RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

MATTERS NOW

SESSION ID: TECH-T07

INDUSTRIAL CYBER ATTACKS: A QUEST FOR NUANCE WITH LESSONS LEARNED FROM THE FIELD

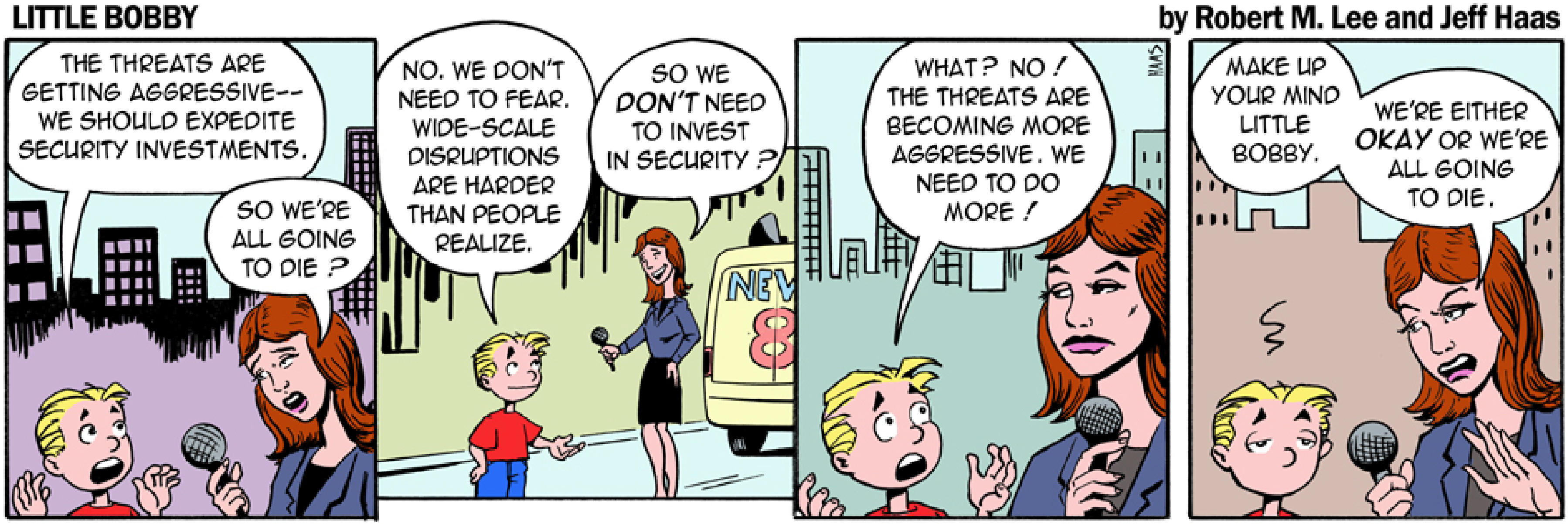
Robert M. Lee

CEO and Founder
Dragos, Inc.
@RobertMLee

About Me

- CEO and Founder of Dragos, Inc
- Started career as a U.S. Air Force Cyber Warfare Operations Officer serving in the National Security Agency
  - Built a first-of-its-kind industrial control system (ICS) threat intel/discovery mission
- SANS Certified Instructor and Course Author
  - FOR578 – Cyber Threat Intelligence
  - ICS515 – ICS Active Defense & Incident Response

The Nuance


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
THE THREATS ARE GETTING AGGRESSIVE-- WE SHOULD EXPEDITE SECURITY INVESTMENTS.
SO WE'RE ALL GOING TO DIE?
NO. WE DON'T NEED TO FEAR. WIDE-SCALE DISRUPTIONS ARE HARDER THAN PEOPLE REALIZE.
SO WE DON'T NEED TO INVEST IN SECURITY?
NEWS 8
HAAS
WHAT? NO! THE THREATS ARE BECOMING MORE AGGRESSIVE. WE NEED TO DO MORE!
MAKE UP YOUR MIND LITTLE BOBBY.
WE'RE EITHER OKAY OR WE'RE ALL GOING TO DIE.

@_LittleBobby_
www.littlebobbycomic.com

Norse's
Iran Cyber Attacks

THE GROWING CYBERTHREAT FROM IRAN

THE INITIAL REPORT OF PROJECT PISTACHIO HARVEST

FREDERICK W. KAGAN AND TOMMY STIANSEN

April 2015

AEI CRITICALTHREATS.ORG

NORSE

Fact: No ICS were harmed in the making of this "report"

2008 Turkey Pipeline Explosion

Bloomberg published “Mysterious ‘08 Turkey Pipeline Blast Opened New Cyberwar” in December, 2014

Fact: BTC Pipeline was attacked

Reality: No “cyber” involved

2015 Turkey Blackout

10-hour Power Failure reported by Bloomberg, CNN, and major media outlets as possible Iranian Cyber Attack

