The 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021)

The Rise of ICS Malware: A Comparative Analysis

October 08, 2021

Yassine Mekdad[1], Giuseppe Bernieri[2], Mauro Conti[2], Abdeslam El Fergougui[1]

[1]Moulay Ismail University of Meknes, Morocco.
[2]University of Padua, Italy.

y.mekdad@edu.umi.ac.ma

UNIVERSITÀ DEGLI STUDI DI PADOVA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

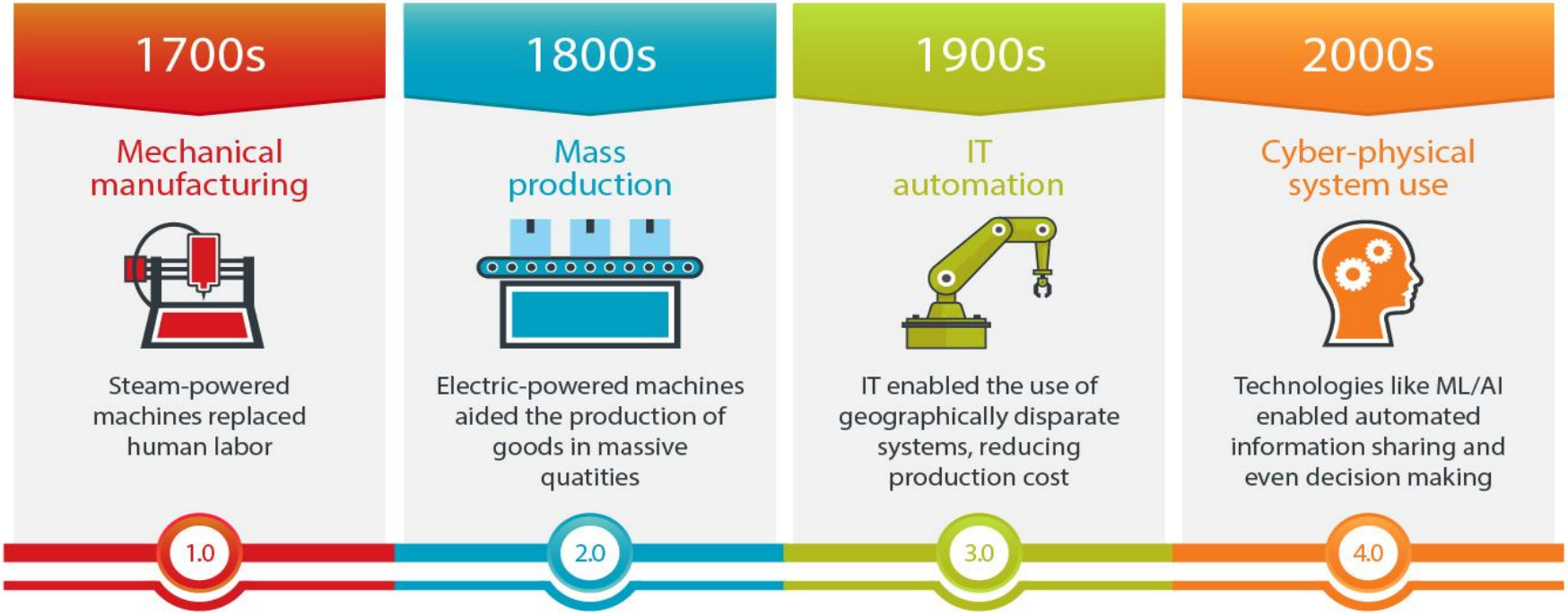
Outline

- Introduction
- Motivations
- Background
- Proposed Framework
- Evaluation and Results
- Conclusions

Introduction (1/2)

The industrial revolution from **Industry 1.0** to **Industry 4.0**

- Nuclear facilities
- Water systems
- Energy
- Chemical
- Emergency services
- Critical manufacturing
- Healthcare
- Transportation systems



Source: TrendMicro

Introduction (2/2)

- Legacy industrial control systems are **NOT** built with a security-by-design approach.
- ICS environments are prone to ***Hardware*** and ***Software*** vulnerabilities.
- In the past decade, the world has witnessed a **rise** in industrial malware.

