Analysis of some case studies on cyberattacks and proposed methods for preventing them

Daniel Mihai LEU[1], Cătălin UDROIU[1,2], Gabriel Mărgărit RAICU[1], Horațius Nicolae GÂRBAN[1,3], Mircea Constantin ȘCHEAU[1,4]*

[1] Constanta Maritime University, Constanta, Romania
daniel.leu@maritimecybersecurity.center, catalin.udroiu@cmu-edu.eu, gabriel.raicu@cmu-edu.eu, horatiu.garban@cmu-edu.eu, mircea.scheau@cmu-edu.eu
[2] ZF Group, Friedrichshafen, Germany
udroiu_catalin@yahoo.com
[3] Ministry of National Defence, Romanian Cyber Defence Command, Bucharest, Romania
hgarban@mapn.ro
[4] University of Craiova, Craiova, Romania

***Corresponding author:** Mircea Constantin ȘCHEAU
mircea.scheau@edu.ucv.ro

Abstract: The last few years have brought about a tremendous increase in the speed of technological advancement and digitalisation which led to an exponential uptick in the amount of data that is being either stored or moved across the cyberspace. This data, either under the ownership of a company operating in the private sector, or of a public sector organization, has become a priority target for malicious actors. From actors that operate under the alleged guise of financially motivated reasons such as ransomware operators to nation state threat groups and politically motivated actors that engage in hacktivist campaigns, an important certainty is that confidential data has become a top priority target for the various types of malicious actors operating across the cyber threat spectrum. Whether it is being sold to the highest bidder, released for free or used in the context of nation state affairs, confidential data became a high-value resource which, in combination with the increasingly complex and politically charged international context of the last few years, has brought about an uptick in number of cyber operations that could be classified as espionage. The aim of this paper is to present a study showcasing the various ways in which data theft, as the main objective, can materialize through malicious cyber campaigns ranging from ransomware operations executed by documented and well-known actors, to malware operations executed under the radar by obscure malicious actors.

Keywords: cyber warfare, exfiltration, state sponsors, strategy, damages.

Analiza unor studii de caz privind atacurile cibernetice și metode propuse pentru prevenirea acestora

Rezumat: Ultimii ani au condus la o creștere extraordinară a vitezei de evoluție tehnologică și digitalizare, ceea ce a impus o creștere exponențială direct proporțională a cantității de date stocate sau migrate în spațiul cibernetic. Informațiile ce pot fi deținute de o companie care operează în sectorul privat sau de o organizație din sectorul public, au devenit o țintă prioritară pentru infractorii rău intenționați. De la actorii care operează sub presupuse pretexte financiare, cum ar fi cei care exploatează și injectează coduri ransomware, până la grupurile susținute statal și actorii motivați politic, care se angajează în campanii hacktiviste, se desprinde cu certitudine ideea importantă că datele confidențiale sunt în acest moment țintă incontestabilă pentru diferite tipuri de actori ce operează pe întregul spectru de amenințări cibernetice. Fie că sunt vândute pe baza celei mai bune oferte, fie că sunt încărcate gratuit pe piața neagră sau sunt utilizate ca monedă de schimb în tranzacții interstatale, datele confidențiale au devenit o resursă de mare valoare care, coroborată cu contextul internațional din ce în ce mai complex și instabil politic din ultimii câțiva ani, a scos în evidență. o creștere a operațiunilor cibernetice ce pot fi catalogate drept spionaj. Scopul prezentului articol este de a realiza un studiu prin care se prezintă diferite moduri în care furtul de date, ca obiectiv principal, se poate materializa prin intermediul campaniilor cibernetice, în care atacurile cu malware sunt executate țintit, în urma unei foarte bune documentări de grupuri infracționale neanonimizate, sau de actori statali cu scopuri nedeclarate.

Cuvinte cheie: cyber warfare, exfiltration, state sponsors, strategy, damages.

1. Introduction

Espionage activity can be broadly defined as the act of collecting sensitive and confidential information from one party on behalf of another. Even though espionage is not by a long shot a new concept, with records of its use dating back to the fifth century, the last years highlighted an

https://doi.org/10.33436/v33i2y202309

observable increase in cyber operations that leverage the exfiltration of confidential data as an end goal.

The progress of digital transformation has inevitably led to new cybersecurity threats. Cybercriminals have taken advantage of the Covid-19 pandemic, in particular by targeting organizations and companies working remotely.

The total number of compromised data in 2021 was approximately 23%, higher than the highest level previously recorded, the number of affected people remaining, however, at a high level, but decreasing for the third consecutive year.

The annual Data Breach Report for the year 2021 elaborated by the Identity Theft Resource Center (Velasquez, 2022) included reference to the fact that the average number of attacks aimed at compromising data increased by about 68% compared to 2020, reaching a total number of over 1800 identified events. The main categories targeted by different actors involved sensitive information such as national security numbers, but with a slight decrease compared to 2020, from 83% to 80%, well below the maximum level reached in 2017, by 95%. As an overall statistic, the total number of involved victims decreased by five percent in the year 2021 compared to 2020, as the main identified actors target a specific type of data and not mass-scrapping data acquisition. Although the total number of targeted victims decreased, the overall number of users whose data had been compromised multiple times in only one year remains still high. 2021 has seen a surge of ransomware and cyberespionage attacks against targets ranging from international meat producers, and oil pipelines, to global technology companies.

According to a report made by Cybersecurity Ventures (Morgan, 2020), cybercrime costs will grow by 15 percent per year to reach US$10.5 trillion by 2025, the third greatest “economy” in the world, after those of the Unites States of America and China.

Cybersecurity Companies predicted that a ransomware attack occurs every 11 seconds and the forecasts of their global ransomware damages will be around $20 billion in 2025 (Morgan, 2021). Getting hit with ransomware is not necessarily a cybersecurity failure, today it is a fact of life.

Given this wide spread of cyberattacks in terms of number, geographical spread and variations in attack methods, this study focused on three current cyberespionage methods used by cybercriminals successfully. The study first analyses the manner in which these two cyberattacks took place and, subsequently, proposes methods for preventing them.

Thus, in the first part of the study the typical steps taken in case of cyber operations for espionage are detailed in view of preparing the analysis of the proposed case studies. Further on, the study aims to present an overview on two distinctive, sophisticated operations in which the malicious actors had the objective to either disrupt normal activities for the target or to secure a foothold in the targeted systems from where they could monitor communications and exfiltrate data. The ransomware attack on Colonial Pipeline is the first use case, as it presents certain techniques and tactics that have been replicated in subsequent similar attacks. The second use case is related to information stealers and the manner in which they are spread across the world in infected devices waiting for commands to exfiltrate data and/or spread. hen, the analysis of the rootkit malware samples signed by valid Microsoft digital certificates, revealed similarities to the methods used by various cyberespionage threat groups that operated under an alleged state-controlled umbrella group. Even though the connection between the incidents presented in this article and state-sponsored activity is at the time of the report, circumstantial at best, it still raises the problem of nation states running operations, under the guise of cybercriminal activity, aimed at advancing their national interests in the cyber space. For each of these three operations the article highlighted, vigilance and good security practices are a key element for deterrence.

