Available online www.jocpr.com

Journal of Chemical and Pharmaceutical Research, 2014, 6(7):572-576

Research Article

ISSN : 0975-7384
CODEN(USA) : JCPRC5

The prevent of advanced persistent threat

Guangmingzi Yang[1]*, Zhihong Tian[2] and Wenliang Duan[3]

[1]*Beijing University of Posts and Telecommunications, China*
[2]*School of Computer Science and Technology, HarBin Institute of Technology, China*
[3]*Beijing Hit Computer Network and Information Security Technology Research, China*

ABSTRACT

Advanced persistent threat (APT) has received broad interest in recent years. APT stands for aiming at specific goal, experienced attackers use advanced technique and take a long period of time to collect information or break the network. APT can't be blocked through traditional ways for the incubation period always being several month even years, and the initial invasion always being too complicated to be prevented. Faced these threats, a new efficient approach should be discovered and applicated to protect our network.

Key words: APT, network security, big data, IDS

INTRODUCTION

1.1. Definition of APT attack

Advanced Persistent Threat is a hotspot in network security nowadays. As its name APT mainly include three aspects.

1) Advanced

When the attackers starts an APT project, they can combine all the instrusionmethods , techniques and tools. Because they think single instrusion method such as SQL injection, trojan always be blocked by the traditional IDS or firewall. So they use their own instrusion tools and combine with other method such as 0day vulnerability to make their first invasion unstoppable. If the first time is failed, they can wait some time and organized another attack. Compared with the traditional invasion method, APT attack is more technical and complicated.

2) Persistent

Not as the traditional hackers who want a small interest or just for fun, APT attackers have clear goal at the very beginning. For the final success, they can spend a long period of time to arrange their attack, several month even years is possible, which makes the defense much more difficult.

3) Threat

As mentioned above, APT attacks need advanced techniques and persistent work, so the result must be deadly. APT attackers always be hired by some organizations even countries, they have enough fund to complete their plan, and finally, they get a very high success rate.

Advanced, persistent and threat are the main aspects in APT attack. If the motion is economic interests or national interests, etc. the process holds a long time and the goal is not a single person in an attack, we can consider it as an APT attack.

1.2. Features of APT attack

As a target and organized way of attack, APT has no significant difference in the procedure from traditional attack. But on the specific steps, APT reflect the following characteristics to make it more destructive and harmful.

1) Highly targeted

APT attacks have clear objects and targets, including the range, target property, time limit and ending condition. They need a whole constructive plan over the target network, the protection method, and make a dynamic adjustment to achieve the best results. The previous attacking method always is always not that useful.

2) Long time persistent

Usually the targets of APT attack are highly important, so the security and protection work are always complete and stable. The attackers may take a long period of time to invade to the system and hide for couple of month or years. The security system may be useful right now, but after years, they may be vulnerable. Then the best chance is coming.

3) Diversity

Not like the traditional attack, the APT attackers may use different methods to make the invasion. Not only the traditional ways like injection, Trojan, but also combine with some method in social engineering, psychology. These combination will help to hide their intention and make the security department hard to defense.[1]

1. Analysis of APT

2.1. Background

There is a long history in attacking and defending in network security. When the enterprise and government deploy part of their affairs on the internet at the very beginning, attacks comes immediately. Some of the technique is simple such as password guessing, blocking the connection, but other comes more difficult and lead to deadly destruction such as stealing the key information, modifying the content and deleting important statistics. The reason why governments and enterprises become the first target is obvious, these organizations always have valued message or secret information.

APT attacks also focus on these organizations, the difference is the techniques and methods being used. The attacking and defending plans are all dynamic. Attackers need finding new vulnerabilities and developing new tools to complete their task while security engineers need updating their firewall and strategies to make sure the information is safe enough. Otherwise, with the development of the cloud computing and distributed framework, there are more vulnerabilities and weakness than before, which makes APT attacks much more destructive.

Table 1.The difference between APT attacks and normal attacks by organizations

Introduction	APT attack	Attack by organizations
Weather ruin the network	No	Yes
Targeted or not	Yes	No
Lifecycle	Long	Once
Method	0day Social engineering	Normal hacking tools Faked URL Trojans, norms
Difficulty to discover	< 10%	> 95%

2.2. Life cycle

According to the analysis to the happened APT attacks, researchers consider the life cycle of APT as 6 parts, which are information collect, initial compromise, command and control, move laterally, data mining and mission complete.

1) Information collect

At the beginning of an APT attack, the attackers will collect all kinds of information and decide which should be used to achieve their goal. They usually focus on the employees of the target organization because this method is simple but efficient. Statistics show that only 31% of the enterprises have a punishment to the employee who paste the secret information on the social website, which makes hackers easy enough to get information they need.

2) Initial compromise

After the information collection, attackers will plan to invade to the internal network of the target. This is always performed by use of social engineering and spear phishing, over email, using zero-day viruses. Another popular infection method was planting malware on a website that the victim employees will be likely to visit. There are people who are likely to click the dangerous links in about 87% of the organizations.

