Cyber-attacks Scenarios Analysis

Serghei Ohrimenco[1], Valeriu Cernei[1], Eduard Ryzhkov[2]

[1] ASEM, Chisinau, Moldova
[2] DSU, Dnipro, Ukraine
osa@ase.md, valeriu.cernei@bsd.md, revord924@ukr.net

Abstract: The digital transformation, in all its aspects, is accompanied by a rapid growth of cyber threats and attacks on various critical infrastructure facilities. Some of cyberattacks target personal data, operations management processes, financial reporting results, etc., having as a final objective monetization of the results. Accordingly, there is a need for a complex and comprehensive analysis of information, which presents key aspects of cyber-attacks. The current paper presents the results of a study aimed to identify and analyze possible scenarios, stages and facets of cyberattacks, highlighting potential motives, goals, objects, means of attack, specific actions, as well as the final potential results of cyber-attacks.

Keywords: Cybersecurity, Attacks, Shadow Digital Economic, Cybercrime, Advanced Persistent Threat

1. Introduction

Cybercrime is a successful business. Reports of world technology and information security leaders confirm this fact. We present some of the analysis results, which are presented further. In 2016, Cybersecurity Ventures predicted that cybercrime would cost the world $6 trillion annually by 2021, up from $3 trillion in 2015.

If it were measured as a country, then cybercrime — which is predicted to inflict damages totaling $6 trillion USD globally in 2021 — would be the world’s third-largest economy after the U.S. and China.

Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined [1].

“In 2021, cyber criminals adapted their attack strategy to exploit vaccination mandates, elections and the shift to hybrid working, to target organizations’ supply chains and networks to achieve maximum disruption,” said Maya Horowitz, VP Research at Check Point Software. “The sophistication and scale of cyber-attacks will continue to break records and we can expect a huge increase in the number of ransomware and mobile attacks. Looking ahead, organizations should remain aware of the risks and ensure that they have the appropriate solutions in place to prevent, without disrupting the normal business flow, the majority of attacks including the most advanced ones. To stay ahead of threats, organizations must be proactive and leave no part of their attack surface unprotected or unmonitored, or they risk becoming the next victim of sophisticated, targeted attacks” [2].

Should we look into the future, global cyber-security predictions for 2022 [3], we state that the cyber space becomes a field for misinformation campaigns, and technology related threats, focused on mobile devises continue to grow. Accordingly:

1. Fake news 2.0 and the return of misinformation campaigns.
2. Supply chain cyber-attacks continue to grow, and governments will address the challenge.
3. The cyber 'cold war' intensifies.
4. Data breaches are larger scale and more costly.

Technology cyber-security predictions for 2022:

1. Mobile malware attacks increase as more people use mobile wallets and payment platforms.
2. Cryptocurrency becomes a focal point for cyberattacks globally.
3. Attackers leverage vulnerabilities in micro-services to launch large-scale attacks.
4. Attackers weaponize deep fake technology.
5. Penetration tools continue to grow.

2. Literature Survey

Among the many specialized sources, we consider important to mention the "classic" work of Adam Shostack "Threat Modeling. Designing for Security" [4]. The work contains is focused on modeling threats for the Windows operating system. This is one of the works, which provides an approach to threats description and modeling. A list of key threats is proposed and their analysis is carried out with the allocation of successive stages: Mitigating threats; Eliminating threats: Transferring threats: Accepting the risk.

A number of interesting works have been presented in the recent years. Among them are such as "Threat Modeling. A Practical Guide for Development Teams" [5] (overview of threat modeling, the future of threat modeling methodologies, automation, and Agile development methodologies and etc.) "An Introduction to Cyber Modeling and Simulation" [6] (An Introduction to Assessment and Maturity Frameworks (including DevOps automation, Technical and Operational Scenarios), "Mental Modeling Approach. Risk Management Application Case Studies" [7] (Overview of Mental Modeling Research Methodology, Key Benefits of Mental Modeling, Mental Modeling Core Technique, Key Steps in the Mental Modeling Process), Foundations of Multi -Paradigm Modeling for Cyber-Physical Systems (Multi-Paradigm Modeling for Cyber-Physical Systems, Unifying Framework for Modeling of Physical Systems, Petri Nets [8]) and others.

