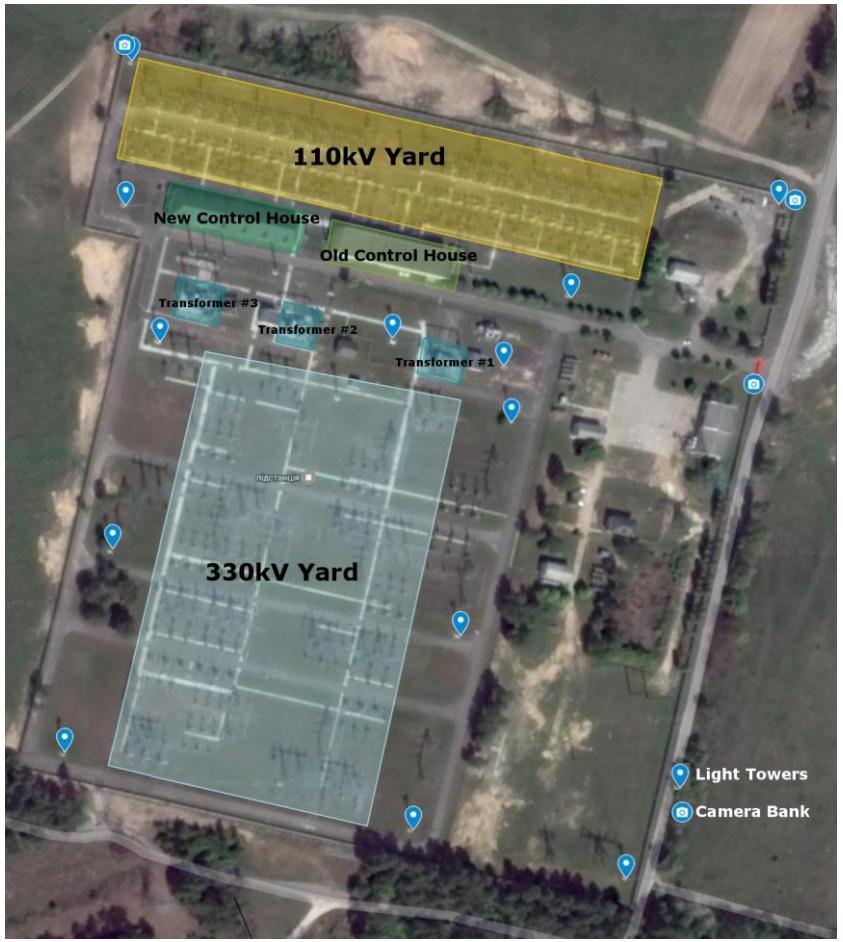
Safeguarding Civilization

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

Agenda

- Background: What Happened
- Explanation: How it Happened
- Defense: How to Detect It

Ukrainian Power Outage



17 Dec 2016, 23:53 Local Time:

- Ukrenergo substation de-energizes
- Resulted in outage for service area

Background: By the numbers

ICS tailored malware families

- Stuxnet
- Havex
- Blackenergy2
- CRASHOVERRIDE

Intent to disrupt industrial processes

Stuxnet and CRASHOVERRIDE

Grid operations enabled

CRASHOVERRIDE is tailored to impacting substation automation technologies exclusively

Dragos Investigation

Activity Group	ELECTRUM
Malware Name	CRASHOVERRIDE
Capabilities	▪ Manipulation of Control ▪ Denial of Control ▪ Denial of View ▪ Data wiping

Stage 1 - Intrusion

- Reconnaissance
- Weaponization
- Targeting
- Delivery
- Exploit
- Install / Modify
- C2
- Act

