RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: SBX4-R1

How Long to Boom?
Understanding and Measuring ICS Threat Maturity

Sergio Caltagirone

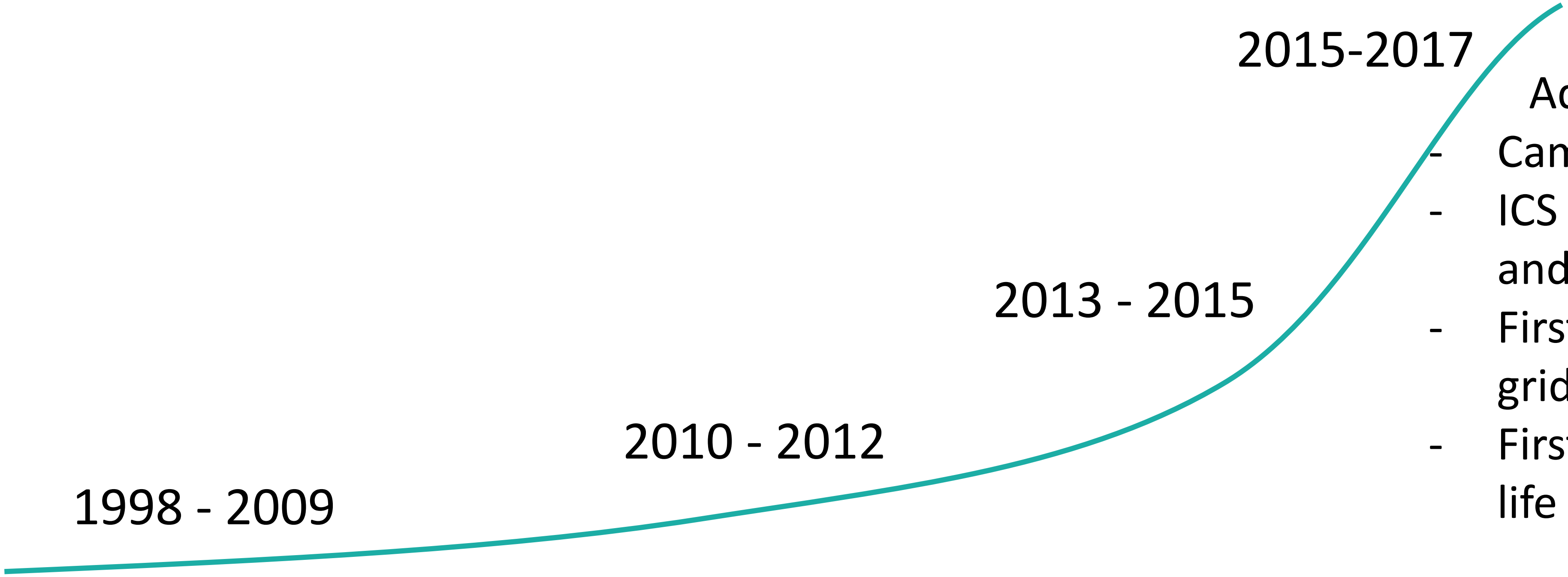
Dragos
sergio@dragos.com
@cnoanalysis

Why Measure ICS Threat Maturity?

Approximate the maturity of ICS threats compared to the "worst" case

- Limited defender resources
- "Bad" vs "Boom"
- Threat behavior proliferation
- Forecast large-scale infrastructure cybersecurity risk

Growth in ICS Threats and Maturity



1998 - 2009

Lack of Collection

- Campaigns: APT1
- ICS Malware: None

2010 - 2012

New Interest in ICS

- Campaigns: Sandworm
- ICS Malware: Stuxnet

2013 - 2015

Campaigns Target ICS

- Campaigns: Dragonfly
- ICS Malware: BlackEnergy 2 and Havex
- First attack to cause physical destruction on civilian infrastructure (German Steel)

2015-2017

Adversaries Disrupt ICS

- Campaigns: 10 Unique
- ICS Malware: CRASHOVERRIDE and TRISIS
- First and second ever electric grid attacks that disrupt power
- First malware to target human life

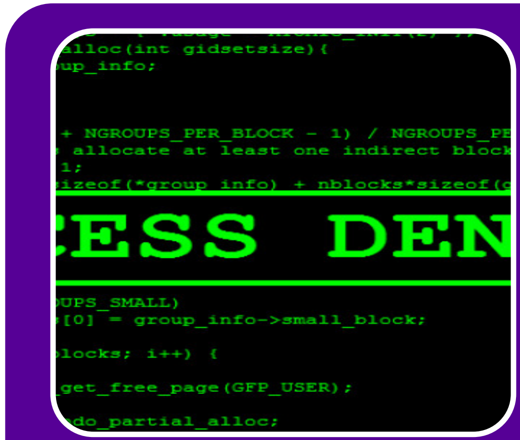
Features to Measure

- Intent?
- Sophistication?
- Scale?
- Sector affected?
- Conduct?
- Demonstrated vs Theorized?

