UKRAINIAN CATHOLIC UNIVERSITY

BACHELOR THESIS

Cyberattacks on Ukraine, classification and prediction attempt

Author:
Sofiia HALETSKA

Supervisor:
Oleksandr KHOLOSHA

A thesis submitted in fulfillment of the requirements for the degree of Bachelor of Science

in the

Department of Computer Sciences
Faculty of Applied Sciences

Lviv 2022

"Most people overestimate what they can do in a day, and underestimate what they can do in a month. We overestimate what we can do in a year, and underestimate what we can accomplish in a decade."

Matthew Kelly

Declaration of Authorship

I, Sofiia HALETSKA, declare that this thesis titled, "Cyberattacks on Ukraine, classification and prediction attempt" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

UKRAINIAN CATHOLIC UNIVERSITY

Faculty of Applied Sciences

Bachelor of Science

Cyberattacks on Ukraine, classification and prediction attempt

by Sofiia HALETSKA

Abstract

In many areas of our lives, learning from mistakes and preventing trouble is an essential part of the job, and the sphere of cybersecurity is no exception. A key tool in this process is the analysis of previously collected data. This work probably would not have been possible without the current events (active phase of the Russian-Ukrainian war). Because of this, I decided to focus this thesis on the attacks on Ukraine. In this paper, I explore possible ways to classify cyberattacks, approaches to analyzing such information, and make hypothesis about future trends in conducting cyberattacks using information available to the general public about attacks on Ukraine. In order to achieve set goals, I applied the knowledge I gained in courses called Cybersecurity, Data Visualization, and Prognostication.

GitHub repository[39].

Acknowledgements

First of all, I would like to express my gratitude to my family, who were helping and supporting me. My research would have been impossible without the aid and support of my supervisor, Oleksandr Kholosha, who helped me write this paper by giving helpful advice. He encouraged me and instilled faith in my own strength. Besides, I am profoundly grateful to my dear friends, who became my helping hand; I could always count on them. They motivated and inspired me to work hard on my achievements and never give up on set goals. And last but not least, I want to thank my faculty for the education and for not letting me relax, constantly challenging me to reach new heights.

Contents

List of Figures

List of Tables

List of Abbreviations

IT	**I**nformation **t**echnology
IP	**I**nternet **P**rotocol
DNS	**D**omain **N**ame **S**ystem
FTP	**F**ile **T**ransfer **P**rotocol
MITM	**M**an-**i**n-**t**he-**m**iddle
DOS	**D**enial **o**f **S**ervice
DDOS	**D**istributed **D**enial **o**f **S**ervice
HTTP	**H**yper**T**ext **T**ransfer **P**rotocol
URL	**U**niform **R**esource **L**ocators
TCP	**T**ransmission **C**ontrol **P**rotocol
UDP	**U**ser **D**atagram **P**rotocol
WMI	**W**indows **M**anagement **I**nstrumentation
MANET	**M**obile **A**dhoc **Net**works
WSN	**W**ireless **S**ensor **N**etworks
RREQ	**R**oute **Req**uest
RREP	**R**oute **Rep**ly
CVE	**C**ommon **V**ulnerabilities **E**xposure
CWE	**C**ommon **W**eakness **E**numeration
CVSS	**C**ommon **V**ulnerability **S**coring **S**ystem
CWSS	**C**ommon **W**eakness **S**coring **S**ystem
CERT	**C**omputer **E**mergency **R**esponse **T**eam
SCADA	**S**upervisory **C**ontrol **a**nd **D**ata **A**cquisition
RCE	**R**emote **C**ode **E**xecution
APT	**A**dvanced **P**ersistent **T**hreat
SSSCIP	**S**tate **S**ervice of **S**pecial **C**ommunications and **I**nformation **P**rotection
LPR	**L**uhansk **P**eople's **R**epublic
COI	**C**apability, **O**pportunity, and **I**ntent
ARIMA	**A**uto**r**egressive **I**ntegrated **M**oving **A**verage

Dedicated to everyone on the bright side.

Chapter 1

Introduction

1.1 Motivation

Although the issue of human rights in cyberspace is relatively new, I doubt anyone will object if I say, "Cybercrime violates human rights such as the right to privacy, the right to secrecy, and so on."

Accordingly, as a human being whose rights may be violated or simply as a person who, for some reason, has always seen herself as a fighter for justice - I have a desire to investigate cyberattacks as a tool used by cybercriminals in conducting cybercrimes. In addition, this work probably would not have been possible without the current events (active phase of the Russian-Ukrainian war). Because of this, I decided to focus my work on the attacks on Ukraine.

My main concern about this work is to make it possible, based on my research, to develop a reasonable, pragmatic strategy to protect Ukraine from cyberattacks in the nearest future.

1.2 Problem

In many areas of our lives, learning from mistakes and preventing trouble is an essential part of the job, and the sphere of cybersecurity is no exception. A key tool in this process is the analysis of previously collected data.

For instance, among jobs done by the IT security office in any organization, one can find Risk assessment, which stands for identifying, analyzing, and evaluating risk, with the intention to prevent potential future attacks or at least be able to face the consequence of it, reduce damage, simplify the process of restoring the system, etc.

In this thesis, I want to explore possible ways to classify cyberattacks, approaches to analyzing such information, and try to forecast using information available to the general public about attacks on Ukraine. In order to achieve set goals, I will apply the knowledge I gained in courses called Cybersecurity, Data Visualization, and Prognostication.

1.3 Goals

Summarizing stated above, I would like to highlight the following goals of my bachelor's paper:

- Conduct research on how cyberattacks are classified, determine the best methods for my particular case of study, and collect and organize data for my project.

- Analyze the collected data, make informative visualizations and draw conclusions.
- Using the collected data and pre-analysis - make a forecast, try to use different methods, and evaluate the results.

1.4 Thesis structure

In the following chapters of this work, one can read about:

Chapter 2 Background
Background information on the concepts, notions, and technologies used or mentioned in the thesis.

Chapter 3 Related Works
Previous work on this topic and studies that may in some way relate to this work. Comparative analysis.

Chapter 4 Dataset collection
Part on how I collected and classified information and created a dataset that I later used in this study.

Chapter 5 Analysis
Description of one of the main parts of this paper - the analysis of previously collected data.

Chapter 6 Forecast
Description of the work done during the attempt to predict possible future attacks.

Chapter 7 Summary
This section will tell about the achievements and conclusions drawn after the work was done.

Chapter 2

Background

2.1 Cyberattacks classification

Before collecting information and organizing it into a database, one should first explore how this information can be characterized and classified. Respectively, in this section, I want to write about found approaches to classifying cyberattacks.

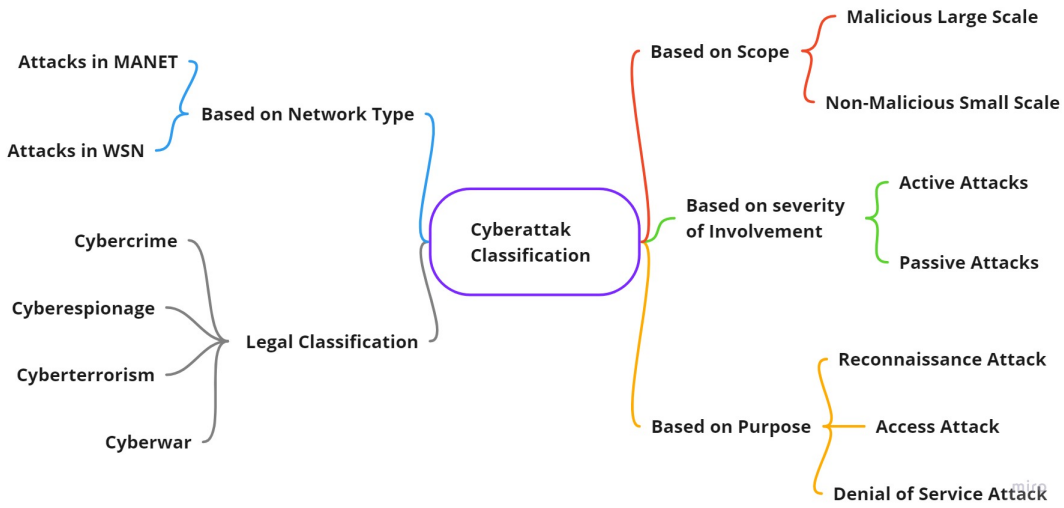


FIGURE 2.1: Attacks classification diagram

Many of the papers I reviewed on this topic referred to the classification made in *A Survey on Various Cyber Attacks and Their Classification* [41]. After reading it, I realized that even though it was written in 2011, it is still quite relevant and worthy of attention. For example, Fig. 2.1 is a diagram that I redrew from this work.

2.1.1 Based on Purpose

It is worth mentioning that the following attacks are only the most typical examples of the possible ones.

Reconnaissance Attack

The primary purpose of a reconnaissance attack is to find out the information needed by the hacker without being caught. These attacks can consist of the following:

Packet Sniffers
In performing such an attack, one needs to use a device to eavesdrop on data traffic

between computers and capture it. Later, after saving, this information will be analyzed.

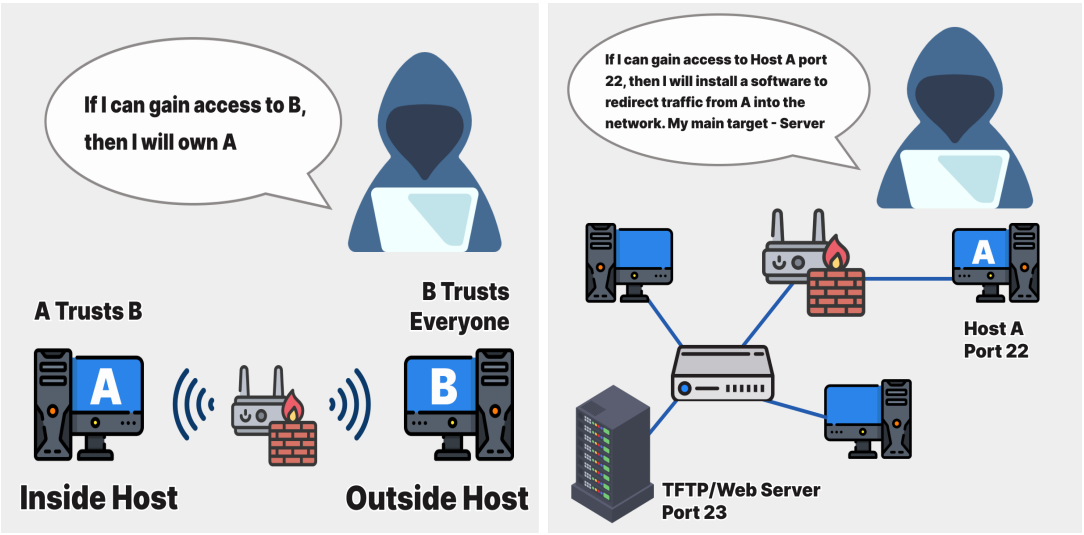
Scanning the Port
An attacker sends a series of messages to break into a computer and discover which computer services are related to a specific port number.

Sweeping the Ping
During this attack, hackers use the scanning method to determine the range of IP addresses mapped to live hosts.

Queries Regarding Internet Information
Exploiting DNS Queries, one can learn who owns a domain and what addresses have been assigned to that domain.

Access Attack

In this type of attack, the aim is to gain access to a device. The unauthorized intruder, who does not have the authority to access, exploits loopholes, also known in cybersecurity as vulnerabilities, in any authentication services, FTP (File Transfer Protocol) services, and web services to get to web accounts, confidential databases, and other sensitive information [41]. Access attacks consist of the following:



(A) Trust Exploitation Attack (B) Port Redirection Attack

FIGURE 2.2: Trust Port Exploitation Attacks

Utilization of Trust Port
An attacker compromises a trusted host by using it to stage attacks on a trusted host. If a host in a network of a company is protected by a firewall (inside host) but is accessible to a trusted host outside the firewall (outside host), the inside host can be attacked through the trusted outside host [40]. (see Fig. 2.2a)

Port Redirection
A compromised trusted host is used to access other hosts protected by a network firewall.The attacker could install software to redirect traffic from the outside host directly to the inside host [48]. (see Fig. 2.2b)

Attacks on Secret Code

It is also called a Dictionary attack. A dictionary file is passed through a user's account or database to crack a password. If any of the words are matched with the password, the user hacking the password gets access to the specific system or service [21].

Man-in-the-middle Attacks

MITM attack is implemented by intruders that manage to position themselves between two legitimate hosts. The attacker may allow the regular communication between hosts to occur but manipulates the conversation between the two. (see Fig. 2.3)

1. When a victim requests a webpage, the victim's host requests the attacker's host.
2. The attacker's host receives the request and fetches the actual page from the legitimate website.
3. The attacker can alter the legitimate webpage and apply any transformations to the data they want to make.
4. The attacker forwards the requested page to the victim [46].

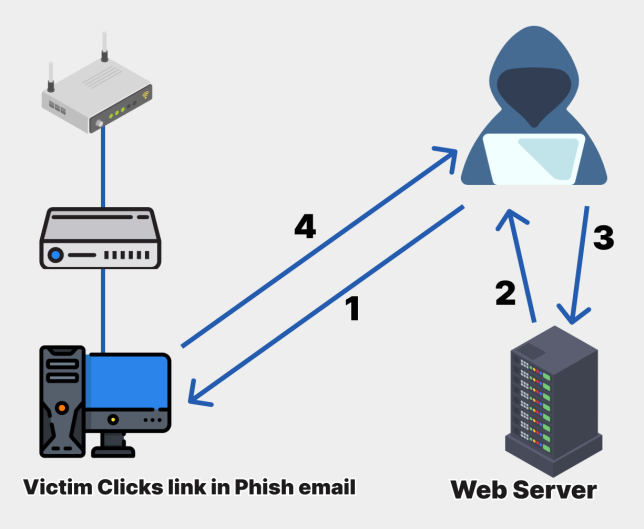


FIGURE 2.3: Man-in-the-middle Attack

Social Engineering and Phishing

Social engineering is a trick used by hackers who exploit the human factor to get what they want. The purpose of any such manipulation is to make a person make a mistake and, even without realizing it, give the attacker what he asks. There are a lot of social engineering techniques, but one of the most famous and common is Phishing.

During Phishing attacks, an attacker sends fraudulent communications that appear to come from a reputable source. It is usually performed through email. The goal is to steal sensitive data like credit card and login information or install malware on the victim's machine [47].

Denial of Service Attack

These types of attacks are initiated by a whole group of attackers or simply an individual to disturb Internet protocols (IPs Packets) to stop users from effectively accessing the internet.
Denial of service attacks are classified into the following three major types:

Resource Degradation
These are the attacks due to which the target (the resource or device) stops working simultaneously and effectively.

