SECURITY ACADEMY
EDUCATIONAL PROGRAM ORGANIZED BY
EUROPEAN VALUES CENTER FOR SECURITY POLICY
IN COOPERATION WITH STRATPOL AND SSPI INSTITUTES

Emerging trends of cybersecurity threats

DÁŠA SEDLÁKOVÁ

Author:

Dáša Sedláková

Proofreading:

Matúš Jevčák
Marián Maraffko
Michaela Ružičková

The views and statements expressed in this document do not represent the official opinions of the donors or organizers of the Security Academy. The content of this document is a responsibility of the author.

EMERGING TRENDS OF CYBERSECURITY THREATS

Dáša Sedláková

Abstract

The cyber security industry advances every day and so do cybercriminals. With every security measure deployed, there happens to be another weak spot that needs to be addressed next as it might get exploited. Security professionals are constantly trying to keep up with attackers and ensure basic security requirements such as confidentiality, integrity and availability for businesses, public services, and individuals. The true challenge comes from an unknown range of possible cyber security threats and their vectors. Therefore, foresights can be given by observing and analysing recent trends of different cyber threats. Looking at the trends of cyber threat vectors, their forms, and targets and the trend of security measures on the other hand, can offer a beneficial overview into how cyber threats might evolve and form in the near future. These tend to be information that hold great value for security professionals and practitioners.

Keywords

cybersecurity; cyber threats; cyber-attacks; vectors

INTRODUCTION

The cyber security industry has been rapidly evolving over recent years. Cyber security professionals are implementing up-to-date security mechanisms to ensure confidentiality, integrity and availability of systems and data, and attackers are parallelly developing new techniques of how to bypass the existing mechanisms. Sometimes they manage to find a unique angle towards outflanking the protection and get what they intended. Such an angle is usually called a Zero-day, which can be exploited by a malicious actor without the target knowing about its existence. Another common scenario is the malicious actor leveraging the publicly known weakest point of all technology, which is a human factor or exploiting publicly known technological vulnerabilities. As the spectrum of possible attack vectors and their specific techniques is wide, it is challenging for security professionals to keep a step ahead of malicious actors. Thus, having an overview of certain trends within cyber security threats can be highly beneficial as it highlights areas that need the most focus.

TRENDS IN ATTACK VECTORS

The vast majority of people in the world use technology. Whether it is an individual seeking relaxation, socialization or information, private companies leveraging a huge spectrum of technology for business-related purposes, or a state providing services to its people. People were given the opportunity to choose which technology they want to use and how based on their preferences. But when it comes to how to use the technology, not all the users are fully aware of the amount of power the technology holds, and therefore might often act irresponsibly. Malicious actors know how to trick people by applying a technique called social engineering and often use this as an initial attack vector. Security professionals see a lot of social engineering attempts daily, especially as different forms of phishing or baiting. Phishing is an act of fraud when the malicious actor pretends to be someone trustworthy and tries to trick the victim into making a security mistake or providing sensitive information. In the early phase of phishing trend growth, the whole procedure was done through email communication. As the occurrence of this trend grows, as well as recently, malicious attackers are leveraging different communication platforms, such as voice calls, SMS, or WhatsApp messages. It can be expected that the trend of enlarging the communication media spectrum would continue to grow, for instance towards highly used Discord or TikTok platforms. Furthermore, over the last year, there was a noticeable improvement in the level of language, graphics, and overall quality the malicious actors have been presenting. The amount of energy and resources put into phishing campaigns leads to the belief this trend will persist and even develop in more sub-forms. Baiting is a form of social engineering when a malicious actor purposely leaves physical media with malicious content to be found and used by the victim. This leverages the victim's curiosity. In comparison to phishing, baiting is expected to lower its occurrences. Digitalization, cloud, and global pandemics are three important variables, which stand in a way of baiting to succeed. Social engineering is not the only attack vector, which is expected to remain its leading position as technical vulnerabilities stand by its side.