3. Cyberattacks key characteristics

Cyberattacks are evolving from the perspective of targets, how they affect organizations, and the methods used. Improving cybersecurity protection can unlock economic value by reducing the cost of cybercrime and opening up new revenue opportunities. By understanding where they can gain value in their cybersecurity efforts, leaders can minimize the consequences and even prevent future attacks. By prioritizing technologies that improve cybersecurity protection, organizations can reduce the consequences of cybercrime and unlock future economic value as higher levels of trust encourage more business from customers.

Improving cybersecurity protection can decrease the cost of cybercrime and open up new revenue opportunities.

According to Bissell et al. (2019) [9], the three steps to unlocking the value in cybersecurity are as follows:

1. Priorities protecting people-based attacks: countering internal threats is still one of the biggest challenges with a rise in phishing and ransomware attacks, as well as malicious insiders.

2. Invest to minimize information loss and business disruption: already the most expensive consequence of cyberattacks, this is a growing concern with new privacy regulations such as GDPR and CCPA.

3. Target technologies that reduce rising costs: use automation, advanced analytics, and security intelligence to manage the rising cost of discovering attacks, which is the largest component of spending.

4. Targeted cyberattacks analysis.

The history of attacks on information systems dates back several decades. It started with the spread of computer viruses. Over time, cyberattacks have changed significantly in terms of the tools used, penetration methods, etc., and currently represents a serious weapon of attack against governments, commercial organizations, as well individuals.

The Table 1 below presents a classification of cyber security threats.

Table 1. Classification of Cyber Security Threats

Target application	Findings and Contributions
Wireless sensor networks	Categorized the security threats into three levels are: data security level (anonymity and freshness), access security level (accessibility, authorization and authentication) and network security level
Information systems	Established a hybrid model for classifying the security threats for information systems. They classified the security threats into three types: human threats, technological threats and environmental threats
Smart grid	Classified the security threats of smart grid into technical and non-technical resource threats. Technical threats was categorized into three types of threats are infrastructure threats, technical operational threats and system data management threats. While non-technical threats were classified into environmental threats and governmental threats
Wireless sensor networks	Classified the attacks that could occur in all layers from application layer to physical layer. For example, at the application layer level, a malicious attack can be added along the communication link to generate fake messages and data in order to attack the ongoing communication and increase the data collision. The attack in transport layer happen through sending unlimited connection request in order to minimize the node's energy and exhaust its resources and this lead to denial of service. Other attack can be occurred in a network layer in several forms such as spoofing, sinkhole, flooding and replay attack in order to create and send fake messages or causing congestion in the network. Jamming attack at the Data link layer can cause loss of signals and data and destroy the channel and

	increased interference. At the physical layer level, the attacker can allow unauthorized nodes to access to the network and damage it
Cloud computing	Categorized the security attacks and threats on cloud computing into four levels: authentication Attacks, side Channel Attacks, cloud Malware injection attack and Denial of Service (DoS) attacks
Mobile edge computing	Classified the security threats of mobile edge computing five assets are: (1) Network infrastructure threats such as man in the middle and denial of service attack, (2) Edge data center threats such as physical damage, privacy leakage, privilege escalation and service manipulation, (3) Virtualization infrastructure threats such as denial of service, misuse of resources, privacy leakage and privilege escalation, (4) core infrastructures threats such as privacy leakage, service manipulation, rogue infrastructure and (5) User devices such as injection of information and service manipulation
Blockchain technology threats	Divided the security threats for blockchain technology into five categories are: (1) Double spending threats, (2) Mining/Pool threats, (3) Wallet threats, (4) Network threats such as DDoS attack, and (5) Smart contracts threats
Cyber security threats	Classified the common cyber security threats by using mapping study, which include phishing, denial of service (DoS), injection attack, man-in- the-middle attacks, session hijacking, SQL injection attack and malware
Classification of RFID attacks	Classified threats associated with Radio Frequency Identification systems. They distinguished attacks in the physical layer, network transport layer, application layer, strategic layer, and multilayer
Social engineering malware	Social engineering malware is both pervasive and persistent. Emphasized the importance for organizations to develop a shared social responsibility to combat social engineering malware and not solely on technical solutions. Social engineering malware proliferation through a variety of infiltration channels such as e-mail, social software, websites, and portable media
Social engineering semantic attacks	Introduced a structured baseline for classifying semantic attacks by breaking down into components and identifying countermeasures