Networks Deluge
Attacks that attempt to submerge network devices' bandwidth tolerance, such as Routers, Modems, etc.

Scathing
Destroying or Disturbing the ability of a device to perform operations accurately and effectively, such as power interruptions, etc., are termed as destructive or scathing attacks.

In the end, the aim of an attacker is basically to disrupt a computer network or smash a computer system by making interferences with the information, to deny the service to the users, for proper development of the economy. Prevention from these attacks is crucial as they can harm various sectors of a state or country [21].

There are also some exciting examples of DoS attacks, which I would like to describe below. They differ significantly from each other in the way of conducting.

One of them is a **Smurf** [45] attack in which an attacker attempts to flood a targeted server with Internet Control Message Protocol (ICMP) packets. By making requests with the spoofed IP address of the targeted device to one or more computer networks, the computer networks then respond to the targeted server, amplifying the initial attack traffic and potentially overwhelming the target, rendering it inaccessible.

The next one is **DDOS** which simply stands for distributed denial-of-service.It differs from the DoS attacks by the number of devices involved in the attack. For DDOS, one needs more than one device or can use one device with a botnet to perform a more powerful and efficient attack.

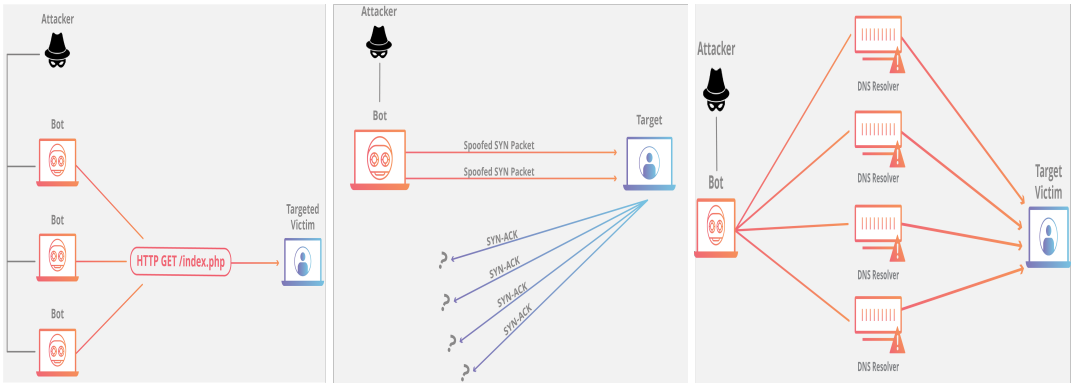
There are also three different most common types of DDOS attacks:

HTTP flood [44] is similar to pressing refresh in a web browser over and over on many different computers at once – large numbers of HTTP requests flood the server, resulting in denial-of-service.

This type of attack ranges from simple to complex. Simpler implementations may access one URL with the same range of attacking IP addresses, referrers, and user agents. Complex versions may use a large number of attacking IP addresses and target random URLs using random referrers and user agents.(see Fig. 2.4a)

A **SYN Flood** [44] is analogous to a worker in a supply room receiving requests from the front of the store.

The worker receives a request, goes and gets the package, and waits for confirmation before bringing the package out front. The worker then gets many more



(A) HTTP flood (B) SYN flood (C) DNS Amplification

FIGURE 2.4: Different types of DDOS Attacks [44]

package requests without confirmation until they cannot carry any more packages, become overwhelmed, and requests start going unanswered.

This attack exploits the TCP handshake — the sequence of communications by which two computers initiate a network connection — by sending a target a large number of TCP "Initial Connection Request" SYN packets with spoofed source IP addresses.

The target machine responds to each connection request and then waits for the final step in the handshake, which never occurs, exhausting the target's resources. (see Fig. 2.4b)

A **DNS amplification** [19] can be broken down into four steps:

1. The attacker uses a compromised endpoint to send UDP packets with spoofed IP addresses to a DNS recursor. The spoofed address on the packets points to the actual IP address of the victim.
2. Each UDP packet requests a DNS resolver, often passing an argument such as "ANY" to receive an enormous response.
3. After receiving the requests, the DNS resolver, which tries to be helpful by responding, sends an extensive response to the spoofed IP address.
4. The IP address of the target receives the response, and the surrounding network infrastructure becomes overwhelmed with the deluge of traffic, resulting in a denial-of-service.

While a few requests are not enough to take down network infrastructure, when this sequence is multiplied across multiple requests, and DNS resolvers, the amplification of data the target receives can be substantial. Explore more technical details on reflection attacks. (see Fig. 2.4c)

2.1.2 Legal Classification

Cybercrime

Canadian law enforcement agencies have increasingly accepted the working definition: "a criminal offense involving a computer as the object of the crime, or the tool used to commit a material component of the offense." The cybercrime target

is to make the system a crime tool and the computer as an incidental to a crime. Computer crimes happen because of their anonymity, the capacity of the computer storage, weakness in an operating system, lacking user awareness [41].

Cyberespionage

Using the cracking techniques and malicious software, including Trojan horses and spyware, it is the act or practice of obtaining secret information of individuals, groups, and governments to gain benefits of their own using illegal abuse methods to obtain information without the permission of the holder. It is otherwise known as cyber spying. It may wholly be perpetrated online from computer desks of professionals on bases in faraway countries. It may involve infiltration at home by computer-trained conventional spies and moles or, in other cases, may be the criminal handiwork of amateur malicious hackers and software programmers [41].

Cyberterrorism

Cyberterrorism is the use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm in order to achieve political or ideological gains through threat or intimidation. Acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet by means of tools such as computer viruses, computer worms, phishing, malicious software, hardware methods, and programming scripts can all be forms of internet terrorism [14].

Cyberwar

Cyberwarfare differs from cyberterrorism as it is an organized effort by a nation-state to conduct operations in cyberspace against foreign nations. Included in this category is the Internet's use for intelligence gathering purposes. Cyberwar has become the little-understood adjunct to cyberspace that has the potential for the greatest impact on the Internet. An all-out assault by nation-states against each other would leave private citizens in its wake. The nations with the most technology integration in their citizens' lives have the most at stake [30].

The consequences of cyber warfare can include the following:

- The overthrow of the system of government or the catastrophic threat to national security;
- Simultaneous initiation of physical warfare or groundwork and facilitating the start of physical warfare soon;
- Catastrophic destruction or damage to the country's image at the international level;
- Catastrophic destruction or damage to the political and economic relations of the country;
- Extensive human casualties or danger to public health and safety;
- Internal chaos;
- Widespread disruption in the administration of the country;
- Destroying public confidence or religious, national, and ethnic beliefs;
- Severe damage to the national economy;
- Extensive destruction or disruption of the performance of national cyber assets.

In addition, five scenarios can be considered for cyber warfare:

(1) Government-sponsored cyber espionage to gather information to plan future cyberattacks
(2) A cyberattack aimed at laying the groundwork for any unrest and popular uprising
(3) A cyberattack aimed at disabling equipment and facilitating physical aggression
(4) Cyberattack as a complement to physical aggression
(5) Cyberattack with the aim of widespread destruction or disruption as the ultimate goal (cyberwarfare) [24].

2.1.3 Based on severity of Involvement

Active vs. Passive Attack

An active attack attempts to alter system resources or affect their operation. A passive attack attempts to learn or make use of information from the system but does not affect system resources [31].

Active Attacks	**Passive Attacks**
Messages are being modified by hackers.	Content of Messages is observed by the hackers.
System gets heavily destructed.	The system does not incur any damage.
System availability and integrity of the resources are damaged.	Confidentiality of data is breached.
Attackers can change the system resources.	Attackers cannot change the system resources.
Very difficult to prevent this attack from entering the network.	Preventing the attack is comparably easy.
The focus is on detection.	The focus is on prevention.
The information about the attack gets notified to the victim.	Notification to the victim is not sent regarding the attack.
Influence the services rendered to the specific system.	Acquire the information of the system.
Information is invoked through passive attacks.	Collection of confidential information.
Examples of an attack: Hijacking session, Impersonating the user.	Examples of an attack: Tapping, Decryption of encrypted messages.

TABLE 2.1: Difference between Active and Passive Attack [32]

2.1.4 Based on Scope

Malicious Large Scale

The term malicious means "with deliberate intent to cause harm". A malicious large-scale attack is carried out by an individual or a group for personal gain or to cause disruption and chaos. Such attacks are large-scale, involving thousands of systems, and cause a worldwide crash of systems with a loss of a huge volume of data and credibility of the company [41].

In addition, it is worth defining the term Malware and its various types.

Malware - a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can do the following:

- Installs malware or additional harmful software
- Covertly obtains information by transmitting data from the hard drive (spyware)
- Disrupts certain components and renders the system inoperable [43]

Malware can be divided into such categories:

Adware

Adware serves unwanted or malicious advertising. While relatively harmless, it can be irritating as "spammy" ads continually pop up while working, significantly hampering your computer's performance. In addition, these ads may lead users to download more harmful types of malware inadvertently.

Fileless Malware

Unlike traditional malware, which uses executable files to infect devices, fileless malware does not directly impact files or the file system. Instead, this type of malware uses non-file objects like Microsoft Office macros, PowerShell, WMI, and other system tools. A notable example of a fileless malware attack was Operation Cobalt Kitty. The OceanLotus Group infiltrated several corporations and conducted nearly six months of stealthy operations before being detected.

Ransomware

Ransomware attacks encrypt a device's data and hold it for ransom until the hacker is paid to release it. If the ransom is not paid by a deadline, the hacker will threaten to delete the data—or possibly expose it. Paying up may not help; often, victims lose their data even if they pay the fee. Ransomware attacks are some of the most newsworthy malware types due to their impact on hospitals, telecommunications firms, railway networks, and governmental offices. A prime example is the WannaCry attack that locked up hundreds of thousands of devices across more than 150 countries.

Spyware

Cybercriminals use spyware to monitor the activities of users. By logging the keystrokes a user inputs throughout the day, the malware can provide access to user names, passwords, and personal data [2].

Virus

A computer virus is represented by a self-replicating program that attaches itself to a program or file. It can spread from one computer to another, leaving infections as it travels. Almost all viruses are attached to an executable file; the virus may exist on the computer, but it cannot infect the computer unless someone runs or opens the malicious program. A virus cannot be spread without running an infected program without human activities.

Worm

A worm is considered to be a sub-class of a virus. It spreads from computer to computer and has the capability to travel without any help from a person. It travels with the file or information on the system. It self-replicates on the system and sends thousands of its copies to create a huge devastating effect.

Trojans

The Trojan appears to be a useful program but damages the system when installed on the computer. The mastermind behind the Trojan can control the infected system without the owner's knowledge. Trojans can change desktop, add silly active desktop icons, deleting files, and destroying information on the system. Trojans can also create a backdoor on the computer. Unlike viruses and worms, Trojans do not reproduce by infecting other files, nor do they self-replicate [25].

Non-Malicious Small Scale

These are typically accidental attacks or damage due to mishandling or operational mistakes done by a poorly trained individual, which may cause a minor loss of data or system crashes. In such cases, only few systems in the network are compromised, and data is usually recoverable. It is associated with little cost [41].

2.1.5 Based on Network Type

Attacks in MANET

***MANET* (Mobile Adhoc Networks)** - is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre-existing infrastructure, such as routers in wired networks or access points in wireless networks. Instead, each node participates in routing by forwarding data to other nodes, so the determination of which nodes forward data is made dynamically based on network connectivity and the routing algorithm in use [49].

One can carry out such attacks through MANET:

Byzantine Attack

It is an attack exclusively on Mobile Adhoc networks where an authentication device or set of devices that usually provide security is compromised due to the leaking of information so that a legitimate device cannot be distinguished from a hostile user.

The Black Hole Attack

Black Hole Attacks mean that all the information transferred will be disappeared by directing all the network traffic to a particular node as though that node does not exist. Here the node is called a black hole. The RREQ (Route Request) and RREP (Route Reply) will be used to form this attack.

Flood Rushing Attack

There will be a race between legitimate floods and the adversaries of that flood. It happens when there is propagation. Though the authentication techniques used will fail to establish an adversarial free route.

Byzantine Wormhole Attacks

The capabilities of compromising more than one node, and there will be an involvement of an attack in the cooperation for the nodes, known as Byzantine Wormhole Attacks. This attack will be created when adversaries tunnel packets between them to create a shortcut among them in the networks. This attack is powerful, but at least two nodes must be compromised.

Byzantine Overlay Network Wormhole Attacks

This attack is otherwise known as a super-wormhole attack. This attack is most vigorous among other attacks, and it is a very efficient attack. By using this attack, one can create enormous traffic in the routing protocols, leading to the disruption of the networks[41].

Attacks in WSN

***WSN* (Wireless Sensor Networks)** - is an infrastructure-less wireless network deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions.

Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station, which acts as a processing unit in the WSN System. Base Station in a WSN System is connected through the Internet to share data [50].

Attacks through WSN can be classified into the following two major types:

Cryptography and non-cryptography related attacks

- Pseudorandom number attack
- Digital signature Attack
- Hash collision attack.

Attacks based on the Network Layers

- Application layer
  - Repudiation
  - Data corruption
- Transport layer
  - Session hijacking
  - SYN flooding
- Network layer
  - Wormhole
  - Blackhole
  - Byzantine
  - Flooding
  - Resource consumption
  - Location disclosure
- Data link layer
  - Traffic analysis
  - Monitoring
  - Disruption of MAC

- Physical layer
  - Jamming
  - Interceptions
  - Eavesdropping
- Multi-layer
  - DOS
  - Impersonation attacks
  - MITM

The table 2.2 summarizes all the above and presents information in a conveniently compact form with a description and examples of each type of attack.