Motivations

Research Questions:

- What is our understanding of the existing ICS Malware threats and their development during the past decade?
- How do adversaries operate in OT networks?

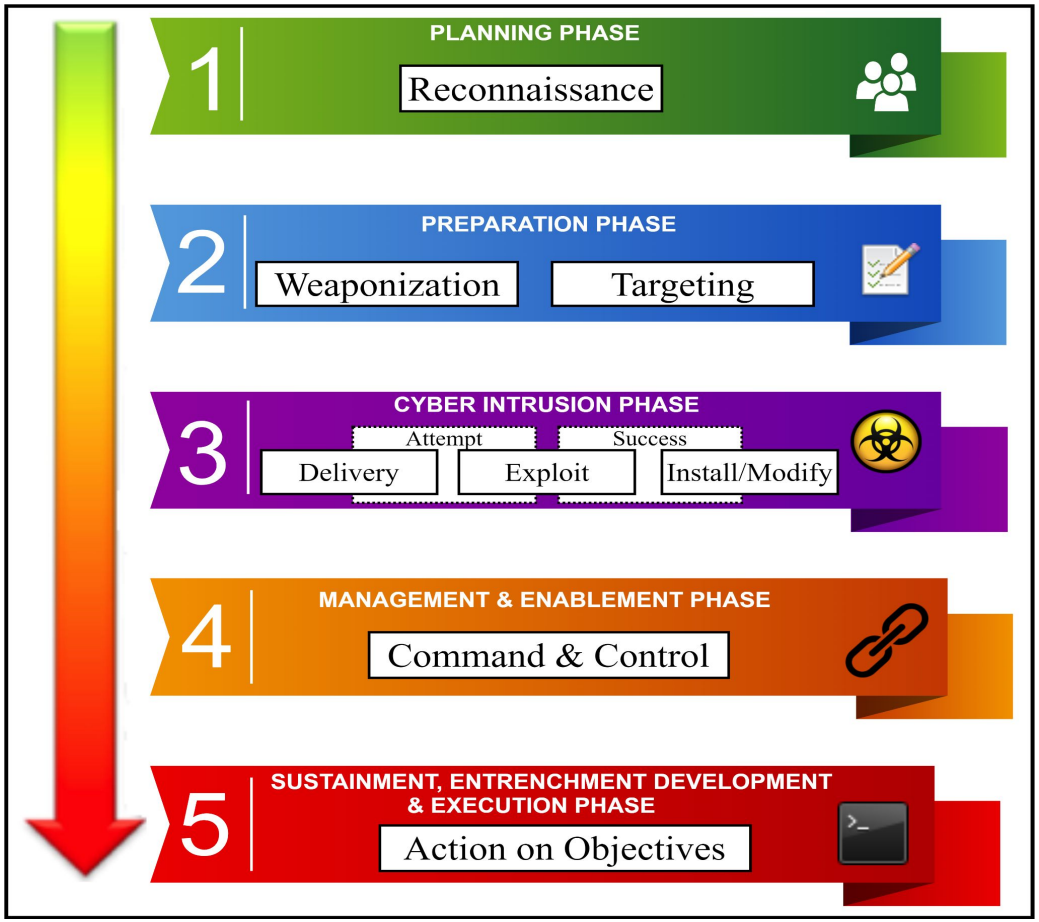
Contributions:

- We develop an original **comparative analysis framework** for ICS malware.
- We evaluate our proposed framework for **five well-known ICS malware**.
- We provide a set of understanding regarding the strategies used by the adversaries in OT networks.

Cyber Threat Intelligence

- Enables understanding the life-cycle of a malicious intrusion activity.
- Consists of gathering a complete understanding of the cyber threat posed by an adversary.
- Describes and characterizes the **cyber threats**.

