Scarlet OT

– OT adversary emulation for fun and profit –

Vic Huang

Sol Yang

Whoami

Vic Huang

UCCU Hacker / member

Vic is interested in Web/Mobile/Blockchain/Privacy issues.
He shared his research on CODE BLUE, HITB, HITCON, CYBERSEC several times.

Sol Yang

Independent researcher

Security Engineer. He is interested in OT security, Crypto, Malware.
He shared his research on CODE BLUE,CYBERSEC before.

Outline

- Introduction
- Adversary emulation
- Review , analyze and reproduce
- Scarlet OT
- Extend the attack chain from ICS malware attacks
- DEMO
- Adversary emulation tool for enterprise
- Takeaway

Introduction

and the background knowledge

Industrial Control System(ICS)

- Industrial control systems (ICS) is a major segment within the operational technology sector, which are used for control and monitor industrial processes

	Supervisory Control And Data Acquisition (SCADA)	Distributes Control Systems (DCS)
Staff computer	Human Machine Interface (HMI)	Engineering Workstation (EWS)
Controller	Programmable Logic Controller (PLC)	Controller + Control card
Architecture	Centralized control room for all the controllers	Different control room for each controller
Protocols	Public control protocols	Customized control protocols
Usage	Remote control	Fine control

Most of security research focus on SCADA

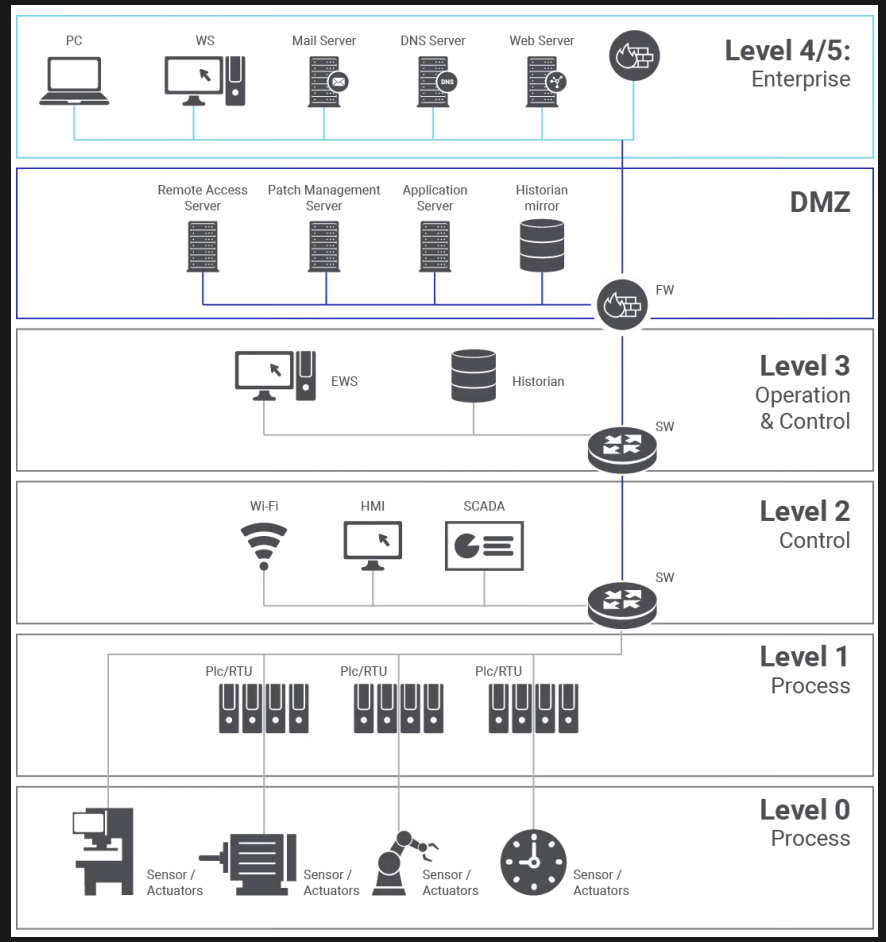
IT & OT

Information Technology (IT) system

Traditional and Known IT domain.
The area that is mostly like to connect to the internet. Most of attacks start from here

Operational technology(OT) system

From level 3 below , all is about manufacture process.
For level 3 and part of level 2 , there are some Windows system for management and monitoring.
From level 2 below , there are devices with special control system(digital or signal)



https://www.zscaler.es/resources/security-terms-glossary/what-is-purdue-model-ics-security

Adversary Emulation

and the existing tools

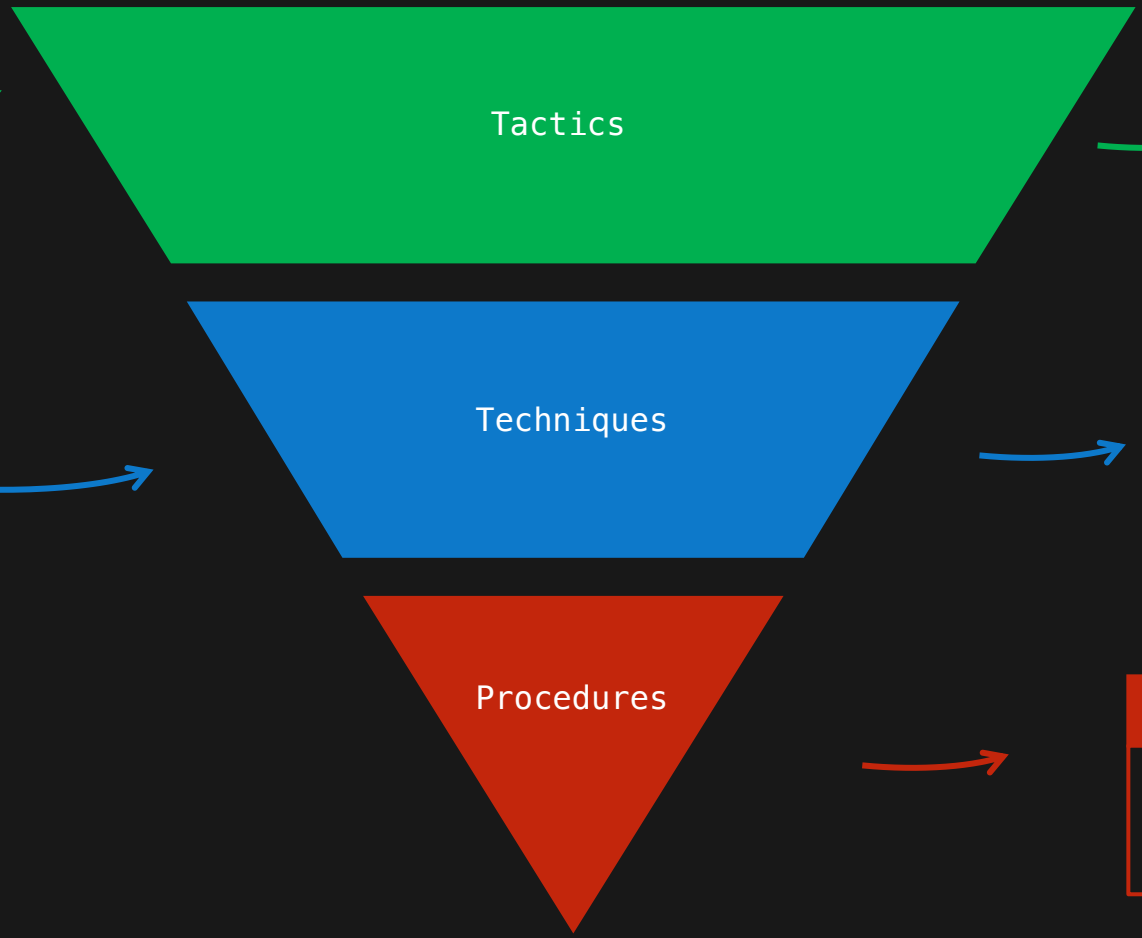
MITRE ATT&CK ICS Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

https://attack.mitre.org/matrices/ics/

TTPs

Execution
Change Operating Mode
Command-Line Interface
Execution through API
Graphical User Interface
Hooking
Modify Controller Tasking
Native API
Scripting
User Execution



