Fantastic Information and Where to Find it:

A Guidebook to Open Source OT Reconnaissance

Daniel Kapellmann Zafra
Technical Analysis Manager
@Kapellmann

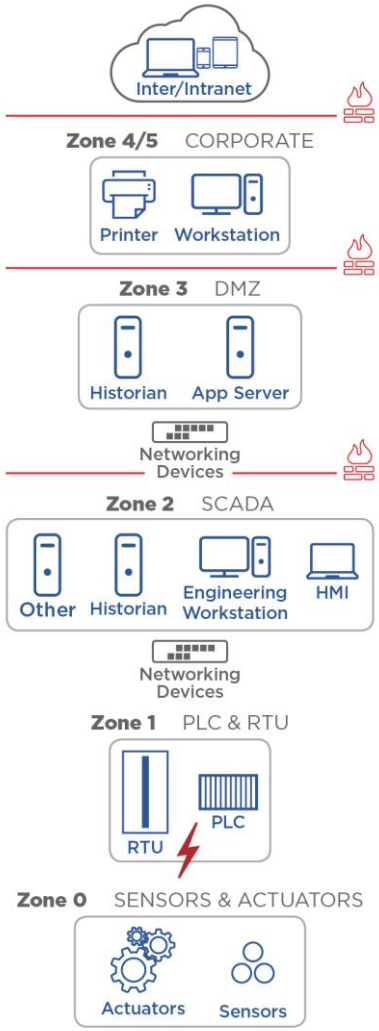
Jeffrey Ashcraft and the Mystery of Sunnyvale

Picture by Geek.com

What are Operational Technologies?

Picture by Korea Shin-Kori NPP

FireEye Reference Architecture



- Historian
- Engineering Workstation
- Human-Machine Interfaces (HMI)
- Distributed Control Systems (DCS)
- Safety Instrumented Systems (SIS)
- Programmable Logical Controller (PLC)
- Sensors and Actuators
- Etc.

~~Click Here to Kill Everybody~~

Attribute	IT Targeted Attack	OT Targeted Attack
Capabilities	Low to High	Very High
Exploit	Single	Multiple
Communication protocols	TCP/IP and UDP	Multiple: TCP/IP, DNP3, ICCP, Modbus, Fieldbus, etc.
Impacts of compromise	Financial or data exposure	Disruption of processes, physical damage, financial
Timing	Delays tolerated	Real-time communications
Bandwidth	High	Normally limited

Based on Protecting Industrial Control Systems from Electronic Threats by Joseph Weiss