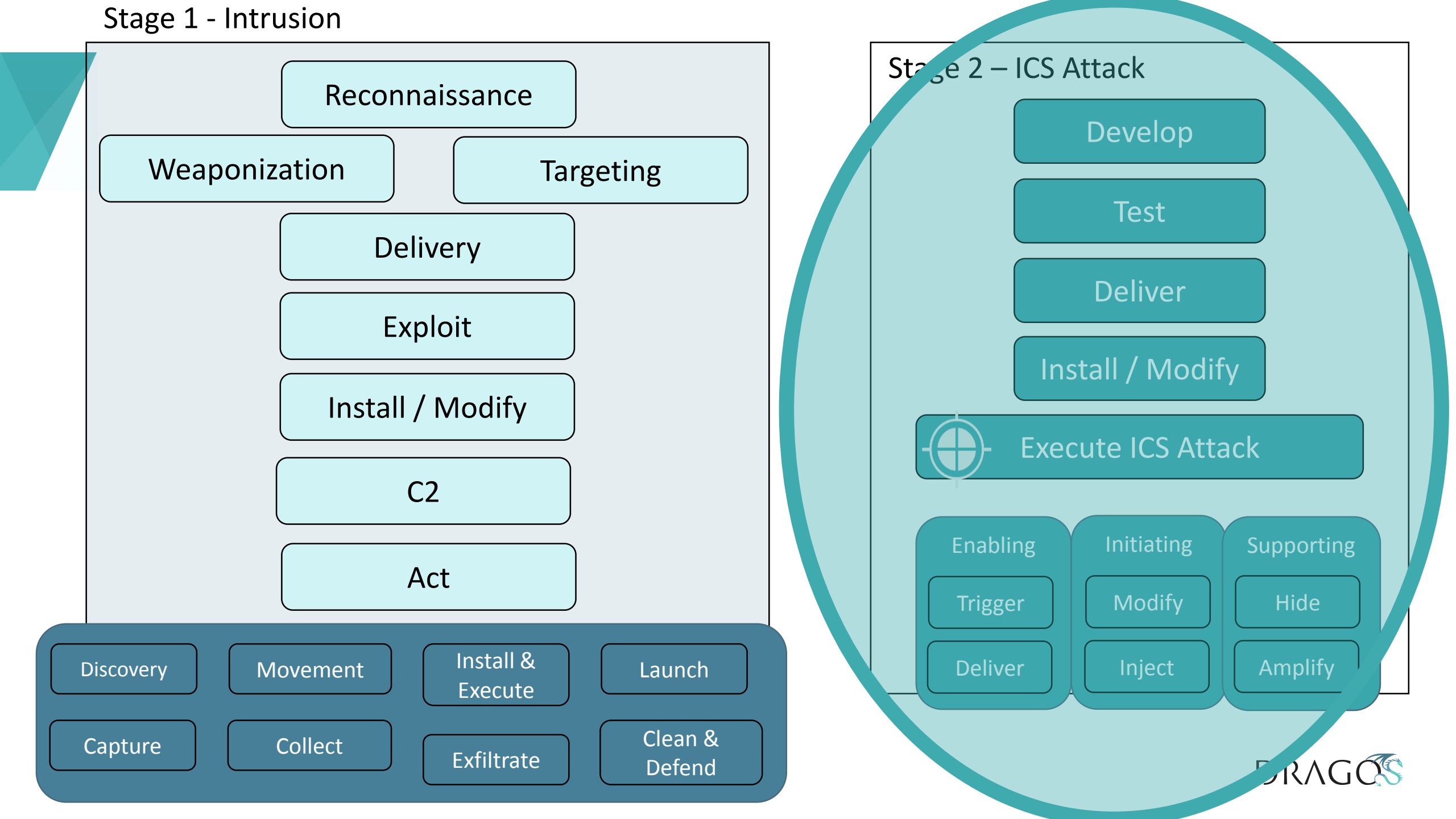
Discovery	Movement	Install & Execute	Launch
Capture	Collect	Exfiltrate	Clean & Defend

Stage 2 – ICS Attack

- Develop
- Test
- Deliver
- Install / Modify
- Execute ICS Attack

Enabling	Initiating	Supporting
Trigger	Modify	Hide
Deliver	Inject	Amplify

DRAGOS


Stage 1 - Intrusion
Reconnaissance
Weaponization
Targeting
Delivery
Exploit
Install / Modify
C2
Act
Discovery
Movement
Install & Execute
Launch
Capture
Collect
Exfiltrate
Clean & Defend
Stage 2 – ICS Attack
Develop
Test
Deliver
Install / Modify
Execute ICS Attack
Enabling
Trigger
Deliver
Initiating
Modify
Inject
Supporting
Hide
Amplify