Tactics

Highest level to describe attacks
Usually the target of a behavior

Techniques

techniques provide a more detailed description of the behavior in the context of a tactic

Procedures

procedures provide a lower-level, highly detailed attack of the behavior in the context of a technique

Adversary emulation tools

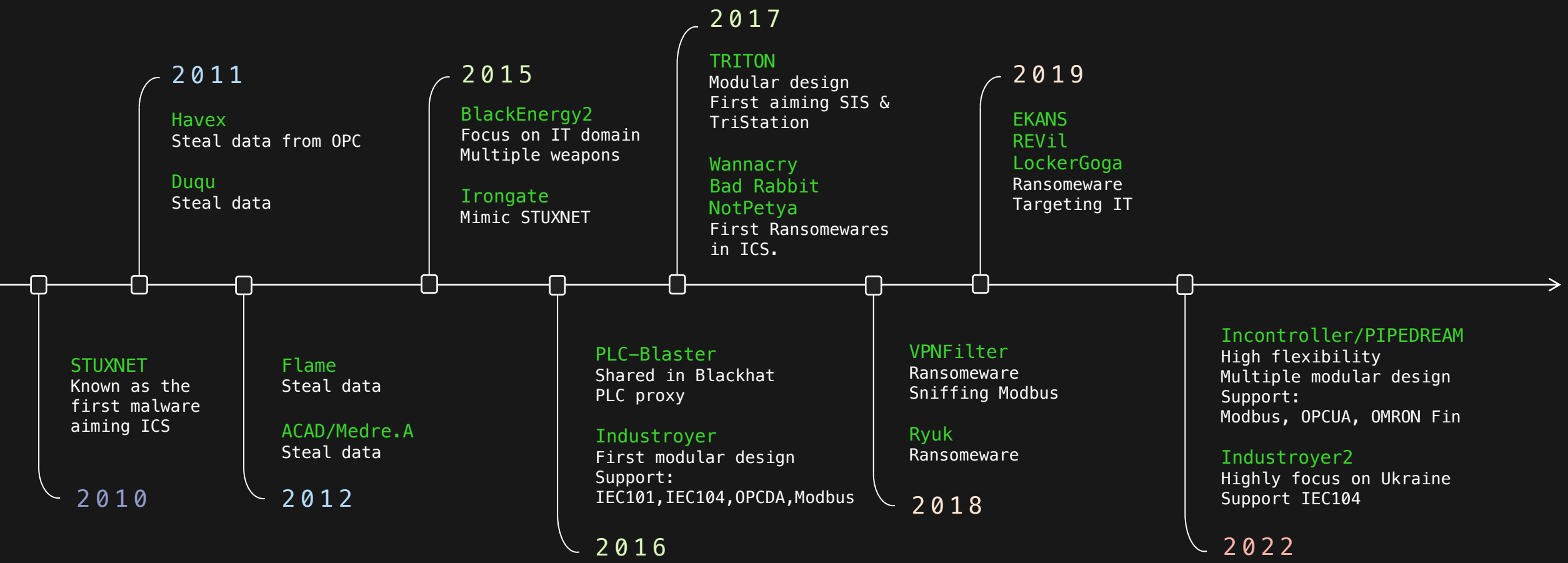
- Use known threat skills and automation to find vulnerabilities in enterprise
- a.k.a. Breach and Attack Simulation(BAS)
- Different from attack frameworks like Metasploit and isf , it focus more on automating instead human decision making and manually execution

Domain / Type	Commercial	Open source
IT	• SafeBreach • AttackIQ • XMCyber • Cymulate …	• APT Simulator • Atomic Red • Caldera • Infection Monkey …
OT focus on devices	• Otorio	?

