American Journal of Applied Sciences

Original Research Paper

Defense Methodologies Against Advanced Persistent Threats

[1]Pedro Ramos Brandao and [2]Viktoriya Limonova

[1]Instituto Superior de Tecnologias Avançadas - Lisbon (ISTEC) Coordinator Professor, Portugal
[2]Instituto Superior de Tecnologias Avançadas - Lisbon (ISTEC) Master's student of Computing, Portugal

Article history
Received: 28-07-2021
Revised: 23-07-2021
Accepted: 27-08-2021

Corresponding Author:
Pedro Ramos Brandao,
Coordinator Professor,
ISTEC, Lisbon Portugal
Email: pb@pbrandao.net

Abstract: Advanced Persistent Threats (APTs) are complex and sophisticated attacks. Their main aim is to obtain unauthorized access to financial and corporate data. As such, it is essential to devise and improve monitoring and defense strategies. This study is intended to analyze various defense methodologies proposed by numerous experts to find a possible solution.

Keywords: APT, Advanced Persistent Threats, Cybersecurity, Targeted Cyberattacks

Introduction

The term Advanced Persistent Threat (APT) is intended to describe an attacker or a group of attackers and their motivations. Attackers make use of a wide variety of specialized techniques and tools, among which are spear-phishing Trend Labs (2021) and email spoofing Mistry *et al.* (2019). There is no practical solution against APTs, as the attackers are persistent and use numerous advanced methods to achieve their purposes.

Protection against this type of attack is essentially based on a combination of different kinds of technologies. The main goal in the defense against APTs is to find several suitable solutions that manage to detect and provide information on the techniques used and the attackers Trend (2013). Attackers quickly obtain all the specific data on their targets and which systems to use to help them achieve their ends. Information can be effectively conveyed through forums or via social engineering. However, along with this data collection, different methodologies are employed to avoid being detected. As such, backdoors are left in place to create open access windows and thus maintaining persistence Fireeye *et al*. (2019). A range of intrusion techniques and a combination of several specific methodologies is employed. Some of the attackers have the technology and knowledge to create their tools and malware. Unlike malware, APTs require human involvement. The attacks are complex, well-coordinated, financed and with a specific purpose. This study is intended to analyze the motivation and the different steps present in attacks to reach a possible solution for detection and defense against APTs. Nevertheless, it's worth considering that the protection against these threats is highly complex. This is because of their ongoing evolution and their constant monitoring of vulnerabilities present in their targets' systems.

Literature Review

According to Daly (2009), access to financial, corporate and defense data has been one of the main goals of APTs. As such, strategies based on layers of defense and subsystem segmentation are devised Daly (2009).

According to Symantec (2011), although APT is always a targeted attack, not all targeted attacks are APTs. Therefore, the best defense method against them consists of good general preparation against this type of threat Symantec (2011).

According to Solutionary (2012), APT changes its attack tactics in case its target modifies its defenses, which makes its detection even more complicated Solutionary (2012).

According to John (2017), APT has become one of the most severe and dangerous attacks in recent times. However, given technology development, machine learning has become an analysis and monitoring solution to aid APTs detection John (2017).

According to Sidiqi, Siddiqi *et al*. (2017), security and privacy have become critical factors for organizations. Due to the fast sophistication of cloaking techniques, minor glitches can result in tragedies, especially in an increasingly digital world. On the other hand, the defense in depth method can protect the system itself and provide crucial information on the attacker Siddiqi *et al*. (2017).

According to Li *et al*. (2018a), defense against APTs can be quantified and modeled to ensure control and systems optimization. Control theory aims to solve optimization problems that are subject to a set of dynamic constraints Li *et al*. (2018b).

According to Nie *et al*. (2019), defense against APTs within a system can be accomplished based on physical and logical resources that contain potential vulnerabilities and backdoors Nie *et al*. (2019).

Science Publications

© 2021 Pedro Ramos Brandao and Viktoriya Limonova. This open access article is distributed under a Creative Commons Attribution (CC-BY) 4.0 license.

