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

Step 1
- **Data Collection and Categorization:** Obtain the cyber incidents in the maritime domain from several reports and literature sources. Categorize the data as cyber groups that are effective in the maritime industry, the malware and operating system tools they use.

Step 2
- **Identify Relevant Tactics and Techniques:** Map the observed cyber incidents in the maritime domain to the tactics and techniques listed in the MITRE ATT&CK framework.

Step 3
- **Threat Actor Profiling:** Identify threat actors that target maritime organizations and map their known behaviors to the ATT&CK framework.

Step 4
- **Threat Hunting:** Proactively search for signs of compromise by looking for indicators that align with the tactics and techniques in the framework.

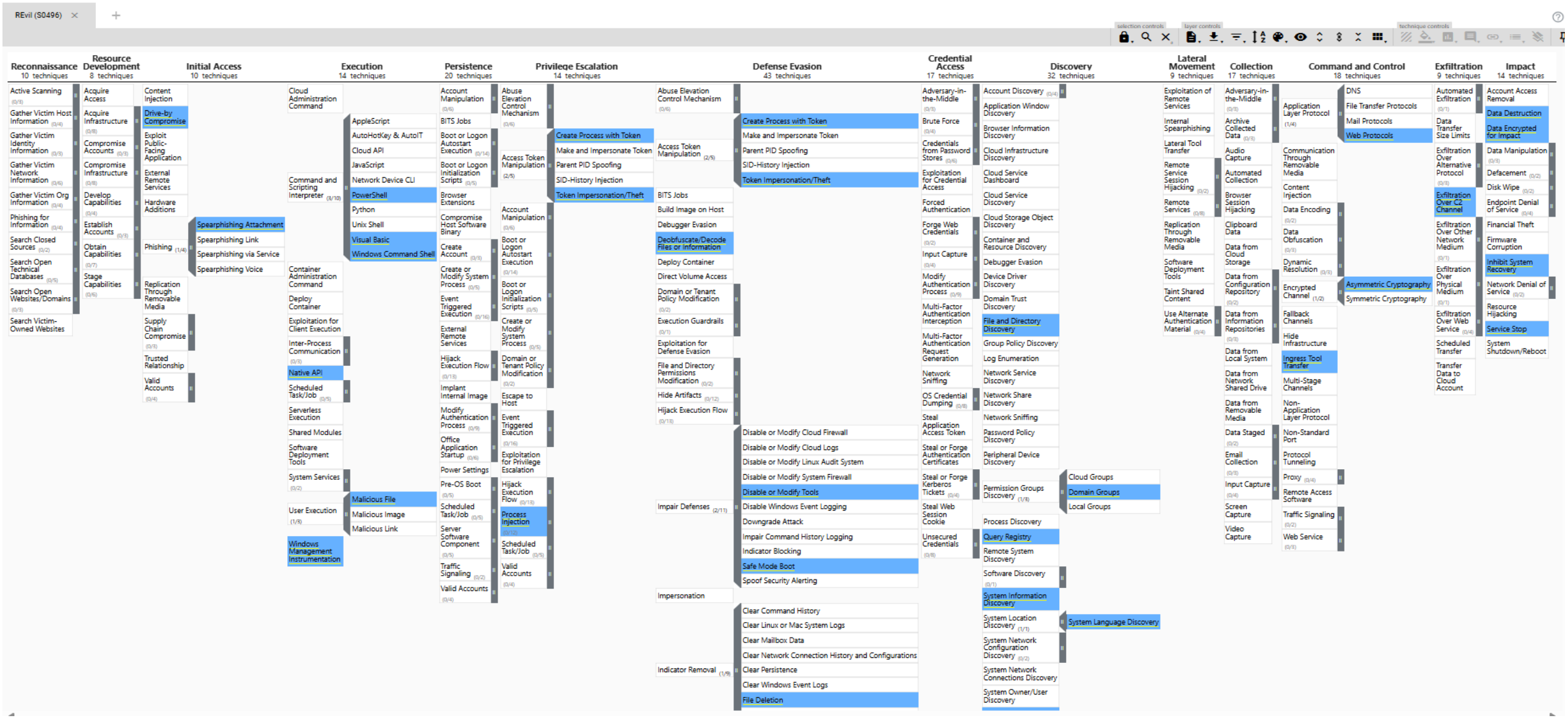
Step 5
- **Attack Investigation:** Use the framework to investigate and understand the nature of an attack for maritime systems.