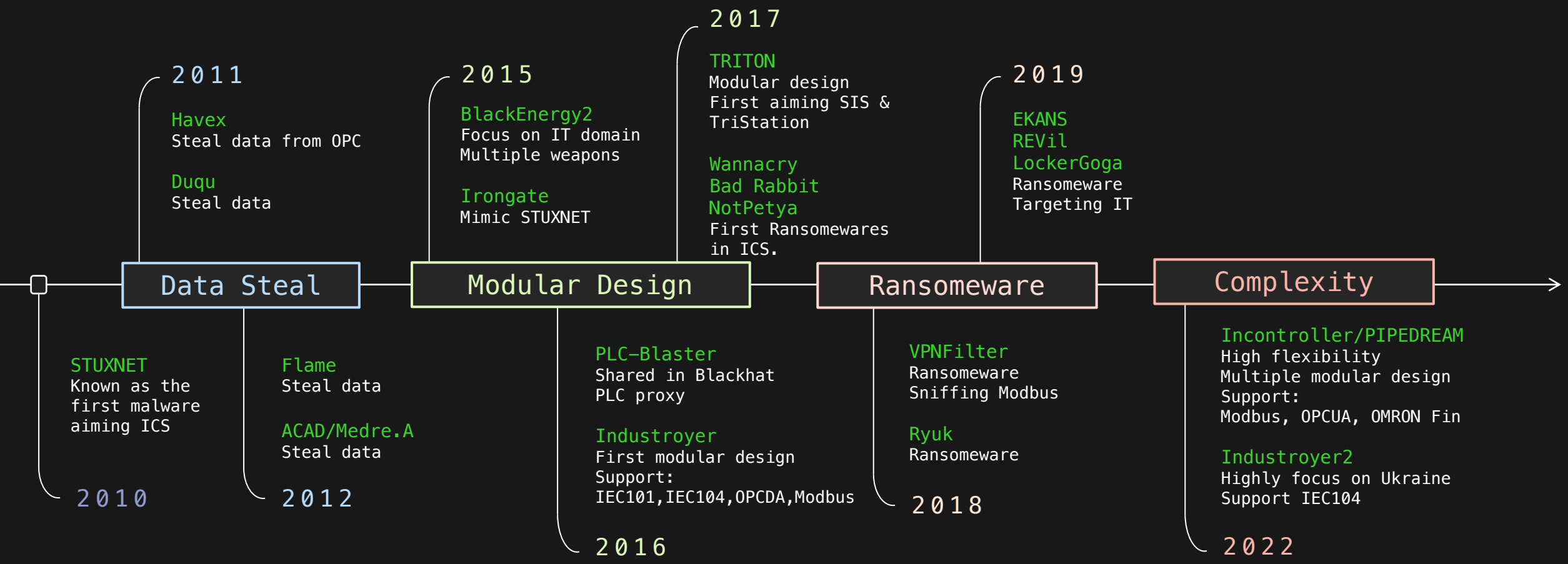
| Review | Analyze | Reproduce |

the ICS malwares in decade and make it as adversary emulation tool

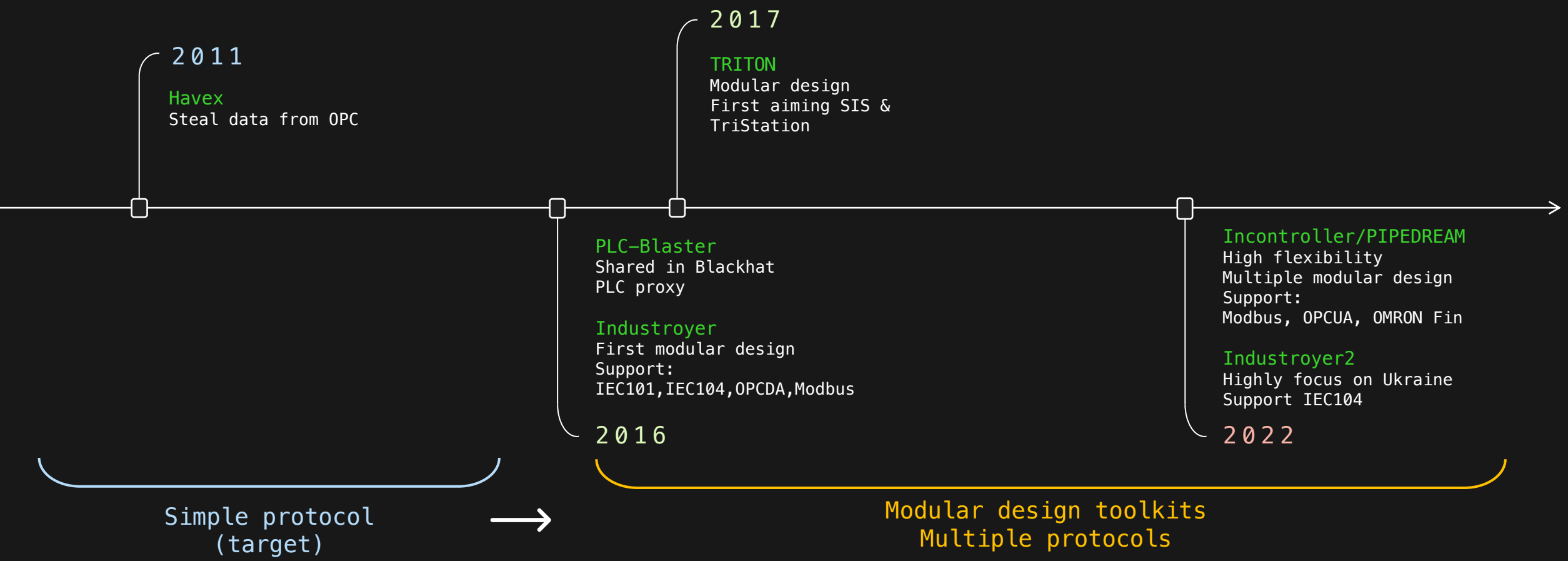
ICS Malware overview 2010 – 2022



ICS Malware overview 2010 – 2022



ICS Malware overview – protocols



Quick summary of malwares – 1

- 2 Main Targets
  - Information collection on devices
  - Break the factory or field operation

- 3 kinds of ICS Malwares
  - Worm

    Focus on spreading and information collection ,like Stuxnet and Havex
  - Ransomware

    Focus on finding specific process on HMI or IT devices and encrypt it to stop the factory operation , like Wannacry
  - Toolkit

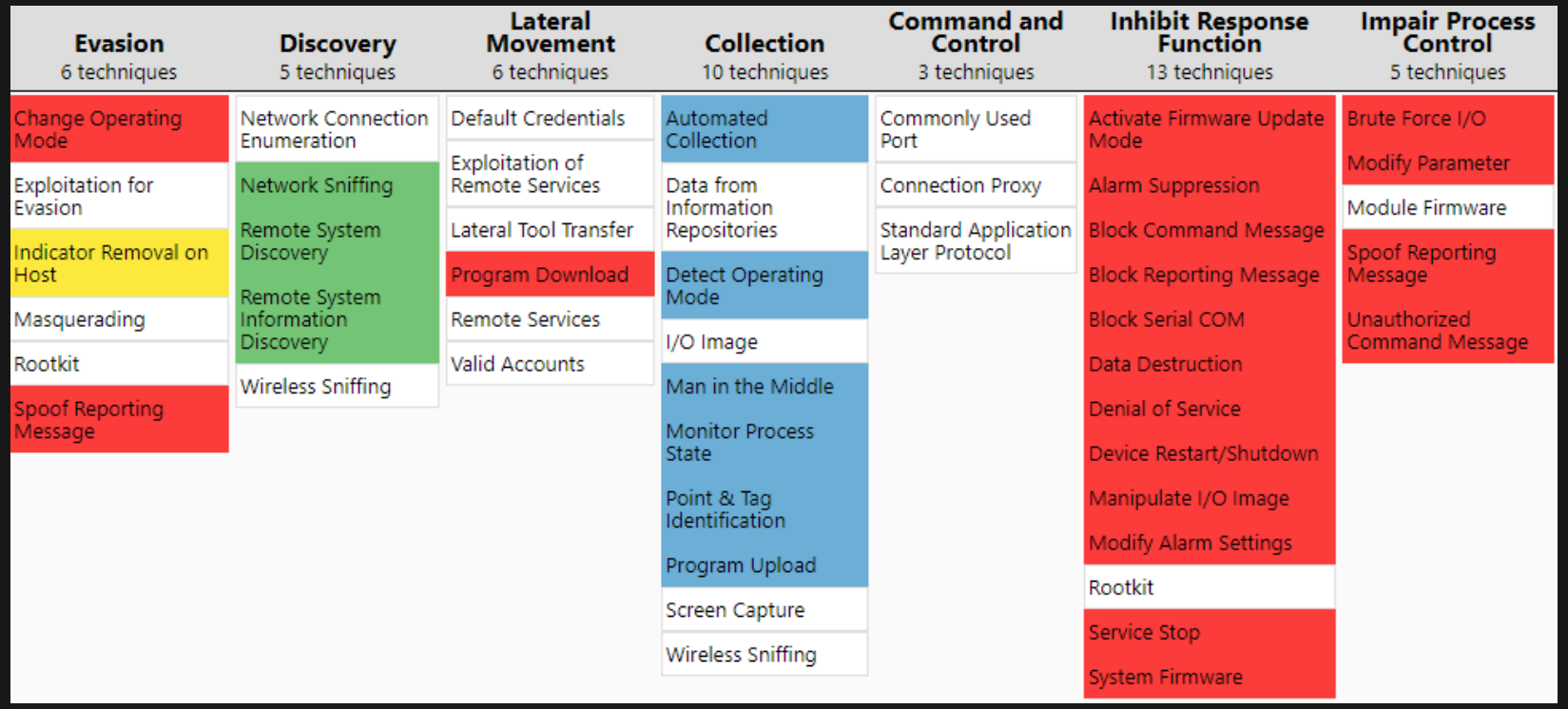
    Build in several scripts with modular design for different fields/devices they might face ,like PIPEDREAM

Quick summary of malwares – 2

- 4 points we want to share
  - Only some of malwares really attack or impact the devices like PLCs & IEDs , rest of them focus on Windows attacks.
  - We saw some hard-coded target IP address and tag name information in the malware source code, which is not normal for a malware know which IP & tag is the target before it goes in.
  - PLCs have 3 modes and need user PHYSICALLY change it by buttons. If the PLCs are in Run Mode, malwares should not able to impact them.
  - Normally HMI <-> PLC will be deployed as 1 to 1 or 1 to multiple IP address binding, which means PLC proxy attack vector like PLC-blaster(BHUS 2016) abusing the connection between PLCs might NOT work