Type of Attack	Description	Examples
Reconnaissance Attacks	Type of attack which involves unauthorized detection system mapping and services to steal data	a) Packet sniffers b) Port scanning c) Ping sweeps d) DNS Queries
Access Attacks	An attack where intruder gains access to a device to which he has no right for access	a) Port trust utilization b) Port redirection c) Dictionary attacks d) Man-in-the-middle attacks e) Social engineering attacks and Phising
Denial of Service	Intrusion into a system by disabling the network with the intent to deny service to authorized users	a) Smurf b) SYN Flood c) DNS attacks d) DDos
Cybercrime	The use of computers and the internet to exploit users for materialistic gain	a) Identity theft b) Credit card fraud
Cyberespionage	The act of using the internet to spy on others for gaining benefit	a) Tracking cookies b) RAT controllable
Cyberterrorism	The use of cyber space for creating large scale disruption and destruction of life and property	a) Crashing the power grids by al-Qaeda via a network b) Poisoning of the water supply
Cyberwar	The act of a nation with the intention of disruption of another nations network to gain tactical and military advantages	a) Russia's war on Estonia (2007) b) Russia's war on Georgia (2008)
Active Attacks	An attack with data transmission to all parties thereby acting as a liaison enabling severe compromise	a) Masquerade b) Reply c) Modification of message
Passive Attacks	An attack which is primarily eaves dropping without meddling with the database	a) Traffic analysis b) Release of message contents
Malicious Attacks	An attack with a deliberate intent to cause harm resulting in large scale disruption	a) Sasser Attack
Non Malicious Attacks	Accidental attack due to mishandling or operational mistakes with minor loss of data	a) Registry corruption b) Accidental erasing of hard disk
Attacks in MANET	Attacks which aims to slow or stop the flow of information between the nodes	a) Byzantine Attacks b) Black Hole Attack c) Flood Rushing Attack d) Byzantine Wormhole Attack
Attacks on WSN	An attack which prevents the sensors from detecting and transmitting information through the network	a) Application Layer Attacks b) Transport Layer Attacks c) Network Layer Attacks d) Multi Layer Attacks

TABLE 2.2: Different types of attacks [41]

2.1.6 Others

CVE, CWE, CVSS, CWSS

CVE and CVSS

***CVE* (Common Vulnerabilities Exposure)** - a dictionary of publicly known security vulnerabilities and exposures. It provides a baseline for evaluating the coverage of an organization's security tools and makes it easier to share vulnerability data across different databases and tools. Various security tools can now "talk" to each other using a common language [5].

***CVSS* (Common Vulnerabilities Scoring System)** - is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of a vulnerability.

CVSS comprises three metric groups: Base, Temporal, and Environmental, each consisting of a set of metrics. These metric groups are described as follows:

- **Base:** represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.
- **Temporal:** represents the characteristics of a vulnerability that change over time but not among user environments.
- **Environmental:** represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

The CVSS base group aims to define and communicate the fundamental characteristics of a vulnerability. This objective approach to characterizing vulnerabilities provides users with a clear and intuitive representation of a vulnerability. Users can then invoke the temporal and environmental groups to provide contextual information that more accurately reflects the risk to their unique environment. This allows them to make more informed decisions when mitigating risks posed by the vulnerabilities [6].

CWE and CWSS

***CWE* (Common Weaknesses Enumeration)** - is a community-developed list of standard software and hardware weakness types that have security ramifications. "Weaknesses" are flaws, faults, bugs, or other errors in software or hardware implementation, code, design, or architecture that, if left unaddressed, could result in systems, networks, or hardware being vulnerable to attack. The CWE List and associated classification taxonomy serve as a language that can be used to identify and describe these weaknesses in terms of CWEs.

The main goal of CWE is to stop vulnerabilities at the source by educating software and hardware architects, designers, programmers, and acquirers on how to eliminate the most common mistakes before products are delivered. Ultimately, the use of CWE helps prevent the kinds of security vulnerabilities that have plagued the software and hardware industries and put enterprises at risk [3].

***CWSS* (Common Weaknesses Scoring System)** - provides a mechanism for prioritizing software weaknesses in a consistent, flexible, open manner. It is a collaborative, community-based effort addressing the needs of its stakeholders across government, academia, and industry.

CWSS is organized into three metric groups: Base Finding, Attack Surface, and Environmental. Each group contains multiple metrics - also known as factors - used to compute a CWSS score for a weakness. (see Fig. 2.5)

- **Base Finding metric group:** captures the inherent risk of the weakness, confidence in the accuracy of the finding, and strength of controls.
- **Attack Surface metric group:** the barriers that an attacker must overcome in order to exploit the weakness.
- **Environmental metric group:** characteristics of the weakness specific to a particular environment or operational context.

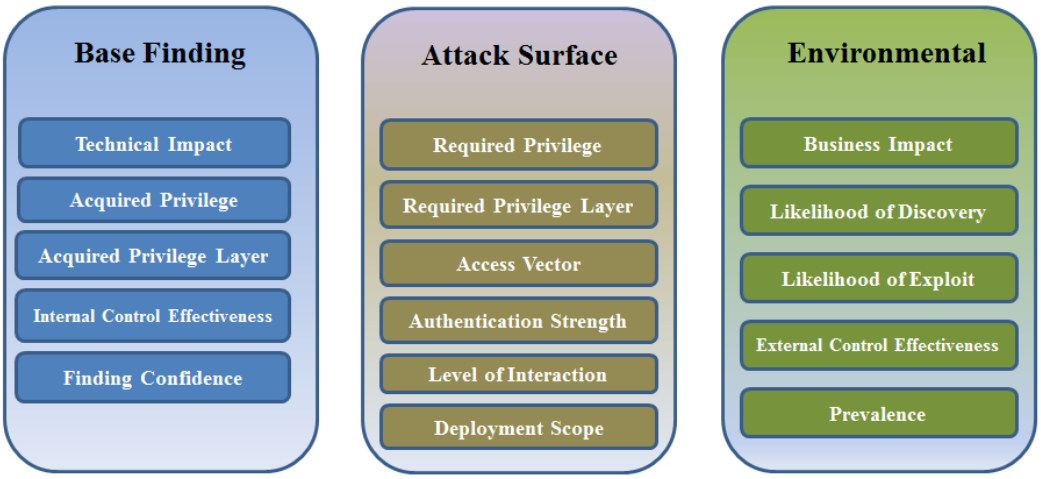


FIGURE 2.5: CWSS Metric Groups

Each factor in the Base Finding metric group is assigned a value. These values are converted to associated weights, and a Base Finding subscore is calculated. The Base Finding subscore can range between 0 and 100. The same method is applied to the Attack Surface and Environmental metric group; their subscores can range between 0 and 1. Finally, the three subscores are multiplied together, which produces a CWSS score between 0 and 100 [29].

Game Theoretic Weighted Metrics Approach

When I was looking for information on the classification of cyberattacks, I came across a fascinating work called *Cyber Attack Classification using Game Theoretic Weighted Metrics Approach* [25].

After reading it, I learned that sometimes there is a problem determining which category this or that attack belongs to because nowadays, more complex attacks are carried out at the same time using techniques of several different types. Therefore, the authors of this paper propose a game theoretic weighted metrics approach to solve this problem.

CERT-UA classification

Code xx	**Category of incident**	**Code xx**	**Type of incident**	**Description**
01	Abusive content	01	Spam	Send unsolicited messages or a large number of messages
02	Malicious code	01	Malware infection	Malicious software was found in the system
		02	Malware distribution	Malware distribution, for example, by sending emails containing attachments with malicious software or a link to download it
		03	Command & Control (C2)	A system is used as a control and management point for a botnet and/or serves as a collection point for information stolen by botnets
		04	Malicious connection	Attempts to connect from/to IP/URL - an address associated with known malicious software, such as C2C or the distribution resource of components related to the activity of a particular botnet
03	Information Gathering	01	Scanning	Collect information about systems or networks
		02	Sniffing	Unauthorized interception (logical or physical) and analysis of network traffic. Unauthorized monitoring and reading of network traffic

		03	Phishing	Attempt to collect information about a user or system using social engineering techniques (mass emailing is aimed at data collection, may contain links to phishing sites)
04	Intrusion Attempts	01	Vulnerability exploitation attempt	An intrusion attempt using a vulnerability in a system, component, or network
		02	Login attempts	Attempt to login to authentication/access services or mechanisms. An unsuccessful attempt to select authentication data or use previously compromised data that is no longer relevant
05	Intrusion	01	Account compromise	An intrusion attempt using a vulnerability in a system, component, or network
		02	System compromise	Actual intrusion into a system, component, or network by compromising a user or administrator account
06	Availability	01	DoS/DDoS	Influence on the normal functioning of the system or service that is achieved by sending requests from one or more sources to the target resource to oversaturate the bandwidth or system resources

		02	Sabotage	Actions (intentional or unintentional) aimed at damaging the system, interrupting processes, changing or deleting information, etc.
		03	Outage, no malice	Failure of the system or its component without malicious interference
07	Information Content Security	01	Unauthorised access to information	Unauthorized access to information. Unauthorized exchange of a specific set of information
		02	Unauthorised modification of information	Unauthorized change or deletion of a particular set of information
08	Fraud	01	Fraudulent site	Creating phishing sites to collect authentication or other user data. Using the resources of the institution for purposes other than those intended
09	Vulnerable	01	Vulnerability	Presence in the system or its components of known vulnerabilities open for exploitation
		02	Misconfiguration	Disadvantages in settings that can be used by an attacker (default settings, etc.)
10	Other	01	Undetermined incident	Not enough data to handle the incident

TABLE 2.3: CERT-UA classification of cyberincidents [37]

In order to briefly indicate the type of cyberincident in CERT-UA, the concatenation of numbers from the first and third columns of the table 2.3 is used, but if only a category without a type can be established, they put "00" instead of two digits that indicate the type. For example, malicious software distribution has the code 02.02 and the category of intrusion without specifying the type - 05.00.

2.2 Dataset notions

2.2.1 YARA rules

YARA rules are used to classify and identify malware samples by creating descriptions of malware families based on textual or binary patterns.

YARA rules are like a piece of programming language, they work by defining several variables that contain patterns found in a malware sample. If some or all of the conditions are met, depending on the rule, then it can be used to identify a piece of malware successfully.

When analyzing a piece of malware researchers will identify unique patterns and strings within the malware that allows them to identify which threat group and malware family the sample is attributed to. Creating a YARA rule from several samples from the same malware family, makes it possible to identify multiple samples all associated with perhaps the same campaign or threat actor [51].

2.2.2 APT

***APT* (Advanced Persistent Threat)** - is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network to mine highly sensitive data.

The targets of these assaults, which are very carefully chosen and researched, typically include large enterprises or governmental networks. The consequences of such intrusions are vast and include:

- Intellectual property theft (e.g., trade secrets or patents)
- Compromised sensitive information (e.g., employee and user private data)
- The sabotaging of critical organizational infrastructures (e.g., database deletion)
- Total site takeovers

Executing an APT assault requires more resources than a standard web application attack. The perpetrators are usually teams of experienced cybercriminals having substantial financial backing. Some APT attacks are government-funded and used as cyber warfare weapons.

APT attacks differ from traditional web application threats in that:

- They are significantly more complex.
- They are not hit and run attacks—once a network is infiltrated, the perpetrator remains to attain as much information as possible.
- They are manually executed (not automated) against a specific mark and indiscriminately launched against a large pool of targets.
- They often aim to infiltrate an entire network instead of one specific part.

More common attacks, such as remote file inclusion (RFI), SQL injection, and cross-site scripting (XSS), are frequently used by perpetrators to establish a foothold in a targeted network. Next, Trojans and backdoor shells are often used to expand that foothold and create a persistent presence within the targeted perimeter.

Advanced persistent threat (APT) progression
A successful APT attack can be broken down into three stages:

1) network infiltration

2) the expansion of the attacker's presence

3) the extraction of amassed data—all without being detected [4].

2.2.3 0-day

A zero-day is a computer-software vulnerability either unknown to those who should be interested in its mitigation (including the vendor of the target software) or known and without a patch to correct it. Hackers can exploit the vulnerability to adversely affect programs, data, additional computers, or a network until the vulnerability is mitigated. An exploit directed at a zero-day is called a zero-day exploit or zero-day attack [52].

Chapter 3

Related Work

3.1 Can the situation in Ukraine be claimed as the very first cyberwar?

Many media platforms can say that the world's first cyberwar is taking place in Ukraine now, but is this a correct statement? Short answer - No. But then why do journalists make such statements? It should probably be noted that such a term as cyberwar is not a well-established concept, so not even experts will be able to say with 100% certainty which cyberincident may be considered involved in cyberwarfare and which may not. However, if we consider cyberwar as a planned decision of the authorities of one or more countries to use mass attacks in cyberspace against one or more countries, mainly pursuing certain political goals, then it is correct to say that such cases have occurred in our history more often than we thought. Let us take a look at some of them.

3.1.1 One of the first uses of cyberwarfare tools - Estonian case

- Is Ukrainian cyberwar the first?
- No

In April 2007, the tensions with Russia significantly increased due to the decision of the Estonian capital city – Tallinn authorities, to remove the statue of the Bronze Soldier of Tallinn, which commemorated the Soviet soldiers who had liberated Estonia. For the Estonians, it was a symbol of oppression. For Russians, it meant the destruction of the cultural heritage and the lack of respect for the Red Army, which fought against Nazi Germans during II World War. After the movement of the Bronze Statue, the relationships between Estonia and Russia became very tense. Kremlin accused Tallinn authorities of breaking human laws and demanded the Estonian prime minister's resignation. Simultaneously, the severe riots on the streets between the police and the Russian minority in Estonia, the protests in front of the Estonian Embassy in Moscow, and the massive cyberattack campaign erupted.

Estonia has been highly dependent on the Internet. Almost the whole country was covered by the WiFi Internet, all Government services were available online, and 86% of the Estonian population did banking online. In 2007 there was an opportunity to vote electronically, and 5,5% of voters did it.

On 26 April, the growing volume of cyberattacks was noticed, and this day is commonly recognized as the beginning of massive cyberattacks. The peak of the attack took place on May 9. Since that date, the number of hostile acts has started to decrease. On May 11, the Paid botnets activity ended; the last attack took place on May 23.

Despite the initial surprise, Estonia was able to organize defense quickly and overcome the dangers with the help of allies. Germany, Israel, Slovenia, and Finland provided assistance to restore normal network operations. NATO Computer Emergency Response Team also helped Estonia.

Cyberattacks on Estonia in 2007 were widespread reflected in media and called the first cyberwar in history. It showed how the new technology could be used to attack a modern country. The attack came from Russia - most of the DDoS attacks were addressed from Russian IP addresses. Many attackers used computers from Estonia – it was the Russian minority. Even though the European Commission and NATO technical experts did not find evidence that Russian authorities perpetrated this attack, these attacks were very favorable to Kremlin.

The presumable aims of the cyberattacks were to try to influence Tallinn authorities to withdraw from their decision to remove the monument. The second was to test Russian cyber warfare capabilities and look for the reaction of NATO when one of the members of this organization is attacked in a new domain. The third one was linked to the fact that Estonian society is dependent on the Internet. Cyberattacks were carried out to show that both NATO and the EU would not defend Estonian society from the Russian attack and that the Russian did not need tanks to inflict damage on Estonia. All political targets were not achieved, the monument was removed, and Estonia became a leader in the cybersecurity field. NATO has sped up its cyberdefence projects and created the Cooperative Cyber Defence Centre of Excellence located near Tallinn [23].

3.1.2 The most famous case - Iranian Stuxnet Virus

- Does the cyberwar held on nowadays in Ukraine - the most famous case in history?
- Probably, no

Arguably one of the most famous cyberattacks in history, Stuxnet is a computer malware that targets supervisory control and data acquisition (SCADA) systems. It is suspected of causing significant harm to Iran's nuclear program.