2. Cyber operations concepts

Cyberspace is defined, in the view of the US Army, “*as a human kind made global borderless domain, within the information environment, creating a strong interdependency between the networks of information technology infrastructures, existing data, and embedded processors and controllers*” (Leitzel & Hillebrand, 2022).

Cyberspace operations are complex, as defined by the US Air Force Doctrine (issued in February 2023), which encompasses complex intelligence and ordinary business operations of all actors involved in and/or running cyberspace, using existing capabilities (technological, knowledge base, personnel, Allies) to provide effects to support planned or ongoing operations in the physical realms (air, water, ground, space) (US Air Force, 2023; Theohary, 2022).

The Cyberspace operations are categorized into:

- *Offensive Cyberspace Operations* organized and authorized like any other operation in the physical realms with the same goal of projecting power through the use of force in and through cyberspace (Theohary, 2022);
- *Defensive Cyberspace Operations*, organized to protect, defend and deter own or allies' infrastructures or cyberspace (US Air Force, 2023).

The Cyber Operations are organized by special designed forces, usually embedded into Departments and / or Ministries of National Defense, with the approval of the national superior bodies (President, Parliament, Congress, Senate, etc.), under strict regulations following the international laws of conflict and rules of engagement. The specific steps and procedures, are described in and supported by national documents like strategies, laws, regulations and policies. (Leitzel & Hillebrand, 2022).

Some of these documents, are:

- National and /or Departmental Cyber Strategy;
- Laws, doctrines, regulations, procedures, Rules of engagement;
- Cyber Operations Mission Forces, chain of Command, Authorities in charge;
- Other Defense Components, support forces actors and coordination.

In this view, the Cyberspace Operations will create effects, and shall be executed independently, or integrated with other kinetic or non-kinetic operations organized and planned into other domains, to achieve primary, complementary, or enabling effects (US Air Force, 2023).

On top of the regular Cyber Operations, the military ones in cyberspace are organized into missions, which are more strictly regulated, and, through a combination of actions, create effects to achieve the established objectives.

However, any other actor, state-sponsored or not, such as hacktivist groups, underground groups or individuals, are organizing Cyber Operations with different aims such as self-/ group recognition, financial gain, testing new vulnerabilities and exploits, and supporting a state/ group ideology. Table 1 includes the main stages of a Cyber Operation, according to Brantly & Smeets (2020).

Table 1. Main Stages of a Cyber Operation (Brantly & Smeets, 2020)

No.	Stage	Short description
1.	Reconnaissance	Research, identification, and selection of targets
2.	Weaponization	Pairing exploit malware into a deliverable payload
3.	Delivery	Transmission of cyber-weapon to target
4.	Exploitation	Cyber-Weapon's code is triggered, exploiting vulnerable applications or systems
5.	Installation	The cyber-weapon installs a backdoor on a target's system allowing persistent access, lateral movement, etc.
6.	Command & Control	Outside server communicates with the cyber-weapons providing "hands-on keyboard access" inside the target's network
7.	Actions on the Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

2.1. Planning and assessment

Cyberspace operations may be planned and designed as part of a major operation and / or campaign, which could be, for example, a homeland, a crisis response, or a limited contingency operation (Theohary, 2022; Leitzel & Hillebrand, 2022).

Timing and tempo are the key considerations for the planning, use, and integration of cyberspace forces to ensure that the effects are available when needed. For a successful cyberspace operation planning, is necessary to understand that they may require weeks, months, or sometimes years of preparation prior to execution (US Air Force, 2023). One of the best examples, widely mentioned, is the STUXNET operation.

In terms of timing, the strategic understanding of the pursued objectives is the most important and takes most of the time, due to the necessity to project the objectives in the future. This long-term view allows the development of technologies, infrastructures, and capabilities that reflect the understanding, analysis, and production time required to provide better tools or capabilities when needed. From this point the strategic view, commercial development and intelligence gathering are the keys in covertly penetrating the adversaries' networks.

To account for potentially lengthened timelines, cyberspace operation planners should perfectly understand and estimate the capacity of own forces to support operations, by using actual, and the prognosed or under development future capabilities and targets, and by providing an accurate estimate of the time and effort required to deliver those capabilities (now, near and far future) (Leitzel & Hillebrand, 2022).

In terms of assessing Cyber Operations, usually, different types of assessments are used according to the level: tactical, operational and strategic.

Tactical assessments are generally conducted by the operational components, which focus on the effectiveness of the tactical operations against the adversary. Main key indicators are the immediate impact and/or secondary effects. Intelligence and any other useful information collected is taken into consideration, to determine if additional effects or targets could be brought about.

Operational-level assessment is supported by the analysts, inside the strategy and resources division, providing broader insights and recommendations on the types of effects created and if those effects met the supported objective. Main key indicators are the ends, ways, means and risks, which are input for the strategic level assessment phase, where the recommendations for strategy adjustments or future actions are made based on measured objectives, and complex indirect effects may be evaluated.

Strategic assessment takes place to determine if the overall objectives are met and if the operation's effectiveness towards achieving strategic or campaign objectives related the associated risk to friendly forces.

2.2. Major operations and campaigns

In addition to ongoing missions, cyberspace operations can be planned as part of larger operations and campaigns. Incorporating a strategy for cyberspace supremacy into formal planning gives commanders many additional options. Cyberspace operations can generate effects that historically required physical attacks instead, enabling new type of warfare forces to exploit enemy capabilities, alter information the enemy receives, and influence enemy's decisions (Leitzel & Hillebrand, 2022; US Air Force, 2023).

When operations are conducted at the operation theatre's level, the planning team should be integrated into a Joint Planning Team, being able to synchronize cyberspace operations with other operational and tactical components involved into the main operation. To be effective, cyberspace operations plans should include guidance, effects prediction, supported component schemes of manoeuvre, friendly capabilities, and likely adversary courses of action. The final plan will guide cyber operators against approved targets.