According to Li *et al*. (2018a), an APT's incubation period may reach five or more years. Therefore, the initial analysis of each attack focuses on collecting data on defense systems and evaluating protection tools Li *et al*. (2018b).

According to Khan (2020), defense solutions are based on understanding the motivation behind APTs attacks, given that traditional security methods are easily circumvented by them Khan (2020).

According to Abdullayeva (2021), APTs use the flaws present in various applications and systems to remain anonymous for as long as possible. Attack detection is highly complex if the intrusion occurs in a dynamic infrastructure such as the cloud. Methods based on simple and deep neural networks aim to detect cyber-attacks better, targeting individuals and systems Abdullayeva (2021).

Advanced Persistent Threats

Concept

APT effectively compromises its targets by applying various techniques, including malware, phishing, spam, Microsoft SQL injection and spyware Symantec (2011), Minds-Distri Net and Leuven (2014). Today, conventional security defenses are no longer enough, as attackers avoid the various forms of detection and remain hidden for long periods. This method allows collecting essential data in the long and medium-term and contributes to its persistence. Moreover, unlike the usual cyberattacks, APTs can go back into previously exploited systems to collect additional data on them Mandiant (2010).

Players and Targets

APT is one of the most sophisticated attacks, requiring vast knowledge and a strong sense of organization. The noticeable characteristics present in invaders, also known as players, are their strong sense of structure, as they are usually a group of individuals who are experts in different fields Minds-Distri Net and Leuven (2014). APTs players can either belong to a military or government cyber group or be professionals hired through private companies Chen *et al*. (2014). The main targets are industries, organizations, or companies with a particular intellectual value, such as telecom operators, high-tech sectors, mass media and government institutions Kaspersky (2013).

Attack

Although attacks are based on a concept divided into phases that remain identical for them, an attack is still unique. It differs because of the set of tools and techniques employed in its execution. Its planning is meticulously laid out and involves numerous steps, elaborated in a structured and refined manner.

Players attack their victims anonymously and persistently. Its discretion allows it to adopt new methods and improve its techniques. However, their interaction is minimal and only done in specific cases, namely for achieving certain goals to minimize the chances of detection. With innovation and advances in technology, numerous APTs use a code snippet that takes advantage of a system's vulnerabilities, referred to as zero-day Vaisla and Saini (2014). This exploit enables higher success rates as it avoids encryption and signature-based detection Chen *et al*. (2014, However, the lack of awareness campaigns on cybersecurity issues causes a huge weakness within organizations. Because of this, the injection of malware into both emails and websites (spear-phishing) continues to be one of the strategies used by invaders.

However, the influx of APTs in recent times has caused new strategic plans to be drawn up. Countless technology companies have begun to train their employees. As a result of such acts, APT players have updated their methods. The initial injection is now done not in emails but the victims' websites (watering-hole) Alshamrani *et al*. (2019), Once access credentials are compromised, the attackers gain access to the victim's system and send corporate emails with embedded malware. The spread results in the creation of several opportunities for the invaders. Nevertheless, this type of method only works if the system's antivirus or firewall does not previously detect it.

The Stages of an APT

Although the main targets are government organizations or institutions, the initial focus is primarily on internal employees who work daily with sensitive data crucial to the attack. Because most employees do not assume that there is a possibility of becoming a victim of an APT, the desired information is efficiently and effectively obtained through social engineering, phishing, or social networking.

There are several approaches related to the number of stages in an attack. However, according to Inspirisys, there are seven essential steps present in most incidents Inspirisys (2020), Fig. 1.

The first stage is responsible for collecting valuable data through vulnerable targets. Here methods such as social engineering, spear-phishing and occasionally port scanning are used to obtain access information. The second, third and fourth steps focus on exploiting the vulnerabilities found in the previous point. Next, the attacker prepares malware with the purpose of infiltrating inside the victim's system. The means of delivery varies from cloud, web, email, or pen. The execution is triggered should the target fall into the trap. The last steps compromise their target entirely; after successful access, a connection is created to collect confidential data. This window may remain open for weeks, months, or even years Inspirisys (2020).