Sourse: Yassine Maleh, Youssef Baddi, Mamoun Alazab, Loai Tawalbeh, Imed Romdhani (2021). Artificial Intelligence and Blockchain for Future Cybersecurity Applications.
ISBN 978-3-030-74575-2, https://doi.org/10.1007/978-3-030-74575-2 [10]

Majority of security experts and analysts split targeted cyberattacks (Advanced Persistent Threat (APT) into a separate class. A feature of targeted attacks (APT) is that attackers are interested in a specific government organization, company or individual.

Targeted attacks are usually well planned and include several stages – starting with passive information gathering and analysis, to systems penetration and evidence destruction. Because of a targeted attack, attackers gain access to the victim's infrastructure and remain undetected for months or even years. During all this time, they have access to corporate information.

According to the well-known consulting firm A.T. Kearney, the main targets of such attacks are the following [11]:

- Companies' Head Offices. Often the equipment is not adequately protected from physical damage (for example, by cleaning or maintenance personnel).

- Research & Development. Usually this department requires the highest level of protection. Companies' knowledge is generated and concentrated there. However, it is often no better protected than other departments.

- Data centers. They provide secure environments for hosting private clouds. The problem is to ensure secure functioning of numerous servers, as well as applications running on these servers.

- Supply Chain. With the increasing use of networked solutions in dealing with suppliers, there are risks associated with the fact that relatively small supplier companies are usually less protected.

- Cloud computing. Basically, providers are responsible for security of cloud environments. In addition, this is a potential problem. Cloud services providers protect only in the case of SaaS services. All other models (IaaS, PaaS) remain to be the responsibility of the service beneficiary. Another point is the fact that the level of data protection depends on the specific adopted law in each country.

- Production systems. Many legacy specialized systems (e.g. SCADA) are increasingly being connected in networks. These are difficult to monitor and control. Attacks by intruders in this case can lead to production losses or even to collapse of a company or even an entire industry (e.g. Critical Infrastructure).

- Databases provide secure storage of important information. Main worries are that hackers can use administrators as "tools" to break into databases.

- Office networks. Offices, systems and PCs are interconnected, which provides many opportunities for network penetration.

- Sales. Leakage of marketing plans, pricing and customer information may lead to reputation loses as well as loss of competitive advantages.

- Mobile devices. If unsecured, sensitive data from a mobile phone can be easily stolen by hackers. One of the basic principle in using mobile devices is to avoid using personal devices for fulfilling job duties.

- Online stores. Use of stolen credit cards data and/or personal data are main tools applied by hackers.

- Phone calls. By exploiting people's willingness to help each other, attackers can use phone calls as a way to easily get the information they need, including financial data, passwords, personal information, etc.

We further present an overall attacks classification which is focused on mobile platforms [10] (Table 2).