Step 6
- **Cyber Mitigations and Strategies:** Plan cyber security actions in maritime by referencing the framework's mitigation and response recommendations for the identified techniques.

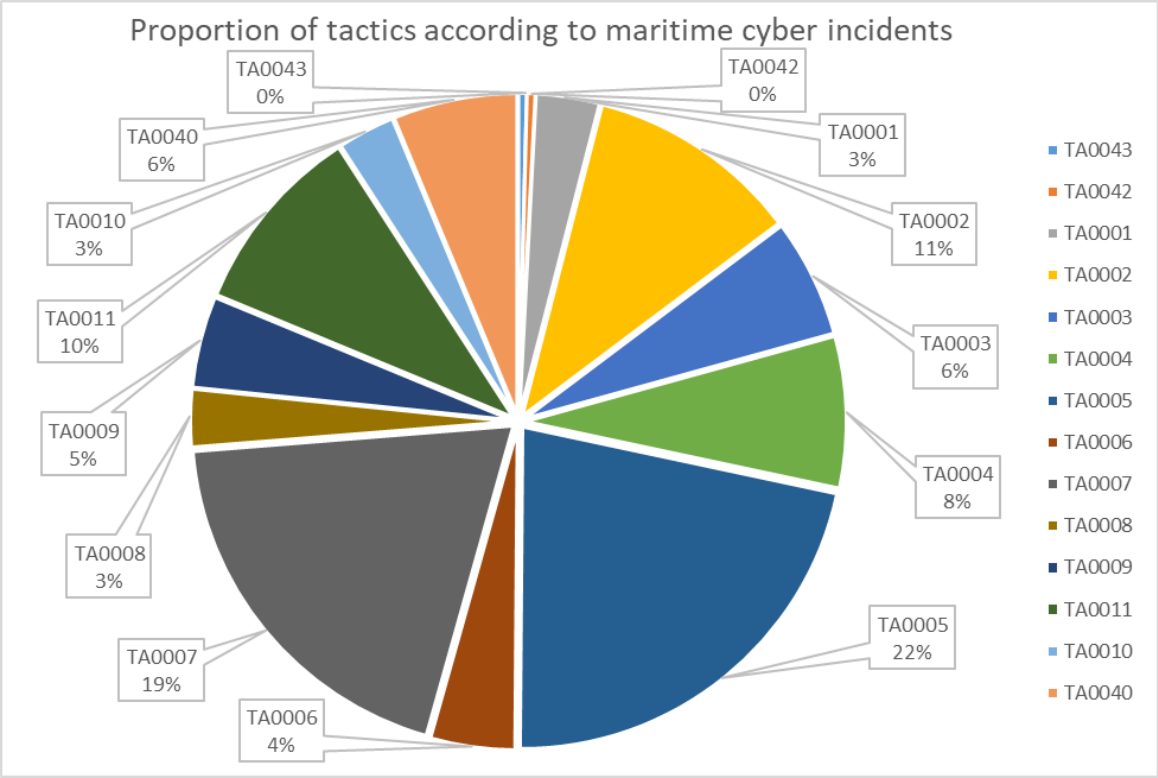
List of cyber gangs, the specific malicious software and operating system utilities impacting the marine sector

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	Livornopress (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



