A Model of APT Attack Defense Based on Cyber Threat Detection

Yue Li[1], Teng Zhang[2(✉)], Xue Li[1], and Ting Li[2]

[1] Dongxun Tech (Beijing) Co., Ltd., Beijing 100097, China
[2] National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China
zt@cert.org.cn

Abstract. The targets of Advanced Persistent Threat (APT) are mainly concentrate on national key information infrastructure, key research institutes, and large commercial companies, for the purpose of stealing sensitive information, trade secrets or destroying important infrastructure. Traditional protection system is difficult to detect the APT attack, due to the method of the APT attack is unknown and uncertain. And the persisted evolution ability destroyed the traditional protection methods based on feature detection. Therefore, this paper based on the theory of red-blue confrontation, to construct the game model of attack and defense. And then combined the APT offense and defense experience, presents a model based on cyber threat detection to deal with APT attacks.

Keywords: Cyber security · Advanced Persistent Threat · Unknown attack · Red-blue confrontation · Threat detection

1 Introduction

Advanced Persistent Threat (APT) is a kind of complex and multi-dimension advanced cyber penetration attack aimed at specific organizations [1]. First of all, the attackers usually conducted long-term information gathering and monitoring to the target or its associated organizations from different sources. And then aimed at the existing defense methods to deal with some targeted confrontation and penetration researches. Through the persistent multi-dimension hidden penetration attack (including Cyber, Realistic, Fraudulent), ultimately achieved the purpose of long-term control, information steal, or target destroy.

From the typical APT attack events, APT attacks have the following features:

Long incubation (or implement) period. As the Fig. 1, these cyber attack incubation periods were about 5 years such as Stuxnet [2], Duqu [3], OceanLotus [4], Mermaid action [5]. And some advanced information stealing APT attack have even longer incubation period, such as Flame.

The attackers had already acquainted the defense systems of the targets. The attackers tried their best to find out the target's protection methods as much as possible, and conducted targeting evaluations such as Anti-Antivirus and penetration abilities before they released the malicious programs, in order to bypass the Antivirus software detection installed on host and evade the detection by mainstream cyber security devices.

X. Yun et al. (Eds.): CNCERT 2018, CCIS 970, pp. 122–135, 2019.
https://doi.org/10.1007/978-981-13-6621-5_10

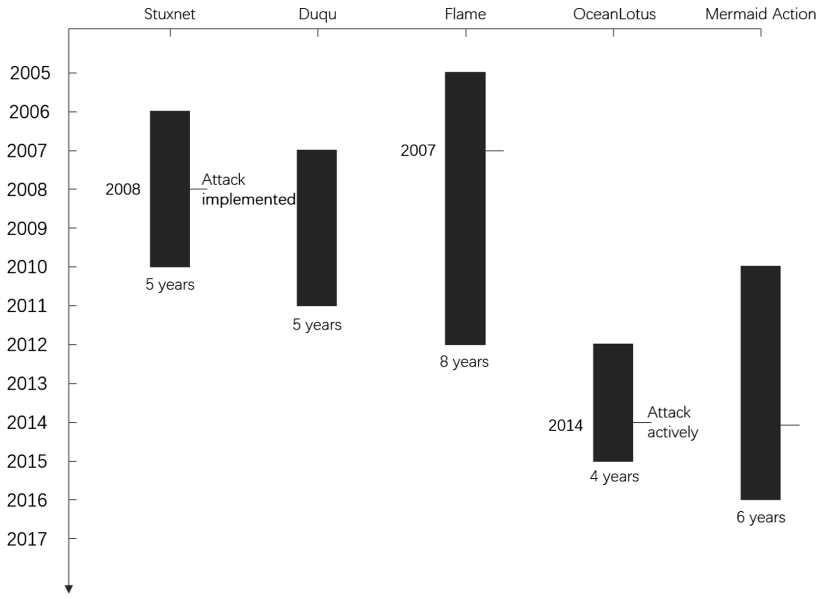

Fig. 1. Typical APT attack events

Various attack techniques and different combinations. From the case studies, the most commonly used APT attack techniques are the Spear Phishing attack and the Watering Hole attack. These two attack techniques could be used with a variety of different social-engineering attack scenarios, created multiple patterns of attack. For example, created a spear Phishing e-mail to trick the developers by simulating the leader's tone. Besides, there still have some other attack techniques which barley reported. Such as exploited the website vulnerabilities to invade into the Demilitarized Zone (DMZ), and then infiltrated into the Intranet.

