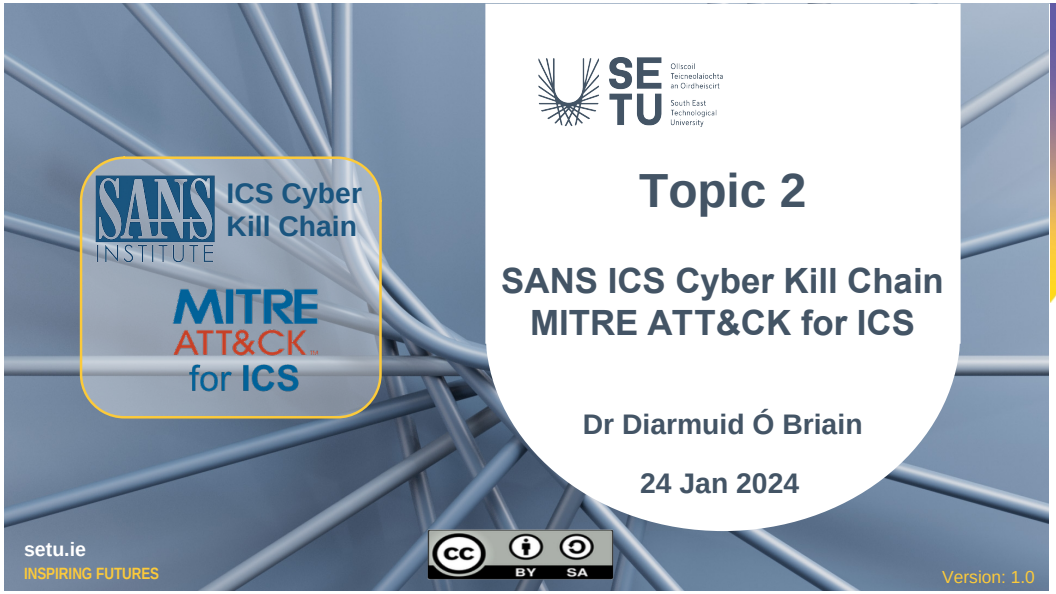


Licence

Learning objectives

- By the end of this topic you will be able to:
  - Understand and apply the SANS Cyber Kill Chain for ICS and MITRE ATT&CK framework to analyse real-world ICS cyberattacks.
  - Identify and analyse the unique cybersecurity challenges faced by ICS systems.
  - Develop comprehensive threat models for ICS systems to identify, prioritise, and mitigate potential attack vectors.
  - Evaluate the effectiveness of ICS security controls in preventing and mitigating cyber threats.

Introduction to ICS Cyber Kill Chain & MITRE ATT&CK

- **SANS Cyber Kill Chain for ICS**
  - A practical framework for ICS security professionals, tailored to the specific needs of ICS systems.
- **MITRE ATT&CK Framework**
  - A more comprehensive and detailed framework, providing a broader understanding of attack techniques.
- Both frameworks break down the attack process from the attacker's perspective, enabling security professionals to develop effective mitigation strategies.

SANS

ICS Kill Chain

setu.ie
INSPIRING FUTURES

What is a Kill Chain

- Structured procedure for identifying, engaging, and neutralising an enemy to achieve a desired outcome
  - Locate suitable adversary targets for engagement
  - Pinpoint their exact location
  - Track and monitor their movements
  - Select the appropriate weapon or asset to produce the desired effects
  - Engage the adversary
  - Evaluate the results.

Advanced Persistent Threats (APT)

- Meticulously planned and executed cyberattacks targeting specific organisations with sensitive information.
- Conventional tools, reliant on signatures and patterns to identify known vulnerabilities, are ineffective against APTs.
- APT attackers often employ zero-day exploits and custom malware to evade detection.
- Organisations need to adopt a more proactive and intelligence-driven approach to cyber defence.

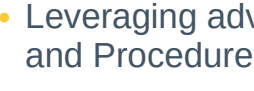
Advanced Persistent Threats (APT)

- Proactive approaches include:
  - Threat intelligence gathering
  - Network segmentation
  - Behavioural anomaly detection.

Intelligence-driven Computer Network Defence (CND)

- Leveraging adversary knowledge and Tactics, Techniques, and Procedures (TTP) for proactive defence.
- Understanding attack stages, mapping TTPs to defence measures, and identifying patterns.
- Proactive anticipation and neutralisation of attacks through continuous intelligence gathering.
- Reduced intrusion likelihood, informed resource allocation, and performance assessment.
- Addressing threat component of risk beyond vulnerability mitigation.

