The Uncharted Industrial Cyber Threat Landscape

DRAGOS

Robert M. Lee
Twitter: @RobertMLee
Email: rlee@dragos.com
Web: www.dragos.com

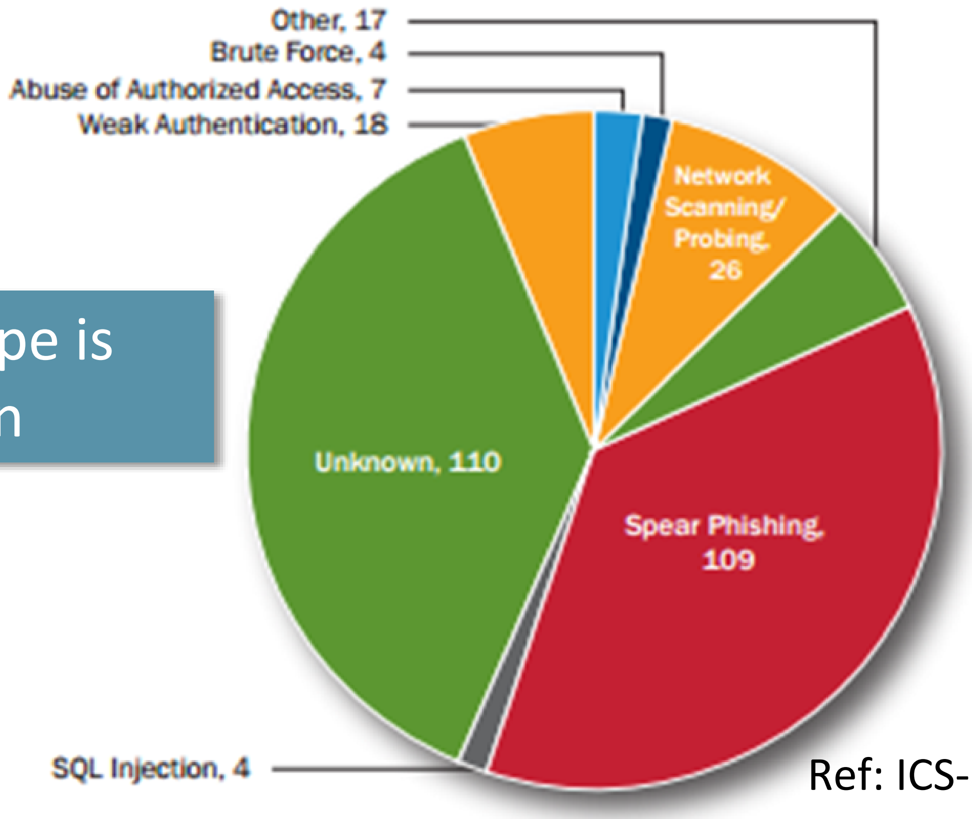
The Unknown Threat Landscape

Few People Know How to Protect the ICS that Run Our World

hundreds
ICS CYBER SECURITY SPECIALISTS
BILLIONS

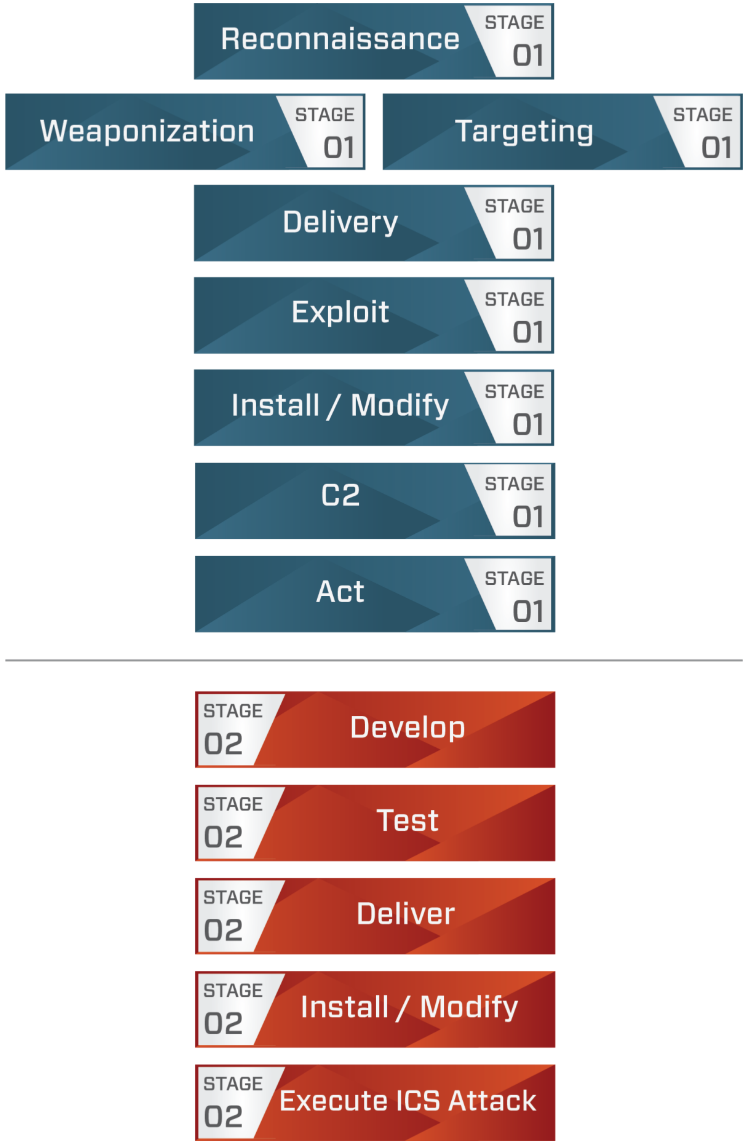
The Threat Landscape is Mostly Unknown

FY 2015 Incidents by Infection Vector (295 total)



Ref: ICS-CERT

ICS Cyber Kill Chain



- Two Phase Kill Chain
- Adversary must understand the physical process and safeguards
- Takes more steps to do the type of attacks we’re most concerned with