3) Command and control
This part is consist of two steps. The first step is establish foothold — plant remote administration software in victim's network, create network backdoors and tunnels allowing stealth access to its infrastructure. And the second step is escalate privileges — use exploits and password cracking to acquire administrator privileges over victim's computer and possibly expand it to Windows domain administrator accounts.

4) Move laterally
When the previous steps are complete, attackers will search for the target information in the internal network. First task is internal reconnaissance, which means collect information on surrounding infrastructure, trust relationships, Windows domain structure. Then the attackers expand control to other workstations, servers and infrastructure elements and perform data harvesting on them.

5) Data mining
To ensure to get the key information in the task, APT will hide for a long time. This reflects the persistent in the attack. The data expert will analyze the information they have got and guide the attackers to search for the most valuable information.

6) Mission complete
The final part is to exfiltrate stolen data from victim's network. It is better to complete this process without causing any attention, because the later to be inspected, the safer they will be.[7]

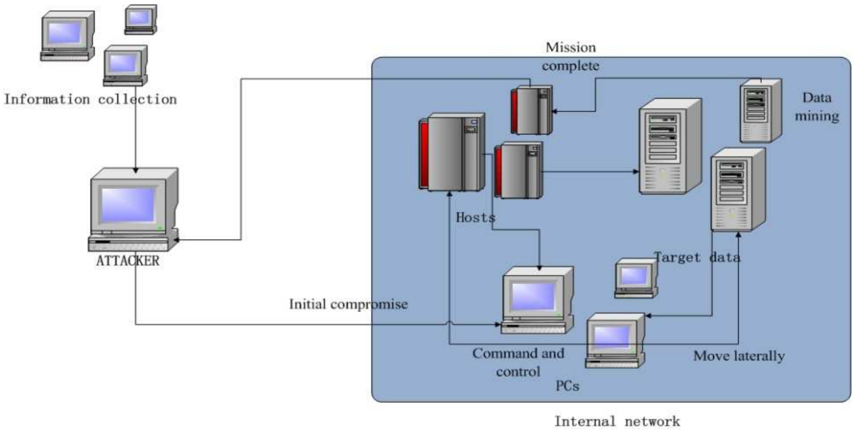

Figure 1.The process of APT attacks

2.3. **Cause analysis**

Security vulnerabilities and the lack of security awareness were the main causes to the security issue. But with the development of the hardware and software techniques, APT attackers can still breakthrough the system. The reasons include:

1) APT attacks always use the 0 day vulnerabilities so that the security system can not recognize the unusual flow.
2) In the internal network, attackers can use the SSL VPN to control the host. Because the data is encrypted, existing content detecting system can not recognize.
3) When the attackers got the target data, they use the legal method to zip and send out, it is also impossible to judge.[2][9]

2. Defense of the APT

3.1 Detection of the APT

It is necessary to detect the security threat at first time when we want to block or defend the APT attacks. Looking at the life cycle of the APT attacks, it's nearly impossible to detect the APT after the attackers control several hosts for they can hide in the normal programs. So the detection must be applied in the steps at beginning.

In the information collecting period, attackers need to use various tools to scan the target network, if we can list the syslog, netflow data, alarms and other information systematically, we can probably discover the signal of APT attacks.
In the initial compromise period, attackers have already found the useful weaknesses and use the Trojan, sql injection or any other tools to complete the invasion. At this time, it reflects on the improvement of the illegal operation, such as

password changing, privilege improving and new startup programs. We can use the IDS or IPS method to detect these kind of invasion and discover the APT attacks.

If the attackers complete the initial compromise, they may turn to hide in the internal network. They may be out of work at most time and only receive little command when necessary. If they get the content be encrypted, the detection work may be very difficult. Only if the content has not been encrypted, we may use the content analysis to discover the APT attacks.

On the whole, the earlier to find the unusual information of APT attacks, the easier to block them. After the attackers control several hosts, it is nearly impossible to detect the attacks. Although the APT attackers always fade themselves very well, there must be some evidence to prove the invasion. But the key information always can't be found easily for there are too much redundant information. Apart from this, the APT attackers always planned a long time action while the existed IDS or IPS system are always work in real time. In order to make the defense more useful and efficient, we suggest to use the big-data to handle the large information.

When we use the traditional IDS systems, there are a lot of alarms and warnings, much of them are incorrect, and the normal way is to ignore these alerts. But if we deploy the distributed big data analyze system, we can store all the information in the database. For example, an alert that shows a blank payload from an IP address maybe useless and be ignored as usual, but if this alert happened frequently or regularly, then it must cause our attention. So a cyclical analysis of the data form a period time of the database will contribute to detect the APT attacks.[3][4]

3.2 The respond to the APT and mitigation strategies

There are millions of malware variations, which make it an extremely challenge to protect organizations from APT. While APT activities are stealthy and hard to detect, the command and control network traffic associated with APT can be detected at the network layer level. Deep log analyses and log correlation from various sources can be useful in detecting APT activities – it's all about the logs. Agents can be used to collect logs (TCP and UDP) directly from assets into a syslog server. Then a Security Information and Event Management (SIEM) tool can correlate and analyze logs.