Dragos Timeline

08 June
- Dragos learns of malware
- Samples located, analysis starts

09 June
- Early Warning sent to Dragos Customers

10 June
- Preliminary analysis concludes
- Confidential notification to impacted parties begins

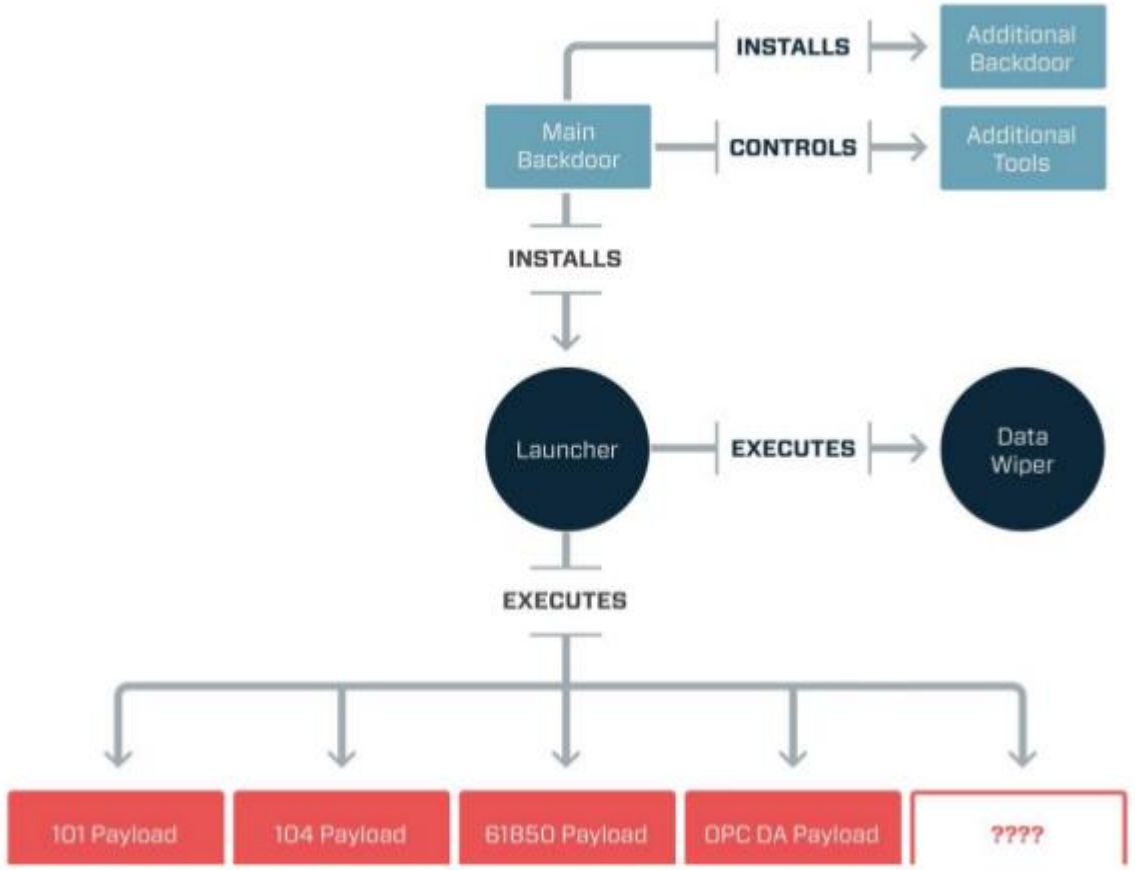
11 June
- Multiple CERTs and other organizations notified
- Initial TLP:AMBER report released

12 June
- Public whitepaper published

The Cause: Malware

- Modular malware used to cause power outage
- Payload DLL specifically designed for ICS effect
- Wiper module included to inhibit or delay recovery

CRASHOVERRIDE Framework



Initial Intrusion

- Dragos has no knowledge of how the network was breached
- However we know how ICS effect later achieved:
  - Proxy-specific beaconing backdoor
  - Provided operator control via staged commands on C2
- Prior foothold and reconnaissance required

The Four Methods to Detect Threats

	Environment	Threat
Unknowns		
Knowns	Configuration Analysis	

The Four Methods to Detect Threats

	Environment	Threat
Unknowns	Statistical Modeling	
Knowns	Configuration Analysis	

The Four Methods to Detect Threats

	Environment	Threat
Unknowns	Statistical Modeling	
Knowns	Configuration Analysis	Indicators

The Four Methods to Detect Threats

	Environment	Threat
Unknowns	Statistical Modeling	Behavioral Analytics
Knowns	Configuration Analysis	Indicators

The Four Methods to Detect Threats

	Environment	Threat
Unknowns	Statistical Modeling	Behavioral Analytics
Knowns	Configuration Analysis	Indicators

The Four Methods to Detect Threats

	Environment	Threat
Unknowns	Statistical Modeling	Behavioral Analytics
Knowns	Configuration Analysis	Indicators

The Four Methods to Detect Threats

	Environment	Threat
Unknowns	Statistical Modeling	Behavioral Analytics
Knowns	Configuration Analysis	Indicators

Requires Deep System Knowledge
(DPI, Vendors Specifics, etc.)

