2024 IEEE 6th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC) | 979-8-3503-1653-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/IMCEC59810.2024.10575432

APT Attack and Detection Technology

Chen Sheng[1], Chen Gang[2]
1. College of Information and Communication, National University of Defense Technology, Wuhan, China
675602093@qq.com

***Abstract*—APT, also called advanced long-term threat, aims at system destruction and information theft, has more political purposes, and seriously threatens national information security. Firstly, the characteristics of APT attack are summarized, the attack chain around the APT attack stage is analysed in detail, and the relevant techniques are listed; then, the APT attack detection techniques are summarized, and the advantages and disadvantages of APT attack detection techniques are summarized; finally, an algorithm is proposed for APT anomalous behaviour detection.**

***Keywords*—APT; information security; attack chain; detection techniques**

I. INTRODUCTION

In recent years, cyber attacks have emerged one after another, posing a serious threat to enterprises, government departments, and in some cases, national security. Among the many malicious code attacks, APT (Advanced Persistent Threat) has become one of the biggest threats to cyberspace security. According to Qianxin's Global Advanced Persistent Threat (APT) 2021 Annual Report, China continues to be the top regional target for global APT activities. According to Qihoo 360's 2022 Global Advanced Persistent Threat (APT) Research Report, in 2022, APT attacks against key industries in China remained highly popular, with a total of 14 APT organizations involved in attacks against China, and 15 industries such as government, education, information technology, and scientific research remained the main target areas of APT attacks.

Foreign APT organisations have never stopped attacking party and government organs and critical infrastructure in China, posing a serious threat to China's cybersecurity [1]. Cyberspace threat or has become one of the important means relied upon by national intelligence agencies and military operations to achieve their intelligence acquisition or sabotage purposes. As an important and urgent new threat to national cyberspace confrontation, APT attack has become a hotspot of common concern for researchers in the field of cyberspace security, this paper provides a detailed and comprehensive introduction to APT attack and detection technology, which provides a theoretical basis for the further study of APT support. Firstly, it briefly introduces the APT attack; then it analyses the APT attack chain and introduces the APT attack process; finally, it summarizes the APT detection technology and proposes an APT log traffic detection method. It helps to grasp the research progress of APT attack and defence in general, and promote the research in this direction.

II. INTRODUCTION TO APT ATTACKS

The Internet has brought great convenience to people's work and enriched their lives, but it has also brought many security problems. For example, personal information is stolen, privacy leakage, uncontrolled spread of Internet rumours, spam, ransomware, etc., and sometimes even threaten the national information security. Malicious code (malware, a portmanteau of malicious software), also known as malware, is the most important tool in most software intrusions [2].APT attacks are able to use a variety of attacks to target a specific target, and disguise themselves after the attack to evade detection by traditional defences [3].APT attacks are usually accompanied by bot programs, malicious Trojans, phishing emails [4], XSS injection, puddle attacks [5], social engineering [6] and other means to enhance the complexity and impact of the attack to an unprecedented

degree, from which the system or administrator privileges are gradually obtained, and then carry out the next step of the attack.The characteristics of the APT are expressed in the A and P. The A is mainly manifested in the high level of the attack, i.e., it is difficult to extract the characteristics of the attacking behaviours, a single point of covertness P is mainly manifested in the long duration of the attack process and the long hiding time after the successful attack. From a comprehensive point of view, APT attacks are different from traditional network intrusion, these new types of attacks and threats to system destruction and information theft for the purpose of more targeted, is a specific organisation or institution to use advanced integrated attack means against a specific target to carry out covert, long-term, sustained network attacks [7].

APT advanced (Advanced) performance in the attack method novel, technical means of various, and according to the characteristics of the target attack customised design; coupled with its covert, very difficult to be detected, so can be in a long time in the continuous (Persistent) attack; and it is in the attack of the success rate is very high, the harm is very great.