Table 2. Attacks Classification which is Focused on Mobile Platforms

Cyber security attack	**Description**
Access attack	Allow unauthorized users access to the network or devices such as smart phones with no right to access
Reconnaissance attack	Attack allows an attacker to capturing, discovering and mapping of system vulnerabilities such as scanning traffic network, network ports and IP address information
Physical attack	This type of attack aims to tamper with hardware devices, for example some technologies such as IOT devices operate in outdoor environments may highly susceptible to physical attacks
Denial-of- service (DoS) attack	Denial-of-service (DoS) attack allow the attacker to make the network or device services unavailable to its intended users due to several reasons such as limited computation resources and low memory capabilities. This make mobile platforms are vulnerable to DOS attack
Attack on privacy	Attack on privacy through using remote access methods and malware to spy or stole sensitive information of users or organizations. Privacy protection in mobile devices has become increasingly challenging due to share large amount of information between mobile devices
Password- based attack	Attackers in two ways can do password- based attack: (1) brute force attack by using cracking tools to guess the correct password in order to access valid password, (2) dictionary attack depends on trying several letters and numbers to guess user passwords
Supervisory Control and Data Acquisition attack	Supervisory Control and Data Acquisition attack using malware such as Trojan to take control of the system. Mobile applications are vulnerable to many cyber-attacks like Trojan virus
Spoofing attack	Spoofing attack is based on obtaining the IP address of the devices to attack the users through enabling attackers to access users' confidential data and use it for malicious purposes
Botnet attack	Botnet attack is based on a collection of Internet-connected devices that have been breached and ceded to a malicious device known as botnet controller. The botnet controller able to direct malicious activities in order to damage the network or exploit users and data for materialistic gain
Sybil attack	Sybil attack is a threat in which attacker attempt to obtain identity of honest user, pretend as a distinct user, and then attempt to create relationships with honest users. If the attacker is successful in compromising one of the honest users, he will gain unauthorized privileges that help in the attacking process

From the perspective of its life cycle, a cyberattack can be split into 4 Stages [12,13]:

1. Preparation - the main objective of the first phase is to find the target, collect enough detailed private information and analyze it. Based on the information analysis, identify weaknesses in the infrastructure, build an attack strategy, select available hacking tools or develop exploits. Typically, the attack strategy will be thoroughly tested in order to ensure non-detection measures.

2. Penetration - the active phase of a targeted attack. Social engineering techniques and zero-day vulnerabilities are applied to initially compromise the target and conduct internal diagnostics. Additional malicious code or special settings are being applied when the ownership of the compromised host (server/workstation) is done.

3. Distribution – the objective is to extend hacker's control as much as possible by inspecting the IT environment and adding new unauthorized code through control centers.

4. Achieving the goal is the key phase of a targeted attack. Depending on the final objectives and chosen strategy, it can be theft of classified information; deliberate change of classified information; manipulation of the company's business processes and so on.

A mandatory activity is to, at every stage, to hide traces and evidence of a targeted attack. It often happens that cybercriminals create "Points of Return", allowing them to return in the future.

There are sources, [14] which split the life cycle of an attack into 6 stages, including:

1. The cyber-criminal, or threat actor, gains entry through an email, network, file, or application vulnerability and inserts malware into an organization's network. The network is considered compromised, but not breached.

2. The advanced malware probes for additional network access and vulnerabilities or communicates with command-and-control (CnC) servers to receive additional instructions and/or malicious code.

3. The malware typically establishes additional points of compromise to ensure that the cyber-attack can continue if one point is closed.

4. Once a threat actor determines that they have established reliable network access, they gather target data, such as account names and passwords. Even though passwords are often encrypted, encryption can be cracked. Once that happens, the threat actor can identify and access data.

5. The malware collects data on a staging server, then exfiltrates the data off the network and under the full control of the threat actor. At this point, the network is considered breached.

6. Evidence of the APT attack is removed, but the network remains compromised. The cybercriminal can return at any time to continue the data breach.

5. Cybercrime Attackers Taxonomy

There are many hacker categories; these categories include different terminology that create controversy over the computer attacker terms. Many of hackers' activities cannot be considered as illegal. We have to distinguish hackers who commit crimes and cybercriminals. The difference rests upon their attitudes and the motives [22-24].

The proposed taxonomy is based on technical experience, behavior, motivation and the level of moral development and is split into seven categories:

- Script Kiddies (SK) - the least skilled and youngest members using the tools created by elite hackers, who run precompiled software to harm individual users, systems and networks.
- Cyber-panks (CP) – these people have disrespect for Governments. They disregard social and moral norms. Recognition offered by peers and the society represent key drivers.

