



4th Maritime Security Conference

Maritime Security Centre of Excellence



Cyber Threat Intelligence Analysis for the Maritime Industry: MITRE ATT&CK Framework Approach

Emre Duzenli, Gizem Kayisoglu and Pelin Bolat

Maritime Security and Cyber Threats Research Laboratory
Istanbul Technical University / Maritime Faculty

Presenter : Emre DUZENLI

The Purpose of The Study

This study focuses on to map the observed cyber incidents in the maritime domain to the tactics and techniques listed in the Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) Framework.

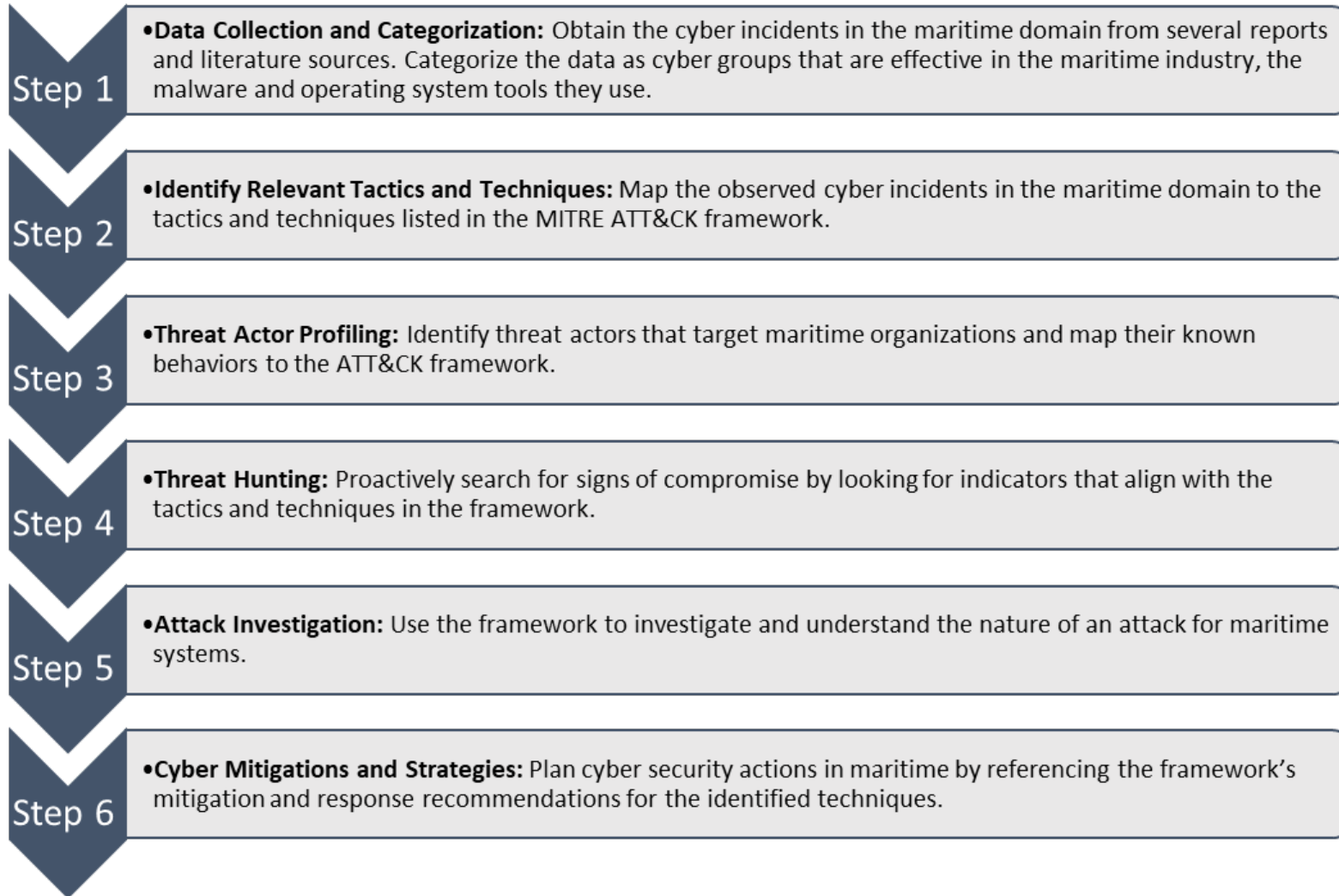
By using MITRE ATT&CK Framework, threat actor profiling that targets maritime organizations is identified and their known behaviors are mapped according to the ATT&CK Framework.