Technologies can be exploited by either human factors or their own technical vulnerabilities. Technical vulnerability means a weak spot, which is pre-built into technology's hardware or software. Users or administrators often cannot patch these weaknesses themselves and are dependent on a vendor to provide security patches or mitigations through updates. This can be tricky in cases the vulnerability is being actively exploited and there has been no patch provided by the vendor yet. In such cases, security professionals rely on generally well-deployed security measures. Typically, right after a certain vulnerability is publicly disclosed, independent people share exploits and proof of concepts on public web domains. The intent is to help security professionals understand the issue deeply and deploy measures as soon as possible. Malicious actors are aware of these procedures and often do not need to create exploits themselves, which makes these types of attacks quick and easy. Especially in case the vulnerability has been disclosed on a publicly accessible and widely used system, attackers are swift like never. A suitable example of such a case is the well-known Log4Shell set of vulnerabilities in Apache Log4j, which were publicly disclosed in December 2021. Apache is a widely used open-source web server usually used for publicly accessible services. These vulnerabilities meet the criteria for quick and easy targets, as was theorized before. All the concerns were at place when shortly after its disclosure, massive attacks targeting these vulnerabilities were spotted all over the world. It has been over two months since the mitigations and patches were published and there are still attempts for exploitation. Due to the simplicity of such attacks and the amount of publicly accessible details and exploits, technical vulnerabilities shall remain known as current threat vectors. What is believed to change are trends in specific attack types used by malicious actors as well as their targets.

TRENDS IN ATTACK TYPES

Cyber-attacks are often being categorized according to their nature. Few categories stand on the top of popularity over recent years and not many companies have succeeded to avoid them. (Distributed) Denial of Service, Malware, Brute force, or Web-based attacks are the favoured. Although, after observing recent trends it is expected they will not remain on the top unchanged, at least not all of them. (Distributed) Denial of Service is a form of cyber-attack when by a variety of means a state of interruption or complete unavailability of the targeted system is achieved. Depending on the targeted system, this can lead to financial loss, massive outages, or in certain cases injuries or even death. This undoubtedly is a serious threat. However, such threats have been known for more than 20 years, which makes them easy to understand. Vendors implement (D)DoS protection by default and security professionals deploy anti-DDoS mechanisms in the early stages of securing their technological environment. As a result of this, traditional (D)DoS attacks usually do not work as expected and need a certain level of intelligence added. This is where Artificial Intelligence or Machine Learning principles might be used, if (D)DoS attacks wish to keep their primacy. AI/ML might be deployed beside the traditional attacks for training on how does target protection mechanism work and how to bypass it. Lots of (D)DoS protection mechanisms are still built on signature-based methods, without any AI/ML components, which makes them vulnerable to more sophisticated attacks. Signature-based protection commonly blocks only what it recognises as malicious rather than correlating malicious patterns or seeking anomalies. (D)DoS attacks are not the only category, which shall not remain unimproved.

Any malicious software created for the purpose of damaging the targeted system falls under the Malware category, but not all are used at the same rate. Malware has been used by attackers for even longer than (D)DoS and yet, it still proudly stays at the top of its fame. The fear of success resides in malware's ability to leverage various techniques to intrude, stay steady for a while if needed and execute in the right moment. Successful malware may corrupt targeted systems and/or spread across the targeted infrastructure to cause greater damage. Nowadays, anti-malware solutions are considered basics and are deployed widely as a standalone solution or as a component, for instance in Operation System. The malware family react and actively seek its vulnerabilities. There has been a noticeable elevation in malware preferences by attackers observed daily over recent years. Traditionally, Trojan horses, viruses or worms had been spread widely. After anti-malware solutions started to be widely deployed and did stop the majority of malware, there was a need of leveraging current technology. Cryptography and Machine Learning principles were interconnected, and as a result, broadly utilized ransomware and crypto-jackers emerged. Ransomware aims for corrupting the targeted system or encrypting the data in it to get a ransom. Crypto-jacker on the other hand tries to stay undetected for as long as possible, utilizing the target machine's hardware to mine cryptocurrency. Attackers are observed to put much emphasis on techniques of intrusion, low-profile keeping and spreading, which results after successful exploitation in huge financial damage. In most cases, even after paying the ransom, the victim does not get the full data back. Moreover, a new trend of Ransomware may be observed nowadays – Ransomware as a hybrid threat. Ransomwares are not explicitly intended to collect ransom, rather to dig sensitive data, psychologically affect business decisions or to blackmail the victim. Unfortunately, not only business-related sectors tend to be the target, but possibly government-related, and healthcare services might also get involved.