DOI: 10.3844/ajassp.2021.207.212

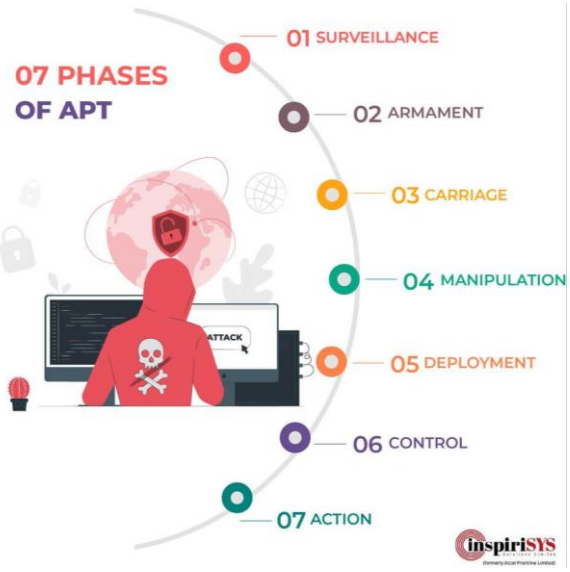

Fig. 1: The seven stages of an APT attack

APT Detection Techniques

Machine Learning and Deep Learning

Due to the sharp growth of cyber-attacks in recent times, detection is one of the most critical factors in securing and protecting a system. According to Cho and Nam (2019), the detection algorithm should be efficient and support the analysis of large blocks of data. There are two types of approaches, signature-based detection and behavior-based detection. However, the first method's effectiveness is much reduced compared to the second method, as the latter allows more significant results to be obtained through code pattern analysis Choa and Nam (2019).

Nowadays, modern techniques use machine learning algorithms and include detecting anomalies both in the network and across the entire length of the traffic. According to Joloudari *et al*. (2020), deep learning is one of the most powerful methods as it allows for more significant analysis accuracy by automatically gathering an attack's key features. The six-layer deep learning model is one of the most specific, with an accuracy rate of 98.85% Bhardwaj and Wei (2018), Table 1.

The six-layer model selects and collects hidden features in the layers of the neural network. The validation is cross-validated and performed about ten times, along with a non-linear activation function that determines the activity of the neurons present in the layers. This is possible due to the Maxout function, which selects the maximum coordinates of the vector responsible for the network input. The output activity is the reverse process and is driven through the Soft max function Bhardwaj and Wei (2018).

Table 1: Detection model classification

Classification models	ACC	TPR	TNR	PPV	F-measure	FPR	FNR
Naïve bayes	88.37	87.12	89.53	88.54	87.82	10.47	12.88
Decision tree of C 5.0	95.64	97.3	97.44	98.15	95.39	2.56	2.7
6-layer deep learning	98.85	98.89	98.87	98.72	95.84	1.13	1.11

An APT can take days, months, or years to be detected. As a result, countless organizations make use of an intrusion detection system. This system reconstructs different scenarios based on the correlation of alerts throughout an attack's life cycle. Markov's static model aids system protection by detecting the stages of an APT. It makes use of a strategy for representing distributed probabilities over sequences Ghafir *et al*. (2019).

Detection Tools

There are numerous detection tools and most use a combination of artificial intelligence and machine learning. Although they are applied for the same purpose, they have different characteristics and goals. Therefore, although organizations are increasingly relying on these solutions, it is crucial to analyze them for a broader perception:

a) User and Entity Behaviour Analytics (UEBA). The UEBA tool Maayan (2020), allows detection of most attacks by creating a behavioral database
b) Solar Winds Security Event Manager (SEM). It allows simplifying the protection process by using a system of filters and correlation rules. Monitoring is performed through centralized logs Solar Winds (2021). Cynet Deception Technology. Deception is a widely used strategy by security professionals, both in offensive and defensive tactics. This method's primary purpose is to deceive the attacker into believing that he is collecting sensitive data (credentials, access points, connections). If the attacker takes the bait, an alert is created containing the attacker's IP address Cynet *et al*. (2021)

APT Defense Methodologies

APTs' persistence and complexity are two critical factors to consider, especially when designing and planning a cybersecurity system. Nonetheless, it must be noted that traditional defenses are not fully effective against this type of threat. Hence, they only delay the first phase responsible for access. Players eventually manage to carry out the attack, so it is crucial to adopt new protection strategies with a more comprehensive and efficient methodology.