For this purpose, the cyber groups that carry out cyber-attacks and the malicious software used by these groups and the tools that come from the characteristics of operating systems are analyzed.

As a result of the study, measures and precautions to be taken for the protection of maritime systems from malicious software and tools used by cyber attackers affecting the maritime industry have been established



Material and Method



List of cyber gangs, the specific malicious software and operating system utilities impacting the marine sector

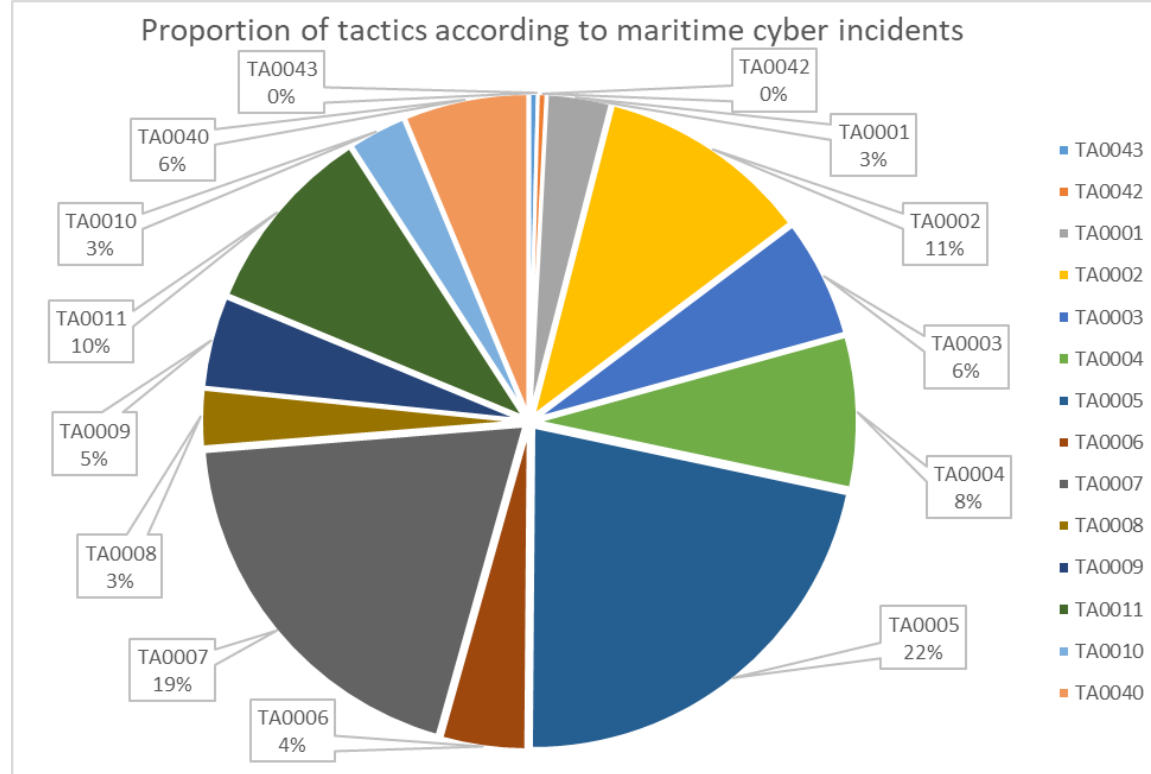
Cyber Group Name	Malware and Tool Lists	Cyber Incident Resource
Noname057(16)	Noname057(16)	Bodnar (2023)
Mysterious Team Bangladesh	Mysterious Team Bangladesh	Radware (2023)
NIL	Clop	Toulas (2021)
NIL	LockBit 3.0	Dragos Inc. (2023)
Killnet	Killnet	Livomopress (2022)
NIL	LockBit 2.0	Halcyon (2022a)
Cleaver	Mimikatz, PsExec, Net Crawler, TinyZBot	Gallagher (2014), Cleaver (2022)
Anchor Panda, APT14	Gh0st RAT, PoisonIvy	Meyers (2013), ETDA (2020)
NIL	Conti	Beer (2022)
Elderwood	Briba, Hydraq, Linfo, Naid, Nerex, Pasam, Vasport, Wiarp	Clayton (2012), Elderwood (2024)
NIL	Maze	Chambers (2020)
Hive Ransomware Group	Hive	The Maritime Executive (2023)
Revil Ransomware Group	Revil (Sodinokibi)	Red Packet Security (2021)
NIL	Black Basta	Daily Dark Web (2024)
NIL	BianLian	Hackmanac (2023a)
NIL	Snatch	Hackmanac (2024)
NIL	NotPetya	Capano (2023)
NIL	ALPHV (BlackCat)	Hackmanac (2023b)
NIL	Egregor	Goud (n.d.)
NIL	Ryuk	Grau (2018)
NIL	Play	Arghire (2023)