Features Chosen

- Observed
- Conduct/ICS Kill Chain Phase
- Scale

Access vs Effects Operations



```
alloc(int gidsetsize){
up_info;


 + NGROUPS_PER_BLOCK - 1) / NGROUPS_PE
 allocate at least one indirect block
 1;
izeof(*group_info) + nblocks*sizeof(g
CESS  DEN
OUPS_SMALL)
[0] = group_info->small_block;

locks; i++) {

get_free_page(GFP_USER);

do_partial_alloc;
```

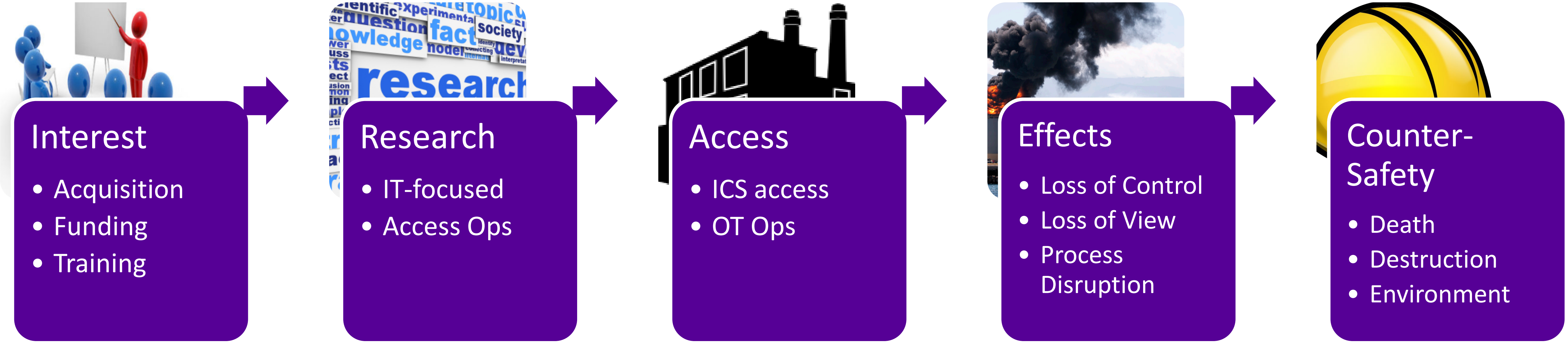
Access

- Reconnaissance, Research, Exfiltration
- IT/OT, Intellectual Property, Pre-position

Effects

- Loss, Deny, Degrade, Disrupt, Destroy
- Control, View, Safety

ICS Threat Conduct “Path”



Interest

- Acquisition
- Funding
- Training

Research

- IT-focused
- Access Ops

Access

- ICS access
- OT Ops

Effects

- Loss of Control
- Loss of View
- Process Disruption

Counter-Safety

- Death
- Destruction
- Environment

*Approximately follows the ICS Kill Chain path

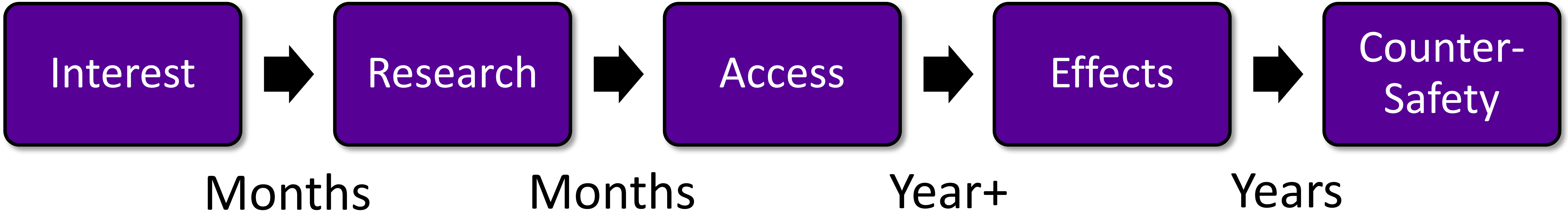
Conduct Scale

Interest	**0**	No information available
	1	Interest in offensive ICS cyber operations
	1.5	Research, Development, or Acquisition of Talent, ICS Equipment, and Resources
Research	**2**	Targeting ICS-related people and information including compromising enterprise IT networks
	2.5	External OT network probing
Access	**3**	Intentional illicit access to OT networks
	3.5	Internal OT network reconnaissance
	4	Access to OT business assets
	4.5	Access to OT process control or view assets
Effects	**5**	Manual effects leading to loss or denial of view or control w/possible process disruption
	5.5	Automated effects leading to loss or denial of view or control w/possible process disruption
Counter-Safety	**6**	Impacting confidence in physical or digital safety controls

