An Advanced Persistent Threats Awareness Technology Based on “Condensed matter”

Yutong Wang[1, a], Chaowen Chang[1, b] and Zengbang Ma[1, c]

[1] Henan Key Laboratory of Information Security, Zhengzhou Information and Science Technology Institute, Zhengzhou 450000, China;

[a]wyt87380345@126.com, [b]ccw@xdja.com, [c]184767606@qq.com

Keywords: APT attacks, Condensed matter, Internal states, Awareness technology

Abstract. Today, Advanced Persistent Threats have become typical network security threats. However, traditional methods of defense such as rule matching, virus database and vulnerabilities database can only reflect the characteristics of the known attacks. For the unknown APT attacks hidden inside the system, traditional methods can’t find them. Since the final results of APT attacks will cause abnormal changes of certain states within the system, based on this method, we studied on the APT attacks Awareness technology based on “Condensed matter” in deep. This technology can depict the security risks which the system faced from the internal states and aware the abnormal changes caused by APT attacks. A new defense method against APT attacks is proposed in this paper.

Introduction

With the rapid development of computer systems, Intrusion attack methods are becoming large-scale, distributed and complex. In June 2010, Stuxnet virus swept the industry across the world. It’s known as the world's first network "Super destructive weapon", “Super factory virus”, "Pandora's Box" and so on. Bushehr nuclear power plant is seriously attacked by Struxnet, suffered huge losses. Stuxnet can invade the system through a special method and easily break the physical limitations of industry-specific LAN, putting the absolutely safe national infrastructure projects into a dangerous situation. APT is a new type of network attack emerged in recent years. Fig. 1 shows the occurrence timeline of recent APT attacks. We can see that APT attacks primarily aimed at business systems of national infrastructure, service systems of major internet companies and confidential documents of important international conferences which have important strategic significance. Some are even the lifeblood of national security. In advanced cyberwarfare doctrine ,US Department of Defense clearly points that detection and defense against APT attacks is the most essential and basic component of the entire risk management chain.

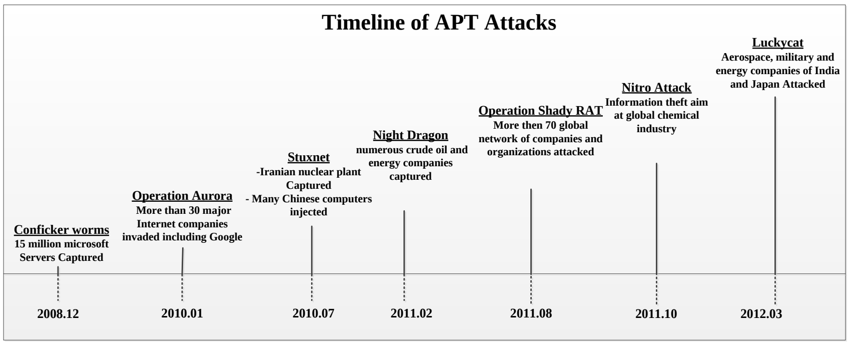
Timeline of APT Attacks
Conficker worms
15 million microsoft Servers Captured
Operation Aurora
More than 30 major Internet companies invaded including Google
Stuxnet
-Iranian nuclear plant Captured
- Many Chinese computers injected
Night Dragon
numerous crude oil and energy companies captured
Operation Shady RAT
More then 70 global network of companies and organizations attacked
Nitro Attack
Information theft aim at global chemical industry
Luckycat
Aerospace, military and energy companies of India and Japan Attacked
2008.12
2010.01
2010.07
2011.02
2011.08
2011.10
2012.03

Fig. 1 Timeline of APT attacks

The reason traditional detection methods are difficult to play a role in APT defense is that APT is a cumulative process of a multi-step attack and a single step has little influence on computer system. Traditional detection methods can’t really reflect the internal security of the computer system. These methods are difficult to find subtle changes inside the computer system. On the external representation, the systems which suffered from APT attacks act the same as those systems under normal operating conditions, but illegal data flow and internal abnormal states will be generated inside the systems. Therefore, we must start from the internal states to find APT attacks by detecting changes of the states within the systems.