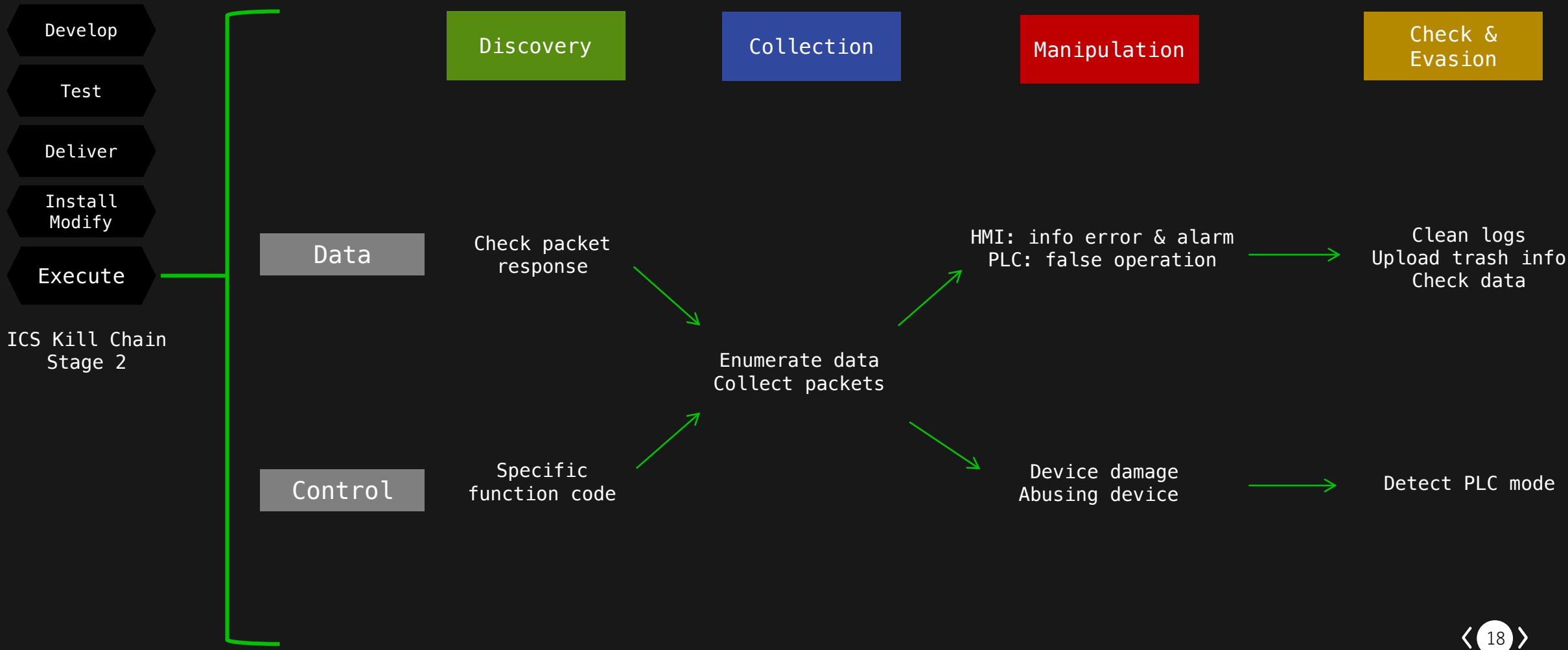
OT targeting attacks

- STUXNET
- HAVEX
- Industroyer
- Trisis
- Industroyer2
- Incontroller



Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 6 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques
Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O
Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter
Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware
Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message
Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message
Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction	
			Point & Tag Identification		Denial of Service	
			Program Upload		Device Restart/Shutdown	
			Screen Capture		Manipulate I/O Image	
			Wireless Sniffing		Modify Alarm Settings	
					Rootkit	
					Service Stop	
					System Firmware	

4 stages


Develop
Test
Deliver
Install
Modify
Execute
ICS Kill Chain
Stage 2
Discovery
Collection
Manipulation
Check &
Evasion
Data
Control
Check packet
response
Specific
function code
Enumerate data
Collect packets
HMI: info error & alarm
PLC: false operation
Device damage
Abusing device
Clean logs
Upload trash info
Check data
Detect PLC mode

4 stages – the main target

- Data
  - Data is given by devices and sensors.
  - If the data leaked or went wrong , (shown on HMI)human may make bad decisions.
  - Some protective actions may be triggered by weird data
  - Focus on data manipulation

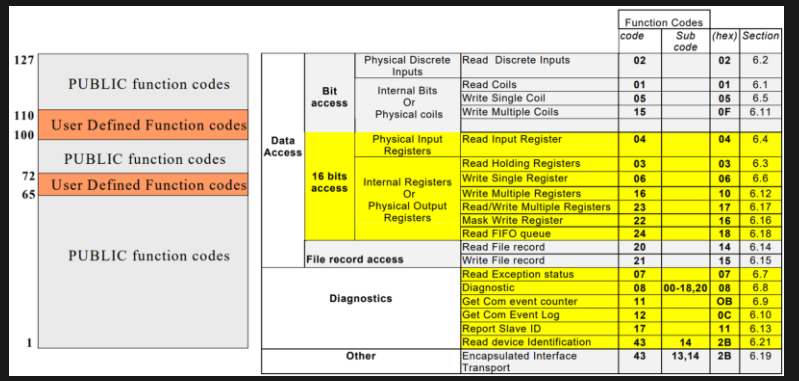
- Control
  - Control is the assigned command on devices.
  - If the wrong or malformed commands run on devices , devices do strange actions
  - Focus on device control

4 stages – (1) Discovery

- Data
  - Find the target by recognizing the response of the packet
  - 2017 TRITON broadcast specific packets and wait for the certain response

```
72      def detect_ip(self):
73          ip_list = set()
74          bc_sock = None
75          try:
76              bc_sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
77              bc_sock.setsockopt(socket.SOL_SOCKET, socket.SO_BROADCAST, 1)
78              bc_sock.settimeout(0.25)
79              TS_PORT = 1502
80              ping_message = '\x06\x00\x00\x00\x00\x88'
81              close_message = '\x04\x00\x00\x00\x010'
82              bc_sock.sendto(ping_message, ('255.255.255.255', TS_PORT))
```

- Control
  - Use known function code to find the target
  - Nmap use Modbus official function code 17 as scanning patterns , malware can use it ,too.
  - Also function code 42 is available.



				Function Codes code	Sub code	(hex)	Section
Data Access	Bit access	Physical Discrete Inputs	Read Discrete Inputs	02		02	6.2
		Internal Bits Or Physical coils	Read Coils	01		01	6.1
			Write Single Coil	05		05	6.5
			Write Multiple Coils	15		0F	6.11
	16 bits access	Physical Input Registers	Read Input Register	04		04	6.4
		Internal Registers Or Physical Output Registers	Read Holding Registers	03		03	6.3
			Write Single Register	06		06	6.6
			Write Multiple Registers	16		10	6.12
			Read/Write Multiple Registers	23		17	6.17
			Mask Write Register	22		16	6.16
			Read FIFO queue	24		18	6.18
	File record access		Read File record	20		14	6.14
			Write File record	21		15	6.15
Diagnostics			Read Exception status	07		07	6.7
			Diagnostic	08	00-18,20	08	6.8
			Get Com event counter	11		0B	6.9
			Get Com Event Log	12		0C	6.10
			Report Slave ID	17		11	6.13
			Read device Identification	43	14	2B	6.21
Other			Encapsulated Interface Transport	43	13,14	2B	6.19

4 stages – (2) Collection

- Data & Control
  - Collecting the data is the purpose
  - Collect data/response for next steps

- Examples
  - 2010 Stuxnet sniff centrifuge speed for 2 weeks for finding the max/min speed
  - 2011 Havex enumerate OPC tags and get values in the tags
  - 2018 VPNfilter sniff and record those Modbus packets

4 stages – (3) Manipulation

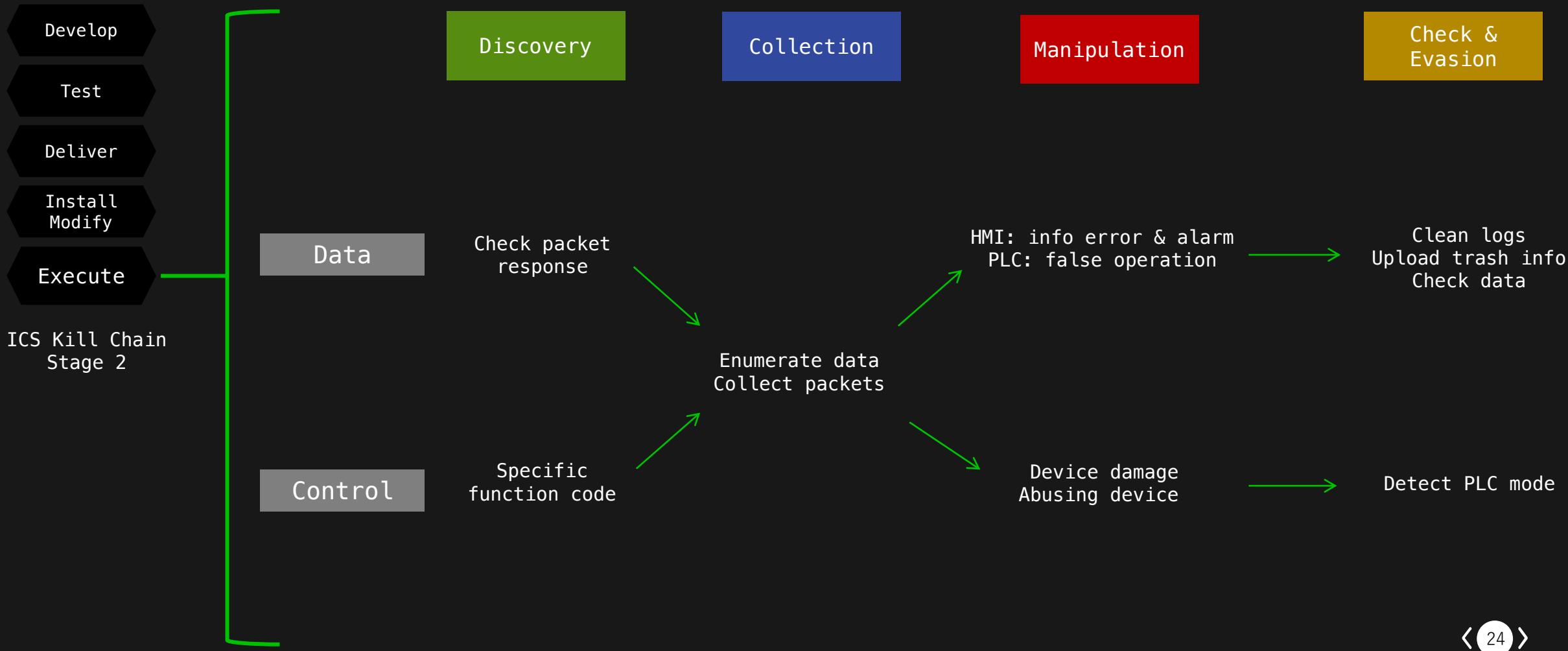
- Data
  - Data manipulation targeting
    - HMI
      - The info that shows on HMI screen , indirectly let human or system makes wrong decisions
      - Manipulate alarm
        - Wrong alarm → Alarm happens while devices without any problem
        - No alarm → No alarm are sent while devices go wrong
    - PLC
      - PLCs follow engineers code & ladder diagram , malformed parameter value lead to wrong code execution
- Control
  - Use CVEs or protocol functions to abuse, damage devices or stop the operation of factories
  - 2016 Industroyer use IEC-61850 to damage devices
  - 2017 TRITON use Tristation protocol to deploy malicious code on PLCs
  - 2022 PIPEDREAM use multiple protocols module to control devices