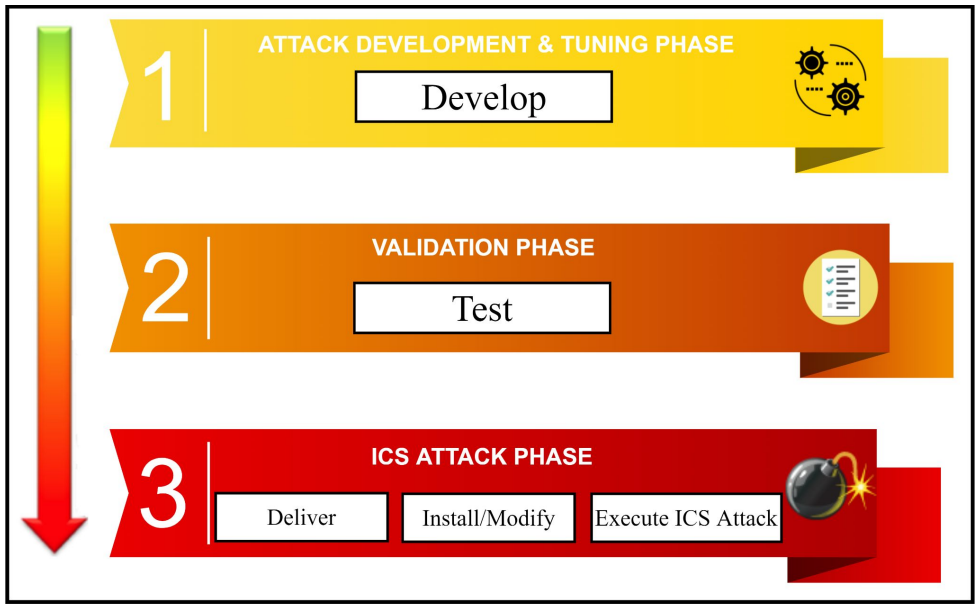
Cyber Threat Intelligence (ICS cyber Kill Chain Stage 1)



- Describe the flow of an adversary cyber attack in ICS scenarios.
- Intelligence-driven model widely used by industrial organizations.
- Enhancement of the traditional Cyber Kill Chain[1], with two stages.
- Provides a better understanding of the adversary's *tactics*, *techniques*, and *procedures* to damage an industrial network.

1: Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. 2011. Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Proceedings of the 6th International Conference on Information Warfare and Security* July 2005 (2011), 113–125.

Cyber Threat Intelligence (ICS cyber Kill Chain Stage 2)

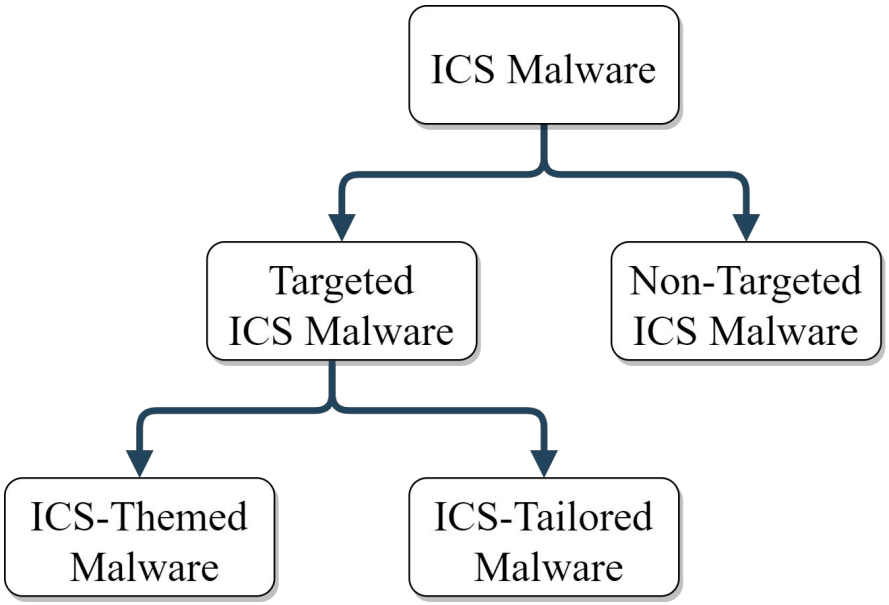


- Describe the flow of an adversary cyber attack in ICS scenarios.
- Intelligence-driven model widely used by industrial organizations.
- Enhancement of the traditional Cyber Kill Chain[1], with two stages.
- Provides a better understanding of the adversary's *tactics*, *techniques*, and *procedures* to damage an industrial network.