Related works

Current studies on APT attacks defense and awareness are mostly about the combination of traditional defense means and defense strategies. In paper [2], the process of APT attacks are analyzed in detail. The abnormal changes caused by APT attacks at early and late stage are given, an enterprise-class APT perception and alarm frame is proposed at last. In paper [3], the author analyzes the main characteristics and life cycle of APT attacks. The author also proposes an eight-layer APT defense system based on a combination of a variety of traditional means such as antivirus, sandbox, and so on. However these studies do not propose a new type of APT defense and awareness technology. These strategies are just the recombination and redeployment of traditional means and have not overcome the shortcomings of traditional means.

Many domestic and foreign internet companies proposed the security platforms such as “FireEye” [4], “FireEye of Kingsoft” [5] and so on. But these products were unable to get rid of the inherent method of analyzing malicious attacks and difficult to analyze thoroughly the ever-changing unknown attacks.

In paper [6], the team of Yuejin Du proposed a security architecture to deal with APT attacks： ”Wizeye”. With high and low monitoring technology coordination，it can monitor and detect the APT from its source，pathway and terminal. However, APT attacks is a cumulative process of attack effect of all layers and stages, the effect of a single stage is next to nothing. The architecture is difficult to effectively detect the minor changes within system.

In this paper, we proposed an Advanced Persistent Threats awareness technology based on “condensed matter” aiming at changing the shortcomings of traditional detection methods. It emphasizes to find the “minor changes” within the system caused by APT attacks and accumulate them to expose APT attacks under the structure. This structure will improve the security of computer systems in a stereoscopic view.

Analyses on APT Attack Process

The network analysts of US Air Force firstly proposed the concept of APT attacks[1]. US National Institute of Standards and Technology gives explicitly definition of APT attack: “Attackers who are proficient at sophisticated attack technologies use a variety of attack vectors (network, physical and fraud) to create the opportunity for achieving their purpose with abundant resources.” In this section, we will analyze the attack process in detail.

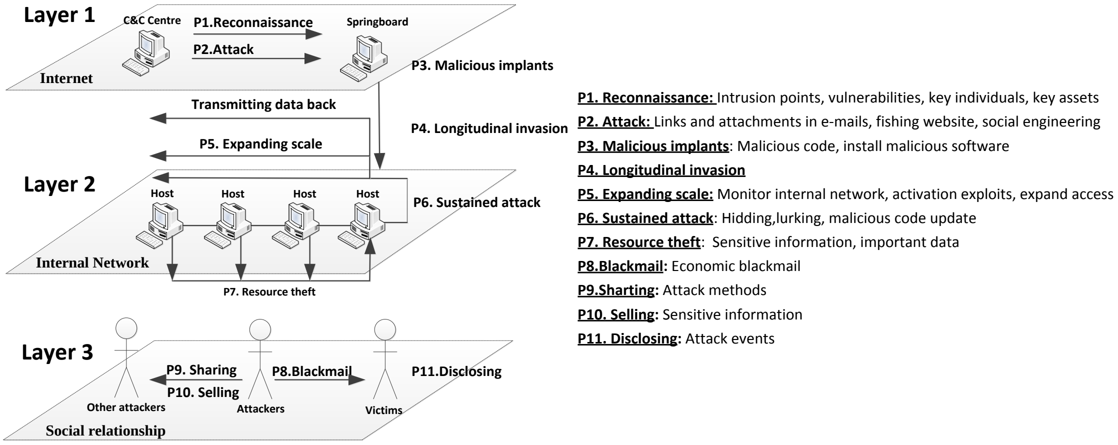
Layer 1
C&C Centre
P1.Reconnaissance
P2.Attack
Springboard
P3. Malicious implants
Internet
Transmitting data back
P4. Longitudinal invasion
P5. Expanding scale
Layer 2
Host
Host
Host
Host
P6. Sustained attack
Internal Network
P7. Resource theft
Layer 3
P9. Sharing
P10. Selling
P8.Blackmail
P11.Disclosing
Other attackers
Attackers
Victims
Social relationship
P1. Reconnaissance: Intrusion points, vulnerabilities, key individuals, key assets
P2. Attack: Links and attachments in e-mails, fishing website, social engineering
P3. Malicious implants: Malicious code, install malicious software
P4. Longitudinal invasion
P5. Expanding scale: Monitor internal network, activation exploits, expand access
P6. Sustained attack: Hidding,lurking, malicious code update
P7. Resource theft: Sensitive information, important data
P8.Blackmail: Economic blackmail
P9.Sharting: Attack methods
P10. Selling: Sensitive information
P11. Disclosing: Attack events

Fig. 2 A three-layer model of APT attacks

Fig. 2 shows the three-layer model of APT attacks. According to the characteristics of APT attacks, APT attack process is divided into three layers, each layer is in different network environment. Each layer contains several steps and has its specific purpose.