4 stages – (4) Check & Evasion (Option)

- Data
  - Evade detection and clean up logs
  - 2015 BlackEnergy use KillDisks to clean up Windows data
  - 2017 TRITON write meaningless code to overwrite the written malicious code

- Control
  - Malware will check the PLC or device status to confirm their malicious action actually works
  - 2017 TRITON detect PLC mode before and after uploading malicious code to PLC confirming the operation works

Quick summary



Scarlet OT

For fun and profit

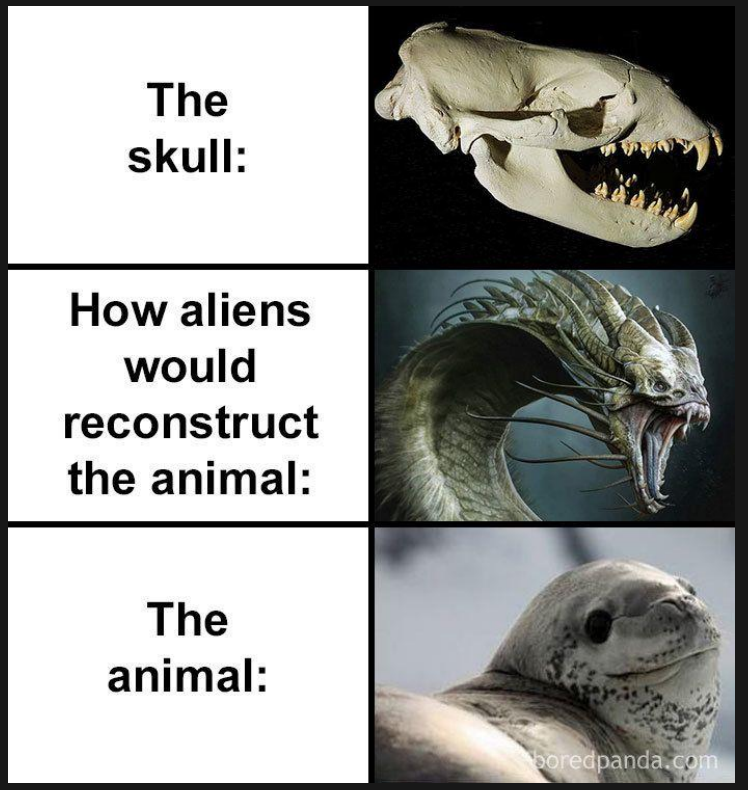
Overview in PLC marking ranks

Ranking	PLC Manufacturers	PLC Brand Names	Protocols
1	Siemens	Simatic	S7
2	Rockwell Automation	Allen Bradley	Ethernet/IP
3	Mitsubishi Electric	Melsec	Melsec
4	Schneider Electric	Modicon	Modbus
5	Omron	Sysmac	Omron
6	Emerson Electric (GE)	RX3i & VersaMax (GE Fanuc)	DeltaV, modbus
7	Keyence	KV & V-8000	Ethernet/IP, modbus
8	ABB (B&R Automation)	AC500 X20 & X90	IEC61850
9	Bosch	Rexroth ICL	CAN, modbus
10	Hitachi	EH & H	CODESYS, FL-NET PROTOCOL…

Reference: https://ladderlogicworld.com/plc-manufacturers/

Design Core

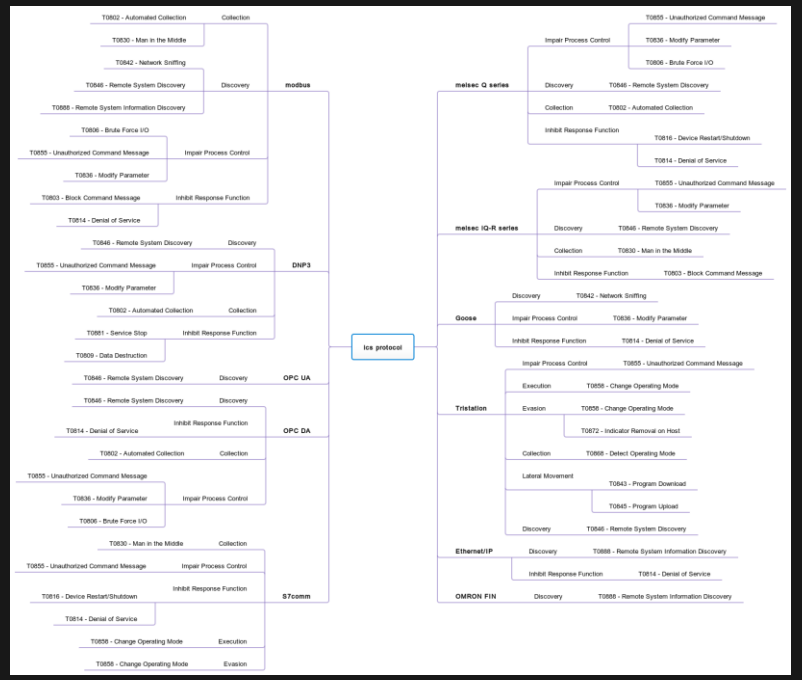
- Inspired by MITRE Engenuity ATT&CK® Evaluations for ICS 2021
- Reconstruct / Reproduce the malware actions by other protocols
- A flexible tool which you could
  - Automation adversary emulation
  - Pause & insert commands in the process
  - Customize the combinations of different protocol payloads
  - Customize the IT attacks for your own environment
- General purpose
  - Test the defense solutions
  - Mapping to ICS Matrix
  - Training



Credit : https://www.borepanda.com/

Scarlet OT

- Caldera plugin
- Support – 10 protocols , 23 techniques
- Reproduce/Reconstruct with 4 sub stages



Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 6 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques
Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O
Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter
Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware
Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message
Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message
Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction	
			Point & Tag Identification		Denial of Service	
			Program Upload		Device Restart/Shutdown	
			Screen Capture		Manipulate I/O Image	
			Wireless Sniffing		Modify Alarm Settings	
					Rootkit	
					Service Stop	
					System Firmware	