The respond to APT attacks relies on the efficient detecting system, the more information we have collected, the more easily to clear the threat. When the APT started to send out the target data, a quick action may minimum the lost. If the big data analysis system has been deployed, we can search the database very quickly and find all information linked to the injured host, and even get information of the attackers and locate them. If we don't have clear awareness of the attack, we can use normal ways to minimum the lost.

1) Disconnect from the infected host.

When an APT attack is confirmed, we must close all the connections to the infected host and execute the anti-virus software immediately.

2) Isolate the core network

Isolation of the core network can prevent the subsequent loss, besides, the isolation may protect the evidence of the APT attacks and might help to locate the attackers.

3) Analyze the attacking routine

Discover the ignored alerts, analyze the system logs, activate the invalid firewall and so on. Make a conclusion to the attack and study the pattern or model of the attack, add the model to the database and submit the event to the security organization is necessary.[8]

3. Key technologies

4.1 Exotic sandbox detection based on full net flow

The new sandbox detection introduce the full netflow information to the sandbox module, to monitor the character of the files, system process and network behavior in a complete condition. Using the dynamic monitor strategies to the system-across calls especially the system process and register jumping, to avoid the threat of harmful codes which can evade from the static code scanning. The difficulty is weather the model of sandbox being complete and efficient. If not, the harmful codes may be ignored.

4.2 Behavior analysis based on identity

The target is to detect the invasion from abnormal behavior. We can build model based on the normal behavior, compare the current behavior of hosts or users to the normal model, to judge if the behavior is an invasion. In the judging process, we can observe the difference of current behavior and normal behavior, if the statistics exceed the threshold, then we can consider the behavior as an invasion. The advantage is that we can discover some of the unknown attacks such as 0day. And the difficulty is the modeling and the analysis of behavior and the comparison algorithm. Besides, the incorrect threshold will lead to the incorrect alerts or the missing of alarms.[6]

4.3 Network flow audition based on big data

As mentioned above, the network flow audition based on big data is very useful when defending the APT attack, but there are many difficulties in the technique currently. The collection of the full information from different layer of the network, different location of the physical equipments, different IO interfaces need a good framework. The analyzing process should be efficient, which can be hardly for the current distributed systems like hadoop because they are not designed to work in real-time. And of course, appropriate plan for the information handling and data mining is of great importance.

4.4 Evidence collection and attacks playback

We can use the cloud storage to keep the status of the network and host, including the system logs and copy of the memories. When the attacks happen, the evidence will help to locate the attackers and the playback is help to study the attack's patterns. The difficulty is not in the storing technique but in the using of the data. Extracting the data like the copy of memories and finding the useful information need a series of tools and methods.[5][10]

CONCLUSION

The traditional security system is not work well when facing the APT attacks while the new technologies are not complete yet. Through analyzing the life cycle of APT, locating the key point in the attacking process and discovering the efficient defense techniques, we can minimum the lost and prevent a part of the APT. The next step is to combine the new technologies, strategies, and build a perfect framework for the security system which can protect us from the APT attacks.

Ackonwledgements

The project supported by the Hi-Tech Research and Development Program of China (Grant Nos.2012AA012506,2012AA01A401,2012AA012901), the Fundamental Research Funds for the Central Universities, Contract No. 2012JBM030.

REFERENCES

[1] "*Anatomy of an Advanced Persistent Threat* (APT)". Dell SecureWorks. Retrieved **2012**-05-21.

[2] "Are you being targeted by an Advanced Persistent Threat?". Command Five Pty Ltd. Retrieved **2011**-03-31.

[3] Eric M. Hutchins, Michael J. Clopperty, Rohan M. Amin, Ph.D. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains". *Lockheed Martin Corporation Abstract*. Retrieved March 13, **2013.**

[4] F. Duran, S. H. Conrad, G. N. Conrad, D. P. Duggan, and E. B. Held. "Building A System For InsiderSecurity". *IEEE Security & Privacy*, 7(6):30{38, **2009**. doi: 10.1109/MSP.2009.111.

[5] "*Understanding the Advanced Persistent Threat". Tom Parker*. February 4, 2010. Retrieved **2010**-02-04.

[6] "Advanced Persistent Threats: Higher Education Security Risks". *Dell SecureWorks*. Retrieved **2012**-09-15.

[7] "What's an APT? A Brief Definition". Damballa. Archived from the original on 11 February **2010**. Retrieved **2010**-01-20.

[8] Sood, Aditya KEnbody, Richard J."Targeted Cyberattacks: A Superset of Advanced Persistent Threats". *IEEE security &amp; privacy*. Retrieved **2013**-01.

[9] Shun-TeLiuYi-Ming ChenHui-Ching Hung. "N-Victims: An Approach to Determine N-Victims for APT Investigations". Retrieved **2012**

[10] Amichai Shulman. "Cyber-Crime and the State: Defining Advanced Persistent Threats (APT)". *Managing Informatio*n. Retrieved **2011**-05.

[11] George V. Hulme. "Advanced persistent threats in the spotlight". *Computerworld Canada*. Retrieved **2011**-04.