There are some phases when planning a Cyber Operation (Brantly & Smeets, 2020; Leitzel & Hillebrand, 2022), like:

- *Planning Initiation* - when the potential for a (non)military capability or operation is identified in support of national objectives or in response to a potential or an imminent crisis. This phase is initiated at the strategic level, and the key outputs are the estimated effects in support of a kinetic / military operation;
- *Mission Analysis* - development of the main actions, reasons and possible effects. This is the phase when intelligence is indeed regarding the adversaries` capabilities, targets, effects, situation templates, necessary capabilities to orchestrate, possible variants, and limitations, constraints and assumptions;
- *Course of Action Development* - a potential way, solution, and methods to accomplish the mission. Usually multiple courses are analysed, to identify the optimal or the proper one. In this phase, the risks, unforeseen events and mitigation possibilities are identified;
- *Course of Action Analysis*, Wargame simulation, Comparison, Approval - in this phase, all courses of actions are deeply analysed, highlighting pros and cons, preparing war game variants, with all resulted and new supportive information. The best Course of Action must be Ethical, and the most effective and efficient one possible;
- *Plan/Order Development* - all the variants and Courses of Action are expanded and transposed into detailed plans or Operation Orders. In this phase, many variables and uncertainty conditions are analysed, for building or revising the course of actions, and defining the necessary capabilities to achieve the aim or scope of a Cyber Operation.

3. Methods of cyberespionage

This study aims to showcase how information compromise, as an objective of malicious cyber operations, can be achieved through a multitude of attack vectors and methods. The authors will showcase two separate incidents in which sophisticated methods were utilized as a means towards data compromise. The paper also aims to emphasize how, while some of the actors behind sophisticated campaigns are documented and well-known, the majority of them are operating under the radar**.**

3.1. Colonial pipeline hack

Ransomware is currently the most dangerous and insidious cyber security threat facing all countries around the world. It is a category of malware designed to obtain payment of a ransom and the attacker reversibly renders the victim’s computer or information system inoperable. In theory, ransomware encrypts computer or system data using different cryptographic techniques, making the data impossible to view or use. Once the data is encrypted, the attacker then sends the victim an unencrypted message offering them the means to decrypt their data, in exchange for paying a ransom.

The year 2021 saw an increase in ransomware attacks against a mix of targets from global technology companies to international meat producers or oil pipelines. As a confirmation of these cyber threat events, on May 10, 2021, the FBI (FBI National Press Office, 2021) confirmed that a major US fuel company fell victim to a ransomware attack which led to its entire fuel distribution. Colonial Pipeline shut down its operations for several days while the problem was investigated, causing shortages across the East Coast of the United States and influencing oil prices globally. It was also confirmed by the authorized authorities that are behind the compromise of the Colonial Pipeline networks affected by ransomware, which used to deliver around 45% of the fuel along the Eastern Seaboard region, that it was the Darkside group.

On April 29, 2021, Darkside managed to gain entry into the Colonial Pipeline networks through a virtual private network (VPN) account which allowed employees to connect remotely to the company's computer network. At the time of the attack, that account was no longer in use, but it

could still be used to access Colonial Pipeline's network. That action has temporarily halted the company`s operations and affected some of its IT systems, according to the company's representatives (Colonial Pipeline, 2021).

Password security is a human-centric approach to cyber security that often becomes neglected and leads the people to a ransomware crisis, such the one that currently plagues the private and public sector alike. Keeping systems up to date and correctly configured may not stop a determined well-funded attacker or one with access to a password, but administrators are able to enforce adoption of proven cyber security practices like MFA and seamlessly roll out the solution to employees all while maintaining zero trust and zero knowledge.

Like most of the ransomware attacks, Darkside follows the double extortion trend, where the threat actors first exfiltrate sensitive information stored on a victim's systems before launching the encryption routine. Once the ransomware encrypts the target's data and issues the ransom demand for payment in exchange for the decryption key, the threat actors make the additional threat of publishing the exfiltrated data online should the target refuse to make the ransom payment with the capability to encrypt files, exfiltrate data, take control and command of the infected device, lateral movement and credential stealing with a huge impact on data loss - loss of important files, documents and other data upon encryption and financial loss - users are asked to pay in order to decrypt files that were affected or data exfiltration that could be sold on dark market (Figure 1).

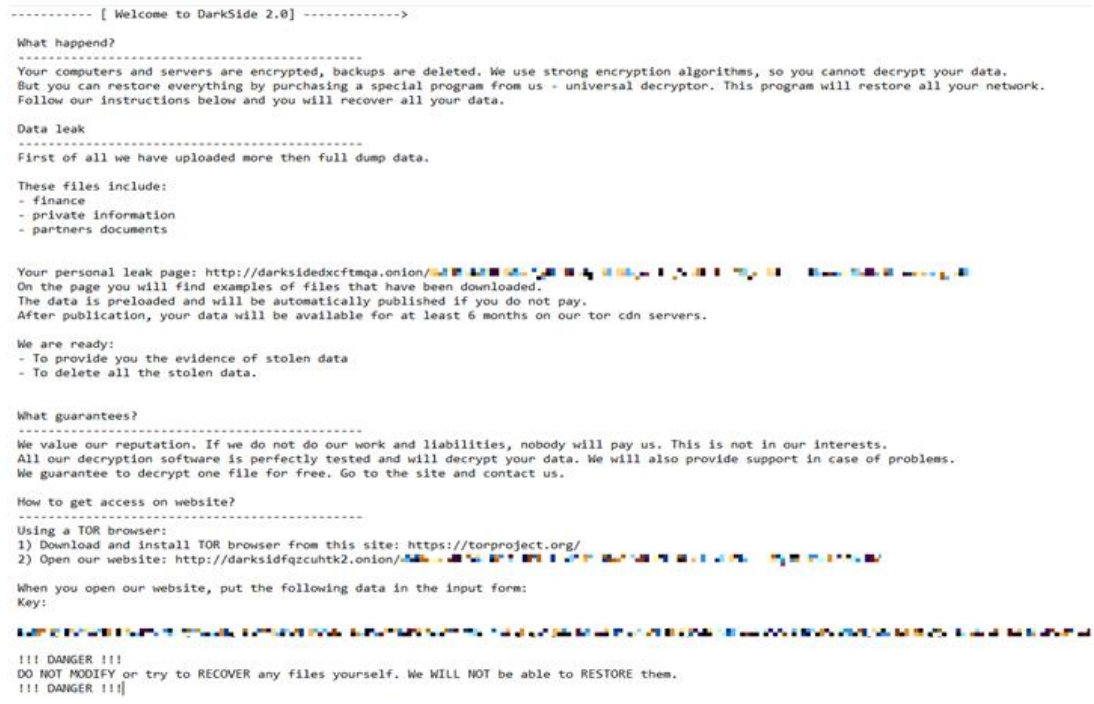

Figure 1. Darkside ransomware note (Malwarebytes Labs, 2021a)

3.2. Attack launched by DarkSide

DarkSide is a group that offers to customers their own version of malware based on a subscription to a Ransomware-as-a-Service (RaaS) product. According to IBM X-Force (Roddie, 2021), the malware, once deployed, steals data, encrypts systems using Salsa20 and RSA-1024 encryption protocols, and executes an encoded PowerShell command to delete volume shadow copies. According to nGuard, as a first step, attackers could have gained access in several different ways – by using TeamViewer, brute force password attacks, by phishing attacks, installing backdoors, SQL Injection against VPN networks and so on. Once inside the network, attackers passed to the second step and escalated privileges by utilizing Mimikatz, exploiting the Zerologon vulnerability, accessing and dumping Local Security Authority Subsystem Service (LSASS) or by another method. Once privileged access is gained, DarkSide uses PowerShell and Certutil (Figure 2) to deploy and execute the ransomware across the internal network (nGuard, 2021).

