2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet) | 979-8-3315-4038-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/RoEduNet64292.2024.10722615

Advanced Persistent Threats

Alexandra Barcan
Software Development Department
Endava SRL
Craiova, Romania
bma.alexandra@gmail.com

Mircea Badoi
Software Development Department
NetDania SRL
Craiova, Romania
mircea.badoi@netdania.net

Gabriel Nedianu
Software Development Department
NetDania SRL
Craiova, Romania
gabriel.nedianu@netdania.net

Daniel Ciochiu
Software Development Department
NetDania SRL
Craiova, Romania
daniel.ciochiu@netdania.net

Claudiu Traistaru
Computer and Information Technology Department
University of Craiova
Craiova, Romania
claudiu.traistaru@edu.ucv.ro

Nicolae Enescu
Computer and Information Technology Department
University of Craiova
Craiova, Romania
nicolae.enescu@edu.ucv.ro

Abstract— This paper provides an in-depth exploration of Advanced Persistent Threats (APTs), introducing a detailed taxonomy of APT attack steps and presenting a hypothetical scenario to illustrate the process. The contributions include a comprehensive classification of APT attacks, a discussion on recent advancements in detection technologies, and potential defense strategies. Future work will focus on expanding these strategies and integrating more real-world case studies.

Index Terms— cyber security, advanced persistent threats (APTs), data exfiltration, zero-day vulnerabilities, cyber-attacks.

I. Introduction

In the contemporary digital landscape, where information technology forms the backbone of numerous essential services and sectors, the security of network infrastructures has become a paramount concern. The proliferation of interconnected devices, the rise of cloud computing, and the increasing dependence on digital communication have magnified the importance of safeguarding network environments from malicious entities. This necessitates a comprehensive understanding of network vulnerabilities, and the diverse array of attack methodologies employed by adversaries.

Network security encompasses a broad spectrum of practices, protocols, and technologies designed to protect the integrity, confidentiality, and availability of data and resources in a networked environment. At the core of this discipline lies the identification and mitigation of vulnerabilities—weaknesses within a system that can be exploited by attackers to gain unauthorized access or cause harm. Vulnerabilities can manifest in various forms, including software bugs, hardware flaws, configuration errors, and even human factors, each presenting unique challenges to security professionals.

II. Attack taxonomies importance and APTs

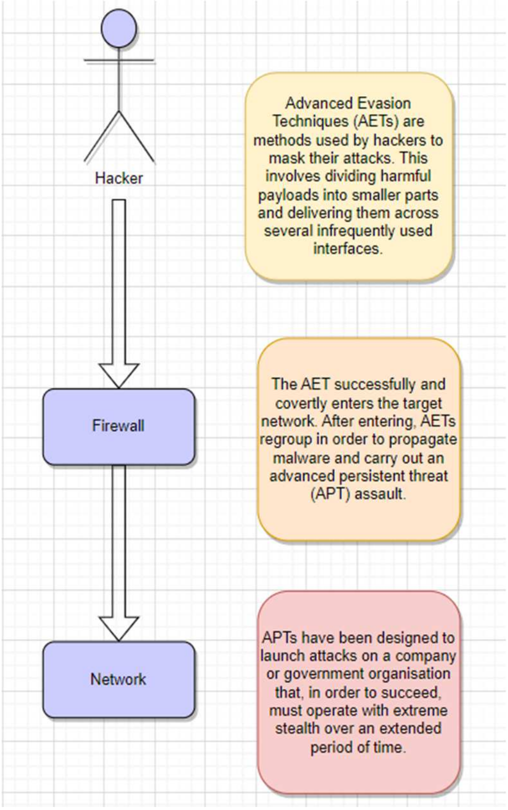
Hacker
Advanced Evasion Techniques (AETs) are methods used by hackers to mask their attacks. This involves dividing harmful payloads into smaller parts and delivering them across several infrequently used interfaces.
Firewall
The AET successfully and covertly enters the target network. After entering, AETs regroup in order to propagate malware and carry out an advanced persistent threat (APT) assault.
Network
APTs have been designed to launch attacks on a company or government organisation that, in order to succeed, must operate with extreme stealth over an extended period of time.

Fig 1 APT attack

To systematically address these vulnerabilities, it is crucial to categorize and understand the different types of attacks that can exploit them. This process is facilitated through attack taxonomies, which provide a structured classification of attacks, based on their characteristics, methodologies, and intended targets. These taxonomies serve as a foundational tool for security analysts, enabling

979-8-3315-4038-8/24/$31.00 ©2024 European Union

them to anticipate potential threats, develop effective countermeasures, and enhance the overall resilience of network systems.