III. Attack Chain of APT Attack

APT attackers, using a variety of advanced attack methods, carry out organised, long-term persistent network attacks on high-value targets. The main purpose is to steal the target's important asset information, obtain the target's system access rights or manipulation rights, and cause damage to the target's various information systems. Its characteristics are: highly purposeful, highly covert, highly harmful, target materialisation and persistence.

Although each specific APT attack strategy will not be exactly the same, the attack chain of APT attacks is largely the same. the APT attack chain consists of six phases: targeted reconnaissance, vulnerability exploitation, command-and-control, power lifting, lateral movement, and data leakage.

A. Targeted Reconnaissance

After an attacker selects a target, the first thing to do is to collect information on all networks and systems related to the target through reconnaissance. Understanding the weaknesses of the target system protection and the possible vulnerabilities of the system, the use of this information, bypassing the protection system, so as to carry out subsequent attacks in a more targeted manner, increasing the probability of success.

The above intelligence is gathered to formulate an attack plan and tailor specialised tools or malicious code. The main ways of reconnaissance are:

1) Network scanning: It is possible to parse a remote network or identify the operating system and applications used. Network scanning techniques are usually divided into two main categories: passive scanning and active scanning. In passive scanning, attackers infer information about the target network by monitoring traffic. Commonly used tools include: tcpdumph, Wireshark, which may also require "mirroring" the ports of network devices to replicate the traffic. Active scanning, on the other hand, collects information by intentionally generating specific packets (aka probe packets), sending them to the network device under consideration, and then analysing the response. Below we describe some of the most popular reconnaissance techniques used to collect network information, categorised by scope.

a) Network and Device Enumeration: Network enumeration and device enumeration, the former is used to discover hosts and servers and the latter is used to identify IoT nodes and other devices exposed by the attack target.

b) Port Scanning. Port scanning is designed to probe devices for open ports and available services. The most popular method is still to take full advantage of the different behaviours of the three TCP handshakes. Port scanning can then discover whether a particular remote TCP port is open by attempting to send SYN/ACK packets and establish a full transport connection, or terminate the process midway.

c) Fingerprint Identification. Scanning is used to identify the device operating system or available applications in the target node. This can be achieved through both active and passive methods. In the case of

OS fingerprinting, for example, this technique takes advantage of the fact that each operating system's network stack exhibits subtle differences in response to well-designed probing packets (e.g., the initial sequence number of a TCP segment and the default TTL value of an ICMP packet, etc.). This type of information can be used to remotely determine the type and version of the operating system of the inspected device. nmap is a typical tool for active scanning.

d) Application-level reconnaissance. Used to infer certain advanced capabilities of the target host. Attackers can use scanning tools to reveal certain weaknesses in the network targeted by the attack. Typical tools include Nessus, Acunetix, and Vulnersm, or open source solutions like IVREn and Vega. Attackers can use probe packets to actually probe the level of protection of the attack target. In this case, the attacker can use the response time obtained to infer whether the anti-virus product is running on the target machine or whether the virus signature has been updated.

2) Internet intelligence gathering: An attacker can search the Internet for publicly available information. There is so much information available on the Internet that an attacker can retrieve many relevant pieces of information, combine them and exploit them. Internet intelligence is "offensive" open-source intelligence, limited to information available on the Internet and its services. Examples include the Web, public databases, dedicated scanning services that resolve Internet of Things nodes, and geographic or geo-referenced information sources.

3) *social engineering:* It exploits the weakest link in the security chain: people. This approach is often effective. Social engineering exploits the trust of the other party, manipulates and deceives them, and persuades the target of an attack to share confidential information or to perform activities that may be favourable to the attacker, such as downloading and installing Trojan-carrying applications. It can greatly reduce the time required to gather information, often with little skill. Technology-based attacks include phishing and spamming, or the use of pop-ups and specially crafted e-mails to trick users into installing malware.