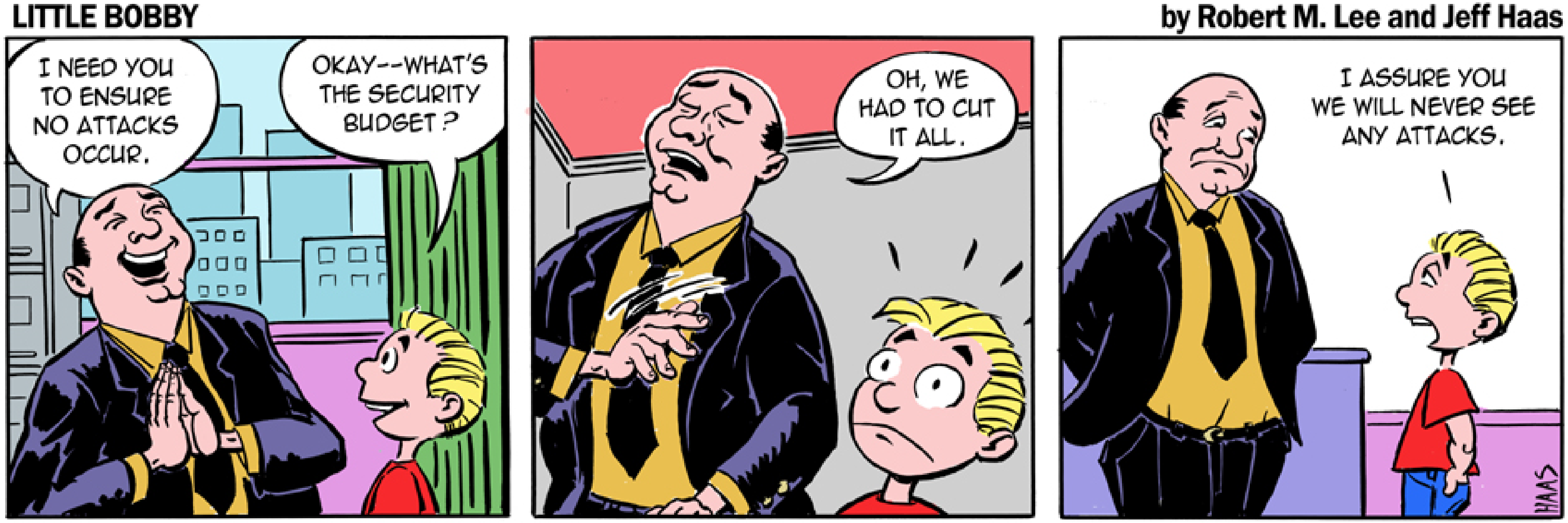
Fact: Aging infrastructure caused outage

Reality: “Cyber” linked through previous reports

The Reality – Defense is Doable

- Industrial infrastructures are some of the most *defensible* networks on the planet
- Predictable high-confidence cyber attacks are difficult, scaling them even more so
- The threats are worse than we realize but not as bad as we want to imagine