Advanced Persistent Threats (APTs) refer to highly sophisticated and prolonged cyber-attacks that are typically orchestrated by well-funded and skilled adversaries. These adversaries often include nation-states, organized crime groups, and other highly organized entities. The primary objectives of APTs are to gain unauthorized access to networks, remain undetected for extended periods, and exfiltrate sensitive information or disrupt operations.

APTs are characterized by their complexity, stealth, and persistence. They employ a variety of tactics, techniques, and procedures (TTPs) to infiltrate, establish a foothold, move laterally within the network, and achieve their objectives.

III. CLASSIFICATION

Advanced Persistent Threats (APTs) represent sophisticated and targeted cyberattacks that often involve prolonged efforts to gain and maintain unauthorized access to a network. These attacks are typically carried out by well-funded adversaries, such as nation-states or organized crime groups. The methods used in APT attacks can be categorized into several stages, each employing specific tactics and techniques.

The initial compromise phase involves methods that attackers use to gain an initial foothold within the target network. Common techniques include spear phishing, where highly targeted emails are used to trick individuals into revealing credentials or downloading malicious attachments. Another method is watering hole attacks, which involve compromising a website frequently visited by the target organization, leading to the exploitation of vulnerabilities on visitors' devices. Supply chain attacks, where attackers infiltrate an organization through vulnerabilities in its suppliers or service providers, are also common, as is exploiting public-facing vulnerabilities in systems like web servers.

Once inside the network, APT actors employ various persistence mechanisms to maintain long-term access. This may involve installing backdoors that provide a persistent connection back to the attackers or stealing credentials to access different parts of the network over time. Other techniques include using rootkits, which are low-level software that hides the presence of malicious code, or leveraging legitimate operating system features, such as scheduled tasks, to periodically run malicious code.

After establishing persistence, attackers move laterally across the network to reach their ultimate targets, often high-value data or systems. This lateral movement can involve techniques such as pass-the-hash, where attackers use captured password hashes to authenticate as users and move between systems or abusing Remote Desktop Protocol (RDP) to move within the network. Weak network segmentation can also be exploited, allowing attackers to move freely between systems that should be isolated.

To carry out their objectives, APT actors often need to escalate their privileges within the network. This can be achieved by exploiting operating system vulnerabilities to gain higher-level access, dumping credentials from memory or storage, or injecting malicious code into legitimate processes to run with higher privileges.

Effective command and control (C2) is essential for APTs, as it allows attackers to issue commands, retrieve data, and update malware within the compromised network. Techniques such as domain fronting, which hides C2 traffic within legitimate traffic, or steganography, which embeds malicious commands in benign-looking files, are commonly used. Some APT groups even develop custom communication protocols that blend in with legitimate network traffic to avoid detection.

Data exfiltration, the goal of many APT attacks, involves stealing sensitive information such as intellectual property, state secrets, or financial data. Attackers may use methods like compressing and encrypting data to evade detection or employ DNS tunneling to smuggle data out of the network without triggering conventional data loss prevention systems. Some APTs also abuse cloud storage services, which are often whitelisted in corporate environments, to exfiltrate information.

To remain undetected for extended periods, APT actors use a variety of evasion techniques. Fileless malware, which operates entirely in memory without writing files to disk, makes detection by traditional antivirus solutions difficult. Time stomping alters file timestamps to blend malicious files into normal system activities, while log tampering involves modifying or deleting logs to cover their tracks and complicate forensic analysis.

After achieving their objectives, APT actors may take steps to cover their tracks, such as using secure deletion tools to remove malicious files or overwriting logs with useless data. Some advanced APT malware is even designed to self-destruct after completing its mission, leaving little to no trace.

Advanced techniques employed by APT groups often involve zero-day exploitation, where attackers utilize previously unknown vulnerabilities to compromise systems, often as part of state-sponsored activities. Island hopping is another technique, where attackers compromise connected networks, such as those of suppliers or business partners, to reach the primary target. Additionally, APT groups often "live off the land" by using existing tools and features of the operating system, such as PowerShell or WMI, to carry out attacks without introducing external malware.

Examples of well-known APT groups include APT28 (Fancy Bear), a Russian cyber espionage group targeting government and military entities, APT29 (Cozy Bear), another Russian group associated with intelligence services and known for its stealth in compromising government organizations, and APT41 (Winnti Group), a Chinese group involved in both state-sponsored attacks and financially motivated cybercrime.