DRAGOS

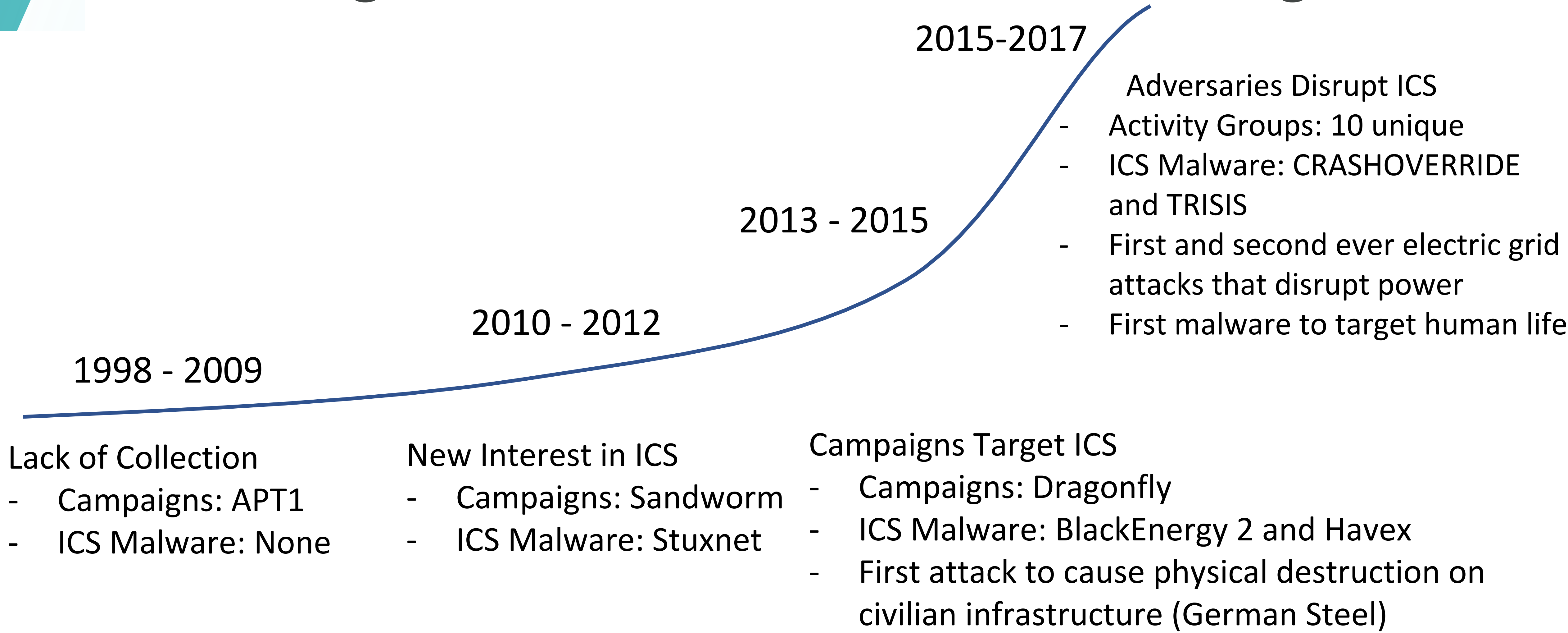
Ref: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

The Reality – Defense is Doable

- Industrial infrastructures are some of the most *defensible* networks on the planet
- Predictable high-confidence cyber attacks are difficult (ICS Cyber Kill Chain)
- The threats are worse than we realize but not as bad as we want to imagine

DRAGOS

Finding More and More Occurring



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)