The Stuxnet worm first appeared in 2010, and it is believed to have been created by the United States and Israel. But, neither government has publicly accepted responsibility.

Iran formed a squad to battle the infection in reaction to it. An official added that the virus was quickly spreading in Iran, with more than 30,000 IP addresses infected, and that the problem had been worsened by Stuxnet's capacity to mutate.

Iran has built up its own infection-cleaning systems, and Stuxnet was successfully neutralized and removed from the country's machinery by Iranian engineers.

While the Stuxnet virus did not cause any direct loss of life, it was a highly sophisticated and well-coordinated cyberattack that caused billions of dollars in damages [38].

3.1.3 Hybrid war - Georgian case

- Okay, maybe what Ukraine is experiencing right now is the first hybrid war?
- Still, no

From the beginning of the 90s, Georgia looked for integration with the West. This trend was strengthened after 2003 when the Rose Revolution erupted, and the current president Eduard Shevardnadze was overthrown. The newly elected president Micheil Saakashvili engaged in integration with Western Structures and tried

to reintegrate Georgian provinces' breakaways – South Ossetia and Abkhazia. His attempts evoked a strong reaction from Russia, which led to the war in 2008.

This conflict started on 7 August and lasted for five days. Even though the war was classical and the behavior of the armies on the battlefield reminds the 20 century, one aspect of it was a complete novelty. It was the first war in the air, on the ground, on the sea, and in a new domain – cyberspace.

The first cyberattacks took place months before the outbreak of war. On 19 July, the security firm informed about the DDoS attack against the Georgian websites. A similar scenario with the attacks on a bigger scale was repeated on 8 August and coincided with the Russian troops entering South Ossetia.

Firstly hackers focused mainly on Georgian news and government websites and used botnets to conduct brute DDoS attacks. The Georgian networks were more vulnerable to attack than the Estonian ones. Then, the list of targets embraced financial institutions, businesses, educational institutions, Western media, and a Georgian hackers website. Besides the DDoS attack, web defacement operations were also done using an SQL injection and the massive spamming of public email to clog them. Till 10 August, the majority of the Georgian governmental Web sites were inoperative, and the Georgian Government was unable to communicate with the world using the Internet. Instead of standard content on the Georgian President's website, images depicted M. Saakashvili as Hitler. Also, banks did not function in Georgia as well as the cellphones.

The attacks came from the territory of Russia. They were a mixture of professional acts carried out using the botnets and the raids conducted by patriotic hackers who, similarly to the Estonia case, could find information and programs on the special forums. The center of this information campaign was the website StopGeorgia.ru.

Two situations could indicate the cooperation between classical and cyber forces. The first was that conventional strikes omitted attacking the media and communication facility, leaving these targets for cyberattacks. The second example was an attack on websites renting diesel-powered electric generators to support conventional strikes against Georgian electrical infrastructure. Also, there were prepared cyber tools, instructions, and particular websites to carry out the strikes. It can indicate that Russia had been preparing for this war for a longer time.

The cyberattack on Georgia was a manifestation of information warfare to cut off Georgian authorities and society from any news, present their propaganda, undermine citizens' morale and faith in government and inflict severe damage on the economic development of Georgia. All aims were not achieved mainly because of the aid from allies. The government websites were restored, and the Georgian society had access to information. The United States promised financial help for the Georgian government [23].

3.1.4 Previous cases of cyberattacks carried out against Ukraine

- Does it the first use of cyberwarfare instruments against Ukraine?
- Again, no

In Cyberworld, Ukraine is known as a country frequently exposed to cyberattacks by Russia. Here are the three most famous examples:

Fancy Bear (2014-2016)

In June 2016, CrowdStrike discovered and ascribed a series of targeted breaches at the Democratic National Committee (DNC) and other political groups that used a well-known implant known as X-Agent.

X-Agent is a cross-platform remote access toolkit linked to an actor called the FANCY BEAR. This actor has been the sole operator of the virus to date and has continued to create the platform for ongoing operations. CrowdStrike believes FANCY BEAR is linked to Russian Military Intelligence (GRU). The FANCY BEAR X-Agent implant was circulated covertly on Ukrainian military forums in a legitimate Android application from late 2014 to early 2016.

According to open-source data, Ukrainian artillery units have lost over half of their guns in the two years of conflict and over 80% of D-30 howitzers, which is the most significant loss of any other artillery pieces in Ukraine's arsenal.

This Russian hacker group is also believed to be responsible for several other high-profile cyberattacks, including the 2015 hack of the German parliament and the 2016 hack of the World Anti-Doping Agency (WADA).

Blackouts In Ukraine (2015)

In December 2015, Ukrainians experienced a series of power blackouts that lasted for several hours. The outage was caused by a cyberattack that targeted Ukraine's power grid. The hackers had successfully cut off the electricity to many Ukrainians in Kyiv and other places.

They used a malicious piece of custom-built software designed to automatically launch a power-killing process by delivering quick commands to circuit breakers in a victim's utility called Crash Override. This was the first cyberattack causing a power outage.

The attack was widely attributed to Russia, but the Kremlin has denied any involvement.

NotPetya (2017)

NotPetya is a ransomware virus that was first discovered in June 2017. The virus quickly spread across Ukraine and then to other countries, including the United Kingdom and the United States.

NotPetya was initially disguised as a piece of software called Petya, which is used to encrypt files on a victim's computer. Once installed, the virus would then spread to other computers on the same network.

The virus was different from other ransomware in that it was designed to destroy data rather than encrypt it permanently. This made it much more destructive and caused billions of dollars in damages.

NotPetya is believed to have been created by the Russian military intelligence agency (GRU).

With all these cyberattacks, one question arises: Is it possible to defend yourself? The great news is that everyone can take measures to protect you in the long run [38]!

Summarizing all the above, we can conclude that since Ukraine is one of the countries with high information development, there is now another hybrid war in world history with possible terrible consequences in physical and cyberspace. Also, works

similar to mine could have already been written since such situations occurred earlier.

3.2 Data-Driven Cyber Prediction in Hybrid Warfare

I would like to start with a paper that seemed probably the most similar to mine. Hannah Devereux - a student at the University of Calgary, wrote her master's thesis called *Data-Driven Cyber Prediction in Hybrid Warfare* [18]. She tasked herself to answer the question: "What is the relationship between cyber attributes and physical attributes in hybrid warfare?" To do this, she used the Ukrainian crisis as a case study.

Since this thesis was written in 2019, it is worth noting that the events analyzed in the work took place before or during the first half of 2019. Also, to make predictions, the author used only five large-scale attacks, and only three of them were applied to the Axelrod-Iliev equation (which was used in the paper). The focus of the work was more on the dependence of cyberattacks on the battlefield. The prediction was made for the most favorable time to deliver mainly large-scale cyberattacks.

Several things distinguish this work and mine. My analysis will be built on data from a different time slot, under different circumstances, events, and in a different context. Also, data on the physical battlefield will not be used in my research. I plan to rely on a much larger dataset of cyberattacks and use other forecasting approaches and methods.

3.3 Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?

The following work was written by Nadiya Kostyuk and Yuri M. Zhukov in 2017 and published in the Journal of Conflict Resolution in 2019 and is called *Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?* [22].

Unlike previous work, this one does not aim to anticipate future attacks but instead seeks to answer the question of whether it is possible to create successful coordination between low-level cyber and kinetic operations, what is the relationship between cyber and physical attacks, and in general, whether low-level cyberattacks can cause strong influence or be a tool of coercion on work or decision-making of the military department in wartime.

This work is based on the case studies of the Ukrainian crisis and the war in Syria and uses data on small-scale cyberattacks on Ukraine collected from 2013 to 2016 and on Syria from 2011 to 2016.

In conclusion, researchers sum up that the timing of cyber actions is independent of fighting on the ground, cyberattacks are not (yet) effective as tools of coercion in war — has potentially significant implications for other armed conflicts with a digital front.

Things that connect this work and mine are the similar context of the dataset (cyberattacks on Ukraine in the Russian-Ukrainian war, but other years) and the fact that they analyze an extensive dataset of attacks in various orientations and complexity.

3.4 Artificial Intelligence and Cyber Security – A Shield against Cyberattack as a Risk Business Management Tool-Case of European Countries

Artificial Intelligence and Cyber Security – A Shield against Cyberattack as a Risk Business Management Tool-Case of European Countries [26]. This article analyzes the willingness of different European countries to use artificial intelligence to conduct risk assessments. The author analyzes the most significant risks faced by countries in cyberspace and, at the end of the work, advises on how to better protect yourself and which areas should be paid the most attention to.

This paper is similar to mine because it aimed to identify a possible tool for predicting cyberattacks or conducting risk assessments in a country context.

3.5 CERT-UA reports

The closest to my thesis is the CERT-UA reports, but currently, only the 2021 report [35] and the 2022 analytics (01.01.2022 - 17.02.2022) [34] are available. Still, these reports have no elements of attack prediction or risk assessment.

In my work, I plan to rely on these reports and analytics to understand whether my dataset correctly reflects the trends that can be identified from the official organization's database, as the whole cyberattack dataset is not publicly available.

Chapter 4

Dataset collection

I decided to start the practical part of my research by finding a set of data that I could analyze and, based on this, attempt to predict.It is worth mentioning that this dataset should contain cyberattacks aimed at Ukraine, i.e., its government agencies, sites popular among Ukrainians, Ukrainian banks, various services, or a large number of people. In other words, most attacks will be carried out to undermine the spirit of Ukrainian citizens, sabotage essential elements of governing the country, prevent the success of the Ukrainian military, harm the economy, etc. Still, at the same time, fraud or other cyberincidents with low impact will be virtually ignored.

4.1 Process of collecting the dataset

Of course, I needed to find a source of information that would be both reliable and present detailed information about each cyber attack. My research on the Internet led me to the site of the Computer Emergency Response Team of Ukraine. At first, I decided to write to the official email of this team with the question of whether they could provide me with such a set of data. I received the answer that the dataset I need is confidential information, so the CERT cannot provide it to me. On the other hand, in response, I was advised by the State Service of Special Communications and Information Protection of Ukraine website and provided links to the CERT-UA report and statistics I mentioned above.

4.1.1 Sources

After the first failed attempt to get the database I needed, I realized that, most likely, I had no other choice but to create one by myself, but I needed a particular source of information for this.

The CERT-UA News section [36] initially became such a source. Most of the news was described in great detail, and it was possible to understand who, when, and how was attacked. Later, I also began to use CERT-UA's unique publications on their official Facebook page [1] as a source of information about cyberattacks. And last but not least, the website of the State Service of Special Communications and Information Protection of Ukraine [33], thanks to which I was able to learn about some events backstory, better describe them in the database, and better understand the quantitative component of attacks on Ukraine in cyberspace.

4.1.2 Bottlenecks

Unfortunately, many bottlenecks sometimes hindered, slowed down, and complicated the data collection process at this stage of my practical work.
Here are some of them:

- Although the CERT has a unique system for classifying cyberincidents, it was not used in the news description, so the classification had to be done by myself.
- Due to each article's diversity and unstructured nature, it was impossible to automate collecting information, which significantly slowed down this process and required more resources, both time and effort.
- Not all cyberattacks were mentioned in one source, so we had to look for additional sources of information. However, the new sources presented the data a little differently. The main goal was to acquaint the masses with the event rather than to describe the event in detail for further analysis, so some details were not specified. It complicated the characterization process of such cyberattacks based on the previously established database structure.
- Another problem was determining the time. Because the date of writing the news was not always the same as the date of the cyberattack for one reason or another. This could be due to the late detection or confidential nature of information needed for the cyberattack description. To ensure the stability of system protection, the details of the cyberattack could only be made public after a certain period. That is why I added a new column and distinguished between the news publication date and the attack date. Also, I had to search for the exact time when the attack occurred because such information was not always specified in the article.
- Also, despite the seemingly detailed description, I lacked specific data on the attack's tools/exploits and its consequences, so I sometimes had to look for this information.

4.2 Dataset structure

As a result of the information gathering, 120 unique records were collected and characterized using 20 characteristics (columns in the table). 75 of 120 - took place before the full-scale invasion (publicly available data for almost the entire 2021 + beginning of 2022), and 45 of 120 - during it (publicly available information for the period: late February - late May 2022). The oldest record in the dataset is dated January 19, 2021, and the most recent is May 20, 2022. This dataset contains attacks and warnings, i.e., 60 records of attacks and 60 records of warnings. The warnings mainly concern vulnerabilities that could potentially be exploited by hackers, and the source also provides advice on how to protect yourself from these vulnerabilities.The dataset was compiled in Google Sheets [15] and later saved as a file with a .xlsx extension. Here are the columns in the dataset and what they mean (see table 4.1)

Column name	**Meaning**
News publication date	the date when the news was published describing this cyberattack.
Date	the specific date of the attack's start, conduct, or recognition.
CERT-UA#	the identification number assigned by CERT-UA to this news.
Attack group(s)	a hacker group(s) that carried out this attack or with whose work this attack was associated.
Target	who was the target victim of the attack, who it was aimed at, who could potentially suffer or have suffered from it.
Theme / Key words	keywords of text, file names, and messages containing attacks (potential phishing triggers).
Framework / Tool / Exploit	the means or tools the attack was carried out.
File extensions involved	extensions of files found during the investigation of a cyberincident.
Type	a type of cyberattack written in words using the CERT-UA classification.
Code	code of the cyberattack's type, using the CERT-UA classification.
Possible outcome	the consequences that the victims of such an attack may face if it is successful.
Network info	email addresses, links, and other network information involved in the cyberattack found during the investigation.
Host info	commands executed on the machine and other host information found during the cyberattack investigation.
Yara	Yara rule for malicious software that appears in the attack.
Short description	a short description of the event.
URL (source)	a link to the source of information.
Status	the status of a cyberattack at the time of its description. Among the options: • **Detected** - if CERT noticed the attack at some point, but no action was taken other than writing an article in the news about it. • **Prevented** - if CERT was somehow informed about a potential cyberattack in advance and they could prevent it so that it could not be carried out successfully. • **Handled** - if a cyberattack was carried out and CERT worked on the consequences and managed to suppress the main problem (blocking the malware distribution site). • **Acquainted** - this status was applied to Vulnerability type events where CERT tried to prevent potentially exploited vulnerabilities by writing articles about them.
CVE	CVE associated with a cyberattack.
CWE	CWE, to the corresponding CVE from the previous column.
CVSS Score	an assessment of the criticality of this vulnerability.

TABLE 4.1: Dataset structure

Chapter 5

Analysis

To analyze the collected data, I decided to use Jupyter Notebook, with which I was able to create the following visualizations. The code, visualizations, and dataset can be found in this GitHub repository [39].