Understanding the various stages and techniques involved in APT attacks is crucial for developing comprehensive defense strategies. These classifications highlight the complexity and persistence of APT threats, emphasizing the need for robust security measures to protect against such sophisticated cyberattacks.

IV. APTs ATTACK STEPS

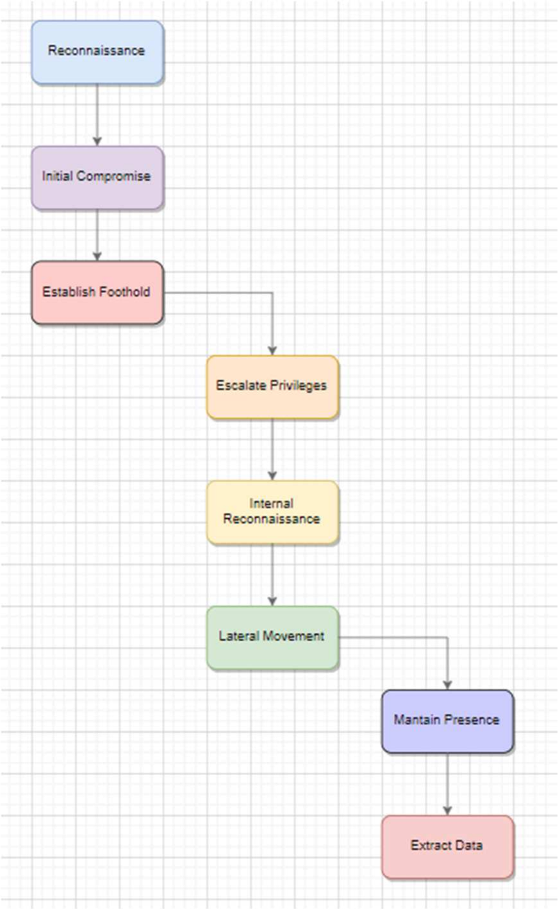

Fig 2 APT Steps

The first key part of carrying out such an attack is the reconnaissance part, which includes gathering key information about the organization that is being targeted, such as identifying key personnel, network infrastructure and any other potential vulnerability. The next step is to gain access to the target's network, which can be achieved through spear-phishing which is a type of phishing that targets a single person rather than many people at once, or exploiting some software vulnerabilities, or perhaps even using social engineering techniques such as cache poisoning, baiting or "quid pro quo".

The next step after successfully gaining access to the targeted network is to establish a foothold, meaning securing access to compromised systems by deploying malware or backdoors. The main goal is to allow the attacker to regain access even if it has been detected or partially removed.

Further, with the help of access gained by exploiting other vulnerabilities or stolen credentials, the attacker's goal is to gain access to more important privileges such as identification of sensitive data, intellectual property or access to some critical systems.

After the attacker succeeds in gaining access to the data of interest, the next step is to transfer the stolen data from the compromised network to a new external location controlled by the attacker. Also continuously, the attacker must maintain access and control over the compromised network to maintain long-term objectives, an example of which is espionage.

These were roughly the main steps in realizing such an attack. In the following, I would like to take a hypothetical scenario where we can better exemplify the creation of an Advanced Persistent Threats attack. Presume our target is a multinational company with a very valuable intellectual property called “X”. Our objective as attackers is to steal their proprietary research and the data developed from their research.

V. IN DEPTH EXAMPLE

In learning how to decide how to infiltrate and what methods to use to gain access to "X" company's network we need to gather information about the company, which can be accomplished through public resources such as articles, conferences, interviews or social media. Another helpful tool is the use of open-source intelligence which is a collection and analysis of data gathered from open sources in aim to produce actionable intelligence that can be divided into six different broad categories of information: media, internet, public government data, commercial data, grey literature and professional and academic publications.

In parallel to information about the company, a key aspect is the identification of appropriate key persons, especially authorized people in areas with sensitive information, for example people who may work in the Research and Development department.

With the help of the information obtained during the reconnaissance stage, it is time for the attacker to tailor an email to the person identified as the key in this process and with the previously obtained data the attacker is allowed to perfectly mimic the person who will be the sender. A malicious document that exploits zero-day vulnerability in a common format such as .pdf or .docx can be added to the email. An example that might illustrate this better was given by Jorge Rey, cyber security and compliance principal at Kaufman Rossin in an interview. He explains: "When people make a change to their LinkedIn and identify that they've joined Kaufman Rossin, in a matter of hours or even minutes they'll get an email from our CEO—not from his Kaufman Rossin email, but something at gmail.com—asking them to buy gift cards and things like that." Of course, this email isn't coming from the CEO at all, but rather an attacker who's hoping to catch a new employee off guard. "All of these bots are monitoring LinkedIn, monitoring everything through scripts, and sending information hoping someone will fall for it,".