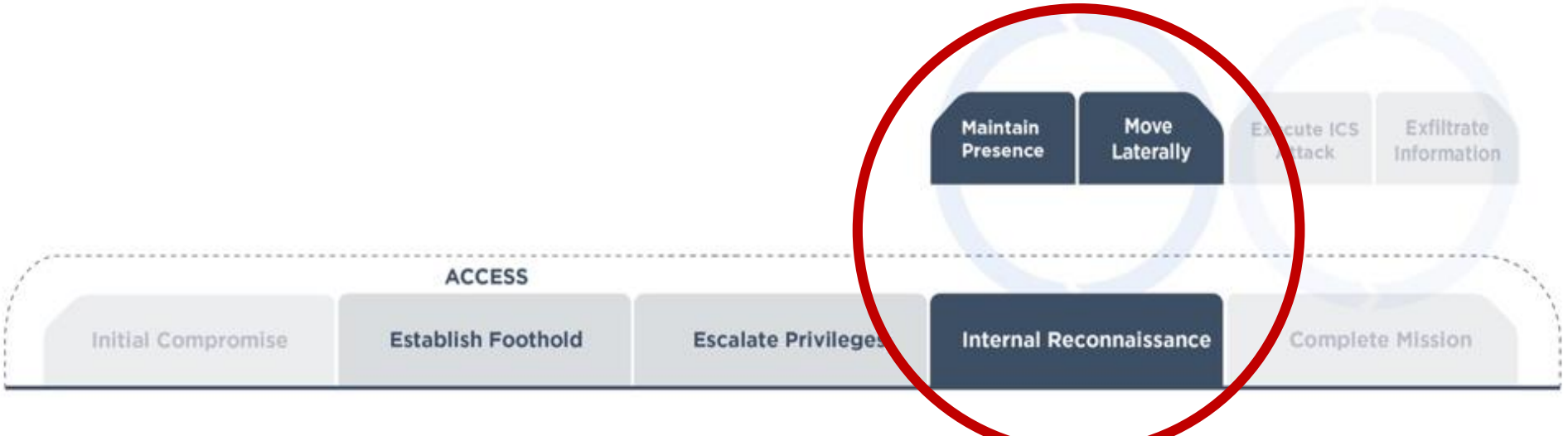
Open Source OT Reconnaissance

Security through obscurity

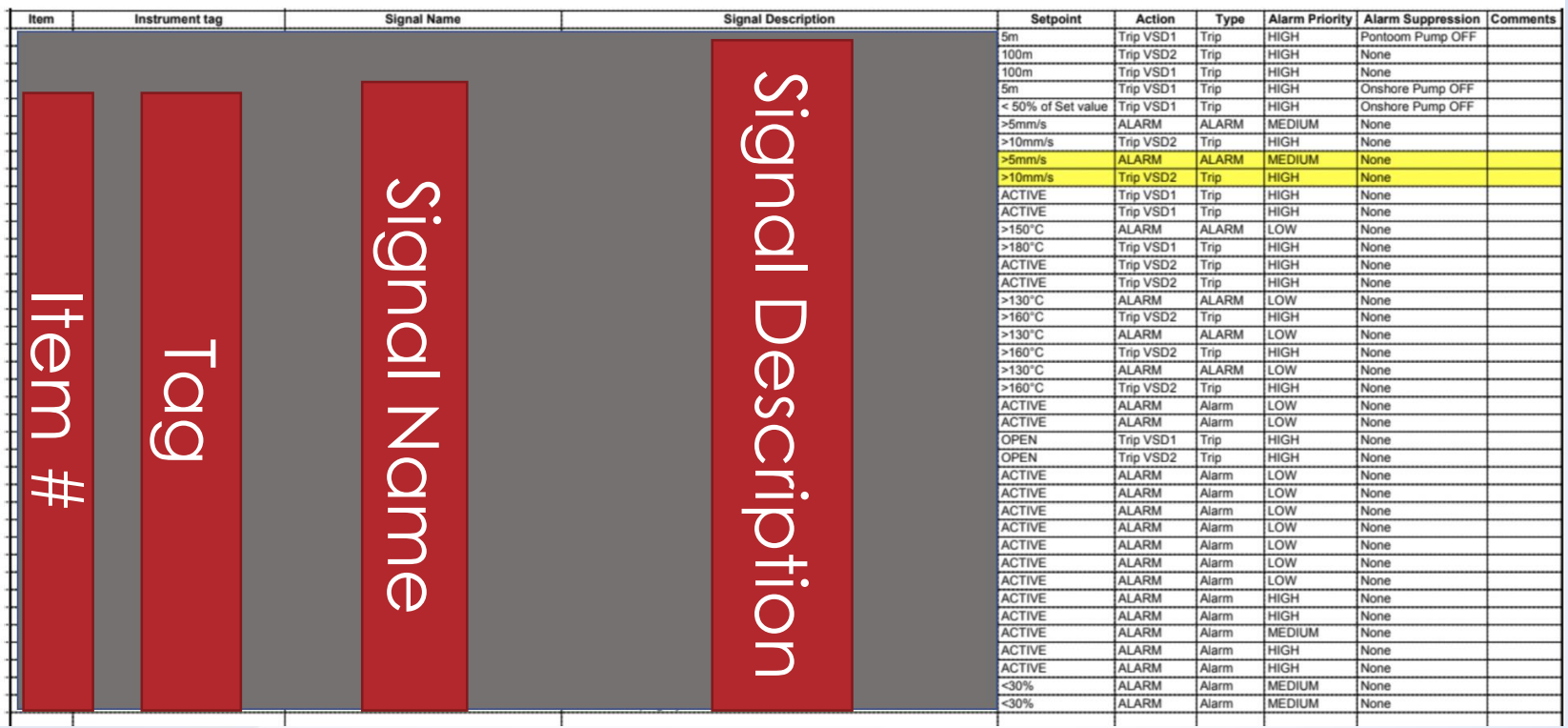
Picture retrieved from Bored Panda

Open Source Intel IT vs. OT

- Asset Inventories
- Network and Architecture Diagrams
- Historian Process Data
- Etc.