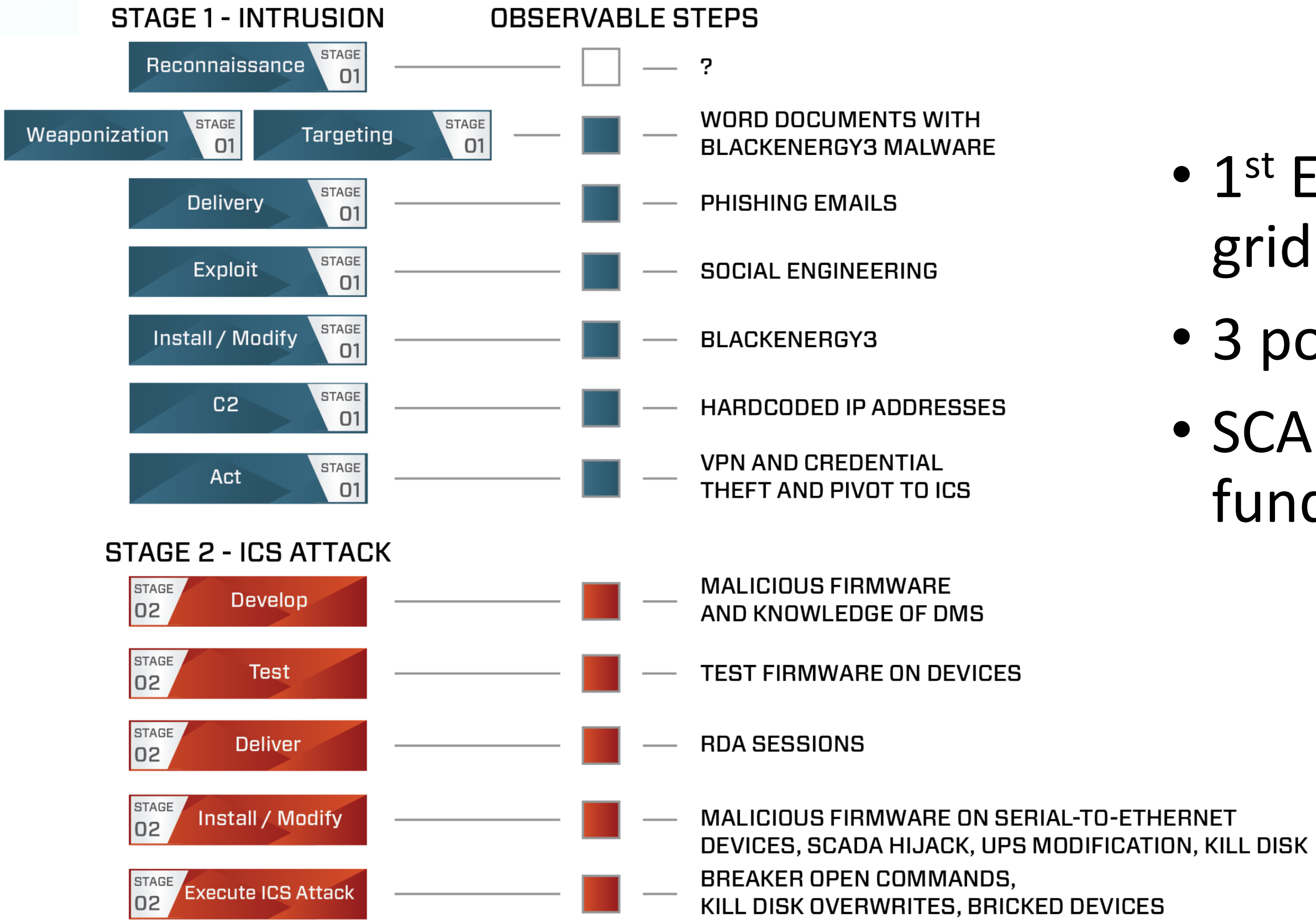
2015-2017

Adversaries Disrupt ICS

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

DRAGOS

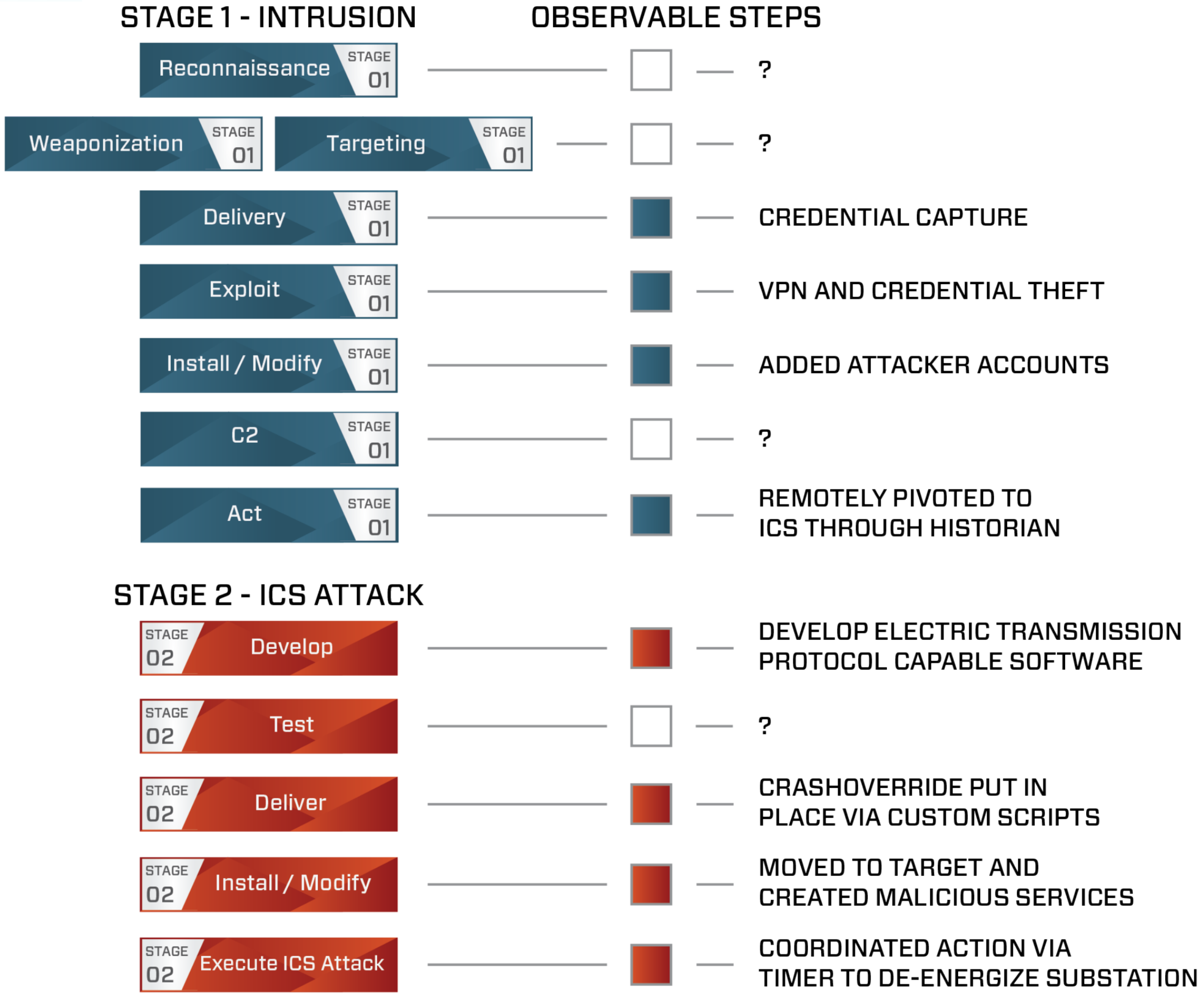
Ukraine 2015



STAGE 1 - INTRUSION		OBSERVABLE STEPS
Reconnaissance STAGE 01	□	?
Weaponization STAGE 01 Targeting STAGE 01	🟦	WORD DOCUMENTS WITH BLACKENERGY3 MALWARE
Delivery STAGE 01	🟦	PHISHING EMAILS
Exploit STAGE 01	🟦	SOCIAL ENGINEERING
Install / Modify STAGE 01	🟦	BLACKENERGY3
C2 STAGE 01	🟦	HARDCODED IP ADDRESSES
Act STAGE 01	🟦	VPN AND CREDENTIAL THEFT AND PIVOT TO ICS
STAGE 2 - ICS ATTACK		
STAGE 02 Develop	🟥	MALICIOUS FIRMWARE AND KNOWLEDGE OF DMS
STAGE 02 Test	🟥	TEST FIRMWARE ON DEVICES
STAGE 02 Deliver	🟥	RDA SESSIONS
STAGE 02 Install / Modify	🟥	MALICIOUS FIRMWARE ON SERIAL-TO-ETHERNET DEVICES, SCADA HIJACK, UPS MODIFICATION, KILL DISK
STAGE 02 Execute ICS Attack	🟥	BREAKER OPEN COMMANDS, KILL DISK OVERWRITES, BRICKED DEVICES

- 1st Ever cyber attack on a power grid to lead to outages
- 3 power companies across Ukraine
- SCADA Hijack scenario by a well funded team