According to Alshamrani *et al*. (2019), defense methodologies are classified into three major groups: Monitoring, detection and mitigation. Each contains essential factors in reducing possible unwanted access.

Monitoring Methodology

Although it's a trivial and straightforward process, it provides more excellent stability, protection and security. Firewall- or antivirus-based monitoring can be carried out on various parts of the system. If necessary, it is possible to apply patches minimizing access and fixing vulnerabilities. Monitoring Central Processing Unit (CPU) usage is also essential, as suspicious behavior can be found. For example, some types of mal ware do not use files as support but rather, the processes embedded in memory Alshamrani *et al*. (2019). This type of attack leaves no trace, as it only affects its usage values. Because of that, it's crucial to analyze not only the CPU but also the Graphics Processing Unit (GPU).

Packet and log analysis are essential. In comparison, the first one can identify new destination addresses, suspicious shipments, or varying packet sizes. Monitoring memory, system and execution logs help detect attacks in their early stages and obtain important information about the attack and the attacker.

Detection Methodologies

Detection must evolve as intrusion attempts increase. To do so, it's essential to apply different types of irregularity categories (static, neural networks, machine learning) Hodge and Austin *et al*. (2004). Anomaly detection helps to identify APTs with a long to medium-term permanence. However, this alone is not enough.

According to Kim *et al*. (2015), irregularities detection can be achieved through two essential steps. The first is responsible for making rules and behavior patterns based on data obtained through machine learning, decision trees and statistical data. The second step is centered on comparing the previously structured regulations and the behavior of a given system. Equating allows you to define whether the behavior is normal or unusual Kim *et al*. (2015).

Mitigation Methodologies

Mitigating an APT can be accomplished through reactive methods, which identify possible paths and scenarios based on the vulnerabilities present at a given time. It can also be achieved by analyzing graphs containing specific metrics for detecting attacks and identifying possible paths. Furthermore, the mitigation methodology can predict the costs and investment returns associated with a given episode. Along with this benefit, it allows for the presumption of critical regions and the level of their severity Alshamrani *et al*. (2019).

Unlike the reactive method, the proactive strategy mitigates attacks based on deception. The main goal of this methodology is to trick the intruder into changing its surface. Honeypots Alshamrani *et al*. (2019), are among the most widely used methods and allow essential data about the perpetrators and their tactics to be extracted.

Defense in Depth

In-depth defense, also known as defense-in-depth, is a multi-layered methodological approach. It is aimed at protecting a network through a set of mechanisms. Should any of this fail, it is quickly replaced by another. This concept not only protects the system but also returns essential information on the attack. The multilayer strategy applies the appropriate protection method according to the layer type (PJCIS, 2016), Table 2.

According to McGuiness (2021), the defense in depth method comprises perimeter defenses, intrusion detection tools, employee awareness and defining strong credential combinations McGuiness (2021). Adequate protection allows you to make the first stage of access more difficult and reduce privilege escalation if credentials are compromised. Additionally, screenings are performed to verify the authors of each process. Finally, even if there is penetration and compromise of data, the defense in depth method allows a comprehensive recovery and screening method to be applied.

It can be observed that the strategies applied to various elements are almost identical to the techniques of an APT attack. For it uses a set of complex and sophisticated methodologies (PJCIS, 2016), Table 3.

Although it is one of the most accurate methods, it is still not entirely effective against the complexity and sophistication of APTs as attackers use the defense methodologies as a knowledge base for developing their attacks.