The occurred cases shows that the traditional defense system has a lot of limitations to deal with the APT attacks. In order to elaborate the defense of APT attack, this paper were focused on the theory of red-blue confrontation to gradually depth the description through the way from APT attacks to APT defenses. Contributes of this paper are as follows:

1. Proposed a model to interpret the thought of APT attacks based on its characteristics.
2. Classified and summarized the common network attack steps and techniques based on cyber kill chain classifications.
3. Proposed a defensive model based on APT threat detected theory, which faced on current limitation of the defense system.
4. Proposed a new framework of APT attack detecting, which is collaborated with "cloud, transport layer, terminals, and manual response".

2 Framework and Techniques of APT Attack

2.1 Framework of APT Attack

The prerequisite to win the battle of cyber red-blue confrontation is fully understanding the enemies' strategies and tactics. So it is very important to research the thoughts of APT attack and establish theoretical guidance systems in the game of offense and defense.

The intention of an APT attack is usually to obtain the highest authority of the target network in order to access the information. Further, it can be described as grasping all the valuable information in the target's network.

Abstractly, the cyber-attack procedure is the process to increase the authority and the volume of information. Each step of the attack acquires new authority and new information. The new authority determines what kind of new information could be acquired. On the other hand, the new information promoted to get new authority (Fig. 2).

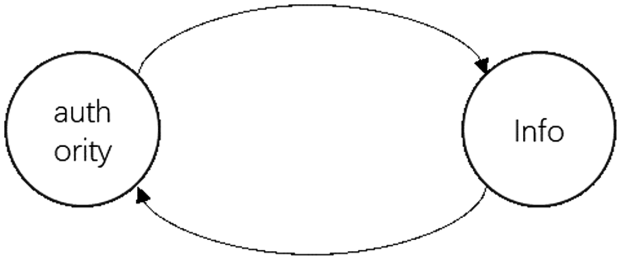

Fig. 2. The view of APT attack

Information is the necessary part during an entire attack. A successful attack is to maximize the effort of information collection, analysis and utilization.

In this paper, we present different views of APT attacks on time dimension and spatial dimension.

On time dimension, attackers generally use the following four methods, and an abstract view of APT attack is shown as Fig. 3.

1. Discovering. To discover new information and clues of sources
2. Detection. To detect the accessed information in order to acquire more sources of information based on acquired authority.
3. Analysis. To analyze effective intelligence based on combining various information and clues.
4. Exploiting. To exploited the acquired information and resources to get more advanced authorities.

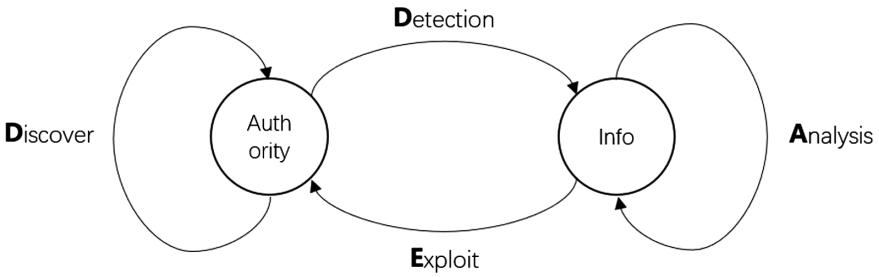

Fig. 3. The view of APT attack on time dimension

On spatial dimension, the APT attack presented the vertical and horizontal features, as shown in Fig. 4.

1. Vertical break refers to acquire more advanced and depth authorities through penetration and breakthrough attack by exploiting the known information. That is the deepening of the authorities.
2. Horizontal break refers to acquire more the same level authorities of different users through penetration and breakthrough attack by exploiting the known information. That is the deepening of the extended authorities.