Web-based attacks have slightly formed over recent years along with web services development, but their nature stays the same, containing the most popular attacks such as Cross-Site Scripting, Injection attacks or Traversal attacks. Security professionals are well-aware of these types of attacks and continually deploy appropriate protection mechanisms. Nevertheless, the majority of critical web systems is highly protected, attackers continue to conduct such attacks as they are easy to build up in comparison with for instance malware. The current trend of web-based attacks is they tend to be mostly untargeted and therefore harmless when proper protection is in place. On the flip side, in extraordinary situations for instance when a critical zero-day vulnerability is disclosed, the severity of web-based attacks rapidly rises. There are still a lot of potential vulnerabilities which are expected to be disclosed and exploited, therefore, security professionals shall not take web-based attacks lightly and be cautious. In contrast with mentioned attack types, some categories seem not to develop that much over recent years. Brute force attacks are still considered time-consuming and pose a high rate of noticeability. Although, the performance of attackers' machines did advance, so did protection mechanisms, which are deployed by security professionals. In addition, there is a strong common knowledge about basic security requirements such as how a strong password should look and why it is important to use multi-factor authentication. Attackers are expected to continue trying brute forcing, especially to exploit publicly accessible services, but it is assumed they will not succeed at a high rate. Looking at the trend of attack types and correlating them with trends in attack targets may provide even more relevant information of how severe certain threat is expected to be.

TRENDS IN ATTACK TARGETS

Generally said, anyone possessing a certain technology may become a victim of cybercriminals, even independent individuals. Lots of people argue with a statement about why there should be anyone interested in exploiting them, resulting in audacious and unaware behaviour. The counterargument can be the time we live in. The time when installing smart bulb may lead to the whole network exploitation and even physical damage. The time when incautious actions can lead to identity and money theft. The time when not knowing is not considered sufficient argument anymore. Besides numerous cybercrime targets, an often-underestimated trend underlies, which belongs to untargeted cyber-attacks. During such types of attacks, malicious actors usually intend to exploit as many targets as possible without knowing the details about them. It may seem random, but there is a certain trend, which can be observed. In terms of network traffic, regular reconnaissance attempts are being observed in the forms of port scanning and webserver querying. Reconnaissance is known as an initial phase of a complex cyber-attack, during which the malicious actor tries to gather as much relevant information about the target as they can. The information gathered is then being leveraged in later phasis of such attack. Within an untargeted attack, reconnaissance is considered a pure attempt to find vulnerabilities, which could be exploited in the following targeted attack. When no exploitable vulnerability is to be found, the attacker continues to scan other victims. From a user point of view, the trendiest untargeted attacks are spam and phishing, during which cybercriminals send huge amounts of tricky messages containing malicious URLs. Malicious actors believe that there is always a chance someone will get caught and typically sent them money, download malware, or provide them with sensitive information. The true risk of untargeted attacks resides in the attacker's ability to quickly shift the scope towards the chosen target when it is not expected the most. Except for general security practices and caution, there is only a little possibility for predicting such attacks. On the other hand, observing trends in targeted attacks may provide particularly helpful information.

Global Pandemics played a huge role in setting a trend of attacks towards remote employees. Remote access systems (VPN), not enough security mechanisms at home network and working from cafes all possess some level of risk. Furthermore, there was a little opportunity window at the beginning of global pandemics when employees went remote and certain companies were not prepared enough. Consequently, not only the private sector has been affected but there has been a noticeable rise of attacks headed towards the public sector. Few malicious actors did leverage the world's focus and conducted cyberattacks targeting critical infrastructure and reportedly by accident hitting even hospitals. Because of such attacks, some public agencies who thought they do not need to invest in cybersecurity protection found themselves wrong. This resulted in new deployments of cybersecurity mechanisms and therefore overall improvement of cybersecurity throughout the public sector. However, what has not changed yet is a general lack of talent, which is still a great challenge. The trend of the public sector being a target yet remains and even rises with the recent situation in Russia. The argument can be seen in a positive correlation of Russia attacking Ukraine and a new type of malware being spread, a notable increase in attacks targeting government-related systems in V4 countries and Anonymous publicly declaring targeted attacks towards the Russian government. Therefore, the emerging trend can be seen in threats headed towards the public sector, especially government systems and critical infrastructure. Critical infrastructure is seen as a strategic point, where high-security measures are hard to implement because of special operational requirements and Internet of Things (IoT) devices. On the other hand, a slightly positive trend is rising, which is independent hackers' group taking a political side.