5.1 Timeline

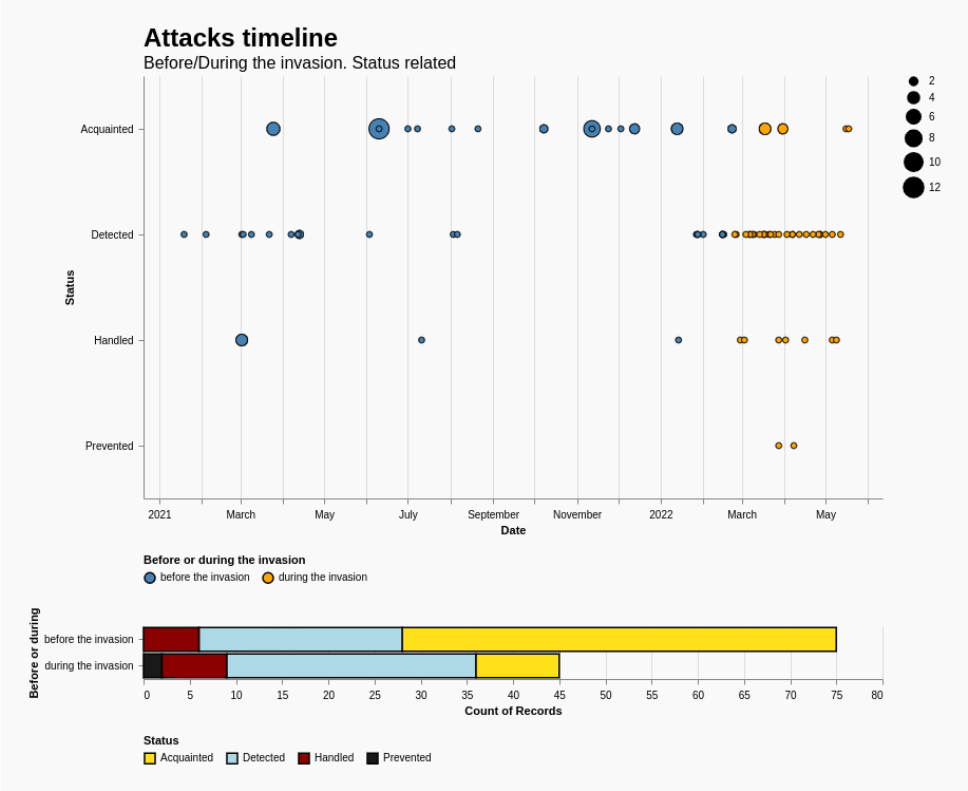


FIGURE 5.1: Timeline of attacks and warnings

This chapter should probably be started with a basic visualization that shows the timeline of all collected attacks and warnings.

The top chart distinguishes records by status. The colors indicate the periods before or during the full-scale war, and the size of the circles indicates the number of records that fell on the same day.

The chart below can help understand how many records belong to which period and the distribution of statuses in accordance (see Fig. 5.1).

Analyzing these plots, one can conclude that there were more reports of warnings last year, and attacks were less frequent and regular. However, when one focuses on the yellow circles, one can see a cluster of attacks in the line "Detected", which indicates the regularity of detected attacks during the invasion. Moreover, some attacks managed to be prevented.

It is also worth noting that I made this chart interactive. If one downloads the Jupyter Notebook from the repository I mentioned above, it will be possible to explore each timeline period in more detail by narrowing or widening the time axis with the mouse wheel. Also, each circle shows the essential information when hovering the mouse over it. Furthermore, if someone wants to read the source of information about a particular attack or warning, it is possible to do so by clicking on the circle. In that case, one will be redirected to the site with the news of the cyberattack, but if one wants to open this site in the next tab, one needs to hold down the Ctrl button while clicking.

5.2 Hacker groups

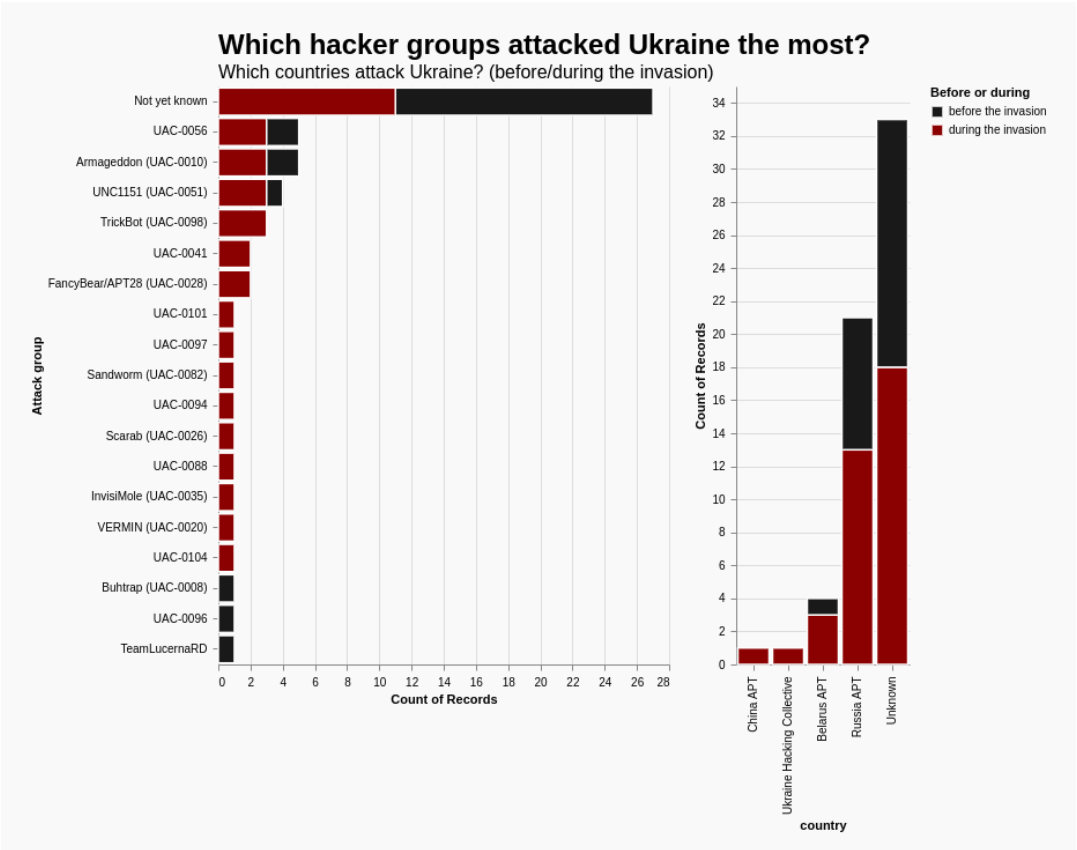


FIGURE 5.2: Hacker groups, who attacked Ukraine

The following graph is intended to answer the question: Which hacker groups attacked Ukraine the most during the observable period, distinguishing the period before the war and during? Moreover, is it possible to establish a relationship between these groups and some countries? In other words, which countries attacked Ukraine and how often? (see Fig. 5.2)

The left graph shows the top of the hacker groups and the right of the countries that attacked Ukraine.

Unfortunately, in both charts, it is not the group or the country that comes first. Most reports of attacks did not provide information on which group the activity was associated with. Even less often, it was possible to trace to which country this group belongs.

However, if we take into account the rest of the information that this visualization is trying to convey to us, we can draw the following conclusions:

- Top 3 hacker groups that most often attacked Ukraine - UAC-0056, Armageddon (UAC-0010), and UNC1151 (UAC-0051), which were associated with Russia (the first two) and Belarus (the last one), respectively.
- From the right graph, it can be understood that Ukraine was attacked mostly by Russian ATPs, which with hacker ATPs from Belarus, carried out attacks even before the invasion.
- During the full-scale war, in attacking Ukraine in cyberspace were also suspected groups from China and the temporarily occupied territory of Ukraine - LPR.
- During the invasion, more unique groups appeared that attacked Ukraine.

5.3 Targets

5.3.1 Attacks/Warnings

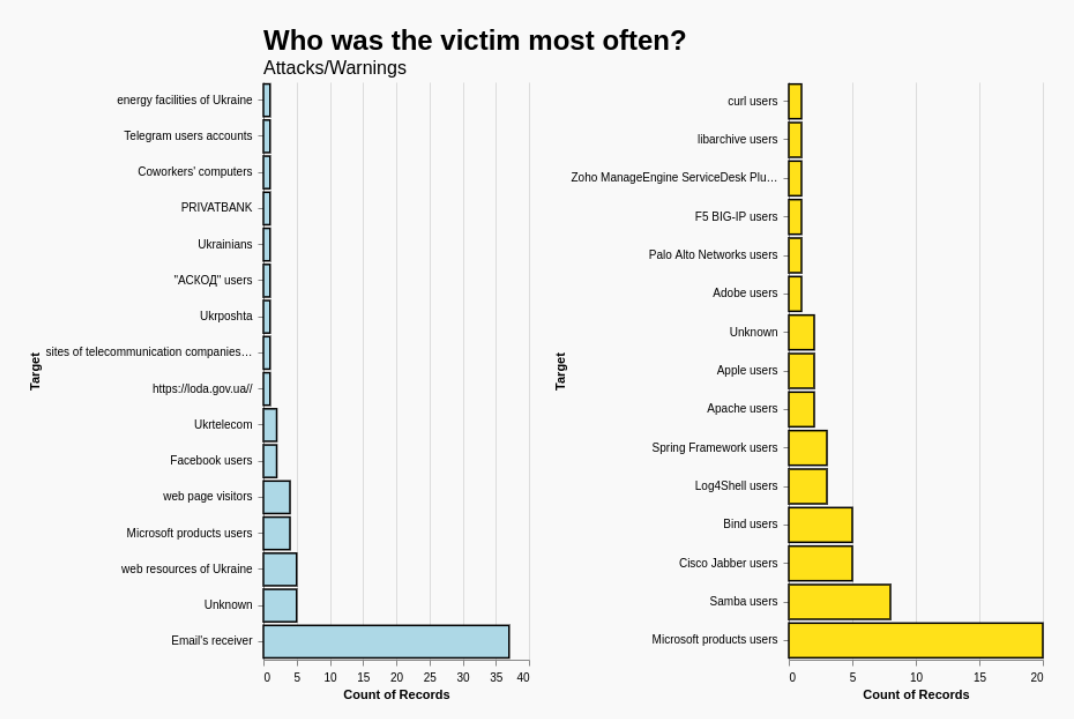


FIGURE 5.3: Who was the victim most often? | Attacks/Warnings

The visualization above shows two graphs: left - the most attacked victims, and right - the most potential targets due to warnings (see Fig. 5.3).

One can see that most people are attacked using mass emails, so inattentive email recipients are the primary target. It is also worth mentioning the attacks on the main web resources of the country, on visitors to the specific sites, and the targets of the attacks that exploited vulnerabilities in the systems of Microsoft products. Accordingly, it is not surprising that the warnings were dominated by Microsoft product users who did not update their system, as well as Samba, Cisco Jabber, and Bind users.

The following two subsections will show these graphs in more detail, examining them separately and in terms of two time periods.

5.3.2 Before/During the invasion | Attacks

The graph below aims to answer the question: Who was the victim most often? It contains only victims of attacks. Yellow indicates attacks during and blue before the active phase of the war (see Fig. 5.4).
The following conclusions can be drawn:

- Email recipients have constantly been attacked almost equally often before and during.
- It was impossible to establish the victim of 5 attacks "during". Note that this has not happened "before".
- During the active phase of the Russian-Ukrainian war, new targets appeared, such as Ukrtelecom, other sites of telecommunications companies, the official website of the Lviv Regional State Administration, Ukrposhta, users of the Telegram messenger, and energy facilities of Ukraine.
- While considering the rest of the victims of attacks that took place "before", then among them, one can find Privatbank. Suppose one looks at this series of cyberattacks in more detail. In that case, one can see that it occurred shortly before the official date of the Russian physical invasion, namely February 15, 2022, and had a substantial impact on resource efficiency, not to mention the undeniable importance of this bank for Ukrainians. Would it be logical to assume the correctness of the statement that this attack was part of a cyberwar and, accordingly, the cyber intrusion took place before the physical one?

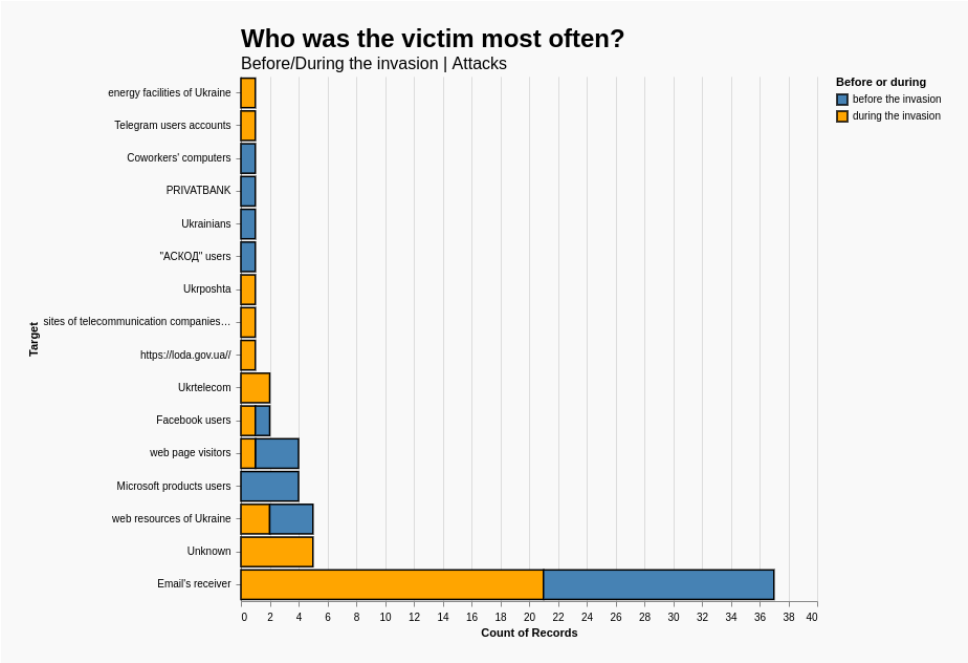


FIGURE 5.4: Who was the victim most often? | Attacks

5.3.3 Before/During the invasion | Warnings

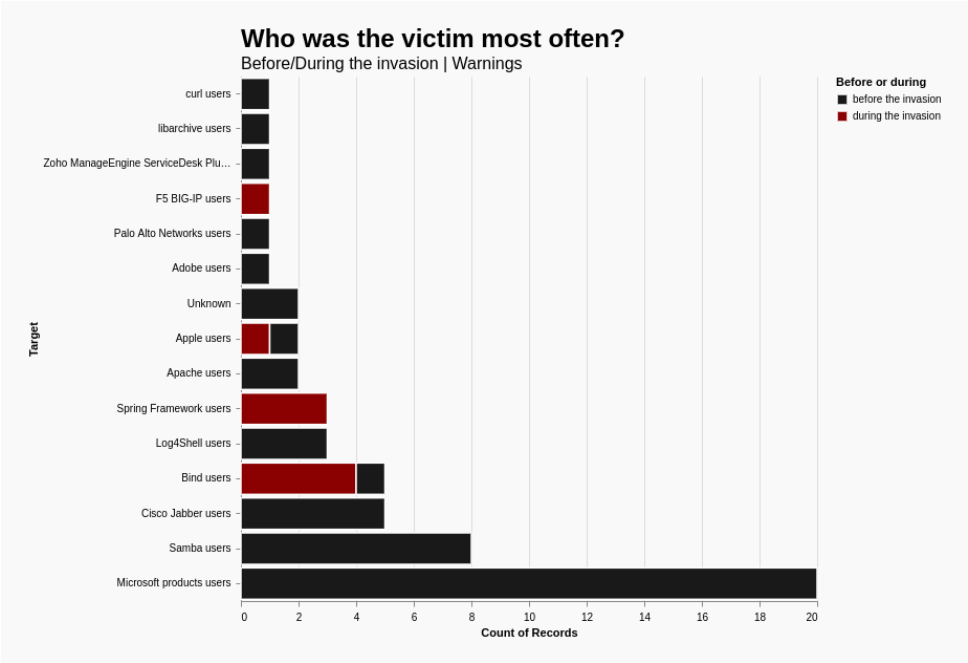


FIGURE 5.5: Who was the victim most often? | Warnings

From the chart above, it can be seen that most of the warnings were made before the war, so it will probably be more interesting to consider what warnings were issued during the Russian invasion of Ukraine (see Fig. 5.5).

