## Cyber Security Threats, Attacks and Vulnerabilities in Enterprises

Podeanu Stefania Adriana

Departament of Computer Science,

Information Tehnology,

Mathematics and Physics

**Abstract**

This article is about the threats, attacks and vulnerabilities encountered, both in general and for small and medium organizations, highlighting the problems they face, the most important being the very rapid development of cyber security, the lack of resources and sufficient documentation, the impact of the pandemic on this area.

The analysis showed an increasing trend towards documenting resources, reports and studies compared to previous years, but also an increasing tendency for companies not to report incidents they are facing.

Communities should address a range of techniques and strategies that are up to date with current trends in attacks. On the other hand, information and resource writing in this area should be encouraged.

**Keywords:**

**Cyber security; Threats; Vulnerabilities; Attacks; Industry;**

1. **Introduction**

Cyber security has particularly developed in recent years after the pandemic triggered at the end of 2019, it has had a major impact in the emergence of new vulnerabilities and attacks on industry and other areas of major importance. Businesses and individuals have not been spared either. Organizations being more susceptible to attacks as opposed to individuals.

According to the ENISA report from 2021[1] and the article "A Comprehensive Review Of Cyber Security Vulnerabilities Threats, Attacks and Solutions" attacks have increased due to two major changes: remote working ("the transition from traditional infrastructures to online and cloud-based solutions"), and another major factor was the interconnectivity and exploitation of new emerging technologies for example: Artificial Intelligence or Large Language Models.[1][4]

Targeted infrastructures were:Social media, smart grid, mobile applications. Industrial control systems, network, distributed system, cloud applications, multiple VLANs.[3].

We can observe an increasing tendency towards analysis, documentation and solution of certain groups of attacks and vulnerabilities present in small and medium enterprises, as well as in other sectors of activity, as evidenced by a brief analysis in the report "Cyber Security Threats and Vulnerabilities: A systematic Mapping Study, where different rankings and classification of resources found on this topic are addressed. One of the most representative rankings is done by countries that provide documentation, reports, studies or research, the top 5 countries with the highest frequency are: USA (16%), India (16%), China (14%), Canada and Australia (4.5%), being taken into account the countries of origin of the first contributors, another aspect is the frequency of publications appearing before 2019, these have an increase up to 17% compared to previous years[3].

The analysis of the resources found in this report showed an unequal distribution of studies, experiments and simulations of attacks, with experimental studies ranking first with a frequency of 46% and a percentage of 59% compared to the second place simulations which have a frequency of 28% and a percentage of 36%. Case studies were last with a frequency of 4% and a percentage of 5%[3].

As there are very few publications that provide information about protecting, combating and resolving attacks and vulnerabilities we can realize that documenting and analyzing them is still in an early stage.

Another point to consider is represented by the top types of attacks from the study "Mind Your Own Business: A Longitudinal Study of Threats and Vulnerabilities in Enterprises" where the most frequently found attacks are documented, among which the most mentioned are: malware and PUP (Potentially Unwanted Program), ransomeware.[5]

Hardware, bug-based or network failures that have irregularities can have various causes such as: bad validation data, problems with user access control, incomplete or incorrect authentication, migration of problematic files; buffer overflow; problems caused by Structured Query Language (SQL), Cross-site scripting (XSS), use of components with vulnerabilities; failures with online services and APIs; inadequate testing of security systems.

1. **OSI model and layer attacks**

In terms of attacks, they have been categorized in several categories and OSI model.

Pentru fiecare nivel au fost identificate ca de exemplu: Application Layer putem vorbi de DoS,DDoS,SMTP, FTP bounce, insecure http, browser hijacking, buffer overflow, malware, atacuri de date. DoS fiind unul dintre cele mai populare atacuri la acest nivel în anul 2019. Presentation Layer prezinta atacuri de manipulare a Secure Socket Layer malformate, SSL Stripping și CCS (Change Cipher Specification). La Session Layer avem session hijacking și strealing seesion ID.Transport Layer implica atacuri precum TCP flooding attack,UDP flooding attack și TCP sequence prediction attack.TCP flooding fiind cel mai recunoscut pe internet. La nivelul Date din modelul OSI putem sa amintim cele mai comune atacuri cum ar fi: Atacuri MAC (forțează un switch să funcționeze ca un hub pentru a trimite pachetele către toate porturile), atacuri STP (forțează Bridge Protocol Data Unit sa schimbe mesajele în topologia Spanning Tree) si atacuri ARP poisoning. Physical Layer au fost prezente atacuri precum wiretapping, jammping si tampering.[4]

1. **Threats si Vulnerabilities**

Current technologies have a wide range of threats, the most recognized being: viruses, Trojans, Rootkits, Worms, Hackers and predators. Organizations have been dealing with these since the earliest technologies and it is still present today, thus 48% of companies have seen a significant increase in threats[2].