Table 2: Defense methods according to the different layers

Layers	Defense methods
Identity and access	Identity and access management
Physical and enviromental	Physical and enviromental security
	1. intrusion detection and prevention system
	2. VOIP security
	3. network segmentation and firewall
Network	4. Web and mail content inspection
	5. secure remote access
	6. data encryption
	7. Network access control
Operating system	operating system security
Application	Application firewall
Data base	Database security

Table 3: Strategic elements of in-depth defense

Defense in depth strategy elements	
Risk management program	1. Indemnify threats
	2.characterize risk
	3. maintain inventory
Cyber security architecture	1. Standards/recommendations
	2. policy
	3. procedures
Physical security	1. Field electronics locked down
	2. control center access controls
	3. remote site video, access control, barriers
ICS network architecture	1. Common architectural zones
	2. Demilitarized Zones (DMZ)
	3. virtual LANs
ICS network perimeter security	1. Firewalls/one-way diodes
	2. Remote access and authentication
	3. jump servers/hosts
Host security	1. Patch and vulnerability Management
	2. field devices
	3. virtual machines
Vendor management	1. Supply chain management
	2. managed services/outsourcing
	3. leveraging cloud services
The human element	1. Policies
	2. procedures
	3. training and awareness

Conclusion

While there is no completely effective solution against APTs, numerous defense strategies could mitigate the initial stages of an attack. Furthermore, the analysis of methodologies proposed by several authors, experts in the field allowed the perception of distinct methods. These methods, combined with others, could complement and raise the detection rate.

Combining specific detection tools with modern defense methodologies can prevent some of the early stages of an attack or identify evidence of the attack at later stages. Nevertheless, even if the defined strategy is not fully effective, it may contribute to monitoring possible attacks.

In short, current defenses are not yet thoroughly studied or equipped against APTs, due to its constant evolution and adoption of new strategies in the face of new defenses devised by organizations. Thus, protection is still one of the most important and coveted research topics in recent times.

Acknowledgements

We are grateful for the support given to research by Prof. António Chaves Fidalgo and the Higher Institute of Advanced Technologies (ISTEC).

Ethics

This article is original and contains unpublished material. The author has read and approved the manuscript and no ethical issues are involved.

Author's Contributions

All authors equally contributed in this work.

References

Abdullayeva, F. J. (2021). Advanced Persistent Threat attack detection method in cloud computing based on autoencoder and softmax regression algorithm. Array, 10, 100067. doi.org/10.1016/j.array.2021.100067

Alshamrani, A., Myneni, S., & Chowdhary, A. (2019). "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges and Research Opportunities," 2019.

Bhardwaj, A., Di, W., & Wei, J. (2018). Deep Learning Essentials: Your hands-on guide to the fundamentals of deep learning and neural network modeling. Packt Publishing Ltd.

Chen, P., Desmet, L., & Huygens, C. (2014, September). A study on advanced persistent threats. In IFIP International Conference on Communications and Multimedia Security (pp. 63-72). Springer, Berlin, Heidelberg. https://link.springer.com/chapter/10.1007/978-3-662-44885-4_5

Cho, D. X., & Nam, H. H. (2019). A method of monitoring and detecting APT attacks based on unknown domains. Procedia Computer Science, 150, 316-323. doi.org/10.1016/j.procs.2019.02.058

Cynet, (2021). https://www.cynet.com/platform/threat-protection/deception/

Daly, M. K. (2009) "The Advanced Persistent Threat," 2009. https://www.usenix.org/legacy/event/lisa09/tech/slides/daly.pdf

Fireeye. (2019). Double Dragon APT41, a dual espionage and cyber crime operation. https://content.fireeye.com/apt-41/rpt-apt41/.

