Research on Prevention Solution of Advanced Persistent Threat

Xiaomei Liu
Information Management School
Beijing Information and Science Technology University
Beijing, China
e-mail: liu_allyssa@163.com

Abstract—This paper analyzes the process of Google Aurora attack, summarizes the typical steps of APT attacks. By analyzing the defects on traditional enterprise security architecture, this paper proposes a new security solution with a central analysis and control module. The module adopts a detection mode based on the storage, and it is divided into storage layer, analysis layer and presentation layer.

Keywords— APT attacks; malicious website; IDS; traffic analysis; anomaly detection

After Google mail servers were penetrated by advanced persistent threat(APT) attacks, the attacks occur frequently in the field of network security. APT attacks don't adopt new attack techniques and tools, but they can get confidential information by using unknown vulnerabilities of the target system and using long-lasting invasion. This paper analyzes the processes of Google Aurora attack, and then summed up the typical steps of APT attacks. By analyzing the defects of traditional enterprise security architecture against APT attacks, this paper presents a new security solution with a centralized analysis and control module. The module uses storage-based detection mode and is divided into storage layer, analysis layer and presentation layer.

I. BACKGROUND OF APT ATTACKS

After Google Aurora attacks in 2010, in information security field there is a new term : APT. Attack processes of the event is as follows : (1)probing the information of Google employees through social engineering. The hacker selected specific Google employees as target, and gathered relevant information from FaceBook, Twitter, LinkedIn and other social network as possible , such as employees' e-mail address , friends list, and so on. ( 2 ) the hacker created a malicious website hosting fake photos and used a dynamic DNS provider to do domain name resolution for this website . Attacked Google employees received the network link from trusted colleague, clicked on it , and entered the malicious website. The malicious web page contained JavaScript program code with shellcode which caused IE by vulnerability. This year, many experts expressed great concern, such as Du Yue jin, director of the National Institute of Information Technology network security, has said APT attacks do not use new technology, it's methods are constantly improved, the hacker's technology is relatively superb, enterprises are increasingly difficult to find and prevent APT attacks. From recent monitoring data , APT attacks which are detected are just a very small part, but the impact of the attack and the resulting harm are indeed great.

II. TYPICAL PROCEDURE OF APT ATTACKS

According to APT attacks occurring in recent years, it can be summed up the typical process includes directional information collection, a single point of attack to break, the construction of control pipeline, expansion of the network penetration and uploading the collected data and other steps:

A. Directional Information Collection

A hacker has targeted to collect network topology of the organization and internal employees' information. There are a lot of information collection methods, including network vulnerability scanning, and social engineering, and so on. According to APT attacks currently found, the majority of APT attacks are starting from the staff in the organization, so a hacker pays much attention to internal staff, such as the...
micro-blog, blog, micro-channel of internal employees, in order to understand their social relationships and hobbies, and then to attack the computers of employees through social engineering methods to enter the organization's internal network. Network vulnerability scanning is to use vulnerability scanning tools to discover the network topology and vulnerabilities. A hacker generally uses vulnerability scanning tools with good concealment, in order to prevent from being found in the first step.

B. A Single Point of Attack to Break

After a hacker collects enough information, he uses malicious code to attack employees' personal computers in the organization. Attack methods include:

- Social engineering methods, such as sending a file attachment that contains malicious code to employees via Email. When employees open the attachment, the computer is infected with malicious code.
- Remote vulnerability attack methods, such as through SQL injection, XSS, CSRF and other means to break through web server facing extranet network. Through invading web server, a hacker does vulnerability scanning to other internal servers or terminal host, and prepare for the further invasion; or placed the Trojan on the web site which the staff frequently visits. When employees visit the site, his computer will be attacked by the Trojan. RSA company was attacked by Watering hole last year which is such an attack method. These malicious code often attacks unknown vulnerabilities in the system, which can't be detected by the existing anti-virus and personal firewall security tools. The final result is that employees' PC is infected with malicious code, and completely controlled by the hacker.

C. The Construction of Control Pipeline

After a hacker controls a computer, he need to build some kind of contact channels and gain further attacks instruction. In this case, the malicious code installed on the computer is usually a client, the server is installed on the hacker host. The hacker will construct a command control pipeline between the personal computer and the hacker computer. This command control pipeline currently uses HTTP protocol to break through the organization's firewall, and more advanced command control pipeline uses the HTTPS protocol.