Example – Trisis

Trisis attack flow on Tristation

Trisis attack

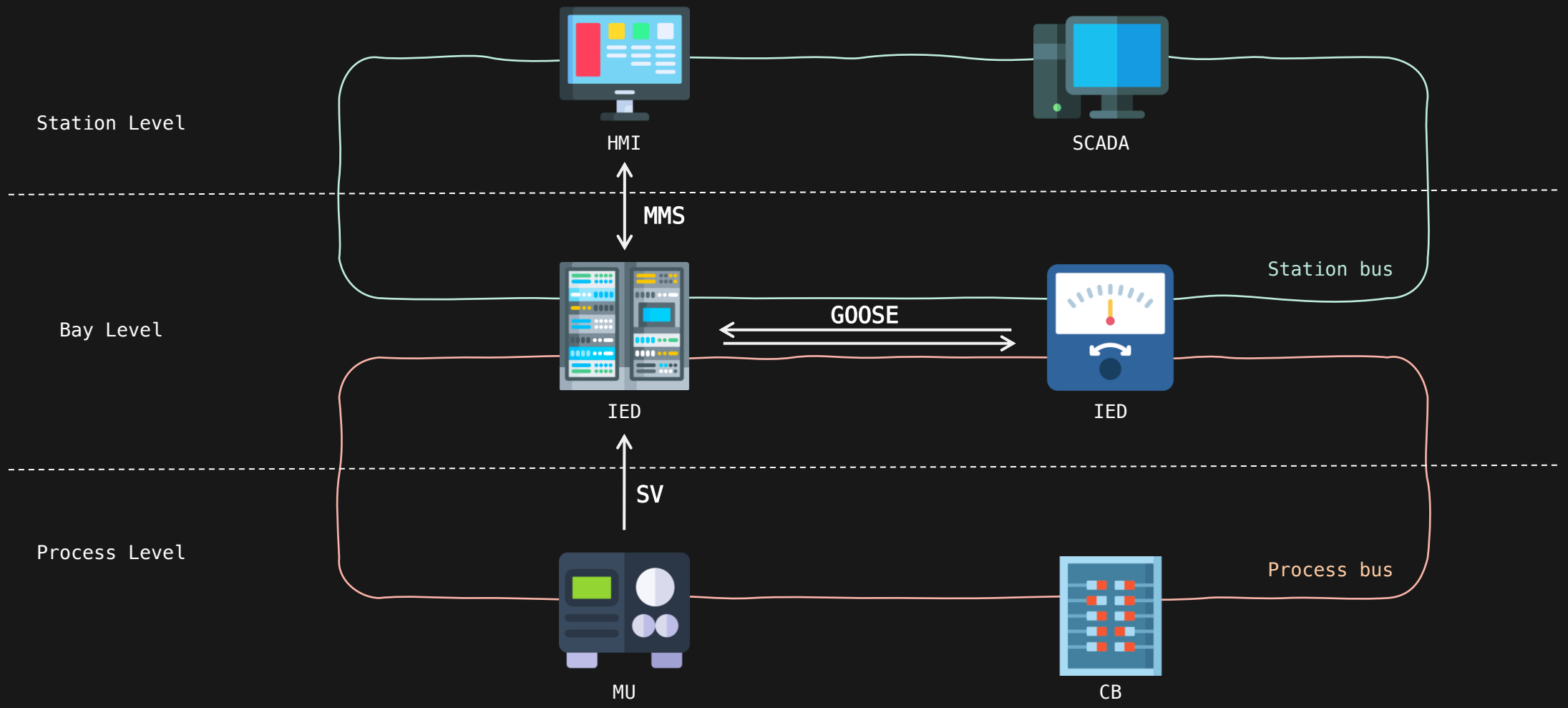
+ Add Ability | + Add Adversary | Objective: **default** | Change | Save Profile | Delete Profile

	Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup	
☰	1	Collect ARP details clone	discovery	Remote System Discovery						×
☰	2	Tristation hello packet discovery	discovery	Remote System Discovery						×
☰	3	Trisis - Detect Operation Mode	collection	Detect Operating Mode						×
☰	4	Trisis - Progaram upload	collection	Program Upload						×
☰	5	Trisis - Halt Program	execution	Change Operating Mode						×
☰	6	Trisis - Download malicious code to PLC	lateral movement	Program Download						×
☰	7	Trisis - Run Program	execution	Change Operating Mode						×
☰	8	Trisis - Upload Program and Download trash code to PLC	lateral movement	Program Download						×

Extend & Reconstruct

the attack chain from malware actions

IEC61850

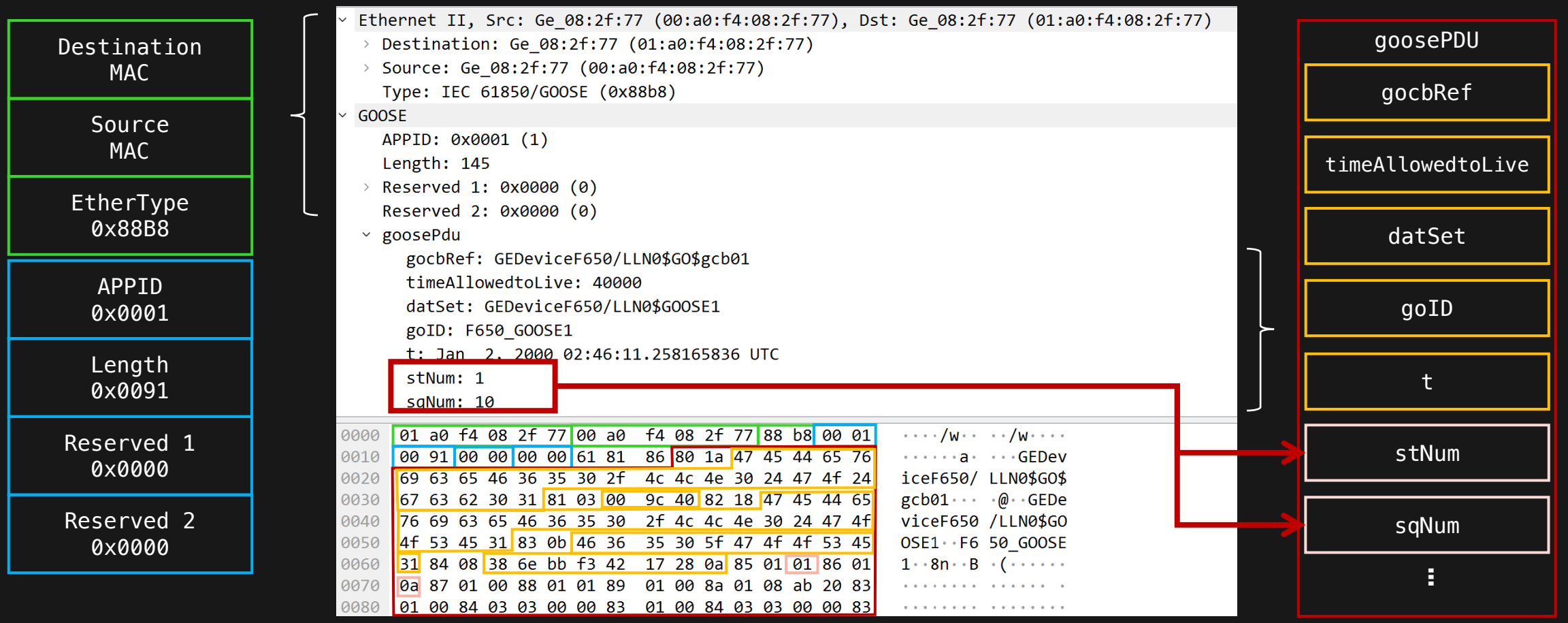

Station Level
HMI
SCADA
MMS
Station bus
Bay Level
GOOSE
IED
IED
SV
Process Level
Process bus
MU
CB

IEC61850 – GOOSE

- Publisher – Subscriber Mode
- Multicast the status or event

- T0 : Retransmission time in stable status (no event)
- T1, T2,.. Tn : Retransmission time in event happened status
- stNum : status number
- sqNum : sequence number