Intrusion Kill Chain



Reconnaissance

1) Reconnaissance

- Attacker gathers information about the target organisation and its systems.
- Info can be obtained from a variety of sources, such as public records, social media, and corporate websites.
- The goal is to identify vulnerabilities that the attacker can exploit to gain access to the target system.

Intrusion Kill Chain

Reconnaissance

2) Weaponisation

- Develop a malicious payload.
- Code that will be used to exploit the vulnerabilities in the target system, such as a virus, worm, or Trojan horse.

Intrusion Kill Chain

Reconnaissance Delivery

3) Delivery

- Deliver the payload to the target system,such as through email, USB drive, or network exploitation.
- Get the payload onto the target system so that it can be executed.

Intrusion Kill Chain

4) Exploitation

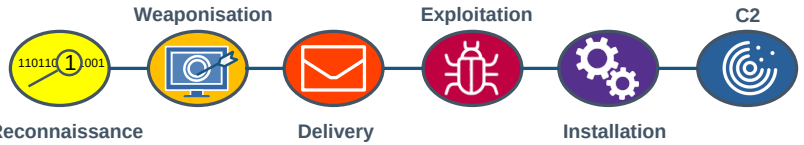
- Attempt to exploit the vulnerabilities that have been identified.
- Use the payload to execute malicious code and gain access to the system.

Intrusion Kill Chain

5) Installation

- Install malware or other malicious software.
- Gains control of the system to facilitate the carrying out of objectives.

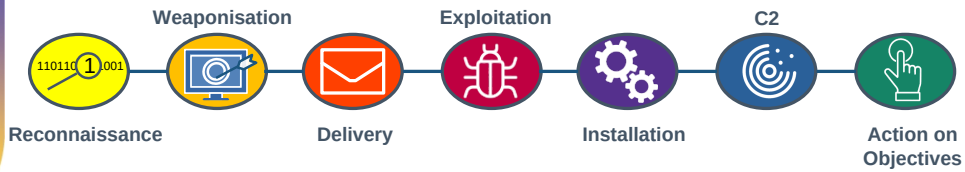
Intrusion Kill Chain



6) Command and Control (C2)

- Establish a communication channel with the compromised system for remote control.
- Facilitates the stealing of data, installation of more malware, or launch other attacks.

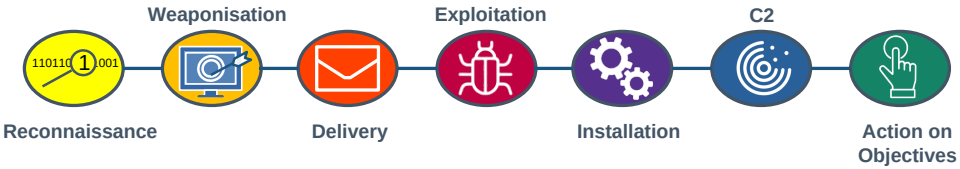
Intrusion Kill Chain



7) Actions on Objectives

- Carry out their objectives, such as stealing data, disrupting operations, or damaging the system.

Intrusion Kill Chain



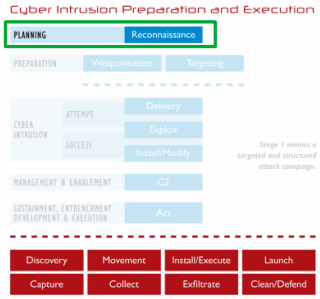
- The intrusion kill chain can be used as a model for actionable intelligence by aligning enterprise defensive capabilities with the adversary's specific processes.
- Defenders can evaluate the performance and effectiveness of their defences by using the intrusion kill chain to track the adversary's progress through the attack lifecycle.
  - This approach allows defenders to identify capability gaps and devise investment roadmaps to address them.
- Intelligence-driven CND is based on a deep understanding of the adversary and enables informed security decisions and measurements.