The MITRE ATT&CK Framework

Reconnaissance														Resource Development														Initial Access														Execution														Persistence														Privilege Escalation														Defense Evasion														Credential Access														Discovery														Lateral Movement														Collection														Command and Control														Exfiltration														Impact																																									
10 techniques														8 techniques														10 techniques														14 techniques														20 techniques														14 techniques														43 techniques														17 techniques														32 techniques														9 techniques														17 techniques														18 techniques														9 techniques														14 techniques																																									
Active Scanning (0/3) Gather Victim Host Information (0/4) Gather Victim Identity Information (0/3) Gather Victim Network Information (0/6) Gather Victim Org Information (0/4) Phishing for Information (0/4) Search Closed Sources (0/2) Search Open Technical Databases (0/3) Search Open Websites/Domains (0/3) Search Victim-Owned Websites														Acquire Access (0/5) Acquire Infrastructure (0/5) Compromise Accounts (0/3) Compromise Infrastructure (0/6) Develop Capabilities (0/4) Establish Accounts (0/3) Obtain Capabilities (0/7) Stage Capabilities (0/6) Replication Through Removable Media (0/4) Supply Chain Compromise (0/3) Trusted Relationship (0/3) Valid Accounts (0/4)														Content Injection (0/4) Drive-by Compromise (0/3) Exploit Public-Facing Application (0/3) External Remote Services (0/6) Hardware Additions (0/4) Phishing (1/4) Spearphishing Attachment (0/3) Spearphishing Link (0/3) Spearphishing via Service (0/3) Spearphishing Voice (0/3)														Cloud Administration Command (0/3) AppleScript (0/3) AutoHotKey & AutoIT (0/14) Cloud API (0/3) JavaScript (0/3) Network Device CLI (0/10) PowerShell (0/3) Python (0/3) Unix Shell (0/3) Visual Basic (0/3) Windows Command Shell (0/3)														Account Manipulation (0/6) BITS Jobs (0/6) Boot or Logon Autostart Execution (0/14) Boot or Logon Initialization Scripts (0/3) Browser Extensions (0/3) Compromise Host Software Binary (0/6) Create Account (0/3) Create or Modify System Process (0/5) Event Triggered Execution (0/16) External Remote Services (0/3) Hijack Execution Flow (0/13) Implant Internal Image (0/3) Modify Authentication Process (0/3) Office Application Startup (0/6) Power Settings (0/3) Pre-OS Boot (0/3) Scheduled Task/Job (0/3) Server Software Component (0/3) Traffic Signaling (0/2) Valid Accounts (0/4)														Abuse Elevation Control Mechanism (0/6) Access Token Manipulation (0/5) Account Manipulation (0/6) Boot or Logon Autostart Execution (0/14) Boot or Logon Initialization Scripts (0/3) Create or Modify System Process (0/5) Domain or Tenant Policy Modification (0/2) Event Triggered Execution (0/16) External Remote Services (0/3) Hijack Execution Flow (0/13) Implant Internal Image (0/3) Modify Authentication Process (0/3) Office Application Startup (0/6) Power Settings (0/3) Pre-OS Boot (0/3) Scheduled Task/Job (0/3) Server Software Component (0/3) Traffic Signaling (0/2) Valid Accounts (0/4)														Create Process with Token (0/4) Make and Impersonate Token (0/5) Parent PID Spoofing (0/3) SID-History Injection (0/3) Token Impersonation/Theft (0/3) BITS Jobs (0/3) Build Image on Host (0/3) Debugger Evasion (0/2) Deobfuscate/Decode Files or Information (0/4) Deploy Container (0/3) Direct Volume Access (0/3) Domain or Tenant Policy Modification (0/2) Execution Guardrails (0/1) Exploitation for Defense Evasion (0/3) File and Directory Permissions Modification (0/2) Hide Artifacts (0/12) Hijack Execution Flow (0/13) Impair Defenses (0/11) Indicator Removal (1/5) Impersonation (0/3) Indicator Removal (1/5)														Abuse Elevation Control Mechanism (0/6) Access Token Manipulation (0/5) BITS Jobs (0/3) Build Image on Host (0/3) Debugger Evasion (0/2) Deobfuscate/Decode Files or Information (0/4) Deploy Container (0/3) Direct Volume Access (0/3) Domain or Tenant Policy Modification (0/2) Execution Guardrails (0/1) Exploitation for Defense Evasion (0/3) File and Directory Permissions Modification (0/2) Hide Artifacts (0/12) Hijack Execution Flow (0/13) Impair Defenses (0/11) Indicator Removal (1/5) Impersonation (0/3) Indicator Removal (1/5)														Adversary-in-the-Middle (0/3) Brute Force (0/4) Credentials from Password Stores (0/6) Exploitation for Credential Access (0/3) Forced Authentication (0/2) Forge Web Credentials (0/2) Input Capture (0/4) Modify Authentication Process (0/3) Multi-Factor Authentication Interception (0/3) Multi-Factor Authentication Request Generation (0/3) Network Sniffing (0/3) OS Credential Dumping (0/6) Steal Application Access Token (0/4) Steal or Forge Kerberos Tickets (0/4) Steal Web Session Cookie (0/4) Unsecured Credentials (0/6) Clear Command History (0/1) Clear Linux or Mac System Logs (0/1) Clear Mailbox Data (0/2) Clear Network Connection History and Configurations (0/2) Clear Persistence (0/1) Clear Windows Event Logs (0/1) File Deletion (0/1)														Account Discovery (0/4) Application Window Discovery (0/3) Browser Information Discovery (0/4) Cloud Infrastructure Discovery (0/3) Cloud Service Dashboard (0/3) Cloud Service Discovery (0/2) Cloud Storage Object Discovery (0/2) Container and Resource Discovery (0/3) Debugger Evasion (0/3) Device Driver Discovery (0/3) Domain Trust Discovery (0/3) File and Directory Discovery (0/3) Group Policy Discovery (0/3) Log Enumeration (0/3) Network Service Discovery (0/3) Network Share Discovery (0/3) Network Sniffing (0/3) Password Policy Discovery (0/3) Peripheral Device Discovery (0/3) Permission Groups Discovery (1/3) Process Discovery (0/3) Query Registry (0/3) Remote System Discovery (0/3) Software Discovery (0/1) System Information Discovery (0/1) System Location Discovery (1/1) System Network Configuration Discovery (0/2) System Network Connections Discovery (0/2) System Owner/User Discovery (0/1)														Exploitation of Remote Services (0/3) Internal Spearphishing (0/3) Lateral Tool Transfer (0/2) Remote Service Session Hijacking (0/2) Remote Services (0/6) Replication Through Removable Media (0/3) Software Deployment Tools (0/3) Taint Shared Content (0/3) Use Alternate Authentication Material (0/4) Data from Local System (0/3) Data from Network Shared Drive (0/3) Data from Removable Media (0/3) Data Staged (0/3) Email Collection (0/3) Input Capture (0/4) Screen Capture (0/2) Video Capture (0/3)														Adversary-in-the-Middle (0/3) Archive Collected Data (0/3) Audio Capture (0/3) Automated Collection (0/2) Browser Session Hijacking (0/2) Clipboard Data (0/2) Data from Cloud Storage (0/3) Data from Configuration Repository (0/3) Data from Information Repositories (0/3) Data from Local System (0/3) Data from Network Shared Drive (0/3) Data from Removable Media (0/3) Data Staged (0/3) Email Collection (0/3) Input Capture (0/4) Screen Capture (0/2) Video Capture (0/3)														Application Layer Protocol (1/4) Mail Protocols (0/3) Communication Through Removable Media (0/3) Content Injection (0/3) Data Encoding (0/2) Data Obfuscation (0/3) Dynamic Resolution (0/3) Encrypted Channel (1/2) Fallback Channels (0/3) Hide Infrastructure (0/3) Ingress Tool Transfer (0/4) Multi-Stage Channels (0/3) Non-Application Layer Protocol (0/3) Remote Access Software (0/3) Traffic Signaling (0/3) Web Service (0/3)														DNS (0/3) File Transfer Protocols (0/1) Web Protocols (0/3) Exfiltration Over Alternative Protocol (0/3) Exfiltration Over C2 Channel (0/3) Exfiltration Over Other Network Medium (0/3) Exfiltration Over Physical Medium (0/3) Exfiltration Over Web Service (0/4) Scheduled Transfer (0/3) Transfer Data to Cloud Account (0/3)														Automated Exfiltration (0/1) Data Transfer Size Limits (0/3) Data Manipulation (0/3) Defacement (0/2) Disk Wipe (0/3) Endpoint Denial of Service (0/4) Financial Theft (0/3) Firmware Corruption (0/3) Inhibit System Recovery (0/3) Network Denial of Service (0/2) Resource Hijacking (0/3) Service Stop (0/3) System Shutdown/Reboot (0/3)														Account Access Removal (0/3) Data Destruction (0/3) Data Encrypted for Impact (0/3) Data Manipulation (0/3) Defacement (0/2) Disk Wipe (0/3) Endpoint Denial of Service (0/4) Financial Theft (0/3) Firmware Corruption (0/3) Inhibit System Recovery (0/3) Network Denial of Service (0/2) Resource Hijacking (0/3) Service Stop (0/3) System Shutdown/Reboot (0/3)													

