



MARITIME CYBER THREAT

OVERVIEW 2022

M-CERT-2023-CTI-001
APRIL 2023

TLP:CLEAR

TLP:EX:NC

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

Sources are free to specify additional limits on sharing: these must be respected by recipients : retransmission prohibited to clients or subscribers (NC).

Reproduction, distribution and commercial use prohibited without written authorization from France Cyber Maritime.

Copyright France Cyber Maritime - 2023



Maritime Cyber Threat Overview 2022

Table of Contents

Table of Contents	2
1 Introduction	4
1.1 The maritime and port sectors	4
1.2 Digital and maritime	6
2 Maritime Cybersecurity: 2022 Overview	8
2.1 Context	8
2.2 Threat Analysis	8
2.3 Key Figures	9
3 The maritime sector faced with opportunistic cybercrime attacks	11
3.1 Phishing: the main initial intrusion vector	12
3.2 Infostealers and the maritime sector	18
3.3 Data leaks and resales in the maritime sector	27
3.4 Business Email Compromise (BEC)	30
3.5 Ransomware	36
4 Targeted attacks against the maritime sector	42
4.1 USB memory sticks, an initial infection vector still relevant to the sector	42
4.2 A maritime ecosystem spoofed for social engineering purposes	43
4.3 Threats targeting « Supervisory Control And Data Acquisition » and « Industrial Control Systems » (ICS)	46
4.4 Submarine Telecommunication Cables	49
4.5 Satellite Communications (SATCOMs)	49
4.6 Global Navigation Satellite System Jamming and Spoofing	50
4.7 Automatic Identification System Jamming and Spoofing	52
5 Maritime stakeholders: collateral victims of political cybercrime?	54
5.1 Distributed Denial of Service Attacks	54
5.2 Threat actors conducting DDoS attacks	57
6 Maritime Cybersecurity: Outlook for 2023	63
7 Glossary	65
8 About France Cyber Maritime and the M-CERT	67
9 About OVN	68
10 References	69



Maritime Cyber Threat Overview 2022

Dear Members and Partners of France Cyber Maritime,

Dear actors of the maritime, port and cybersecurity sectors,

As France Cyber Maritime celebrates its second year of existence, I'm delighted to share with you its first annual overview of the maritime cyber threat for the year 2022, produced in cooperation with OWN.

The year 2022 saw a strong recovery of the global maritime activity, thanks to the decline of the pandemic. But the year was also tragically marked by a war at Europe's borders, which had a major impact on our economies and on the maritime and port sector. This conflict, combined with recurring tensions in Asia, makes it difficult to establish a clear picture of the future of the security of our common maritime horizons.

The pandemic has reminded us of the importance of the maritime and port sector to our economies, and the vital role played by ports, ships, sailors and all maritime and port logistics and support teams. The increasing digitalization of the entire maritime ecosystem directly contributes to its performance, safety and security. But it also brings new vulnerabilities. Many players, in France and abroad, face cybersecurity challenges and incidents on a daily basis. Cyberattacks perpetrated by state actors, cybercriminals and hacktivists impact the operation of the sector, and can have serious financial and physical consequences. It is essential to give the highest priority to our digital resilience.

This threat overview aims to give a global panorama of the cyber threats having affected the maritime sector in 2022, and to offer some perspectives for 2023, to help our members, partners and readers share a common vision. Working together to share and better understand this evolving threat landscape is, more than ever, essential for conducting our maritime activities in security.

France Cyber Maritime continued to grow in 2022, welcoming new major players in the maritime and port sector, new cybersecurity companies and public administrations and services, as new members and partners. We would like to thank them all. We look forward to meeting you in 2023, at our Annual General Meeting, at the *European Maritime Days*, at the *European Cyber Week*, at the Assises de l'économie de la mer or during *Battleship 2023*, our live European *Bug Bounty* event!

We hope you enjoy reading this report as much as we enjoyed co-writing it!

Xavier REBOUR, Managing Director of France Cyber Maritime



Maritime Cyber Threat Overview 2022

1. Introduction

Our partners, members and other public and private entities in the maritime and cybersecurity sectors regularly request an annual, open overview of the maritime cyber threat. Drafting this type of report requires care and precaution, due to the sensitivity of the information, the volume of information to be processed and the multiplicity of sources.

Of course, this annual report is not intended to summarize or evoke the full spectrum of events shared by M-CERT with its members and partners, but we have tried to synthesize the relevant information as best as we can.

This threat overview owns the **TLP:CLEAR** mark. As defined by¹, this mark indicates that readers may distribute this information without any particular restrictions, while respecting the rights and obligations associated with copyright.

In order to respect the **TLP:CLEAR** protocol, the information contained in this report comes exclusively from public information available from open sources on the Internet, combined with analyses carried out by M-CERT and/or OWN-CERT.

Due to their public nature, these figures represent only a fraction of the attacks targeting the sector in 2022. As a result, the detection of state-sponsored and advanced threats (such as *Advanced Persistent Threats - APT*) is rarely publicized, or only possible with a sometimes long delay. Their partial nature, coupled with analyses of other sources available to M-CERT and/or OWN, nevertheless enable us to identify some interesting trends.

The ADMIRAL public database², provided by M-CERT, provides a good overview of the majority of public attacks recorded by M-CERT that have affected the sector over the years.

1.1. The maritime and port sectors

The maritime and port sector (Figure 1-1) is a global, complex and interwoven industrial sector, involving numerous players on land and at sea, including:

- Ports: whether trading, fishing, multimodal, of local, regional, national or international importance: with their *hinterland*³, they supply the economy with raw materials, goods and services essential to our economies;
- Ships, in all their diversity: passenger ships, container ships, LNG carriers, oil tankers, support vessels, research vessels, cable-laying ships;
- Shipowners;
- Offshore installations;

Maritime Cyber Threat Overview 2022

- Numerous companies in the maritime sector: suppliers, integrators, manufacturers, subcontractors, shipyards;
- Naval industry;
- Yachting;
- The fisheries, aquaculture and seafood sector;
- Transport, logistics and materials handling professionals;
- Classification and insurance companies;
- Shared maritime digital services;
- Maritime public bodies;
- Marine Renewable Energies (MRE);
- Maritime schools and research centers;
- Submarine infrastructures: submarine cables, gas and oil infrastructures.



Figure 1-1 : Schematic representation of part of the marine ecosystem. © Cluster Maritime Français, reproduced with their kind authorization.

The Cluster Maritime Français estimates that, in 2021, the French maritime economy represented 386,000 direct jobs, and was responsible for a production value of 90.6 billion euros⁴. On a global scale, 80% of the world's goods are transported by sea. The free movement of goods and people at sea, the smooth operation of ports and, consequently, of the digital systems that make them up, are therefore of particularly strategic importance.

The way the maritime sector operates is sometimes misunderstood, and can be perceived as complex. There are several reasons for this:

- Global nature of shipping, with numerous global, national, regional and local players;



Maritime Cyber Threat Overview 2022

- Rich and diverse regulations, issued by international, national and regional bodies;
- Impact of geopolitics on the sector;
- Variety of ships, ports and associated industrial and digital facilities.

The civil maritime sector is also at the crossroads of a number of other sectors, with which it interacts or is interconnected:

- Naval defense, often with possible dual-use technologies;
- Trade and logistics;
- Energy;
- Telecommunications.

1.2. Digital and maritime

In digital terms, a port and a ship are complex systems of systems, combining traditional information systems (*Information Technology*, IT) with industrial, cyber-physical or dedicated systems, often grouped together under the term OT (*Operational Technology*)⁵.

The digitization of ships and ports has developed considerably over the last ten years, bringing greater flexibility, speed, security and traceability throughout the maritime logistics chain. This ongoing digital transformation continues with the development of *smart shipping* technologies (remote monitoring, preventive and corrective maintenance), *green shipping* (integration of environmental issues) and the development of maritime drones and autonomous ships.

This digitization is also leading to a level of interdependence and digital exposure of maritime and port systems never seen before. In addition to this observation, which can be made in other industrial sectors, there are a number of sector-specific peculiarities:

- Connectivity constraints for ships, which remain dependent on the smooth operation of their satellite telecoms systems at sea, or 4G/5G telephony networks close to shore. Even if telecommunication systems have drastically improved in recent years, these dependence, bandwidth and cost characteristics restrict maintenance, administration and remote monitoring operations;
- The sector's highly competitive environment is a major constraint on ship operations, as ships have to optimize their journey times, their presence in port and their loading and unloading operations: availability times, and therefore quayside intervention times, are therefore limited;
- The almost general absence of human cyber resources, or even digital specialists on board most civilian ships, makes any investigation or intervention on digital systems more complex;
- The peculiarities of ships' IT and OT systems, with their heterogeneous technologies from multiple manufacturers and integrators, sometimes with poor awareness to cybersecurity issues, lead to significant "black box" effects and difficulties in patch management and the rapid onset of obsolescence.



TLP:CLEAR

TLP:EX:NC



Maritime Cyber Threat Overview 2022

Potential breaches of confidentiality, integrity or availability of maritime and port information systems can have major consequences for the sector. While their occurrence and potential impact depend heavily on the systems concerned and their use, the consequences can be:

- Loss of business continuity (e.g. port operations);
- Compromised safety or security of ship and crew;
- Malfunctions due to circumvention of safety measures and procedures.

The financial, regulatory, human, environmental and brand image stakes for the company or organization are critical.

TLP:CLEAR

TLP:EX:NC



Maritime Cyber Threat Overview 2022

2. Maritime Cybersecurity: 2022 Overview

2.1. Context

From a geopolitical and economic point of view, the year 2022 was marked by two major events for the maritime sector:

- The need for the sector to get back up and running very quickly, after two years of pandemics that had severely slowed down activity and complicated the organization of the supply chain;
- Russia's invasion of the Ukraine on February 24th, 2022, with major geopolitical, military and economic consequences not seen since the Second World War. This invasion has led to the reinforcement of the bipolarity of certain cybercrime players, and even to their clear affiliation in support of certain countries or zones of influence. In a globalized context, this invasion will have lasting consequences for all the countries on the planet, which remain uncertain, if not unknown, today.

The strategic nature of the maritime and port sectors was regularly recalled during 2022, with concerns on freedom of movement at sea, and on the integrity and resiliency of undersea infrastructures (submarine telecommunication cables, pipelines, Marine Renewable Energies (MRE)).

2.2. Threat Analysis

Like other industrial sectors, the maritime and port sector faces three types of threat:

1. The state and state-sponsored threat, either frontal or covert. The highly strategic nature of the sector can make it a « target » in the eyes of certain competitor countries. The technical, human and hybrid attack capabilities of these countries are significant, and need to be constantly monitored and assessed, whether for espionage, sabotage or pre-positioning purposes.
2. The cybercrime threat, which can take two forms:
 - The first, purely opportunistic, aims to exploit vulnerabilities in maritime and port information systems exposed on the Internet (services not updated or poorly secured, etc.). This is essentially the case with ransomware attacks and extortion attempts during data leaks. In the case of certain groups, state support is no longer in doubt.
 - The second, which targets the maritime and port sectors in particular, uses techniques such as spear-phishing and Business Email Compromise, with the aim of reselling access and running scams (e.g. fake bank wire transfer orders). These attacks and attempts, which are ongoing, often use the creation of similar domain names and e-mails that are sometimes correctly forged to deceive the victim. Beyond the damage to reputation, this type of attack can be a precursor to more advanced and destructive attacks.
3. The hacktivist threat, which particular feature in 2022 was a clear reinforcement of bipolarization. Thus, attacks that had become less high-profile than before, such as Distributed



Maritime Cyber Threat Overview 2022

Denial of Service (DDoS) attacks, were once again detected in support of politically influential actions, as in the cases of the "Killnet" or "NoName057(16)" groups. These attacks, although often temporary and of relatively limited complexity, are now coordinated in real time via social networks, with an almost daily list of targets to aim at. The consequences, albeit limited, tend to be attacks on reputation from an influence perspective. In some cases, there is little doubt of affiliation, or even coordination, with certain states.

2.3. Key Figures

2.3.1. Global Trends

At the time of writing, and with the usual precautions regarding figures, over 90 notable and public cybersecurity incidents were detected in the maritime and port sector worldwide in 2022, an increase of 21% compared to the previous year, and of 135% compared to 2020. The continuous increase seen in recent years, is essentially attributable to the strengthening of cybercriminal activity.

Proportionally, the four maritime and port sub-sectors most affected by public cyber attacks in 2022 are, in ascending order:

1. Shipowners (15%), stable compared to 2021;
2. Ports (17%), an increase of 70% compared to 2021;
3. Logistics and transport (18%), an increase of 50% compared to 2021;
4. The shipping industry and suppliers (21%), with a 6-fold increase compared to 2021.

These figures seem to provide the following insights:

- Shipowners continue to fall victim to serious attacks, particularly by ransomware. While coordination and action by law enforcement agencies, combined with certain measures taken by shipowners, appear to be bearing their first fruits, the situation remains highly heterogeneous, depending on the size of the shipowner, its level of maturity and, often, the cyber dynamism of its home country and partners.
- The number of attacks on ports continues to rise significantly, mainly outside Europe. Many of these complex ecosystems, with their many players, are still struggling to achieve in-depth security.
- Logistics and transport continue to be the main victims. Our analyses show that they are particularly exposed to *phishing* and *spearphishing* attempts, which are highly realistic and specifically target this type of player. Acting in direct digital link with many other players in the sector (forwarding agents, ports, shipowners...), securing them in the years to come is a major challenge.
- Successful attacks targeting the maritime industry and the supply chain in general, even beyond logistics and transport, are particularly worrying. By opportunistically or deliberately targeting these players (digital or physical service providers, maintenance operators, equipment

Maritime Cyber Threat Overview 2022

manufacturers, etc.), attacks can have a global impact on a large number of ships and shipowners, who may lose the access they need for their day-to-day operations (e.g. cloud or managed services).

- The precursors, already noted in 2021, relating to Marine Renewable Energies (MRE) and river transport, continue into 2022.
- In terms of geographical zones, Europe was the continent proportionally most affected in 2022 (40% of attacks reported, stable), followed by Asia (34%, down) and North America (21%, down). The number of attacks in Europe is higher than in 2021, as the impact of the Russian-Ukrainian conflict has led to a number of opportunistic attacks on Western public and private maritime entities. The main events on the European continent are shown in Figure 2-1.

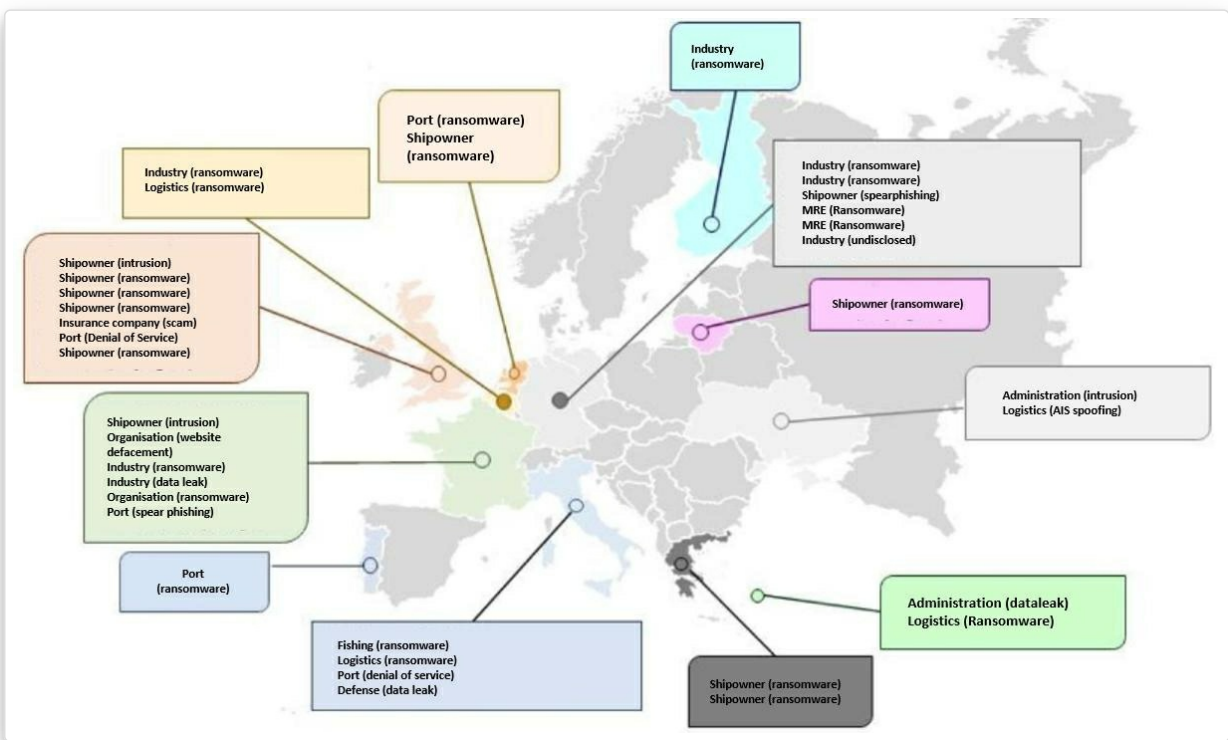


Figure 2-1 : Breakdown of the main maritime cybersecurity incidents in Europe. Source: M-CERT/ADMIRAL



Maritime Cyber Threat Overview 2022

3. The maritime sector faced with opportunistic cybercrime attacks

Opportunistic cybercriminal attacks aim to exploit one or more vulnerabilities in a service generally exposed on the Internet to compromise an organization for profit. Although no cybercriminal group stands out for activities specifically targeting the maritime sector, the strategic and global nature of the sector, on which many business sub-sectors depend, can make it a prime target for profit-driven attacks.

The key issue is the collection of credentials in order to gain initial access. To achieve this, attackers rely on three types of operation:

Exploitation of vulnerabilities: initial access data can be obtained by exploiting vulnerabilities on exposed equipment. The main types of access sold include VPN, RDP, Pulse Secure, Fortinet and Citrix. The vulnerabilities exploited vary according to the adversary's *modus operandi*, their technical level and the availability of exploitation tools. Several vulnerabilities released in 2021 and 2022 are still being actively exploited by attackers. The most common in 2022 were those relating to Fortinet, Zimbra, VMWare, Citrix and Microsoft products (notably Exchange⁶).

Recommendation

An exhaustive mapping of the information system, together with a vulnerability management policy, is essential to quickly identify and fix any vulnerability which exploitation would enable the compromise of critical credentials.

Force brute attacks: the attacker uses « off-the-shelf » tools, with dictionaries or algorithms to test, one after the other, every possible combination of a password for a given identifier, in order to identify privileged accounts that are insufficiently secure or which default passwords have not been changed.

Recommendation

The most obvious recommendation is to block accounts after a defined number of failed authentications, or to use Multi-Factor Authentication (MFA). Tools for detecting and countering brute-force attacks are fairly common, but still insufficiently present throughout the perimeter of information systems in the maritime sector, particularly on certain proprietary equipment. Nor are they necessarily contractually required for subcontractors and hosting providers. Here again, sharing information related to this type of detection with M-CERT enables global analysis at the sectoral level, and alerts the entire maritime and port community.

Phishing attacks: the orchestration of *phishing* campaigns is made easy by the existence of dedicated services (« Phishing as a Service » platforms) and the distribution of phishing kits. Targeted e-mail addresses are also easy to list, through the use of e-mail address databases recovered from data leaks (*combo-list*), the automated collection of exposed addresses (*email web scraping*) or the identification of default address formats and technologies used within an organization, (eg



Maritime Cyber Threat Overview 2022

firstname.name@entity.tld combinations).

Recommendation

Protection against phishing is still insufficient in many entities. A combination of organizational, technical and human measures is required. Centralized efforts to target *phishing* infrastructures and attacker groups are still insufficient, given the quickly evolving nature of the threat. Reporting phishing-related technical and operational intelligence to the M-CERT is therefore essential if the M-CERT is to analyze and counter this type of threat. These reports and analyses contribute directly to the rapid and effective sharing of information within the sector, to improve protection for all stakeholders.

Every month, OWN produces sectoral cyber threat intelligence for the M-CERT, based on the detection, investigation and analysis of attack campaigns affecting the maritime sector. This work shows that, in 2022, the maritime sector was the target of numerous *phishing* campaigns delivering *infostealer* malicious code. This data is generally offered for resale, then exploited for *Business Email Compromise* or by ransomware operators.

3.1. *Phishing*: the main initial intrusion vector

Phishing remains the preferred intrusion vector across all business sectors, accounting for almost 70% of cyberattacks⁷. The maritime sector is no exception to these generic campaigns (eg, prompts to connect to fake cloud platforms, with the aim of recovering login credentials/passwords for subsequent resale). However, some players are taking a particular interest in the sector, and tailoring their attack campaigns to maximize their chances of success. Several operations identified during 2022 exploit keywords, images, document formats, signatures or attachments rooted in the realities of the sector.

OWN-CERT tracks phishing campaigns impersonating major shipowners on a daily basis. Over the year 2022, a predominance in the spoofing of shipowners Maersk and CMA-CGM has been noted (Figure 3-1). Among these campaigns, it is possible to distinguish phishing operations specifically targeting players in the maritime sector from those spoofing the maritime ecosystem to target companies in other sectors, such as logistics (Figure 3-2).

We also dissociate *phishing* campaigns distributing links leading to a page impersonating the owner (*typosquatting*), from those directly distributing malicious attachments.

Maritime Cyber Threat Overview 2022

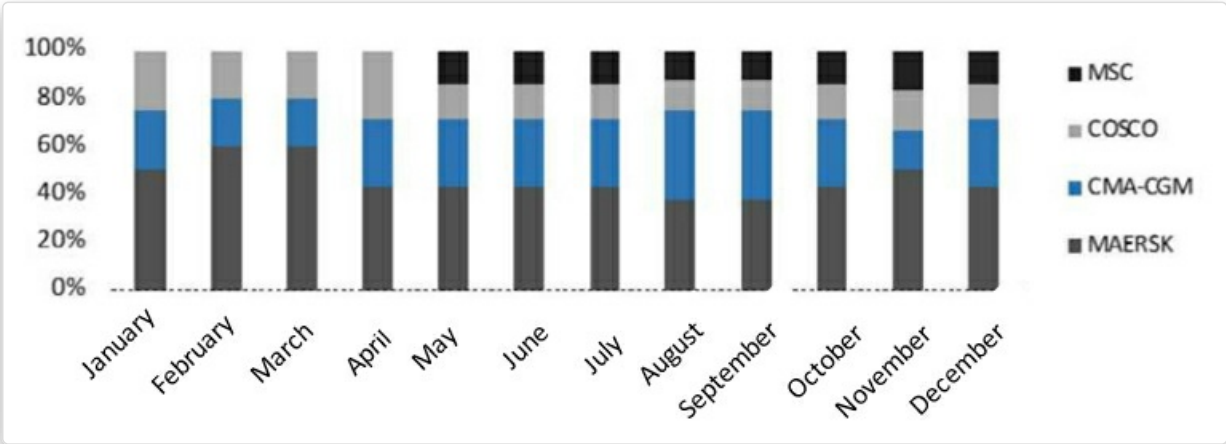


Figure 3-1 : Breakdown of major phishing campaigns identified in 2022. Source: OVN-CERT.

Please find H/BL and TDR in attached files.

POL: HO CHI MINH
 POD: LATAKIA
 T/S PORT: WEST PORT KLANG // JEBEL ALI
 Vot: 15S
 ETD: 04/07/2022
 Carrier: (VIETNAM) CO., LTD

1. BL Number: OVG/SGN/LTK-9820/22

- BK No. B-11000/22
- Freight status: PREPAID
- HS code: 400110
- Vol: 1x20'GP
- BL Status: PLEASE HOLD TELEX TILL FURTHER INFORM

Kindly check and advise connection details once available. Thanks team.

Kindly acknowledge PRE ALERT by replying.

Thanks & Best regards,

Shipping Line CO. LTD (SLD)

 Add: Floor 20
 Mobile: (84)937
 Website: <https://sealind.com>

From no-reply@cma-cgm.com <it@37-74-68-126.biz.kpn.net> @

To [Redacted]

Subject **Bill of Lading**

Dear Consignee,

Please find attached your Bill of Lading for the current shipment heading to your port. Shipping customer advised us to contact your email [Redacted] as the consignee/receiver of the goods in transit.

ETA of cargo also included in the attached file. Download to view and also print a copy.

Thank you for your support.

Best regards,
 The CMA CGM Group
CMA CGM | A world leader in shipping and logistics.

From Mearsk Shipping <es@offass.ga> @

To [Redacted]

Subject **Mearsk Shipping Notification**

<https://www.opportunitiesforafricans.com/wp-content/uploads/2018/05/maersk.png>

hello, [Redacted]

Please find attached below your Bill of Lading, Packing List and Invoice for the current shipment headed to your port. Shipping customer advised us to contact your email [Redacted] as it was listed as the consignee/receiver of the goods in transit.

ETA of cargo also included in the attached files.