Scale of Operations

Single Process	1
Cross-Process / Single-Plant	2
Cross-Sites / Cross-Plants	3
Regional / Larger	4

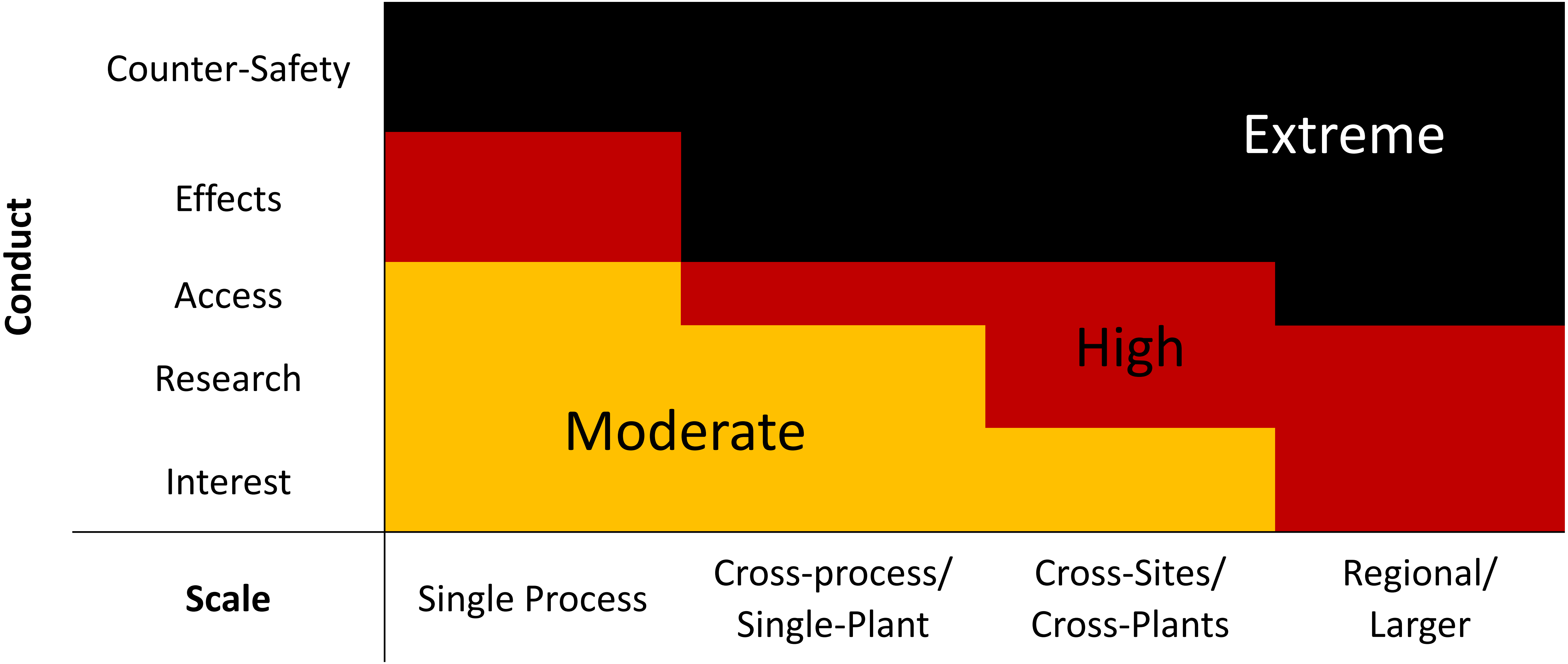
Time to Maturity



Complications

- Foreign Technical Assistance (FTA) or other coordination
- Sector-specific knowledge & capabilities
- Behavioral and technical proliferation