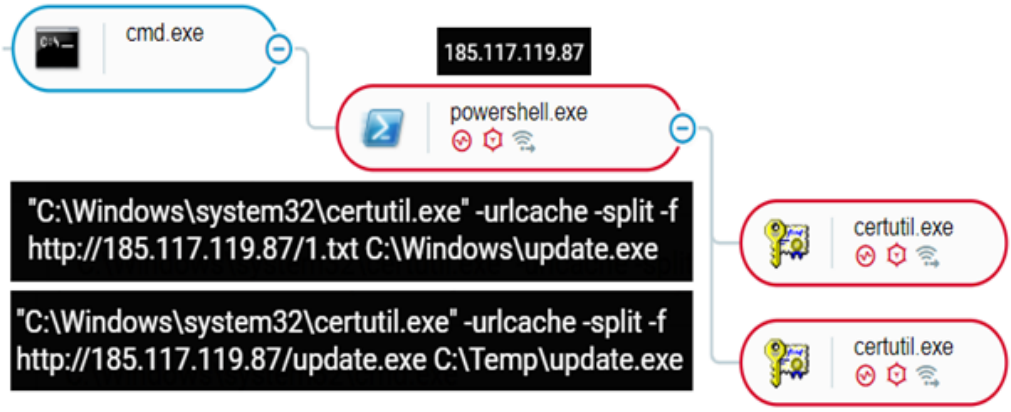

Figure 2. DarkSide ransomware binary using Certutil.exe (TrendMicro, 2021b)

Although the FBI, CISA and many others clearly recommend not paying a ransom, Colonial Pipeline is reported to have authorized a $4.4 million payment only to find out that restoring encrypted data this way was too slow. The US Department of Justice has been able to follow the money by reviewing the Bitcoin public ledger, which shows the value of reporting attacks to the proper authorities.

3.3. Timeline of Colonial Pipeline ransomware attack

According to Dixon & Nakashima (2022), in April 2019 there was the first evidence of Darkside tools being tested on the Internet and at the end of 2020, the service was already being widely used.

On May 6th, the group executed a ransomware campaign by stealing around 100 GB of data moments before locking computers with Darkside ransomware and demanding the payment of a ransom. On May 7th, the oil company decided to pay nearly $5 million to Russian hackers (Eaton & Volz, 2021). On May 8th, Colonial Pipeline notified the FBI with regard to their network disruption and along with the U.S. Government organizations (CISA, NSA, FBI, and the White House) decided to power off their current IT infrastructure and temporarily paused production on many of their pipelines. The company issued a press release regarding the attack through which they reported that their system was a victim of a ransomware attack and alerted law enforcement and engaged an external cyber security contractor to find the breach in their network. A second statement next day, May 9, 2021, by Colonial Pipeline, gave an update on its current investigation related to the ransomware attack and the current status of its pipeline operations. The Federal Bureau of Investigation (FBI) confirmed on May 10 that the DarkSide group was behind the attack that compromised the Colonial Pipeline networks.

The following day, on May 11, 2021, CSIA and FBI issued a cybersecurity advisory that described and detailed the DarkSide ransomware and associated risk mitigation strategies. At that time, the Colonial Pipeline's website was offline most of the day. On May 12, 2021 (5:00 p.m. ET) Colonial Pipeline company managed to restore the pipeline service although it took a few days to use it again at optimal capacity. At that time, more than 1,000 fuel stations had run out of gasoline amid "panic buying" in the Southeastern United States. Also, the company website was restored to its initial state in order to display information related to the attack.

On January 14, 2022, the White House confirmed that the people behind the Colonial Pipeline ransomware attack were arrested during the Russian REvil raid (Greig, 2022). The raid was carried out by authorized agencies in 25 different locations in the Darkside group's home country, which arrested 14 people allegedly involved with this organization. According to the media statements, many of those detained are now also being charged with illegal activities; several assets were confiscated, about $600,000 and €500,000, 20 luxury cars, and about 400 million rubles.

The personal computer equipment used by the attackers was seized and the police investigators gained access to several electronic crypto wallets. Further on, this paper presents

another incident which almost slipped under the radar that involved valid digital signatures to enhance the propagation of malware. The next subsection of this report will showcase the incident as well as similarities to well known state sponsored groups involved in cyberespionage and data theft.

3.4. The method used by DarkSide

The techniques used by the attackers in DarkSide Ransomware were very complex. A bug, a glitch, or a design vulnerability in the system may be forced as Initial access by using Exploiting thePublic-Facing Applications (e.g. RDP) (Praetorian &Weizman, 2018), Privilege Escalation through a local admin or user with higher privileges than needed, and Impair Defenses by disabling defensive mechanism (Smith & Kanthak, 2020). For this type of attack, DarkSide ransomware uses the well-known vulnerabilities CVE-2019-5544 and CVE-2020-3992, vulnerabilities with available patches, but attackers target organizations that are still using unpatched, outdated, or older versions of the software (Figure 3).