1: Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. 2011. Intelligence Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Proceedings of the 6th International Conference on Information Warfare and Security* July 2005 (2011), 113–125.

Industrial Malware Analysis

We aim to analyze ICS malware to understand the malicious intrusion activity.



ICS malware classification

- Two approaches: **Static analysis** and **Dynamic analysis.**
- In both approaches, we rely on the **sandboxing technology.**

Industrial Malware Analysis (Static Analysis)

In ***static analysis***, *we get ICS malware features without its execution.*

- Fingerprinting, strings extraction, and packer detection to gather static information.
- The use the control flow and data flow analysis techniques to draw conclusions about the functionality of the malware.
- Analyze the file format and binary disassembly.

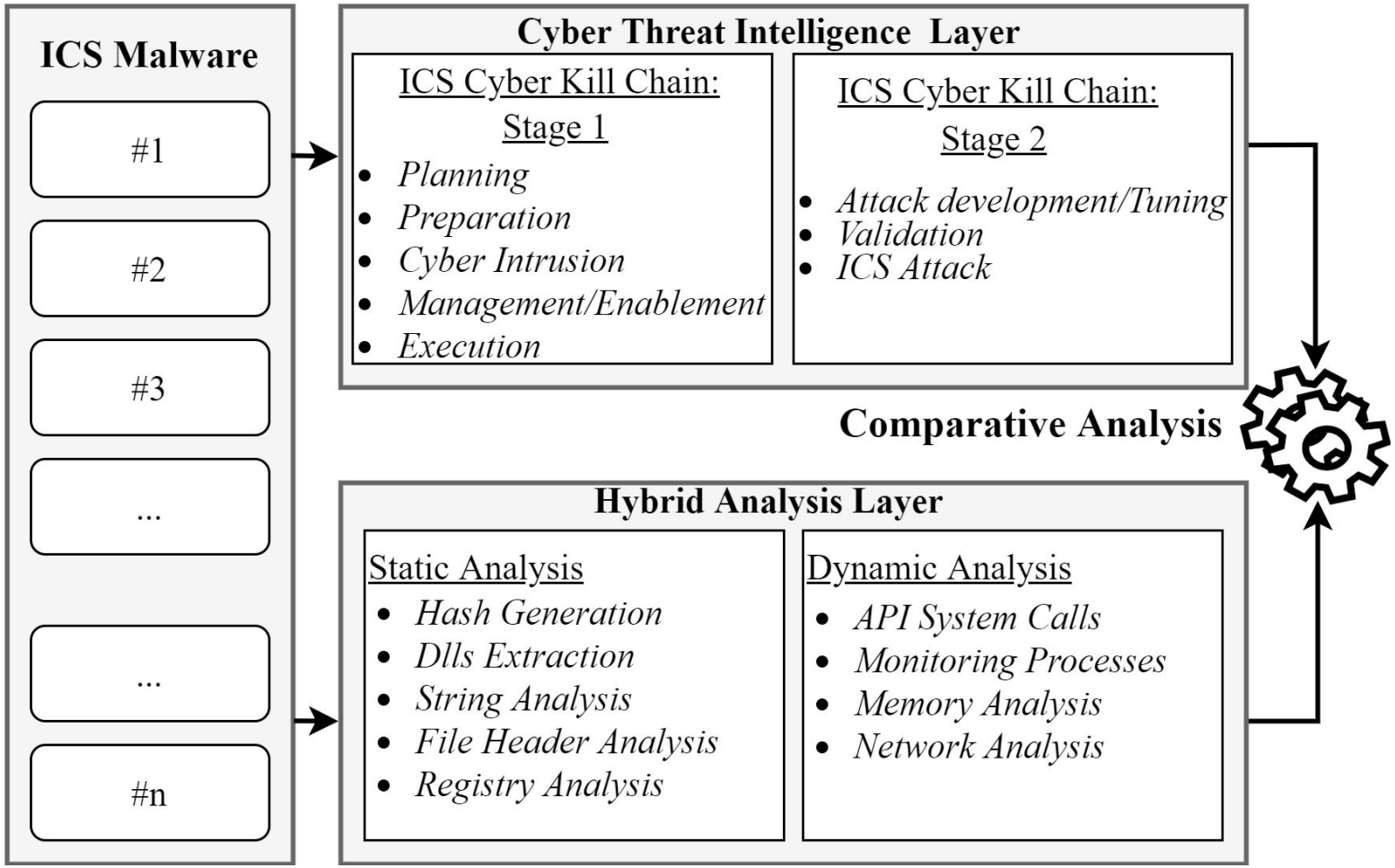
Industrial Malware Analysis (Dynamic Analysis)