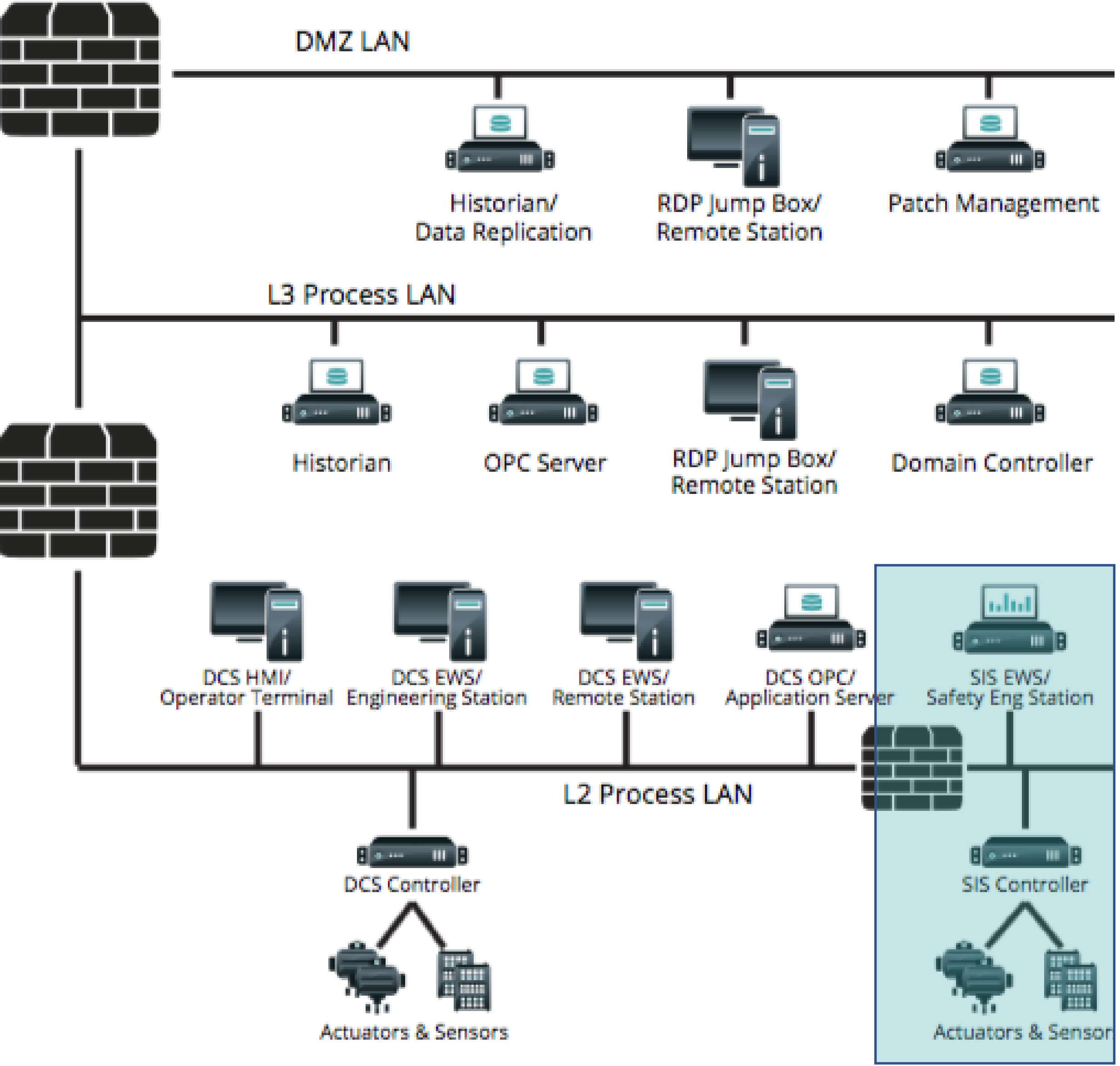
Ukraine 2016 - CRASHOVERRIDE



STAGE 1 - INTRUSION		OBSERVABLE STEPS
Reconnaissance STAGE 01	□	?
Weaponization STAGE 01 Targeting STAGE 01	□	?
Delivery STAGE 01	■	CREDENTIAL CAPTURE
Exploit STAGE 01	■	VPN AND CREDENTIAL THEFT
Install / Modify STAGE 01	■	ADDED ATTACKER ACCOUNTS
C2 STAGE 01	□	?
Act STAGE 01	■	REMOTELY PIVOTED TO ICS THROUGH HISTORIAN
STAGE 2 - ICS ATTACK		
STAGE 02 Develop	■	DEVELOP ELECTRIC TRANSMISSION PROTOCOL CAPABLE SOFTWARE
STAGE 02 Test	□	?
STAGE 02 Deliver	■	CRASHOVERRIDE PUT IN PLACE VIA CUSTOM SCRIPTS
STAGE 02 Install / Modify	■	MOVED TO TARGET AND CREATED MALICIOUS SERVICES
STAGE 02 Execute ICS Attack	■	COORDINATED ACTION VIA TIMER TO DE-ENERGIZE SUBSTATION

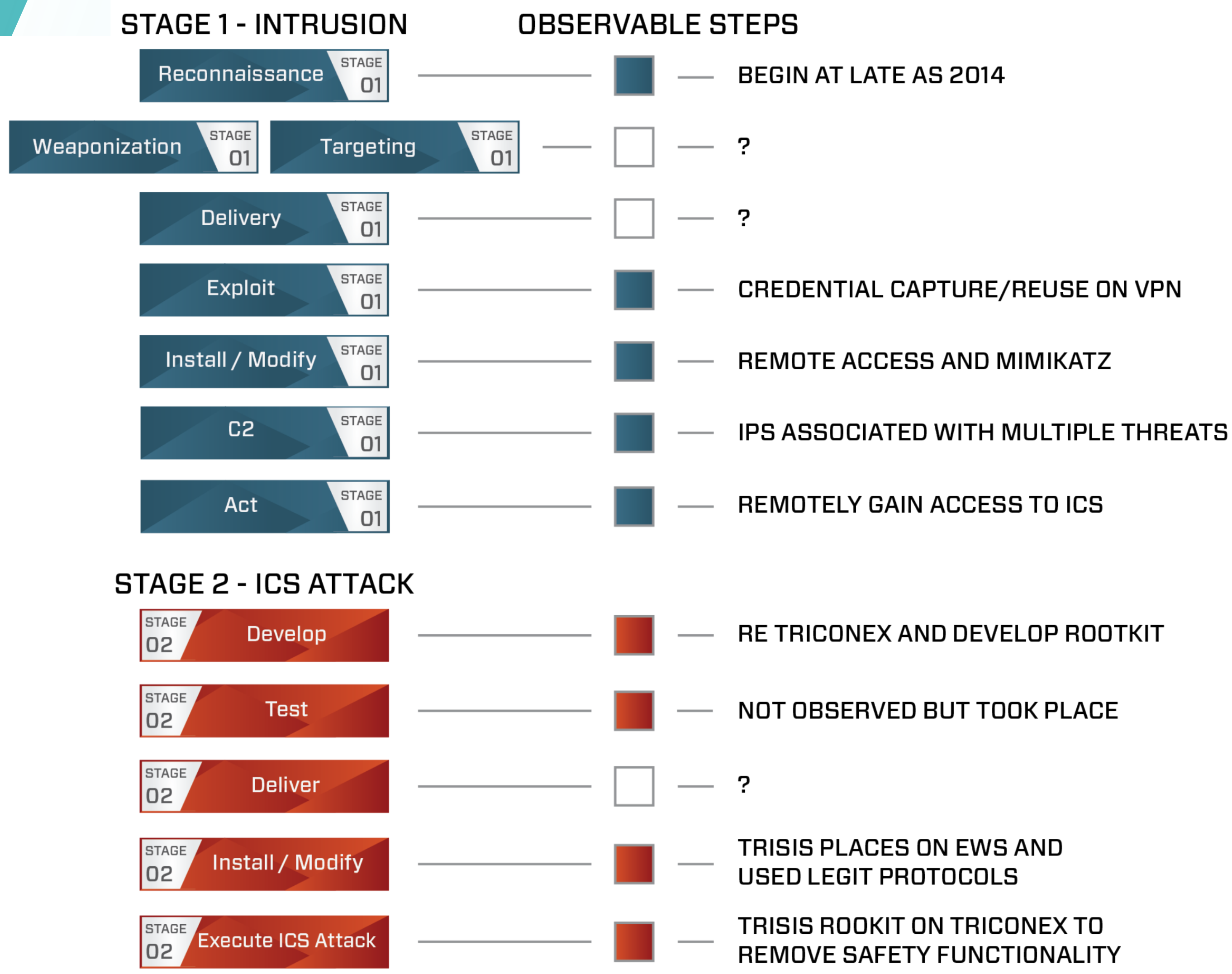
- 2nd Every cyber attack to cause loss of power; 1st due to malware
- 1 Transmission substation in Kiev
- Activity Group – ELECTRUM
  - Still active in Central Europe
  - Water and Electric utility early recon