5.4 Keywords

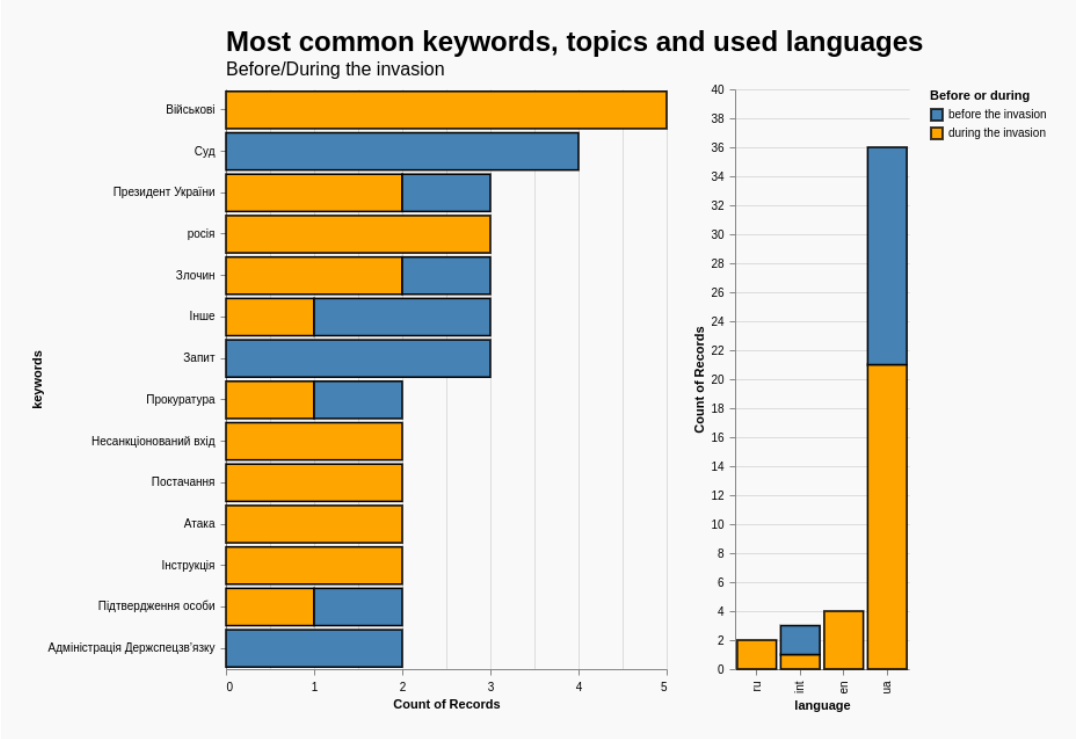


FIGURE 5.6: Most common keywords and topics and used languages

The following visualization demonstrates the keywords and topics used in phishing emails during attacks, as well as the languages in which those words were written. It is also worth noting that the graph shows only keywords and topics repeated at least two times (see Fig. 5.6).
Therefore, the following conclusions can be drawn:

- The word "Військові" (Military) was used very often and only during a full-scale war.
- The word "Суд" (Court) is precisely the opposite of the prior. It was in second place in the ranking but used only "before".
- Only during active hostilities were the following topics popular: "росія" (Russia),"Несанкціонований вхід" (Unauthorized entry),"Постачання" (Supply),"Атака" (Attack), "Інструкція" (Instruction).
- Popular before the war were the words:"Запит" (Inquiry) and the "Адміністрація Держспецзв'язку" (State Service of Special Communications and Information Protection of Ukraine)
- Interestingly, the terms "Президент України" (President of Ukraine) and "Злочин" (Crime) were popular both before and during the full-scale invasion but became dominant "during".
- Regarding languages, the most frequently used messages were in Ukrainian, but there were, although insignificant, cases of using Russian and English.

5.5 Tools

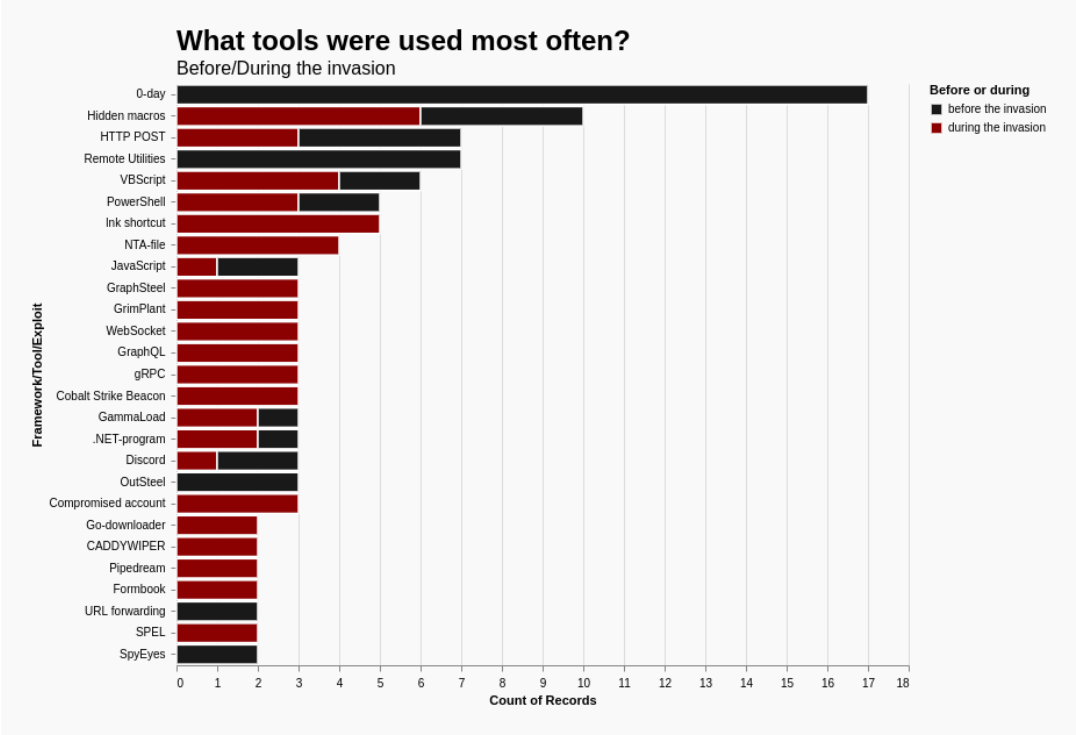


FIGURE 5.7: What tools were used most often?

The graph above answers the question: What tools are most often used by hackers to attack? It is also worth mentioning that the graph shows only tools, frameworks and exploits repeated at least two times (see Fig. 5.7).
It can be seen that many of them were popular only before or only during the full-scale invasion of Ukraine.

5.6 Extensions

The graph below shows a rather specific set of data - the extension of files that occurred during a particular cyberincident investigation. Distinguishing the number of repetitions of such files before and during the large-scale war. The graph shows only extensions repeated at least two times (see Fig. 5.8).
The following conclusions can be drawn:

- exe files - used most often and evenly before and during.
- Attackers like to use a variety of archives; apparently, they are more likely to encourage people to download and, as a result, open files in it, so as if initially hiding the content so as not to arouse suspicion.
- You can see the growing popularity of lnk, xsl, and dll files during the invasion and files htm and dat, used only in attacks after February 24, 2022.

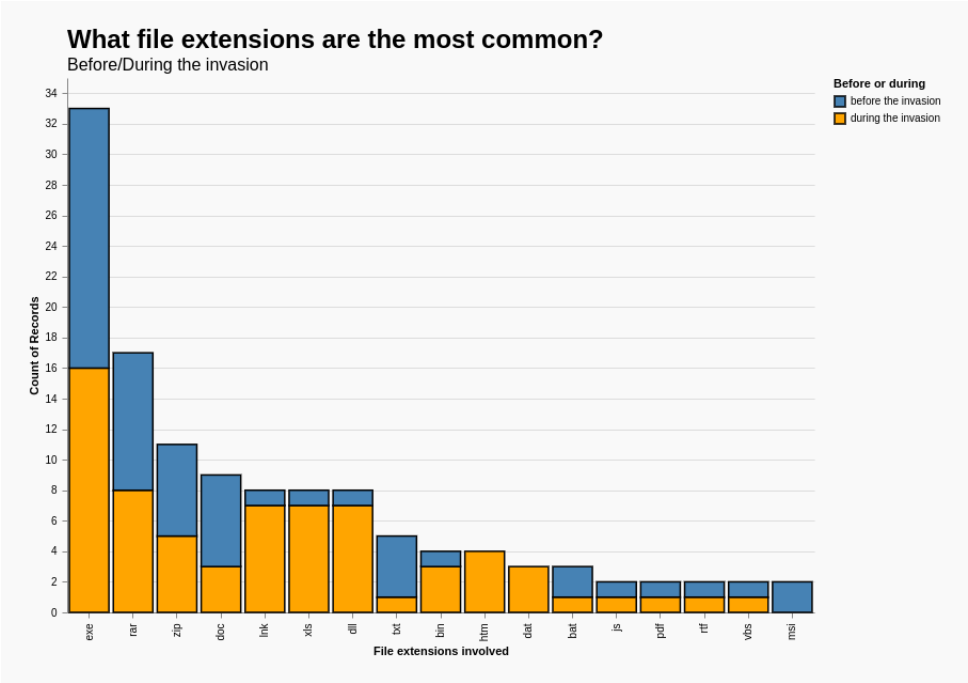


FIGURE 5.8: What file extensions are the most common?

5.7 Types

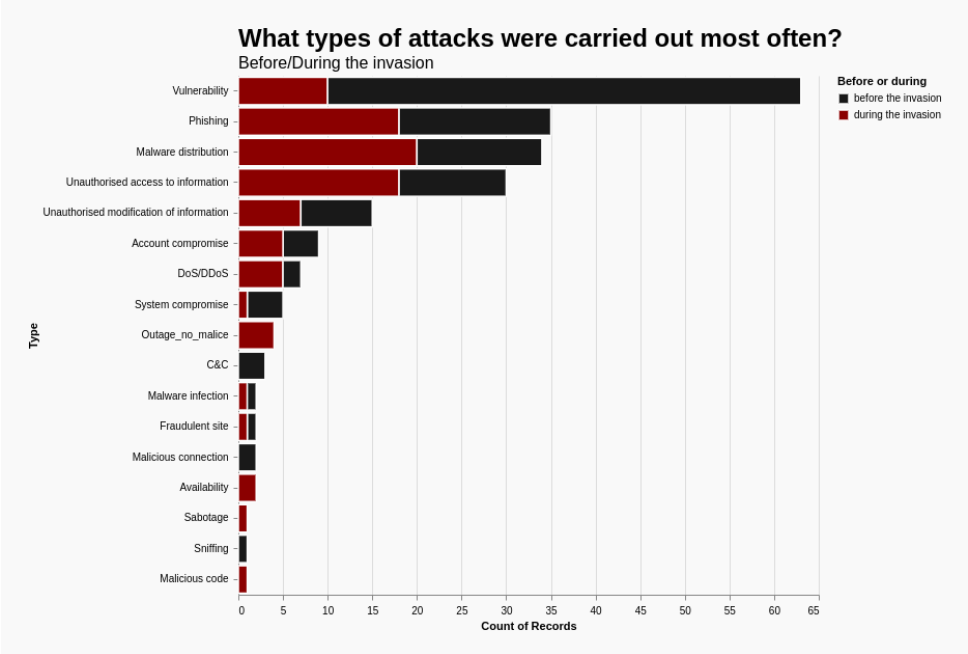


FIGURE 5.9: What types of attacks were carried out most often?

This visualization shows the distribution of types of attacks based on the collected dataset. It is possible to estimate which types of attacks were popular only before or during a full-scale war(see Fig. 5.9).

5.8 Outcomes

This chart tries to answer the question: What outcomes did hackers want the most? The graph shows only outcomes repeated at least two times (see Fig. 5.10).