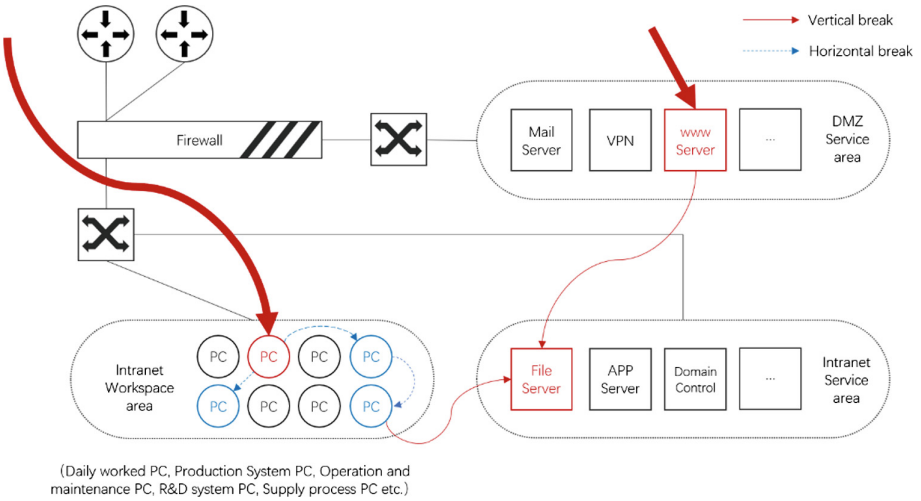

Fig. 4. The view of APT attack on spatial dimension (Color figure online)

Common attacks typically involved both vertical and horizontal break. After each successful breakthrough, the attacker will acquire new authorities. And at the same time the additional information obtained by the new authorities will become an important prerequisite for the next breakthrough.

In Fig. 4 is shown a topological intranet graph of the enterprise. Assuming that the attack target is a file server, and the red solid line is shown as a vertical break. For

example, a vertical break for a PC often by using Spear Phishing emails or Watering Hole websites to attack and exploit, commonly known as "point attack". After obtained the control right of a certain PC, by using this PC as the stepping stone to attack other PCs within the Intranet workspace area to obtain more rights of the same level. In Fig. 4, it is indicated by a blue dotted line, which is a horizontal breakthrough.

In summary, the abstracted thought and method of APT attack in time dimension and space dimension can be expressed as shown in Fig. 5.

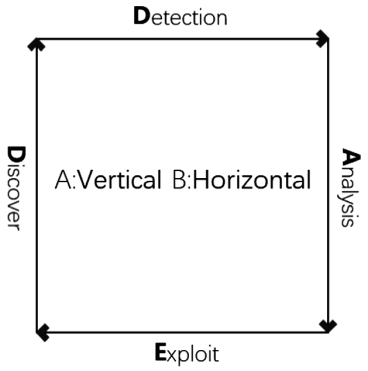

Fig. 5. The thought and method of APT attack

ATP attack could be further analyzed by using the Intrusion Kill Chains [6]. The Intrusion Kill Chains could be divided into 7 layers: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, Actions on Objectives.

Each layer is represented as a phase. It helps the defender to recognize and analyze the attack events by abstracted and classified the attack process. Based on the Intrusion Kill Chains and the above thought and method of APT attack, the attack event can be presented in the manner of Fig. 6.

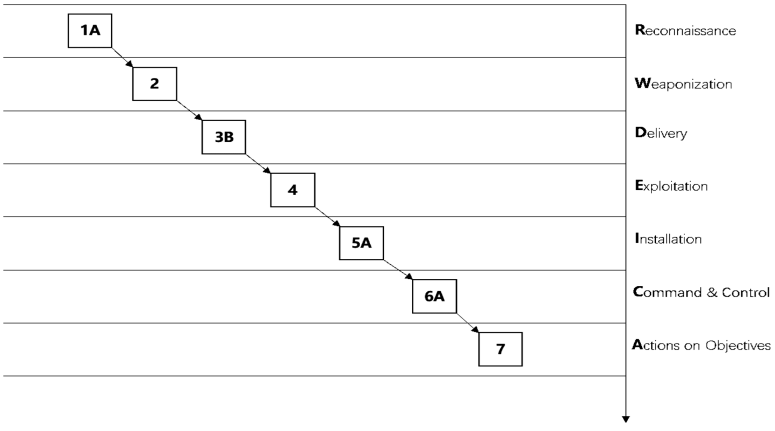

Fig. 6. The Schematic of APT attack event

In Fig. 6, the squares represent a method of attack, the A or B is used to indicate the breakthrough modes, and the serial number is used to indicate the attack implementation steps. The schematic diagram can be used to visualize the whole process from reconnaissance, weaponization, delivery, exploitation, installation, command & control, actions on objectives.