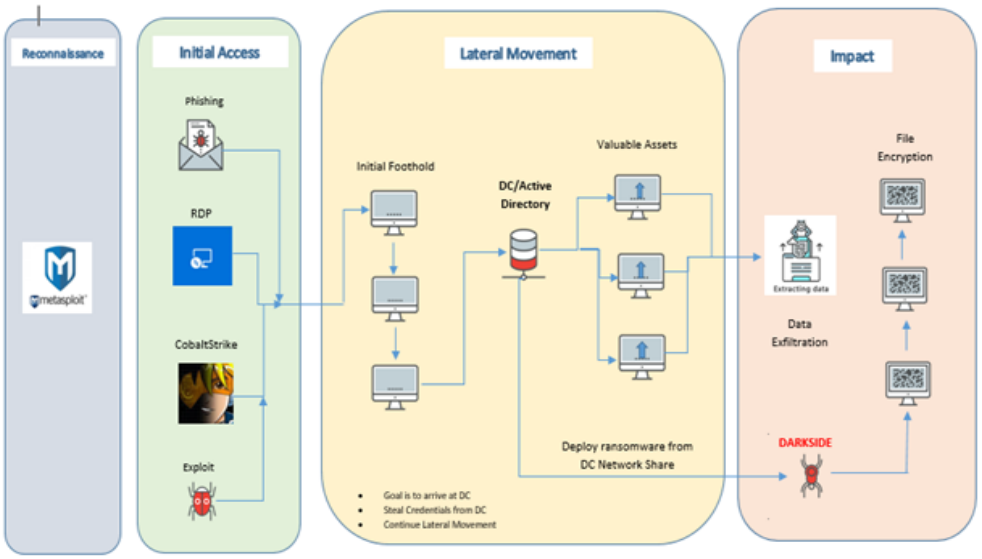

Figure 3. Darkside ransomware infection routine (TrendMicro, 2021a)

3.5. Short technical analysis of used steps

In the first phase of its deployment, DarkSide ransomware performs brute force attacks to exploit existing vulnerabilities in Windows environments caused by Remote Desktop Protocol (RDP) to gain initial access. Once they manage to gain intended access, DarkSide ransomware gathers information and validates prerequisites about the target environment and system language upon initial code execution. As default filter parameters are concerned, this type of ransomware is used to target English-speaking countries in particular by checking the default language used by the system.

Once access to the system is granted, a lateral movement technique is used for privilege escalation. The privilege escalation technique is used to get higher-level privileges over the infected system or network. Privilege escalation can occur through abuse of a breach or enforcement of a vulnerability in the operating system environment or application when there is a misconfiguration, bug, or outdated package. This kind of technique is usually used to elevate gained access to resources or services for a specific user that normally does not have the right privileges.

Since the attackers often require administrative privileges on the targeted computer, they check whether the user has administrative privileges, and if not, they attempt to gain elevated privileges by using a UAC (User Account Control) bypass technique on a process running with higher levels access is performed by using CMSTPLUA COM.

DarkSide Ransomware identifies data backup applications and exfiltrates data, which is followed by local file encryption as part of the ransomware delivery process. In most analyzed cases where computers have been infected with this type of ransomware, the attacker first tries to locate

every available type of volume shadow copies and delete those files from that particular asset so that their victims don't access files or restore them to the original version of this environment.

To be sure of their success, Darkside ransomware deletes the volume shadow copies via a PowerShell script that is executed.

To ensure that the security layer doesn't interfere with the delivery of the ransomware, security protection services are disabled using the last defense envasion technique like Impair Defenses to avoid and block possible detection of their tools and activities by changing the target environment. This can be done by terminating security software processes, adding, removing, or modifying registry keys, or creating exclusions for malware artifacts so tools don't start as soon as the system boots, or by using other methods of skipping the security tools, scan or report the information.

When it is run, the ransomware script generates a custom file based on an 8-digit Global Universally Unique Identifier (GUUID) machine that uses the API RtlComputeCRC32 algorithm, which is added to each encrypted file.

To prevent any sort of ransomware detection, the program uses encrypted APIs and strings and automatically posts a ransom note on the victim's computer after infection (Figure 1).

3.6. Information stealers as a means for data exfiltration

Before discussing the predominance of information thieves among other types of malware, a comprehensive definition must be given. An information stealer is a type of malicious software designed with the ultimate goal of stealing sensitive information from compromised systems. This sensitive information falls into the realm of private documents, login credentials such as usernames and passwords, browser cookie data, and cryptocurrency wallet information.

Given the versatility that this type of malware brings, it is not surprising that information theft has become one of the most popular and widely promoted types of malware in the cybercriminal underground. This popularity also made them very easy to purchase and deploy by various threat actors, ranging from sophisticated advanced persistent threat groups to less sophisticated threat actors motivated by financial gains.

Recent activity in the cybercriminal underground revealed various technology frameworks for information stealers such as the C++, C#, Rust and Python programming languages. In a usual campaign which employs information stealers as a tactic, a threat actor attaches the payload to either a phishing email or a pirated software. There are also instances in which information stealers are dropped only after initial access was obtained in the first stage of a compromise. An actor would then use the malware to further extract information from the compromised system.

Even though this type of malware is predominantly used by financially motivated threat actors, there are instances in which advanced persistent threat groups utilized information stealers. One such example is SideCopyAPT which has been active since at least 2019. As it was detailed in a report published by Malwarebytes on December 2, 2021 (Malwarebytes Labs, 2021b), the initial infection vector used by SideCopy APT included Microsoft Publisher documents and Trojanized applications. The same report also stated that the aforementioned threat actor also employed the use of an information stealer malware allegedly written in the C++ programming language dubbed AuTo stealer. This stealer was allegedly able to collect PowerPoint, Word, Excel and PDF documents as well as text files, images and database files which were subsequently uploaded to a command and control server.

In some situations, the attack infrastructure used by some information stealers can be uncovered through the use of the Shodan search engine for inter-connected devices and systems. An example that could fit the aforementioned category would be the Golang-based information stealer dubbed Titan Stealer. Several web servers that host command and control infrastructure for this specific stealer could be identified using the Shodan query: http.html:"Titan Stealer" (Figure 4). Running the aforementioned query revealed 13 results: six hosted in the Netherlands, five in the Russian Federation, one in Germany and one in Latvia.

Figure 4. Result of the Shodan query http.html: "Titan Stealer" (own source)

3.7. Microsoft signed rootkits

Rootkits used to be one of the most successful attack vectors employed in cybercrime operations. Threat actors leveraged the covert nature of this type of malware in order to secure a foothold into a compromised system's kernel, hidden from the regular checks performed by the operating system as well as from antivirus software. Even though this type of threat has been reduced by the fact that, since Windows Vista, every piece of code that ran in kernel mode was required to have a valid digital signature attached, there are still situations in which threat actors manage to fraudulently obtain this type of certificate, either by tricking the verification system put in place by the vendor or through the help of an insider, and thus manage to successfully inject malicious software in the kernel.

On June 17, 2021, a G Data security researcher, Karsten Hahn, claimed in a Twitter post (Hahn, 2021) that he identified a network filter rootkit with the SHA-256 hash 63d61549030fcf46ff1dc138122580b4364f0fe99e6b068bc6a3d6903656aff0, digitally signed by Microsoft, that was allegedly sending traffic to the China-based IP address hxxp://110.42.4.180:2081/u. The malware was allegedly being mostly distributed in the China gaming community. The netfilter rootkit file was identified as malicious by 45 vendors out of the 69 available on the VirusTotal malware intelligence platform at the time of the report (VirusTotal platform, owned by Google LLC, 2021). Based on the aforementioned URL, researchers were able to identify a dropper used for malware delivery as well as several other netfilter samples, with the oldest dating back to March 2021.