Middle East 2017 - TRISIS


DMZ LAN
Historian/ Data Replication
RDP Jump Box/ Remote Station
Patch Management
L3 Process LAN
Historian
OPC Server
RDP Jump Box/ Remote Station
Domain Controller
DCS HMI/ Operator Terminal
DCS EWS/ Engineering Station
DCS EWS/ Remote Station
DCS OPC/ Application Server
SIS EWS/ Safety Eng Station
L2 Process LAN
DCS Controller
SIS Controller
Actuators & Sensors
Actuators & Sensor

- TRISIS was delivered into a petrochemical facility in the Middle East by a well funded attack team
- Targeted Safety Instrumented System (SIS) and failed causing a stop in operations
- 1st malware to specifically target human life

Saudi Arabia 2017 - XENOTIME

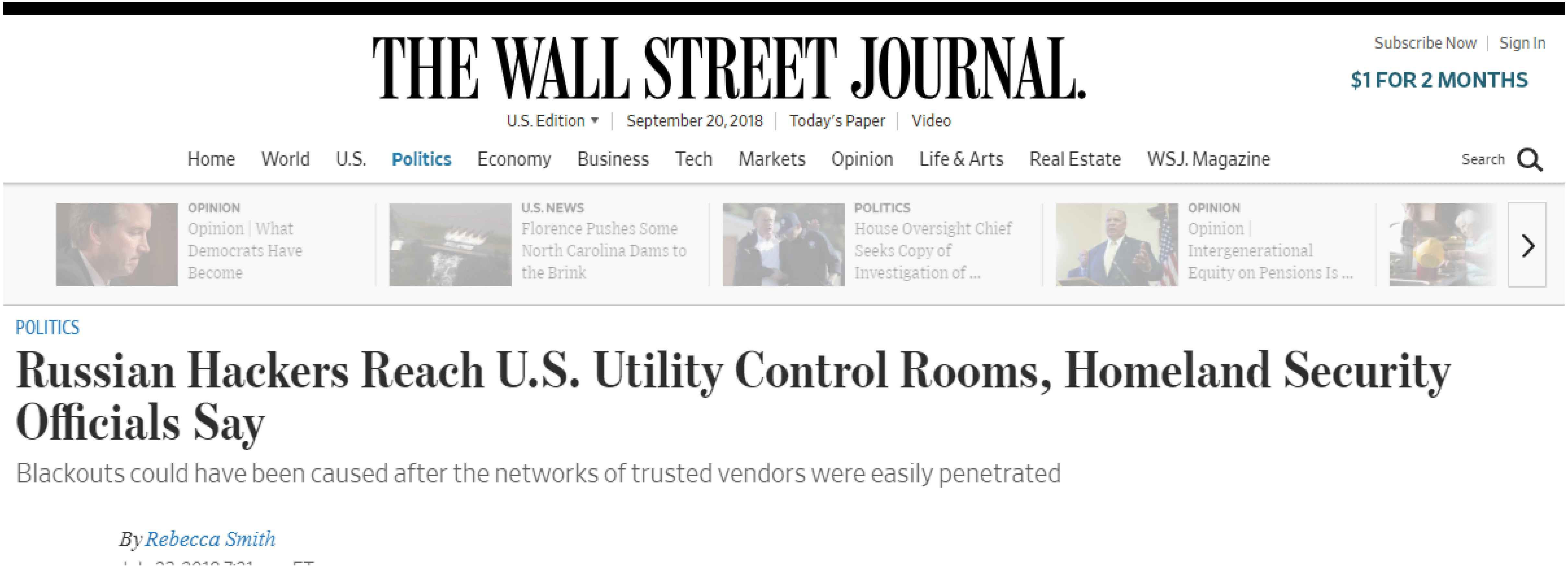


STAGE 1 - INTRUSION		OBSERVABLE STEPS
Reconnaissance STAGE 01	■	BEGIN AT LATE AS 2014
Weaponization STAGE 01 Targeting STAGE 01	□	?
Delivery STAGE 01	□	?
Exploit STAGE 01	■	CREDENTIAL CAPTURE/REUSE ON VPN
Install / Modify STAGE 01	■	REMOTE ACCESS AND MIMIKATZ
C2 STAGE 01	■	IPS ASSOCIATED WITH MULTIPLE THREATS
Act STAGE 01	■	REMOTELY GAIN ACCESS TO ICS
STAGE 2 - ICS ATTACK		
STAGE 02 Develop	■	RE TRICONEX AND DEVELOP ROOTKIT
STAGE 02 Test	■	NOT OBSERVED BUT TOOK PLACE
STAGE 02 Deliver	□	?
STAGE 02 Install / Modify	■	TRISIS PLACES ON EWS AND USED LEGIT PROTOCOLS
STAGE 02 Execute ICS Attack	■	TRISIS ROOKIT ON TRICONEX TO REMOVE SAFETY FUNCTIONALITY

- Attacks are not 1 single action
- TRISIS was just the final steps of XENOTIME’s attack
- Activity Group: XENOTIME
  - Compromises of at least 6 other entities in North America and Europe included Electric, Oil and Gas, and OEMs

DRAGOS

But Be Warned of Hype



THE WALL STREET JOURNAL.

Subscribe Now | Sign In

$1 FOR 2 MONTHS

U.S. Edition ▾ | September 20, 2018 | Today's Paper | Video

Home World U.S. **Politics** Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine Search

OPINION
Opinion | What Democrats Have Become

U.S. NEWS
Florence Pushes Some North Carolina Dams to the Brink

POLITICS
House Oversight Chief Seeks Copy of Investigation of ...