Going back to our example, after the target person opens the malicious document, the exploit executes and a malware program that opens a backdoor named remote access Trojan enable administrative control over the victim's computer.

Advancing using remote access Trojan, the attacker identifies and attempts to exploit additional vulnerabilities on the victim's computer to gain administrative privileges. Once the credentials have been identified, they will be downloaded to the attacker's network and used to gain access to other systems on the network. With higher credentials an internal reconnaissance can be performed, i.e. mapping the internal network and clearly identifying the systems that contain the desired research data. The attacker can also use lateral movement to use stolen credentials and exploited vulnerabilities to move laterally and compromise additional systems, including servers storing sensitive data.

After the data has been fished out, the next phase is known as exfiltration where the stolen data is encrypted and compressed to avoid detection while the attacker will use covert channels such as HTTP/S or DNS tunnels to exfiltrate the data to external servers under his control.

Once the stolen data has been transferred to a server where the attacker is in control, the perpetrator can focus on maintaining a presence on the compromised network so that they can continue to access future data. To accomplish this, it will install additional backdoors and other persistence mechanisms. It will regularly monitor the compromised network and continue to export additional data on an ongoing basis.

VI. Ways to defense

Knowing that we have explained through an example how such an attack can be realized, it is now time to discuss the methods that can help us to counter these various attacks, including a multifaceted approach to network security.

A first defense strategy is to segment the network, divide it into smaller, isolated parts to limit access and reduce the spread of potential attacks. The main advantage is that by controlling traffic between segments, the attacker's ability to move laterally in the network is limited and overall security is improved and thus helps to separate sensitive assets from less critical ones, meaning if one segment is compromised, attackers cannot so easily access the rest of the network.

Another very popular security method is Multi-Factor Authentication (MFA) which requires users to provide two or more forms of identification before gaining access to a system or application. It typically combines something you know (password or PIN), something you have (an authentication device, such as a cell phone or hardware token) and something you are (biometrics, such as fingerprint or facial recognition). The use of MFA significantly improves security because even if one component (such as a password) is compromised, unauthorized access is prevented by the need for the other forms of authentication.

As in any other activity, prevention is also important in this case. So, to properly handle security vulnerabilities or any other errors, regular patch management is necessary, a continuous process that involves identifying, testing and applying software updates also known as patches.

Another approach that can be used to prevent an intrusion is the use of intrusion detection and prevention systems to monitor network traffic and detect suspicious activity that indicates an APT attack. It analyzes network traffic in real time to detect suspicious activity such as unauthorized access attempts, Denial of Service (DoS) attacks, or exploits of known vulnerabilities, using a combination of predefined and customizable rules to identify and respond to potential threats.

In parallel with the previously defined systems, endpoint compromise detection and response solutions can also be used, which tools that analyze the activity on end devices are identifying signs of malicious or intrusive behavior. These solutions work by collecting endpoint data and analyzing it in real time using advanced machine learning and analytics techniques.

And finally, other defensive solutions can be security information and event management to aggregate and analyze logs from various sources, allowing the detection of abnormal behavior and potential threats, training and awareness of users by organizing certain Security training programs with the aim to educate employees about phishing attacks and social engineering tactics. Also conducting regular security audits and penetration tests to identify and address vulnerabilities before they are exploited by attackers remains another important mechanism to prevent these types of attacks.

VII. Real World Example

One of the most notable examples of an Advanced Persistent Threat (APT) attack is the Stuxnet worm, discovered in 2010. Believed to be developed by the United States and Israel, Stuxnet was aimed at sabotaging Iran's nuclear enrichment program, specifically targeting the Natanz facility.

The attack began with gathering intelligence on Siemens industrial control systems (ICS) used at the facility. The worm was likely introduced via USB drives, eventually spreading through the network by exploiting multiple zero-day vulnerabilities in Windows systems. Once inside, Stuxnet sought out the PLCs (Programmable Logic Controllers) controlling the centrifuges and executed its payload. This payload altered the speed of the centrifuges, causing physical damage while simultaneously sending normal readings to the monitoring systems to avoid detection.