Actually, the APT attack events are often presented as shown in Fig. 7. Before the final attack launched on the target (indicated in red in the figure), large number of pre-attacks (shown in black in the figure) had been implemented for a long time.

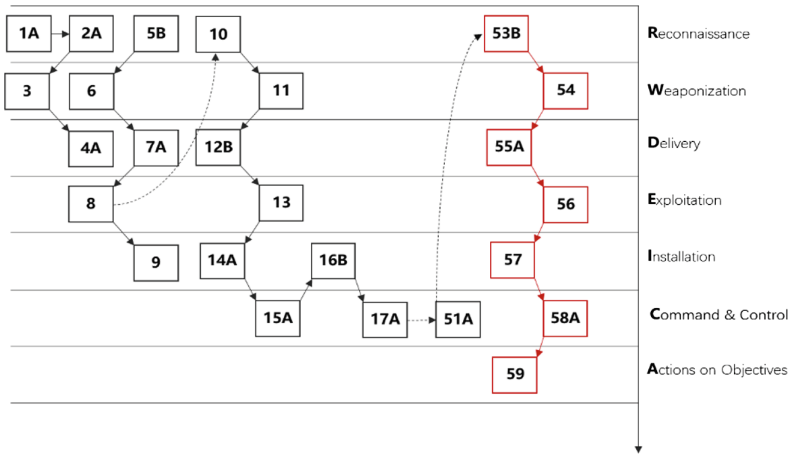

Fig. 7. The Schematic of actually APT attack event (Color figure online)

2.2 Techniques of APT Attack

Although different steps and techniques used in each attack phases may have lots of crossovers, it could be described by the Intrusion Kill Chains model shown as Table 1. When the suspicious actions such vulnerability scanning, port scanning, password cracking were detected in the networks, it could be inferred to the attack is in the reconnaissance stage. After some controlled actions were detected, such as webshell, advanced Trojan, Command & Control actions etc., it could be inferred to the attacker was about to control or had already controlled the target. Therefore, combing the attack procedures and techniques helps the defenders to accurately estimate the current situation and make reasonable inferences after the threat was discovered.

The development of cyberattack technology is essentially based on the current defense technology. At the same time the development of defense technology is essentially base on the currently discovered attack techniques. Therefore, adhering to the thought of red-blue confrontation, classified the attack techniques, and discovered more new methods and new modes of attack are the effective ways to improve the technical capabilities of the defenders.

Table 1. Common used network attack steps and techniques

Intrusion kill chains	Serial	The attack procedures and techniques
Reconnaissance	1	External information acquisition
	2	Vulnerability scanning
	3	Password cracking
	4	Port scanning
Weaponization	5	Carrier selection (file carrier, flow package)
	6	Choices about vulnerabilities and ways to exploit
	7	Choices about penetration tools
	8	Choices about the control weapons
	9	Anti-antivirus techniques (packing, feature confusion etc.)
Delivery	10	Spear Phishing attack
	11	Watering Hole attack
	12	Supply chain attack
	13	Proximity attack
	14	Ferry attack (USB ferry attack etc.)
Exploitation	15	Overflow vulnerabilities exploit
	16	Web vulnerabilities exploit
	17	Logical vulnerabilities combined exploit
	18	Verity of elevated privileges techniques
Installation	19	Botnets, Trojans, worms
	20	Backdoors of operation systems or devices
	21	RootKit embed
	22	WebShell
	23	Advanced Trojans
Command & Control	24	Command and Control
	25	Covert channels
	26	Abnormal communication modes
Actions on objectives	27	Destroyed the data or devices
	28	Data leakage
	29	Data defacement
	30	Long-term monitoring

3 A Model of APT Attack Defense

The starting point for both sides of the offense and defense is the same. Attackers understood the target network and the defense system to find breakthroughs by using various information gathering tools. Defenders also needed to deploy enough probe suites in the network system to detect malicious behavior, recognize attackers, and block attacks. However, in the network security constructions the managers of the security department had a common understanding of security protection as shown in Fig. 8. Deployed moderate security products and implemented the emergency response by professional security practitioners after a security incident event occurred.