Thank you for your continued support.

Note: We will not be responsible for any charges incurred due to late confirmation of shipping documents.

MAERSK LINE - The Shipping & Logistics Group.

Figure 3-2 : Realistic phishing emails targeting the supply chain.

Maritime Cyber Threat Overview 2022

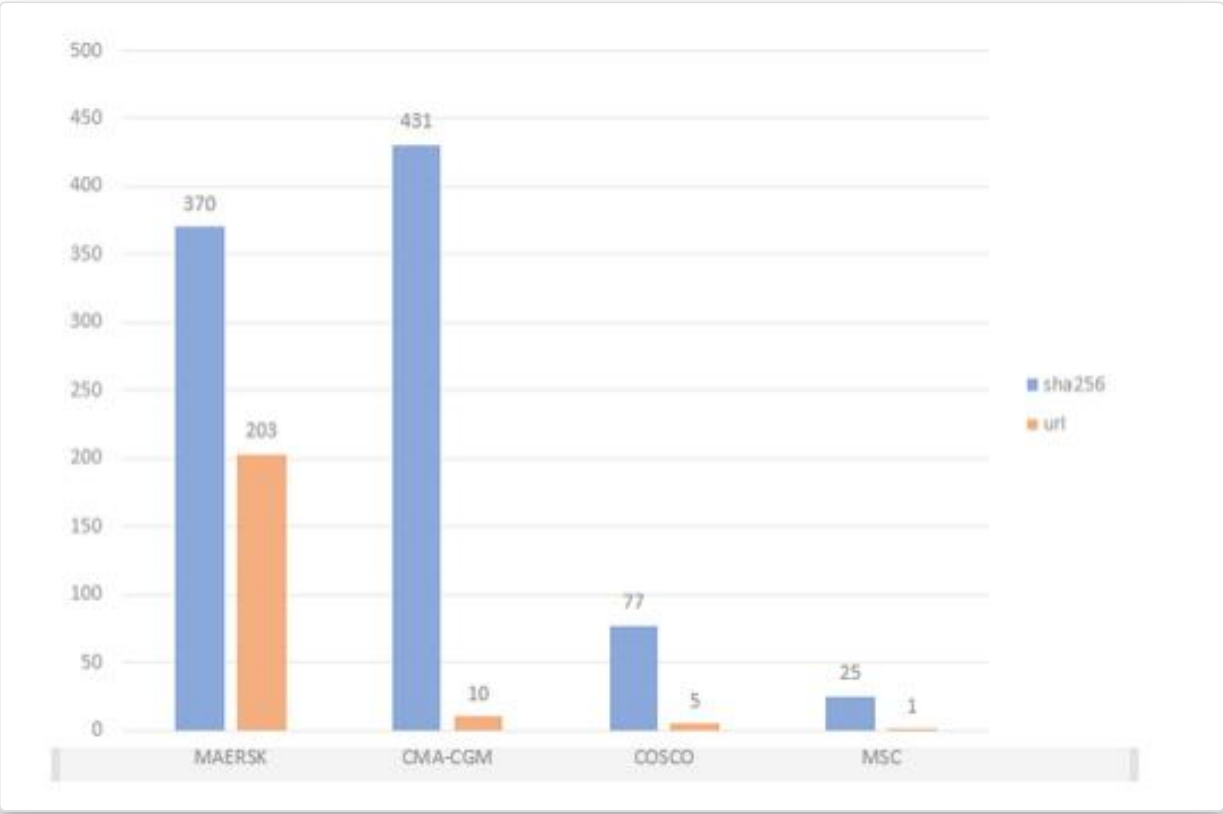


Figure 3-3 : Breakdown of major phishing campaigns identified in 2022, by spoofed shipowner, distinguishing the technique used: links (URL) and attachments (SHA256). Source: OWN-CERT.

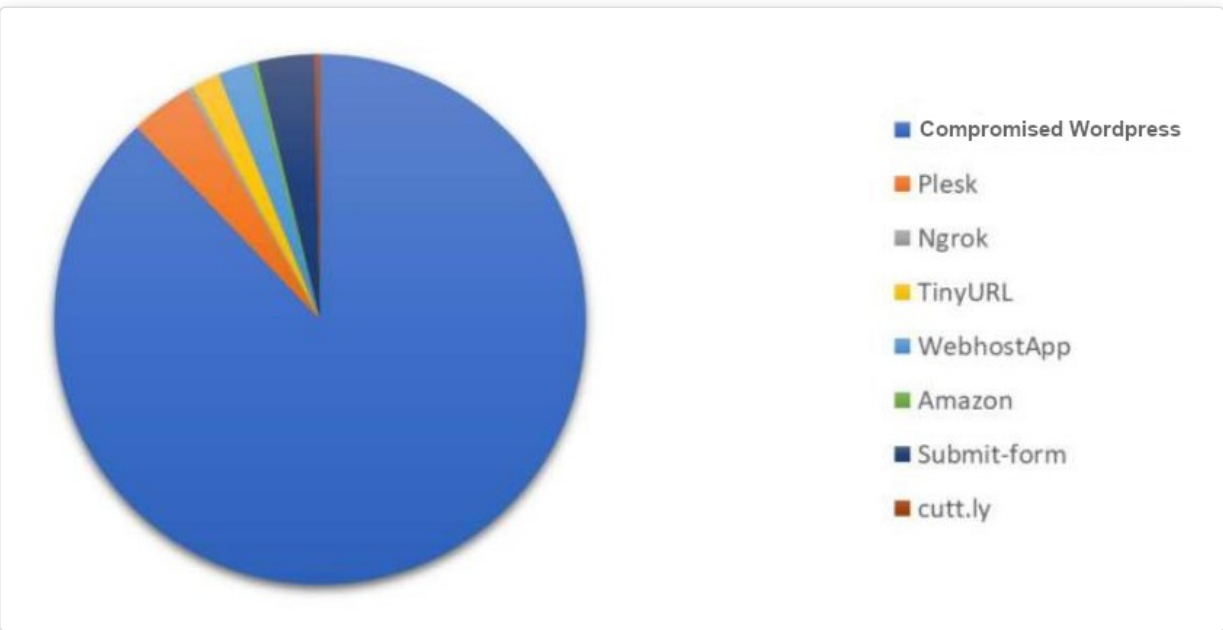


Figure 3-4 : Main services used to host phishing infrastructures. Source: OWN-CERT.

Maritime Cyber Threat Overview 2022

MITRE ATT&CK⁸'s distinction of the two sub-techniques (*Spearphishing Link* (T1566.002) and *Spearphishing Attachment* (T1566.001)) enables precise analysis of the corresponding malicious infrastructures. Over 87% of the *phishing* pages distributed were hosted on compromised Wordpress sites. This was followed by Plesk, WebhostApp and Submit Form services (Figure 3-4).

3.1.1. Spearphishing Link (T1566.002)

The social engineering themes used (Figure 3-5) take up terms specific to the maritime sector (*Bill of lading, Terminal departure report, shipping documents...*), associated with names of players in the maritime world or maritime and port logistics. The most common are shown Figure 3-6.

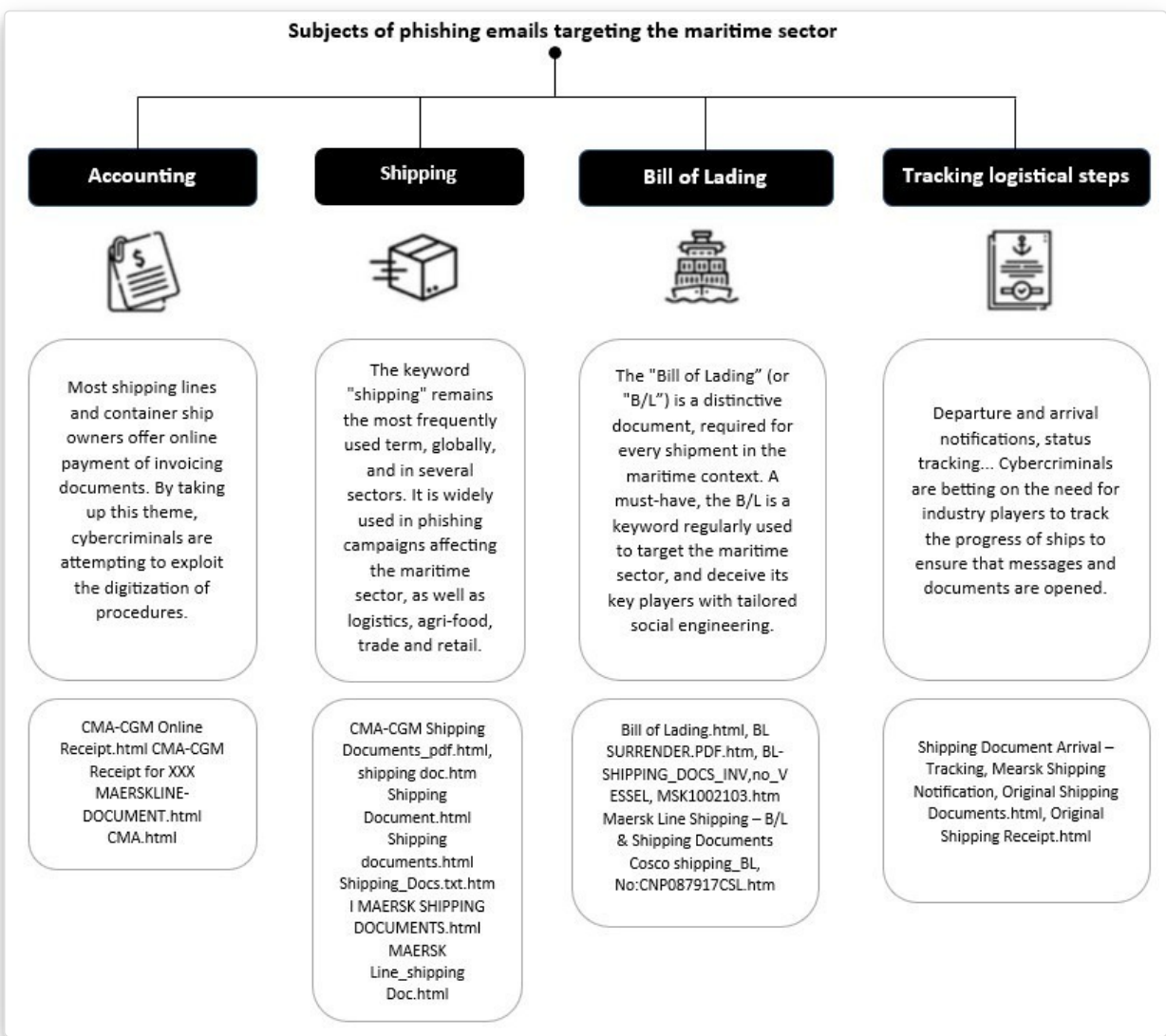


Figure 3-5 : Objects of phishing e-mails targeting the maritime sector. Source: OWN-CERT.

Maritime Cyber Threat Overview 2022



Figure 3-6 : Word cloud of all social engineering themes used in 2022. Source: OWN-CERT.

3.1.2. Spearphishing Attachement (T1566.001)

In order to be credible, the names of malicious files attached to phishing campaigns addressed to players in the maritime sector use the following 5 themes, sometimes combined: ship names, names of maritime and port stakeholders, geographical areas, logistics and invoicing.

The word cloud Figure 3-7 shows the keywords appearing in the executable files sent to the victims. Here too, the lexical field specific to the maritime and goods transport is recurrent, with the predominance of the term « *Bill of Lading* » (Figure 3-8).

Maritime Cyber Threat Overview 2022

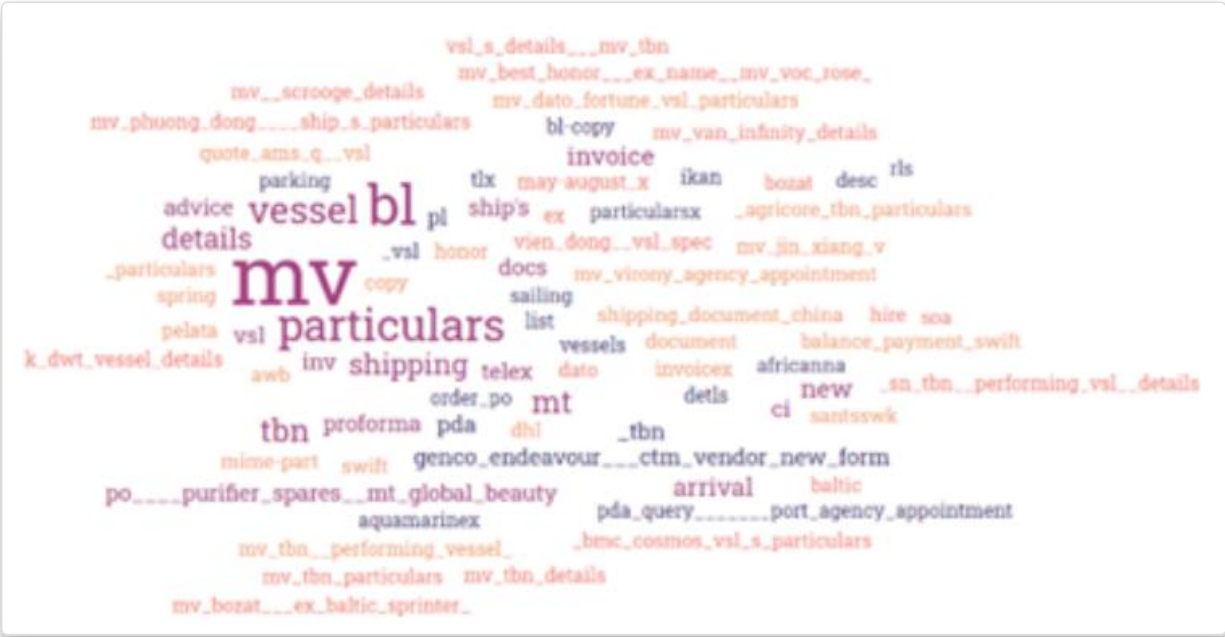


Figure 3-7 : Keywords cloud for malicious filenames targeting the maritime sector. Source: OWN-CERT.

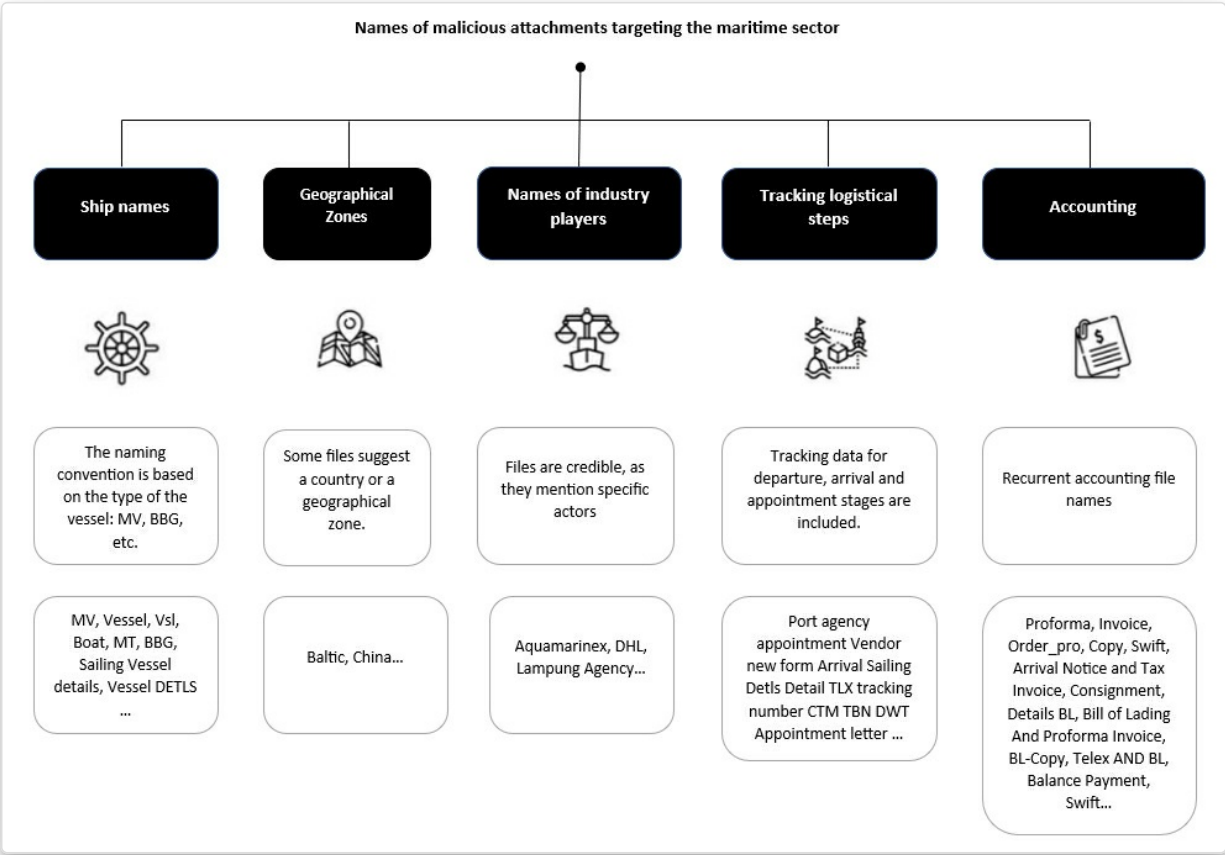


Figure 3-8 : Names of malicious file attachments targeting the maritime sector. Source: OWN-CERT.

Maritime Cyber Threat Overview 2022

3.2. Infostealers and the maritime sector

During its monitoring of threats affecting the maritime sector, OWN collected over 2,200 unique malicious binaries in 2022, over 1,600 of which were *infostealers*. These figures confirm the general trend: OWN was able to identify that the majority of malicious code topics on cybercrime forums in 2022 concerned *infostealers*. These malicious codes are sold on cybercriminal channels as « *malware-as-a-service* ».

Definition

An *infostealer* is a malicious code designed to collect data on an information system. This data includes connection information (banking or session cookies) (Figure 3-9).

From a methodological point of view, all the indicators collected for 2022 have been enhanced to identify the malicious codes distributed, the techniques used, the malicious infrastructures and the adversary operating modes in use.

24 families of *infostealers* targeting the maritime sector were detected over the year, with a large majority of samples of **Formbook** (also known as **Xloader**), **Agent Tesla**, **Snake Keylogger** and **Lokibot** (Figure 3-10).

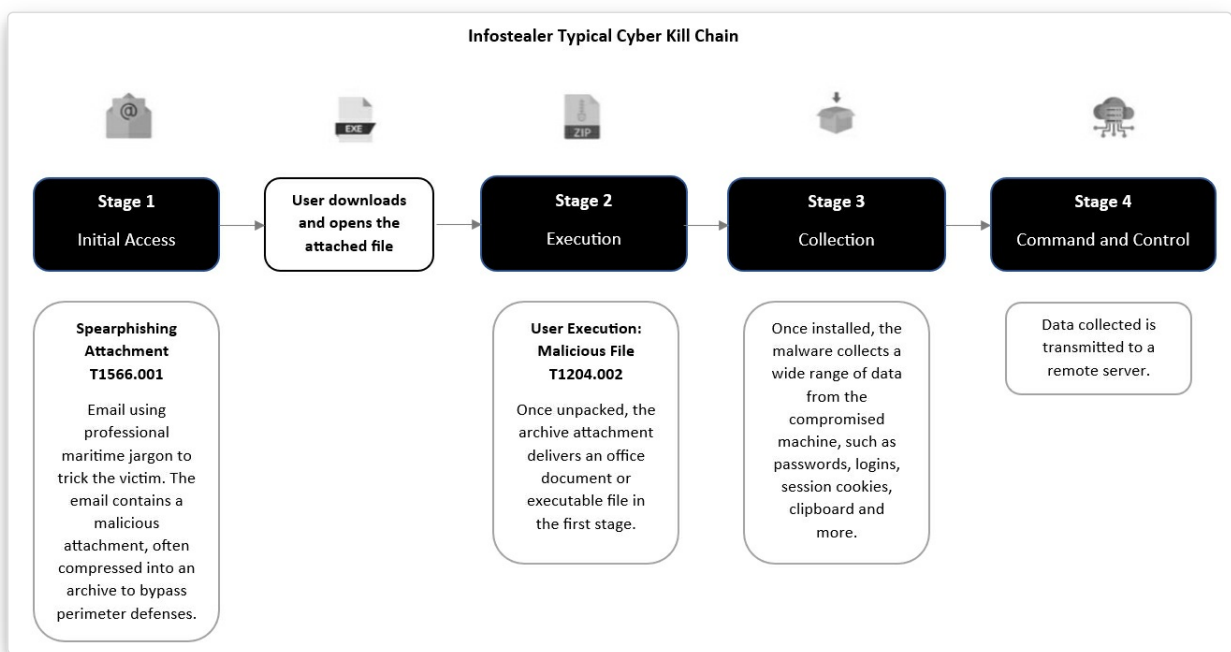


Figure 3-9 : Generic Cyber kill chain of the infostealer. Source: OWN-CERT.

Maritime Cyber Threat Overview 2022

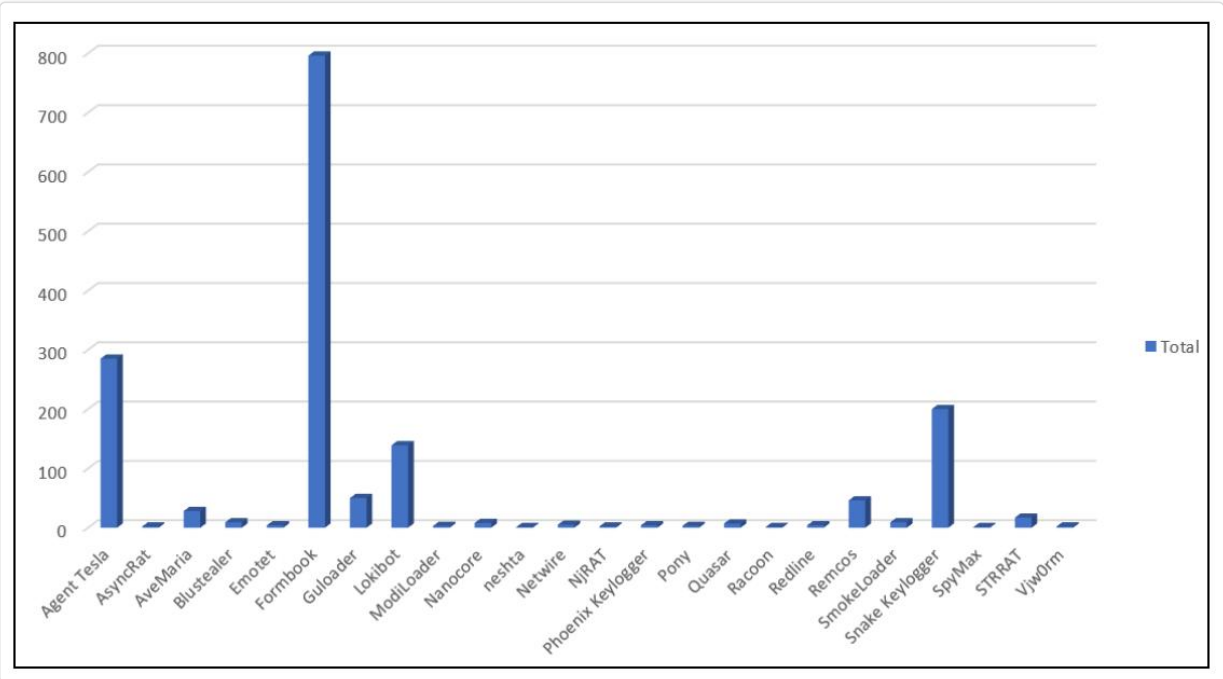


Figure 3-10 : Number of files per malicious code family. Source: OWN-CERT.