- Haktivists (H) – the name “hacktivist” sounds more respectful for themselves than calling criminals. These actors tend to justify their destructive behavior, including defacing websites, by labeling them as civil activists and attributing to their actions political and moral correctness.
- Thiefs (T) – this group targets information systems for financial gain. They will be focused on illegal collecting of credit card and bank account numbers that can be used for immediate personal gain. This group can accurately be called “light” criminals, as their actions are usually not sophisticated.
- Virus Writers (VW) – this category includes both, technically trained and beginner actors. This category combines four subcategories, namely: teenager, college student, adult and former virus writer. Viruses still form a very profitable segment of the crime software market.
- Cyber terrorist (CT) – members of this group may be part of military or paramilitary forces of a nation. They may be seen as “soldiers” or “freedom fighters” in the new cyberspace. Their activities are associated with the commission of terrorist acts in the cyberspace.
- Professionals (P) / Elite – They have the knowledge and skills of the highest level. This is the most elite of the cybercriminal groups. This status can be gained by a particularly famous exploit, hack or longevity on the scene. Representatives of this group may be involved in sophisticated scams or corporate espionage. They will sell confidential information and intellectual property for the highest price. Only limited information is known about this underground group as they use strict anonymity to hide their activities. The criminal activity is associated with day-to-day work.

In [15], the model includes eight main categories: 1. Novice (NV), 2. Cyber-punks (CP), 3. Internals (IN), 4. Petty Thieves (PT), 5. Virus Writers (VW), 6. Old guard hackers (OG), 7. Professional criminals (PC), 8. Information Warriors (IW).

Taking into account the motivation of criminals, cybercrime can be conditionally divided into the following categories:

- cyber fraud with a final objective to steal funds;
- cyber fraud a final objective to steal information (for own use or for subsequent sale);
- information systems disruption in order to gain control (for deliberate damage for a fee or to damage competitors);
- Other crimes.

6. A new segment – cloud computing

One of the new targets for cybercriminals is the cloud computing (CC) environments. The cloud computing technology in used not only for optimizing investments, better accessibility, less risks, increased collaboration, etc., but also hackers, spammers, and scammers use criminal software (Crimesoftware-as-a-Service) to access resources, fulfill their computing needs, organize a set of attacks on a competitor's resources, or develop new malicious technologies [16-18].

Hackers exploit benefits of cloud technologies as well. They do not need to invest heavily in building their own computer networks of information resources with high bandwidth. All these services are provided through cloud computing at a low cost. By developing and using criminal software as a commercial product (Software-as-a-Service) to gain access to resources, they are able to organize sets of attacks on the resources of a competitor or develop new malicious technologies.

Using the cloud computing environments facilitates realization of attacks as distributed denial of service (DDOS), password decryption (password decryption), hash cracking, organize activities related to shadow economy (e.g. drugs/arms/malicious software trafic) etc. It should be noted that there are automated technologies aloowing to plan and conduct DDoS attacks, Port Scanning, Flooding Attack DNS attacks, Sniffer attacks, Prefix Hijacking, IP Address reuse, IP Spoofing, Fragmentation Attack, Deep Packet Inspection, Active and Passive Eavesdropping, and so on.

Gaining access to the cloud-computing environment by simply passing the registration process enables easy distribution of criminal products and services. As it was mentioned earlier, this environment is also used as a commercial platform and distribution of malicious products (e.g. viruses, trojan horses, keyloggers, ransomware, botnets, etc.). Subscribed users get access to functionalities allowing distribution of protected archive files, they get guarantees for the performance of certain applications, get acquainted with the reviews of other users and so on.

7. Conclusion

The threats forms and composition is constantly changing and a constant increase in the number of negative cyber impact is expected.

One of the main threats is the COVID-19 pandemic, which has revealed many problems related to remote user access and "home" work. First, these are information security risks - connecting personal computing devices to information networks. Once the COVID-19 [19-21] problem spread all over the world, phishing activities grew significantly. Remote access devices, not prepared and configured to face the new reality, have become themselves additional threats. The goals of cybercriminals have changed - if earlier financial organizations were considered as main targets of cyberattacks, during the pandemic there was a shift. Hackers understood that by compromising end users, they can easier target government organizations, industrial enterprises, the energetic sector, medical institutions and so on.