Another important aspect is that despite the major external threats they are also facing internal vulnerabilities and threats that derive from existing software, on the other hand 44% of companies have reported an incident in the last 12 months, and data loss is also targeted with 10% of organizations being victims of sabotage or fraud.

A at first glance comparison of the two reports shows that PUPs and malware claim the top threat to small and medium sized businesses, with PUPs having a greater impact than malware.

Malware affected between 10-34% of hosts and between 87-96% of organizations, as opposed to PUPs which recorded between 87-89%.[5]

On the other hand, another report from which came out threat classifications, the first places are occupied by sending files, social networking, personal emails.

From all this we can realize that attacks on organizations are targeted on teams or people who do not have sufficient training in the field of vulnerabilities and threats, leaving the business environment, one easily compromised using social engineering techniques.

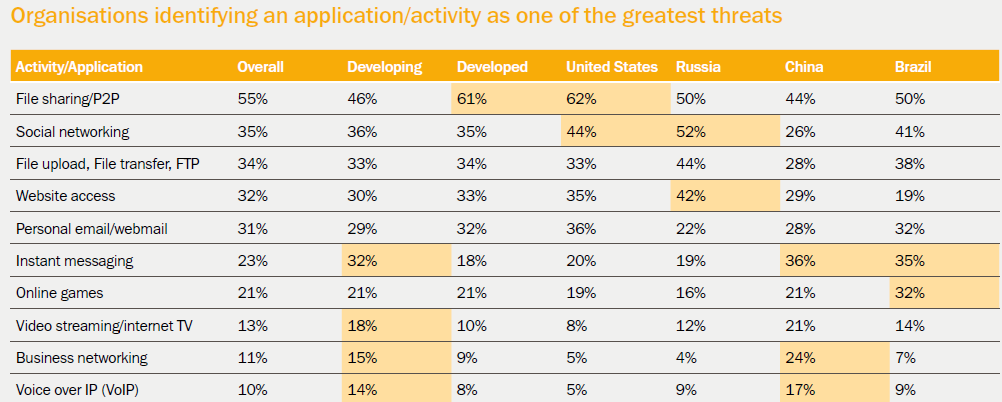
****

Fig 1. Organizations identifying an application/activity as one of the greatest threats.[2]

**IV. Industries affected**

The most affected industries are represented in the figure below:

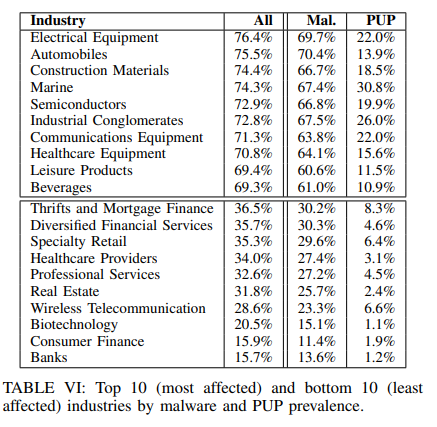


Fig 2.Top 10 (most affected) and bottom 10(last affected) industries by malware and PUP prevelance.[5]

It can be observed that malware has a higher success rate than PUPs, and at the same time, both threats represent a significant percentage in all 10 listed industries. According to this study, ransomeware attacks and threats are not avoided either, from this family the most used ones are wannacry, locky, petya[5].

Vulnerabilities in software systems are also being targeted by attackers, the most significant being client-side vulnerabilities in applications and frameworks such as .NET, Adobe Air, Adobe Reader, Chrome, Firefox.[5]

1. **Conclusion**

Both threats, attacks and vulnerabilities are becoming more widespread every day.

Organizations lack clear strategies to combat or protect against possible attacks, making them a safe target for attackers.

The documentation, research and inclusion of companies in studies and reports is an important step in the development of cyber security, but these are still in a developmental stage because from traditional infrastucture to online, the use of remote working and the emergence of artificial intelligence or LLMs have had a direct impact.

This study aimed to encourage the documenting and writing of resources for this area of major importance, as there was not enough resources in terms of firms' approach to strategies to combat and prevent possible attacks or threats.

**References**

1. (2021). *ENISA THREAT LANDSCAPE 2021.*
2. Costin Raiu, S. T. (2013). *The-Kaspersky-Lab-Global-IT-Risk-Report\_Kaspersky-Endpoint-Security-report.* Kaspersky.
3. Mamooma Humayun, M. N. (2020). *Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study.*
4. Omer Aslan, S. S.-O. (2023). *A Comprehensive Review Of Cyber Security Vulnerabilities Threats, Attacks and Soutions.*
5. Platon Kotzias, L. B.-A. (2020). Mind Your Own Business:A Longitudinal Study of Threats and Vulnerabilities in Enterprises.