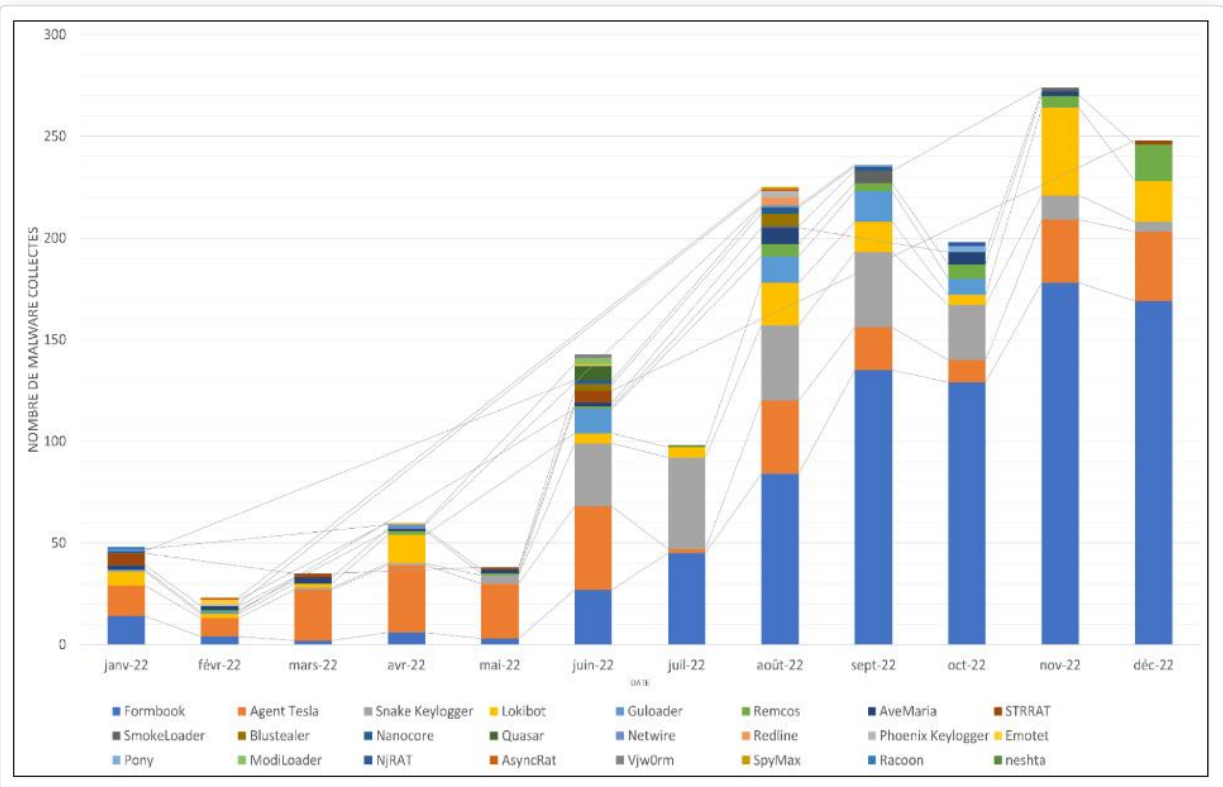


Figure 3-11 : Monthly evolution of the volume of infostealers in 2022. Source: OWN-CERT.

Maritime Cyber Threat Overview 2022

Figure 3-11 shows the evolution of the number of files collected each month per malicious code family. Several observations can be made:

- A steady increase in the number of malicious files targeting the maritime sector, with a peak at the end of the year;
- A balanced presence throughout the year of the Formbook, Agent Tesla and Lokibot infostealers;
- A sharp increase in the number of files linked to Snake Keylogger and Remcos from summer 2022.

3.2.1. Formbook (Xloader)

Over the course of 2022, OWN identified 796 samples delivering Formbook to targets in the maritime sector. This « malware as a service » is sold on several cybercriminal forums. It is often distributed via e-mail, with social engineering to encourage the victim to run it on his or her computer.

Definition

Formbook, also known as Xloader, is an *infostealer* dedicated to stealing data, forms and passwords. The malicious code injects itself into various processes and installs functions enabling it to record keystrokes (*keylogger*), retrieve clipboard contents, take screenshots or extract data from http sessions. It can also execute commands from a command and control (C2) server. Over 92 applications have been identified as targets of the malicious code, including « firefox.exe », « chrome.exe », « microsoftedgecp.exe », « opera.exe », « safari.exe » or « WhatsApp.exe »⁹.

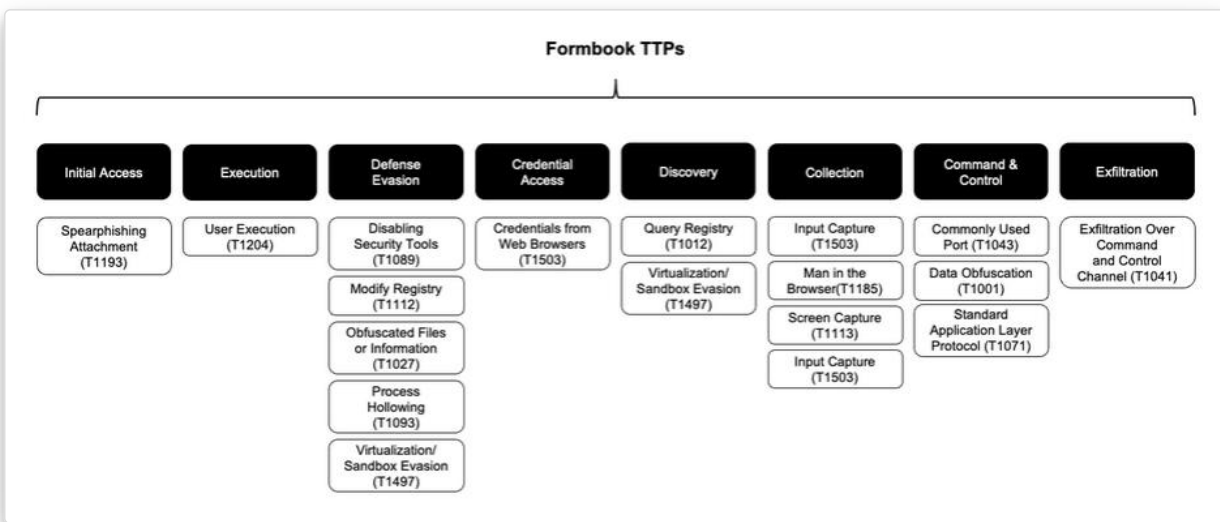


Figure 3-12 : Tactics, Techniques and Procedures of Formbook. Source: MITRE ATT&CK.

Once decompressed, the file¹⁰ in .rar archive format deposits a *Formbook* executable on the compromised workstation¹¹. The executable takes up the sector vocabulary, using the existing ship

Maritime Cyber Threat Overview 2022

naming format « MV¹² ship name ». Over various campaigns, it has displayed several ship names (Figure 3-13).

By analyzing the e-mail headers, OWN was able to observe the impersonation of a Singapore-based freight forwarding company: PLATINA BULK CARRIERS. The body of the e-mail confirms that the attacker is well versed in industry jargon and uses it to harvest information about the targeted port and entice the victim to execute the attachment. By pivoting on the IPv4 address of the sending server, OWN was able to identify numerous other emails specifically targeting the maritime sector over the same period. All delivered a malicious attachment (Figure 3-14).

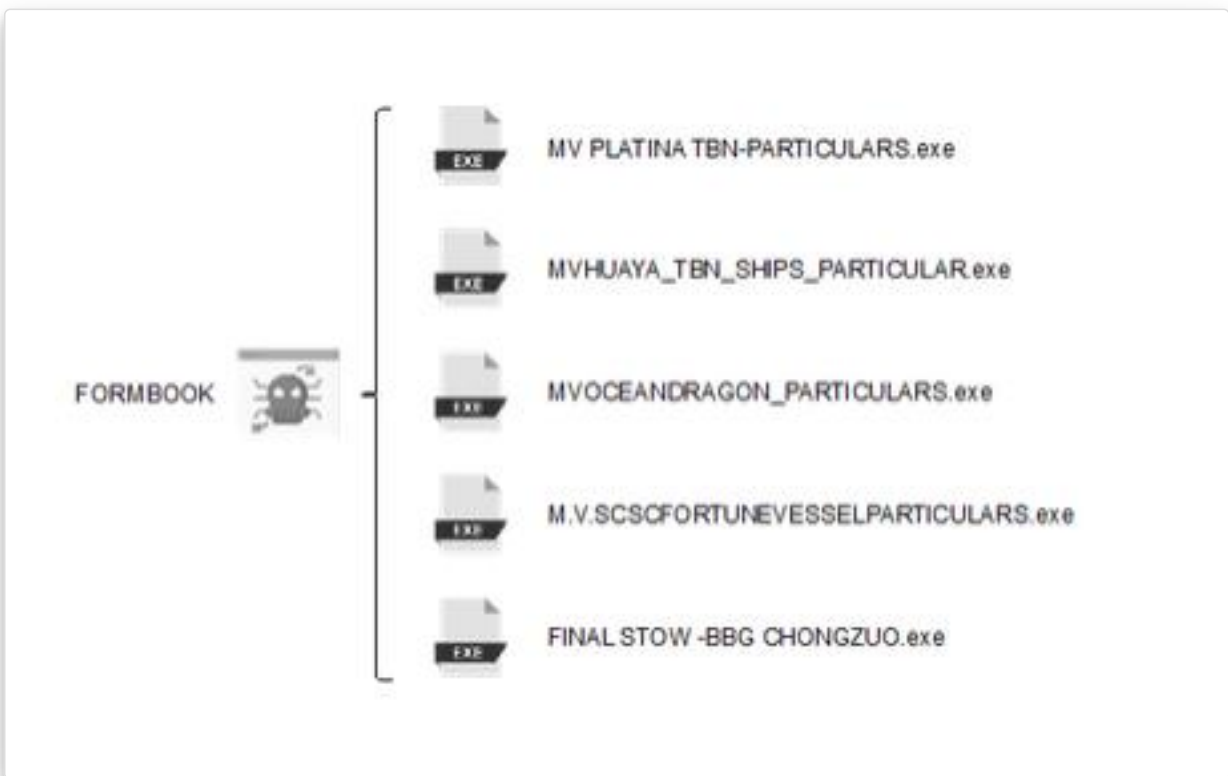


Figure 3-13 : Ship names used during the campaigns.

During the investigation of this specific cluster, OWN was able to identify more than 600 other Formbook-related malware files sharing command and control servers. All these files point to a campaign specifically targeting the maritime sector and its ecosystem.

Maritime Cyber Threat Overview 2022

```
Medi Paestum Template Form.rar
MV_KSL_SEVILLE.rar
PROPEL TBN - VESSEL PARTICULARS.rar
MULTIMAX_TBN_VSL_DETAILS.rar
SWIFT COPY PDA NS EXPLORER.rar
Ship Particular Mv Yildizlar 2.rar
/tmp/emi_attach_for_scan/317af55ea2b9f0de5ae112ef5a4a4f9.file
W_PACIFIC_VESSEL_S_SPEC.rar
Q88_V.5__JEY_HOPE_20221123.rar
mime-part--92187-68917.rar
/home/farm/anteroom/065/d25/065d258b078c4746f1ee57e931db677ef9c97092c476178d1ad968186690a400
Ship_Particulars_Hai_Duong_09.rar
MV_GREAT_JIN_QUOTATION_GJN22ST_D026.rar
0821f5674ad4c289f7427d30cb4fab55a0d1e2e47cc3a63ee6ab93250985a0c5.exe
ES0609022_FOR_ME_LO.rar
ULTRABULK_TBN_PARTICULARS.rar
MV_GREAT_JIN_QUOTATION_GJN22ST_D026.rar
%HOME%\unpackPROPEL TBN - VESSEL PARTICULARS.exe
SHIP_PARTICULARS__MV_TBN.rar
/Volumes/krism5bb635/Purchase Order.exe
TBN_VESSEL_DETAILS_.rar
/home/farm/anteroom/0b6/cc1/0b6cc152d26eef44fb5e3a98fa52df8bfc2a272c35ebbdbfd2e274479ad43d09
MV_ALTAN_TBN__SHIP_PARTICULARS.rar
/tmp/emi_attach_for_scan/e316e8bf50f8eeb6b0ea7f3704b5daa2.file
Red_Line_Ship_Particular.HEIC_14.10.22.rar
```

Figure 3-14 : Examples of filenames delivering Formbook.

3.2.2. Agent Tesla

Definition

Discovered at the end of 2014, Agent Tesla is a keystroke recorder (*keylogger*) with many features such as clipboard recording, screen capture, extraction of stored passwords from many browsers. It supports all versions of the Windows operating system and is written in .NET.

Maritime Cyber Threat Overview 2022

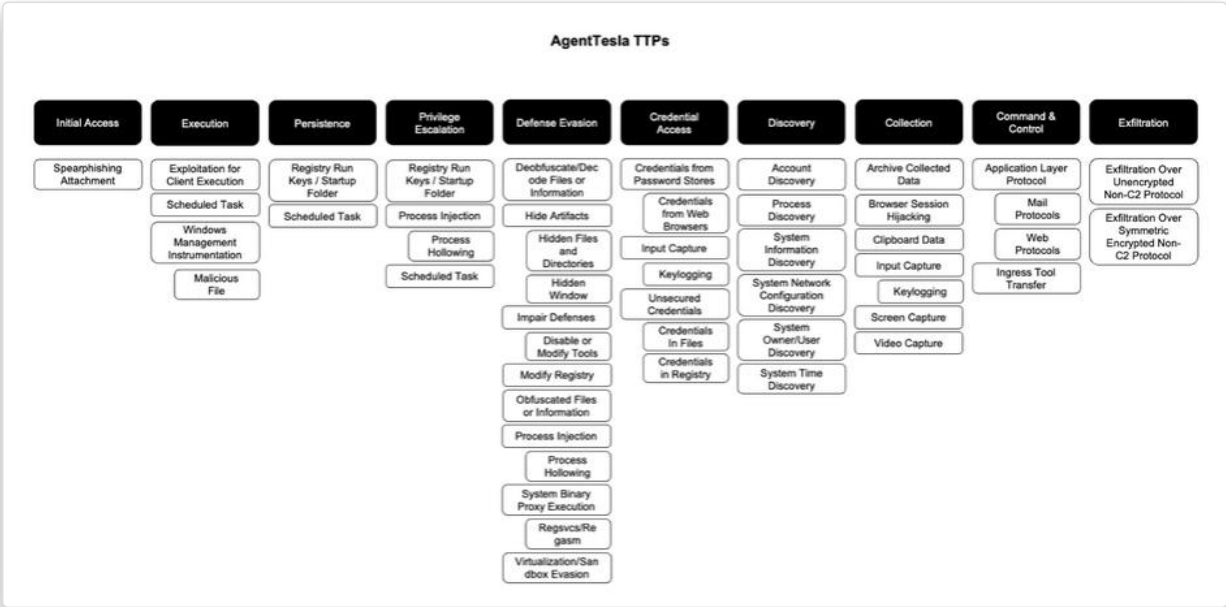


Figure 3-15 : Tactics, Techniques and Procedures of Agent Tesla. Source: MITRE ATT&CK.

Agent Tesla was omnipresent throughout 2022. In several collected e-mails, the attacker spoofs the identity and infrastructure of ship owners (Figure 3-16). The archive attached to the e-mail is decompressed and executes a sample of Agent Tesla¹³. This retrieves e-mail identifiers, as well as data stored by browsers. The collected information is then exfiltrated to a Telegram bot.

```
Received: from unknown by localhost (amavisd-new, unix socket) id 89ldNodfiRbV
for <brotaru@electroputere.ro>; Tue, 11 Oct 2022 10:48:34 +0300 (EEST)
Received: from maersk.com (unknown [45.137.22.249])
by spin.electroputere.ro (amavisd-milter) with ESMTMP id 29B7mRnp021289;
Tue, 11 Oct 2022 10:48:27 +0300
(envelope-from <info@maersk.com>)
From: "services" <info@maersk.com>
To: brotaru@electroputere.ro
Subject: TOP URGENT//RE:SHIPMENT SCHEDULE/MAERSK SHIPPING LINE.
```

Figure 3-16 : Header samples of e-mails delivering Agent Tesla, and spoofing Maersk.

3.2.3. Lokibot

Definition

Lokibot is a malware program sold on cybercriminal forums. It is designed to steal data from infected machines, then submitting this information to a command-and-control host via HTTP POST. This data mainly consists of stored passwords, web browser credentials and cryptoasset wallets.

Maritime Cyber Threat Overview 2022

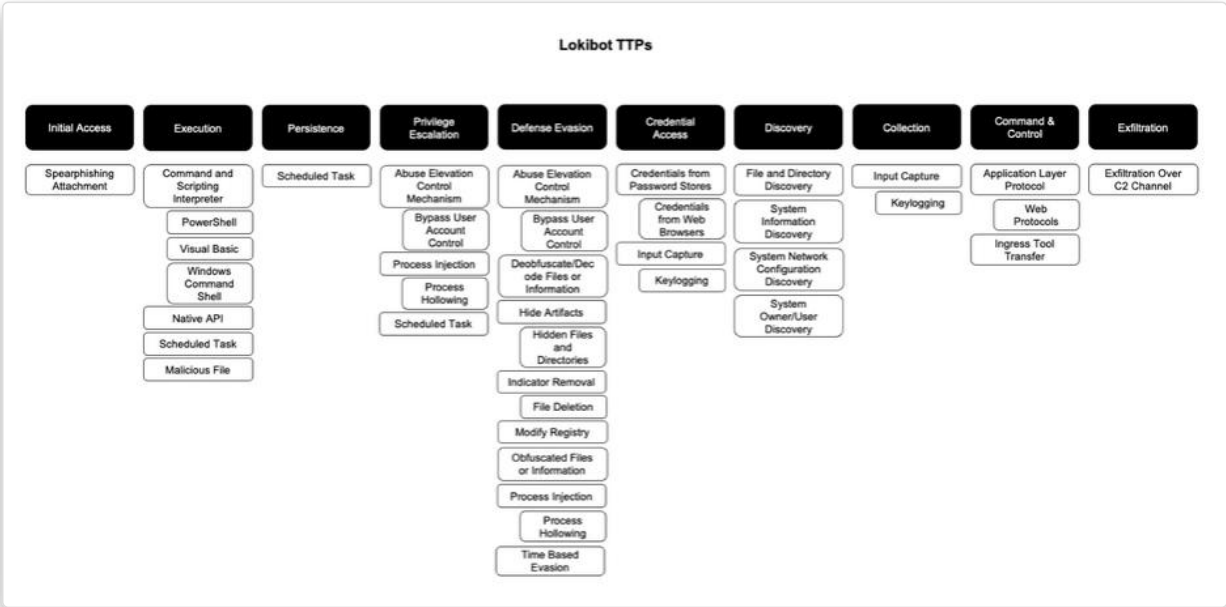


Figure 3-17 : Tactics, Techniques and Procedures of Lokibot. Source: MITRE ATT&CK.

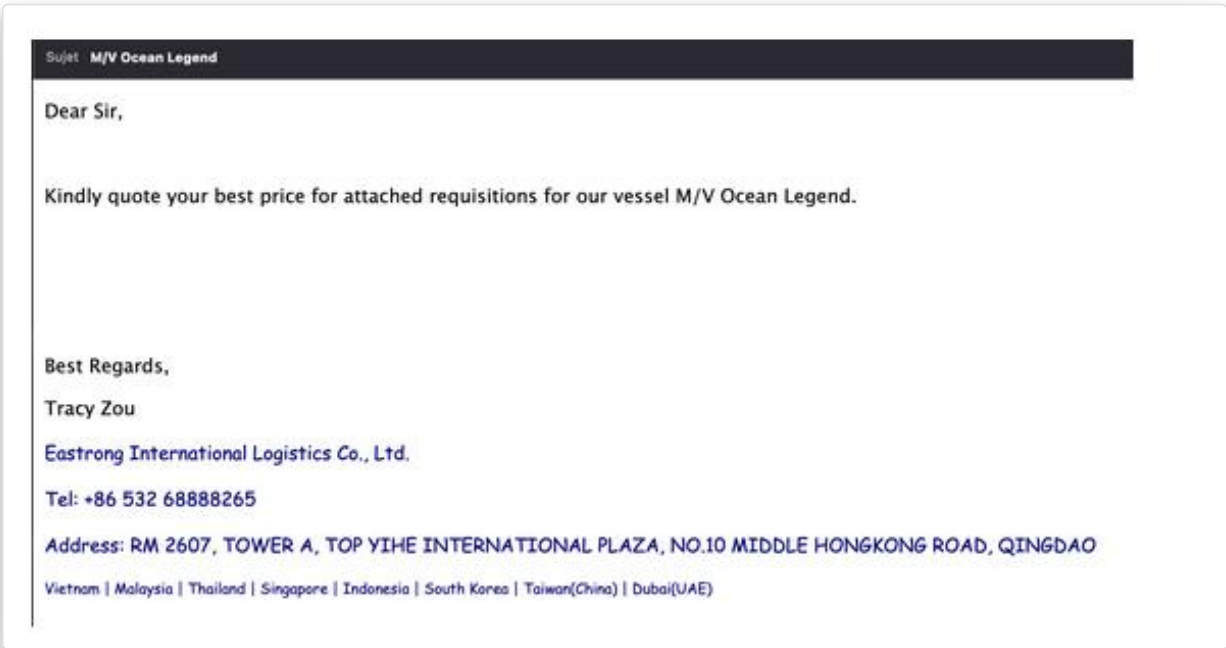


Figure 3-18 : Malicious e-mail distributing Lokibot in a campaign targeting the maritime sector.

One of the samples¹⁴ distributed during attack campaigns targeting the maritime sector, and collected by OWN, delivers the Lokibot malicious code via an Excel file sent as an attachment to a *phishing* e-mail (Figure 3-18). The Excel file¹⁵ follows the nomenclature « MV_SHIP_NAME » and, this time, uses the name of the ship « *Ocean Legend* ». Once the document has been opened, a fake Office notification appears, asking the user to enable document editing (Figure 3-19).

Maritime Cyber Threat Overview 2022

This activation will enable exploitation of the CVE-2017-11882 vulnerability (*Microsoft Office Memory Corruption Vulnerability*), which affects an MS Office component called « *Equation Editor* » and leads to remote code execution on the infected machine. For Lokibot, this flaw is used to connect to the command and control server and retrieve the final stage of its execution.

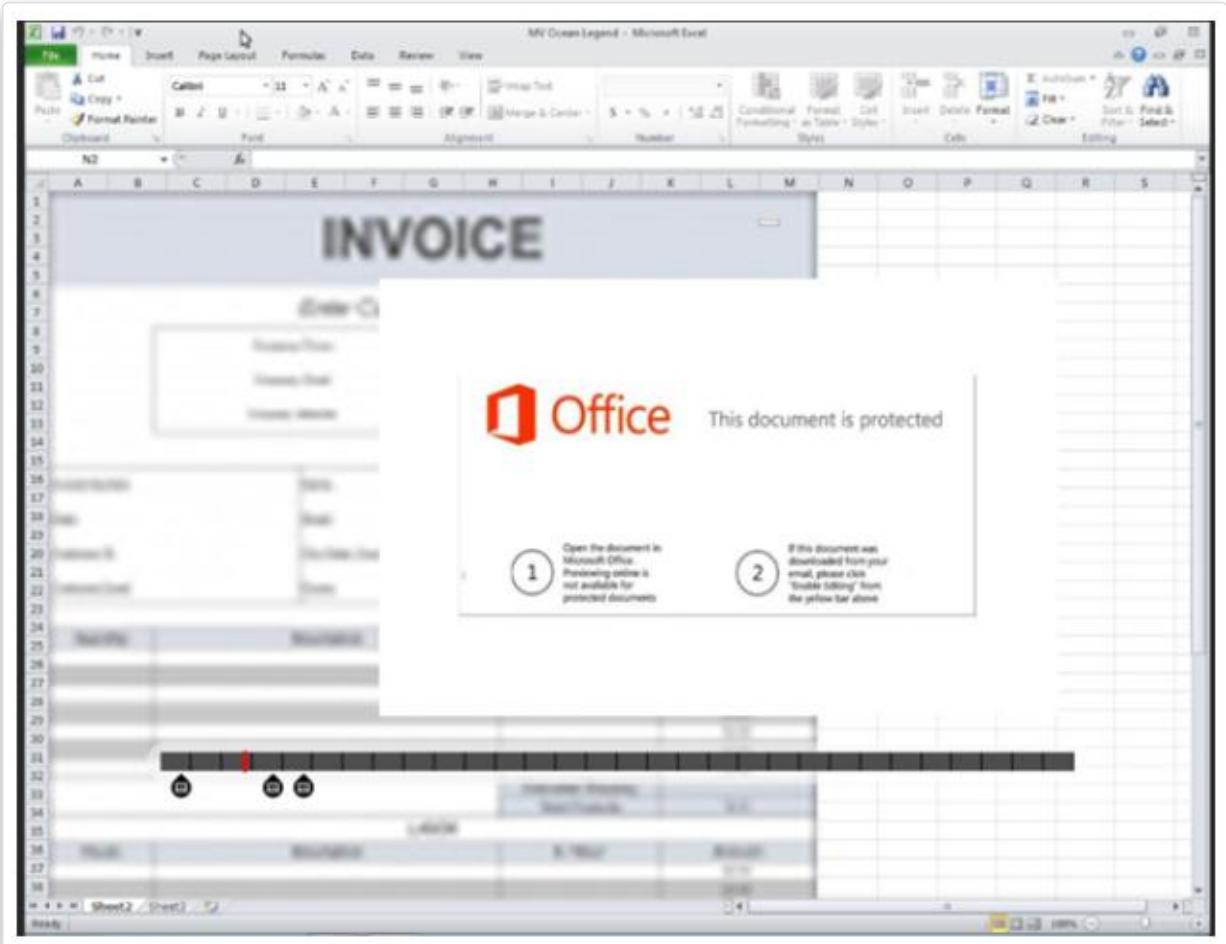


Figure 3-19 : Malicious Microsoft Excel File.