OPINION
Opinion | Intergenerational Equity on Pensions Is ...

POLITICS

Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say

Blackouts could have been caused after the networks of trusted vendors were easily penetrated

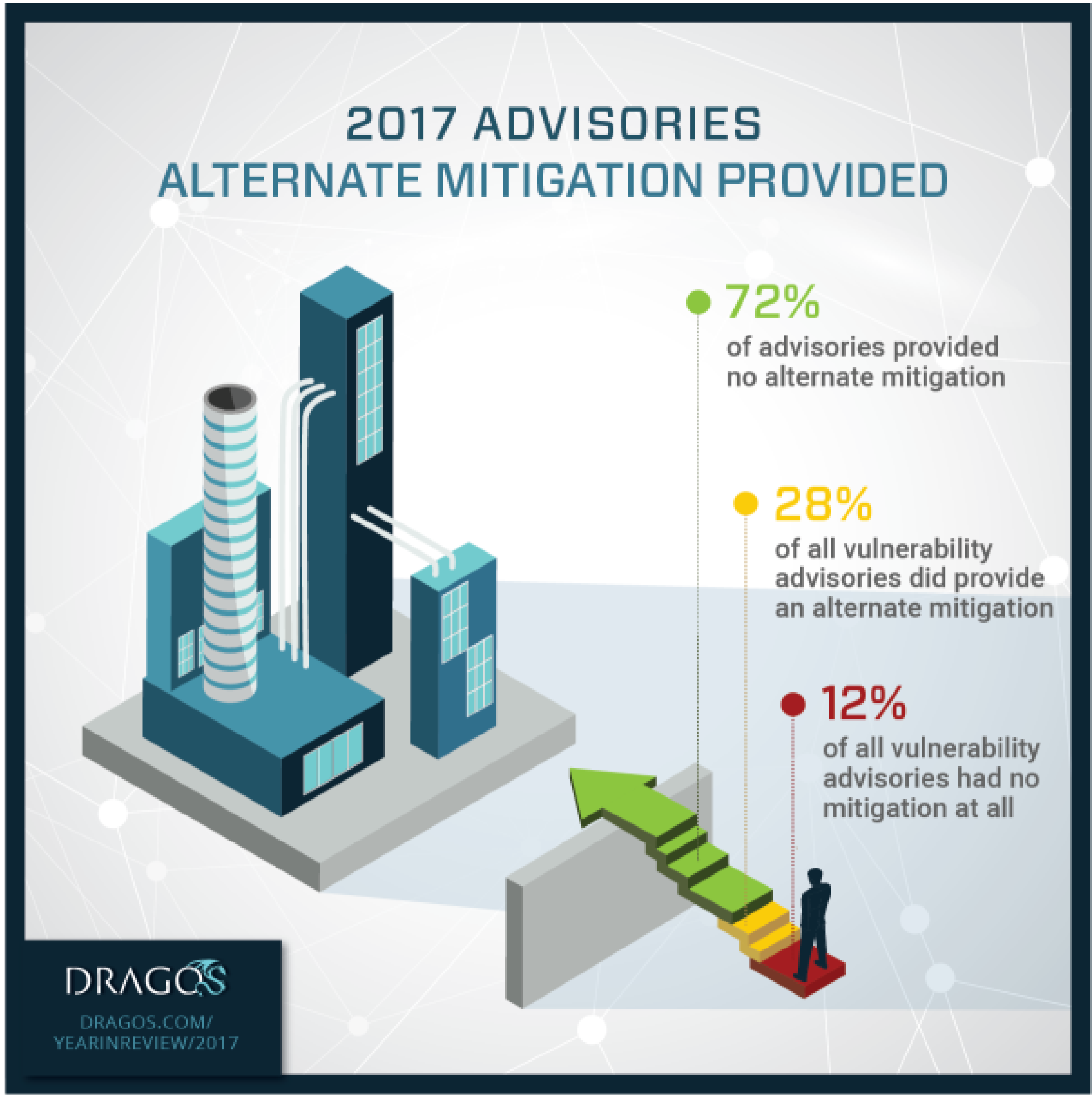
By Rebecca Smith

July 23, 2018 7:21 p.m. ET

You Cannot Just Patch Away the Problem

Dragos’ 2017 in Review reports revealed that for ICS vulnerabilities:

- 64% of all vulns didn’t eliminate the risk
- 72% provided no alternate mitigation to the patch
- Only 15% could be leveraged to gain initial access



2017 ADVISORIES
ALTERNATE MITIGATION PROVIDED

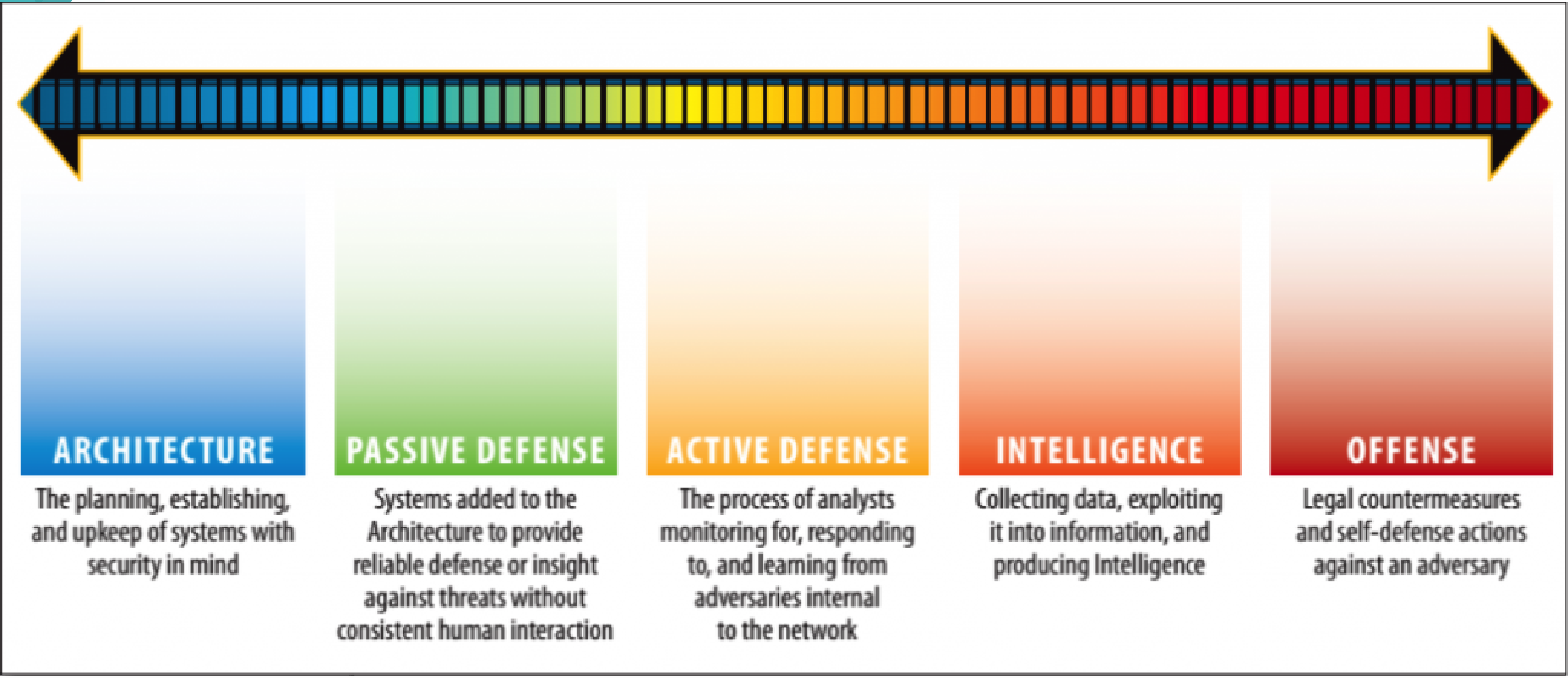
72% of advisories provided no alternate mitigation