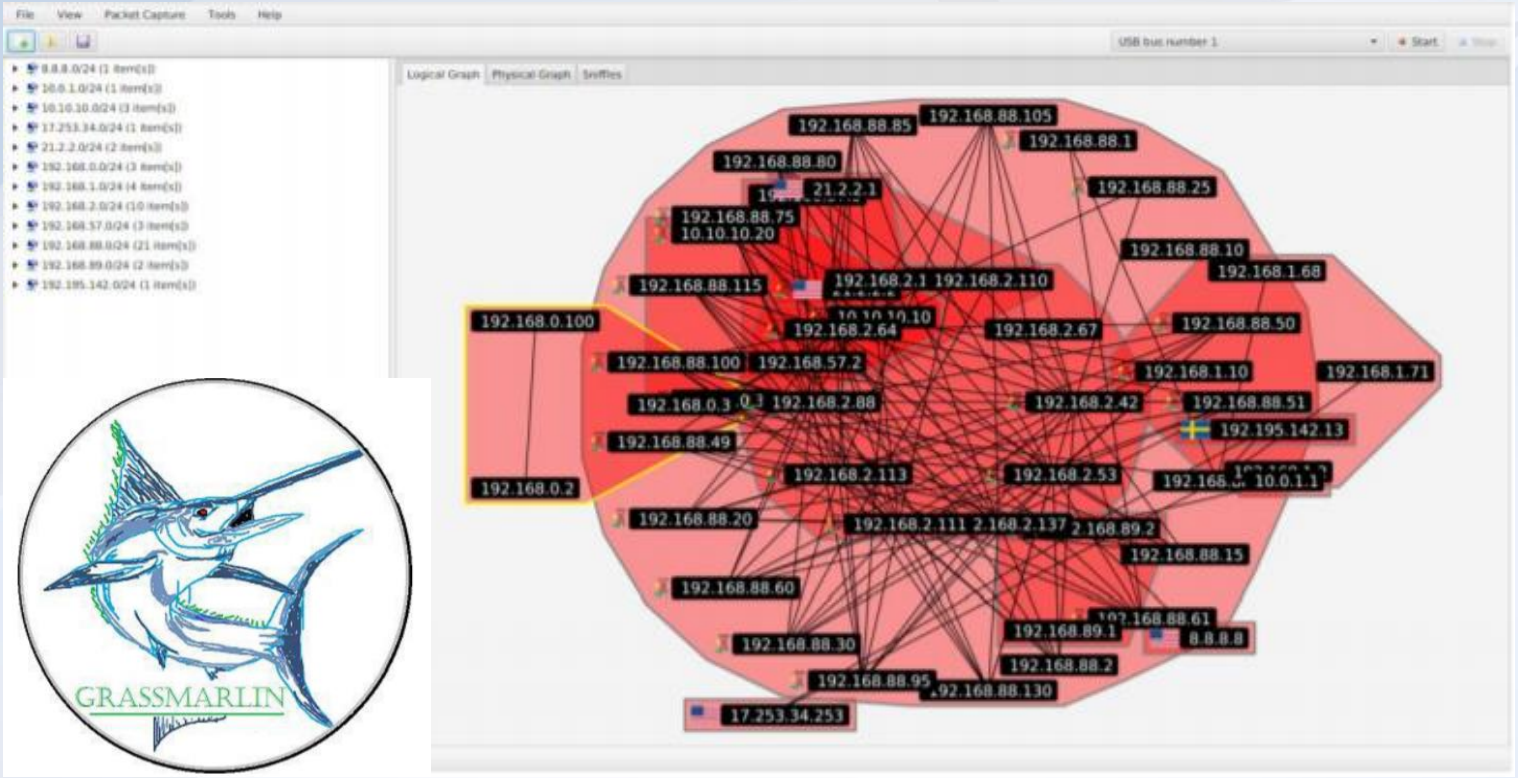
Asset Inventories



Item	Instrument tag	Signal Name	Signal Description	Setpoint	Action	Type	Alarm Priority	Alarm Suppression	Comments
				5m	Trip VSD1	Trip	HIGH	Pontoom Pump OFF	
				100m	Trip VSD2	Trip	HIGH	None	
				100m	Trip VSD1	Trip	HIGH	None	
				5m	Trip VSD1	Trip	HIGH	Onshore Pump OFF	
				< 50% of Set value	Trip VSD1	Trip	HIGH	Onshore Pump OFF	
				>5mm/s	ALARM	ALARM	MEDIUM	None	
				>10mm/s	Trip VSD2	Trip	HIGH	None	
				>5mm/s	ALARM	ALARM	MEDIUM	None	
				>10mm/s	Trip VSD2	Trip	HIGH	None	
				ACTIVE	Trip VSD1	Trip	HIGH	None	
				ACTIVE	Trip VSD1	Trip	HIGH	None	
				>150°C	ALARM	ALARM	LOW	None	
				>180°C	Trip VSD1	Trip	HIGH	None	
				ACTIVE	Trip VSD2	Trip	HIGH	None	
				ACTIVE	Trip VSD2	Trip	HIGH	None	
				>130°C	ALARM	ALARM	LOW	None	
				>160°C	Trip VSD2	Trip	HIGH	None	
				>130°C	ALARM	ALARM	LOW	None	
				>160°C	Trip VSD2	Trip	HIGH	None	
				>130°C	ALARM	ALARM	LOW	None	
				>160°C	Trip VSD2	Trip	HIGH	None	
				ACTIVE	ALARM	Alarm	LOW	None	
				ACTIVE	ALARM	Alarm	LOW	None	
				OPEN	Trip VSD1	Trip	HIGH	None	
				OPEN	Trip VSD2	Trip	HIGH	None	
				ACTIVE	ALARM	Alarm	LOW	None	
				ACTIVE	ALARM	Alarm	LOW	None	
				ACTIVE	ALARM	Alarm	LOW	None	
				ACTIVE	ALARM	Alarm	LOW	None	
				ACTIVE	ALARM	Alarm	LOW	None	
				ACTIVE	ALARM	Alarm	LOW	None	
				ACTIVE	ALARM	Alarm	LOW	None	
				ACTIVE	ALARM	Alarm	HIGH	None	
				ACTIVE	ALARM	Alarm	HIGH	None	
				ACTIVE	ALARM	Alarm	MEDIUM	None	
				ACTIVE	ALARM	Alarm	HIGH	None	
				ACTIVE	ALARM	Alarm	HIGH	None	
				<30%	ALARM	Alarm	MEDIUM	None	
				<30%	ALARM	Alarm	MEDIUM	None	

Image retrieved from open source sandboxing product.

Network and Architecture Diagrams



Images retrieved from "Passive Analysis of Process Control Networks" by Jennifer Janesko and GrassMarlin Github.