DRAGOS

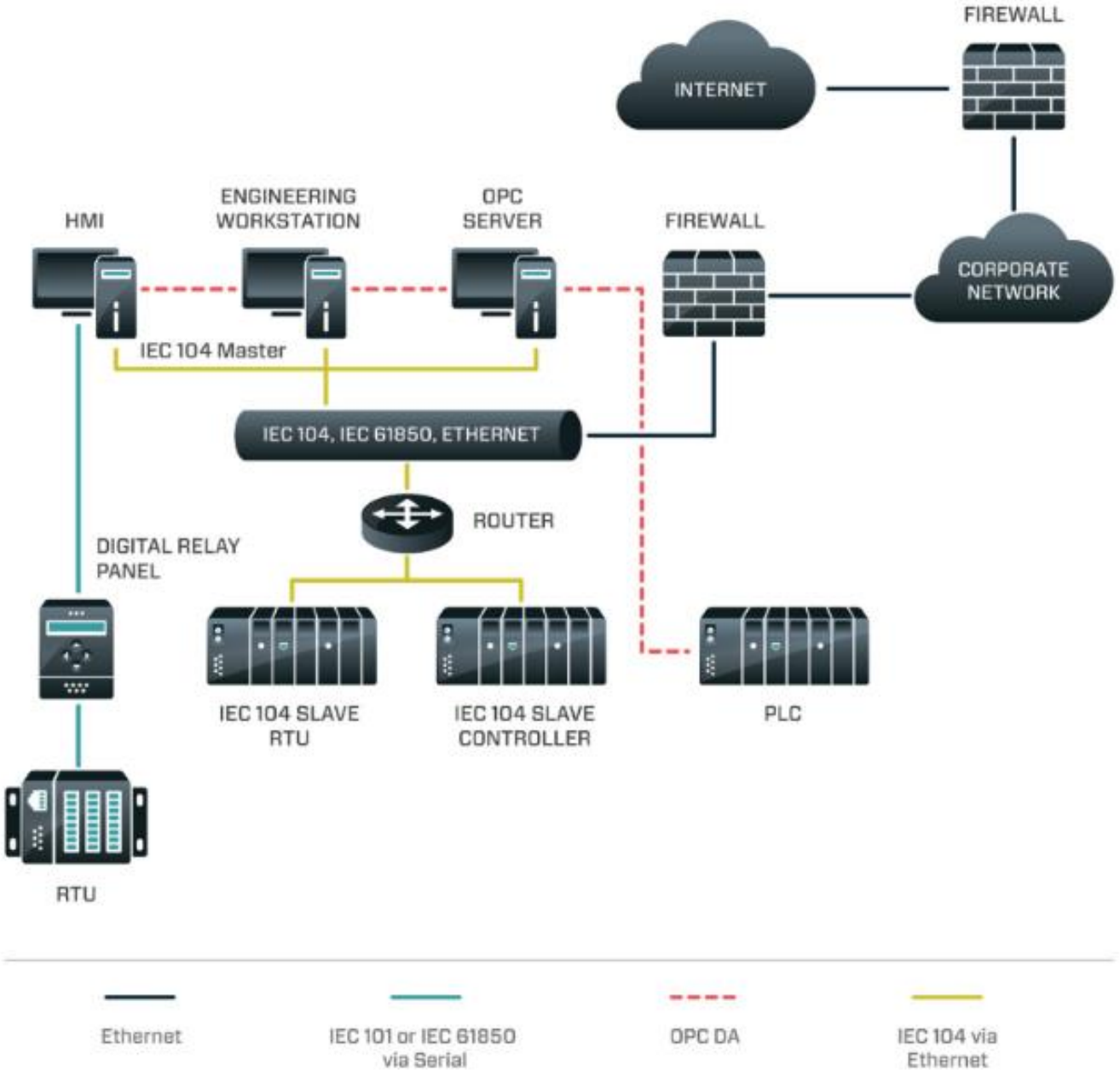
The Four Methods to Detect Threats

	Environment	Threat
Unknowns	Statistical Modeling	Behavioral Analytics
Knowns	Configuration Analysis	Indicators

