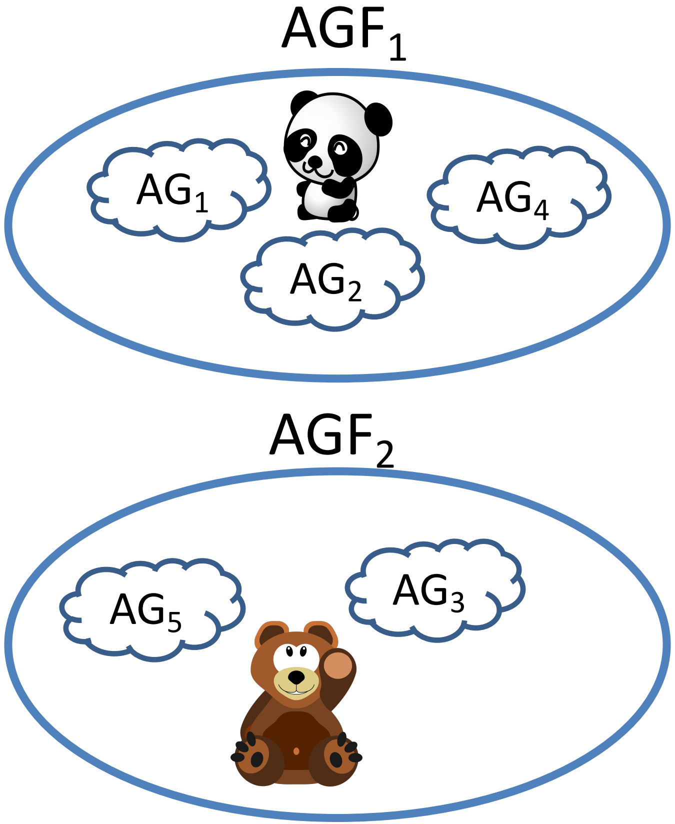
Mitigation

Mitigate whole classes of threats

Define and control the physics

Mitigate Strategically not Tactically

Activity Group Families



Source: diamondmodel.org

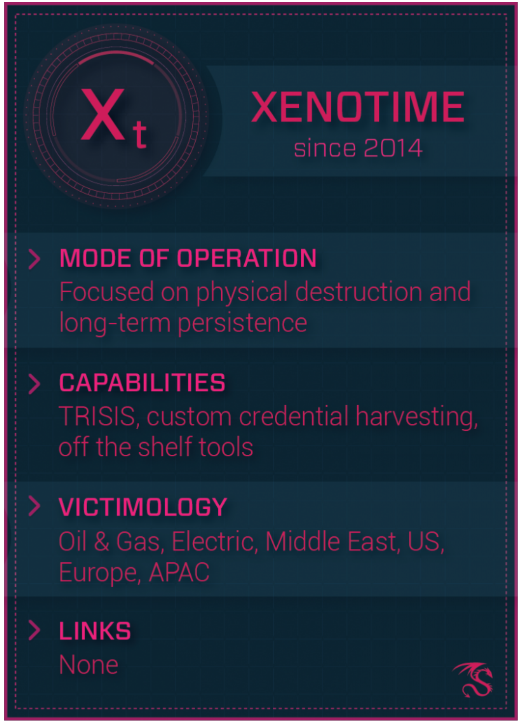
Attribution

Activity Groups are not equivalent to attribution

ICS threat environments are too complex for a simple attribution model

Soft Attribution is not Hard Attribution

Some Dragos Activity Groups



XENOTIME

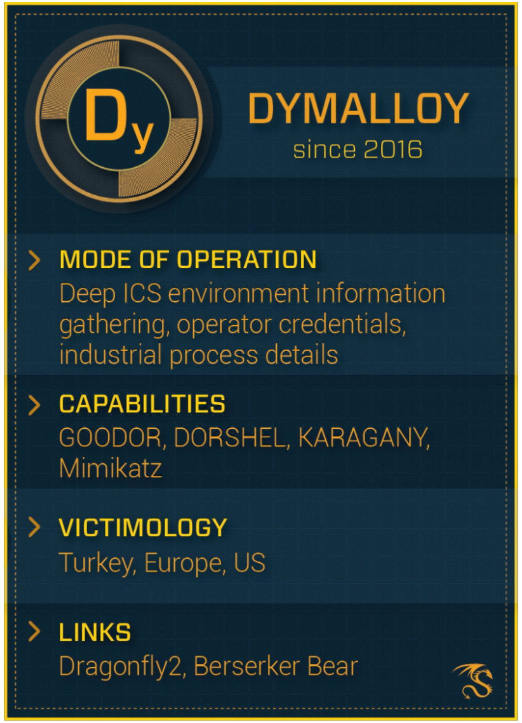
since 2014

MODE OF OPERATION
Focused on physical destruction and long-term persistence

CAPABILITIES
TRISIS, custom credential harvesting, off the shelf tools

VICTIMOLOGY
Oil & Gas, Electric, Middle East, US, Europe, APAC

LINKS
None



DYMALLOY

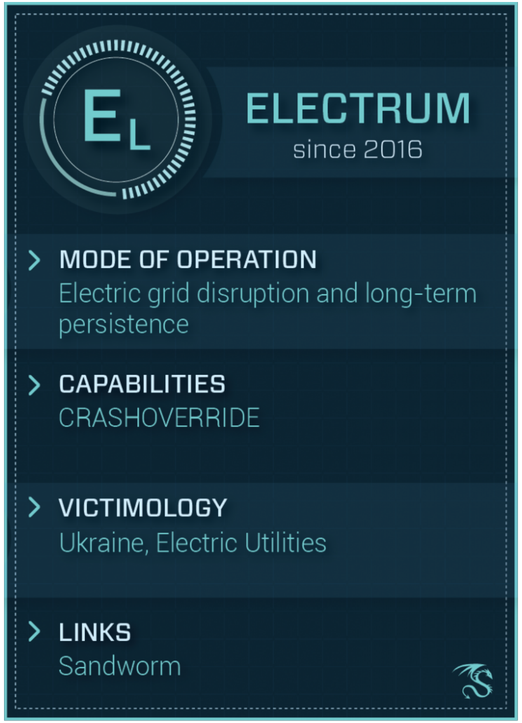
since 2016

MODE OF OPERATION
Deep ICS environment information gathering, operator credentials, industrial process details

CAPABILITIES
GOODOR, DORSHEL, KARAGANY, Mimikatz

VICTIMOLOGY
Turkey, Europe, US

LINKS
Dragonfly2, Berserker Bear



ELECTRUM

since 2016

MODE OF OPERATION
Electric grid disruption and long-term persistence

CAPABILITIES
CRASHOVERRIDE

VICTIMOLOGY
Ukraine, Electric Utilities

LINKS
Sandworm

https://www.dragos.com/threat-activity-groups/

Q&A

DRAGOS

the cyberwire

Sergio Caltagirone
VP Threat Intelligence
Dragos

Dave Bittner
Producer & Host
The CyberWire Podcast

Thank You!

Sergio Caltagirone
VP Threat Intelligence
Dragos

Dave Bittner
Producer & Host
The CyberWire Podcast