Historian Process Data

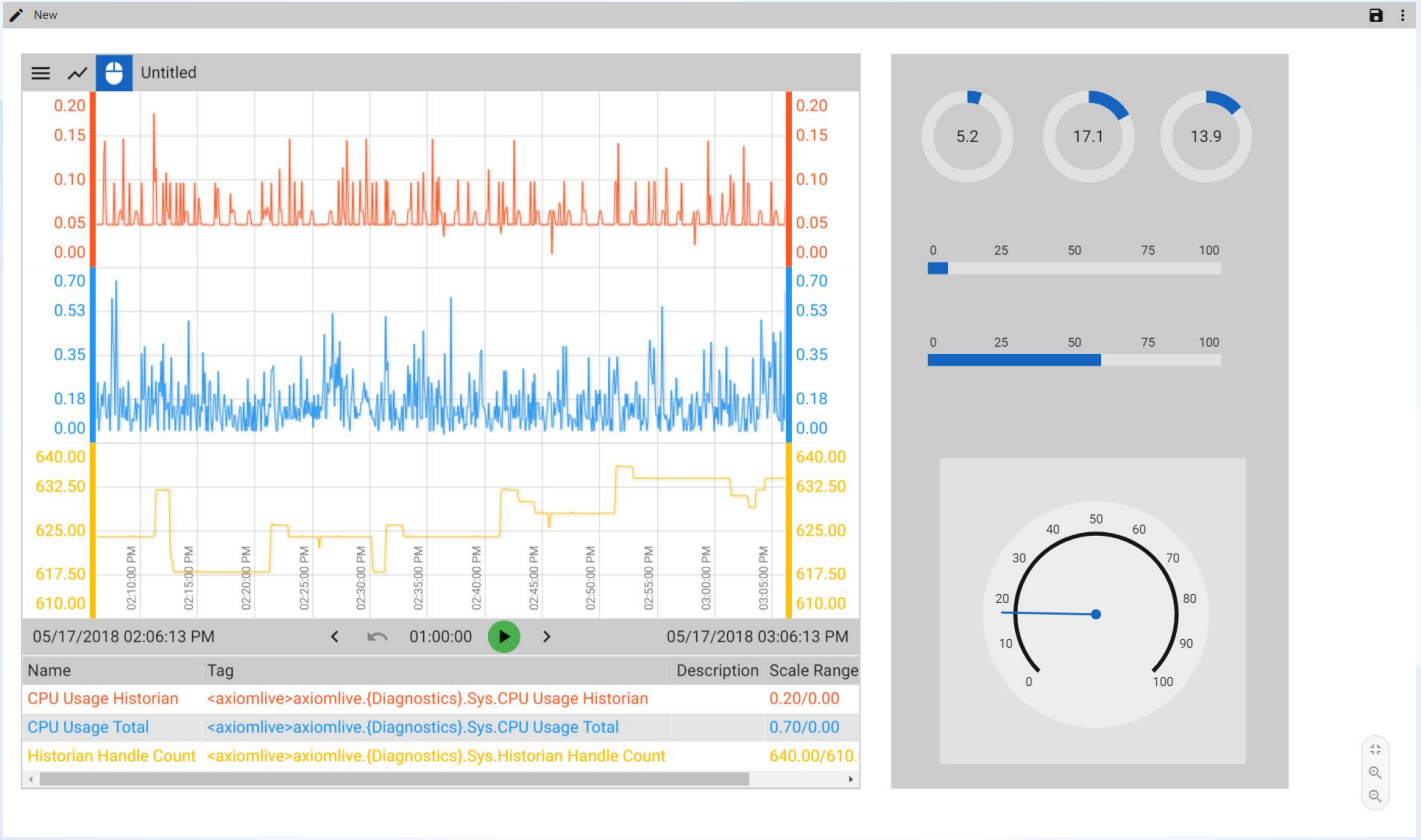


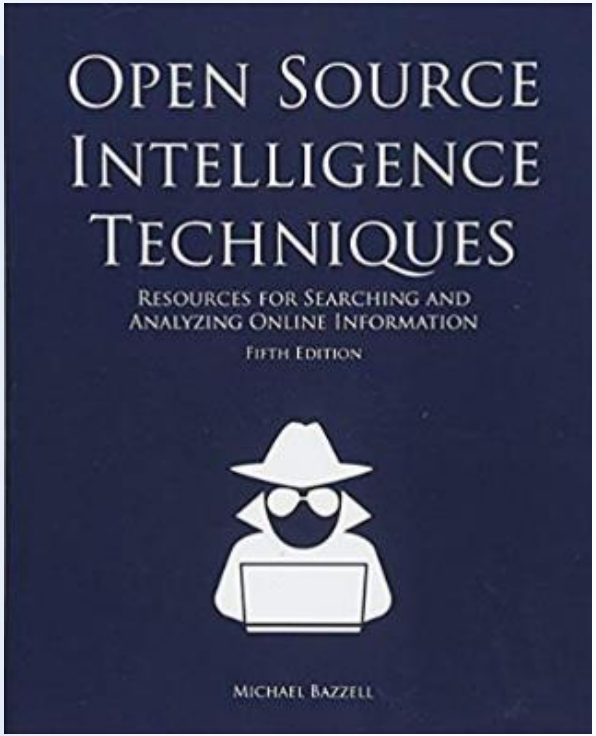
Image retrieved from Canary Labs blog..

Purpose of OT recon info

- Leverage upstream equipment suppliers to compromise the victim
- Identify third party vendors/contractors with access to OT network
- Learn about manufacturing environments/processes
- Social engineer key stakeholders to compromise credentials/documents

Picture retrieved from 02Varvara

Why Open Source For OT?



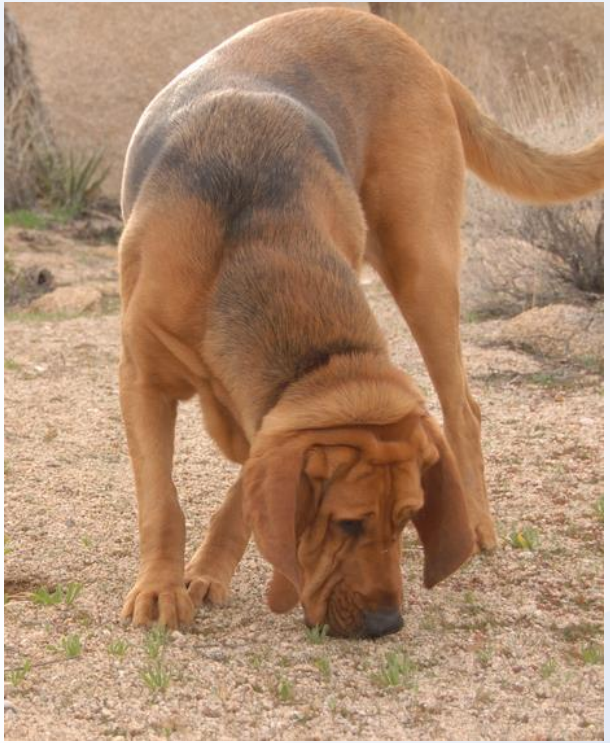
- Low cost
- Simple
- Legal(ish)
- Contextual
- Untraceable
- Fun and amazing