D. Expansion of the Network Penetration.

In general, the employee's computer which the hacker first breaks is not his target. His target is other servers which contain the organization's important assets. So the employee's computer is just regarded as a springboard, a hacker will penetrate laterally the internal network to capture more computers and servers. The methods of expansion of the network penetration include password guessing and vulnerability attack.

E. Uploading the Collected Data

During expansion of the network penetration and long-term latent process, the hacker consciously collects important asset data on each server, compresses and encrypts and packages the data, and then through a hidden pipe transfers the data back to the hacker.

III. THE SHORTCOMINGS OF TRADITIONAL NETWORK SECURITY ARCHITECTURE AGAINST APT

Traditional enterprise network security architecture is often a security mode with three layers which is "Firewall + Intrusion Detection System + Host Protection " mode. First, in order to prevent unauthorized access to the enterprise, a firewall is usually deployed in the network, which can analyze and control various network traffic, including the network layer, transport layer, application layer and data. when the firewall finds illegal invasion, it will cut off the network connection. Secondly, through the deployment of intrusion detection systems, it can monitor the network, and find a variety of attacks, aggressive behavior or attack results in order to ensure the confidentiality, integrity and availability of network resources. Finally, network security products are deployed on critical business servers and terminal hosts, such as the anti-virus and data access control software on file servers, mail filtering security software on the mail server, and client security products on the terminal hosts. In this mode, the security module is scattered in various nodes of the network shown in Figure 1.

Figure 1. Traditional network security architecture

It seems that this three-layers architecture provides an enterprise with a full range of protection, both in the network entry position, the internal network, or servers, and terminal hosts. But in practice, there are some shortcomings in this solution[2]:

A. Inadequate Protection

Most intrusion detection systems use feature matching as principle judgment, which can only detect known attack behavior whose feature is extracted. While APT attacks usually use unknown attacks such as 0 Day, special Trojans, hidden channel transmission, which can not be identified by way of misuse detection. And suspicious attacks can be
identified only by anomaly detection. Similarly, the
discovery of the virus is usually based on pattern matching.
The speed of the virus database update and the accuracy of
virus database have a greater impact on the effectiveness of
the result. Only when the corresponding virus samples are
found, the anti-virus companies develop the code of killing
the virus, and a user updates the virus database, virus
protection is effective. Existing intrusion detection system
and virus software are actually passive protection.

B. Ineffectiveness Against APT

Traditional intrusion detection system detects real-time
network traffic data, and only determines whether there are
aggressive behaviors. APT attacks intrude internal network
for few months, and the time span of the whole process is
very long, so analysis in a single time point can not identify
the real intentions of the hacker. Only association analysis
many single attacks can effectively detect APT, and find out
the whole picture of the attack.

C. Lack of Integrity

Bucket theory applies to enterprise security which should
be an organic whole. The damage of any piece of wood can
cause enterprise security problems, and all other security
measures are useless. The three-layers network security
system actually is in different network locations. These three
layers exist independently and do not form an organic whole.
The information which they gain is not sharing in the whole
system. Despite in the small number of enterprises the
linkage between the firewall and intrusion detection system
has been achieved, but the effect is not significant [2].

IV. THE SOLUTION OF ATP DETECTION AND PREVENTION

Considering these shortcomings, in order to effectively
defend APT and offer an enterprises an organic unity of the
security environment, an enterprise can deploy the security
architecture in Figure 2 which is centralized and hierarchical.
The network security architecture is based on the traditional
three-layers security mode (Firewall + Intrusion Detection
System and Host Protection) and adds a centralized analysis
and control module. On the one hand, the module expands
the detection area which save data captured by the IDS
sensor to make the overall analysis in the future, so the
architecture supports not only real-time network traffic
detection, but also asynchronous detection based on
historical time windows. The module enriches judgment
methods which adopt anomaly detection based on misuse
detection, so the architecture can detect unknown attacks, as
well as known attacks[6]. This paper proposes a new
detection module based on storage, which is divided into
three layers:

A. Storage Layer

This layer storages full flow captured by IDS sensor.
Because of preserving all the historical traffic data, when
IDS detects attacks and alarms, the analyst can analyze the
alarm and alarms which were occurred before and failed to
arouse attention of analyst. Thereby through this
retrospective correlation analysis, the analyst can grasp the
whole picture of the attack process and effectively identify
the real intention of the hacker. With the full flow of data
storage, you can use detailed analysis of historical data,
analyze data at any time, take a variety of detection and
analysis techniques and tools. This is the biggest highlight of
the solution[6].