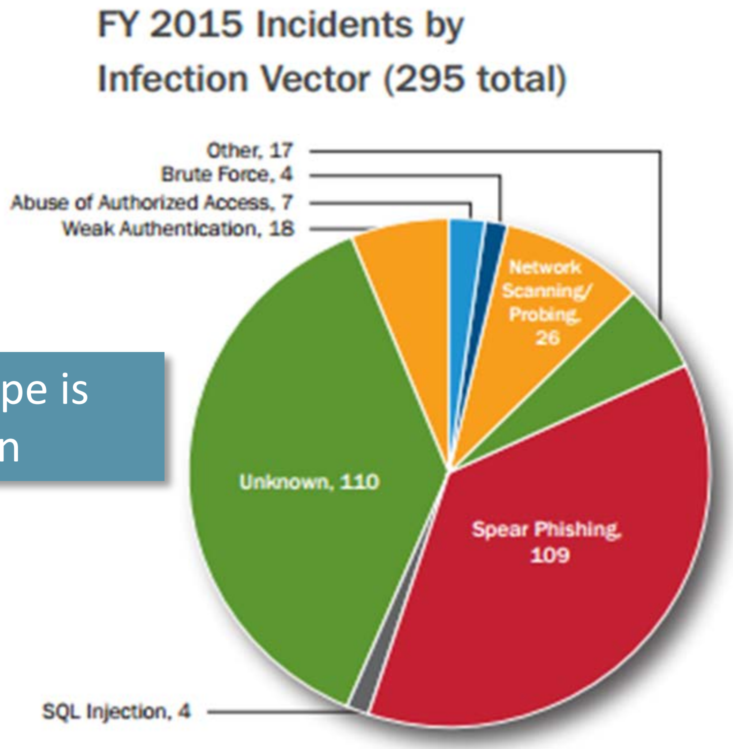
The Challenge


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

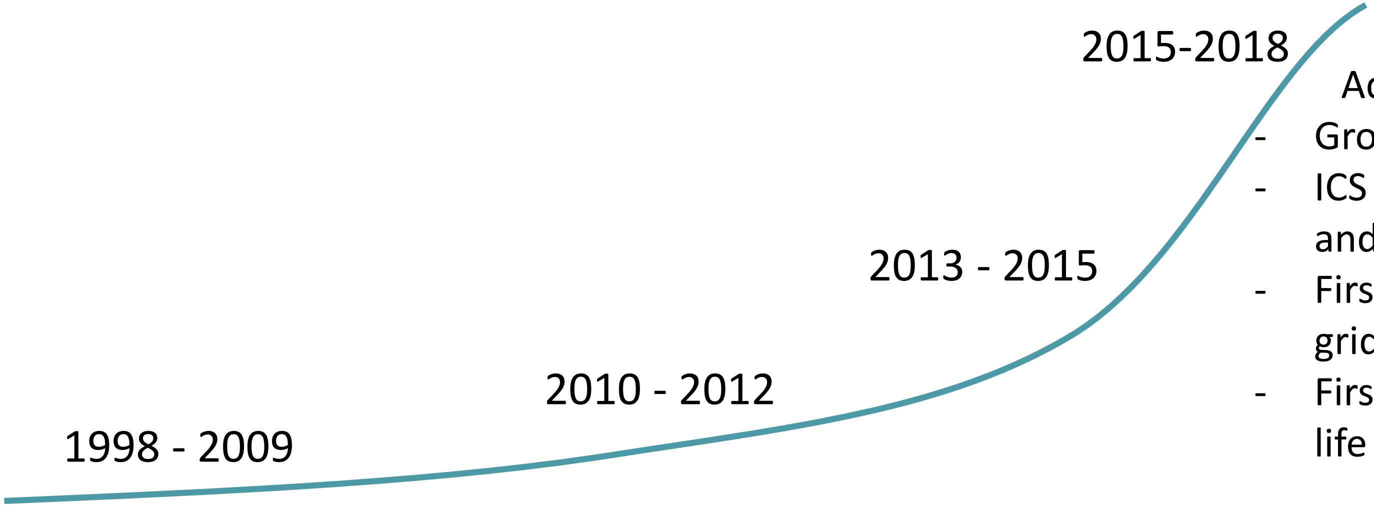
The Unknown Threat Landscape

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

The Threat Landscape is Mostly Unknown



Finding More and More Occurring



1998 - 2009

What’s ICS?

- Groups: APT1
- ICS Malware: None

2010 - 2012

New Interest in ICS

- Groups: Sandworm
- ICS Malware: Stuxnet

2013 - 2015

Campaigns Target ICS

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

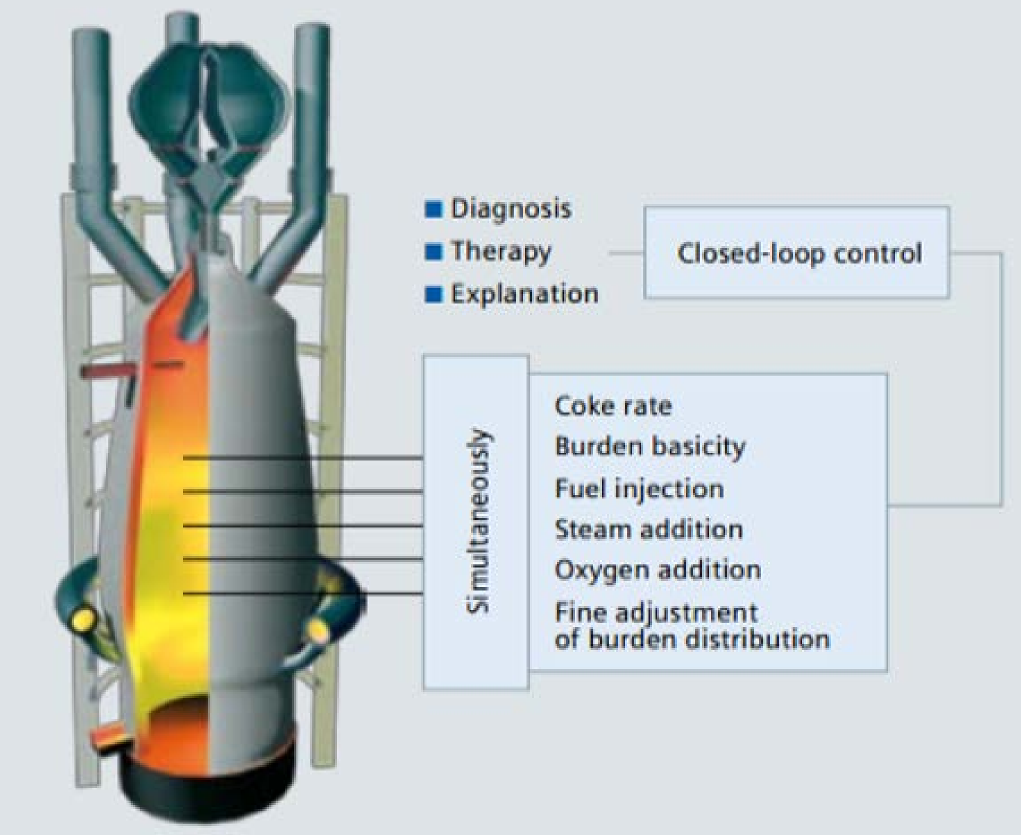
2015-2018

Adversaries Disrupt ICS

- Groups: 7 Unique
- ICS Malware: CRASHOVERRIDE and TRISIS
- First and second ever electric grid attacks that disrupt power
- First malware to target human life

German Steel Plant - 2014

- Dec 18, 2014 German Government’s BSI released annual report highlighting incidents
- Identified “massive damage” in a steel facility due to a cyber attack
- 2nd publicly known case of physical damage to control systems from a cyber attack