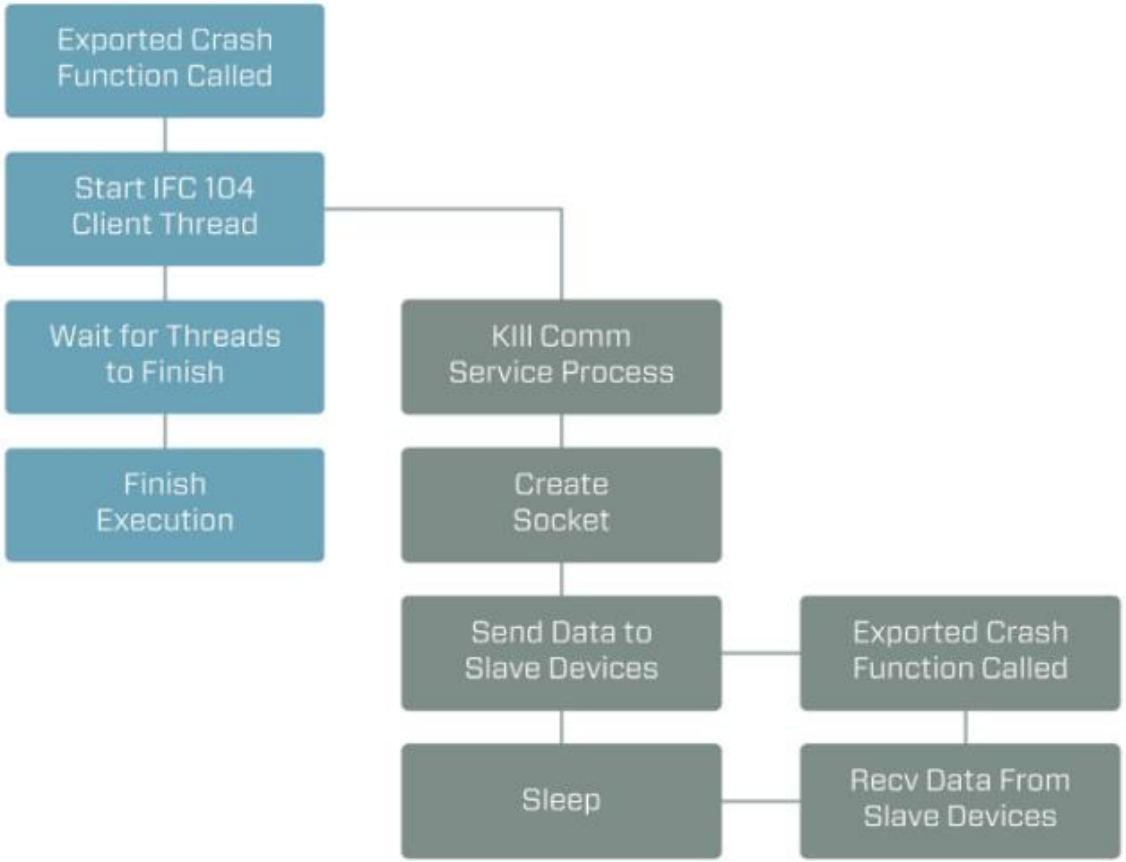
Requires Deep Threat Knowledge
(Incident Response, Intrusion Analysis, etc.)

DRAGOS

IEC 104


FIREWALL
INTERNET
HMI
ENGINEERING WORKSTATION
OPC SERVER
FIREWALL
CORPORATE NETWORK
IEC 104 Master
IEC 104, IEC 61850, ETHERNET
ROUTER
DIGITAL RELAY PANEL
IEC 104 SLAVE RTU
IEC 104 SLAVE CONTROLLER
PLC
RTU
Ethernet
IEC 101 or IEC 61850 via Serial
OPC DA
IEC 104 via Ethernet