Layer 1: network detection, Attack initialization and malicious implantation.

Network Reconnaissance: Attackers use the internet to reconnoiter target network and study the invasive points, vulnerabilities, key individuals and key assets. This may contain the top-level management personnel, IT managers and the hosts which can access the internal resources.

Attack initialization： This step involves a variety of means and intends to obtain access rights of target hosts. Attackers start targeted attacks, spear phishing and keep a low profile to avoid detection. The following means included:

- E-mails with embedded website links which will download malwares.
- E-mails with attachments which are common format files (such as OFFICE documents, PDF documents, etc.).
- Phishing sites which the key individuals are interested.
- Getting users' credentials which have high-level access rights through a social engineering approach.

Malicious implantation: The attackers usually install malicious code on the hosts with privilege on the internet. They would remotely manipulate the infected hosts through C&C services and implant other related services on the hosts. The services allow attackers to remotely update malware, add new malware and send commands to the infected hosts. Then, the services send back the network information and other important data back to the command center through internet. The information will assist the attackers in the next attack step.

Layer 2: longitudinal penetration, expanding scale, sustained attack and resources theft.

Longitudinal penetration: Sensitive information which is related to the internal private network may be stored in the infected hosts on the internet. The attackers may take the infected hosts as a springboard, or use sensitive information to longitudinally permeate to the internal private network.

Expanding scale: Once attackers gain a foothold on the internal private network, they will try to expand their access rights with greatest efforts. At the same time, the malware starts to monitor the internal private network connections collecting related information. According to the information, they will find server addresses, network structure and the possibility of expanding access rights. Attackers could also attempt to activate the system-level security vulnerabilities to infect other known hosts on internal private network in order to gain more control authority.

Sustained attack: After the attackers invade to the internal private network, they will conceal themselves to lurk for a long time. They will send update instruction back to the C&C center via the springboard hosts. Then they download and update malicious code to evade the detection of updated anti-virus software in order to achieve the purpose of sustained attack.

Resources theft: At this step, the attackers have taken control of multiple hosts within the internal private network. For ensuring to get sensitive information and valuable data which is more important within the broken network, attackers will deeply excavate all the advantageous resources. Then, the stolen data will be sent to the C&C center. If the new data keeps valuable for the attackers, this step will continue for a long period of time. Ultimately, if the attackers complete its target or the victims find and cut off the attack, the entire process will be terminated.

Layer 3: blackmail, sharing, selling and disclosing

Blackmail: The attackers will demand for economic benefits from the victims and threat the them with disclosing the stolen information. The victims will pay money to avoid regulatory fines, brand damage or loss of customers. This is a common way for the attackers converting stolen information to economic interests.

Sharing: If the whole attack process is not impeded, the attackers may share or sell the attack methods to other attackers. Then other attackers will repeat the whole attack process in order to achieve their purpose.

Selling: If the victims' sensitive information (such as names, credit card numbers and passwords, e-mail address, etc.) is stolen, the attackers may sell the information to low-level attackers. Low-level attackers will keep further data theft. For example: they may steal money with victims' credit card numbers and passwords.

Disclosing: Finally, under the pressure of laws and regulations, victims have to disclose the attack events.

APT Awareness Technology

According to the characteristics and process of APT attacks, the victims can be regarded as a three-layer system composed of internet layer (including internet and the hosts on it), internal private network layer and internal terminals layer from a technical analysis. To start from the internal network and the terminals to find the influence traces of the system caused by APT attacks, we need to establish a state model which can depict the internal working status of the system from multiple dimensions. The state model should include multiple dimensions such as data, behavior, resources and network. Then security risks of the system can be found through a full and effective deployment with a variety of detection technologies and methods. Thus we are able to accurately aware the security status of the system and discover the hidden APT attacks.