*In **dynamic analysis**, we execute the ICS malware in a controlled and secured environment without compromising our live system.*

- Flow tracking.
- Execution control.
- API Function call analysis.
- Graph Execution. (e.g., Network, Processes).

Proposed Framework

Our proposed comparative analysis framework is defined in a bi-layered approach.



Experimental Industrial Malware

- In our comparative analysis framework, we used five well known ICS malware: *Stuxnet*, *Havex*, *BlackEnergy2*, *CrachOverride*, and *TRISIS*.
- The five **ICS malware** are obtained from public sources.
- We applied our **framework** for each ICS malware.

ID Malware	Name	md5 hash value
#1	Stuxnet	68eb6d3adc49da0a79aff2202bbb3bea
#2	Havex	1080e27b83c37dfeaa0daaa619bdf478
#3	BlackEnergy2	17b00de1c61d887b7625642bad9af954
#4	CrashOverride	f67b65b9346ee75a26f491b70bf6091b
#5	TRISIS	6c39c3f4a08d3d78f2eb973a94bd7718

Cyber Threat Intelligence Layer Evaluation

➢ ICS Cyber Kill Chain - Stage 1

- In the **planning and reconnaissance phase**, we found that each adversary conducts his own way of gathering information from the victim.
- In the **preparation phase**, the adversaries weaponized specific files containing an exploit or targeted potential victims inside the facility.
- In the **cyber intrusion phase**, the initial access to the victim's network mostly relied on existing vulnerabilities or through zero-days.
- In the **management and enablement phase**, most of ICS malware utilize Command & Control servers to persist into the IT network.
- In the **execution phase**, the adversary possess the required capabilities to compromise industrial components.

Cyber Threat Intelligence Layer Evaluation

➢ ICS Cyber Kill Chain - Stage 2

- In the **attack development phase**, we found that each adversary develop a tailored capability to target specific ICS devices.
- In the **validation phase**, the adversaries test their capabilities in similar ICS scenario to validate the malicious intrusion.
- In the **ICS attack phase**, the adversaries disrupt and compromise the targeted ICS environment.

Hybrid Analysis Layer Evaluation

➢ Dynamic Linked Libraries Analysis:

DLLs	S	H	B	C	T
ADVAPI32.dll	✓	✓	✓	✓	×
COMCTL32.dll	×	✓	×	×	×
CRYPT32.dll	×	×	×	✓	×
DNSAPI.dll	✓	×	×	×	×
GDI32.dll	×	✓	×	×	×
IPHLPAPI.dll	✓	×	×	×	×
KERNEL32.dll	✓	✓	✓	✓	✓
MSVCR90.dll	×	×	×	×	✓
NETAPI32.dll	✓	×	×	×	×
OLE32.dll	✓	✓	×	✓	×
OLEAUT32.dll	✓	×	×	✓	×
PSAPI.dll	✓	×	×	×	×
RPCRT4.dll	✓	×	×	✓	×
SHELL32.dll	✓	✓	✓	✓	×
SHLWAPI.dll	✓	×	✓	×	×
URLMON.dll	×	×	✓	×	×
USER32.dll	✓	✓	✓	✓	×
USERENV.dll	✓	×	×	×	×
VERSION.dll	✓	✓	×	×	×
WINHTTP.dll	×	×	✓	×	×
WININET.dll	✓	×	×	×	×
WSOCK32.dll	✓	×	×	×	×

✓: Imported by the ICS Malware ×: Not imported by the ICS Malware
S:Stuxnet **H**:Havex **B**:BlackEnergy2 **C**:CrashOverride **T**:TRISIS

- ❑ `KERNEL32.dll` is a very common DLL used every ICS malware.
- ❑ **Stuxnet** uses more libraries than any other ICS malware.
- ❑ TRISIS import only two DLL files: `MSVCR90.dll`, and `KERNEL32.dll`
- ❑ Each ICS malware import specific DLL files.