Analysis and Results



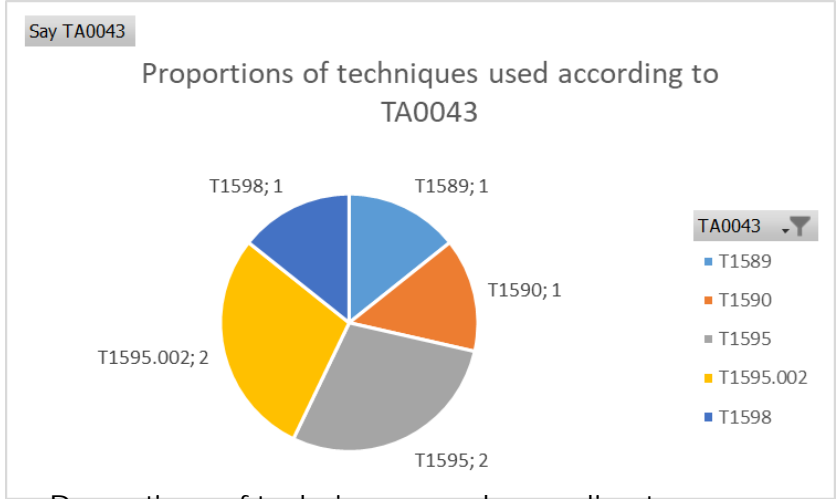
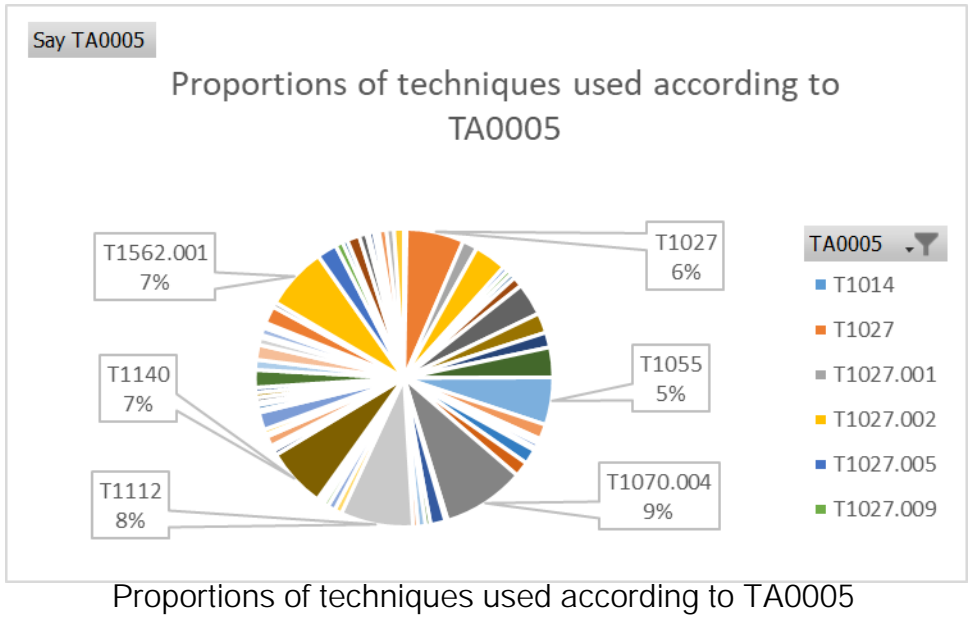
The proportion of the tactics, which is used most by cyber gang in the maritime sector