B. Vulnerability Exploitation

After reconnaissance and intelligence gathering, it is time to consider how to use the vulnerabilities to infiltrate the organisation. After the attack strategy is determined, the next step is to create specific malware based on the vulnerabilities. Generally, APT organisations will have specialised agencies engaged in the mining and exploitation of zero-day vulnerabilities, and they will also pay close attention to the latest announcements on some vulnerability reporting platforms, and make use of such publicly or semi-publicly disclosed vulnerabilities as well as available POC (EXPLOIT) code to further produce APT organisations' arsenals, such as pdf files with malicious code (shellcode) or office documents with malicious code (shellcode). Anti-detection methods such as code obfuscation, encryption, shelling, etc. are employed and tested with various up-to-date anti-virus software before delivery to prevent detection after delivery to the target network.

APT attackers deliver crafted malicious code and malicious files to the target network, and common techniques include.

1) *Phishing email attack:* Only for the target network members to carry out phishing email attacks, the attacker carefully constructs an email that is sufficiently fake. The title of the email, the content of the email, the name and type of attachments, all to let the recipient relax their vigilance, interest, and ultimately open the email attachment or the URL in the body of the email. e.g., combined with the stock market hotspots or current news to send phishing emails or create bait files.

2) *Websites (Horse Mounting):* Finding the weaknesses of websites frequently visited by target personnel (e.g. the existence of zero-day vulnerabilities that can be exploited), and then launching infiltration and attack on the website, and then placing well-designed malicious scripts after breaking through, so that the target users visiting the webpage can download the malware containing malware to the local area without knowing it, and at the same time, use the browser loopholes to install and execute it.

3) *Pendulum attack:* When the target of the attack is not connected to the external network, the ferry attack is a means. For example, military networks can use USB flash drives and other mobile storage devices as a medium to achieve the purpose of indirectly transferring or secretly stealing military secrets.

4) *Network hijacking:* The attacker destroys the network communication mechanism, hijacks the target's

network data flow, and then obtains all of the target's interactions on the Internet, or puts malicious code.

C. Command-and-Control

When a target user opens a file with malicious code using a client program or browser that contains a vulnerability, the malicious code hits the vulnerability, gains control of the target host, and controls the target host to download and install malware. The malware is usually a Trojan horse that is used to establish a C&C (Command and Control) channel with the control server. Generally, C&C servers are servers with well-hidden dynamic domain name IPs. The attacker gives commands to the Trojan through the C&C server to perform the desired action.

C&C servers generally avoid detection by reducing the frequency of communication and changing the IP address of the domain name, and commonly used techniques include domain name generation algorithms, attacking legitimate sites to become C&C servers, and Fast Flux techniques [8].

D. Power Lifting

After command and control, attackers use malicious programs to elevate privileges or add administrator users to gain control of more hosts, set them to boot, shut down or modify host firewall policies in the background, conceal behaviour, and achieve persistent control. Common means of power lifting are system kernel overflow vulnerability power lifting, database power lifting, wrong system configuration power lifting, group policy preference power lifting, stolen token power lifting, bypassuac power lifting, third-party software/service power lifting, WEB middleware vulnerability power lifting and so on.

E. Lateral Movement

Lateral movement means that the attacker uses the controlled host or server as a springboard to transfer malicious code to other hosts in the internal network and establish a connection with the target host. Office hosts within the same organisation are often the same system, similar application software environment, and therefore largely have the same vulnerabilities. After attacking an intranet host, the malicious code will spread horizontally to other hosts within the subnet or vertically to the organisation's internal servers. After controlling the internal target host, it is easy to obtain users' domain passwords, mailbox passwords and various server passwords.

F. Data Leakage

Each step of the APT attack process is self-protected by means of anonymous networks, encrypted communications, and removal of traces. After collecting the secret information, the attacker will hide the data temporarily and compress and encrypt the data, and leak it out by controlling the target host. In the process of outgoing secret information, various technical means will be used to bypass the protection of security systems and anomaly detection. On the one hand, the whole into pieces, the confidential information will be broken up, encrypted or obfuscated, to avoid being detected by the scanning of DLP equipment; on the other hand, the rate of sending will be limited to try not to exceed the detection thresholds of various types of security equipment, to avoid being detected. These methods are usually: data encryption, use of legitimate servers to store data, transmission through an anonymous network via onion routers, erasure of traces, and deep penetration [8].