IEC61850 – GOOSE Frame

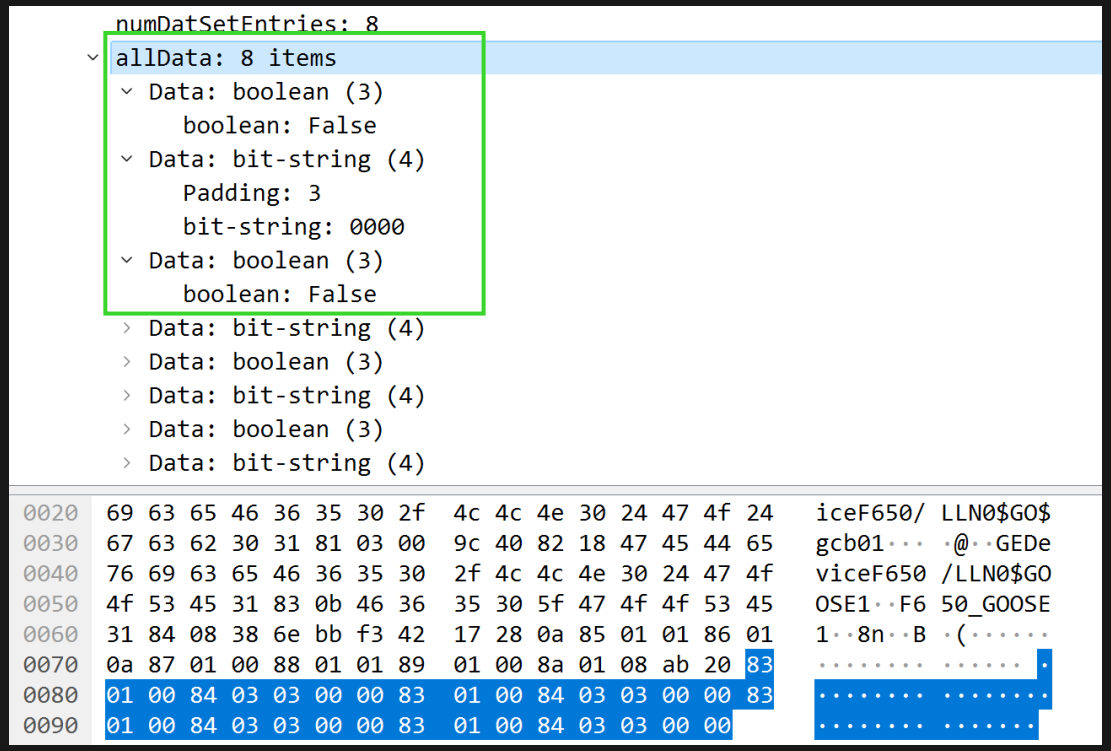


IEC61850 – GOOSE Frame

- allData
  - These data should stand for something
  - As an attacker, it’s not easy to understand the meaning

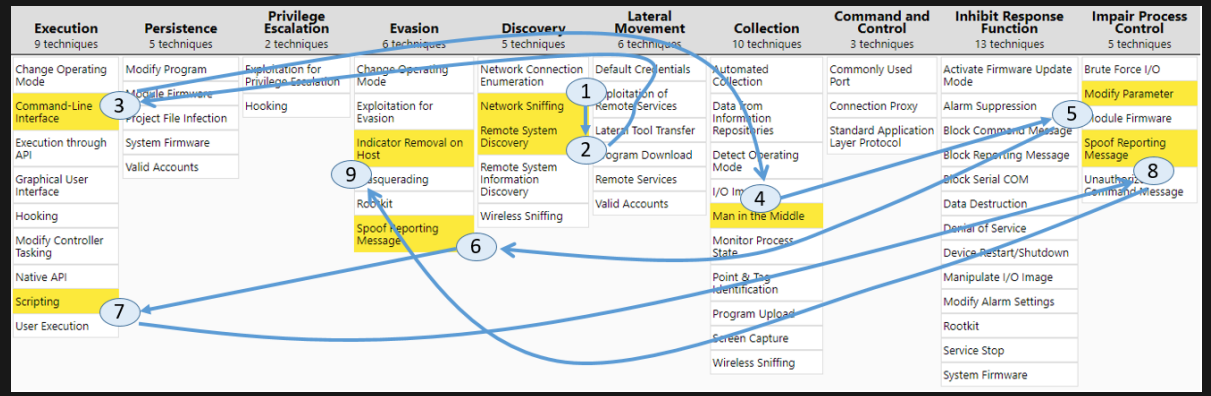
- “Effective” abusing way
  - It is hard if you want to manipulate specific device by guessing the value of these data
  - It’s not so hard to manipulate Boolean value

  –> make it reverse!! 😈



IEC61850 – GOOSE attacks

- Abnormal cases
  - Drop or Jump frame
  - Delay
  - Repeat or disorder frame
  - Manipulated stNum , sqNum ,data



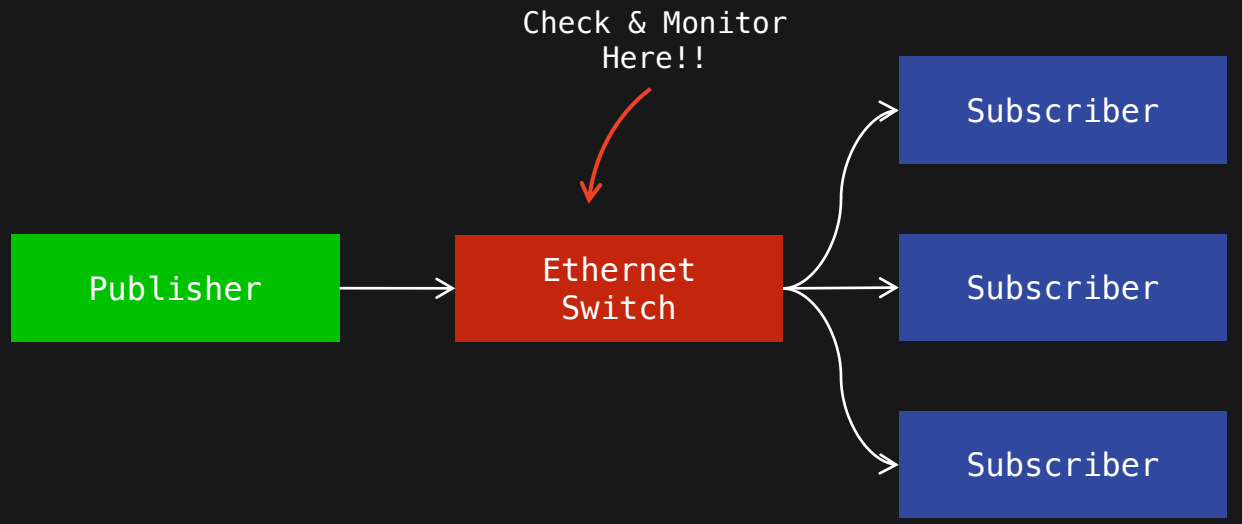
- Flow
  - Tshark capture the traffic
  - Analyze and destruct the frame and goosePDU
  - Edit the stNum , sqNum pretending as a new event or disorder..
  - Edit the data (especially boolean)
  - Send the malformed frame

Demo

:D

IEC61850 – GOOSE attack mitigation

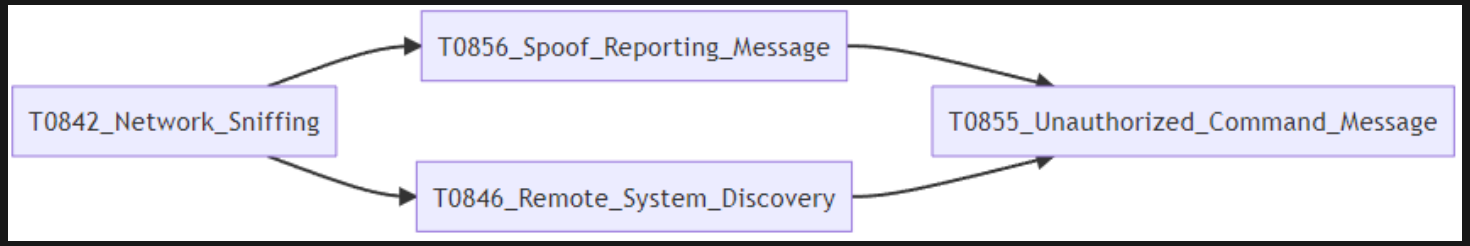
- From Attack
  - Denial of Service
  - Replay Attack
  - Data / sxNum Manipulation



- To Defense
  - Check the repeated/disordered frame
  - Confirm the publishing resource
  - Monitor the delay

IEC-61850 Attack Chain in demo

- 2 ways to do DoS(Power trip)
  - Fake/malformed Goose frame trigger the alert -> power trip
  - Malformed the MMS to make power trip(The device information is needed to malform specific MMS)