VirusTotal analysis of the C2 IP address 110.42.4.180 revealed that it was allegedly associated with the China-based company Ningbo ZhuoZhi Innovation Network Technology Co Ltd. In an initial blog release, BleepingComputer reported on claims made by another security researcher that Ningbo ZhuoZhi Innovation Network Technology appeared on a U.S. Department of Defense (DoD) list as a "Communist Chinese military" company. The claim was subsequently retracted as no such list was identified.

Microsoft admitted the incident and claimed that the malicious drivers were submitted for certification by a threat actor through the Windows Hardware Compatibility Program (WHCP). Even though the threat actor's account was allegedly suspended, it is not yet clear why the malicious drivers were approved in the first place (Sharma, 2021).

The aforementioned mode of operation displayed some similarities with that of the PassCV group which was notorious for leveraging stolen Authenticode signing certificates alongside different remote administration tools (RAT) and custom code.

PassCV is also associated with the Winnti Umbrella which consists of several APT groups including Winnti, Gref, PlayfullDragon, APT17, DeputyDog, Axiom, BARIUM, LEAD, Wicked Panda and ShadowPad, allegedly associated with the Chinese State intelligence apparatus.

According to researchers, threat actors under the Winnti Umbrella engaged in cyberespionage operations, leveraging phishing attack vectors in order to harvest credentials and deliver malware. According to Malpedia, the Winnti Umbrella targets companies and political organizations in the United States, China, Japan and South Korea.

4. Outputs of the analysis and proposed prevention methods

Before discussing the predominance of information thieves among other types of malware, a comprehensive definition must be given. An information stealer is a type of malicious software designed with the ultimate goal of stealing sensitive information from compromised systems. This sensitive information falls into the realm of private documents, login credentials such as usernames and passwords, browser cookie data, and cryptocurrency wallet information. Given the versatility that this type of malware brings, it is not surprising that information theft has become one of the most popular and widely promoted types of malware in the cybercriminal underground. This popularity also made them very easy to purchase and deploy by various threat actors, ranging from sophisticated advanced persistent threat groups to less sophisticated threat actors motivated by financial gains.

In summary, the analysis of information stealers as a means of data exfiltration, Microsoft-signed rootkits, and the Colonial Pipeline hack illustrates the severity and complexity of cyber threats targeting organizations and critical infrastructure. These incidents highlight the evolving nature of cyberattacks and the need for robust preventive measures. Information theft poses a significant risk to organizations as it can compromise sensitive data and have serious financial and reputational consequences. Preventative mechanisms to mitigate information theft include implementing strong endpoint security solutions, educating employees about phishing risks, and enforcing multi-factor authentication for access to critical systems.

The presence of Microsoft-signed rootkits indicates a worrying compromise in the software signing process. Strengthening security when signing software is crucial to prevent signing a malicious code. Improving software signing authentication and verification mechanisms and conducting regular security audits can help prevent the proliferation of Microsoft-signed rootkits.

The Colonial Pipeline Hack is a stark reminder of the potential impact of cyberattacks on critical infrastructure. Preventative measures against similar attacks include comprehensive incident response planning, regular vulnerability assessments, and secure supply chain management. Collaboration between public and private entities and the sharing of threat intelligence are critical to identifying emerging threats and developing proactive countermeasures.

To protect against this type of attack, organizations should adopt a holistic approach that combines technical safeguards, employee training, awareness programs, and effective incident response planning. Implementing robust endpoint security, network monitoring systems, and access controls can help detect and prevent information thieves. Regular security reviews, strong software signing practices, and supply chain security assessments can mitigate the risk of Microsoft-signed rootkits. In addition, organizations should invest in comprehensive incident response plans, employee training, and collaboration with industry peers and law enforcement agencies.

Ultimately, preventing and mitigating cyber threats requires a continuous and proactive approach. By staying informed about evolving attack techniques, implementing preventative measures, and fostering a culture of cybersecurity, organizations can improve their resilience and protect themselves from information stealers, rootkits, and other sophisticated cyberthreats.

Cyber espionage attacks like the Colonial Pipeline hack are sophisticated and targeted actions aimed at gaining unauthorized access to sensitive information or systems. These attacks can have serious consequences, including disrupting critical infrastructure and stealing valuable data. Understanding the methods used in cyberespionage attacks is crucial for developing effective prevention mechanisms. Below there are some common methods used in cyberespionage attacks and the suggested mechanisms to prevent them in the event of a Colonial Pipeline-style hack:

- *Phishing and spear phishing*: Attackers can use fraudulent emails, messages, or websites to trick employees into disclosing confidential information or providing

access to credentials. To prevent this, organizations should implement robust email security measures, educate employees about phishing risks, and use multi-factor authentication (MFA) to protect access to critical systems.

- *Malware and ransomware*: Attackers use malicious software to gain unauthorized access, steal information, or disrupt systems. Organizations should deploy strong endpoint protection solutions, regularly update software and security patches, and conduct regular vulnerability assessments to identify and mitigate potential vulnerabilities.
- *Supply chain attacks*: Attackers can compromise the software or hardware supply chain to deliver malware or gain unauthorized access to targeted systems. Organizations should implement robust vendor management practices, conduct thorough third-party security assessments, and ensure software and hardware integrity through secure development practices.
- *Insider threats*: Malicious insiders or compromised employees can grant access to sensitive systems or data. Organizations should enforce strong access controls, regularly review and monitor user rights, and implement robust employee training programs to increase awareness of the risks of insider threats.
- *Network exploitation*: Attackers can exploit vulnerabilities in network infrastructure to gain unauthorized access or conduct reconnaissance. Organizations should implement robust network security measures, including firewalls, intrusion detection and prevention systems, and regular network monitoring to detect and respond to suspicious activity.
- *Threat Intelligence and Information Sharing*: Organizations should establish mechanisms to collect threat intelligence from various sources, including government agencies, industry groups, and security vendors. Sharing this information can help identify emerging threats, improve situational awareness, and develop proactive defenses.
- *Incident Response and Recovery Planning*: Organizations should have comprehensive incident response plans in place to quickly detect, respond to, and recover from cyberespionage attacks. This includes regular testing of incident response procedures, data backups, and disaster recovery plans to minimize the impact of an attack.
- *Collaboration and partnerships*: Collaboration between government agencies, private organizations, and cybersecurity professionals is critical for sharing best practices, threat intelligence, and best expertise. Public-private partnerships can help establish standards, policies, and initiatives to prevent and mitigate cyberespionage attacks.