SANS ICS Kill Chain
Stage 1

setu.ie
INSPIRING FUTURES

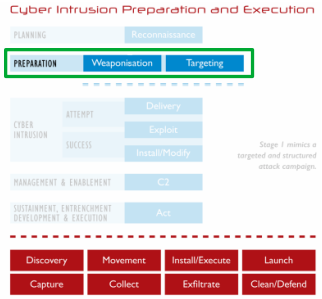
SANS Cyber Kill Chain for ICS – Stage 1

- **Planning Phase**
  - ***Reconnaissance***: Attackers gather information about their target, including public announcements, social media profiles, and company websites, to identify weaknesses and plan the attack.
  - ***Target Selection***: Attackers select targets based on factors such as perceived value, vulnerability, and ease of access.
  - ***Developing Exploits***: Attackers develop exploits to take advantage of vulnerabilities in the target's systems.
  - ***Establishing Command and Control (C2)***: Attackers establish a communication channel with their C2 server so they can remotely control the compromised system.



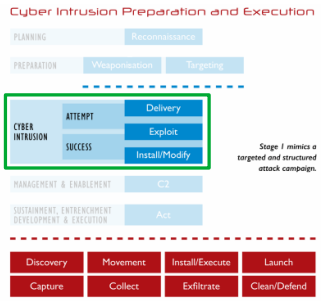
SANS Cyber Kill Chain for ICS – Stage 1

- **Preparatory phase**
  - ***Weaponisation***: Attackers modify innocuous files to embed exploits or enhance their malicious capabilities.
  - ***Target Identification***: Attackers analyse and prioritise potential victims, based on factors like perceived value, vulnerability, and ease of access.
  - ***Attack Strategy Development***: Attackers devise appropriate attack strategies to exploit vulnerabilities and achieve specific objectives.
  - ***Target Selection***: Attackers select the most suitable target based on weaponisation capabilities and attack strategy.



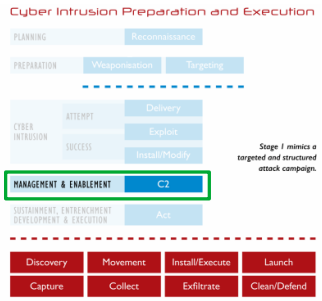
SANS Cyber Kill Chain for ICS – Stage 1

- **Cyber Intrusion phase**
  - ***Delivery***: Attackers deliver malicious payloads to the target system or network.
  - ***Exploitation***: Attempt to exploit vulnerabilities in the target system to gain initial access.
  - ***Installation***: Install malware or other tools to establish a persistent presence on the system.
  - ***Persistence***: Attackers take steps to ensure that their access to the system is not easily detected or removed.



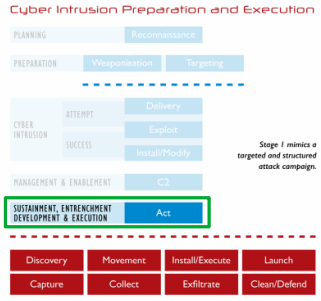
SANS Cyber Kill Chain for ICS – Stage 1

- **Management and Enablement phase**
  - ***Establishing C2***: Attackers establish a communication channel with their C2 server to remotely control the compromised system.
  - ***Maintaining C2***: Attackers establish multiple C2 paths to ensure that connectivity is not interrupted if one is detected or removed.
  - ***Hiding C2***: Attackers hide their C2 communication in normal outbound and inbound traffic, hijacking existing communications.
  - ***Enabling access***: Attackers gain managed and enabled access to the environment, allowing them to execute their attack goals.



SANS Cyber Kill Chain for ICS – Stage 1

- **Sustainment, Entrenchment, Development, and Execution phase**
  - Gather information
  - Move laterally within the network
  - Install additional capabilities
  - Launch attacks
  - Capture data
  - Exfiltrate data
  - Employ anti-forensic techniques



SETU Oliscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

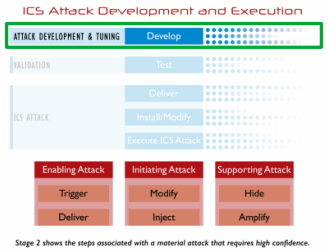
SANS

ICS Kill Chain
Stage 2

setu.ie
INSPIRING FUTURES

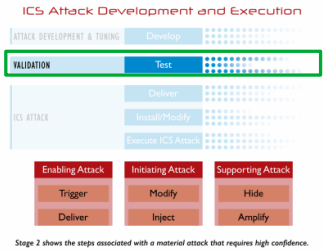
SANS Cyber Kill Chain for ICS – Stage 2

- **Attack Development and Tuning phase**
  - ***Tailoring attack capabilities to specific vulnerabilities***: Attackers use info from Stage 1 to develop customised attack tools and techniques.
  - ***Utilising exfiltrated data***: Attackers may use the data they steal from Stage 1 to better understand the target system and its weaknesses.
  - ***Limited live in-production testing***: Due to the risk of detection, attackers are less likely to test their attacks in real-time during Stage 2.
  - ***Challenges for defenders***: The lack of live activity makes it difficult for defenders to detect adversary activities during Stage 2.
  - ***Delays between Stage 1 and Stage 2***: The need for extensive development and testing may lead to delays between the completion of Stage 1 and the initiation of Stage 2 operations.