3.2.4. Vector Stealer

In February 2023, a recent strain of infostealer was flagged by OWN-CERT detection rules as potentially targeting the maritime sector: Vector Stealer. Although these campaigns were initiated in 2023 (Figure 3-20), Vector Stealer has been on sale on cybercriminal channels since 2022.

Maritime Cyber Threat Overview 2022

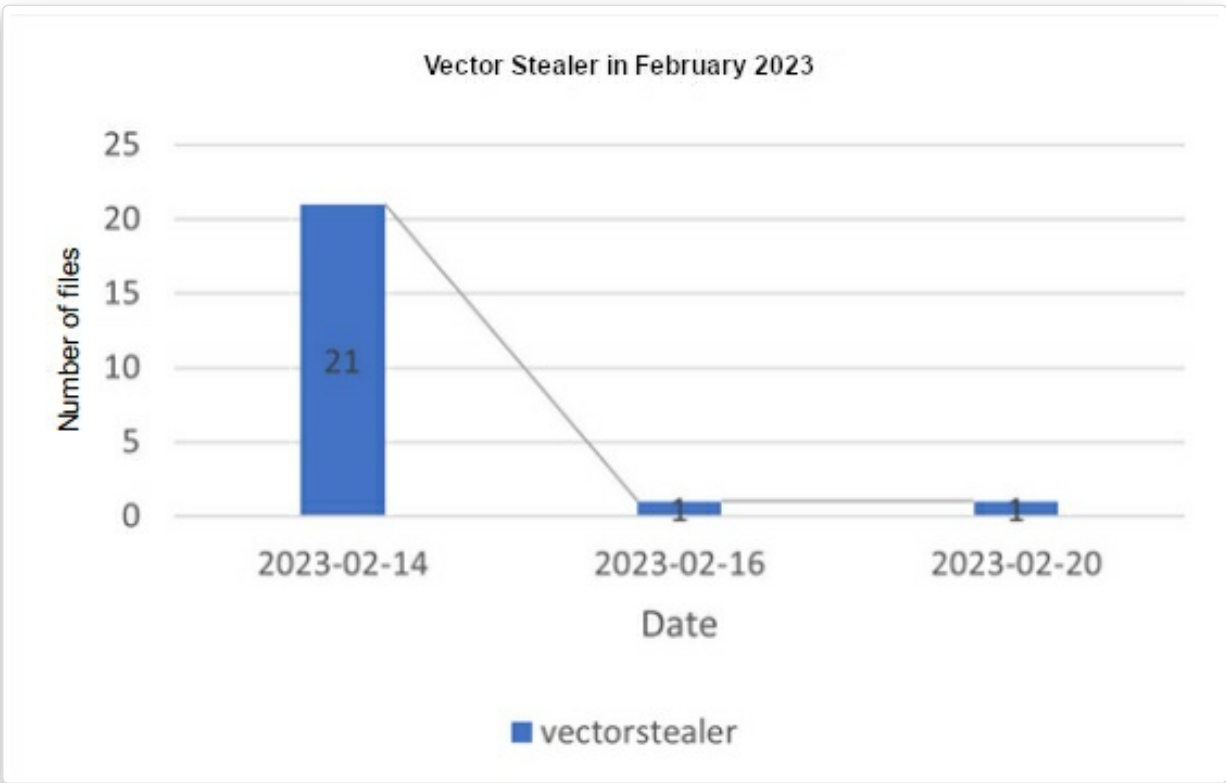


Figure 3-20 : 23 distribution campaigns of Vector Stealer have been identified.

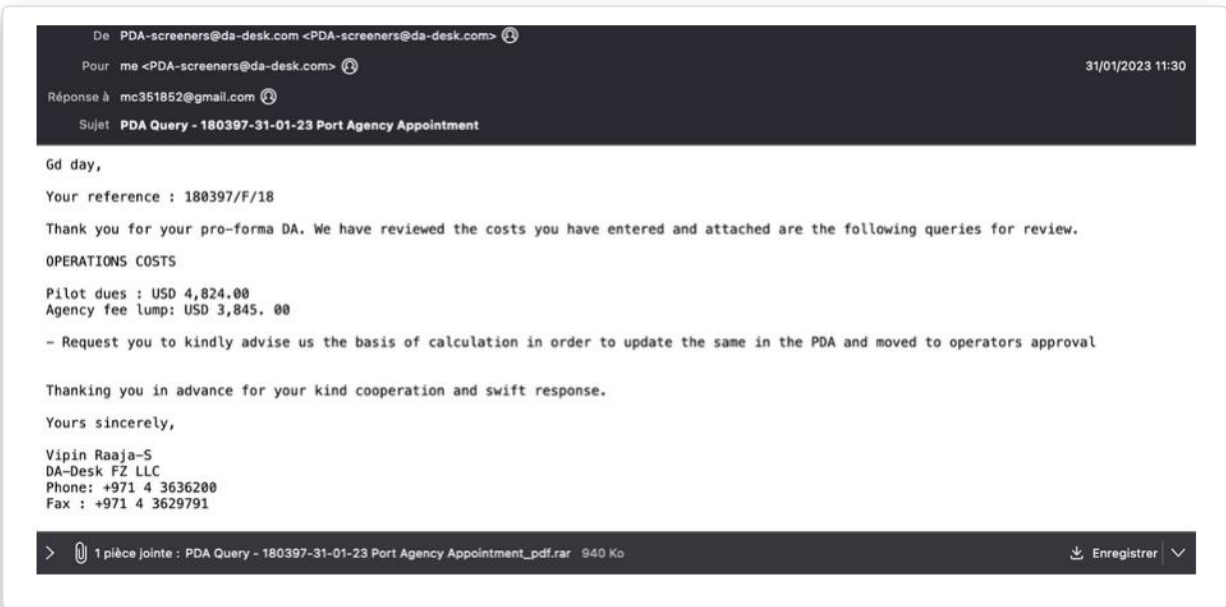


Figure 3-21 : E-mail delivering Vector Stealer to the maritime sector.

The malicious code spreads via e-mail, in the form of an attachment, like the previous * infostealers* documented. In the example chosen, the e-mail contains a .rar archive purporting to be a ship call

Maritime Cyber Threat Overview 2022

invoice named « PDA Query - 180397-31-01-23 Port Agency Appointment_pdf.exe ». The archive delivers a *Vector Stealer* executable named « KOREA SHIPPING - KLCSM)_pdf.exe » ¹⁶(Figure 3-21).

Once executed, the malicious code delivers a randomly named executable. The file collects data from e-mail clients such as Outlook and Foxmail. Vector Stealer also has the particularity of targeting files linked to the RDP protocol to maintain access to the targeted machine. It creates an exfiltration folder in the «AppData» directory to store the stolen data. This data will be exfiltrated to a Telegram bot (Figure 3-22).



Figure 3-22 : Data exfiltration to Telegram.

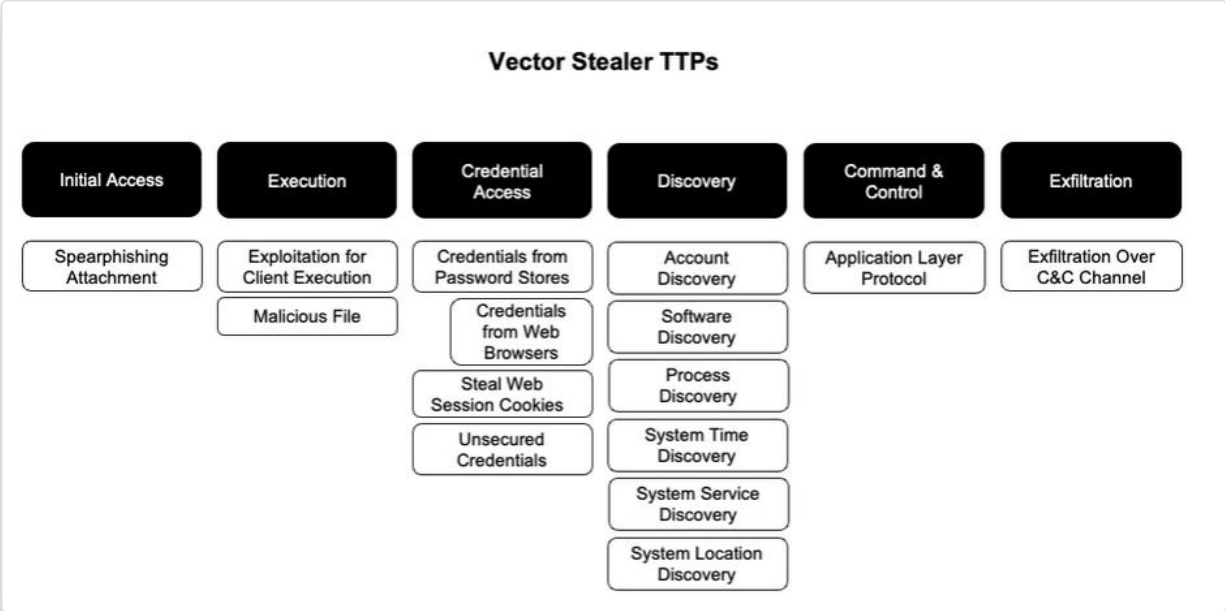


Figure 3-23 : Tactics, Techniques and Procedures of Vector Stealer. Source: OWN.

3.3. Data leaks and resales in the maritime sector

Initial Access Brokers platforms (IAB) have become key crossroads in the cybercriminal ecosystem, essential to the operation of « *Ransomware as a Service* » platforms. In the same way that some ransomware tools are sold to affiliates, the search for entry points to victims' information systems (*initial access*) can also be outsourced. OWN is conducting increased surveillance of cybercriminal channels in search of potential data leaks or sales concerning the maritime sector. Although isolated, some cases of sales or leaks have been identified in 2022.

Cybercriminal channels (marketplaces, forums, Telegram channels, etc.) enable the sale of the tools

Maritime Cyber Threat Overview 2022

needed to carry out attacks, such as malicious code, identifiers or banking information (credit card numbers, verification codes, etc.). No sector is specifically targeted, because in this ecosystem, players act opportunistically: they sell databases from any company, as long as it is profitable for them to do so. Some examples of data leaks are detailed below.

Active since March 18th, 2022, user Kelvinsecurity specializes in data leaks. He has published two sets of data relating to two entities in the maritime sector (a company supplying marine electronics and a public maritime agency). The leaks reportedly concern the private keys of Very Small Aperture Terminal (VSAT) systems on private yachts and military vessels (Figure 3-24), as well as data such as surnames, first names, e-mails, addresses, telephones, etc. (Figure 3-25).

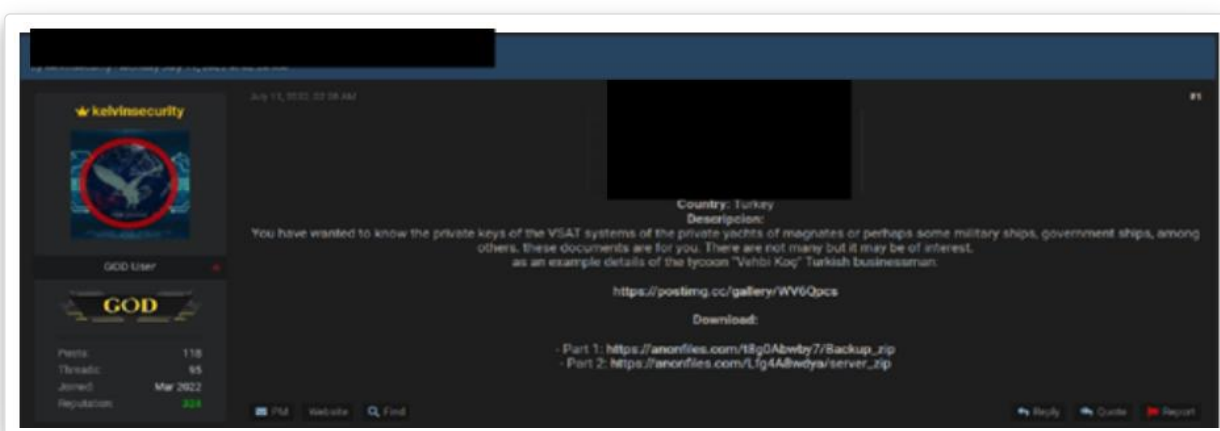


Figure 3-24 : Dataleak announcement by user Kelvinsecurity. Source: OWN-CERT.

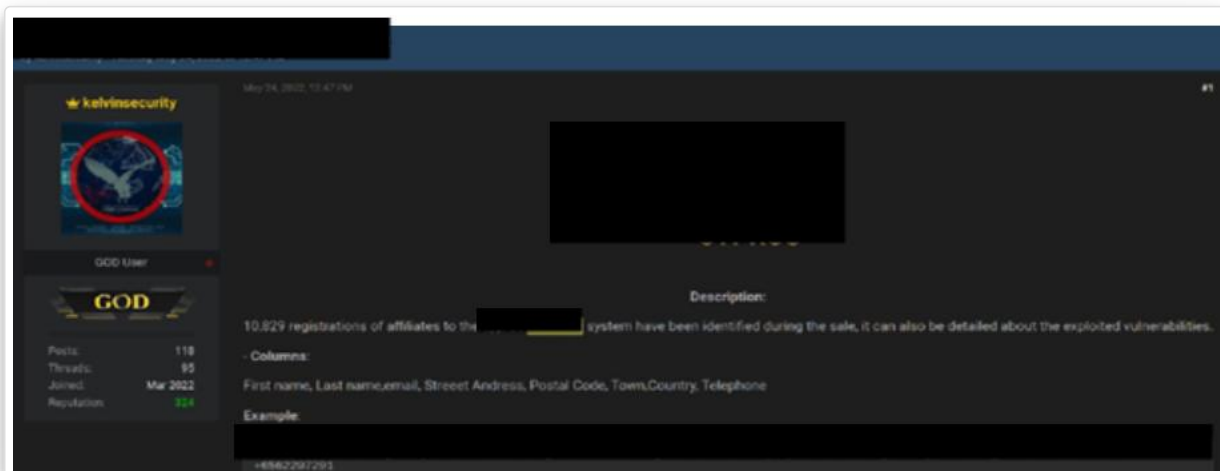


Figure 3-25 : Dataleak announcement by user Kelvinsecurity. Source: OWN-CERT.

Another user, YourAnonWolf, active since March 2022, is known to be the leader of SiegedSec, a cybercriminal group that emerged in February 2022 and specializes in selling data from leaked and defaced websites. Typical *modus operandi* of the group's members may involve SQL injection, exploitation of XSS flaws, vulnerabilities in site-building platforms, or even brute-force attacks.

Maritime Cyber Threat Overview 2022



Figure 3-28 : Dataleak announcement concerning a shipyard on a specialized forum. Source: OWN-CERT.

Recommendations

In case of the announcement of a data leak, it is necessary to assess the importance of the potential leak and its origin. Data may have been stolen through the exploitation of a vulnerable asset publicly available on the Internet, through compromise by malicious code, or through legitimate access using stolen credentials. A server or application misconfiguration can also be the cause of the leak. A complete analysis of the assets exposed, as well as the source of the threat and the files it publishes, will help prioritize these investigations. Only a full investigation of the information system will enable the assessment of the veracity of the leak and its impact on the information system.

Raising awareness of this type of risk among senior management, IT monitoring teams, communications managers and even the legal department can help the organization to cope better in the event of a data leak.

Initial Access Brokers may work for their own account: in this case, once initial access has been obtained, they sell the stolen data directly to the highest bidder, without continuing the attack. They may also participate in the execution chain of a global operation (*Business Email Compromise* or ransomware), where initial access is subcontracted to them.

3.4. Business Email Compromise (BEC)

The *Business Email Compromise (BEC)*, or false wire transfer order scam, is a technique where the attacker uses e-mail to trick an employee into making money transfers or divulging confidential company information.

The malicious actor poses as a trusted figure (hierarchical authority, finance department, administration, regular customer, partner, bank, etc.) and requests payment of a false invoice or transmission of sensitive data. Corporate e-mail accounts are usurped or compromised beforehand to initiate discussions and carry out fraudulent transfers.

In 2022, more cases of instant messaging systems (such as Whatsapp) being used in an attempt to carry out this type of attack were reported to M-CERT. While the principle is similar to that of



Maritime Cyber Threat Overview 2022

phishing, these more targeted attacks rely on a stronger sense of trust, through the use of much more sophisticated social engineering techniques than a simple e-mail. As a result, they are often harder to recognize, and sometimes more costly in their consequences, than other, less targeted attacks.

In May 2022, the FBI Internet Crime Complaint Center published a report highlighting the continuing growth of *Business Email Compromise (BEC)* attacks¹⁷. Global losses due to BEC between July 2019 and December 2021 increased by 65% on the previous year, and accounted for 35% of all losses attributable to cybercrime.

In 2022, this included the case of an organization in the maritime sector that fell victim to this type of scam in April¹⁸.

3.4.1. A look back at the SILVER TERRIER operating mode

In January 2022, Interpol arrested several people involved in BEC operations in Nigeria, following cooperation with Palo Alto¹⁹. Their *modus operandi* was the following:

1. Sending of generic malicious e-mails (invoices, SWIFT payment confirmations, order forms, etc.) designed to deceive the victim in order to install malicious code without his knowledge, or to entice him to visit a *phishing* site with the aim of stealing his e-mail login details;
2. Connection to the victim's mailbox and implementation of automatic forwarding rules based on certain keywords, or manual monitoring of e-mails;
3. When a payment discussion is initiated between the victim and one of his service providers or suppliers, the fraudsters register a domain name close to the partner concerned (*typosquatting*: for example marrinsa[.]com to usurp marinsa.com) and use this domain name to insert themselves into the conversation by taking over the entire message chain. The fraudster then requests that the payment be made to another bank account, claiming, for example, that the bank is unavailable or that there is an account error.

If the involved parties do not notice the change of domain name in the e-mails, or if there is no protocol for verifying this type of change, the risk of making the payment to this new bank account (held by the fraudsters) is very high.

Among those arrested, one in particular targeted logistics companies, creating numerous domains to mislead users, such as:

- atlanticexpresslogistics[.]com
- clarionsshipping[.]com
- dpdexpressuk[.]com
- dynamicparceldelivery[.]com
- shipatlanticlogistics.co[.]uk.



Maritime Cyber Threat Overview 2022

According to PaloAlto, this person had registered more than 250 domain names, and these domains were linked to the use of various families of malicious code (Trojans or infostealers), including Formbook, Agent Telsa, PredatorPain, Nanocore, DarkComet, and others. This person often used the pseudonyms « Fyzee » and « Encryption Code » on various cybercriminal forums, as well as on social networks such as Facebook. His activity on these sites reflects his criminal activity: he acquires software to copy sites, create infected Word files or develop Trojans, such as Nanocore or Betabot. OWN-CERT's monitoring of this individual's activity confirms his modus operandi: creating sites for scam purposes, then infecting users in order to steal their data.

Although these techniques are relatively simple, they have been tried and tested for several years, and are extremely effective: nearly 20,000 victims are recorded every year in the USA, for fraud amounts of between 1 and 2 billion dollars. The risk of this type of attack is primarily financial, as these actors seek to divert money flows, and therefore appears minimal for the operational aspect of the maritime sector.

It is occasionally possible to trace the identity of the fraudster, as they are often rather carefree about their operational security, which facilitates their arrest. Nevertheless, the fact that individuals who have already been arrested by Interpol in 2020 will be arrested again at the end of 2021 reflects the difficulties of containing this type of crime on a permanent basis. The impact of these arrests will certainly be painless, given the volume of attacks observed. Indeed, tens of thousands of domain names are registered every year to carry out this type of fraud, which implies significant logistics and automation on the part of these actors. The investigations carried out by OWN-CERT in 2022 have identified several similar schemes targeting the maritime sector, including POSEIDON-IS_001.

3.4.2. Focus on POSEIDON-IS_001 operating mode

A threat actor targeting the maritime sector has been identified by OWN-CERT teams. Dubbed POSEIDON-IS_001, it has been operating since 2019 and is still active today. Its *modus operandi* is characterized by the use of phishing techniques and the Lokibot *infostealer*. Phishing campaigns impersonating DHL, Excel, Outlook and Yahoo have also been identified.

A number of clues point to POSEIDON-IS_001 being linked to the SilverTerrier cluster. OWN-CERT is highly confident that POSEIDON-IS_001's ultimate goal is probably to steal data and reuse it in BEC attacks. In a first example of a campaign dubbed « Aldo Group », POSEIDON-IS_001 sends its phishing e-mails from the domain aldoqroup[.]com, usurping the company name Aldo group (Retail), as well as the name of a real company employee (Figure 3-29).

Maritime Cyber Threat Overview 2022

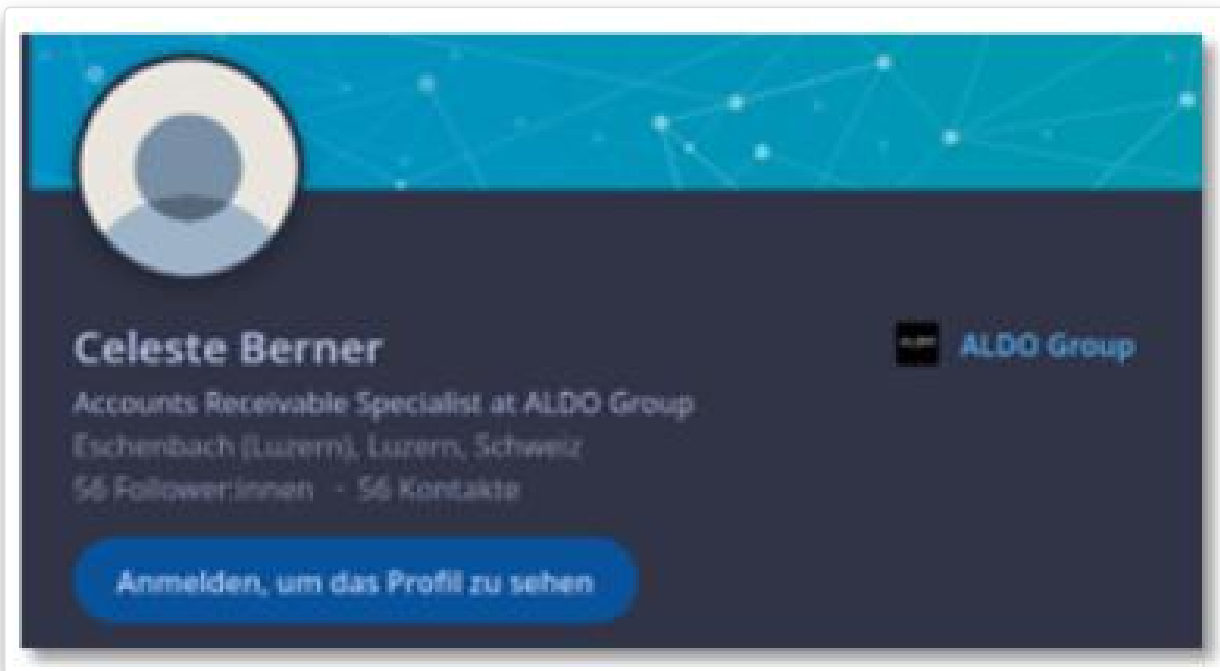


Figure 3-29 : Legitimate employee account spoofed by POSEIDON-IS_001. Sources: LinkedIn, OWN-CERT.

The e-mail sent to the victim (Figure 3-30) contains an attachment named « 44 R.I MI2KT.rar ». This archive contains a Lokibot executable (named: « EYQشف0بج.exe »²⁰). The exfiltration domain of this executable is another domain owned by POSEIDON-IS_001: allamaldives[.]com.

In a second campaign, POSEIDON-IS_001 sends a malicious e-mail to its target (whose business is the development of onboard systems), impersonating « PetroSeis Asia » (whose business is hydrographic surveys for port authorities). The attached archive also contains a Lokibot executable (named FERRETTO6.exe²¹). The subject and content of the e-mail contain terms relating to the maritime sector (Figure 3-31). The exfiltration domain of this executable is another domain owned by POSEIDON-IS_001, gensis-advpg[.]com.



TLP:CLEAR

TLP:EX:NC



Maritime Cyber Threat Overview 2022



Figure 3-30 : Malicious e-mail sent by POSEIDON-IS_001. Source: OWN-CERT.

TLP:CLEAR

TLP:EX:NC



Maritime Cyber Threat Overview 2022

From: Operations@petroseis.asia <Operations@petroseis.asia>
Sent: Monday, April 29, 2019 3:18 PM
Subject: DDU quotation from Singapore to Mangalore, 1x20'FR //MV NALUHU - Anchor, 7000.0kgs// - Translog

Dear customer

Fyi,

We've an enquiry 20'FR from Singapore to Mangalore. Pls quote DDU charges.

Commodity: 1 unit of anchor

Weight: 7000.0kgs

Dim: 3000 x 2720 x 832mm (draft as per attached)

Delivery address:

Kulur, Mangalore 575013

Office address

51, Jalan Anggerik Vanilla AB 31/AB,

Kota Kemuning,

40460 Shah Alam,

Selangor, Malaysia.