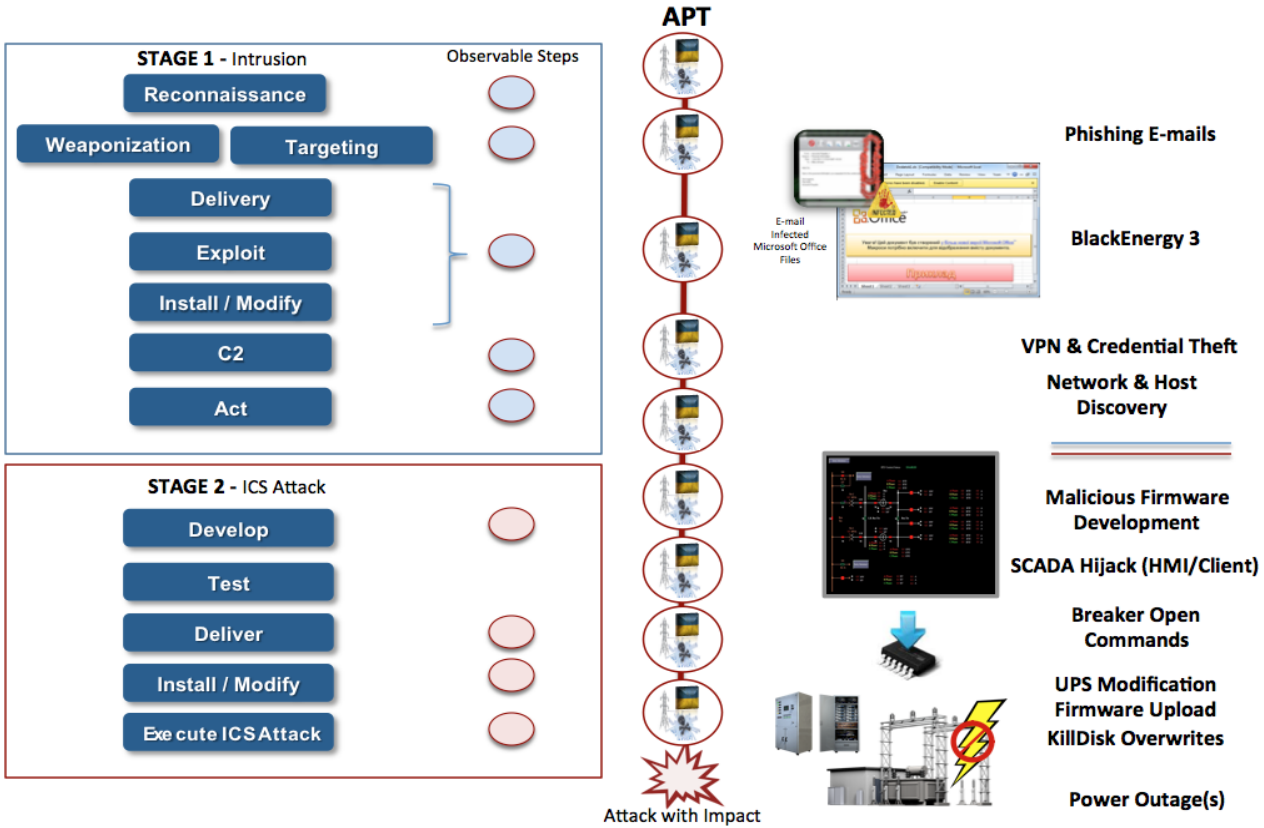
■ Diagnosis
■ Therapy
■ Explanation

Closed-loop control

Simultaneously

Coke rate
Burden basicity
Fuel injection
Steam addition
Oxygen addition
Fine adjustment of burden distribution

Ukraine 2015



APT

STAGE 1 - Intrusion

Observable Steps

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

STAGE 2 - ICS Attack

- Develop
- Test
- Deliver
- Install / Modify
- Exe cute ICS Attack

Attack with Impact

Phishing E-mails

BlackEnergy 3

VPN & Credential Theft

Network & Host Discovery

Malicious Firmware Development

SCADA Hijack (HMI/Client)

Breaker Open Commands

UPS Modification

Firmware Upload

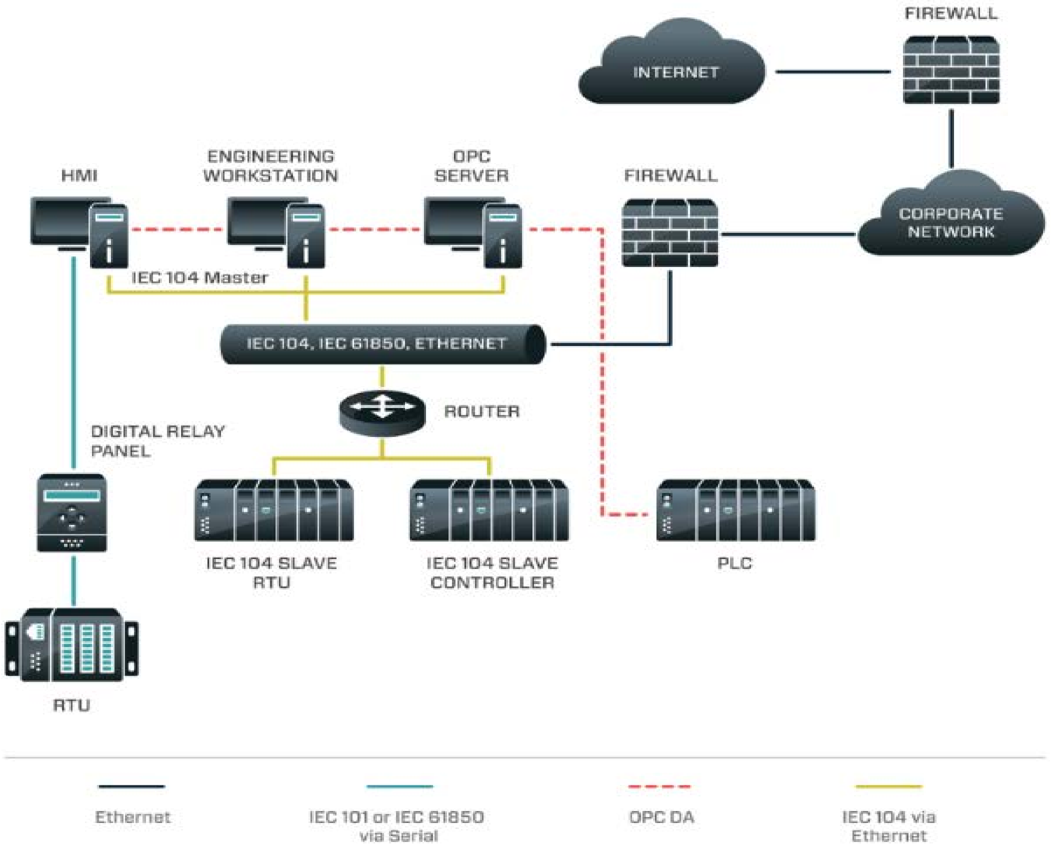
KillDisk Overwrites

Power Outage(s)