28% of all vulnerability advisories did provide an alternate mitigation

12% of all vulnerability advisories had no mitigation at all

Ref: www.dragos.com/YearInReview/2017

Understand Where You Are and Want to Be



ARCHITECTURE
The planning, establishing, and upkeep of systems with security in mind

PASSIVE DEFENSE
Systems added to the Architecture to provide reliable defense or insight against threats without consistent human interaction

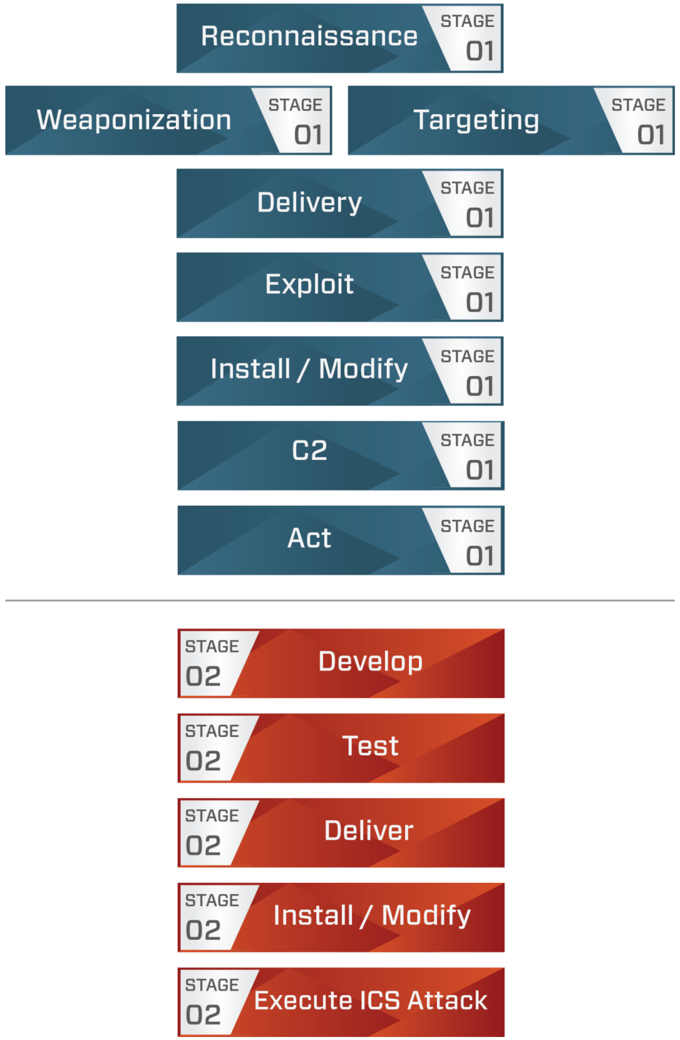
ACTIVE DEFENSE
The process of analysts monitoring for, responding to, and learning from adversaries internal to the network

INTELLIGENCE
Collecting data, exploiting it into information, and producing Intelligence