Picture retrieved from inteltechniques.com

The Mapping Marauders

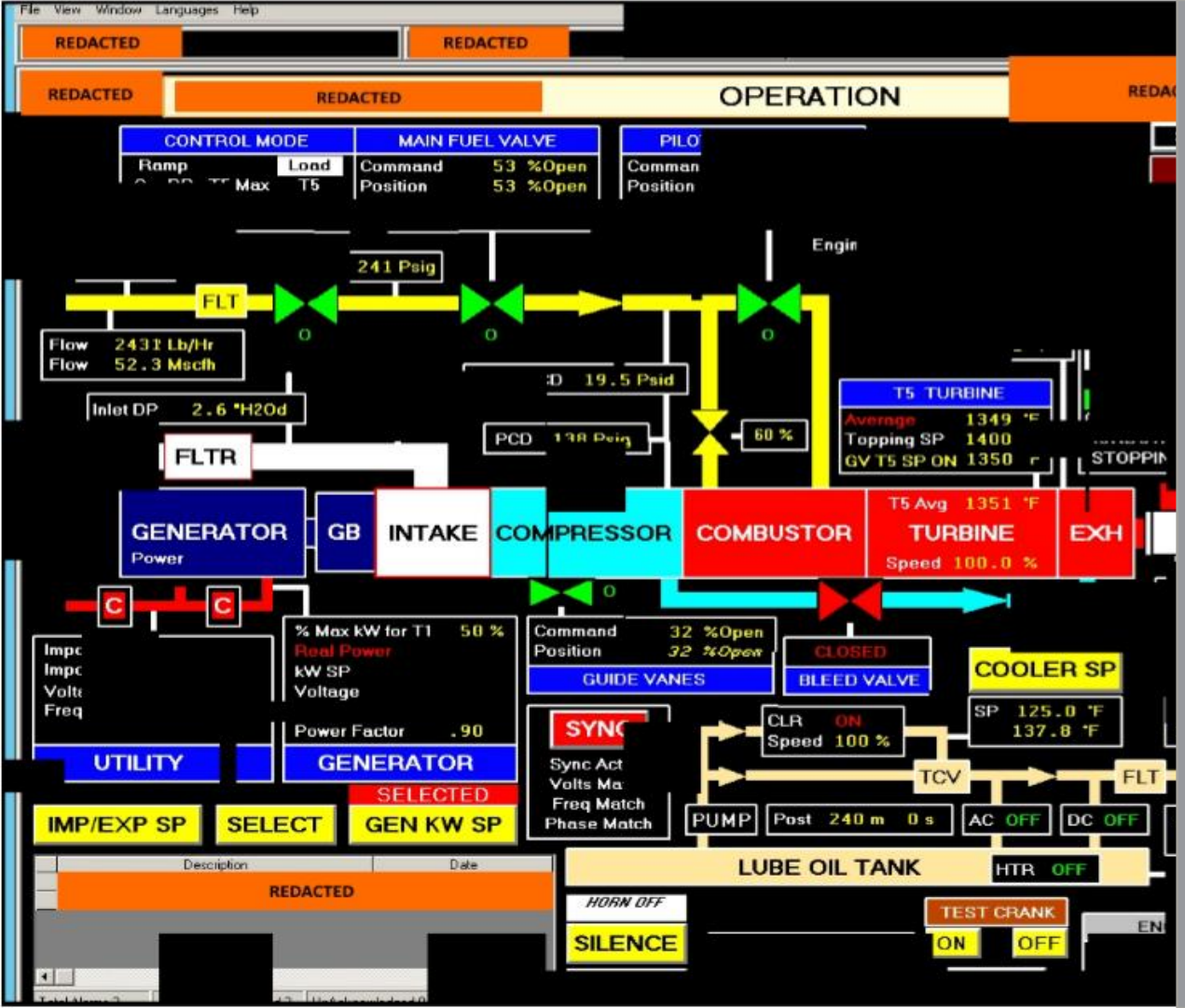
Hallmark Reconnaissance Campaigns

Threat Actor	Initial Detection	Known For
Sandworm Team	2009	Ukraine 2014-2016
Koala Team	2011	Havex
Temp.Isotope	2015	ICS CERT TA17-293A
Temp.Hermit	2017	Spear Phishing (Sep. 2017)
Temp.Veles?	~2014	TRITON



TEMP.Isotope

- Spear-phishing/web compromises to steal engineer credentials
- Group performs reconnaissance on corporate networks possibly to:
  - Steal intellectual property
  - Learn about targets' OT and plan disruptive operations

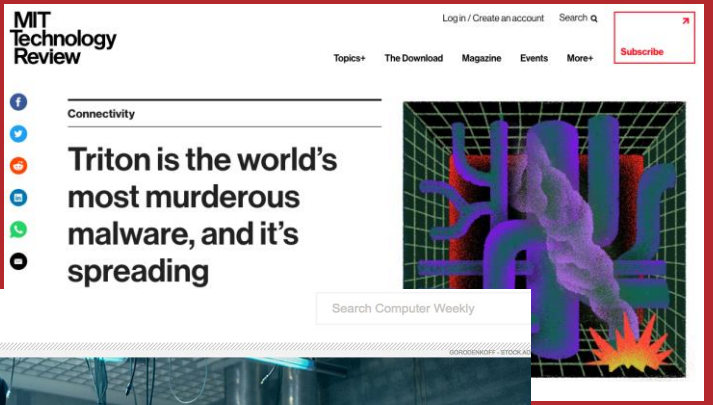


TEMP.Isotope findings:

HMI access
SCADA WIRING Diagram.pdf
SCADA PANEL LAYOUTS.xlsx
HR Website Images

Image from TA17-293A by ICS/US CERT.

What is TRITON?