IV. APT Attack Detection

APT detection includes all stages of the APT attack life cycle, but mainly focuses on the middle and late stages, and the detection techniques used are mainly divided into virtual execution analysis detection and anomaly detection [9]. From the point of view of analysing specific objects, it can be further divided into malicious code detection and traffic detection.

A. Malicious Code Detection Technologies

Current APT attacks often obfuscate and shell the code in order to resist malicious code detection techniques and thus evade detection. Code obfuscation has layout obfuscation, control obfuscation, data obfuscation, and prevention obfuscation. Code shelling refers to a piece of code attached to the source

programme, compression of executable file data, encryption, and decompression, decryption algorithms attached to the protected object. It prevents the executable file from being decompiled and prevents reverse. By these methods, detection can be made more difficult and thus evaded. Literature [10] proposes that in order to combat code obfuscation or encryption and speed up the detection efficiency, control flow features with relatively high accuracy rate are selected to reduce the detection difficulty caused by code obfuscation.The commonly used means of APT attacks are 0day attacks, morphing Trojans [11].0day attacks are vulnerabilities that are known before they are made public, and their detection is very difficult. However, it is relatively easy to detect morphing Trojans, and APT attacks can be detected by detecting morphing Trojan detection, but it is not good to distinguish whether it is an APT attack or not, and there will also be underreporting.Mungyu Lee et al [12] used the FP-Growth algorithm to obtain the malicious behavioural patterns based on the API information of the PE file, and from that, they can detect APT attack behaviours. The authors conducted experiments on 200 samples of malicious code that can be used in APT attacks and 50 samples of generic programs, and about 70% of the patterns containing malicious code were detected.Joshua Saxe et al [13] counted the entropy values of the character and byte values in the binary file of the malicious code for APT attacks and used the statistics as a dataset to train machine learning models. Giuseppe Laurenza et al [14] generated a dataset by collecting public APT reports and retrieving the binaries of the malware cited in these reports, then extracted static features from the binaries including Optional Header, MS-DOS Header, File Header, Obfuscated String and other features, and finally the APT malware classifier is trained using Random Forest algorithm.

B. Anomalous Traffic Detection Techniques

APT anomaly detection determines APT anomalous behaviour by detecting anomalous traffic in the network. Generally speaking, when APT steals data or other data, it needs to send back a large amount of unauthorised data, and the data traffic may show a sudden surge, which is suspicious as a feature for detection. However, current APT attacks usually use P2P self-organising networks, certain websites, VPNs and tunneling technologies to adaptively adjust the traffic in order to hide their own traffic.Xuan D et al [15] proposed an analysis method based on network traffic datasets to detect the abnormal behaviour of APT attacks. Firstly, the network traffic data is preprocessed to extract the traffic features; then, the IP groupings are put into the combined deep learning models CNN-LSTM and CNN-MLP to extract the basic features of IPs respectively. Finally, the IPs are classified into normal IPs and IPs of APTs.Lu Jiazhong et al [16] compared normal traffic and traffic containing malicious loads by a time transformed feature method for distinguishing APT attacks, captured the signals of malicious loads, and then deduced whether there is an APT attack or not, and then detected APT attacks in big data by using machine learning methods. Weixiang Chen et al [17] proposed a method based on APT malicious behaviour gene pool detection. In literature [18], gene construction is carried out using populated data streams, which is used to detect malware through classifiers such as support vector machines, and gene sequences are constructed by separating the malicious data flow direction of key parts, after which sequence comparison is used to distinguish between malicious and non-malicious software.Sperotto A [19] comprehensively analyses the methods of acquiring network data streams and the existing network stream-based detection schemes and concluded that network stream-based detection is a useful complement to other detection schemes. Du Zhenyu et al [20] proposed APT sample logic expression generation algorithm.