Tel: +603 5131 9899

Fax: +603 5131 9855

>  1 attachment: AC-14 6525KGS.PDF.arj 151 KB

Figure 3-31 : Malicious e-mail sent by POSEIDON-IS_001. Source: OWN-CERT.

If the use of Lokibot is the core of the campaign of POSEIDON-IS_001, it is very probable that POSEIDON-IS_001 also uses stolen data to hack in the network of target companies as part of BEC attacks. OWN-CERT has identified similarities in the *modus operandi* with the SilverTerrier threat actor:

- the use of Lokibot with e-mails incoming from typosquatted domains,
- similar victimology (companies in the « Technology » and « Manufacturing » sectors),
- the identification of a Nigerian telephone number registered by POSEIDON-IS_001 and directly

Maritime Cyber Threat Overview 2022

linked to its e-mail address.

The threat actor POSEIDON-IS_001 *modus operandi* remained very active in 2022, as evidenced by its rate of new domain name registrations (Figure 3-32).

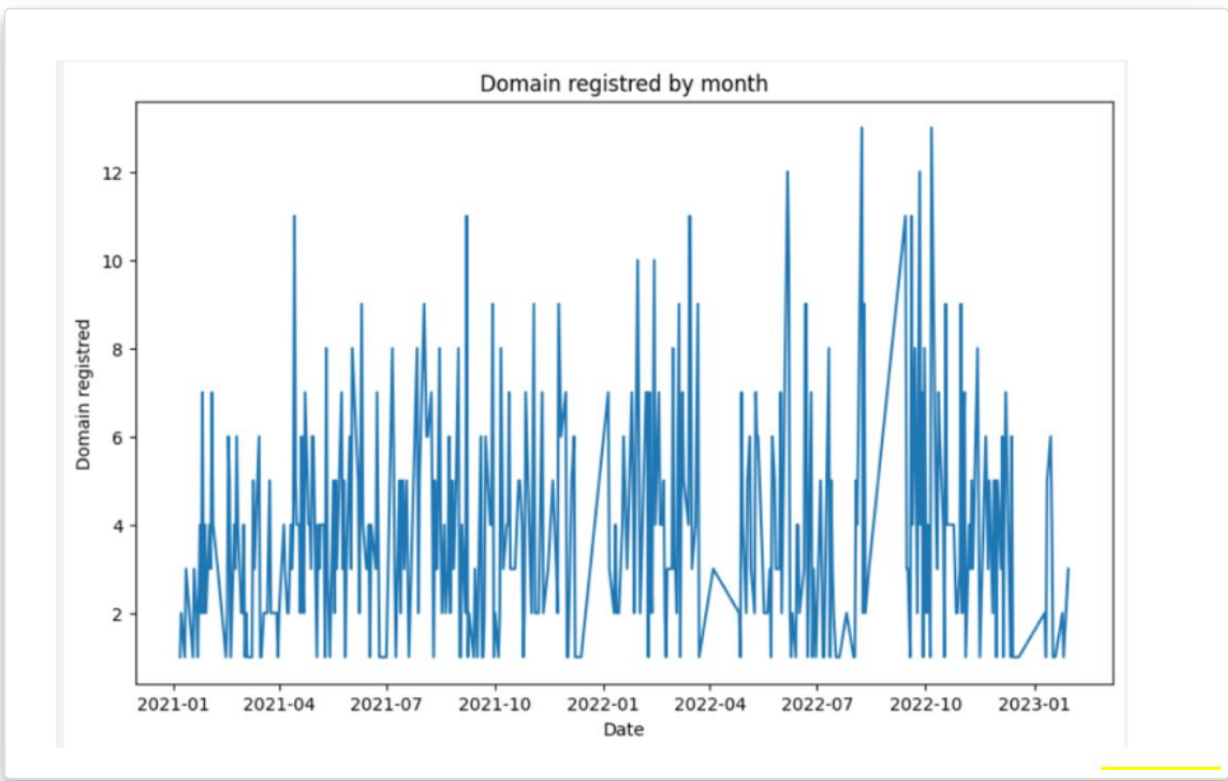


Figure 3-32 : Domains registered by POSEIDON-IS_001 over the last months. Source: OWN-CERT.

Recommendations

- Raise awareness of all employees on how to detect phishing attempts.
- Raise awareness and trained all employees responsible for payments on how to detect fraudulent bank transfer orders.
- Create procedures for verifying bank account changes internally and with partners (controls, irregularity detection and fraud prevention).
- Quarantine all executable files sent by e-mail (even without the .exe extension or contained in archives).
- Implement Multiple Factors Authentification (MFA) on account. Physical or FIDO2 keys enhance protection against phishing.
- Rely on designated individuals using MFA for money transfers.
- Verify the authenticity of information contained in correspondence.
- Monitor access to e-mail accounts and check rules concerning unauthorized e-mail and forwarding parameters.
- Be highly vigilant when receiving e-mails or links that do not belong to the organization.

3.5. Ransomware

Maritime Cyber Threat Overview 2022

With over 56 attacks recorded against the sector in 2022, compared with 51 in 2021, the pressure exerted by ransomware threat sources has increased. To date, no ransomware group has specialized in attacking companies in the maritime sector. In the vast majority of cases, attacks are opportunistic. The fight against these groups has also intensified, with several arrests and dismantlings.

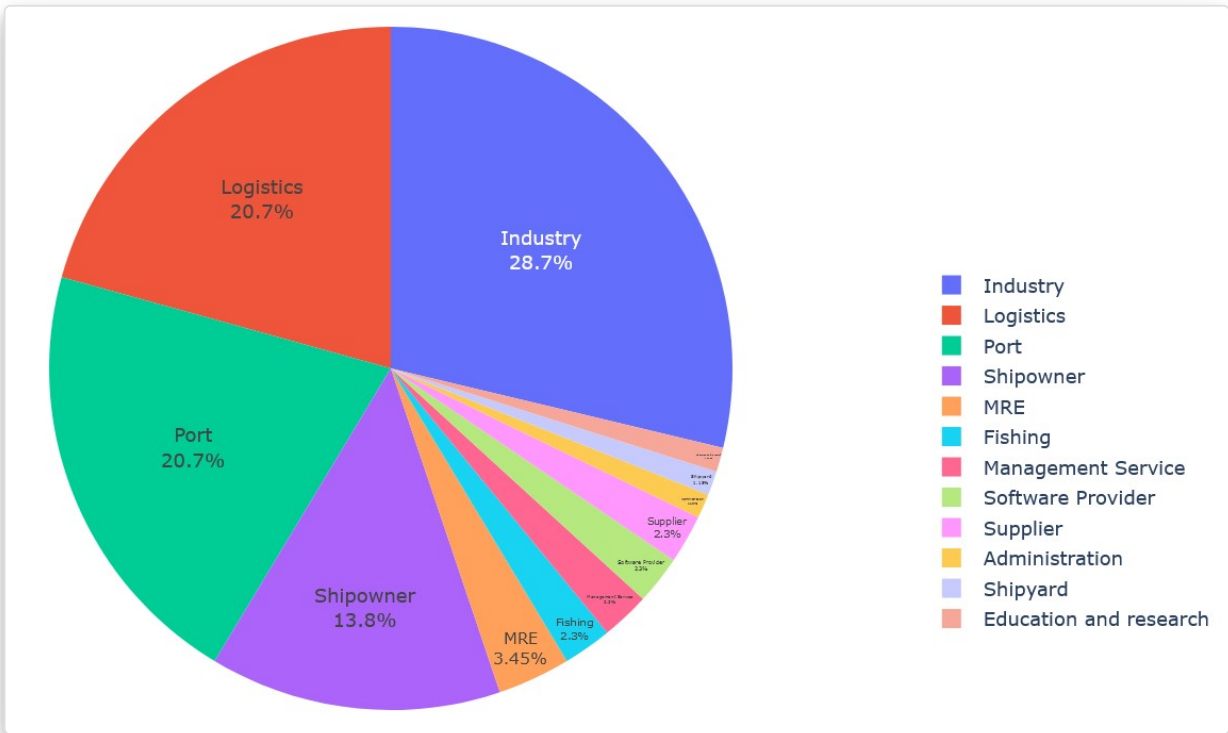


Figure 3-33 : Number of ransomware attacks by maritime industry in 2022. Source: OWN-CERT.

Maritime Cyber Threat Overview 2022

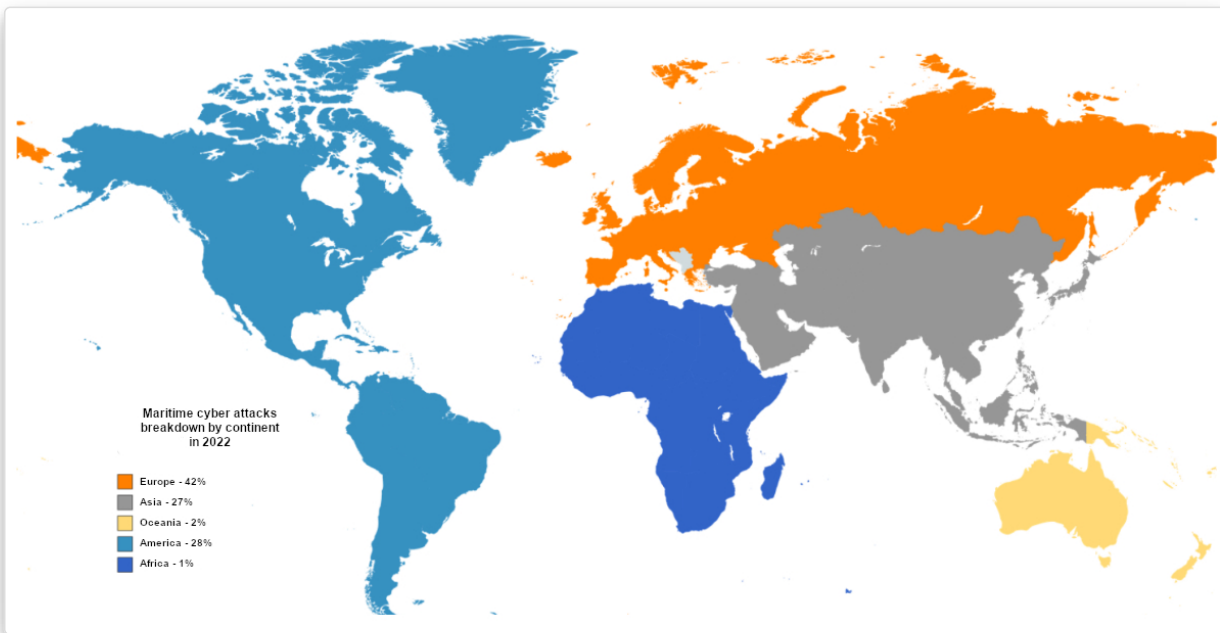


Figure 3-34 : Geographical distribution of ransomware attacks by maritime industry in 2022. Source: OWN-CERT.

During 2022, the ransomware groups that most impacted the maritime sector were Lockbit, Conti and Play. Unsurprisingly, these were the same main ransomware groups targeting other sectors during the same year (Figures 3-31, 3-32).

Among the techniques favored by ransomware groups are:

1	2	3
<p>Pre-infection with malicious code Emotet, Dridex, Trickbot, BazarLoader, Qbot, IcedID, SquirrelWaffle...</p>	<p>Compromise of assets exposed to the Internet (RDP, VPN, gateways, etc.) by exploiting vulnerabilities The PulseSecure (CVE 2019-11510) and Citrix (CVE-2019-19781) vulnerabilities are known to be frequently exploited by ransomware groups. ProxyShell (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207), PrintNightmare (CVE-2021-34527) and the Log4Shell (CVE-2021-44228) vulnerabilities are often exploited by the ransomware operators LockFile, Magniber and Vice Society.</p>	<p>The purchase of identifiers and access to third parties on cybercriminal sites.</p>

Maritime Cyber Threat Overview 2022

The final objective of ransomware use is also evolving. In January 2022, the « Belarusian Cyber Partisans », a hacktivist group, launched a ransomware attack on Belarusian railway infrastructure²².

Instead of demanding a ransom to recover data from encrypted servers, the group provided a series of political conditions in exchange for decryption keys: withdrawal of Russian troops present on the territory, release of political prisoners (Figure 3-38). Launching a ransomware attack in this case is not about financial gain, but about getting a political message across.

The only visible impact of this attack would have been the impossibility for employees to access the transport company's databases, and for customers to use the online booking system. However, as the rail network is a strategic element of military logistical support, the attack could also have affected a joint Russian-Belarusian military exercise, making it a symbolic target.

Attacking transport infrastructures is not an end in itself, but a means of imposing oneself on the balance of power by affecting a strategic sector. This is the first time that a hacktivist group has used ransomware as a means of protest. The year 2022 demonstrated, in connection with the war in Ukraine, that the maritime sector could be affected by this kind of hacktivism.

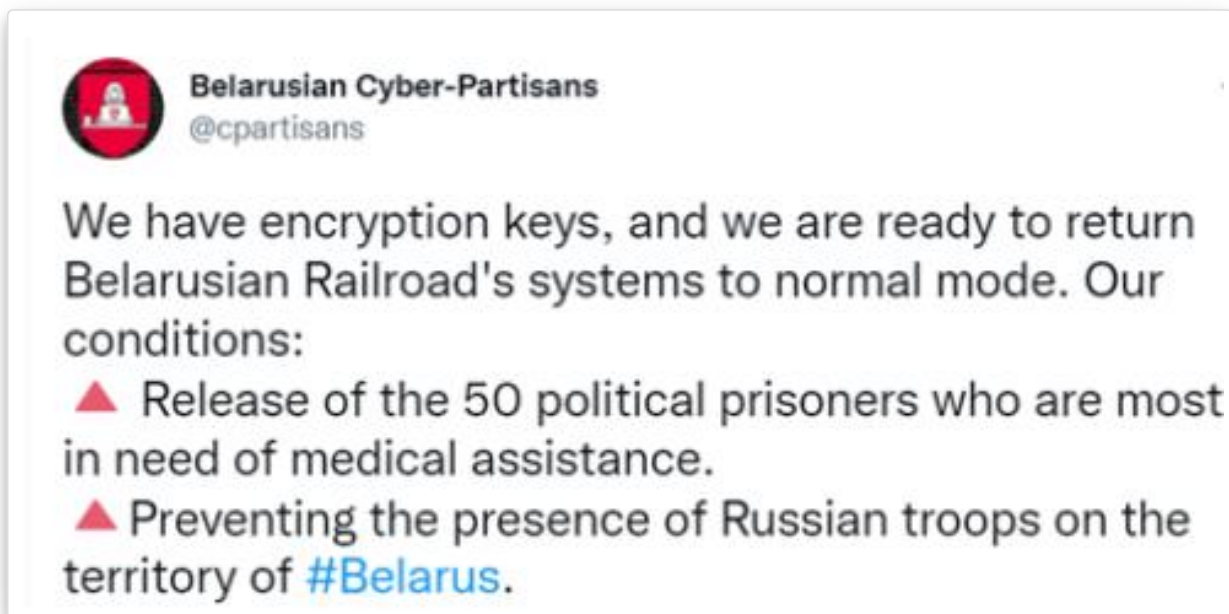


Figure 3-35 : Claim of the attack. Source: Twitter.



Maritime Cyber Threat Overview 2022

Prospective scenario: the impact of ransomware on the maritime ecosystem.	
August 2022	Using a tool to identify vulnerable websites, an attacker spotted a vulnerable Content Management System (CMS) at a shipowner's premises. The CMS, set up a few years ago by a service provider, has not been updated since 2018. Numerous vulnerabilities on this CMS have been published, but contracting with a new provider took too long, slowed down by COVID, the work overload of certain key players and the lack of interest (the website working properly).
Step 1 - Discovery and initial compromise	By exploiting a vulnerability in this CMS, the attacker was able to obtain the list and e-mail addresses of 37 employees with access to the CMS, which is also used to distribute documents to the shipowner's staff and partners (intranet and extranet). However, the attacker was unable to recover the passwords associated with the accounts. This attack goes unnoticed, as no one - and no technology - is monitoring the CMS.
Step 2 - Phishing	The attacker then conducts a phishing attack against the organization, targeting the accounts previously gathered. The attack invites users to log on to Office365 to view a document recently sent to the shipowner for proofreading and indicated as urgent. Connexion to the cloud requires the user to identify himself and authenticate, which 2 of the 37 employees do. For the others, the e-mail appeared suspicious and they did not click on the link. However, due to a lack of internal communication and training, no general alert is sent out.
Step 3 - Resell	The attacker then sells the two recovered logins/passwords on the platform of an Initial Access Broker. 48 hours later, the accounts are purchased by a ransomware operator.
Step 4 - Compromise	Using the accounts obtained, one of which is a privileged account, the ransomware operator gains access to the company's internal messaging system. He spoofs an internal address to send an e-mail with an attachment containing malware. This software has two functions: on the one hand, to enable the exfiltration of sensitive company data (accounts and passwords, logical network architecture) and, on the other, to provide the attacker with full access to the shipowner's information system.
Step 5 - Installation	Several of the shipowner's employees open this attachment: the attacker then carries out the last two phases of the attack: first, he exfiltrates all the data present on the infected client workstations and on the network drives to which they have access. Then, using the privileged account he possesses and exploiting a vulnerability present on the shipowner's <i>Active Directory</i> server, he manages to exfiltrate new data and, finally, activates the encryption of the shipowner's entire IT infrastructure.



Maritime Cyber Threat Overview 2022

Prospective scenario: the impact of ransomware on the maritime ecosystem.	
Impacts on the internal IT	<p>Gradually, all 120 of the shipowner's workstations become unreachable: the <i>Active Directory</i> server is encrypted, as is the backup server, which did not provide off-line backup, depriving the organization of all internal communication, file access and messaging capabilities.</p> <p>The telephone network, which had recently been migrated at the request of a service provider to connect to the <i>Active Directory</i>, is also out of service.</p>
Impacts on the ecosystem	<p>This organization, which performs the functions of a coastal shipowner, has lost its Safety Management System, files and electronic communication with ships. For the past two years, a client workstation of the company's network has been installed on board each ship, with a 4G/5G connection to the shipowner's network.</p> <p>Fortunately, this workstation is isolated from the ship's other workstations and business information systems. The operational consequences for the ships are, therefore, minimal.</p>
Impacts on the internal IT	<p>For the shipowner, the consequences are major: it will take three weeks to rebuild its information system. All the work carried out over the last three months is lost for good. Fortunately, off-line archiving carried out a few months earlier to free up space on the servers will enable essential data to be recovered. All workstations and servers will have to be reinstalled and secured.</p>
Outcome	<p>The director belatedly mandated a forensics investigation team to analyze the event: this team recommended that he files a complaint, which was done once the workstations had been reinstalled, limiting the investigators' investigation capacities. However, their analysis identified the CMS as the initial intrusion vector, which had not been identified at all internally. The CMS was placed in "maintenance" mode for several days, until an emergency service provider could be found to update and secure it properly.</p>
Financial impact	<p>For the shipowner, this is a major operational and financial event: he also realizes that his insurance does not cover this type of claim. The total cost of the attack, the investigation, the recovery, the loss of data and the emergency reinforcement of the information systems would later be calculated at over €180,000, a particularly high cost for this small shipowner who was already experiencing some financial difficulties.</p> <p>While other shipowners around the world have fallen victim to this very same type of attack, the loss of some customers fearing for the security of their data will require a long-term effort on the part of the company to regain their trust.</p>



Maritime Cyber Threat Overview 2022

4. Targeted attacks against the maritime sector

State players have long shown a keen interest in the maritime and port sector, due to its highly strategic nature. The objectives are threefold:

- Pre-positioning, to carry out sabotage actions against critical information systems, on land or at sea.
- Carry out espionage campaigns to gain a strategic or economic advantage, particularly on shipyards or naval defense companies.
- Be active in the information space, conducting disinformation or influence campaigns.

While some of these actions are often difficult to detect, or are detected *a posteriori*, sometimes several months or years late, others can be detected more quickly, but remain confidential. Finally, other actions are carried out more openly, particularly when it comes to influence cyberwarfare.

At the beginning of 2022, many fears were expressed about the outbreak of a cyber conflict in parallel with the Russian offensive against Ukraine. Despite the actual existence of certain actions that should be highlighted, the threat to Western information systems has, in many cases, and in the opinion of many players, not materialized, if at all.

On the other hand, a bipolarization of several cybercriminal groups was confirmed, leading to tensions within certain franchises (Conti). Finally, this bipolarization has also triggered a resurgence of attacks that had tended to be more discreet in recent years, such as Distributed Denial of Service (DDoS) attacks. By coordinating their activities via social networks (listing targets, providing tools, communicating procedures, making claims and, in some cases, making payments), these groups contribute to the struggle for influence of the states they support.

Definition

APT, for *Advanced Persistent Threat*, refers to a type of attack carried out by actors with significant resources who wish to pre-position themselves strategically, discreetly and over a long period of time in order to achieve their objectives (espionage, sabotage, etc). The execution of an APT attack often requires more resources than an opportunistic cybercriminal attack. The perpetrators are usually experienced teams with substantial financial backing, such as government funding, to contribute to meet certain national challenges.

Faced with this type of attack, it is often difficult to have a comprehensive situational awareness of the threat. However, the information made public enable us to analyze the techniques used by these actors. Some open-source elements, as well as OWN-CERT's own sources, have enabled us to identify the following trends in the maritime sector for the year 2022.

4.1. USB memory sticks, an initial infection vector still relevant to the sector

USB media remain potential vectors for the propagation of malicious code in the maritime sector. Indeed, many ship and port information systems, particularly Industrial Control Systems (ICS), Closed

Maritime Cyber Threat Overview 2022

Circuit TeleVision (CCTV) and security systems, remain disconnected from the Internet and « traditional » IT infrastructures. However, preventive and corrective maintenance operations (program and firmware updates, etc.) are carried out using USB media. However, these USB media are all too rarely the property of the shipowner or the ships themselves, and may be brought in by maintenance operators who use them for the benefit of several shipowners, without prior decontamination: the risk of spread infection of one or more information systems over one or many ships, even from different shipowners, is therefore a likely scenario.

Among the malicious codes propagated by this type of method is the PlugX malicious code. PlugX is mainly used by reputed Chinese state groups. The use of USB sticks has been identified as one of the infection vectors used by these attackers. Indeed, when PlugX compromises a machine, the malicious code also infects any USB devices connected to it or subsequently connected. The technique used allows PlugX to be almost undetectable on this type of medium (Figure 4-1)²³.

OWN-CERT is aware of the infection of at least seven ships by the PlugX malicious code during 2022. Given the increasing use of USB sticks for software installation and updates within the sector, and particularly on ships, this vector therefore represents an initial means of infection that could be favored by state actors to target the maritime sector.

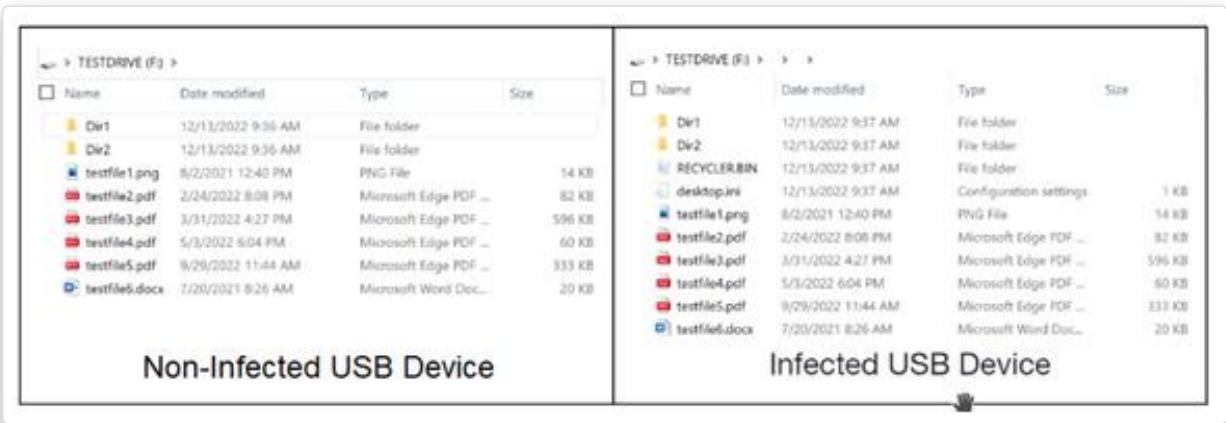


Figure 4-1 : Comparison of the root directories of an uninfected USB stick and of an infected USB stick. Source: Unit42.

4.2. A maritime ecosystem spoofed for social engineering purposes

Like the *Business Email Compromise* campaigns, which use fraudulent e-mails to spoof official procedures and documents used by administrations on ships, attackers also use these practices, but often go further in understanding their victims' ecosystems.

Social engineering via spearphishing emails remains the primary intrusion vector for these attackers, particularly for espionage campaigns. In 2022, several *phishing* campaigns targeting the maritime sector were identified.