Ghafir, I., Kyriakopoulos, K. G., Lambotharan, S., Aparicio-Navarro, F. J., AsSadhan, B., BinSalleeh, H., & Diab, D. M. (2019). Hidden Markov models and alert correlations for the prediction of advanced persistent threats. IEEE Access, 7, 99508-99520. doi.org/10.1109/ACCESS.2019.2930200

Hodge, V., & Austin, J. (2004). A survey of outlier detection methodologies. Artificial intelligence review, 22(2), 85-126. https://link.springer.com/article/10.1023/B:AIRE.0000045502.10941.a9

Inspirisys, (2020). https://www.inspirisys.com/blog-details/Break-the-Chain%CB%977-Phases-of-Advanced-Persistent-Threats/64

John, J. T. (2017). State of the art analysis of defense techniques against advanced persistent threats. Future Internet (FI) and Innovative Internet Technologies and Mobile Communication (IITM) Focal Topic: Advanced Persistent Threats, 63. https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2017-09-1.pdf#page=73

Kaspersky, (2013). https://www.mendeley.com/catalogue/8be824fe-d709-3998-a44a-94e7172a0031/

Khan, M. B. (2020). Advanced persistent threat: Detection and defence. arXiv preprint arXiv:2004.10690. https://arxiv.org/abs/2004.10690

Kim, H., Kim, J., Kim, I., & Chung, T. M. (2015). Behavior-based anomaly detection on big data. doi.org/10.4225/75/57b69d1ed938e

Li, P., Yang, X., Xiong, Q., Wen, J., & Tang, Y. Y. (2018a). Defending against the advanced persistent threat: An optimal control approach. Security and Communication Networks, 2018. doi.org/10.1155/2018/2975376

Li, Y., Zhang, T., Li, X., & Li, T. (2018b, August). A model of APT attack defense based on cyber threat detection. In China Cyber Security Annual Conference (pp. 122-135). Springer, Singapore. https://link.springer.com/chapter/10.1007/978-981-13-6621-5_10

Maayan, G. D. (2020). https://hakin9.org/how-to-prevent-and-detect-apt-attacks/

Mandiant, M. (2010). Trends. The Advanced Persistent Threat.

Siddiqi, M., Oad, K., & Aziz, A. (2017). Advanced Persistent Threats Defense Techniques: A Review.

McGuiness, T. (2021). https://sansorg.egnyte.com/dl/B3uguj8Rvo/

Minds-Distri Net, E., & Leuven, K. (2014). https://link.springer.com/content/pdf/10.1007%2F978-3-662-44885-4_5.pdf

Mistry, N., Bhati, R. S., Jain, H., & Parmar, M. (2019). Paper on Email Spoofing Analysis. https://www.researchgate.net/publication/332877193_Paper_on_Email_Spoofing_Analysis

Nie, D., Yu, H., Lu, X., & Cui, C. (2019, July). A Method to Defense APT Based on Dynamic ID Transformation. In International Conference on Artificial Intelligence and Security (pp. 541-550). Springer, Cham. doi.org/10.1007/978-3-030-24271-8_48

PJCIS. (2016). Pakistan Journal Pakistan Journal of Computer and Information Systems. http://pastic.gov.pk/downloads/PJCIS/PJCIS_V1_2.pdf

Solar Winds, 2021. https://www.solarwinds.com/pt/security-event-manager/use-cases/apt-security-software.

Solutionary. (2012). White Paper: Defending Against Advanced Persistent Threats. https://www.necam.com/docs/?id=759a3111-a395-4c40-ae0a-43e299159c81

Symantec, (2011). http://index-of.es/Varios/b-advanced_persistent_threats_WP_21215957.en-us.pdf

Trend, (2013). https://www.trendmicro.co.in/cloud-content/us/pdfs/business/white-papers/wp_deepdiscovery.pdf

TrendLabs, (2021). https://documents.trendmicro.com/assets/wp/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

Vaisla, K. S., & Saini, E. R. (2014). https://www.researchgate.net/publication/260489192_Analyzing_of_Zero_Day_Attack_and_its_Identification_Techniques.

Joloudari, J. H., Haderbadi, M., Mashmool, A., Ghasemi Gol, M., Band, S. S., & Mosavi, A. (2020). Early detection of the advanced persistent threat attack using performance analysis of deep learning. *IEEE Access*, *8*, 186125-186137. https://ieeexplore.ieee.org/abstract/document/9214817