ICS Threat Maturity Matrix



Conduct

Counter-Safety

Effects

Access

Research

Interest

Scale

Single Process

Cross-process/ Single-Plant

Cross-Sites/ Cross-Plants

Regional/ Larger

Moderate

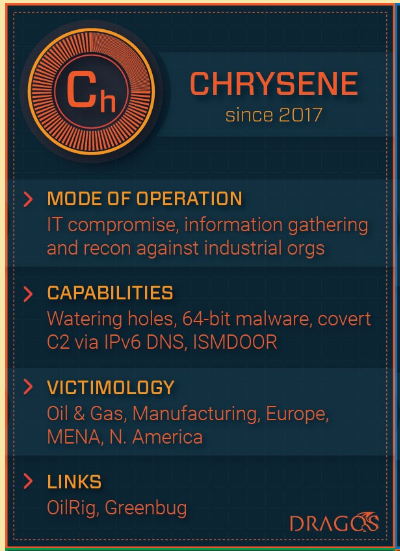
High

Extreme

Why Does This Matter? What Can We Do With This?

- Project activity maturation timelines
- Align defensive priorities to the threat environment
- Separate “bad” from “boom”
- Define the global ICS risk environment
- Measure changes in proliferation

MODERATE



CHRYSENE
since 2017

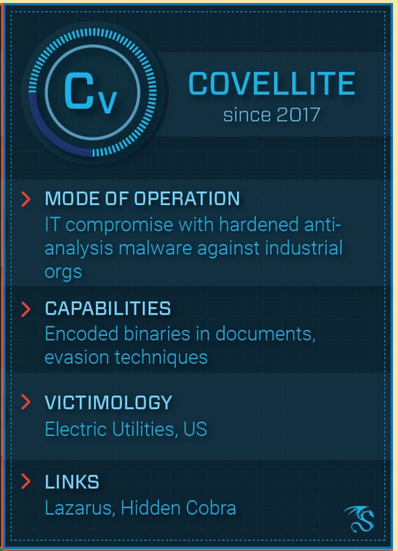
MODE OF OPERATION
IT compromise, information gathering and recon against industrial orgs

CAPABILITIES
Watering holes, 64-bit malware, covert C2 via IPv6 DNS, ISMDOOR

VICTIMOLOGY
Oil & Gas, Manufacturing, Europe, MENA, N. America

LINKS
OilRig, Greenbug

DRAGOS



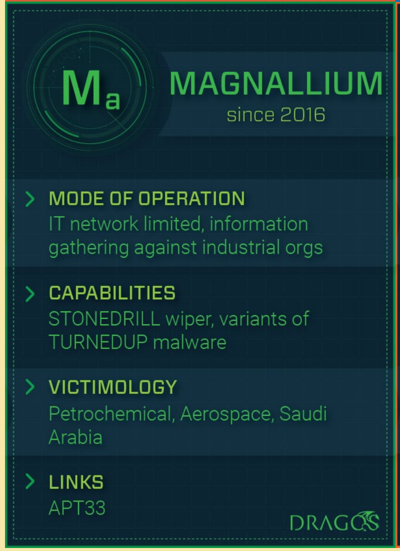
COVELLITE
since 2017

MODE OF OPERATION
IT compromise with hardened anti-analysis malware against industrial orgs

CAPABILITIES
Encoded binaries in documents, evasion techniques

VICTIMOLOGY
Electric Utilities, US

LINKS
Lazarus, Hidden Cobra



MAGNALLIUM
since 2016

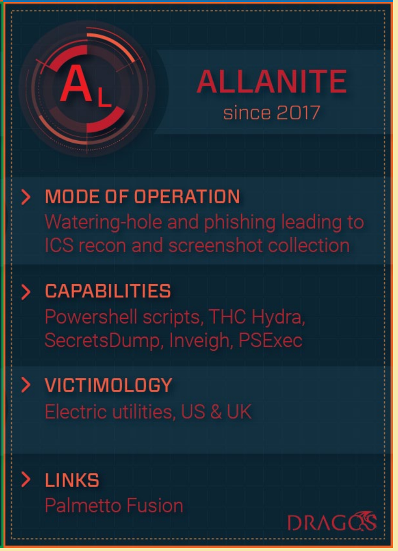
MODE OF OPERATION
IT network limited, information gathering against industrial orgs

CAPABILITIES
STONEDRILL wiper, variants of TURNEDUP malware

VICTIMOLOGY
Petrochemical, Aerospace, Saudi Arabia

LINKS
APT33

DRAGOS



ALLANITE
since 2017

MODE OF OPERATION
Watering-hole and phishing leading to ICS recon and screenshot collection