Maritime Cyber Threat Overview 2022

According to an analysis by Proofpoint²⁴, TA423²⁵, a group active for ten years and considered close to the Chinese government, is behind *phishing* campaigns distributing a link that redirects victims to a malicious site posing as an Australian media (Figure 4-2) and delivering the ScanBox malicious code. The targets are mainly countries or entities operating in the South China Sea, including wind turbine operators and a European manufacturer supplying equipment for the Yunlin *offshore* wind farm in the Taiwan Strait. The fraudulent e-mails use subjects such as « *Sick Leave* », « *User Research* » and « *Request Cooperation* ».



Figure 4-2 : Screenshot from the article by Fortinet comparing the publication from *australianmorningnews[.]com*, presenting itself as « the biggest information website of Australia », with a similar article from the BBC. Source: Fortinet.

According to Mandiant²⁶, the UNC3890 cluster, reputedly linked to Iran, targeted Israeli entities, including shipping companies, with fake job offers, as part of a phishing or watering hole campaign, using a decoy .xls file designed as a fake job offer (Figure 4-3). Opening this file would then allow the installation of the SUGARDUMP malicious code, a tool for collecting identification information.

Maritime Cyber Threat Overview 2022

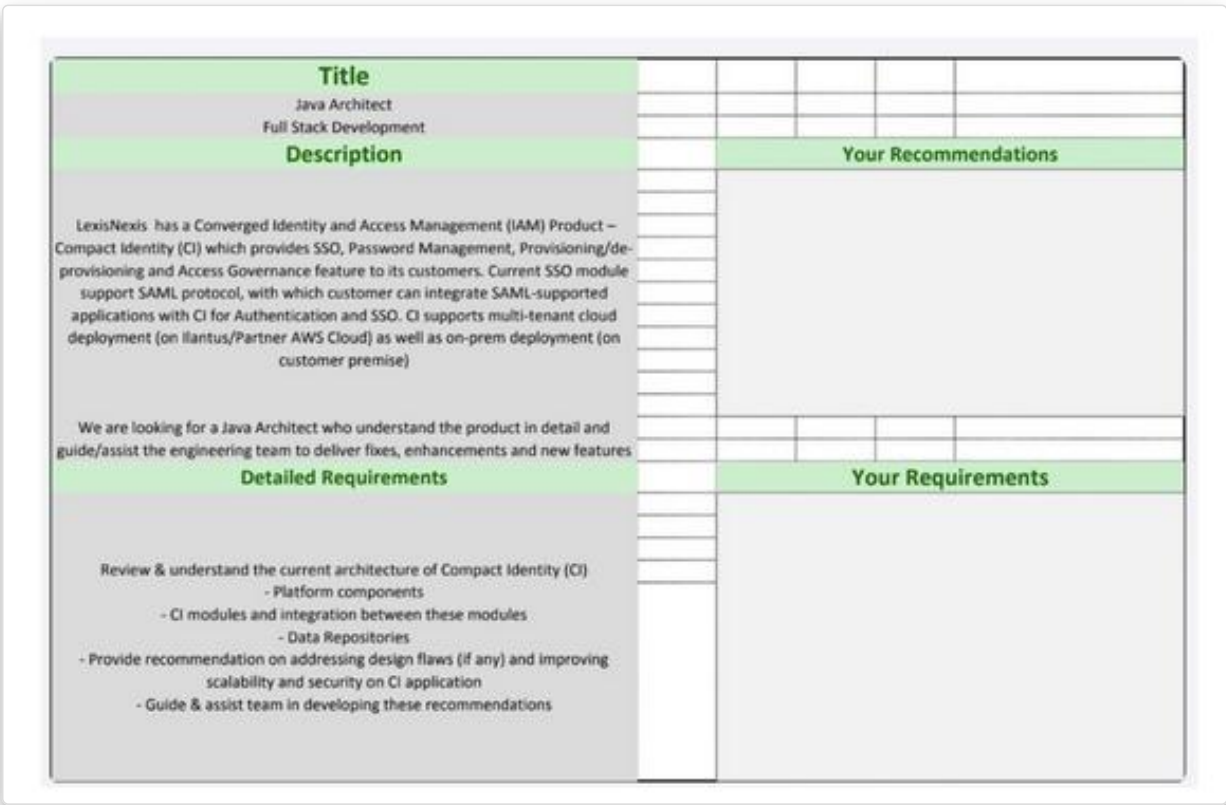


Figure 4-3 : Fake job offer from LexisNexis delivering the malicious file Sugardump. Source: Mandiant.

Symantec teams²⁷ have also identified the actor named Hydrochasma as the source of phishing attacks against shipping companies and medical laboratories in Asia. The group sends a document with a file name adapted to the target organization's native language, such as « *Product Specification-Freight-Company Qualification Information wps-pdf Export.pdf.exe* ». A number of technical elements point to Hydrochasma's origins: the domains used by Hydrochasma use the « .cn » TLD, which refers to China. These domains are hosted on Internet Protocol (IP) addresses located in China. In addition, these domains relate to Chinese companies. Taken together, these elements could indicate a targeting of China, reminiscent of the campaign attributed to APT32 - a reputed state-owned group linked to Vietnam - in early 2020²⁸. Most of the indicators shared by Symantec²⁹ are open-source software used for penetration testing, or generic intrusion tools such as Cobalt Strike. None of these tools is attributable to a specific player, which suggests that Hydrochasma wishes to remain discreet.

Some events organized by the maritime community have also been used to target victims. This is the case of the *Pakistan International Maritime Expo & Conference (PIMEC-2023)*, which aims to develop the country's maritime ecosystem. BlackBerry teams discovered a *phishing* campaign attributed to an actor named « NewsPenguin »³⁰. The attacker used a digitally distributed phishing document in the form of an « exhibitor manual », targeting visitors to the event (Figure 4-4). The payload is an

Maritime Cyber Threat Overview 2022

advanced encrypted espionage tool, with a « penguin » encryption key.

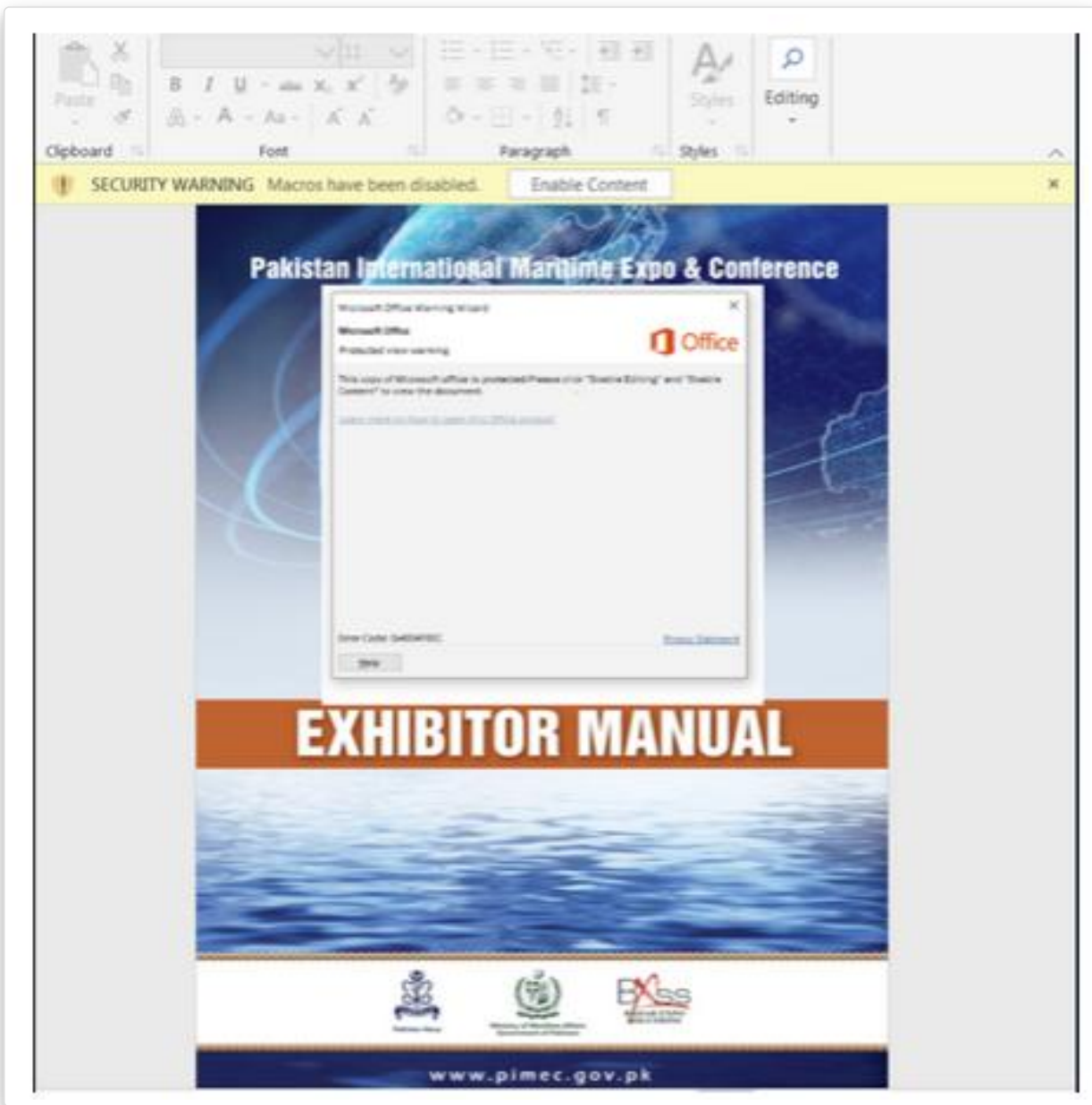


Figure 4-4 : Malicious file used to target exhibitors of the PIMEC-23 Conference. Source: Blackberry.

4.3. Threats targeting « Supervisory Control And Data Acquisition » and « Industrial Control Systems » (ICS)

Ports and ships depend on complex systems, combining traditional information systems (*Information Technology, IT*) with industrial, cyber-physical or business systems, often referred to as *OT (Operational Technology)*. While historically, IT systems associated with office tasks remain the main targets, Industrial Control Systems (ICS) have gradually become strategic targets. These systems use



TLP:CLEAR

TLP:EX:NC



Maritime Cyber Threat Overview 2022

digital technology to manage industrial operations. On a ship, for example, these include propulsion, navigation, power generation, transformation, storage and distribution, etc.

According to a report by Dragos³¹, vulnerabilities impacting industrial systems increased by 27% in 2022. The fact that attacks on industrial systems are complex and resource-intensive explains why they are usually attributed to state-linked attackers. However, the same report indicates that ransomware attacks targeting companies in the industrial sector have increased by 87%, mainly due to the Russia/Ukraine conflict and the « Ransomware as a Service » ecosystem.

Although the threat is very real, it is difficult to have a global view of the attacks that have taken place, and a precise knowledge of the attackers. Because of their technical nature, these attacks are only carried out by specialized groups. This is the case of a group that recently appeared, Bentonite, which targeted the maritime oil and gas sector. According to Dragos, this group carries out this type of attack for espionage and disruption purposes, exploiting mainly remote access or resources exposed on the Internet.

During the year 2022, a report by Forescout³² reported 56 critical vulnerabilities grouped under the name « IceFall », and affecting more than nine IoT system suppliers (Honeywell, Motorola, Omron, Siemens, Emerson, JTEKT, Bentley Nevada, Phoenix Contact, Code). The vulnerabilities identified could lead to the compromise of credentials, manipulation of firmware, remote execution of arbitrary code or bypassing of authentication mechanisms.

Attackers reported as close to the Chinese government are also said to have exploited a vulnerability in Microsoft Exchange (CVE-2021-26855) against the industrial systems of companies located in Pakistan, Afghanistan and Malaysia, including a shipping company³³. This exploit would have enabled the installation of the « ShadowPad » backdoor (Figure 4-5). Known for several years, this backdoor, which targets the logistics sector in particular, enables attackers to download other malicious modules or steal data.

TLP:CLEAR

TLP:EX:NC

Maritime Cyber Threat Overview 2022

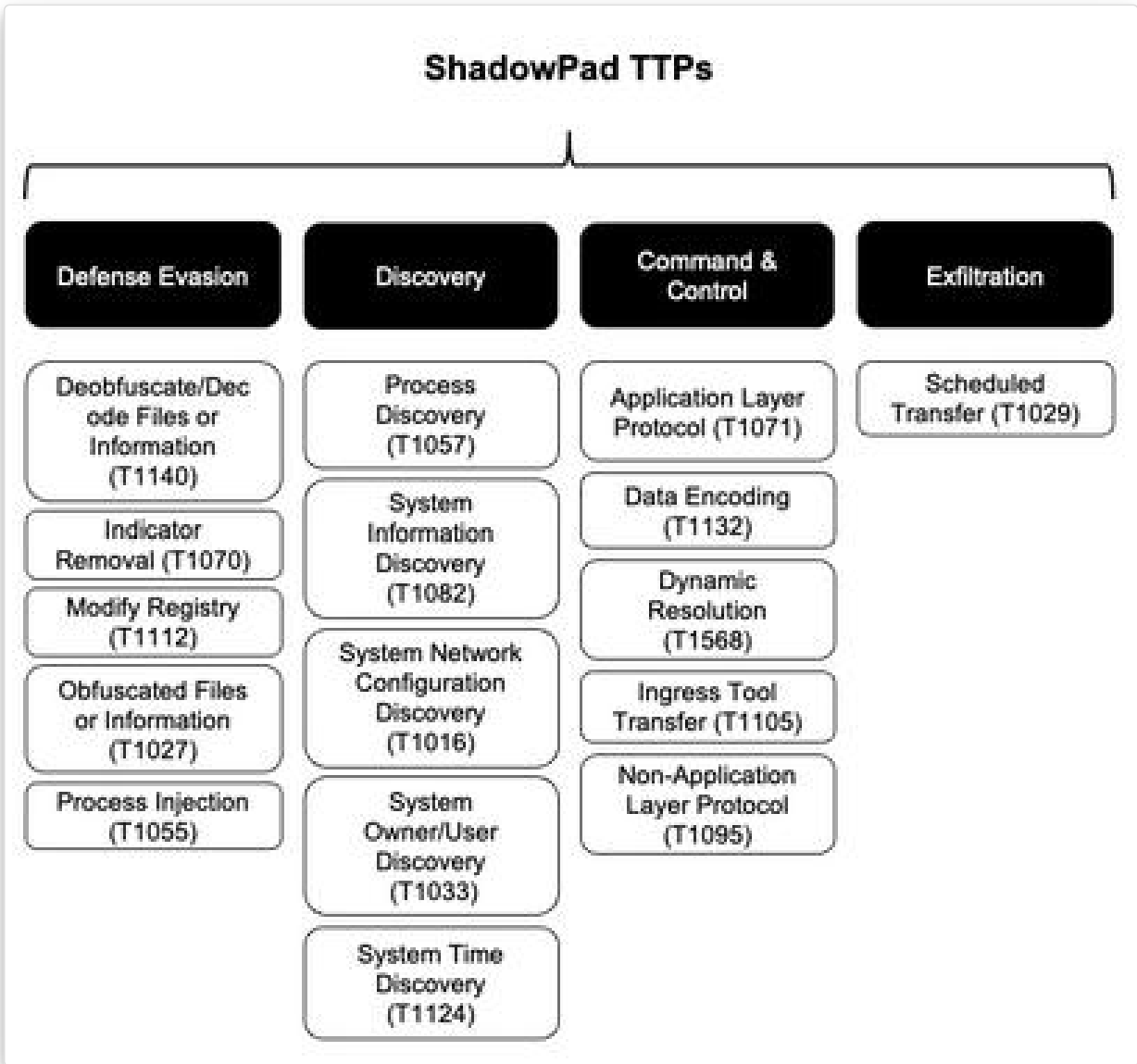


Figure 4-5 : Tactics, Techniques and Procedures of ShadowPad. Source: MITRE ATT&CK.

Another malicious code was specifically designed to target industrial systems. This is the malicious code named « *Incontroller* » (Pipedream)³⁴. This malicious code, which appeared in 2022 in connection with the war in Ukraine, has been specially developed to interact with industrial equipment integrated into various machines used in several sectors. This tool thus enables attackers to gain full system access to several ICS and supervisory control and data acquisition (*Supervisory Control And Data Acquisition, SCADA*) devices, once initial access to the industrial network has been established (Figure 4-6). Dragos believes that the most likely targets of this malicious code are Liquefied Natural Gas (LNG) equipment and power grids.

Maritime Cyber Threat Overview 2022

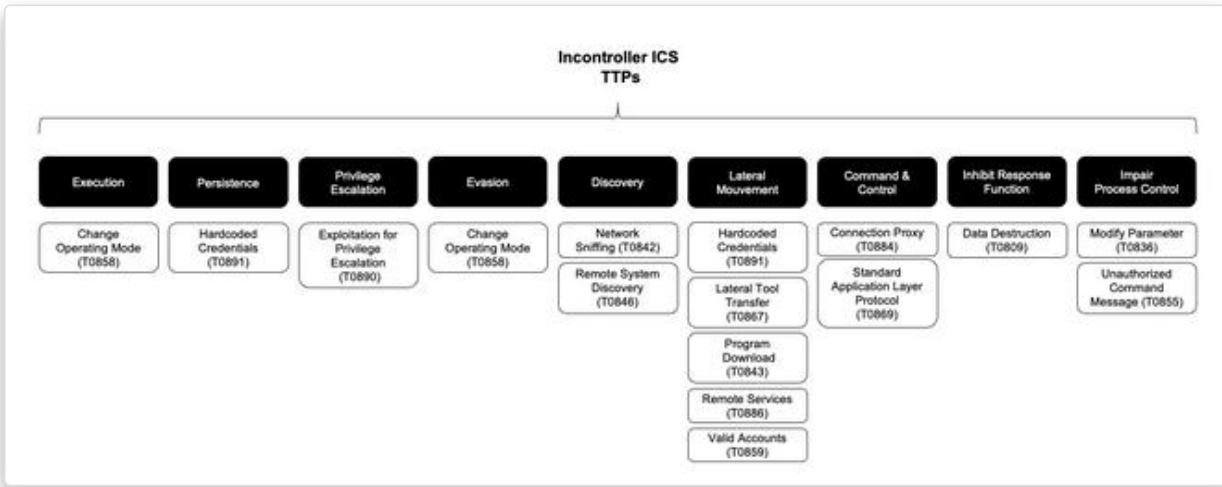


Figure 4-6 : Tactics, Techniques and Procedures of Incontroller. Source: MITRE ATT&CK ICS.

These few examples demonstrate the ability of attackers to specialize in the OT ecosystem and develop increasingly sophisticated malicious code that adapts to their environment.

4.4. Submarine Telecommunication Cables

As essential infrastructure for global electronic communications, submarine cables have repeatedly been mentioned as potential targets in the context of the conflict between Russia and Ukraine, or the tensions between China and the United States³⁵.

These fears follow, on the one hand, the sabotage of the Nordstream 1 and 2 gas pipelines at the end of September 2022 and, on the other, the supposed interest of numerous military, « fishing » or « research » vessels in intercontinental, regional or even local submarine cable routes.

In 2022, apart from hooking incidents (sometimes presumed to be physical attacks when vessels of interest were in the vicinity), a cyber attack on a submarine cable infrastructure was publicly acknowledged³⁶.

4.5. Satellite Communications (SATCOMs)

At a time when data is central and essential to the industry's operational functions, there is a continuing interest in satellite communications equipment and infrastructure. There are two main reasons for this interest:

- On the one hand, vulnerabilities are frequently identified in the various segments of these installations, such as modems and on-board facilities, but also in telecommunications equipment and onshore infrastructures, used in particular for the benefit of the maritime sector. These vulnerabilities can generally be explained by a failure to integrate cybersecurity



Maritime Cyber Threat Overview 2022

measures *by design*, in the absence of contractual requirements, implementation of best practices, evaluation and, lastly, the absence of secure configuration and maintenance to ensure a good level of cybersecurity over time.

- In addition, although some shipowners and offshore companies have taken encryption issues into account on these links, it is still all too common for them not to be encrypted. In many cases, therefore, interception remains a possibility for attackers with relatively unsophisticated means.

The fact that, in the vast majority of cases, the default passwords for these assets are not changed to facilitate subsequent remote maintenance, particularly by third-party maintainers, also presents a major risk of compromise.

In a context of increasing digitalization of ships and gradual migration to connected technologies known as « smart shipping » and « green shipping », remote connections between land and ships are set to multiply, as are « smart bridges » solutions, notably to facilitate navigation chart updates.

Finally, a number of events have had an impact on this sector in recent months:

- The attack on the KA-SAT ground segment at the start of the Russia-Ukraine conflict. This destructive attack, which has been the subject of several detailed analyses, including one by SEKOIA³⁷, may have impacted a small part of the maritime sector using this type of equipment, mainly in the fishing industry. On the other hand, the MRE sector was heavily impacted³⁸.
- The compromise of certain SATCOM equipment manufacturers may also have led to the leakage of sensitive information from satellite telecommunications installations.

4.6. Global Navigation Satellite System Jamming and Spoofing

Position, Navigation and Time (PNT) systems such as GNSS are crucial for the maritime and port sector. Prohibiting access to information obtained or calculated from one of these sources can have significant consequences that need to be anticipated:

- In the case of jamming, the loss of geographical references has an immediate impact on the bridge, where the loss of GPS through jamming normally generates alarms. It is essential that crew personnel are trained to react effectively in this case, and that efficient response procedures are formalized. The loss of GNSS has an immediate impact, through propagation, on other systems: Voyage Data Recorder (VDR), Automatic Identification System (AIS), as well as satellite telecommunication systems, which use information from GPS to correctly position their satellite dishes.
- In the case of spoofing attacks, targeting a particular vessel to make it deviate from its trajectory is a complicated attack to carry out, which often requires being close to or even on board of the vessel. The most frequently studied cases involve zone spoofing, in which a multitude of ships are displaced from their position by several hundred meters or even miles.



Maritime Cyber Threat Overview 2022

In both cases, the potential loss of the time reference may cause problems for certain information systems that use GNSS systems as a time reference, either directly or to feed an on-board NTP service. The impact may differ depending on the configuration of the equipment concerned.

Often overlooked, ports also use satellite positioning systems for crane positioning and, in some cases, for time synchronization.

Recommendations

Bypass solutions exist, depending on the type of vessel or its navigation zone, for example: use of interference-protected antennas (*Controlled Reception Pattern Antennas, CRPA*), use of dual- or tri-constellation receivers, detection of anomalies, use of third-party positioning resources: inertial units, other satellite systems.

France Cyber Maritime organized a specific webinar on this subject for its members at the end of 2022.

In general, certain maritime areas are subject to permanent jamming from state sources. Other, more ephemeral zones can be detected, notably in case of nearby of military deployments. The Russia-Ukraine conflict has led to the emergence of some new Anti Access/Area Denial (AA/AD) zones compared to 2021 (Figure 4-7).

The following zones remains at risk:

- Barents Sea, Baltic Sea and North Sea zone: permanent and significant disturbances have been noted in the area near Murmansk since at least August 2022. In addition to a small zone already established at the bottom of the Gulf of Finland, a new zone of disturbance appeared off the Kaliningrad enclave mid-December 2022, which appeared to extend up to a hundred nautical miles off the coasts of Lithuania, Poland and Latvia.
- Mediterranean zone: a zone that had been present for several years off the coast of Libya diminished during the second half of 2022 and no longer appears to represent a permanent threat. A large zone that has been present for several years between Port Said, Cyprus, south-east Turkey, Syria, Lebanon and Israel remains particularly active, at times disrupting as far as Sinai and the anchorage areas near Port Said and the entrance/exit to the Suez Canal.
- Black Sea zone: a major zone of GPS interference affects the Sea of Marmara, the Bosphorus Strait and the entire south-western Black Sea, as far as the Romanian coast, from Burgas to Constanta. The eastern Black Sea is also frequently affected, as far as Sochi in particular. In the absence of sensors further north, military operations in the north of the zone make AA/AD on frequencies used by GNSS systems permanent.
- Persian Gulf zone: no significant permanent GNSS interference zones are detected, certain military exercises or operations may result in occasional losses of GNSS reference.
- Asian zone: occasional presence of jammers, probably non-state-owned, in certain major port cities, which can lead to denial of access during ship port of calls. There have also been cases of interference during military exercises.

Maritime Cyber Threat Overview 2022



Figure 4-7 : Areas at risk of GNSS interference. Source: M-CERT.

4.7. Automatic Identification System Jamming and Spoofing

While cases of AIS jamming are poorly documented, there is continuing interest in AIS spoofing. This can take two main forms:

- Injecting false information directly to the API of maritime information fusion platforms. This preferred technique makes it easy to compromise information. While some spoofing attempts are easy to detect (Figure 4-8), not all are. Some cases of spoofing at the API level of large AIS information fusion platforms may also involve dozens, or even hundreds, of « ghost » vessels.
- There are also cases of spoofing using exclusively the radio frequency support: their primary purpose is often to mask the intentions or type of vessel, or even its actual position, in the case of military operations, smuggling, illegal fishing, etc. They can take place in the open sea or close to the coast.