CONCLUSION

Observing the recent evolution of cybersecurity threats can provide a beneficial insight needed for security planning and matching or even outrunning cybercriminals. Keeping in mind that cybersecurity threat is such a complex phenomenon, division, and more detailed elaboration of scopes of views is needed for exceptional understanding. When looking back to recent trends in initial attack vectors, a slight shift of social engineering scope can be expected in terms of leveraging current media dominances such as Discord or TikTok. The exploitation of technical vulnerabilities shall remain highly used is it is often quick and easy to conduct. Examination of recent attack types has indicated a trend of threats being intelligent to survive longer. Artificial Intelligence and Machine Learning principles tend to be implemented into well-known attack types such as (D)DoS or Ransomware to find their way through protection mechanisms. Beyond emerging trends, there is an expectation of brute-force attacks and web-based attacks not being so efficient. Especially, when put into context with untargeted cyberattacks. Findings from the analysis of the untargeted attacks highlight the objective to stay alert as cybercriminals constantly work their way through protection. Lastly, an emerging trend has been spotted in cyber threats headed towards the public sector, especially facing critical infrastructure and its Operational Technology infrastructure. Because of the persistent lack of talent, working cooperation between cybersecurity professionals is crucial.

LITERATURE

The Apache Software Foundation. (2022, February 23). Apache Log4j 2. Logging Services. Retrieved February 28, 2022, from https://logging.apache.org/log4j/2.x/

Národní úřad pro kybernetickou a informační bezpečnost. (2022, February 25). Upozornění Na Výskyt Nového Destruktivního Malware Typu Wiper. Retrieved February 28, 2022, from https://www.nukib.cz/cs/infoservis/hrozby/1813-upozorneni-na-vyskyt-noveho-destruktivniho-malware-typu-wiper/

SK-CERT. (2022, February 25). TLDR: Kybernetické útoky na Ukrajine a jedna otvorená databáza (7. týždeň). Retrieved February 28, 2022, from https://www.sk-cert.sk/sk/tldr-kyberneticke-utoky-na-ukrajine-a-jedna-otvorena-databaza-7-tyzden/index.html

Národní úřad pro kybernetickou a informační bezpečnost. (2022, February 25). NÚKIB v rámci preventivních kroků vydal v souvislosti s ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou Varování. Retrieved February 28, 2022, from https://www.nukib.cz/cs/infoservis/hrozby/1814-nukib-v-ramci-preventivnich-kroku-vydal-v-souvislosti-s-ozbrojenym-konfliktem-mezi-ruskou-federaci-a-ukrajinou-varovani/

Dayanandam, G., Rao, T. V., Bujji Babu, D., & Nalini Durga, S. (2019). DDoS attacks—analysis and prevention. In Innovations in Computer Science and Engineering (pp. 1-10). Springer, Singapore, Retrieved February 28, 2022, from https://link.springer.com/chapter/10.1007/978-981-10-8201-6_1

Milošević, N. (2013). History of malware. arXiv preprint arXiv:1302.5392, Retrieved February 28, 2022, from https://arxiv.org/abs/1302.5392

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry, 137, 103614. , Retrieved February 28, 2022, from https://www.sciencedirect.com/science/article/pii/S0166361522000094?casa_token=p9k_bCzBaLoAAAAA:GdgM7icLY9qOkMCCJWKzdVYDSfclfEoS1wym9aYeHsay0uXxfcOby136AH7uujAB4FX87omUjw

Williams, T. L. (2021). Cybersecurity: Zero-Day Vulnerabilities and Attack Vectors (Doctoral dissertation, Northcentral University), Retrieved February 28, 2022, from https://www.proquest.com/openview/a445c956560360bc48c393e0c03d900f/1?pq-origsite=gscholar&cbl=18750&diss=y