Discovery 5 techniques	Lateral Movement 6 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques
Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O
Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter
Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware
Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message
Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message
	Valid Accounts	Monitor Process State		Data Destruction	
		Point & Tag Identification		Denial of Service	
		Program Upload		Device Restart/Shutdown	
		Screen Capture		Manipulate I/O Image	
		Wireless Sniffing		Modify Alarm Settings	
				Rootkit	
				Service Stop	
				System Firmware	

Melsec Testbed

Device Name	Mitsubishi Electric – iQ-R Series Integrated Controller
Protocol	Melsec
Port	5002
Code of communication data	Binary Code
Network interface	3E Frame

https://www.mitsubishielectric.com/fa/products/cnt/plc/pmerit/index.html

Example – 3E Frame Format (READ D1000, D2000, D3000)

Format:

sub title	network code	plc no	io code	station code
length	timeout	command	sub command	number of devices
device number	device code

– : Fingerprint

– : Value that you should manipulate

```
0000   10 4b 46 28 db ed ec 21   e5 95 76 40 08 00 45 00
0010   00 4b b0 d3 40 00 80 06   00 00 0a 04 00 76 0a 04
0020   00 a8 45 0e 13 8a 60 dc   82 cb 0e b5 0b bf 50 18
0030   fa f0 15 63 00 00 50 00   00 ff ff 03 00 1a 00 04
0040   00 03 04 02 00 02 01 e8   03 00 00 a8 00 d0 07 00
0050   00 a8 00 b8 0b 00 00 a8   00
```

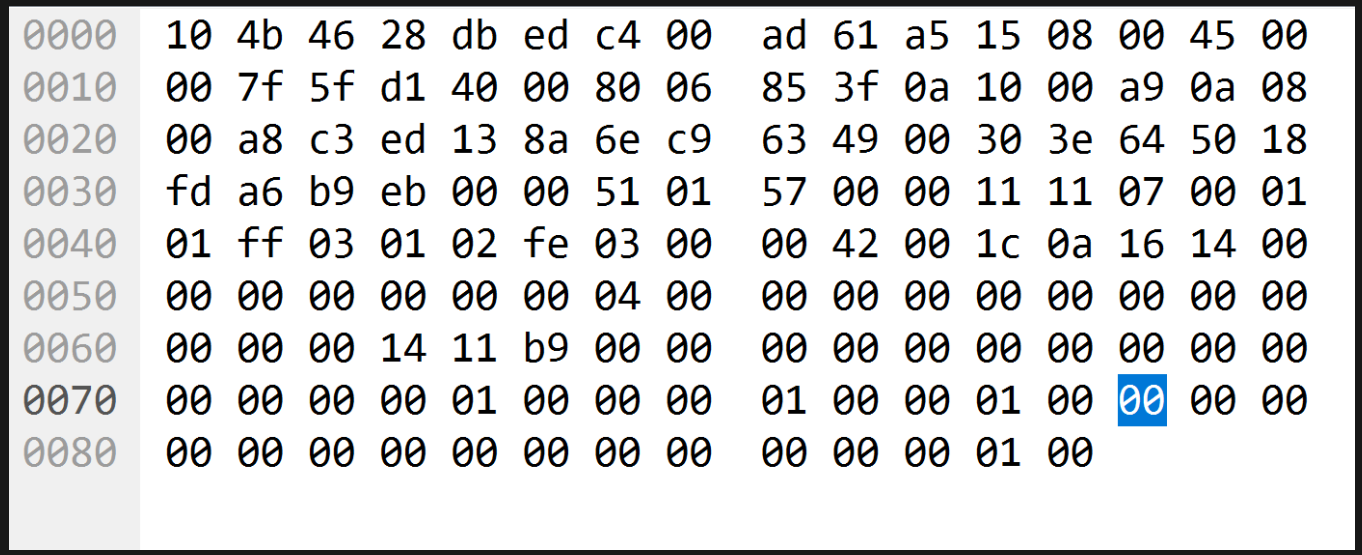
https://dl.mitsubishielectric.com/dl/fa/document/manual/plc/sh080008/sh080008ab.pdf

Example – 3E Frame Format (READ D1000, D2000, 3000)

Name	value	note
Sub title	50 00	Fingerprint
Network code	00	Fixed
PLC no	ff	Fixed
IO code	ff 03	Fixed
Station code	00	Fixed
Length	1a 00	Depends on data
Timeout	04 00	1 sec
Command	03 04	Random read
Sub command	02 00	iQ-R Series
Number of devices	02 01	Number of word and number of double word
Device number 1 & device code 1	e8 03 00 00 a8 00	D: A8, e8 03: 1000
Device number 2 & device code 2	d0 07 00 00 a8 00	D: A8, d0 07: 2000
Device number 3 & device code 3	b8 0b 00 00 a8 00	D: A8, b8 0b: 3000

Melsec Command Message

- 00 : Air compressor on
- 01 : Air compressor off
- 0a : Valve on
- 0b : Valve off



```
0000  10 4b 46 28 db ed c4 00  ad 61 a5 15 08 00 45 00
0010  00 7f 5f d1 40 00 80 06  85 3f 0a 10 00 a9 0a 08
0020  00 a8 c3 ed 13 8a 6e c9  63 49 00 30 3e 64 50 18
0030  fd a6 b9 eb 00 00 51 01  57 00 00 11 11 07 00 01
0040  01 ff 03 01 02 fe 03 00  00 42 00 1c 0a 16 14 00
0050  00 00 00 00 00 00 04 00  00 00 00 00 00 00 00 00
0060  00 00 00 14 11 b9 00 00  00 00 00 00 00 00 00 00
0070  00 00 00 00 01 00 00 00  01 00 00 01 00 00 00 00
0080  00 00 00 00 00 00 00 00  00 00 00 01 00
```

- We have analyzed the data first so that we know the [offset:value]
- In the blind attacking condition & automation ,enumerate [offset:value] is one of the reasonable actions

Reconstruct STUXNET on Melsec

- STUXNET
  - Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart

- In the factory
  - There are pre-defined range for certain value on devices for safe operation
  - If the value getting out of control , the emergency mode will be triggered and forcing the device shutdown

- As an attacker
  - Make(or cheat the monitoring system) the value out of safe range is a way to break the operation or damage the devices

Melsec Attack Chain

- ARP Scan -> Find Devices -> Check version -> read data -> change parameter -> send control -> Dos

Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 6 techniques	Collection 10 techniques	Command and Control 3 techniques	Inhibit Response Function 13 techniques	Impair Process Control 5 techniques
Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O
Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter
Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Module Firmware
Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message
Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message
Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction	
			Point & Tag Identification		Denial of Service	
			Program Upload		Device Restart/Shutdown	
			Screen Capture		Manipulate I/O Image	
			Wireless Sniffing		Modify Alarm Settings	
					Rootkit	
					Service Stop	
					System Firmware	

Demo

:D

S7 Attack Chain

- ARP Scan -> Find Devices -> Sniff Packets -> Adversary-in-the-Middle

Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
	Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
	Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
		Point & Tag Identification		Denial of Service		Loss of Safety
		Program Upload		Device Restart/Shutdown		Loss of View
		Screen Capture		Manipulate I/O Image		Manipulation of Control
				Modify Alarm Settings		Manipulation of View
				Rootkit		

Demo

:D

Adversary emulation tool for enterprise

- Even it’s an emulation, the operations could damage your devices
  - CVEs
  - DoS
  - Abnormal operation

- If enterprise don’t have beta environment, Digital twin may help
  - Pros
    1. No damage in production environment
    2. Good for the unknown vulnerabilities discovery
    3. No limitation on testing time
  - Cons
    1. Hard to 100% make a digital twin
    2. Take a lot of time for simulating a single device to digital version(ex. Firmware debug , bootloader revision)
    3. The reaction of commands may not be same as the real device

Takeaway

- Adversary emulation
  - Use known threat skills and automation to find vulnerabilities
- According to the ICS malwares and their targets, we found a trend
  - Single target → Modular design → Ransomeware → More complex(?)
- Summarize the attack flow in OT
  - Discovery → Collection → Manipulation → Check & Evasion
- Extend / Reproduce the attacks
  - OPC, IEC61850, Melsec
- Adversary emulation for Enterprise
  - Digital twin

Thanks for listening

Vic Huang

Sol Yang