OFFENSE
Legal countermeasures and self-defense actions against an adversary

Ref: https://www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

Map the Models Together



Reconnaissance STAGE 01

Weaponization STAGE 01

Targeting STAGE 01

Delivery STAGE 01

Exploit STAGE 01

Install / Modify STAGE 01

C2 STAGE 01

Act STAGE 01

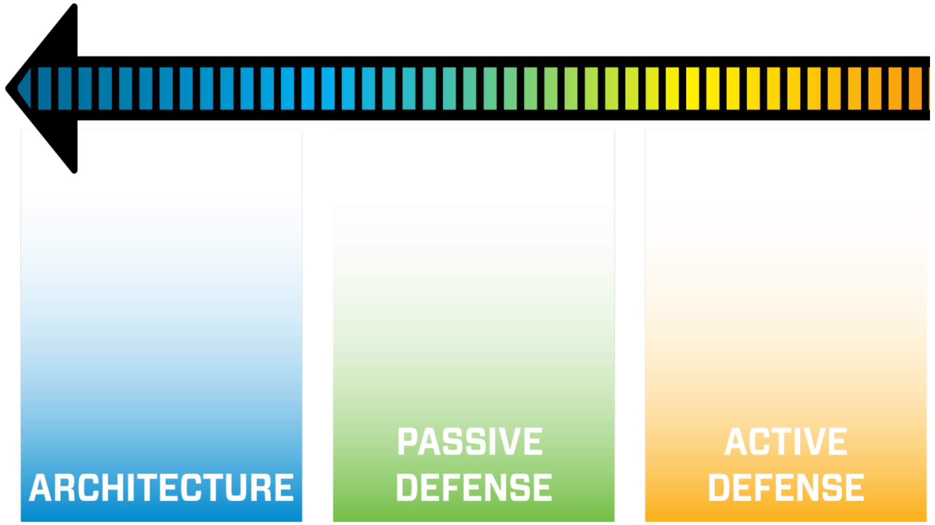
STAGE 02 Develop

STAGE 02 Test

STAGE 02 Deliver

STAGE 02 Install / Modify

STAGE 02 Execute ICS Attack



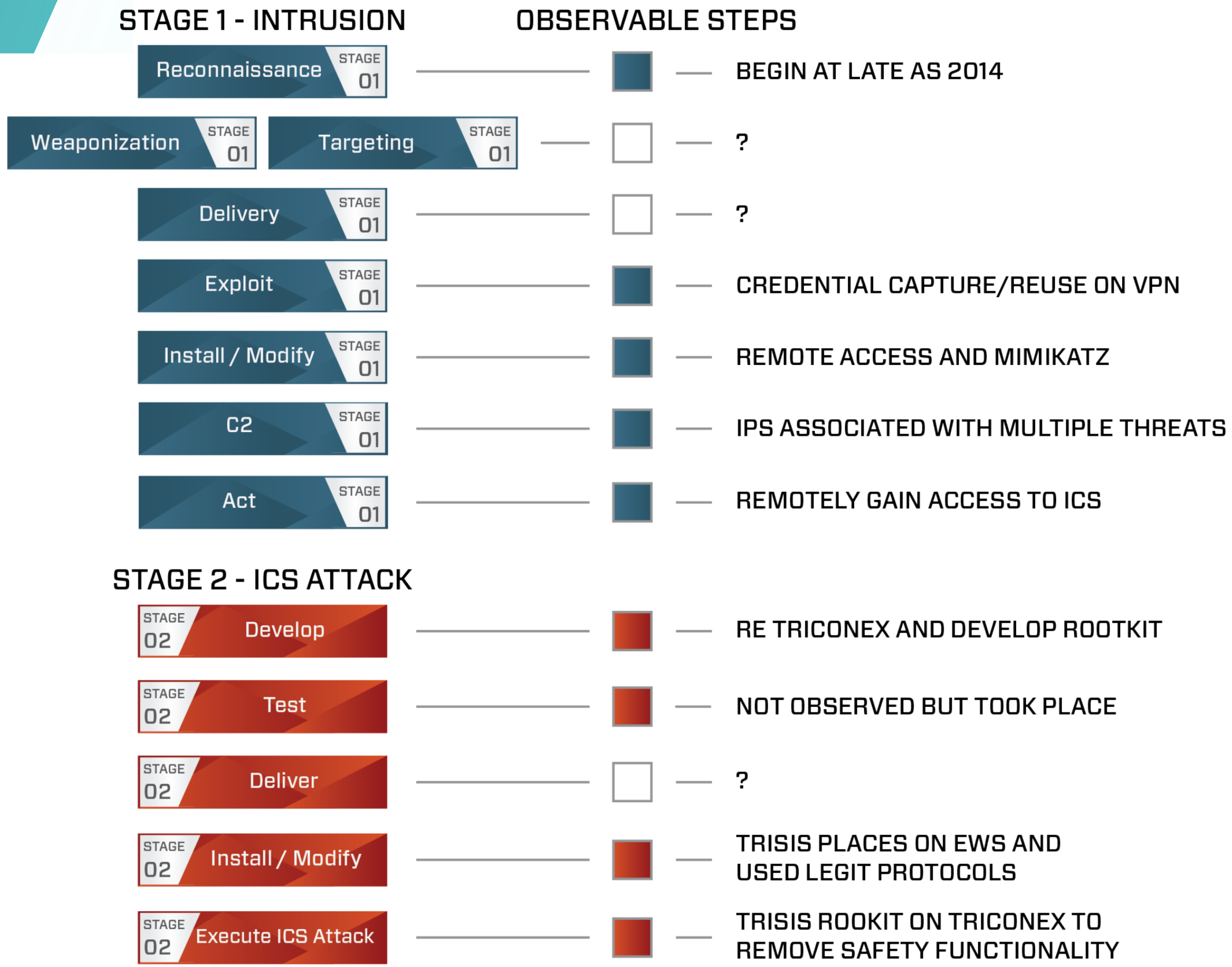
ARCHITECTURE

PASSIVE DEFENSE

ACTIVE DEFENSE

- For every observable step on Architecture, Passive Defense, and Active Defense note what is in place today and proposed for later
- Take the top few controls across the total of your intrusions for ~6 months – 1 year and those are *your* best practices off of *your* industrial threat landscape

XENOTIME Kill Chain and Sliding Scale



STAGE 1 - INTRUSION		OBSERVABLE STEPS
Reconnaissance STAGE 01	■	BEGIN AT LATE AS 2014
Weaponization STAGE 01 Targeting STAGE 01	□	?
Delivery STAGE 01	□	?
Exploit STAGE 01	■	CREDENTIAL CAPTURE/REUSE ON VPN
Install / Modify STAGE 01	■	REMOTE ACCESS AND MIMIKATZ
C2 STAGE 01	■	IPS ASSOCIATED WITH MULTIPLE THREATS
Act STAGE 01	■	REMOTELY GAIN ACCESS TO ICS
STAGE 2 - ICS ATTACK		
STAGE 02 Develop	■	RE TRICONEX AND DEVELOP ROOTKIT
STAGE 02 Test	■	NOT OBSERVED BUT TOOK PLACE
STAGE 02 Deliver	□	?
STAGE 02 Install / Modify	■	TRISIS PLACES ON EWS AND USED LEGIT PROTOCOLS
STAGE 02 Execute ICS Attack	■	TRISIS ROOKIT ON TRICONEX TO REMOVE SAFETY FUNCTIONALITY

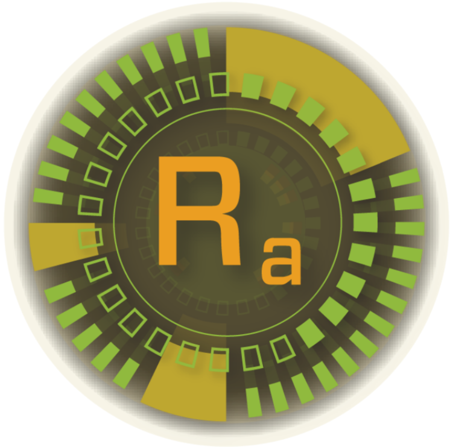
- Today: (whatever you have)

- Stage 2 Execute ICS Attack Proposed:
  - Architecture:
    - Segmentation of SIS
  - Passive Defense:
    - Detection capabilities that can inspect and analyze SIS protocols such as Tristation
  - Active Defense:
    - Incident responders should train and prepare for responding to an incident in an environment with unsafe conditions and no SIS

DRAGOS

ICS Threat Activity Groups

XENOTIME



RASPITE

ALLANITE

MAGNALLIUM

ELECTRUM

DYMALLOY

CHYRSENE

COVELLITE

DRAGOS

https://dragos.com/year-in-review/

Questions?

LITTLE BOBBY
by Robert M. Lee and Jeff Haas
I NEED YOU TO ENSURE NO ATTACKS OCCUR.
OKAY--WHAT'S THE SECURITY BUDGET?
OH, WE HAD TO CUT IT ALL.
I ASSURE YOU WE WILL NEVER SEE ANY ATTACKS.
HAAS

Robert M. Lee
Twitter: @RobertMLee
Email: rlee@dragos.com
Web: www.dragos.com