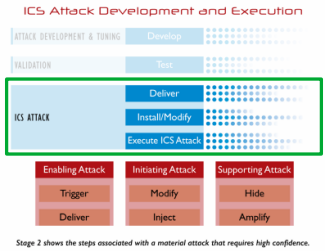
SANS Cyber Kill Chain for ICS – Stage 2

- **Validation phase**
  - ***Attack code testing on similar or identically configured systems***: To ensure the effectiveness and reliability of their attack code, attackers will trial code on simulations.
  - ***Importance of testing for precise timing and execution***: For attacks that require precise timing and execution, such as DoS attacks, thorough testing is crucial.
  - ***Physical ICS equipment or software component acquisition for complex attacks***: Attackers may acquire physical ICS equipment or software components to conduct rigorous testing.
  - ***Difficulty of detecting attacker validation activities***: This level of validation may be challenging for typical defenders to detect.
  - ***Government agencies' potential identification of unusual equipment acquisitions***: Identity of unusual equipment acquisitions, which could indicate the start of Stage 2 operations following an established Stage 1 intrusion.



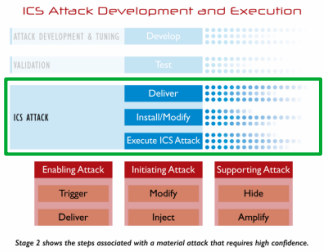
SANS Cyber Kill Chain for ICS – Stage 2

- **ICS Attack phase**
  - ***Execution***: The adversary unleashes their attack capabilities to achieve objectives.
  - ***Attack components***: Multiple attack components may be involved, such as enabling, initiating, or supporting actions.
  - ***Spoofing state information***: Attackers may deceive plant operators to maintain a facade of normality.
  - ***Complexity of ICS attacks***: Varies based on system security, process type, safety measures, and attacker objectives.



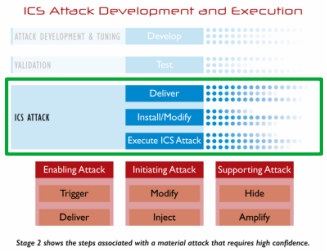
SANS Cyber Kill Chain for ICS – Stage 2

- **ICS Attack phase -** ICS attack types:
  - ***Loss***: Loss of view and of control.
  - ***Denial***: Denial of view, of control and of safety systems: Activation of safety systems is prevented.
  - ***Manipulation***: Manipulation of view, of control, of sensors and instruments, and of safety systems
  - ***Activation of safety systems***: Safety protocols are unconventionally triggered.



SANS Cyber Kill Chain for ICS – Stage 2

- **ICS Attack phase –** Impact:
  - ***IT systems***: DoS attacks are disruptive to business operations.
  - ***ICS systems***: Manipulation of sensors or processes poses a significant threat to safety and human life.
  - ***Potential attack scenarios***:
    - Power grid failures
    - Dam overflows
    - Release of hazardous materials
    - Degradation of manufacturing products
    - Financial losses due to unusable product



ICS Cyber Kill Chain summary

- A model that helps defenders understand the phases of an adversary's campaign into an ICS.
- Can be used to identify opportunities for detection, remediation, and defence.
- ICS networks are more defensible than traditional IT networks, but it is important to maintain this defensible architecture by limiting the integration of safety systems with operations networks and removing ICS components from direct Internet access.

SETU Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

MITRE ATT&CK™ for ICS

setu.ie
INSPIRING FUTURES

Introduction to MITRE ATT&CK® framework

- Developed by a non-profit organisation MITRE in 2013, to consider each stage of the cyberattack lifecycle from the perspective of the attacker
- Globally accessible knowledge base of adversary TTPs based on real-world observations
- Used as a foundation for the development of specific threat models and methodologies

MITRE ATT&CK™

MITRE ATT&CK® phases

- Reconnaissance
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Lateral Movement
- Collection
- Exfiltration

MITRE ATT&CK Reconnaissance phase

- **Discovery**
  - The attacker discovers information about the target and its environment.
- **Weaponisation**
  - The attacker prepares malware or exploits.
- **Delivery**
  - The attacker delivers the malware or exploit to the target.