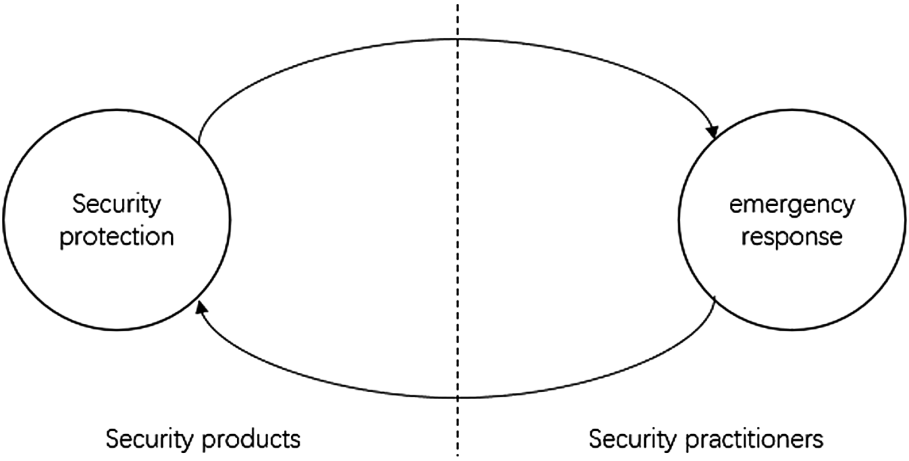

Fig. 8. Traditional thought of defense

In the procurement of products, they also did not analyze their own business scenarios in detail, blindly pursued coverage, and purchased a large number of technical homogenized protective products. The security modules crossed each other. By this way built a seemingly stable defense system. But during the event of a major cybersecurity incident, all deployed security products lost their utility at the same time. And the employed security administrators were also at a loss. At this time, it may be necessary to find a more professional external security team for emergency response, resulting in waste of resources.

Through the analysis, the root cause for this passive situation was that during the construction of cybersecurity systems, the idea of offense and defense game model and red and blue confrontation was not been introduced, and didn't pay enough attention at the detection of potential risks and unknown threats. Eventually, the information on both sides of the offensive and defensive was seriously unequal. The security operation and maintenance employees didn't know what the attackers were doing, what they wanted to do next and what they had done before. Therefore, it must transform the thought of defense and it is the key to build the protection system concentrated on threat detect which based on the theory of the red-blue confrontation.

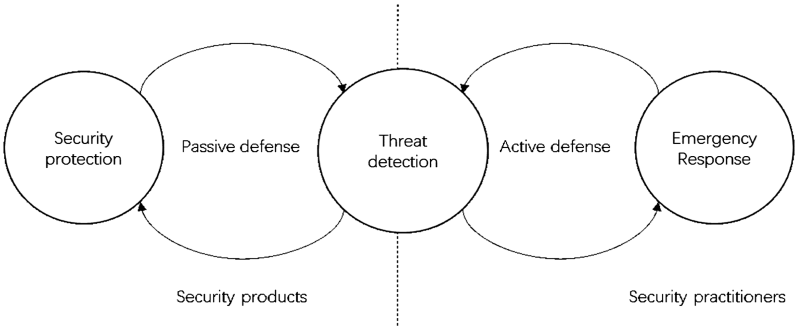

Fig. 9. Defensive thought based on red-blue confrontation

The defensive thought based on the threat detection is shown in Fig. 9. Threat detection refers to the discovery process of attack threats and the compromised hosts in the attacked network. Attack threats are descriptions of attack attributes such as attackers, attack tools, delivery methods, exploits, and control methods. The compromised host are the description of the target attributes such as attacked hosts, servers, switches, firewall, etc. Threat detection is the process by which the defenders acquiring the attackers. The starting point of the process may be an attack threat event that has already occurred, or it may be a compromised host that has been discovered. By analyzing the attack threats, more compromised hosts may be detected and by analyzing the compromised hosts, more attack threats may also be detected. Shown as Fig. 10.