Hybrid Analysis Layer Evaluation

➢ Dynamic Graph Execution of ICS malware:

- ❑ High execution of *Stuxnet* and *BlackEnergy2* occurs in the operating system.
- ❑ High execution of *TRISIS* and *CrashOverride* on the registry.

Categories (%)	S	H	B	C	T
Exception	1.08	0	0	0.18	1.43
Resource	0	0.52	0	0.36	4.29
Process	25.27	2.79	31.43	5.83	8.57
System	**51.61**	5.36	**41.43**	31.33	31.43
Registry	9.14	17.02	11.43	**35.52**	**50**
File	4.3	5.88	10	6.74	2.86
Synchronisation	6.99	**66.14**	5.71	4.55	1.43
Object linking	0	0.22	0	0	0
User interface	1.61	1.94	0	0	0
Services	0	0.03	0	0	0
Network	0	0.09	0	15.48	0

S:Stuxnet **H**:Havex **B**:BlackEnergy2 **C**:CrashOverride **T**:TRISIS

ICS Malware characteristics comparison

	S	H	B	C	T
Size	1.2MB	2.4MB	717.0KB	10.5KB	21.0KB
Date of disclosure	July, 2010	February, 2013	October, 2014	June, 2017	December, 2017
Type	Worm	RAT	Trojan	Backdoor	TRISIS malware
Number of 0-Days	5	0	0	0	1
Number of rootkits	3	0	1	0	1
Targeted Systems	Siemens Simatic S7-300 PLC	ICS Software	HMIs products of ICS	ICS Protocols for electrical engineering and power system automation	Schneider Electric's Triconex SIS
Payload Type	Physical	Software	Software	Software	Physical
Targeted Countries	Iran	USA and Europe	Asia and Europe	Ukraine	Saudi Arabia
Antivirus Bypass	Two certificates (Realtek and Jmicron)	Certificate looks like signed by IBM	code obfuscation	N/A	N/A
File modification	No	Yes	Yes	No	No
File deletion	No	Yes	No	Yes	No
Registry Modification	No	yes	No	No	No
Registry Deletion	No	yes	No	No	No
Number of Sections	7	5	5	5	4
Number of imported Dlls	16	8	8	7	2
Number of functions	3359	79	164	46	74

S:Stuxnet **H**:Havex **B**:BlackEnergy2 **C**:CrashOverride **T**:TRISIS

- The size of ICS malware is decreasing.
- The two recent ICS malware do not need to bypass antivirus.
- ICS malware with a physical payload do not perform actions on files and registries.
- The number of 0-days and rootkits decreased in the past decade.
- The number of imported DLLs and functions used by each ICS malware decreased.

Security Discussion:

- ICS malware authors are lightweighting their malicious code while maintaining physical damage to ICSs.
- The necessity to adopt ICS cybersecurity standard.
- Most of existing ICS malware in the wild target specific industrial devices or software: **Stuxnet**(Siemens Simatic S7-300 PLC), **TRISIS** (Schneider Electric's Triconex SIS), **Havex** (ICS software), **BlackEnergy2** (HMI products).
- The need to consider a specific defense-in-depth strategy according to the existing ICS architecture.
- ICS Malware are built upon the combination of **inside knowledge**, **advanced skills**, and **vast resources**.

Conclusions

- We presented the **first comparative analysis framework** of ICS Malware cyber attacks in a bi-layered approach.
- We evaluated our framework using **five well-known ICS malware** from two different points of view: A Cyber Threat Intelligence Layer and a Hybrid Analysis Layer.
- We demonstrated that the **cyber threat intelligence** is helpful to understand the general behavior of ICS malware, and the **hybrid ICS malware analysis** reinforces the correlation of the obtained results.
- Our investigation can help to develop a **standardized set of expectations** for the next generations of ICS malware-based cyber attacks.
- We can use our approach to ascend from case studies to **general theoretical models**.

Thank you for you Attention!

Yassine Mekdad
y.mekdad@edu.umi.ac.ma