Maritime Cyber Threat Overview 2022

The screenshot shows the Marine Traffic interface for a vessel named 'GRACEFUL', a yacht. The vessel's name and type are displayed at the top. Below is a photo of the yacht. The interface includes several data sections:

- Details:** ANONYMOUS, ETA: Apr 1, 14:00. Speed: 0.0 kn, Course: 12.0°, Draught: 3.8 m (max 3.8). Status: Aground, Last report: Feb 26, 2022 01:09 UTC.
- Location:** Hamburg, Germany, ATD: Feb 7, 06:26 UTC.
- PORT CALLS:** (Dropdown menu)
- WEATHER:** (Dropdown menu)
- VESSEL PARTICULARS:**

Gross Tonnage:	Built:	IMO number:
2685	2014	1011551
Deadweight:	Size:	MMSI:
540	80 / 20 m	273294110
- Navigation Data:** Predicted ETA: -, Distance / Time: -, Course / Speed: 0.0° / 0.0 kn, Current draught: 3.8 m, Navigation Status: Drifting, Position received: 11 mins ago, IAO / MMSI: 1011551 / 273294110, Callsign: FCKP1N, Flag: Russia, Length / Beam: 80 / 20 m.
- MAP POSITION & WEATHER:** A map of Europe with a red box highlighting the location in the Baltic Sea. Coordinates: Lat: 45.547, Lon: 21.64 (45° 32.920' N, 21° 40.800' E). Weather: 6°C / 43°F, Wind: 10.2 kn / 5.3 m/s, Waves: N/A.

Figure 4-8 : Example of spoofing on the position and navigation information of a vessel, in conjunction with the conflict between Russia and Ukraine. Action claimed by « Anonymous ». Source: Marine Traffic.



Maritime Cyber Threat Overview 2022

5. Maritime stakeholders: collateral victims of political cybercrime?

5.1. Distributed Denial of Service Attacks

Over the year 2022, several Distributed Denial of Service (DDoS) attacks affected both « showcase » websites and business servers exposed on the Internet. With the Russian invasion of Ukraine in 2022, DDoS has taken on a new dimension. Indeed, DDoS attacks are increasingly carried out by politically-motivated cybercriminals.

The Russian-Ukrainian conflict has led to a resurgence of nationalism, which in turn has led to the emergence of political cybercriminal groups (hacktivists), whose actions are mainly aimed at attacking Ukrainian institutions or countries that support them in any way.

The attacks carried out by these actors are mainly DDoS or defacement attacks. While no sector is specifically targeted by these attackers, whose aim is to destabilize a country, companies in the maritime sector have been symbolically targeted, because they are considered essential organizations for states that are really in the cybercriminals' sights.

Indeed, in addition to well-known entities such as *Anonymous*, new hacktivist groups sympathetic to Ukraine or Russia have emerged, targeting, among other things, enemy critical infrastructures. The main ones are the pro-Russian group *Killnet* and the pro-Ukrainian group *UA IT Army*. The DDoS attacks carried out in 2022 on critical infrastructures and geopolitically exposed multinational companies demonstrate that the danger is very real for the maritime sector, whose key role in the supply and operation of Western countries is beyond dispute.

Target	Origin / Motivation
Port of London Authority ³⁹	Killnet/Altahrea Team/Political
Port of Klaipeda ⁴⁰	NoName057(16)/Political
Port of Ventspils	NoName057(16)/Political
Port of Tallin	NoName057(16)/Political
Bulgarian ports infrastructure company	Killnet/Political
Port of Nagoya	Killnet/Political
LTM Livorno Terminal	Killnet/Political
Port of Venice	Killnet/Political
Ports & Maritime Organization of Iran	Army of Thieves/Political

Maritime Cyber Threat Overview 2022

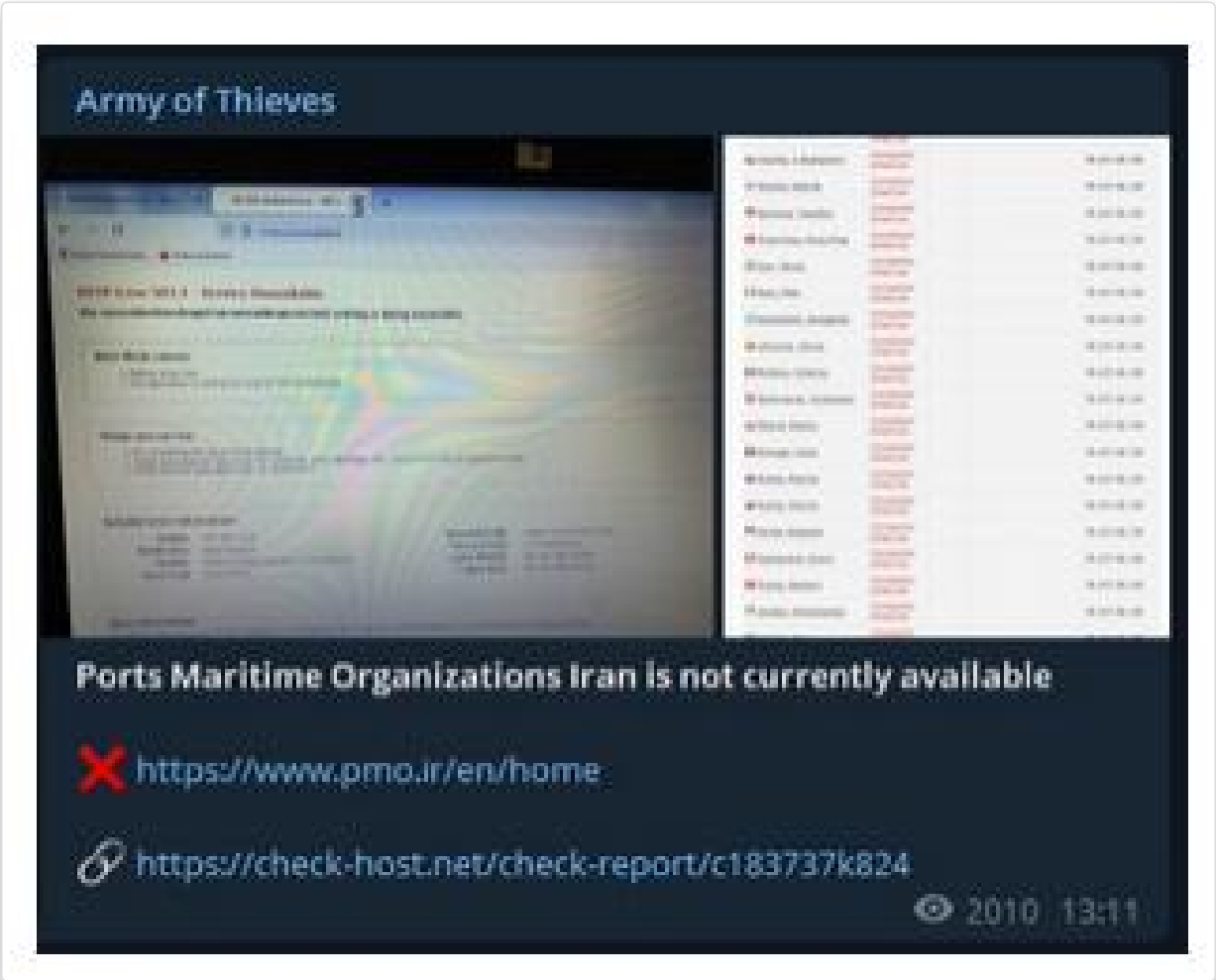


Figure 5-1 : On August, 31st 2022, the Internet website of the Ports & Maritime Organization of Iran is targeted by an attack. Source: t.me/ArmyThieves/125

Telegram

Telegram channels - as well as forums and marketplaces - are both the end and the beginning of the attack chain. They are the outlet for successful attacks and enable other attackers to plan their own attacks.

Maritime Cyber Threat Overview 2022

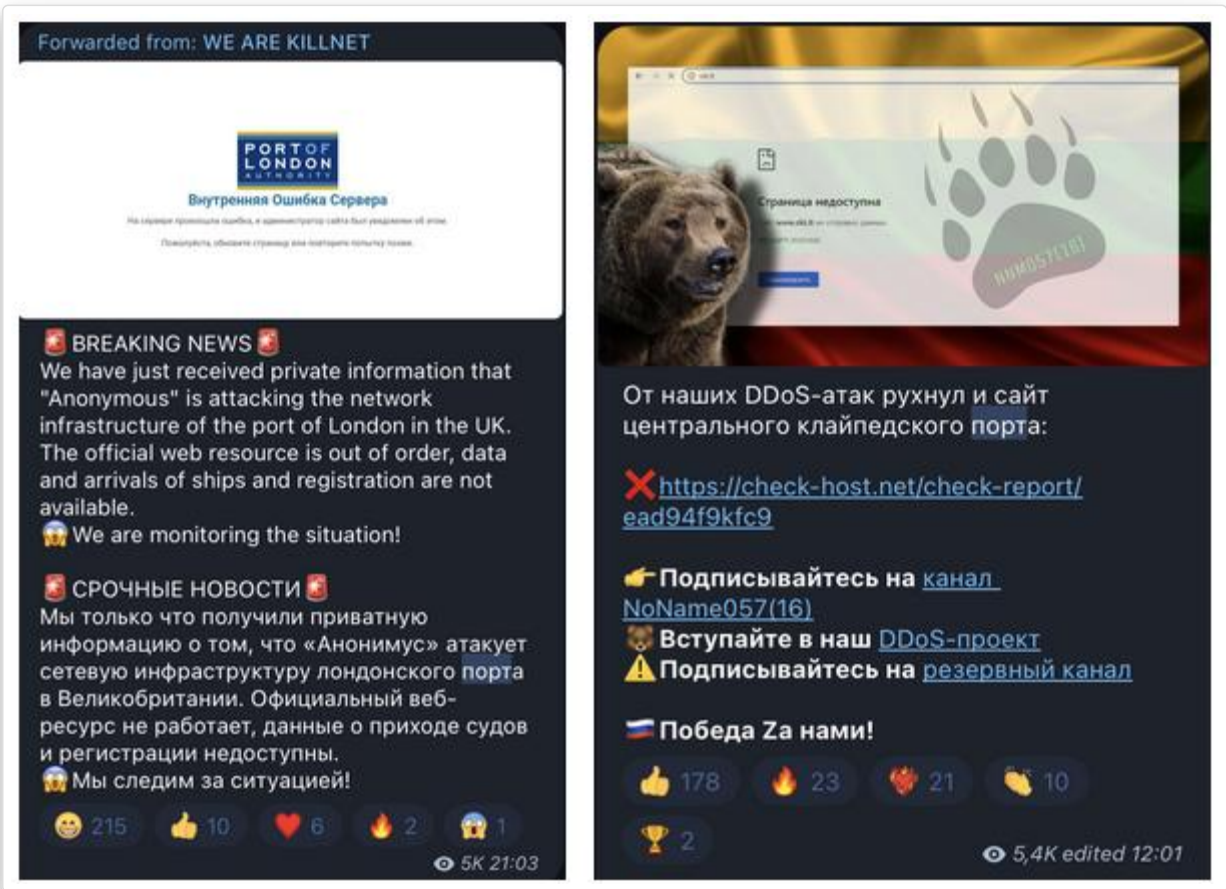


Figure 5-2 : Claims by Killnet and NoName057(16) of the DDoS attack on the Port of London and on the Port of Klaipeda.

DDoS attacks

DDoS attacks are recurrent, due to the - relative - ease to conduct them, making them accessible to any level of threat actors. Their aim is to disable one or more targeted services by exploiting hardware or software vulnerabilities. Denial of access involves the intervention of a network of - often compromised - machines to interrupt the targeted service(s). Whether it's a website or another application server, once paralyzed by the attack, the service will be unavailable and unusable, which can lead to financial and reputational losses. The financial impact of a DDoS attack should not be overlooked, as it can run into millions of euros. For example, Bandwidth Inc. estimates that a DDoS attack in 2021 could cost between \$9 and \$12 million⁴¹. According to a study by Imperva, based on a survey of 270 companies, a DDoS attack costs an average of \$40,000 per hour, or around \$500,000 on average⁴². The level of expertise and resources of the malicious actors behind these attacks varies cardinally. OWN-CERT has observed novice hackers (so-called script-kiddies) joining an attack organized by a group like *Killnet*, simply by downloading a script and procuring a VPN. Smartphone versions of these scripts are also available. By contrast, the best-organized cybercriminals specializing in « DDoS as a Service » often carry out their attacks using a network of compromised machines known as a « botnet ».



Maritime Cyber Threat Overview 2022

5.2. Threat actors conducting DDoS attacks

Four types of malicious actors involved in DDoS attacks can generally be identified: ** state actors, financially motivated actors, hacktivists** and, more marginally, individuals using these attacks as a diversion.

In the case of state-employed and state-controlled actors, DDoS attacks generally have a political objective, that of disabling targets designated as important. One state group known to specialize in DDoS attacks and the use of *wiper* malware⁴³ is «Unit 74455⁴⁴», which US intelligence services link to Russia, and more specifically to the GRU's *Main Center for Special Technologies*⁴⁵. The group is believed to have been operating since at least 2009, and to have specifically targeted critical infrastructure, including the transport systems of NATO member states.

Some malicious actors use DDoS attacks for financial gain. There are several ways of monetizing DDoS attacks.

5.2.1. Methods and organization of DDoS threat actors

Malicious actors observed by CERT OWN offer DDoS as a commercial service (Figure 5-3). One of the objectives may be to harm a competitor by making their website inaccessible.

Another means of monetization is to force the victim to pay a subscription fee to protect against future attacks. In this case, cybercriminals usually also guarantee protection against DDoS attacks carried out by other cybercriminal groups.

A final example of a monetization method is to require a ransom from the target of the attack. This last case can be coupled with other attacks, such as ransomware encryption. Indeed, the LockBit ransomware group declared in August 2022 that it wished to couple its ransom demands with DDoS attacks, in order to increase the pressure on its victims and force them to pay.

Maritime Cyber Threat Overview 2022

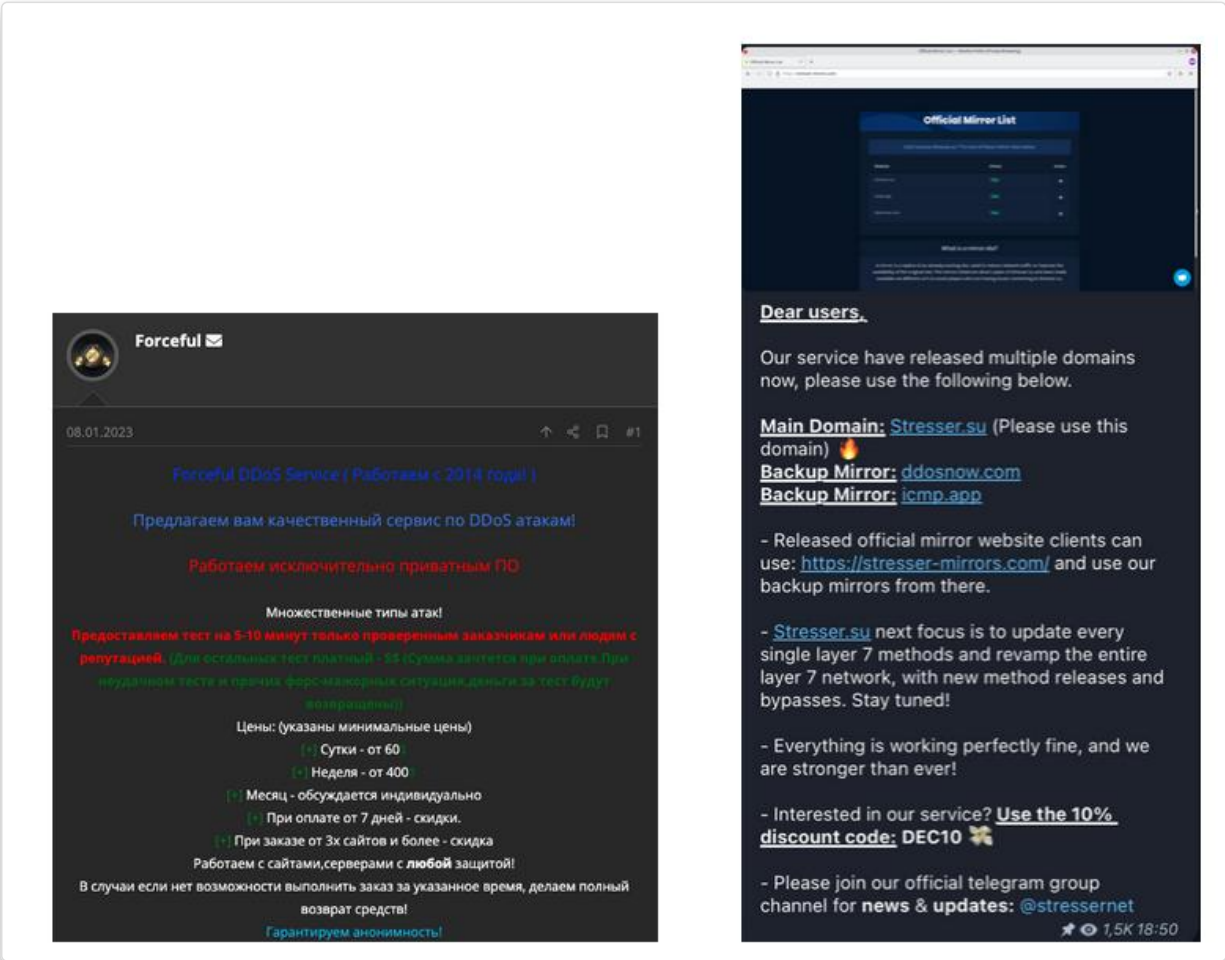


Figure 5-3 : On the left, a DDoS service for sale on a Russian-speaking cybercriminal forum. On the right, a DDoS service for sale on an English- and Chinese-speaking Telegram channel. Source: OWN-CERT.

DDoS attacks carried out by hacktivists have attracted particular media attention due to the geopolitical context with the Russian invasion of Ukraine. Dozens of groups such as Killnet, NoName057 and its «DDoSia» project, Infocentr and Anonymous Russia are known for their commitment to Russia and their attacks on Western companies and institutions (Figure 5-4).

Less numerous, well-organized pro-Ukrainian groups also exist. The most important of these are the « IT Army of Ukraine », and the « Student Committee of Cybersecurity and Defense of Ukraine ».

Maritime Cyber Threat Overview 2022

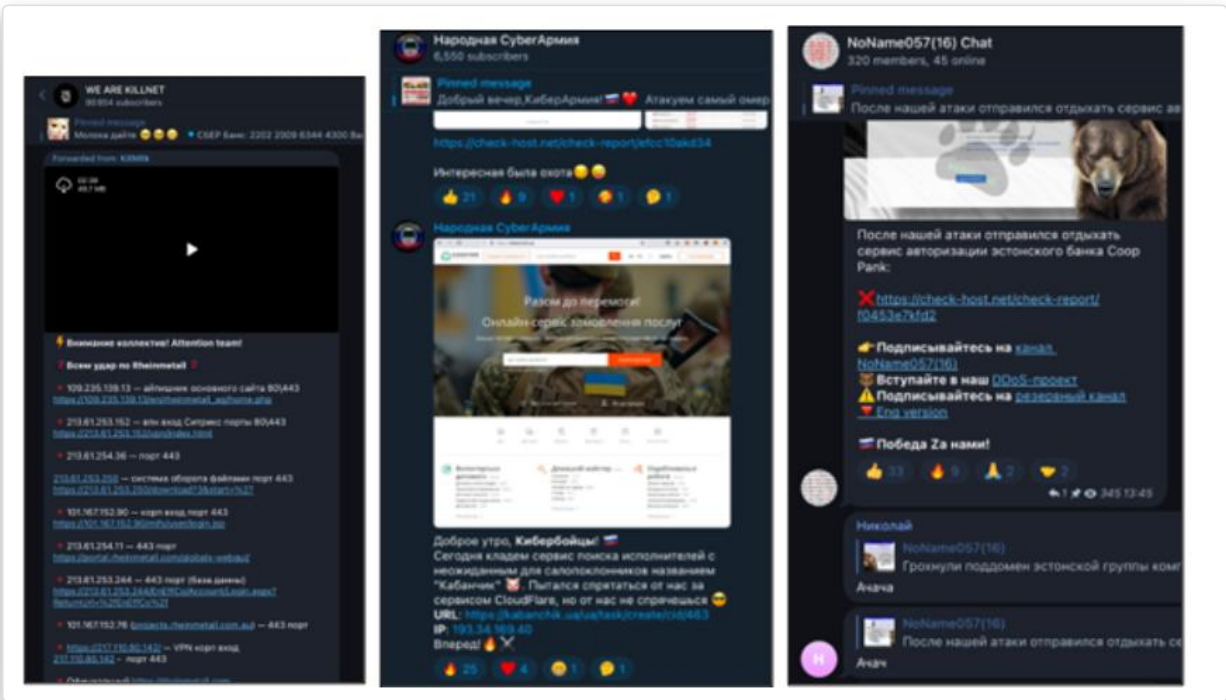


Figure 5-4 : Examples of Telegram channels belonging to pro-Russian hacktivist groups specializing in DDoS attacks. Source: OWN-CERT.

The IT Army of Ukraine has its own website, where it is possible to obtain the tools and information needed to conduct attacks against targets named by the entity. In addition, the site presents a ranking of the top players who have carried out the most attacks against enemy infrastructures (Figure 5-5).

The above examples illustrate the fact that DDoS attacks are currently extremely commonplace, with relatively easy access to DDoS tools. Cybercrime forums feature dedicated sections, with tutorials and manuals for training (Figure 5-6).

An alternative for cybercriminals not wishing to carry out attacks themselves is to pay for a DDoS service. « DDoS as a Service » is easily accessible to anyone looking for information on cybercriminal forums, Telegram channels or simply on the web. Indeed, sites advertising « IP Stressers » services and offering comparisons according to attack type and price are easily identifiable via a simple Internet search (Figure 5-7). Prices can vary from a few dozen euros for low-level attacks, to tens of thousands of euros for the most sophisticated and long-lasting.

Maritime Cyber Threat Overview 2022

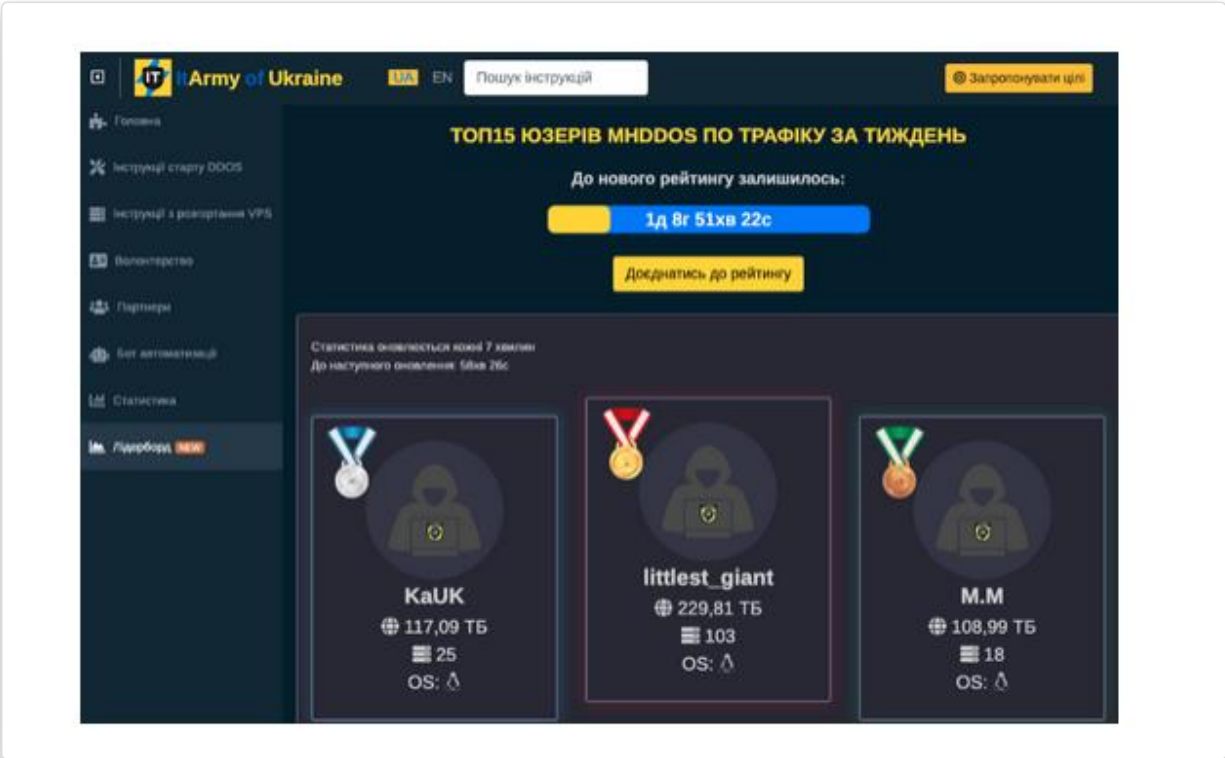


Figure 5-5 : Official website of the IT Army of Ukraine. Ranking of the « best » DDoS actors. Source: OWN-CERT.