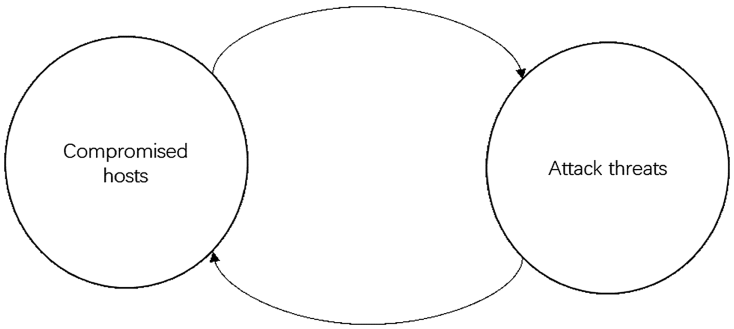

Fig. 10. Threat detection model

Corresponding to the thought of attack, threat detection could be used the following four methods:

1. Analysis: Analyze the system, log, abnormal operation and other information of the compromised host to get more intrusion cues.
2. Inference: Infer attack threats by associating all clues, including attack tools, malicious samples, C&C flow, etc.
3. Discovery: Discover the purpose of the attack by reversely mining value information of the threats such as attack tools and samples.
4. Detection: By leveraging the newly discovered attack threats to create new detection features or scenarios. By using them to scan the entire network and detect unknown compromised hosts.

The thought of threat detection is shown in Fig. 11. Compared with the thought of attack shown in Fig. 3, it can be seen that it is a mutual game.

Defensive work will be no longer just concentrated at the beginning of the attack by adopting the defensive thought which based on the threat detection. It will be changing and adapting around the process of the attack such as detection, delivery, exploitation, installation, control, etc.

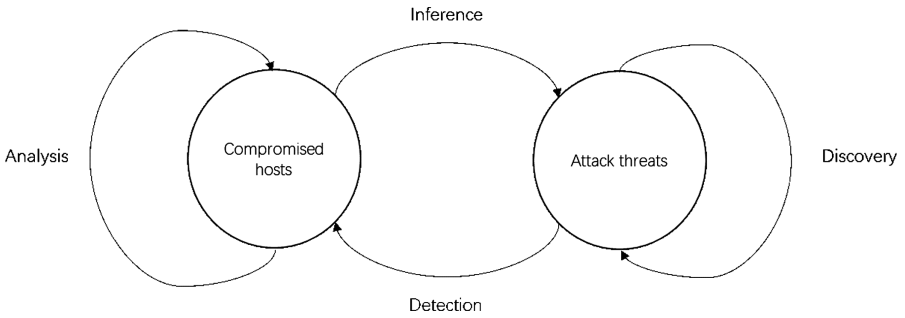

Fig. 11. The thought of threat detection

4 APT Attack Defense Based on Threat Detection

4.1 APT Attack Defense Model Based on Threat Detection

Most of the traditional protection products adopt feature-based detection technology. For example, the antivirus engines mainly detect the file characteristics of malicious samples, and network devices such as IDS and IPS are mainly detected the features of network flow. The advantages of feature detection are identifying the known malicious files or attack techniques quickly, and telling the threats accurately. But the limitations are also obvious, which is, if the features of threats are not contained in the database, the protection will lose its effectiveness.

Therefore, if we meet unknown threats, we will build our protection based on a high view of red-blue confrontation instead of using a single feature-based detection. As shown in Fig. 12, adopting the integrated security technology framework collaborated with "cloud, transport layer, terminals, and manual response", collecting program behavior and network traffic behavior in the system at the terminal and network nodes by the probes, focus on threat intelligence and big data platform, combined with threat perception and anomaly detection model, to analyze the unknown threats semi-automatically.