MITRE ATT&CK Discovery tactic

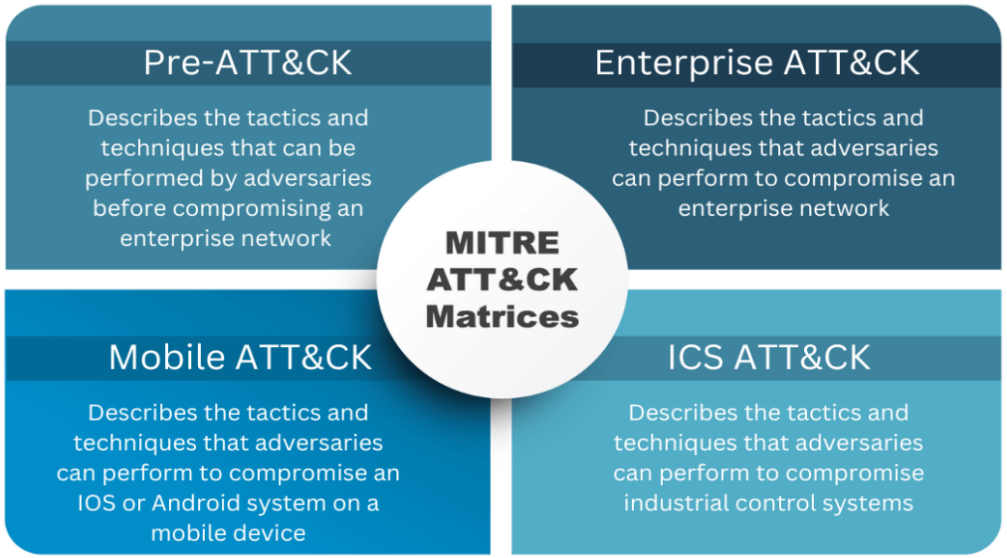
- **Network Mapping**
  - The attacker maps the target's network.
- **Data Credential Discovery**
  - The attacker discovers data and credentials.
- **Domain Discovery**
  - The attacker discovers the target's domain structure.

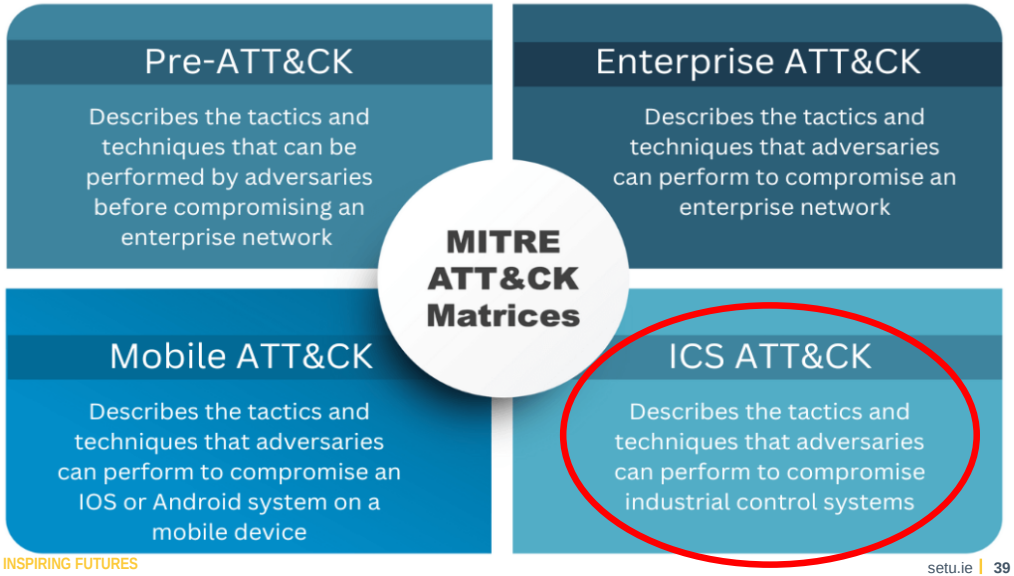
Benefits of using the MITRE ATT&CK framework

- Improved threat awareness
- Better threat detection
- More effective threat response
- Improved communication about threats

The MITRE ATT&CK framework can be used for

- Threat modelling
- Threat intelligence
- Vulnerability assessment
- Incident response





ATT&CK - Tactics

- 12 tactics employed in the framework
  - Each tactic cover the ***why*** of an attack
  - Tactics serve as a higher-level notation for the actions being carried out during an attack.