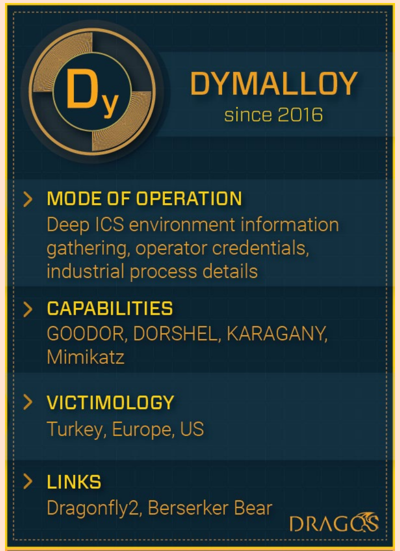
CAPABILITIES
Powershell scripts, THC Hydra, SecretsDump, Inveigh, PSExec

VICTIMOLOGY
Electric utilities, US & UK

LINKS
Palmetto Fusion

DRAGOS

HIGH



DYMALLOY
since 2016

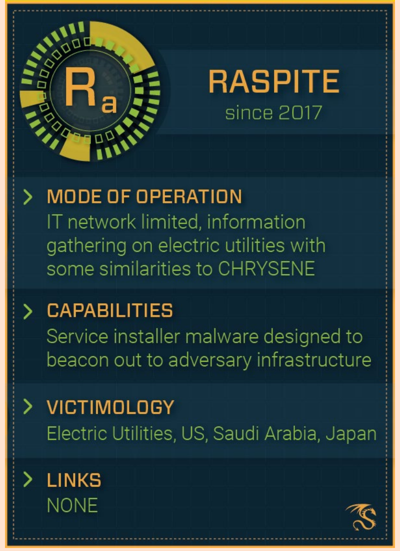
MODE OF OPERATION
Deep ICS environment information gathering, operator credentials, industrial process details

CAPABILITIES
GOODOR, DORSHEL, KARAGANY, Mimikatz

VICTIMOLOGY
Turkey, Europe, US

LINKS
Dragonfly2, Berserker Bear

DRAGOS



RASPITE
since 2017

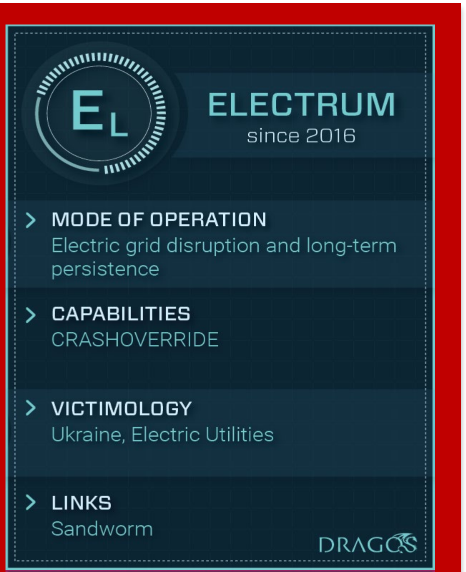
MODE OF OPERATION
IT network limited, information gathering on electric utilities with some similarities to CHRYSENE

CAPABILITIES
Service installer malware designed to beacon out to adversary infrastructure

VICTIMOLOGY
Electric Utilities, US, Saudi Arabia, Japan

LINKS
NONE

EXTREME



ELECTRUM
since 2016

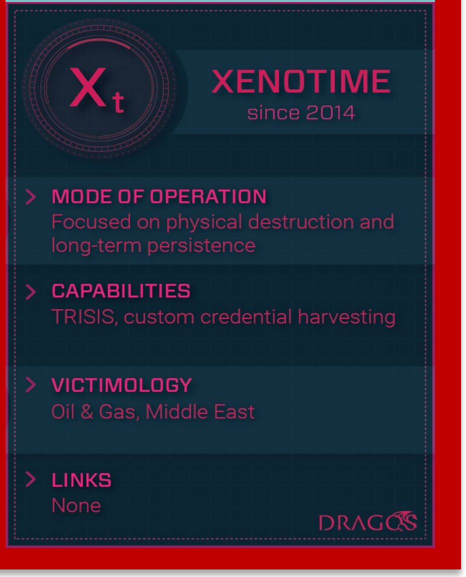
MODE OF OPERATION
Electric grid disruption and long-term persistence

CAPABILITIES
CRASHOVERRIDE

VICTIMOLOGY
Ukraine, Electric Utilities

LINKS
Sandworm

DRAGOS



XENOTIME
since 2014

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

CAPABILITIES
TRISIS, custom credential harvesting

VICTIMOLOGY
Oil & Gas, Middle East

LINKS
None

DRAGOS

Questions?

Email sergio@dragos.com

Twitter @cnoanalysis