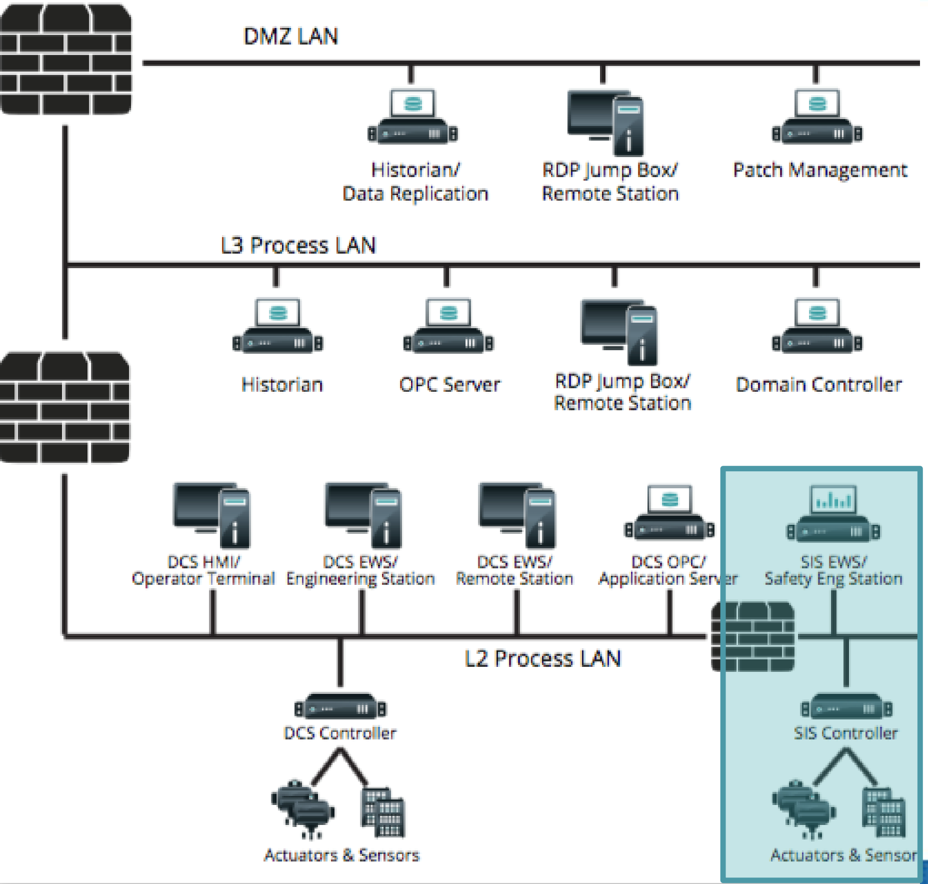
- 1st Ever cyber attack on a power grid to lead to outages
- 3 power companies across Ukraine
- SCADA Hijack scenario by a well funded team

Ukraine 2016 - CRASHOVERRIDE

- CRASHOVERRIDE is not like traditional malware and instead leverages legitimate protocols and functionality
- Modules include OPC, IEC61850, IEC104, and IEC101 (IEC104 was used)
- 1st malware designed to cause disruption in an electric grid