References

1. Steve Morgan (2021). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
2. Check Point Software 2022 Cyber-security Predictions also anticipates an increase in supply chain attacks in the new year. https://blog.checkpoint.com/2021/10/26/deepfakes-cryptocurrency-and-mobile-wallets-cybercriminals-find-new-opportunities-in-2022/
3. Cybercrime predictions for 2022: Deepfakes, cryptocurrencies and misinformation. https://www.weforum.org/agenda/2021/11/2022-cybercrime-predictions-checkpoint/
4. Shostack A. (2014). Threat Modeling/ Designing for Security. John Wiley & Sons. ISBN: 978-1-118-81005-7
5. Izar Tarandach, Matthew J. Coles (2021). Threat Modeling. A Practical Guide for Development Teams. O’Reilly Media .ISBN 9781492056553
6. Jerry M. Couretas (2019). An Introduction to Cyber Modeling and Simulation. John Wiley & Sons. ISBN 9781119420835
7. Matthew D. Wood, Sarah Thorne, Daniel Kovacs, Gordon Butte, Igor Linkov (2017). Mental Modeling Approach. Risk Management Application Case Studies. Springer Science+Business Media. ISBN 978-1-4939-6616-5 DOI 10.1007/978-1-4939-6616-5
8. Paulo Carreira, Vasco Amaral, Hans Vangheluwe (2020). Foundations of Multi-Paradigm Modelling for Cyber-Physical Systems. ISBN 978-3-030-43946-0 https://doi.org/10.1007/978-3-030-43946-0
9. Kelly Bissell, Larry Ponemon (2019). The Cost of Cybercrime. Ninth Annual Cost of Cybercrime Study Unlocking the Value of Improved Cybersecurity Protection. https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

10. Yassine Maleh, Youssef Baddi, Mamoun Alazab, Loai Tawalbeh, Imed Romdhani (2021). Artificial Intelligence and Blockchain for Future Cybersecurity Applications. ISBN 978-3-030-74575-2 https://doi.org/10.1007/978-3-030-74575-2
11. Advanced persistent threat (APT): Targeted or targeted attacks, ttps://www.tadviser.ru/index.php/Статья: APT_Таргетированные_или_целевые_атаки
12. Advanced persistent threat (APT). https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/
13. Advanced Persistent Threat (APT) Attacks. https://www.cynet.com/network-attacks/advanced-persistent-threat-apt-attacks/
14. Anatomy of Advanced Persistent Threats. https://www.fireeye.com/current-threats/anatomy-of-a-cyber-attack.html
15. Marcus K. Rogers (2005). The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach. CERIAS Tech Report 2005-43
16. Malte Ackermann (2021). Mobility-as-a-Service: The Convergence of Automotive and Mobility Industries. ISBN 9783030755898
17. Peter Elger, Eoin Shanaghy (2020). AI as a Service: Serverless machine learning with AWS. Manning Publications. 9781617296154
18. Enrique Castro-Leon, Robert Harmon (auth.) (2016). Cloud as a Service: Understanding the Service Innovation Ecosystem. Apress. ISBN 9781484201046
19. Adrian T. H. Kuah, Roberto Dillon (2021). Digital Transformation in a Post-COVID World. Sustainable Innovation, Disruption, and Change. CRC Press. DOI: 10.1201/9781003148715
20. Levi West (2020). The Coronavirus Cybersecurity Survival Guide. Top Tips to Protect You from A Cyber Attack.
21. Robert Slade (2021). Cybersecurity Lessons from CoVID-19. CRC Press. ISBN: 978-1-003-13667-5
22. Ben Buchanan (2020). The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics. Harvard University Press. ISBN 9780674246010
23. Clement Guitton (2017). Inside the Enemy’s Computer Identifying Cyber Attackers. Oxford University Press. ISBN: 9780190699994
24. Akashdeep Bhardwaj, Varun Sapra (2021). Security Incidents & Response Against Cyber Attacks. ISBN 978-3-030-69174-5 https://doi.org/10.1007/978-3-030-69174-5