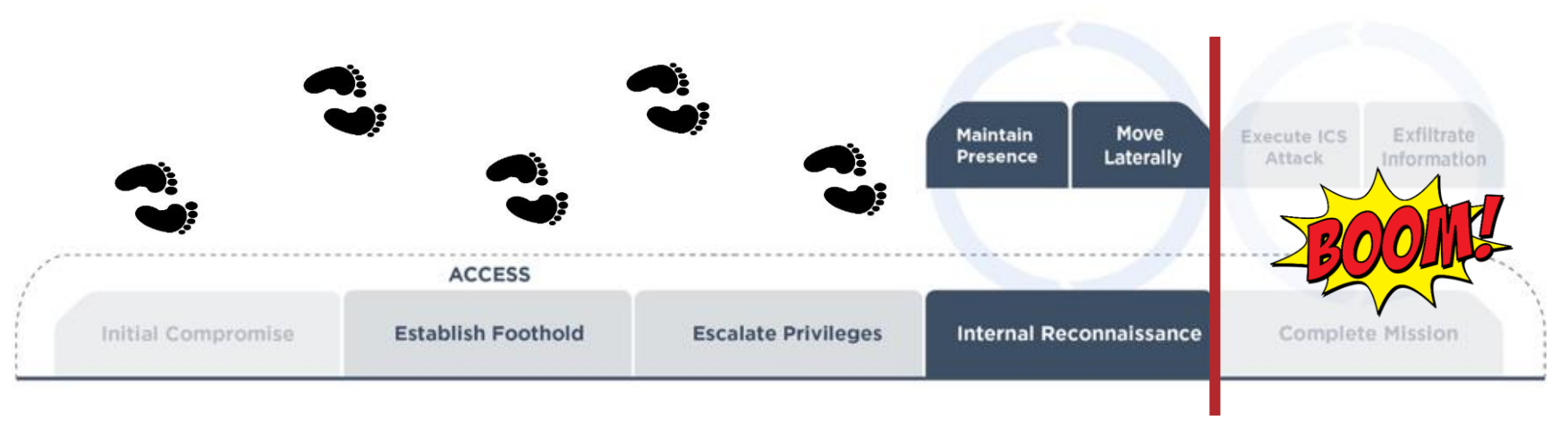
Schneider Exec on Why Triton Malware Still Matters

In 2017, so-called Triton malware attacked a safety system at an industrial facility in the Middle East. In this Q&A, Schneider Electric's director of cybersecurity explains why the incident should be a wake-up call to all industrial companies.

Written by Brian Buntz 6th September 2018

TRITON Attack Lifecycle

- TRITON attacker exploited Windows and Linux conduit systems to reach OT DMZ, plant backdoors, move to the DCS, SIS engineering station, and deploy TRITON to SIS controllers.



What happened on the SIS controller?

- SIS are last line of defense for a controlled process
- Actors accidently tripped safety systems, leading to safe but unplanned shutdown of systems

Image from Schneider Electric.

Totally Tubular Treatsie on TRITON/TriStation

TriStation is a proprietary protocol and there is no official information detailing its structure. It remains a mystery what resources were used by the actor to understand the protocol.

Value at 0x0	Message Type
1	Connection Request
2	Connection Response
3	Disconnect Request
4	Disconnect Response
5	Execution Command
6	Ping Command
7	Connection Limit Reached
8	Not Connected
9	MPS Are Dead
10	Access Denied
11	Connection Failed

A Guidebook for Fantastic OT Reconnaissance

Malware Analysis and Sandboxing Platforms

- Engineering Diagrams
- Configuration Documents
- Manuals and Operation Guidelines
- ICS software executables
- Purchasing Documentation