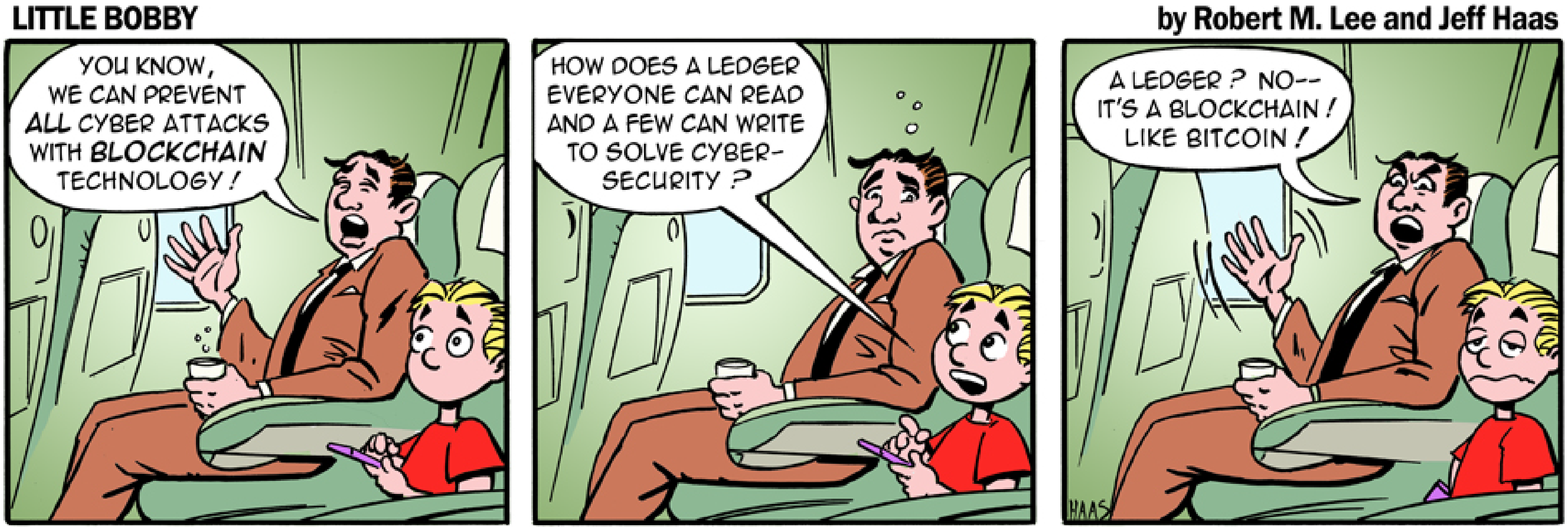


Middle East 2017 - TRISIS

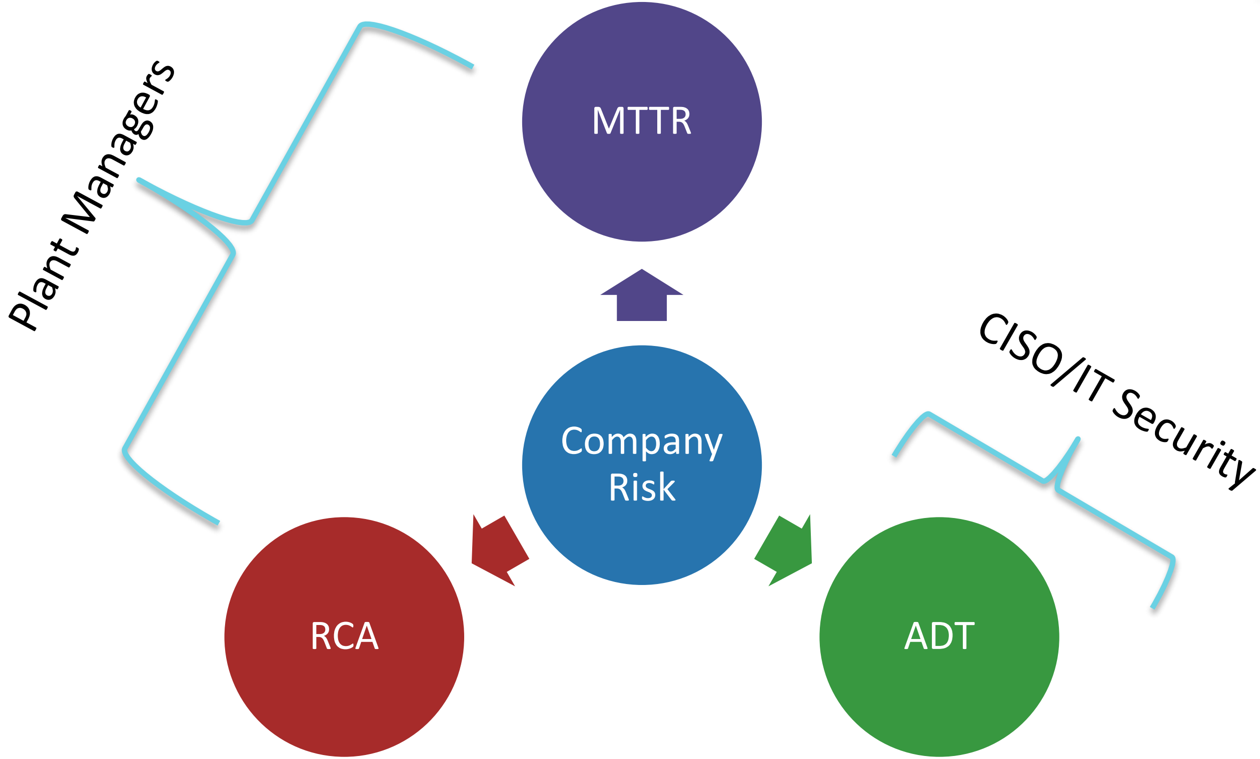


- TRISIS was delivered into a petrochemical facility in the Middle East by a well funded attack team
- Targeted Safety Instrumented System (SIS) and failed causing a stop in operations
- 1st malware to specifically target human life

Lessons Learned - The Approach Required


LITTLE BOBBY
by Robert M. Lee and Jeff Haas
YOU KNOW, WE CAN PREVENT ALL CYBER ATTACKS WITH BLOCKCHAIN TECHNOLOGY!
HOW DOES A LEDGER EVERYONE CAN READ AND A FEW CAN WRITE TO SOLVE CYBER-SECURITY?
A LEDGER? NO-- IT'S A BLOCKCHAIN! LIKE BITCOIN!
HAAS