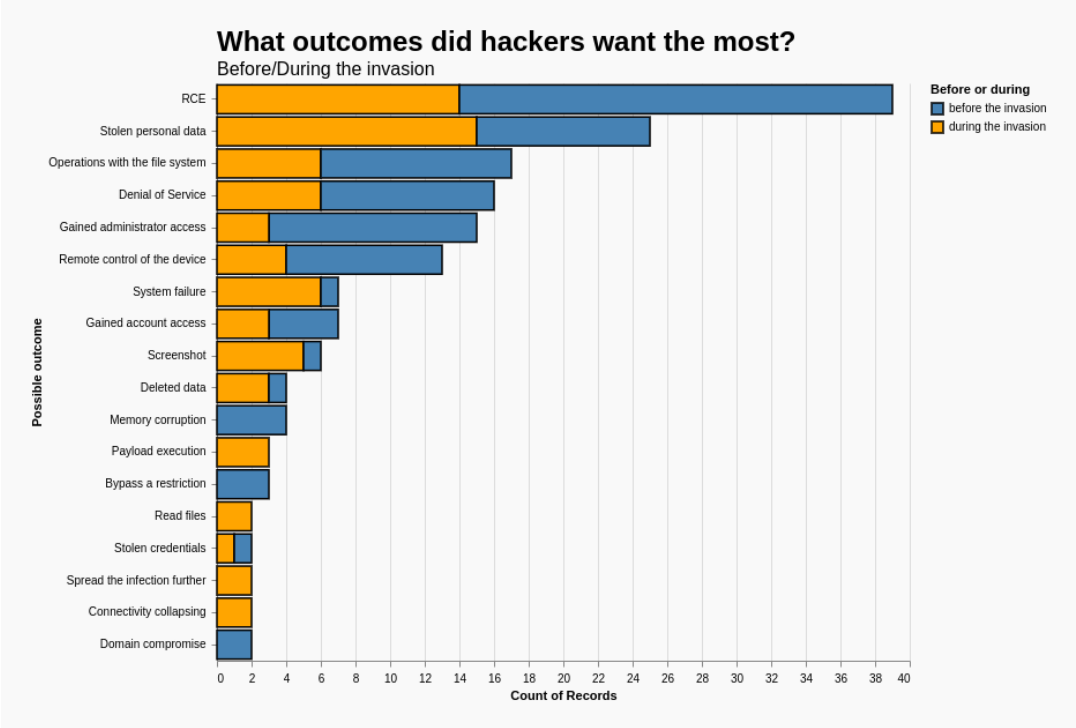


FIGURE 5.10: What outcomes did hackers want the most?

After a detailed review of this bar diagram, I concluded that:

- The most common intentions of attackers were to be able to execute code on someone else's device, steal information, be able to operate the file system of the victim device, and arrange a denial of service. All of them were popular before and during the Russian-Ukrainian war of 2022.
- They were popular only during this war: Payload execution, Read files, and Connectivity collapsing.
- Were popular only before: Memory corruption, Bypass a restriction, and Domain compromise.

5.9 CWE

The picture below shows the distribution of CWE (see Fig. 5.11).
It is crystal clear that the number of records before a full-scale intrusion in the country is more significant than others. At the same time, it shows very few specific CWEs used "during", so I think it is worth it to analyze them in more detail (see table 5.1).

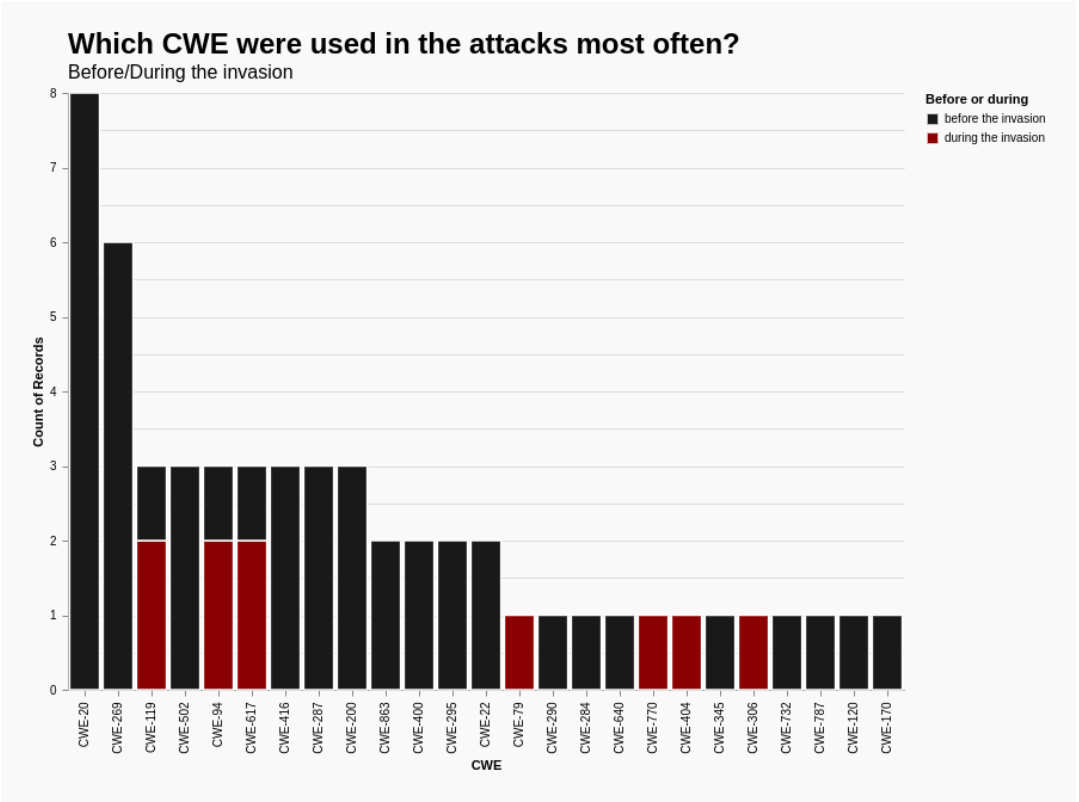


FIGURE 5.11: Which CWE were used in the attacks most often?

5.10 CVSS Distribution

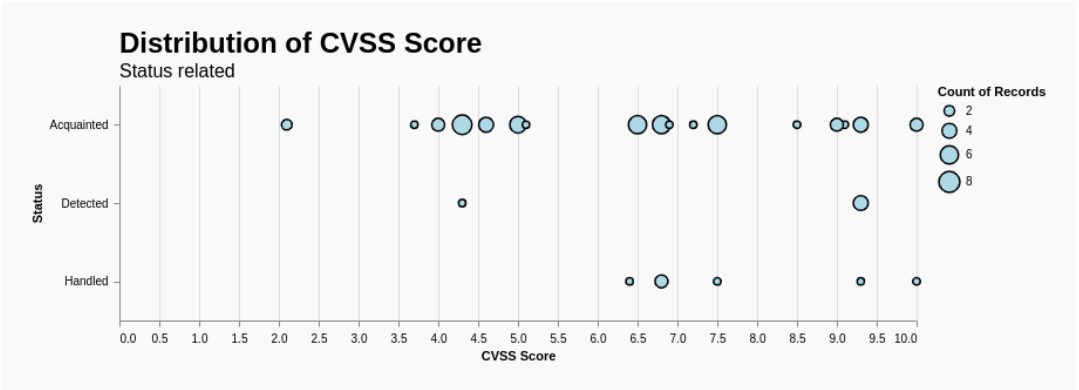


FIGURE 5.12: Distribution of CVSS Score

The last but not the least visualization shows the distribution of the CVSS Score. This distribution also takes into account the status of the record, and the size of the ball indicates the number of matches in one place on the scale (see Fig. 5.12).
It is fascinating to look at such a graph regarding the criticality of vulnerabilities. After all, it is clear that more critical vulnerabilities fall under Handled status. Very few of the vulnerabilities were detected. And, reports of threatening vulnerabilities - Acquainted (because there are many such records in the dataset), demonstrate a wide range of vulnerabilities of different levels of criticality.

CWE	Name	Description
CWE - 119	Failure to Constrain Operations within the Bounds of a Memory Buffer	The software performs operations on a memory buffer, but it can read from or write to a memory location that is outside of the intended boundary of the buffer. Certain languages allow direct addressing of memory locations and do not automatically ensure that these locations are valid for the memory buffer that is being referenced. This can cause read or write operations to be performed on memory locations that may be associated with other variables, data structures, or internal program data [7].
CWE - 94	Failure to Control Generation of Code ('Code Injection')	The product does not sufficiently filter code (control-plane) syntax from user-controlled input (data plane) when that input is used within code that the product generates. When software allows a user's input to contain code syntax, it might be possible for an attacker to craft the code in such a way that it will alter the intended control flow of the software. Such an alteration could lead to arbitrary code execution [13].
CWE - 617	Reachable Assertion	The product contains an assert() or similar statement that can be triggered by an attacker, which leads to an application exit or other behavior that is more severe than necessary. For example, if a server handles multiple simultaneous connections, and an assert() occurs in one single connection that causes all other connections to be dropped, this is a reachable assertion that leads to a denial of service [10].
CWE - 79	Failure to Preserve Web Page Structure ('Cross-site Scripting')	The software does not sufficiently validate, filter, escape, and/or encode user-controllable input before it is placed in output that is used as a web page that is served to other users. Cross-site scripting (XSS) vulnerabilities occur when: The same origin policy states that browsers should limit the resources accessible to scripts running on a given web site , or "origin", to the resources associated with that web site on the client-side, and not the client-side resources of any other sites or "origins". The goal is to prevent one site from being able to modify or read the contents of an unrelated site. Since the World Wide Web involves interactions between many sites, this policy is important for browsers to enforce[12].
CWE - 770	Allocation of Resources Without Limits or Throttling	The software allocates a reusable resource or group of resources on behalf of an actor without imposing any restrictions on how many resources can be allocated, in violation of the intended security policy for that actor[11].
CWE - 404	Improper Resource Shutdown or Release	The program does not release or incorrectly releases a resource before it is made available for re-use.When a resource is created or allocated, the developer is responsible for properly releasing the resource as well as accounting for all potential paths of expiration or invalidation, such as a set period of time or revocation[9].
CWE - 306	Missing Authentication for Critical Function	The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources[8].

TABLE 5.1: Used CWEs during the invasion

Chapter 6

Forecast

6.1 Is it even possible to predict cyberattacks?

If one considers standard prognostication methods, one can see that for most of them, large datasets with well-defined points of time of the attack's carrying out is needed for more accurate results.

Since vague predictions will not be helpful and most attacks do not have a specific time, it is challenging to make a good prediction.

Experts assume that the attack's conduction time can be set based on the time of sending the email in such an attack, which uses mass malware email distribution. Despite Malicious emails being believed to be a more forecastable type of cyberattack than others, it still requires a unique approach because of the complex time series to achieve any actionable results [42].

Modern businesses typically use the following approaches and technologies to predict potential attacks:

- Systems that identify network vulnerabilities that could potentially be used in an attack.
- Attack graphs - graphs that show all possible ways to exploit existing vulnerabilities in the network and thus allow one to analyze any particular system.
- Dynamic Bayesian Network - works similarly to previous graphs but is based more on the statistical tools.
- COI - stands for capability, opportunity, and intent and is mainly used by intelligence agencies and the military.
  - Capability: previous targets exploited by a hacker.
  - Opportunity: access to insider information
  - Intent: attacker motivation and social influence.
- Recommendation systems - these systems that help us choose a movie on the streaming service or product to buy on the shopping site can also be used to identify vulnerabilities based on monitoring the behavior of malicious IP addresses.
- Well, we can not exclude AI technologies either, which are now intensively being developed to perform this task [28].

6.2 Datasets

Two new datasets were made for this thesis's practical part based on the main one. Both report the number of "Malicious code (02.00)" and "Information Content Security (07.00)" type attacks carried out during 2022. The *Dataset of Cyberattacks on Ukraine in dates (2022)* [16] shows the specific dates when these attacks were carried out, and the *Dataset of Cyberattacks on Ukraine in numbers (2022)* [17] - their number for each week of this period (20 weeks in total).

It is also worth mentioning why I limited myself to data from this dataset only for 2022. Given the results and conclusions obtained from the extensive dataset analysis, it became clear that the attacks carried out in the context of a full-scale invasion of Ukraine began around the beginning of the year. Unfortunately, according to all forecasts at the moment, in the nearest future, the country will still be in this context for an indefinite period. Accordingly, to increase the accuracy of the prediction - it should be based on data collected under similar geopolitical circumstances.

One can view these datasets in the GitHub repository [39] in the Data folder or by following the links in the bibliography.

6.3 ARIMA

Initially, when it was time to choose a topic and work had not yet started, I thought I would use ARIMA to simulate a possible prediction for cyberattacks conduction.

So what does ARIMA mean?

***ARIMA* (Autoregressive Integrated Moving Average)** is a statistical analysis model that uses time-series data to understand better the data set or predict future trends. A statistical model is autoregressive if it predicts future values based on past values. For example, an ARIMA model might seek to predict a stock's future prices based on its past performance or forecast a company's earnings based on past periods.

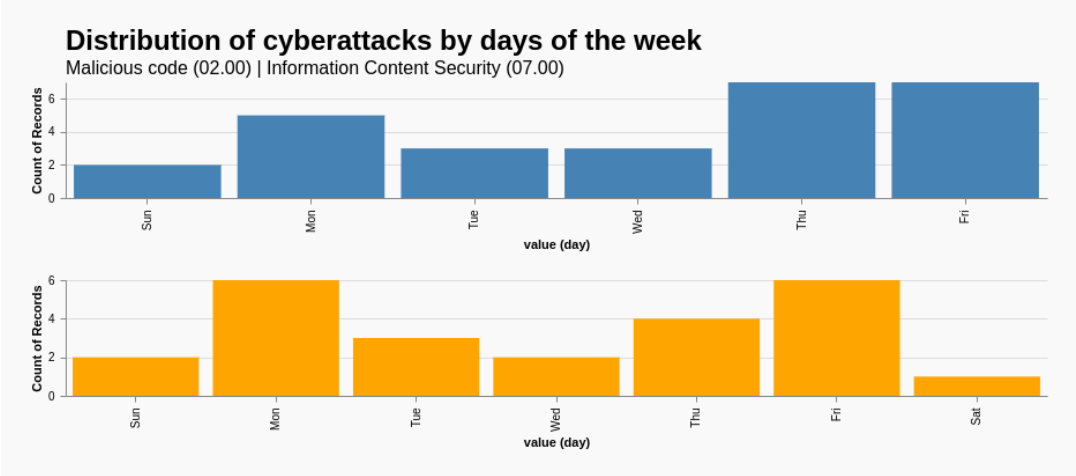
An autoregressive integrated moving average model is a form of regression analysis that gauges the strength of one dependent variable relative to other changing variables.