Preventing cyberespionage attacks requires a multi-layered approach that combines technical measures, employee awareness and training, and effective incident response planning. By remaining vigilant, implementing robust security measures, and fostering a culture of cybersecurity, organizations can reduce the risk of becoming a victim of such attacks and minimize their potential impact on critical infrastructure.

5. Conclusions

It can be difficult to know where to begin when it comes to protecting your business from cybercrime and cyberattacks. There's so much information out there that it can become overwhelming, especially when that information is conflicting. This study included the analysis of the three types of cyberespionage attacks based on publicly available information and, thus, the study is limited to such information.

As it can be seen, a coordinated and organized cyberspace operation is different from an isolated cyberattack, the use of an exploit on multiple targets, etc. For both categories there is a need for planning, collecting intelligence about targets, preparation for the attack, developing the tools, infrastructure, and means to hide the source, establishing the effects, and collecting the "losses" of the victim.

In a coordinated (military) or a state-sponsored cyber operation, the target is usually a very wide palette of services, institutions and infrastructures in order to create chaos and distract, to confuse, to kick down the adversaries' governmental services and produce direct effects for the population.

The more companies which expose how they were attacked, the more one can learn about attacker tactics, techniques, and procedures to build better defenses: Forewarned is Forearmed. A shared belief is that the people are stronger together. Information sharing is the only way to get ahead of the cybercriminals. They collaborate to make their attacks more successful, so the people should collaborate to make the defenses stronger.

The methods that had been used by the DarkSide group to attack the end organizations should trigger an alert signal for companies to review, update or upgrade any security assessment programs to ensure that any critical assessment activities such as Penetration Testing, Internal and External Penetration Testing, Social Engineering, Password Database Testing or Red Team Testing are counteracted in advance.

As possible future research concerning the aspects mentioned in this study, the updated versions of these attacks could be studied, as they appear in order to identify new techniques and tactics used by the cyberattackers.

Further on, an analysis of aggregated data about more attacks featuring a similar approach could be beneficial for extracting further prevention mechanisms.

Acknowledgment

All authors have read and agreed to the published version of the manuscript. The data used in this analysis is not public, but available upon request. The authors declare no conflict of interest. This research was founded through the project "CYMAROP – Centrul operational, educational si de cercetare in securitate cibernetica maritima si operare autonoma/Operational, educational and research center for maritime cybersecurity and autononous operation, SMIS Code 151003".

REFERENCES

Brantly, A. & Smeets, M. (2020) Military Operations in Cyberspace, *Virginia Tech (Virginia Polytechnic Institute and State University)*, https://www.researchgate.net/publication/343399173_Military_Operations_in_Cyberspace [Accessed 15th December 2022].

Dixon, R. & Nakashima, E. (January 14, 2022) *Russia arrests 14 alleged members of REvil ransomware gang, including hacker U.S. says conducted Colonial Pipeline attack, The Washington Post*, https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil/ [Accessed 17th February 2023].

Eaton, C. & Volz, D. (May 19, 2021) *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*. *Wall Street Journal*, https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636 [Accessed 15th January 2023].

FBI National Press Office. (2021) https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks [Accessed 02th January 2023].

Greig, J. (January 14, 2022) *White House confirms person behind Colonial Pipeline ransomware attack nabbed during Russian REvil raid*. https://www.zdnet.com/article/white-house-says-person-behind-colonial-pipeline-ransomware-attack-nabbed-during-russian-raid [Accessed 14th December 2022].

Hahn K. (2021), Tweet posted by Karsten Hahn on June 17, 2021, https://twitter.com/struppigel/status/1405483373280235520?lang=en [Accessed 28th November 2022].

Identity Theft Resource Center. (2022) *Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises*, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromise [Accessed 11th January 2023].

Leitzel, B. C. & Hillebrand, G. D. (September 28, 2022), *Strategic Cyberspace Operations Guide, United* States Army War College. https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf [Accessed 20th February 2023].

Malwarebytes Labs. (2021a) https://blog.malwarebytes.com/detections/ransom-darkside/ [Accessed 10th January 2023].

Malwarebytes Labs. (Dec. 2, 2021b) *SideCopy APT: Connecting lures to victims, payloads to infrastructure*. https://www.malwarebytes.com/blog/threat-intelligence/2021/12/sidecopy-apt-connecting-lures-to-victims-payloads-to-infrastructure [Accessed 19th November 2022].

Morgan, S. (2020) *Global Cybercrime Damages Predicted to Reach $6 Trillion Annually By 2021*. *Cybercrime Magazine, Cybersecurity Ventures*, https://cybersecurityventures.com/annual-cybercrime-report-2020/ [Accessed 04th December 2022].

Morgan, S. (December 30, 2021) *Cybersecurity Predictions and Statistics For 2021 To 2025*, https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/ [Accessed 04th December 2022].

nGuard. (May 27, 2021), *Colonial Pipeline - Timeline of Events*. https://www.nguard.com/colonial-pipeline-timeline-of-events/ [Accessed 12th December 2022].

Praetorian & Weizman, Y. (18 April, 2018) *Exploit Public-Facing Application*. https://attack.mitre.org/techniques/T1190/ [Accessed 12th December 2022].

Roddie, M. (May 10, 2021) IBM X-Force, *DarkSide Malware Profile*. https://exchange.xforce.ibmcloud.com/collection/06d0917405c36ca91f5db1fe0c01d1ad [Accessed 08th January 2023].

Sharma, A. (2021) *Microsoft admits to signing rootkit malware in supply-chain fiasco. Bleeping Computer*, https://www.bleepingcomputer.com/news/security/microsoft-admits-to-signing-rootkit-malware-in-supply-chain-fiasco/ [Accessed 25th January 2023].

Smith, C. & Kanthak, S. (30 Jan, 2022) Abuse Elevation Control Mechanism: Bypass User Account Control. https://attack.mitre.org/techniques/T1548/002/ [Accessed 12th February 2023].

TrendMicro. (2021a) Available solutions for Darkside Ransomware. https://success.trendmicro.com/dcx/s/solution/000286466 [Accessed 24th November 2022].

TrendMicro. (2021b) Cybereason vs. DarkSide Ransomware. https://www.cybereason.com/blog/research/cybereason-vs-darkside-ransomware [Accessed [Accessed 18th December 2022].

Theohary. C. A. (December 9, 2022) *Defense Primer: Cyberspace Operations*, Congressional Research Service (CRS), US Congress. https://crsreports.congress.gov/product/pdf/IF/IF10537 [Accessed 08th January 2023].

US Air Force. (February 1st, 2023) *Cyberspace Operations, US Air Force Doctrine Publication*. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf [Accessed 22th February 2023].

VirusTotal platform, owned by Google LLC. (20 Mar, 2023) The netfilter rootkit sample on the VirusTotal intelligence platform. https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromise [Accessed 24th February 2023].