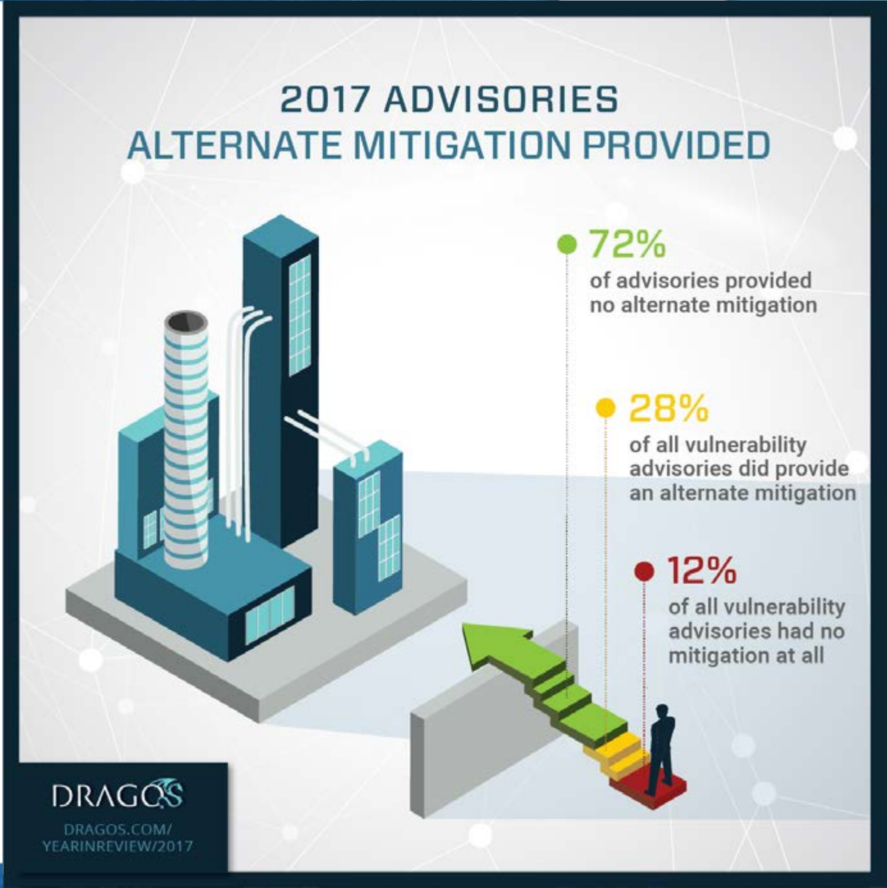
Your Goal – Satisfy the Right Requirements



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

Ref: www.dragos.com/YearInReview/2017

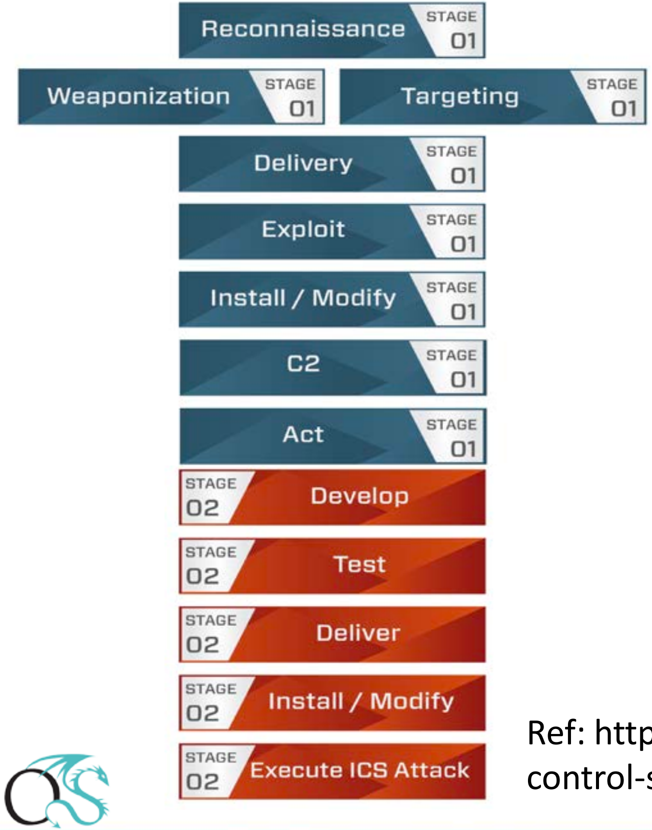

2017 ADVISORIES
ALTERNATE MITIGATION PROVIDED
72%
of advisories provided no alternate mitigation
28%
of all vulnerability advisories did provide an alternate mitigation
12%
of all vulnerability advisories had no mitigation at all
DRAGOS
DRAGOS.COM/
YEARINREVIEW/2017

Understand The Types of Detections

Environment	Threat
Modeling	Threat Behavior Analytics
Configuration Analysis	Indicators