1. Cloud: Threat intelligence big data platform

Threat Intelligence Big Data Platform is a platform for monitoring and related intelligence data analysis and processing the advanced threats. It can be deployed in the intranet machine rooms. Adopt artificial intelligence technology, combined with Indicator of Compromise information [7] (IOC) to automatically collect and clean threat data, intelligently integrate clue data, automatically mine high-value threat intelligence, and long-term track and analyze the potential threat sources. Targeting on the advanced attacks in cyberspace, it can conduct specific services such as event restoration, attacker intent analysis, attack investment evaluation, attack source tracing, and identification, and at the same time build efficient threat detection and event handling capabilities.

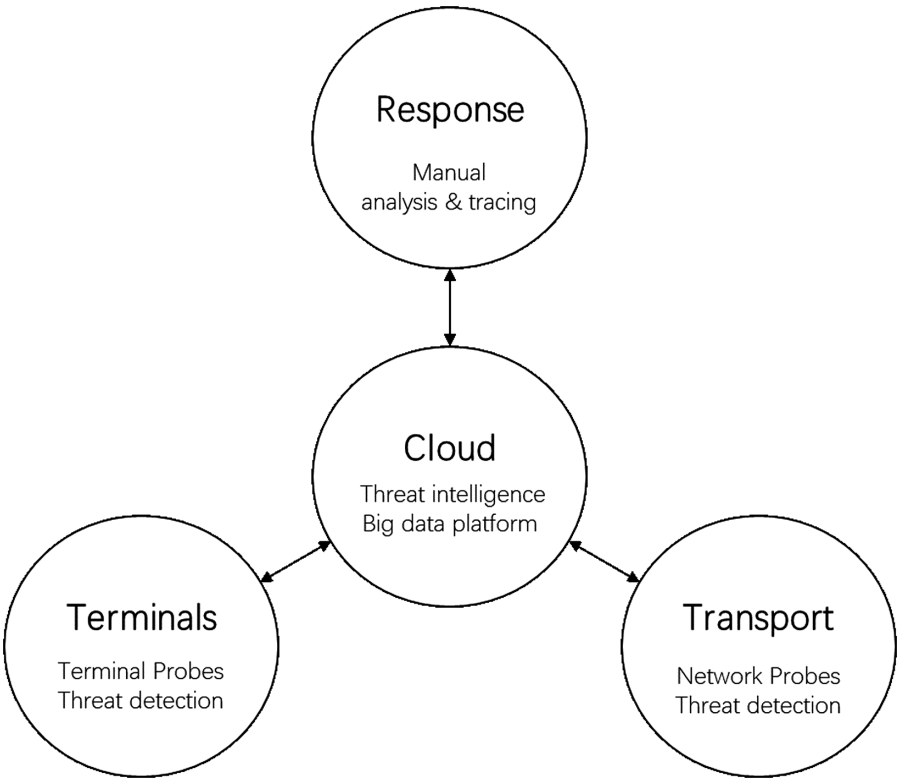

Fig. 12. Techniques framework for unknown threat detection

2. Transport layer: Network probes and threat monitoring

The network probes bypass deployed on the network gateway to collect transmission flow, identifying and filtering the protocols of the data link layer, the network layer, the transport layer, the session layer, the presentation layer, and the application layer, restoring the file and traffic characteristics in the flow, and performing preliminary analysis and evidence collection. The benefit of adopting a bypass deployment was that it did not impact the flow and process of original system. Depending on the performance of the probe devices, additional detection modules such as anti-virus engine, file sandbox, traffic sandbox, hidden channel detection, User and Entity Behavior Analytic (UEBA) can be integrated to share the computing pressure of the cloud Threat Intelligence Big Data Platform.

3. Terminals: Terminal probes threat detection

The terminal probe works in the driver layer of the terminal system, and performs real-time, comprehensive and deep collection and forensic on suspicious data involved in malicious program execution such as terminal processes, files, services, memory, registry, hooks, and network flow. The terminal probe will spend a little amount of terminal system overhead, which has a certain impact on CPU performance.

4. Response: Manual analysis and tracing

It is necessary to conduct manual analysis and tracing for the high-risk threats or high-risk events based on threat intelligence big data platform, network probes and terminal probes.

The analysis process of malicious samples is also the process of recognizing the attackers [8, 9], from which the purpose and target of the attack can be inferred. Features extracted from the sample can be further correlated with merged homologous events, proactively detect potential compromised hosts, trace the source of attack, and even implement counter-attack strategies.