Online Retail Stores, Auction Sites, and Vendor Download Centers

Honeywell FMS

Koyo DirectSoft

Triconex communication PLC module

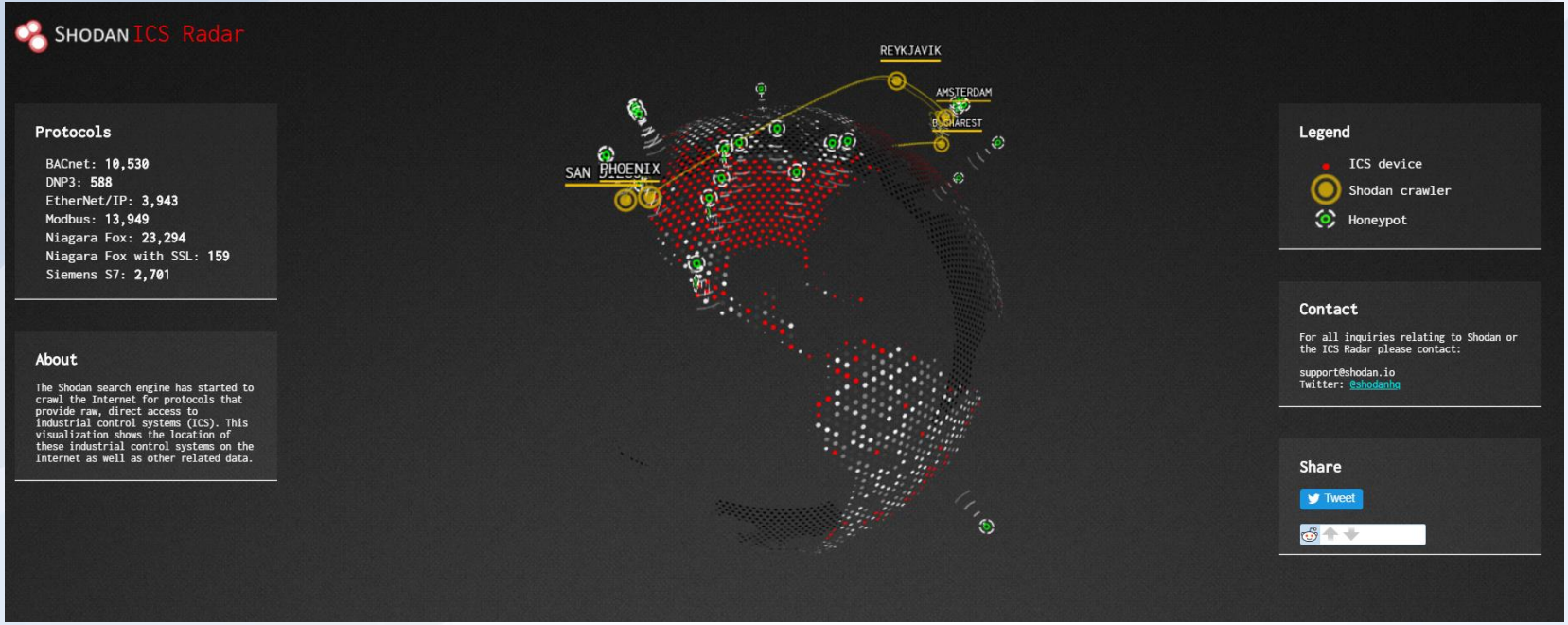
Fanuc industrial robot

Images from Kisspng, eBay and AutomationDirect

Manual Repositories and Vendor Websites

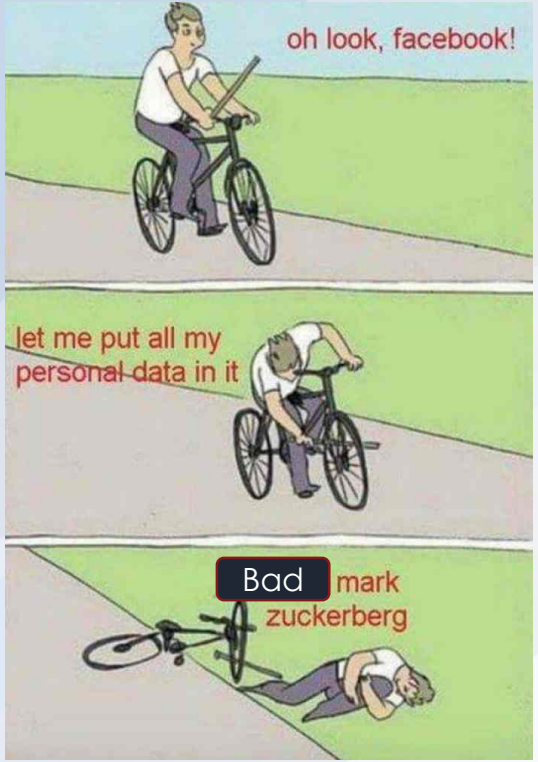
Honeywell manuals by category as presented on Manuals Directory