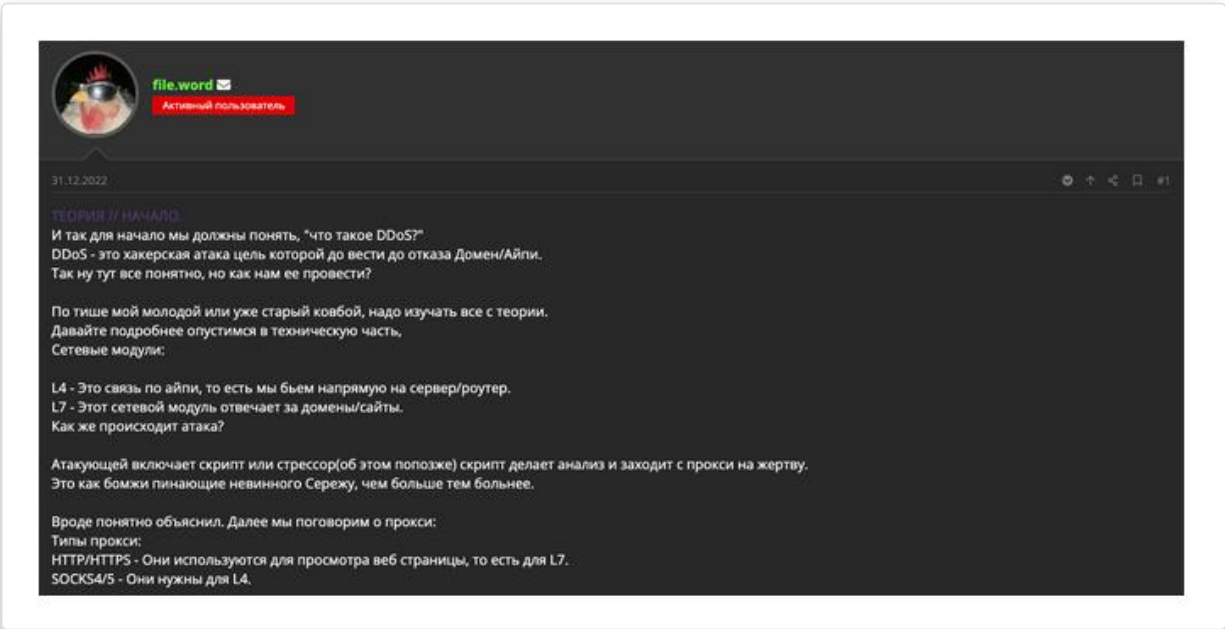
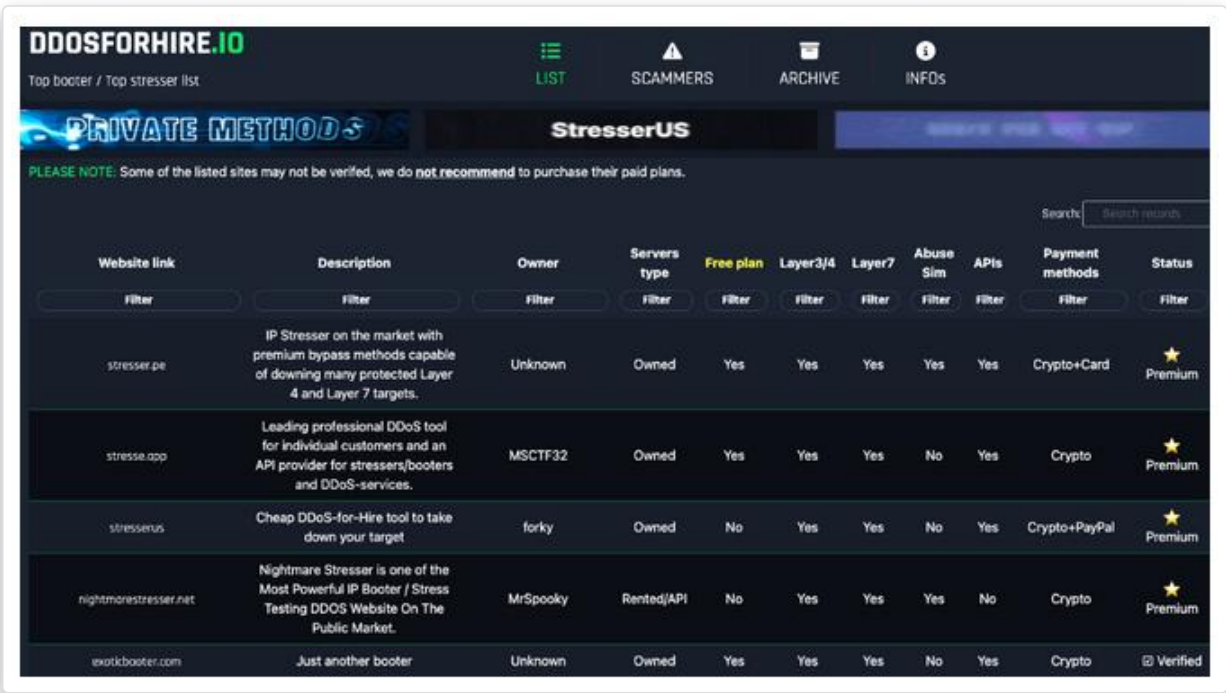


Figure 5-6 : A threat actor gives basic explanations on DDoS for novice. Source: OWN-CERT.

Services offering to test the solidity and reliability of a network or, for example, an Internet site, exist both legally and illegally. Indeed, IP *stresser* and *booter* services are legitimately offered to network

Maritime Cyber Threat Overview 2022

administrators wishing to assess the stability of their system. A *stresser* is a tool designed to test the robustness of a network or server. In particular, it enables the administrator to assess whether existing resources - such as bandwidth or computing capacity - are sufficient to handle an additional load. The IP stresser can, however, be hijacked and used to block access to the targeted service.



Website link	Description	Owner	Servers type	Free plan	Layer3/4	Layer7	Abuse Sim	APIs	Payment methods	Status
stresser.pe	IP Stresser on the market with premium bypass methods capable of downing many protected Layer 4 and Layer 7 targets.	Unknown	Owned	Yes	Yes	Yes	Yes	Yes	Crypto+Card	Premium
stresser.app	Leading professional DDoS tool for individual customers and an API provider for stressers/booters and DDoS-services.	MSCTF32	Owned	Yes	Yes	Yes	No	Yes	Crypto	Premium
stresser.us	Cheap DDoS-for-Hire tool to take down your target	forky	Owned	No	Yes	Yes	No	Yes	Crypto+PayPal	Premium
nightmarestresser.net	Nightmare Stresser is one of the Most Powerful IP Booter / Stress Testing DDoS Website On The Public Market.	MrSpooky	Rented/API	No	Yes	Yes	Yes	No	Crypto	Premium
workbooter.com	Just another booter	Unknown	Owned	Yes	Yes	Yes	No	Yes	Crypto	Verified

Figure 5-7 : A website giving a comparison of existing DDoS services. Source: OWN-CERT.

Booters, also known as *service booters*, are on-demand DDoS attack services offered by certain criminals with the aim of disabling websites and networks. In other words, booters encompass the hijacked use of IP stressers⁴⁶.

Both tools are frequently presented as SaaS (Software as a Service). Prices range from a few dozen dollars a month to several thousand dollars for the most comprehensive services (Figure 5-8).

Last but not least, malicious actors wishing to go into this business on their own can do so, with virtually no outlay.

Scripts are, for example, freely available on GitHub (Figure 5-9) and are widely exploited by cybercriminals like Killnet. These scripts, initially dedicated to auditing and penetration testing, end up being hijacked and used for malicious purposes. For example, CERT-UA discovered that the BrownFlood JavaScript, used to attack Ukrainian sites, was published on GitHub a month before the attack⁴⁷.

Maritime Cyber Threat Overview 2022

BASIC	ADVANCED	EXPERT	MASTER
€65.00 per month	€192.00 per month	€315.00 per month	€620.00 per month
86,400 Seconds Maximum Attack Time	86,400 Seconds Maximum Attack Time	86,400 Seconds Maximum Attack Time	86,400 Seconds Maximum Attack Time
1 Simultaneous Attacks (€ 65.00 each)	3 Simultaneous Attacks (€ 64.00 each)	5 Simultaneous Attacks (€ 63.00 each)	10 Simultaneous Attacks (€ 62.00 each)
UNLIMITED PREMIUM NETWORK	UNLIMITED PREMIUM NETWORK	UNLIMITED PREMIUM NETWORK	UNLIMITED PREMIUM NETWORK
No API Included	No API Included	API Included	API Included
Unlimited Daily Attacks	Unlimited Daily Attacks	Unlimited Daily Attacks	Unlimited Daily Attacks
Gain €2.60 Reward Points!	Gain €7.68 Reward Points!	Gain €12.50 Reward Points!	Gain €15.00 Reward Points!
UPGRADE PLAN	UPGRADE PLAN	UPGRADE PLAN	UPGRADE PLAN
GODLIKE	MONSTER	ENTERPRISE	OVERKILL
€1,800.00 per month	€2,900.00 per month	€5,500.00 per month	€15,600.00 per month

Figure 5-8 : Example of stresser services and corresponding prices. Source: OWN-CERT.

MHDDoS

MHDDoS - DDoS Attack Script With 56 Methods

(Programming Language - Python 3)

FORKS 1.8K | LAST COMMIT YESTERDAY | STARS 9.7K | LICENSE MIT | ISSUES 63 OPEN

Please Don't Attack websites without the owners consent.

- Layer 7 Dstats

Figure 5-9 : Example of a DDoS script with up to 56 attack methods. Source: OWN-CERT.



Maritime Cyber Threat Overview 2022

6. Maritime Cybersecurity: Outlook for 2023

The outlook chapter is always a difficult exercise in cybersecurity: anticipating remains a challenge, given the constantly evolving nature of the threat and the complexity of the maritime sector. However, the long-term trends identified in 2022 offer some perspectives:

- First of all, there is no doubt that **cyber activity in 2023 will remain more closely linked than ever to the geopolitical context**. At the time of writing, there is little doubt that the Russia-Ukraine conflict will continue in the coming months: the various events identified in 2022 in connection with this conflict (sabotage attempts, informational influence struggles, criminalization of DDoS-type activities) are likely to continue, targeting in particular the naval defense sector, administrations and, more broadly, all maritime, naval, port and industrial entities considered to be playing a role in supporting the conflict⁴⁸.
- Particular attention will need to be paid to the strengthening of bipolarization on a more global scale, with geopolitical tensions likely to intensify and have consequences in cyberspace, prior to or accompanying military action: new cyber players would bring new techniques, tactics and procedures, new platforms and new targets.
- The growing number of attack campaigns against industrial systems demonstrates the adaptation of players in this field, with some even specializing in this type of attack. The specific characteristics of the maritime sector make it a direct or indirect target: ports and ships depend on complex systems, which for a long time were disconnected from the rest. Today, this compartmentalization is much less clear-cut in the face of growing hyperconnectivity. In the current geopolitical context, it's not out of the question for attackers close to governments to use specialized malicious code on industrial systems.
- The cybercriminal threat, politicized or otherwise, should not be discounted either, since ransomware attacks have already targeted this type of facility. Particularly revealed during 2022, this type of attack continues into 2023 and, while not a destructive tool, it can have reputational and financial impacts on companies.
- The use of various infostealers such as Vector Stealer, initiated at the end of 2022, continues into 2023.
- As a primary target, opportunity or collateral victim, **the maritime sector will have to constantly adapt to the innovations of malicious actors**. OWN-CERT has already identified, for example, the widespread use of OneNote attachments in all sectors by early 2023. To make their social engineering methods even more credible, threat actors will continue to personalize their content (e-mails, files, etc.) using professional vocabulary or references to industry events. If they already rely on the standard documents exchanged by maritime IT (*Bill of lading, Notice of readiness...*), **it is possible that certain actors with advanced capabilities will broaden their scope to include OT jargon** (SCADA themes, automation, cargo or propulsion control).
- **The potential use of alternative means to phishing** by e-mail in order to obtain information (e.g. professional or private social networks, telephone calls, *smishing...*) should increase.



TLP:CLEAR

TLP:EX:NC



Maritime Cyber Threat Overview 2022

- The heterogeneity of information systems, whether connected or disconnected, onshore, offshore or on ships, reinforces **the need for vigilance regarding propagation methods on physical devices**.
- The continued discovery of **vulnerabilities** in widely-used development libraries which, **in a context of increased outsourcing**, are sometimes difficult to identify in the absence of mapping shared by all players, should remain a topical issue.
- In the face of a fiercer battle against ransomware, **data leaks are likely to remain a major pressure point**.
- While some may have doubted the value of artificial intelligence (AI) for the design of a cyber attack, demonstrations by some researchers of tools such as ChatGPT should alert the community to the existence and performance of certain tools available to the public. Increased competition in this sector, with the arrival of new players, will accentuate the number of tools available, their capabilities, timeliness and accuracy. Beyond the preparation of attacks, there is little doubt that the development of automated AI-based attack tools will continue, both by state or pseudo-state agencies and by cybercriminals.
- **Attacks deliberately or opportunistically targeting players in the maritime and port supply chain, in the broadest sense, are likely to continue**, for several reasons: the number and sometimes low technological and organizational maturity of certain players in terms of cybersecurity, the strong digital transformation of the sector with heavy reliance on outsourcing and the cloud. In a context of strong interdependence, an attack on a *supply chain* player such as an outsourcer or MSP (*Managed Service Provider*) has considerable consequences: for example, a multitude of ships belonging to different shipowners could find themselves impacted by the loss of a common information system operated by a *supply chain* player.

With direct links to the logistics supply, industrial supervision systems, agri-food, retail, telecommunications, defense and energy sectors, the maritime sector needs to broaden its threat and risk model towards a contiguous, global approach to cyber threat intelligence.

In this context of ongoing digital transformation of the sector, we can acknowledge the gradual rise in maturity of certain players, grouping together within partnerships such as France Cyber Maritime to encourage the sharing of cyber information, which remains a particularly effective means of preventing attacks, not only in France but also internationally and not forgetting overseas: efforts in this direction deserve to be continued and supported.

TLP:CLEAR

TLP:EX:NC



Maritime Cyber Threat Overview 2022

7. Glossary

This glossary explains the meaning of some of the acronyms and expressions used in this bulletin. The maritime and port experience of the people to whom these bulletins are addressed may differ, and a common language is necessary for a proper understanding of the concepts addressed.

A2/AD

Anti Access/Area Denial: tactics designed to prevent the use of an area and, by extension, any means of carrying out operations in that area.

ADMIRAL

Advanced Database of Maritime cyber Incidents Released for Litterature

AIS

Automatic Identification System

APT

Advanced Persistent Threat

BEC

Business Email Compromise

CERT

Computer Emergency Response Team

CMS

Content Management System

CRPA

Controlled Radiation Pattern Antenna

CTI

Cyber Threat Intelligence

DDoS

Distributed Denial of Service

GNSS

Global Navigation Satellite System

GPS

Global Positioning System

IAB

Initial Access Broker

IoC

Indicator of Compromise

IT



TLP:CLEAR

TLP:EX:NC



Maritime Cyber Threat Overview 2022

Information Technology

LNG

Liquefied Natural Gas

M-CERT

Maritime Computer Emergency Response Team

MRE

Marine Renewable Energy

OSINT

Open Source Intelligence

OT

Operational Technology

PNT

Position, Navigation, Time

RAT

Remote Administration Tool

RDP

Remote Desktop Protocol

SSH

Secure SHell

SQL

Structured Query Language

TLP

Traffic Light Protocol

TTP

Techniques, Tactics, Procedures ! USB

Universal Serial Bus

VDR

Voyage Data Recorder

VPN

Virtual Private Network

VSAT

Very Small Aperture Terminal

XSS

Cross Site Scripting

TLP:CLEAR

TLP:EX:NC



Maritime Cyber Threat Overview 2022

8. About France Cyber Maritime and the M-CERT

France Cyber Maritime is a French « Loi 1901 » non-profit organization created in November 2020 and backed by the French national cybersecurity agency (Agence Nationale de Sécurité des Systèmes d'Information, ANSSI) and by the French inter-secretary for the Sea (Secrétaire Général de la Mer, SGMer).

The main objectives of the association are:

- develop a network of expertise in maritime cybersecurity, stimulating the creation of high value-added services tailored to industry needs;
- improve the resilience of maritime and port operations in the face of cyber threats by developing and operating the M-CERT (Maritime Computer Emergency Response Team), which provides information and assistance to all operators.

The activity of M-CERT started in March 2021. M-CERT produces regular analysis bulletins for the members of the organization. In addition to Cyber Threat Intelligence services, M-CERT is also a committed player in cyber risks prevention and in the coordination of incident response, in relation with state authorities and cybersecurity organizations.

As of early 2023, France Cyber Maritime brings together 70 members of the maritime sector at large, as well as cybersecurity and maritime administrations, and benefits from national and international partnerships.

To contact us:

	France Cyber Maritime	M-CERT
Website	https://www.france-cyber-maritime.eu	https://www.m-cert.fr
E-mail	contact@france-cyber-maritime.eu	contact@m-cert.fr
Twitter	@FrCyberMaritime	@M_CERT_FR
LinkedIn	https://www.linkedin.com/company/france-cyber-maritime	

Maritime Cyber Threat Overview 2022

9. About OWN



Figure 9-1 : OWN's Logo

Founded in 2008, OWN is a cybersecurity Pure Player with a lucid and perceptive vision of its customers' cybersecurity challenges, through a rich portfolio of activities divided into 5 competencies: Audit, Consulting, Threat Intelligence, CERT and SOC.

On a daily basis, OWN supports small, medium-sized and large organizations, enabling them to carry out their business in the best possible conditions, by offering continuous improvement of their cybersecurity and assistance in anticipating, detecting and reacting to cyber threats. OWN's cybersecurity approach focuses on the threat and risks in their technical, organizational and geopolitical dimensions, and constitutes its DNA, the sequencing of which is based on : Operate, Warn, Neutralize. Three actions that fully symbolize the day-to-day role of our experts: advising and taking part in cyber-defense actions, informing and alerting when the risk is imminent, and finally contributing to remediation to neutralize the threat.

Website: <https://ww.own.security>

Contact: contact@own.security



Maritime Cyber Threat Overview 2022

10. References

1. <https://www.first.org/tlp/>
2. <https://gitlab.com/m-cert/admiral>
3. *Inland zone of influence and economic attraction of the port.*
4. <https://www.cluster-maritime.fr/la-filiere-maritime/leconomie-maritime/>
5. <https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft>
6. See <https://nvd.nist.gov/vuln/detail/CVE-2022-40684> (Fortinet), <https://nvd.nist.gov/vuln/detail/CVE-2022-41352> (Zimbra), <https://nvd.nist.gov/vuln/detail/CVE-2022-22947> (VMWare), <https://nvd.nist.gov/vuln/detail/CVE-2022-27518> (Citrix) and <https://g3.cert.edf.fr/alert/2022/27eb58eb-e273-44d1-86ca-bf67c93979ce.html> (Microsoft), of which Exchange : <https://msrc.microsoft.com/blog/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/>
7. <https://thedfirreport.com/2023/03/06/2022-year-in-review/>
8. MITRE ATT&CK is an open knowledge base on threat actors, their tools, tactics, techniques and attack procedures. MITRE ATT&CK offers its own kill chain, listing attack techniques. cf <https://attack.mitre.org>
9. <https://www.fortinet.com/blog/threat-research/deep-analysis-formbook-new-variant-delivered-phishing-campaign-part-ii>
10. SHA256: [edf47cd187c4b8d92f09152b5e1285366c03afa1a4be4815f853ded3b1240ce6](https://www.fortinet.com/blog/threat-research/deep-analysis-formbook-new-variant-delivered-phishing-campaign-part-ii)
11. SHA256: [bc3a22bf48c38ec75a45f8d70f04af9fee4f58b190dada24c2f65fe73184b596](https://www.fortinet.com/blog/threat-research/deep-analysis-formbook-new-variant-delivered-phishing-campaign-part-ii)
12. MV: Motor Vessel
13. SHA256: [5b312f6c8aaea04ae089007f9429a8e651bb73fa2069fb9418d0fa85f04f7c17](https://www.fortinet.com/blog/threat-research/deep-analysis-formbook-new-variant-delivered-phishing-campaign-part-ii)
14. SHA256: [4797d55178aa25fa8e5938b65162d71dc4da21bc8bc51d3138bfb09a805190bd](https://www.fortinet.com/blog/threat-research/deep-analysis-formbook-new-variant-delivered-phishing-campaign-part-ii)
15. SHA256: [63c6132898aa1688e9cbc165713df00213d9aee29127aa710d138e0d55eb5145](https://www.fortinet.com/blog/threat-research/deep-analysis-formbook-new-variant-delivered-phishing-campaign-part-ii)
16. SHA256: [11f59f304cbb0d10023ff8e405f28bc52e02cfefa963ff35e79e66020770703b](https://www.fortinet.com/blog/threat-research/deep-analysis-formbook-new-variant-delivered-phishing-campaign-part-ii)
17. <https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf>
18. <https://britanniapandi.com/2022/04/cyber-fraud-incident/>
19. <https://unit42.paloaltonetworks.com/operation-falcon-ii-silverterrier-nigerian-beck/>
20. SHA256: [46b006db8260be2e32171038ee3fe8cc52552d460efef4ab8cf2c549a778dc86](https://unit42.paloaltonetworks.com/operation-falcon-ii-silverterrier-nigerian-beck/)
21. SHA256: [d968ed7e0301421afa50ab0996cb7874744c4d0caedf39a856322d5d1bbd0129](https://unit42.paloaltonetworks.com/operation-falcon-ii-silverterrier-nigerian-beck/)
22. <https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/>
23. <https://unit42.paloaltonetworks.com/plugx-variants-in-usbs/>
24. <https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea>
25. also known as Leviathan or APT40.



TLP:CLEAR

TLP:EX:NC



Maritime Cyber Threat Overview 2022

26. <https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping>
27. <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hydrochasma-asia-medical-shipping-intelligence-gathering>
28. <https://www.mandiant.com/resources/blog/apt32-targeting-chinese-government-in-covid-19-related-espionage>
29. <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hydrochasma-asia-medical-shipping-intelligence-gathering>
30. <https://blogs.blackberry.com/en/2023/02/newspenguin-a-previously-unknown-threat-actor-targets-pakistan-with-advanced-espionage-tool>
31. <https://www.dragos.com/year-in-review/>
32. <https://www.forescout.com/blog/ot-icefall-56-vulnerabilities-caused-by-insecure-by-design-practices-in-ot/>
33. <https://ics-cert.kaspersky.com/publications/reports/2022/06/27/attacks-on-industrial-control-systems-using-shadowpad/>
34. <https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool>
35. <https://www.ege.fr/infoquerre/les-cables-sous-marins-nouvel-echiquier-du-conflit-americano-chinois>
36. <https://www.hawaiinewsnow.com/2022/04/13/hsi-agents-honolulu-disrupted-cyberattack-undersea-cable-critical-telecommunications/>
37. <https://share.sekoia.fr/s/B6s8EtRp2G8EnT>
38. <https://securityintelligence.com/news/acidrain-malware-modems-ukraine-germany/>
39. Claudia Glover, « Port of London Authority Hit by "politically Motivated" Cyberattack », Tech Monitor (blog), 24 mai 2022, <https://techmonitor.ai/technology/cybersecurity/port-of-london-authority-cyberattack>
40. Ylabs, « Analysis of the Russian-Speaking Threat Actor NoName 057(16) », YLabs, 13 octobre 2022, <https://labs.yarix.com/2022/10/analysis-of-the-russian-speaking-threat-actor-noname-05716/>
41. <https://www.sec.gov/Archives/edgar/data/1514416/000151441621000280/q32021exh991-preliminaryth.htm>
42. <https://www.imperva.com/blog/ddos-impact-cost-of-ddos-attack/>
43. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | CISA", Cybersecurity and Infrastructure Security Agency CISA, 9 mai 2022, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>
44. <https://intelnews.org/tag/gru-unit-74455/>
45. <https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>
46. <https://www.imperva.com/learn/ddos/booters-stressers-ddosers/>
47. <https://www.malwarebytes.com/blog/news/2022/04/ukraine-government-and-pro-ukrainian-sites-hit-by-ddos-attacks>
48. considering that "playing a role" is seen from the perspective of the attacker, it will continue to be particularly subjective.

TLP:CLEAR

TLP:EX:NC