Massive historical data takes up a lot of space, which is
impractical, so data degradation measure must be taken to
save space. On the one hand, full flow data in the current
month is backed up (the length of time is selectable for a
user), and historical data before is degraded. According to
the result of IDS alarms, only attack-related data is saved for
subsequent analysis. On the other hand, this layer does
anomaly detection analysis of deleted data, leaving the
suspect data, and completely removes data unrelated with
attacks to save space. This degradation operation makes the
storage layer practical, which offers service to analysis layer
and presentation layer.
B. Analysis Layer

This layer analyzes remaining data. It uses anomaly detection and alarms. Main means include:

1) Abnormal Traffic Detection and Statistical Analysis: Its main function is to identify attacks which cause significantly abnormal network traffic, such as DoS, vulnerability scanning, worm propagation and so on. Abnormal traffic detection need to build comprehensive and accurate safety guidelines. Statistical analysis can accurately locate the cause and location of abnormal behavior.

2) Suspicious Behavior Modeling: Its main role is to identify unknown attacks which can cause traffic anomaly, such as 0Day, special Trojans, hidden channel. For example, although the feature of special Trojan is not extracted, some kind of behavior may happen, such as unknown encrypted transmission when the console is connected by the server, a malicious domain name access, intermittent connectivity, abnormal flow down the line, and so on. So it is possible to detect these suspicious behaviors by association analysis.

3) Detailed Analysis of Alarm Data: Its main function is to reduce the false alarm rate of anomaly detection. Anomaly detection module is lack of attack signature to match. Compared with misuse detection based on feature matching, anomaly detection is with high false alarm rate and low False negative rate, so it is necessary to analyze in detail and regenerate original packet which causes anomaly detection alarms. The analysts analyze not only protocol header information of each layer, but also the application data which can help analysts to determine whether the contents of the session include the attack data to further generate accurate alarm.

C. Presentation Layer

The presentation layer is not focused on detecting a step in APT attacks. It covers the entire process of APT attacks. In fact, it is a network forensics technology, and it can integrate all kinds of alarms which isolated attacks cause. This layer can identify the semantic of these attacks, and establish a complete attack scenarios. So presentation layer will provide front-end visual analysis tool for the analysis, and a user will have a comprehensive understanding of the attacks.

Association rules can be used to match attack scenarios. Due to the diversity and complexity of APT attacks, it is difficult to detect all attacks. Finally, both the establishment of APT scene and construction of a complete attack path diagram will fail. For this problem, the system presents scenarios matching program which uses an incomplete attack path of attack, and use multi-dimensional data visualization analysis. So the presentation layer can display the result from address, port, protocol type, data content and other dimensions.[7].

ACKNOWLEDGMENT

This project is supported by school fund of Beijing Information and Science Technology University in 2013

REFERENCES

[1] Jiang Yuan, “Those Things of APT attacks,” Information Security and Communications Privacy, Nov. 2011, pp. 22–23
[2] Xu Ting, "A Hierarchical-centralized Network Security Architecture Effectively Preventing APT Attacks," Information Security and Communications Privacy, Jun. 2013, pp. 65-67
[3] Electronic Publication: Detailed Processes of Eight Typical APT Attacks
[4] Zhang Shuai, "The Detection and Defense about APT Attack," Information Security and Technology, Sep. 2011, pp. 125-127
[5] Liu Ting Ting, "APT Attack Creeping and Enterprise Information Facing "Precision Strike"," Information Security and Communications Privacy, Mar. 2013, pp. 39-40
[6] Electronic Publication: APT Detection Principle Based On Memory
[7] Liu Zhi Jie, "An alert correlating algorithm based on multi-step attack path graphs: MSACA," Journal of Nanjing University, Dec. 2008, pp. 56-59