With the rapid development of machine learning in recent years, applying machine learning methods has become one of the innovative techniques applied in this direction.Bhupendra Ingre et al [21] proposed a machine learning based system for MLAPT, which runs three main phases: threat detection, alert correlation, and attack prediction.Guanghua Yan et al [22] proposed the APT detection framework AULD, which extracts host-,

domain-, and time-related features from DNS request data from a large amount of DNS log data and uses unsupervised machine learning for clustering to provide a list of suspicious domains in APT activities. Sichuan University designed Goss IP [23], a framework for detecting malicious domains in forum-like discussion forums. In a literature [24] on Mathematical Problems in Engineering, the authors proposed an anomaly detection algorithm GAF to detect malicious domains and in an international conference of IEEE, the researchers proposed independently accessed features and a C&C detection method for detecting malicious domains [25].In a study by Khalil I et al. literature [26] found relationships between malicious domains by transforming between graph relationships A deterministic algorithm is proposed to detect malicious domain names. Detection of APT attacks should give due consideration to the detection of unknown threats, judgement of APT attacks, analysis of some historical data and real-time detection [27].

C. APT Attack Abnormal Behaviour Detection

The key to detecting APT anomalous behaviour lies in how to detect the attack more accurately and quickly, and take strategies to block APT attacks as early as possible. Although the existing methods based on machine learning to detect malicious domain names have made great breakthroughs, there are still shortcomings, such as the small number of black and white samples in APT attacks makes the use of supervised learning very limited. In the detection methods of machine learning, supervised learning is applied more, but supervised learning has high requirements for samples and needs to mark the samples. The samples of APT attacks are extremely small, and APT attack traffic is hidden in big data traffic, which brings great difficulties to the detection.APT attack behaviours are extremely covert, and the event links between different phases are very weak and not easy to be detected, which also means that it is very tough to capture the complete APT attack data.Therefore, it can be considered that we can start from the log data related to the DNS requests left by the APT attack, and detect the data related to the APT attack by using the Unsupervised learning method to detect the suspicious DNS related to APT attack.Due to the lack of real attack samples, we can use the K-means unsupervised learning clustering algorithm which has low requirements on sample labelling. Through the clustering algorithm, normal data and abnormal suspicious data are classified to achieve the detection of APT abnormal behaviours, which can help the defender to discover APT abnormal behaviours in time and adjust the defence strategy to block APT attacks.

REFERENCES

[1] Chen Ruidong, Zhang Xiaosong, Niu Weina, Lan Haoyue.Research on APT Attack Detection and Countermeasure Technology System[J]. Journal of University of Electronic Science and Technology,2019,Vol.48(6): 870-879

[2] G.S. Xu, S. Zhang, G.A. Xu. Software security [M]. Beijing: Beijing University of Posts and Telecommunications Press, 2020, 112

[3] Y.X.Gao,Z.X.Lu,Y.Q.Luo. Survey on malware anti-analysis[C]. 2014 IEEE Fifth International Conference on Intelligent Control and Information Processing,Dalian China, 2014,270-275

[4] Daniel Pauly;Dirk Zeller.Accurate catches and the sustainability of coral reef fisheries(Review)[J].Current Opinion in Environmental Sustainability,2014,Vol.7: 44-51

[5] YANG Weiyong,LIAO Peng,LIU Jinlock,et al. Research on data protection technology in response to new network threats[J].ELECTRIC POWER, 2014,12(5): 136-139

[6] Brief Analysis of APT Situation Involving China in 2019 by Netland Vertical and horizontal

[7] NIU Yanli,LI Yubiao,LUO Shuangchun,ZHENG Xiaokun War Zone Computer Network Response to APT Attack Prevention Strategy 78111 Force

[8] He Shijie,Huang Wenpei.APT Attack Detailed Explanation and Detection Technology[J]. Computer Applications,2018,Vol.38(202): 170-173, 182

[9] Chen Ruidong, Zhang Xiaosong, Niu Weina, Lan Haoyue.Research on APT Attack Detection and Countermeasure Technology System[J]. Journal of University of Electronic Science and Technology,2019,Vol.48(6): 870-879

[10] COLLBERG C,THOMBORSON C,LOW D.A taxonomy of obfuscating transformations[R].New Zealand:Department of Computer Science,The University of Auckland,1997.