Daniel Mihai LEU is a Cyber Threat Intelligence researcher focusing on understanding the complex dynamics of financially motivated threat actors and hacktivism. He earned a bachelor degree in Computer Science and Engineering from the University Politehnica of Bucharest, and is currently studying Risk Management in Cyber Security at the Maritime University of Constanta.

Daniel Mihai LEU este cercetător în Cyber Threat Intelligence, axându-se pe înțelegerea dinamicii complexe a actorilor din domeniul amenințărilor cibernetice, motivați financiar, precum și a amenințării hacktiviste. A obținut diploma de licență în Informatică și Inginerie, în cadrul Universității Politehnica din București, iar în prezent studiază Managementul Riscului în Securitate Cibernetică, la Universitatea Maritimă din Constanța.

Cătălin UDROIU operates in the IT field being a DevOps, Hybrid Cloud and Security Specialist, with a Master's degree in Business Information Systems, in the last 10 years he had worked on multi-level support for various clients around the world. With expertise in operating systems such as Windows and Linux and also in the Cloud Providers' category, he has assisted a lot of teams, and implemented different continuous integration and automation workflows for different organizations.

Cătălin UDROIU activează în domeniul IT, fiind specialist în DevOps, Hybrid Cloud și Securitate, deține o diplomă de master în Sisteme informaționale pentru afaceri, iar, în ultimii 10 ani, a lucrat pentru diverși clienți din întreaga lume, în structuri multi-level. Având experiență în sisteme de operare precum Windows și Linux și, de asemenea, în furnizarea serviciilor Cloud, el a supravegheat o mulțime de echipe și a implementat diferite fluxuri de lucru de integrare continuă și automatizare, pentru diferite organizații.

Gabriel Mărgărit RAICU is the Vice-Rector for Research and Innovation at the Maritime University of Constanta (CMU) and the Director of the Center for Excellence in Maritime Cyber Security (MarCySCoE). He has coordinated the development of the first maritime cyber security simulator within CMU since 2017, the year when the International Maritime Organization (IMO) took into account for the first time maritime cybersecurity risks. He is the initiator and coordinator of the annual BSCySeC#X conferences series, this year at its sixth edition together with the European Security and Defense College. He holds a degree in Maritime Engineering and a PhD in Cybernetics. He has contributions in the area of early warning systems for cyber security, in the area of critical maritime systems protection, as well as in the area of development of cyber security infrastructures and logistics. He is also the Vice-President of the Cyber Security Cluster of Excellence (CYSCOE), an organization that brings together companies, public authorities and academia in order to support the development and integration of cyber security at the level of the society as a whole.

Gabriel Mărgărit RAICU este Prorector Cercetare și Inovare, la Universitatea Maritimă din Constanța (CMU) și Director al Centrului de Excelență pentru Securitate Cibernetică Maritimă (MarCySCoE). Coordonează dezvoltarea primului simulator de securitate cibernetică maritimă în cadrul CMU, începând cu 2017, anul în care Organizația Maritimă Internațională (IMO) a luat în considerare, pentru prima data, riscurile de securitate cibernetică maritimă. Alături de Colegiul European de Securitate și Apărare, este inițiatorul și coordonatorul seriei anuale de conferințe BSCySeC#X, aflate, anul acesta, la a șasea ediție. Deține o diplomă în Inginerie Maritimă și un doctorat în Cibernetică. Are contribuții în domeniul sistemelor de avertizare timpurie pentru securitatea cibernetică, în domeniul protecției sistemelor maritime critice, precum și în zona

dezvoltării infrastructurilor și logisticii de securitate cibernetică. De asemenea, este Vicepreședintele al Cyber Security Cluster of Excellence (CYSCOE), o organizație ce reunește companii, autorități publice și mediul academic, pentru a sprijini dezvoltarea și integrarea securității cibernetice la nivelul societății în ansamblu.

Horațius Nicolae GÂRBAN is a military engineer with bachelor's degree in both, Mechanical and ICT degrees, and a MSc degree in Cyber Security and ICT, with over 20 years of experience in the Cyber Defence Sector, from the operational level to planning and strategic level. He was seconded between 2019 - 2022 to the European External Action Service, Belgium. With expertise in the field of Cyber Defence, Cyber Diplomacy and External Relations in the Cyber Domain, he is working, also, in the research sector, at the Maritime University of Constanta for the CYMAROP Project.

Horațius Nicolae GÂRBAN este inginer militar, având diplomă de licență atât în domeniul Mecanicii, cât și în cel al Tehnologiei informației și a comunicațiilor, precum și o diplomă de master în Securitate cibernetică și Tehnologia informației și a comunicațiilor, cu peste 20 de ani de experiență în Sectorul apărării cibernetice, de la nivel operational, până la nivel de planificare și strategic. A fost detașat la Serviciul European de Acțiune Externă, în Belgia, în perioada 2019 – 2022. Având experiență în domeniul apărării cibernetice, al diplomației cibernetice și al relațiilor externe în domeniul cibernetic, lucrează, de asemenea, în domeniul cercetării, la Universitatea Maritimă din Constanța, în cadrul proiectului CYMAROP.

Mircea Constantin ȘCHEAU is Ph.D. in Public Order and National Security focusing on economics and security, particularly cybercrime and financial transactions. He is the author or co-author of three volumes, one of which – *Cybercrime Regarding Financial Transfers* – received the "Victor Slăvescu" Prize awarded by the Romanian Academy, and of over fifty scientific articles related to management, law enforcement, critical infrastructures, information technology, artificial intelligence, defense, and cybersecurity. He has served as a lecturer in numerous international conferences, he is an Honorary Associate Researcher at the University of Craiova, the Maritime University of Constanța, and at Danubius University of Galati, and is a member, inter alia, of the European Research Institute at Babeș-Bolyai University.

Mircea Constantin ȘCHEAU este Doctor în Ordine Publică și Securitate Națională, axându-se pe economie și securitate, în special pe criminalitatea cibernetică și tranzacțiile financiare. Este autorul sau co-autorul a trei volume, unul dintre acestea – *Criminalitatea Informatica privind Transferurile Financiare* – primind Premiul „Victor Slăvescu", acordat de Academia Română, precum și a peste cincizeci de articole științifice despre management, aplicarea legii, infrastructure critice, tehnologia informației, inteligență artificială, apărare și securitate cibernetică. A fost lector în numeroase conferințe internaționale, este Cercetător Asociat Onorific la Universitatea din Craiova, Universitatea Maritimă din Constanța și la Universitatea Danubius din Galați și, printre altele, este membru al Institutului European de Cercetare, la Universitatea Babeș-Bolyai.