- TA0108 – Initial Access
- TA0104 – Execution
- TA0110 – Persistence
- TA0111 – Privilege Escalation
- TA0103 – Evasion
- TA0102 – Discovery
- TA0109 – Lateral Movement
- TA0100 – Collection
- TA0101 – Command and Control
- TA0107 – Inhibit Response Function
- TA0106 – Impair Process Control
- TA0105 – Impact

ATT&CK Techniques, Procedures and mitigations

- **Techniques**: Techniques cover the how and what an adversary gains when carrying out an action and can often be a single step in a string of activities to achieve goal.
- **Sub-Techniques**: Sub-techniques offer a granular description of a technique, are more specific in description and often platform or OS specific.
- **Procedures**: Procedures offer particular instances of how a technique or sub-technique has been used and can offer several additional behaviours in the way they are performed.
- **Mitigations**: Mitigations offer what to do when under attack so are countermeasures that may help prevent the adversary from achieving their goal.

ICS Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

MITRE ATT&CK™ ICS

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

ICS Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Conficker
- Exploit of Windows drive shares
- **ICS Techniques**
  - Loss of Availability
  - Loss of Productivity and Revenue
  - Replication Through Removable Media
- **ICS Mitigations**
  - Disable AutoRun
  - Limit Hardware Installation
  - OS Configuration

ATT&CK Example - Techniques

- Techniques of the tactic - TA0108 – Initial Access

TA0817 – Drive-by Compromise

TA0819 – Exploit Public-Facing Application

TA0866 – Exploitation of Remote Services

TA0822 – External Remote Services

TA0883 – Internet Accessible Device

- TA0886 – Remote Services
- ***TA0847 – Replication Through Removable Media***
- TA0848 – Rogue Master
- TA0865 – Spear-phishing Attachment
- TA0862 – Supply Chain Compromise
- TA0864 – Transient Cyber Asset
- TA0860 – Wireless Compromise

ATT&CK Example - Procedures

- The TA0847 – Replication Through Removable Media technique has two ***Procedures***
  - **S0608 – *Conficker, an exploit of Windows drive shares***
  - S0603 – Stuxnet, able to self-replicate by being spread through removable drives.

ATT&CK Example - Techniques

- The ***S0608 – Conficker, an exploit of Windows drive shares*** has three techniques associated with it for ICS
  - ICS T0826 – Loss of Availability
  - ICS T0828 – Loss of Productivity and Revenue
  - ICS T0847 – Replication Through Removable Media

ATT&CK Example - Mitigations

- The ***S0608 – Conficker*** exploit can be mitigated by:
  - M0942 – Disable or Remove Feature or Program
    - Disable AutoRun
  - M0934 – Limit Hardware Installation
    - Limit hardware such as USB drives
  - M0928 – OS Configuration

ATT&CK Example - Detection

- The ***S0608 – Conficker*** exploit can be detected by:
  - DS0016 – Drive Creation
    - Monitor for new drives or mount points.
  - DS0022 – File Access
    - Monitor for files accessed on removable media.
  - DS0009 – Process Creation
    - Monitor for new processes from removable media.

Threat Modelling

setu.ie
INSPIRING FUTURES

Threat Model

- A threat model is a process that helps organisations identify, assess, and prioritise cybersecurity threats.
- It involves understanding the potential threats that an organisation faces, the likelihood of those threats being realised, and the potential impact of those threats if they are realised.
- Threat models can be used to inform security decisions, such as which security controls to implement and where to focus security resources.