Ref: https://dragos.com/media/sans-webinar-q417.html

Understand Your Detection Coverage



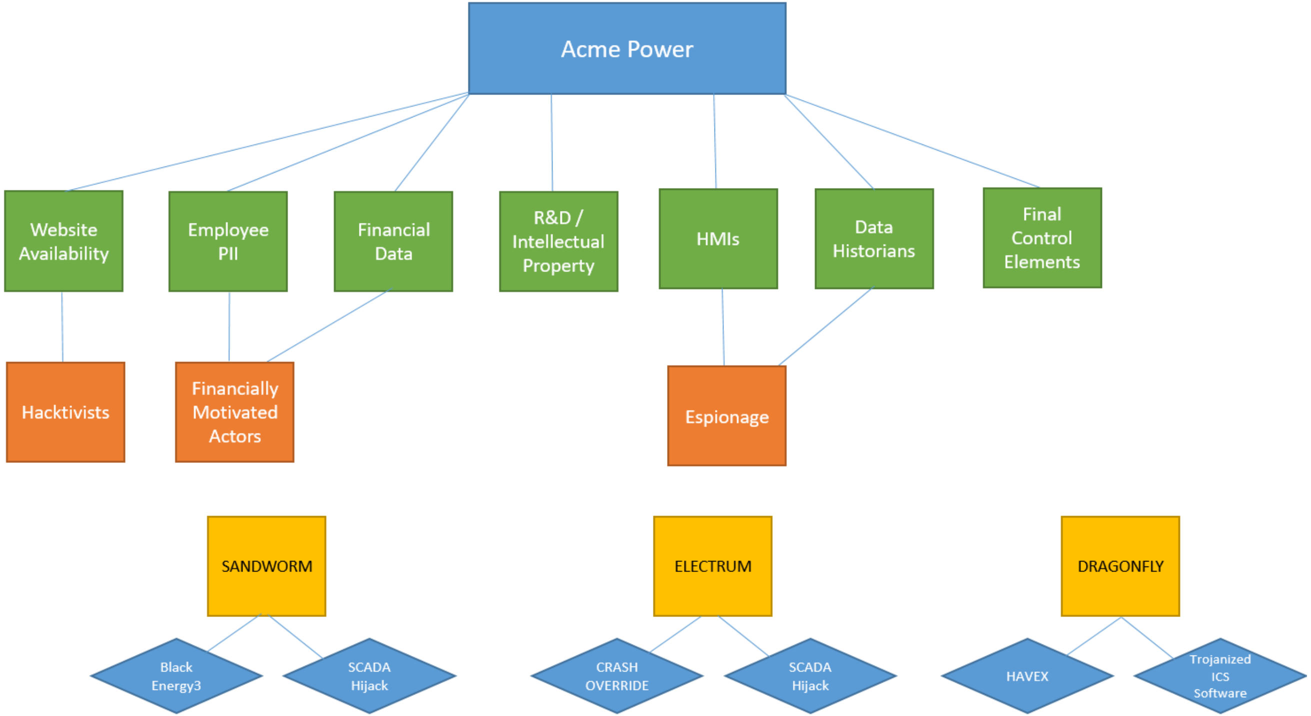
- Map your detection capabilities to each stage of the ICS Cyber Kill Chain
- Ensure analytical coverage
- There is no such thing as an undetectable attack

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

Build Your Collection Management Framework

	Control Center Endpoint Protection Systems	Control Center Windows Systems	Substation Network	DMZ Firewall
Data Type	System Alert	Host Based Logs	Netflow	System Alert
Kill Chain Coverage	Exploitation & Installation	Exploitation, Installation, and Actions on Objectives	Internal Reconnaissance, Delivery, and C2	Internal Reconnaissance, Deliver, and c2
Follow on Collection	Malware sample	Files and timelines	Packet Capture	Netflow
Storage in Days	30 days	60 days	23 days	60 days

Understand Your Threat Model



Acme Power

Website Availability

Employee PII

Financial Data

R&D / Intellectual Property

HMIs

Data Historians

Final Control Elements

Hacktivists

Financially Motivated Actors

Espionage

SANDWORM

Black Energy3

SCADA Hijack

ELECTRUM

CRASH OVERRIDE

SCADA Hijack

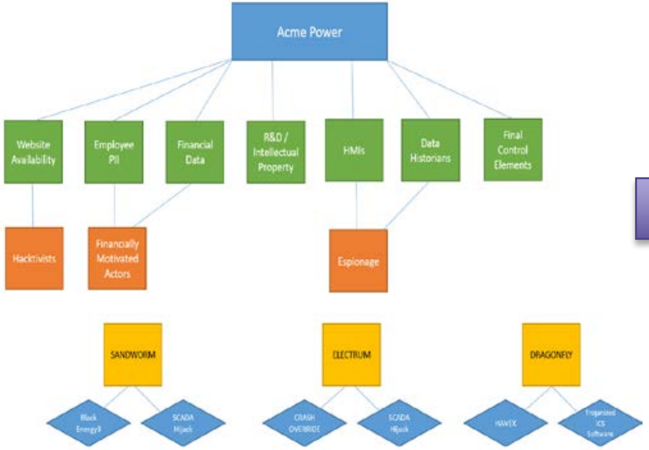
DRAGONFLY

HAVEX

Trojanized ICS Software

Take an Intelligence-Driven Approach

- Use your threat model to develop an intelligence-driven hypothesis
- Develop a threat hunt leveraging the hypothesis and the CMF, then test
- Develop playbooks as you go through the investigation



	Control Center Endpoint Protection Systems	Control Center Windows Systems	Substation Network	DMZ Firewall
Data Type	System Alert	Host Based Logs	Netflow	System Alert
Kill Chain Coverage	Exploitation & Installation	Exploitation, Installation, and Actions on Objectives	Internal Reconnaissance, Delivery, and C2	Internal Reconnaissance, Deliver, and c2
Follow on Collection	Malware sample	Files and timelines	Packet Capture	Netflow
Storage in Days	30 days	60 days	23 days	60 days

Summary

- The threats are worse than we realize but not as bad as we want to imagine
- Industrial focused threat activity groups are becoming worryingly numerous
- Industrial cyber attacks and malware are becoming bolder
- Industrial cyber security requires a different approach than IT security
- Know thyself, know the adversary, and know what to do about it
- Do more, fear less

Thank You For Attending

LITTLE BOBBY
by Robert M. Lee and Jeff Haas
DID YOU HEAR ABOUT THE MANUFACTURING PLANT GOING DOWN?
YES, IT STOPPED PRODUCTION BRIEFLY, I WONDER WHY?
HAAS
MA'AM, THE RUSSIANS LAUNCHED A CYBER ATTACK!
SIR, I UH... I MAY HAVE ACCIDENTALLY CRASHED A SYSTEM.
TIM, DO YOU THINK WE SHOULD CALL SECURITY IN?
NAH, LOOKS LIKE IT WAS JUST A NETWORKING ISSUE.

@RobertMLee
www.Dragos.com
@DragosInc