Tactics	Techniques and Sub-techniques
TA0043	T1589, T1590, T1595, T1595.002, T1598
TA0042	T1583, T1583.003, T1584, T1587, T1587.001, T1608
TA0001	T1078, T1566, T1566.001, T1190, T1133
TA0002	T1059.003, T1059.001, T1106, T1569.002, T1047
TA0003	T1543.003, T1547.001, T1053.005
TA0004	T1543.003, T1547.001, T1055
TA0005	T1070.004, T1112, T1140, T1562.001, T1027, T1055
TA0006	T1555, T1555.003, T1003, T1003.001, T1056.001
TA0007	T1082, T1083, T1057, T1016
TA0008	T1021, T1021.001, T1021.002, T1570
TA0009	T1005, T1113, T1056.001, T1560
TA0011	T1105, T1071.001, T1573.001, T1090
TA0010	T1041, T1567, T1567.002, T1048, T1048.003
TA0040	T1485, T1486, T1489, T1490

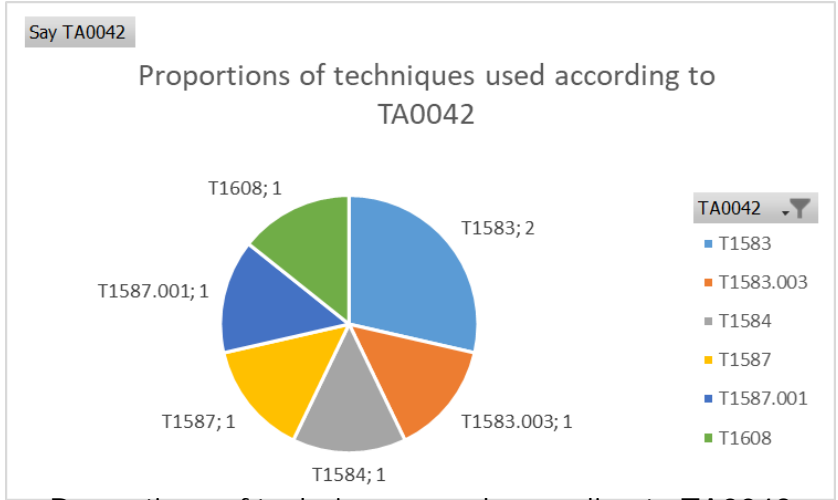
List of the most used techniques and sub techniques within the framework of MITRE ATT&CK in cyber-attacks against the maritime sector.



Discussion



Proportions of techniques used according to TA0043



Proportions of techniques used according to TA0042



Conclusion

The contribution of this study is to provide to maritime organizations systematic measures to mitigate and prevent the effects of cyber-attacks on maritime IT and OT systems. This study;

- (i) provides comprehensive mapping to helps organizations understand the full spectrum of adversary behavior and map it to their own security controls and defenses;
- (ii) enables the development of specific detection and mitigation strategies based on known adversary techniques and procedures;
- (iii) facilitates the integration of threat intelligence into security operations by providing a structured way to categorize and analyze threats;
- (iv) provides a common language for discussing and sharing information about adversary tactics and techniques among security professionals;
- (v) assists in identifying gaps in defenses and prioritizing security investments to protect against the most relevant threats.



Thank you for listening...

Istanbul Technical University Maritime Faculty
Maritime Security and Cyber Threats Research Laboratory