Analysis and Results

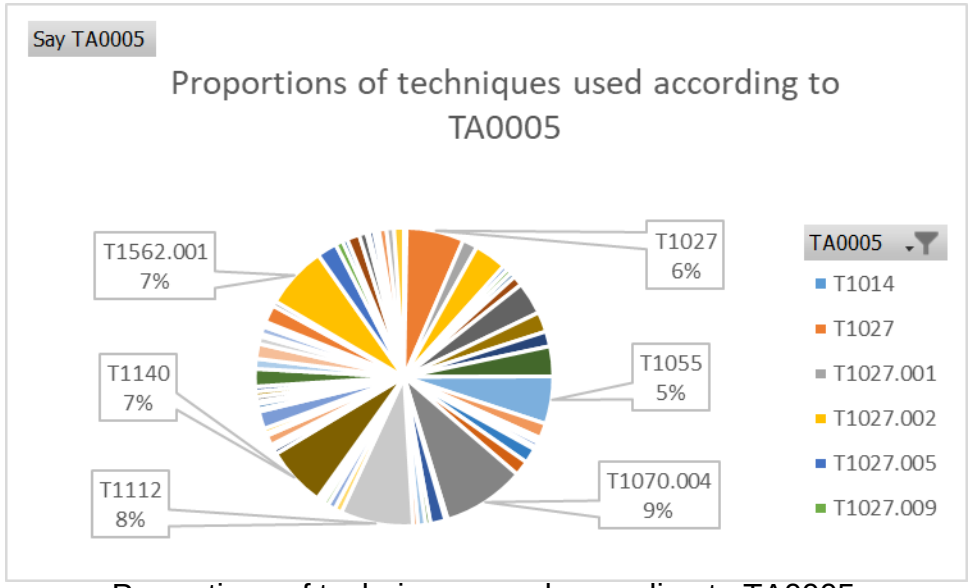


The proportion of the tactics, which is used most by cyber gang in the maritime sector

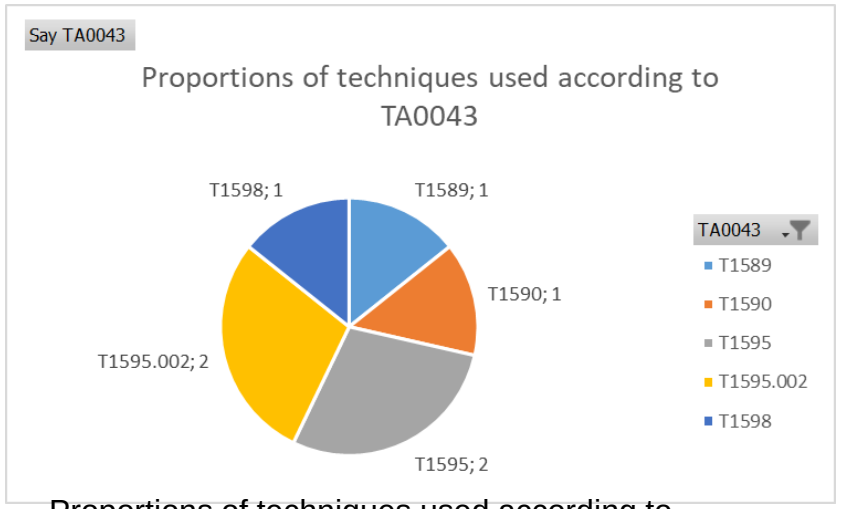
Tactics	Techniquies and Sub-techniques
TA0043	T1589, T1590, T1595, T1595.002, T1598
TA0042	T1583, T1583.003, T1584, T1587, T1587.001, T1608
TA0001	T1078, T1566, T1566.001, T1190, T1133
TA0002	T1059.003, T1059.001, T1106, T1569.002, T1047
TA0003	T1543.003, T1547.001, T1053. 005
TA0004	T1543.003, T1547.001, 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.

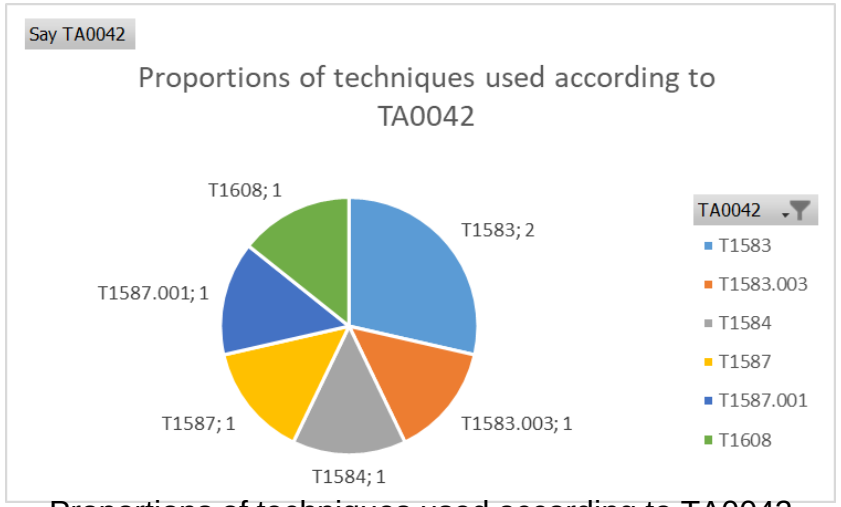
Discussion



Proportions of techniques used according to TA0005



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