[11] C.Cadar,K.Sen.Symbolic execution for oftware testing:three decades later- [J].Communications of the ACM, 2013, 56(2): 82-90

[12] M. Lee, J. Choi, C. Choi and P. Kim, APT attack behavior pattern mining using the FP-growth algorithm,2017 14th IEEE Annual Consumer Communications &Networking Conference (CCNC), 2017, pp. 1-4.

[13] Panda M, Abraham A, Patra M R. A hybrid intelligent approach for network intrusion detection[J]. Procedia engineering, 2012, 30: 1-9.

[14] Hu W, Gao J, Wang Y, et al.Online adaboost-based parameterized methods for dynamic distributed network intrusion detection[J].IEEE Transactions on Cybernetics, 2013, 44(1):66-82.

[15] Moon D,Im H,Lee J D,et alMLDS:Multi-layer defense system for preventing advanced persistent threats[J].Symmetry,2014, 6(4):997-1010.

[16] Li M,Huang W,Wang Y, et al.The optimized attribute attack graph based on APT attack stage model[C].IEEE International Conference on Computer and Communications.IEEE,2017:2781-2785.

[17] Chen wei xiang,Advanced persistent threat organization identification based on software gene of malware,Transactions on Emerging Telecommunications Technologies, January 2020, 31(12)

[18] Caballero,J.,Yin,H.,Liang,Z.,and Song,D.Polyglot:Automatic extraction of protocol message format using Dynamic binary analysis[A].In Proceedings of the 14th ACM conference on Computer and communications security[C], 2007, 317–329

[19] Sperotto A,Schaffrath G,Sadre R,et al.An Overview of IP Flow-based Instrusion Detection [J].IEEE Communications Survey&Tutorials 2010,23(3):343-356.

[20] Zhenyu Du, Yihong Li, Liang Zhang.Algorithm for APT sample logic expression generation[J]. Computer Engineering and Applications,2018,Vol. 54(1): 1-10

[21] Bhupendra Ingre;Anamika Yadav.Performance analysis of NSL-KDD dataset using ANN[A].2015 International Conference on Signal Processing and Communication Engineering Systems[C],2015

[22] Yan, GH (Yan, Guanghua);Li, Q (Li, Qiang);Guo, D (Guo, Dong);Li, B (Li, Bing).AULD: Large Scale Suspicious DNS Activities Detection via Unsupervised Learning in Advanced Persistent Threats.[J].Sensors,2019,Vol.19(14): 3180

[23] Huang C, Hao S, Invernizzi L, et al. Goss IP: Automatically Identifying Malicious Domains from Mailing List Discussions[C]// ACM on Asia Conference on Computer and Communications Security. ACM, 2017:494-505.

[24] Niu, WN (Niu, Weina);Zhang, XS (Zhang, Xiaosong);Yang, GW (Yang, Guowu);Zhu, JA (Zhu, Jianan);Ren, ZW (Ren, Zhongwei).Identifying APT Malware Domain Based on Mobile DNS Logging.[J].Mathematical Problems in Engineering,2017,Vol.2017: 1-9

[25] Wang X, Zheng K, Niu X, et al. Detection of command and control in advanced persistent threat based on independent access[C]// IEEE International Conference on Communications. IEEE, 2016:1-6.

[26] Khalil I, Yu Ting, Guan Bei. Discovering malicious domains through passive DNS data graph analysis [C] //Proc of the 11th ACM on Asia Conf on Computer and Communications Security. New York: ACM, 2016: 663-674.

[27] He Shijie, Huang Wenpei.APT Attack Detailed Explanation and Detection Techniques[J]. Computer Applications,2018, Vol. 38 (202): 170-173, 182