IEC 104 Module Execution Flow



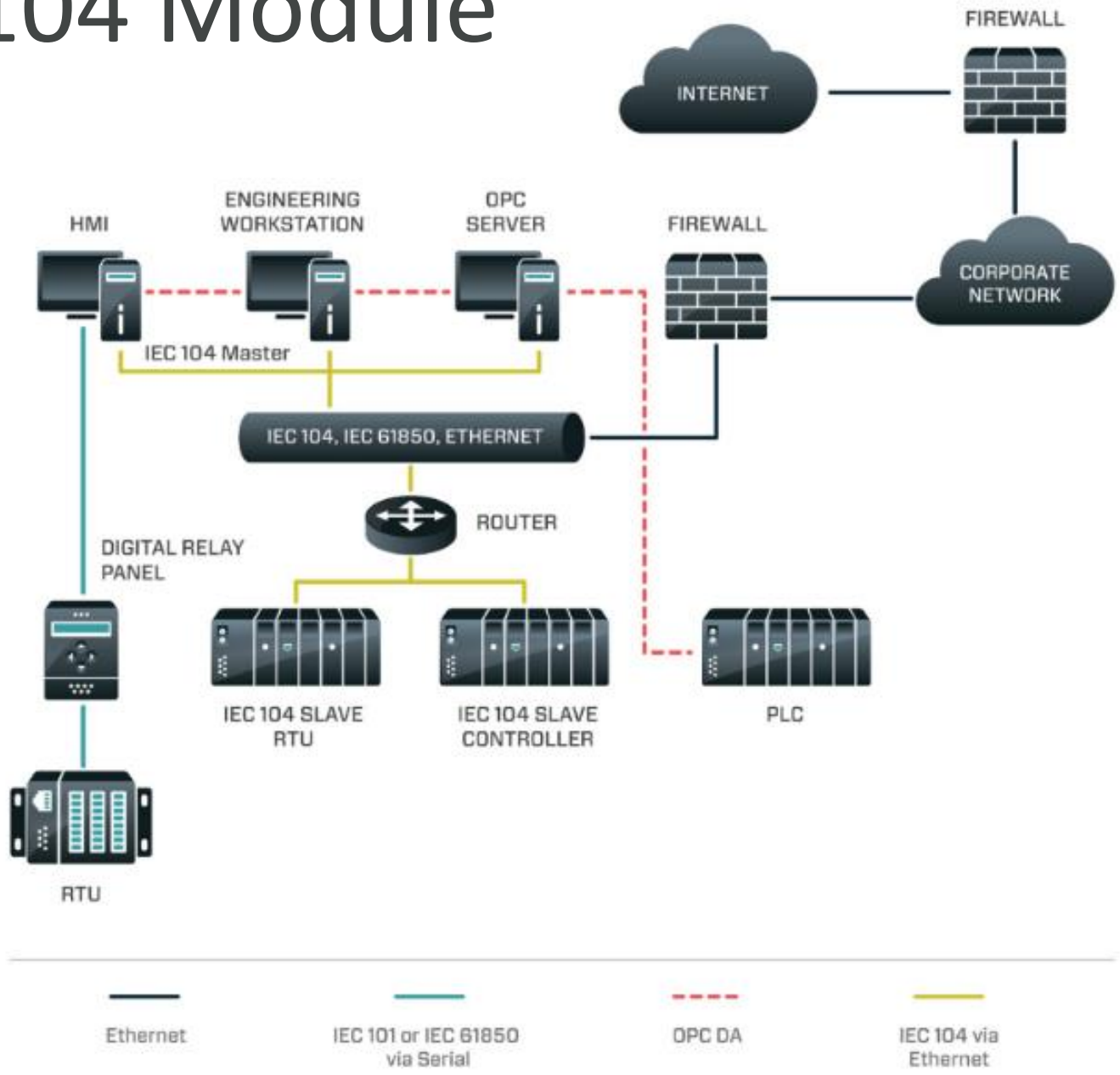
IEC 104 Module

Configuration Analysis
- New Process Spawned on HMI
- (Maybe) New Ports Used

Statistical Analysis
- IEC104 wasn't used in that way before
- "Those commands are anomalous"

Indicator Analysis:
- This IP address is associated with CRASHOVERRIDE
- This digital hash is associated with CRASHOVERRIDE

Behavioral Analytics:
- The way IEC104 is being used in conjunction with the other information is associated with CRASHOVERRIDE tradecraft



CRASHOVERRIDE Resources

- Indicators:
- https://github.com/dragosinc/CRASHOVERRIDE

- In-depth whitepaper:
  https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

Common Questions

- No 0days?
- How scalable is this attack?
- What is the impact to multiple attacks?
- IS THIS AURORA?
- Why did it take so long to discover?
- Will using Linux instead of Windows prevent this?
- Is command and control required?
- What was the infection vector?
- Were HMI credentials stolen?
- Is a SQUID proxy required for the attack or corporate?

Questions?

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