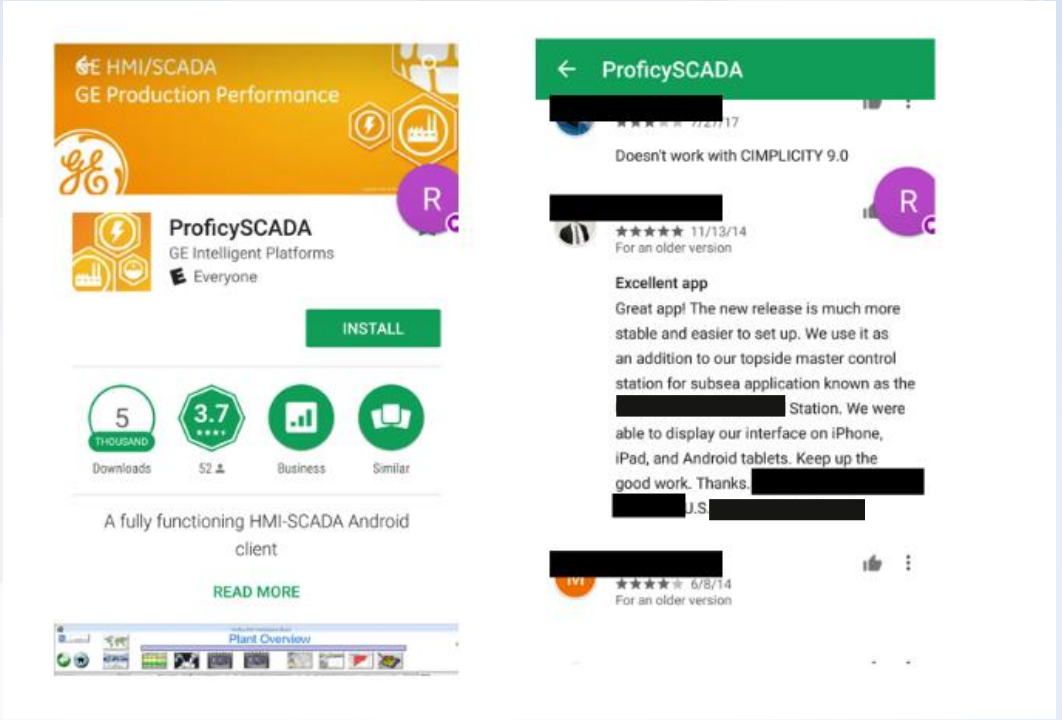
Specialized and Customer Search Engines



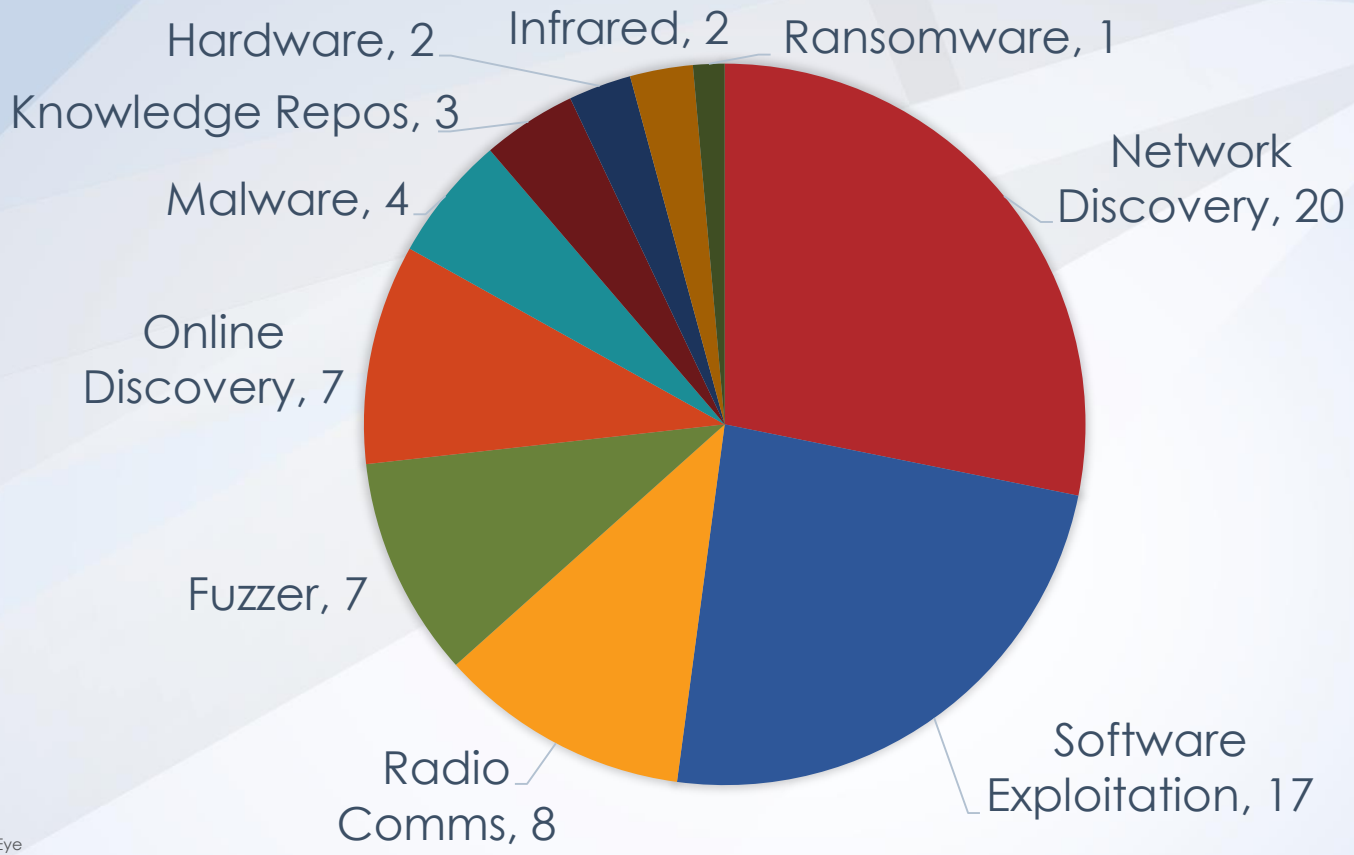
Shodan's own ICS Pew Pew map.

Social Media

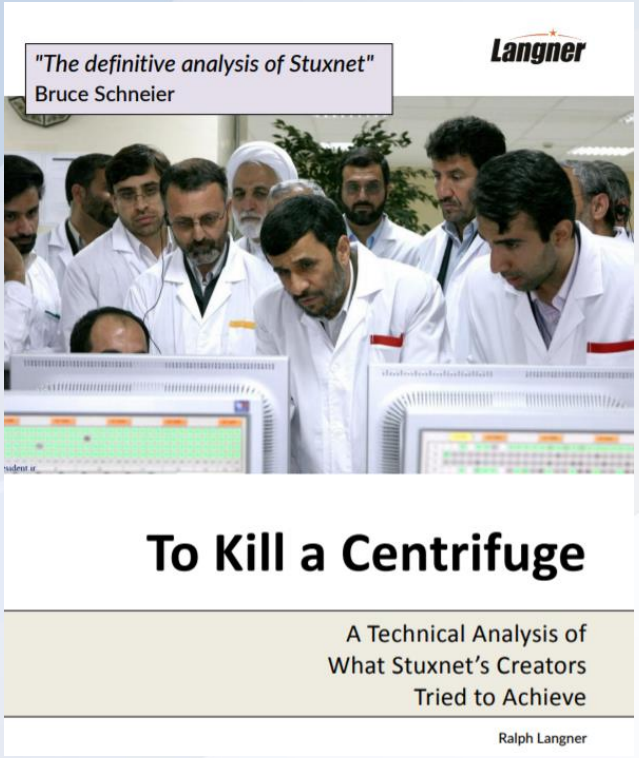


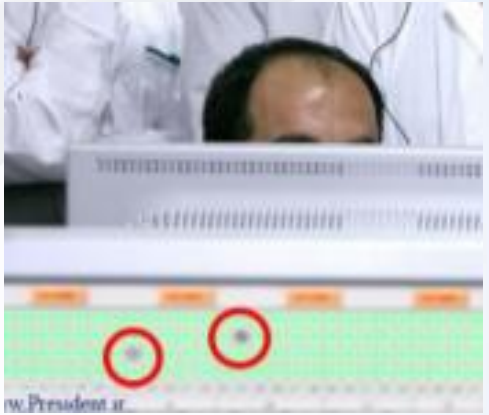


OT-specific Attack Tools



Some Hands-On OSINT…





Those Who Seek Shall Find...

1. Security through obscurity is dead

Picture retrieved from Flickr by lovecatz.

2. Please Mind What You Share

Picture retrieved from Flickr by gardenmey.

FIREEYE™

THANK YOU!

Danielkapellmann.z@fireeye.com
@Kapellmann