Threat Models are used to

- Identifying and prioritising risks
- Developing security controls
- Communicating security risks
- Preparing for incidents

Threat Models example

- Identify
  - Threat Actor(s)
    - Type
    - Motivation
    - Capabilities
  - Attack Vector
    - Method
    - Vulnerability
    - Exploit

Threat model
S0608 – *Conficker*, an exploit of Windows drive shares

Threat Actor
- **Type**: Advanced Persistent Threat (APT)
- **Motivation**: Gain unauthorised access to systems and networks to steal data, disrupt operations, or conduct espionage
- **Capabilities**: Highly skilled technical expertise, advanced tools and techniques, sophisticated attack methods

Attack Vector
- **Method**: Exploiting vulnerabilities in Windows drive shares
- **Vulnerability**: MS08-067, a vulnerability in the Server Message Block (SMB) protocol that allows attackers to execute arbitrary code on vulnerable systems
- **Exploit**: *Conficker*, a worm that exploits the MS08-067 vulnerability to spread to other systems through shared drives

Threat Models example

- Identify
  - Attack Path
    - Reconnaissance
    - Delivery
    - Exploitation
    - Installation
    - Persistence
    - Lateral Movement
    - Collection
    - Exfiltration

Attack Path

- **Reconnaissance:** The attacker gathers information about the target system, such as its network configuration and vulnerabilities.
- **Delivery**: The attacker sends a malicious file to the target system, often disguised as a legitimate file.
- **Exploitation**: When the victim opens the malicious file, the Conficker worm is executed, allowing the attacker to gain control of the system.
- **Installation**: The worm installs itself on the system and spreads to other systems through shared drives.
- **Persistence**: The worm creates persistence mechanisms to ensure that it remains active on the system even after reboots.
- **Lateral Movement**: The worm moves laterally through the network, infecting other systems and gaining access to sensitive data.
- **Collection**: The worm gathers sensitive data from the infected systems, such as personal information, financial data, and intellectual property.
- **Exfiltration**: The worm exfiltrates the stolen data to the attacker's command and control server.

Threat Models example

- Identify
  - Mitigation Strategies

Mitigation Strategies

- **Patch systems promptly**: Keep all systems patched with the latest security updates, including the MS08-067 patch.
- **Disable unnecessary shares**: Disable unnecessary network shares to reduce the attack surface.
- **Implement strong access controls**: Enforce strong access controls on shared drives, restricting access to authorised users only.
- **Use intrusion detection and prevention systems (IDS/IPS)**: Deploy IDS/IPS systems to detect and block malicious activity on the network.
- **Educate employees about cybersecurity threats**: Educate employees about cybersecurity threats and how to identify and avoid suspicious emails and attachments.
- **Implement a vulnerability management program**: Regularly scan systems for vulnerabilities and prioritise patching the most critical ones.
- **Use endpoint security solutions**: Deploy endpoint security solutions to detect and block malware infections.

Learning objectives

- Understand and apply the SANS Cyber Kill Chain for ICS and MITRE ATT&CK framework to analyse real-world ICS cyberattacks ✓
- Identify and analyse the unique cybersecurity challenges faced by ICS systems ✓
- Develop comprehensive threat models for ICS systems to identify, prioritise, and mitigate potential attack vectors ✓
- Evaluate the effectiveness of ICS security controls in preventing and mitigating cyber threats ✓

SETU Oliscoil Teicneolaíochta an Oirdheiscirt South East Technological University

Exercise

setu.ie
INSPIRING FUTURES

Exercise 1: Applying ATT&CK

Student	Tactic	Technique
Harshith	TA0108 – Initial Access	T0817 – Drive-by Compromise
Harshith	TA0104 – Execution	T0807 – CLI
3	TA0110 – Persistence	T0889 – Modify Program
Sanjeev	TA0111 – Privilege Escalation	T0890 – Exploit for Privilege Escalation
Sanjeev	TA0103 – Evasion	T0820 – Exploit for Privilege Evasion
6	TA0102 – Discovery	T0842 – Network Sniffing
Khyati	TA0109 – Lateral Movement	T0812 – Default Credentials
Khyati	TA0100 – Collection	T0893 – Data from Local System
9	TA0101 – Command and Control	T0885 – Commonly Used Port
James	TA0107 – Inhibit Response Function	T0878 – Alarm Suppression
James	TA0106 – Impair Process Control	T0836 – Modify Parameter

Take Home

TUS
Ollscoil Teicneolaíochta na Sionainne: Lár Tíre, An tIarthar Láir
Technological University of the Shannon: Midlands Midwest

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

E diarmuid.obriain@tus.ie | W tus.ie
Campas Maoilis, Páirc Maoilis, Luimneach, V94 EC5T, Éire

CISSP®

Thank you

TUS