The Concept of “Condensed Matter”

“Condensed matter” we called means an assemblage of various states within the system at a moment. It’s a cumulative process of APT attacks impacting on the target network and hosts in each step. It’s also a process which the system gradually deviates from normal operation status. We can call it an abnormal transfer process of “Condensed matter”

We characterize the “condensed matter” as a four-tuple $C =< D, B, R, P >$. “Condensed matter” model is a state model designed to fully depict security status within the system. Four dimensions of “condensed matter” model are shown in Table 1.

Table 1 “Condensed matter” and its four dimensions

Parameters	Implications
D	Data dimension
B	Behaviour dimension
R	Resource dimension
P	Network dimension

The Transfer Model of “Condensed Matter” based on Hidden Markov Models (HMM)

Every network attack will change one or several coagulation dimension of “condensed” matter” within the system. Its intended effect is any abnormal “condensed matter”. We can depict the entire attack process as an abnormal transfer process of “condensed matter”.

In order to describe the transfer model of “condensed matter” more clearly, we use hidden Markov model (HMM) to describe the transfer process. HMM is a double random process. One is used to describe the transfer of implicit state and the other one is used to describe the statistical relationship between the states and the observed values. HMM has three assumptions: the current status is only relevant to the previous status, the probabilities of states transfer is unrelated to time, the observed value is only relevant to current states. These three assumptions greatly reduce the complexity of the model.

We assume state sequence as $q = (q_1, q_1, \dots q_T)$ and the corresponding sequence of observed value as $O = (o_1, o_1, \dots o_T)$. So the transfer model can be characterized as a quintuple $\Omega = (V_S, V_o, \alpha, \beta, \pi)$ with the following parameters:

V_S is the state collection $q_i \in V_S = (\theta_1, \theta_2, \dots \theta_n)$; V_O is the collection of the observed values $o_i \in V_O = (v_1, v_2, \dots v_n)$; α is the state transfer matrix; β is the probability matrix of the observed values; π is the probability vector of the initial state. They satisfy the following formula:

$$\alpha = (a_{ij})_{N\times N}, a_{ij} = P(\frac{q_{t+1} = \theta_j}{q_t = \theta_i}), 1 \le i \le N, 1 \le j \le N \qquad (1)$$

$$\beta = (b_{jk})_{N\times M}, b_{jk} = P(\frac{O_t = v_k}{q_t = \theta_j}), 1 \le j \le N, 1 \le k \le N \qquad (2)$$

$$\pi = (\pi_1, \pi_2, \ldots \pi_N), \pi_i = P(q_1 = \theta_i), 1 \le i \le N \qquad (3)$$

The construction of this model usually contains three stages: training, decoding and evaluating.

Training: According to the observed values of one dimension, the sequence of the observed values *O* can be determined. Based on the sequence *O*, the model will be continuously trained with Baum-Welch Algorithm and the parameters collection $\lambda = (\alpha, \beta, \pi)$ will be obtained which makes $P(q / 0, \lambda)$ maximum[8].

Decoding: According to the sequence of the observed values *O* and the obtained parameters collection $\lambda = (\alpha, \beta, \pi)$, we will obtain the state sequence *q* which makes $P(q / 0, \lambda)$ maximum with Viterbi Algorithm[9].

Evaluating: According to the obtained parameters collection $\lambda = (\alpha, \beta, \pi)$, we will obtain the Occurrence probability of the sequence 0 with Forward-backward Algorithm[10].

Finally, we use the historical monitored data of system under normal operating conditions to get the transfer model of “condensed matter” in one dimension. Then the four-dimension model will be obtained.

An “Abnormal matter” Awareness method based on the leaky integrate-and-fire model

“Abnormal matter” we called means the assemblage of system states which deviate from the normal transfer trail during the working process. “Abnormal matter” can be also understood as the risky “condensed matter” which deviates from the normal working status. The process of APT attacks awareness can be understood as an “Abnormal matter” awareness process.

At time *t*, we assume the distance between the “condensed matter” point C_t and standard “condensed matter” point C_t^* as $dist(C_t, C_t^*)$. In order to describe the process of the gradually deviation distance from the standard model of the “condensed matter”, we use the leaky integrate-and-fire model (LIF) to calculate the cumulative change of the deviation distance and make a judgment about whether the system deviates from the standard based on the cumulative change. Here, we select Hellinger distance (HD) as the main indicator. We use the following formula (5) to calculate the Hellinger distance:

$$dist(C_t^*, C_t) = \sum_{i=0}^{n-t} (\sqrt{C_t^*[i]} - \sqrt{C_t[i]})^2 \qquad (4)$$

In the formula, $C_t^*[i]$ represents the values of one “condensed matter” point in the standard transfer trail; $C_t[i]$ represents the observed values current transfer trail. *n* represents the length of the test window.