An ARIMA model can be understood by outlining each of its components as follows:

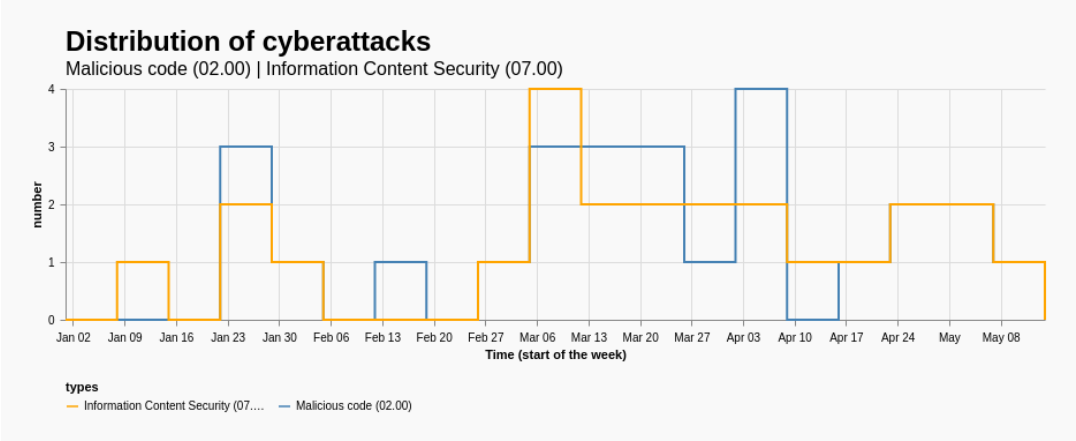
- **Autoregression (AR)**: refers to a model that shows a changing variable that regresses on its own lagged, or prior, values.
- **Integrated (I)**: represents the differencing of raw observations to allow the time series to become stationary (i.e., data values are replaced by the difference between the data values and the previous values).
- **Moving average (MA)**: incorporates the dependency between an observation and a residual error from a moving average model applied to lagged observations [20].

However, after I failed to get a large set of data due to the confidentiality of the information in it and, accordingly, it could not be collected manually by myself either. Then it became clear that usage of the approach with the given dataset will result in an inaccurate prediction because, for an accurate one, more timestamps and information than I possess is required.

6.4 Results



(A) Distribution of cyberattacks by days of the week



(B) Distribution of cyberattacks

FIGURE 6.1: Two main types of cyberattacks in numbers

However, I could not just end my research on that point and not make at least some hypotheses relying on the database that I managed to collect.

6.4.1 Prediction about days of the week

If one looks at this chart Fig. 6.1a, it becomes clear on which days of the week the most frequent attacks of this type are carried out. The upper graph describes the malicious attack code (02.00) and the lower - Information Content Security (07.00), respectively. Based on this, it can be assumed that the most significant flow of the attacks should be expected on Monday, Thursday, and Friday if this trend is confirmed.

6.4.2 Prediction about number of attacks

Let us take a look at this visualization Fig. 6.1b.It describes the number of such attacks per week during these 20 weeks.
The following conclusions can be drawn from the graph: potential attacks:

- In some parts of the graphics, attacks coincide, which in most cases indicates that hackers used these two types simultaneously. For example, they sent malicious software by email, through which they gained access to information or even the ability to change it.
- The most significant number of attacks of both types was carried out during March and April.
- In early May, there is a decline, which coincides with the commentary on the SSSCIP of Ukraine. So, we can hypothesize that hackers who aimed to attack Ukraine have already reached their highest potential in March-April, and now there is a small likelihood that this trend will be refuted.

6.4.3 Prediction based on context

For this simple hypothesis, I propose to draw attention to a specific attack carried out on April 22, 2022 - namely, a series of DDoS attacks on the services of Ukrposhta (Ukrainian Postal Service). The targeting of the post office comes just after Ukrposhta launched sales of a new stamp last week showing a soldier making a crude gesture to the Moskva Russian cruiser, a reference to an encounter between Ukraine and Russia at Snake Island that went viral in the early days of the invasion [27]. From this, it can be concluded that the cyberattack that aimed to cause a denial of service was highly politically motivated. This gives us reason to consider the COI method, which I talked about earlier, as an excellent way to predict future attacks if we think on a national scale. In other words, if something has political overtones and can be attacked somehow, it is likely to happen soon, given the strong involvement of many hackers in the process, such as ATP, hacktivists, and ordinary people who follow the instructions described in some resources.

Chapter 7

Summary

7.1 Results

As a result of the productive work done during these several months, all the goals were achieved almost wholly.

- A detailed study of ways to classify cyberattacks was conducted. The ones suitable for the research topic of the bachelor thesis have been selected. Also, I managed to collect a set of data for a year and a half, containing 120 records, of which 60 attacks and 60 warnings were classified by 20 characteristics.
- After the dataset analysis, 12 informative visualizations were plotted, each of which led to certain conclusions being drawn, which were also described in the paper.
- A study of existing, available, and accurate methods and approaches to forecasting this data type was conducted. Then the search for the best way to predict was carried out. An attempt to predict was unsuccessful due to the limits of information available. However, by analyzing other types of visualizations and considering specific examples in more detail - I was able to form 3 main hypotheses.

7.2 Conclusion

The results of this bachelor thesis can be summarized as follows:

The weakest factor that hackers tried to exploit was the human factor, as the primary victim of the attacks was email recipient. Although this is not a revelation, it is definitely another confirmation of why it is good practice to conduct training among all people, shape the trend of cyber hygiene, give recommendations, and, in general, engage in educational activities in this sector. It is also a rule of thumb to create possible scenarios and attack graphs that will allow one to understand system vulnerabilities. People should also be constantly reminded of the importance of upgrading specific systems, older versions of which contain vulnerabilities, especially critical ones.

All of the above is already being used successfully in the work of the CERT-UA team, but what could potentially be improved in the future?

Let us go back to the story of the cyberattack on the Ukrainian Postal Service, which I told above, and reflect a little bit on it. I immediately remember my assumption that if something has political overtones and it is possible to attack it somehow, it will be

done shortly. With such a rapid response to emerging potential targets, it is understandable how vital contextual and background data are for predicting cyberattacks. In the future, It will be challenging to do so without an anticipatory program. In my opinion, the development of such a program should take into account both quantitative statistical analysis that can be obtained using only a set of data and any available contextual information. And if one asked me which of these factors I would rely on more, I would most likely answer that on the second.

7.3 Future work

The main stumbling block that constantly hindered me from conducting this study thoroughly was the confidentiality of the information I had the honor to work with. Accordingly, such a scale of an investigation, which was planned from the beginning of this work, requires data that would describe every threat recorded by Ukraine's systems. Still, it is not yet possible to disseminate in public because of security concerns. Therefore, later, due to the indefinite time when it will be publicly available, it will be possible to reconduct the research using this dataset. It is worth mentioning that the Russian-Ukrainian hybrid war, both in its physical part and in cyberspace, can quickly become a fascinating case for research to form a strategy to protect Ukraine in the future and an example to review and update such methods in other countries.

Bibliography

[1] Ukrainian. URL: https://www.facebook.com/UACERT.

[2] *8 Most Common Types of Malware Attacks*. URL: https://arcticwolf.com/resources/blog/8-types-of-malware. (21.10.2021).

[3] *About CWE*. URL: http://cwe.mitre.org/about/index.html. (13.03.2021).

[4] *Advanced persistent threat (APT)*. URL: https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.

[5] *Better scan results with CVSS, CVE and CWE*. URL: https://www.acunetix.com/blog/articles/better-scan-results-cvss-cve-cwe/. (05.05.2014).

[6] *Current CVSS Score Distribution For All Vulnerabilities*. URL: https://www.cvedetails.com/cvss-score-distribution.php.

[7] *CWE - 119 : Failure to Constrain Operations within the Bounds of a Memory Buffer*. URL: https://www.cvedetails.com/cwe-details/119/Failure-to-Constrain-Operations-within-the-Bounds-of-a-Memor.html.

[8] *CWE - 306 : Missing Authentication for Critical Function*. URL: https://www.cvedetails.com/cwe-details/306/Missing-Authentication-for-Critical-Function.html.

[9] *CWE - 404 : Improper Resource Shutdown or Release*. URL: https://www.cvedetails.com/cwe-details/404/Improper-Resource-Shutdown-or-Release.html.

[10] *CWE - 617 : Reachable Assertion*. URL: https://www.cvedetails.com/cwe-details/617/Reachable-Assertion.html.

[11] *CWE - 770 : Allocation of Resources Without Limits or Throttling*. URL: https://www.cvedetails.com/cwe-details/770/Allocation-of-Resources-Without-Limits-or-Throttling.html.

[12] *CWE - 79 : Failure to Preserve Web Page Structure ('Cross-site Scripting')*. URL: https://www.cvedetails.com/cwe-details/79/Failure-to-Preserve-Web-Page-Structure-039-Cross-site-Scr.html.

[13] *CWE - 94 : Failure to Control Generation of Code ('Code Injection')*. URL: https://www.cvedetails.com/cwe-details/94/Failure-to-Control-Generation-of-Code-039-Code-Injection-.html.

[14] *Cyberterrorism*. URL: https://en.wikipedia.org/wiki/Cyberterrorism.

[15] *Dataset of Cyberattacks on Ukraine*. URL: https://docs.google.com/spreadsheets/d/1_ylrIZm-jlRhTBjKKCcNqTHYJQEPXaRy6tuTOQZZHl0/edit?usp=sharing.

[16] *Dataset of Cyberattacks on Ukraine in dates (2022)*. URL: https://docs.google.com/spreadsheets/d/16P4ZtwuZ-8GQ-HzCNEYJRuyTTIQh0Gez6UJMB8OoNF0/edit?usp=sharing.

[17] *Dataset of Cyberattacks on Ukraine in numbers (2022)*. URL: https://docs.google.com/spreadsheets/d/1umli8r0jS2MCu2WhkHyD8Vjfzdp95JQp7a2eEZOElzg/edit?usp=sharing.

[18] Hannah Devereux. "Data-Driven Cyber Prediction in Hybrid Warfare". URL: https://prism.ucalgary.ca. (17.06.2019).

[19] *DNS amplification attack*. URL: https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/.

[20] ADAM HAYES. *Autoregressive Integrated Moving Average (ARIMA)*. URL: https://www.investopedia.com/terms/a/autoregressive-integrated-moving-average-arima.asp. (12.10.2021).

[21] Gurminder Kaur Jaideep Singh Simarpreet Kaur and Goldendeep Kaur. "A Detailed Survey and Classification of Commonly Recurring Cyber Attacks". In: *International Journal of Computer Applications* 141.10 (2016), pp. 15–19.

[22] Nadiya Kostyuk and Yuri M. Zhukov. "Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?" In: *Journal of Conflict Resolution* 63(2) (2019), pp. 317–347.

[23] Andrzej Kozlowski. "Comparative analysis of cyber attacks on Estonia, Georgia, and Kyrgyzstan". In: *International Scientific Forum* 3 (2013), pp. 236–245.

[24] Yuchong Li and Qinghui Liu. "A comprehensive review study ofcyber-attacks and cyber security; Emerging trends and recent developments". In: *Energy Reports* 7 (2021), pp. 8176–8186.

[25] Bimal Kumar Mishra and Hemraj Saini. "Cyber Attack Classification using Game Theoretic Weighted Metrics Approach". In: *World Applied Sciences Journal 7 (Special Issue of Computer & IT)* (2009), pp. 206–215.

[26] Narcisa Roxana MOSTEANU. "Artificial Intelligence and Cyber Security – A Shield against Cyberattack as a Risk Business Management Tool – Case of European Countries". In: *INFORMATION SECURITY MANAGEMENT* 21.175 (2020), pp. 148–155.

[27] Carlie Porterfield. *Ukraine Postal Service Hit With Cyberattack After Selling Viral Anti-Russia Stamps*. URL: https://www.forbes.com/sites/carlieporterfield/2022/04/22/ukraine-postal-service-hit-with-cyberattack-after-selling-viral-anti-russia-stamps/?sh=1b42d0635e60. (22.04.2022).

[28] *Predicting cyber attacks: What are the best methods?* URL: https://www.triskelelabs.com/blog/predicting-cyber-attacks-what-are-the-best-methods.

[29] *Scoring CWEs*. URL: http://cwe.mitre.org/cwss/cwss_v1.0.1.html. (05.09.2014).

[30] Todd G. Shipley and Art Bowker. *Investigating Internet Crimes. An Introduction to Solving Crimes in Cyberspace*. English. 2014. Chap. 2. ISBN: 9780124078178.

[31] R. Shirey. *Internet Security Glossary*. URL: https://datatracker.ietf.org/doc/html/rfc2828. (May 2000).

[32] Urvashi Singhal, ed. *Difference Between Active And Passive Cyber Attacks Explained*. URL: https://dare2compete.com/blog/difference-between-active-attack-and-passive-attack. (02.02.2022).

[33] Всі новини. Ukrainian. URL: https://cip.gov.ua/ua/news.

[34] Довідкова інформація з питань діяльності CERT-UA за фактами впливу на стан кібербезпеки у 2022 році. Ukrainian. URL: https://cert.gov.ua/article/37121. (17.02.2022).

[35] ЗВІТ РОБОТИ СИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ. Ukrainian. 2021. URL: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf.

[36] Новини. Ukrainian. URL: https://cert.gov.ua/articles.

[37] ПЕРЕЛІК категорій кіберінцидентів. Ukrainian. URL: https://cert.gov.ua/recommendation/16904. (10.11.2021).

[38] *THE FIRST CYBERWAR IS NOW; WHAT IS CYBERWAR?* URL: https://geniusee.com/single-blog/what-is-cyberwar. (04.04.2022).

[39] *Thesis cyberattacks on Ukraine*. URL: https://github.com/sofiyahaletska/Thesis_cyberattacks_on_Ukraine.

[40] *Trust Exploitation Attack?* URL: http://www.orbit-computer-solutions.com/type-of-network-attack-trust-exploitation/. (09.11.2015).

[41] M. Uma and G. Padmavathi. "A Survey on Various Cyber Attacks and Their Classification". In: *International Journal of Network Security* 15.5 (2013), pp. 390–396.

[42] Kimberly Underwood. *The Plausibility of Forecasting Cyber Attacks. Experts examine if and how cyber attacks can be predicted.* URL: https://www.afcea.org/content/plausibility-forecasting-cyber-attacks. (30.10.2018).

[43] *What Is a Cyberattack?* URL: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.

[44] *What is a DDoS attack?* URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/.

[45] *What is a Smurf attack?* URL: https://www.cloudflare.com/learning/ddos/smurf-ddos-attack/.

[46] *What is Man in the middle Attacks ? Explained with Examples*. URL: http://www.orbit-computer-solutions.com/network-attack-man-in-the-middle-attacks/. (09.11.2015).

[47] *What Is Phishing?* URL: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html.

[48] *What is Port Redirection Attack?* URL: https://www.orbit-computer-solutions.com/port-redirection-attack/. (09.11.2015).

[49] *Wireless ad hoc network*. URL: https://en.wikipedia.org/wiki/Wireless_ad_hoc_network#cite_note-2.

[50] *Wireless Sensor Network (WSN)*. URL: https://www.geeksforgeeks.org/wireless-sensor-network-wsn/. (03.06.2021).

[51] *YARA Rules Guide: Learning this Malware Research Tool*. URL: https://www.varonis.com/blog/yara-rules. (17.05.2021).

[52] *Zero-day (computing)*. URL: https://en.wikipedia.org/wiki/Zero-day_(computing).