The security Operation Center (SOC) and Security Information and Event Management (SIEM) were two kind of mainstream platform which can represent the collaboration theory of "Cloud, Transport layer, Terminals and Manual Response". SIEM focused on statistical analysis of security logs, system assets, user behavior, and assisted analysts in threat monitoring and location. The SOC focused on the management of the security incident analysis process upon the SIEM, and it was adapt to the companies with independent security and maintenance department. But independent of what kind of the platforms used by the upper layer, the essential core capabilities were depend on the capabilities of the network probes and terminal probes, the analysis ability of the algorithms, and the experience of the security analysts.

4.2 Best Practices in WannaCry Ransomware Response

This kind of APT attack defense model had played an important role in the detection and response on the WannaCry ransomware attack. WannaCry ransomware spread and invaded the hoses by using the EternalBlue program which exploded the vulnerability of MS17-010. EternalBlue is an advanced exploit tool leaking from NAS (National Security Agency) [10]. Feature-based detection such as HASH detection and CVE detection were not able to detect this ransomware.

By adopting the thread detection model, the APT attack defense system of Dongxun Tech successfully detected the WannaCry ransomware. First of all, the network probes deployed in the transport layer discovered the attack package exploited the ms17-010 vulnerability and then locked the destination hosts. The terminal probes deployed at the destination hosts detect a suspected sample named 'wcry.exe'. The wrcy.exe evaded feature-based detection such as HASH detection and CVE detection. Terminal probes upload this sample to the cloud platform. Cloud platform analyzed the sample's behavior. The sample wrcy.exe could create three system processes: attrib.exe, taskdl.exe, cmd.exe, at the same time this sample invoked sensitive API, and existed obviously behavior of ransomware characteristics such as encryption behavior and writing behavior. Based on the above information, the defense system identified this sample as a high-risk threat. The defense system automatically cut off the attack traffic and alarmed to the cyber security administrator. The administrator responded to this alarm and further analyzed the assets under this threat. By adopting this thread detection model and the corresponding defense system, the WannaCry ransomware attack had been prevented timely.

5 Conclusion

APT attack offense and defense is a long-term continuous confrontation process. Focus on the problem of detecting unknown threats hidden in APT attacks, this paper presented a novel model of APT attack defense based on threat detection. Based on the model, this paper presented a technique framework with the collaboration theory of "Cloud, Transport layer, Terminals and Manual Response" to detect the threat of APT attack. Compared with traditional security methods, out method is more effective on detecting unknown attack threats. This paper is based on years of practical experience of Dongxun Tech. and try to deconstruct the APT attack framework and techniques from a more unique perspective by establishing an attack model. And then described the defense model according the features of APT attack. The authors of this paper hoped through this elaboration to inspire the readers of cybersecurity practitioners.

References

1. Daly, M.K.: Advanced persistent threat. Usenix **4**(4), 2013–2016 (2009)
2. Thabet, A.: Stuxnet malware analysis paper. Code Project (2011)
3. Bencsath, B.: The cousins of stuxnet, duqu, flame, and gauss. Future Internet **4**(4), 971–1003 (2012)
4. SkyEye: OceanLotus APT Report. https://ti.360.net/static/upload/report/file/OceanLotus Report.pdf. Accessed 29 May 2015
5. SkyEye. APT-C-07 Report. https://ti.360.net/uploads/2018/01/26/ea9d6d29c2218746acaf 87a68a2bbc1e.pdf. Accessed 30 May 2016
6. Hutchins, E.M.: Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, vol. 1(1), p. 80 (2011)
7. Indicator of compromise [EB/OL]. https://en.wikipedia.org/wiki/Indicator_of_compromise. Accessed 19 Jan 2018
8. Shufu, L.: Analysis of Typical APT Attack Cases. Netinfo Securtiy, pp. 85–88 (2016)
9. DongXun 2046Lab: APT Report: Harvest Event (DX-APT1) [EB/OL]. http://www.freebuf. com/articles/paper/111557.html. Accessed 22 Aug 2016
10. Nakashima, E., Timberg, C.: NSA officials worried about the day its potent hacking tool would get loose. Then it did, Washington Post. Accessed 19 Dec 2017. ISSN 0190-8286