Fig. 3 shows the schematics of the leaky integrate-and-fire model (LIF). The model can integrate the system input in a period of time, then it will trigger some response based on the integration results. *I(t)* is the drive current, the input of the model. When the capacitor *C* is charged by the drive current, resistor *R* is constantly consuming the current. Therefore we get the formula (5):

$$I(t) = I_R(t) + I_C(t) = \frac{u}{R} + C\frac{du}{dt} \qquad (5)$$

The integration result at time t can be calculated by the following formula (6):

$$u(t) = u_r \exp(-\frac{t}{RC}) + \frac{1}{C}\int_0^t \exp(-\frac{s}{RC}) I(t - s)ds \qquad (6)$$

Since the deviation distance from the system under normal work conditions $dist(C_t^*, C_t)$ does not always equal to 0, In order to more accurately reflect the cumulative effect of the “abnormal matter” and tolerate deviation distance under normal work conditions, we will calculate the average deviation distance from under normal work conditions $dist(C_t^*, C_t)_{Ave}$ and the D-value between $dist(C_t^*, C_t)$ and $dist(C_t^*, C_t)_{Ave}$ will be used as the drive current *I(t)* (the input of the LIF). After calculation, the result will be regarded as the evaluation criteria whether the "condensed matter" transfer trail deviates from the standard model.

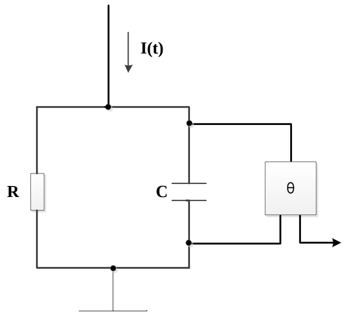

Fig. 3. The schematics of the leaky integrate-and-fire model (LIF)

Summary

In this paper, we analyzed the process of APT attacks in detail. In order to depict the security status within the system, we studied APT awareness technology. We also proposed the definitions of "Condensed matter", "Abnormal matter". However, we only proposed a new method, there are still many technical difficulties such as internal relations between the various dimensions, detection technology and implementation, etc. We will start a further study on these technical difficulties.

References

[1] Tankard c. Advanced persistent threats and how to monitor and deter them[J]. Network security，2011(8)：16-19.

[2] Mehresh R. Schemes for surviving advanced persistent threats[D]. Faculty of the Graduate School of the University at Buffalo, State University of New York, 2013.

[3] Advanced Persistent Threats: Detection, Protection and Prevention

[4] Hoover J N. In-Q-Tel Joins Forces With FireEye To Fight Cyberthreats[J]. DarkReading. Retrieved, 2009: 11-30.

[5] Fireeye. Kingsoft Fireeye online virus ldentify service [EB/OL], (2012-07-09) [2013-07-11]. http://www.egouzcom/topics/429j.html (In Chinese) (2012-07-09)[201 3-07-11]. http://www. Egouz.com/topics/4295.html)

[6] Yuejin Du, Lidong Zhai, Yue Li ,Zhaopeng Jia. Security Architecture to Deal with APT Attacks:Abnormal Discovery [J]. Journal of Computer Research and Development, 2014,07: 1633-1645.

[7] Welch L R. Hidden Markov models and the Baum-Welch algorithm[J]. IEEE Information Theory Society Newsletter, 2003, 53(4): 10-13.

[8] Viterbi A J. A personal history of the Viterbi algorithm[J]. IEEE Signal Processing Magazine, 2006, 23(4): 120-142.

[9] Yu S Z, Kobayashi H. Practical implementation of an efficient forward-backward algorithm for an explicit-duration hidden Markov model[J]. Signal Processing, IEEE Transactions on, 2006, 54(5): 1947-1951.6. Hu P, Li H, Fu H, et al. Dynamic Defense Strategy against Advanced Persistent Threat with Insiders[C]//Proc. of INFOCOM. 2015.