Stuxnet was engineered to remain undetected and persist within the network, employing advanced evasion techniques and self-updating capabilities. Its impact was significant, reportedly destroying around 1,000 centrifuges and delaying Iran's nuclear program. Stuxnet not only demonstrated the potential of cyber warfare to cause physical damage but also highlighted the vulnerabilities in critical infrastructure and the need for robust cybersecurity measures.

VIII. Conclusion

Having a well-defined taxonomy in the realm of cyber-attacks, particularly Advanced Persistent Threats (APTs) is of paramount importance. Such taxonomy provides a standardized framework that enhances understanding, communication, and collaboration among cyber security professionals. It allows for the systematic classification of different types of threats, their methods, and their impacts, thereby facilitating more effective identification, analysis, and response strategies.

Taxonomy helps in delineating the complex landscape of cyber threats, enabling organizations to prioritize resources and defenses based on the most pressing risks. It fosters a common language that bridges the gap between different stakeholders, from technical teams to executive management, ensuring that all parties are aligned in their threat perception and mitigation efforts.

In the context of APTs, which are sophisticated and often state-sponsored, having a precise taxonomy is crucial. It helps in distinguishing these high-level threats from more routine cyber-attacks, ensuring that the unique characteristics and tactics of APTs are adequately understood and addressed. This, in turn, supports the development of specialized defense mechanisms and incident response plans tailored to counteract the specific challenges posed by APTs.

In conclusion, taxonomy in cyber-attacks and APTs is indispensable for enhancing the effectiveness of cyber security measures. It ensures clarity, consistency, and comprehensiveness in threat assessment and response, ultimately contributing to a more resilient and secure digital environment.

RELATED WORK

This section discusses the current state of research in Advanced Persistent Threats (APTs). Recent Systematization of Knowledge (SoK) papers provide a comprehensive overview of APTs, emphasizing the evolving nature of these threats and the techniques used to detect and mitigate them. By comparing these works with our study, we identify gaps in the existing literature and position our contributions within this context. Key contributions of this paper include the development of a detailed taxonomy for APT attacks, the proposal of a hypothetical scenario to illustrate these attacks, and an analysis of defense strategies that go beyond the current state of the art.

This paper provides a comprehensive analysis of Advanced Persistent Threats (APTs), highlighting a detailed taxonomy of APT attack steps, a hypothetical scenario illustrating these attacks, and a discussion on effective defense strategies. The contributions go beyond the state of the art by offering a structured classification of APTs and integrating recent advancements in detection technologies. Future work will focus on expanding these strategies, incorporating more real-world case studies, and refining the proposed taxonomy to adapt to the evolving landscape of APTs.

References

[1] Palo Alto Networks, “The Lifecycle of an Advanced Persistent Threat,” *Palo Alto Networks Report*, vol. 1, no. 1, pp. 1-25, January 2017.

[2] Lockheed Martin, “Understanding the Advanced Persistent Threat,” *Lockheed Martin Report*, vol. 1, no. 1, pp. 1-30, April 2011.

[3] Kaspersky, “APT Trends Report 2022,” *Kaspersky Report*, vol. 1, no. 1, pp. 1-35, March 2022.

[4] FireEye, “The Evolution of Advanced Persistent Threats: A 10-Year Review,” *FireEye Report*, vol. 1, no. 1, pp. 1-40, September 2020.

[5] National Institute of Standards and Technology (NIST), “Combating Advanced Persistent Threats,” *NIST Special Publication 800-61 Revision 2*, vol. 1, no. 1, pp. 1-50, August 2017.

[6] Rashid, Fahmida Y., “Advanced Persistent Threats: How to Combat Them,” *InformationWeek*, vol. 1, no. 1, pp. 1-15, June 2015.

[7] Cunningham, Dr. Chase, “Cyber Warfare – Truth, Tactics, and Strategies,” *Cybersecurity Review*, vol. 1, no. 1, pp. 1-40, March 2016.

[8] FireEye, “Advanced Persistent Threats: Realizing the Potential of Cybersecurity Beyond Detection,” *FireEye Report*, vol. 1, no. 1, pp. 1-45, June 2018.

[9] Clapper, James R., “APT Reports and the Future of Cyber Security,” *Journal of National Security*, vol. 1, no. 1, pp. 1-30, October 2019.

[10] E. Mandiant, “APT1: Exposing One of China's Cyber Espionage Units,” *Mandiant Report*, vol. 1, no. 1, pp. 1-74, February 2013.

[11] S. Karnouskos, “Stuxnet Worm Impact on Industrial Cyber-Physical System Security,” *IEEE International Symposium on Industrial Electronics*, pp. 3817-3822, July 2011.