Analysis of Advanced Persistent Threats (APT)

Waleed Al-Sit, [1] Hani Al-Zoubi, [2] Khaldoun Qtaishat [3]
1and 2, Department of Computer Engineering
3, Department of Civil Engineering
Mu'tah Unversity
Al-Karak, Jordan
w_sitt@hotmail.com

***Abstract*— Despite the large numbers of malware programs, Advanced Persistent Threat (APT) has an appreciable impact in attack environment nowadays. APT is a deliberately cyber-attack that is utilized to target specific and sensitive information in systems without revealing itself. APTs usually use several methods of attack to have possibility of unauthorized access to system and get the targeted information. This survey studies and analysis three types of attack model and consider the attack pyramid as the model of APTs attack. Also, we present a detection framework as well as the methodology of its implementation. The method proposes to use the MapReduce operation to evaluate all the possible events and context where the attack might take place. The results show that using these methods will improve the performance as well as reduce the overall load.**

keywords: Network Security, Advanced Persistent Threats, APT detection

I. INTODUCTION

APTs are one of the most security threats that is keep fast and growing information threats. They are controlled by very skilled, motivated and organized attackers whose function is targeting the sensitive information related to political, military and financial issues from different organizations.

An investigation report in [1] shows the evidences about the data breach that was recorded in the organization logs as well as the detection mechanisms failure. This failure illustrates that traditional protection techniques can be ineffective in detecting APTs. So, a new approach is required to solve this problem.

In the last years, the number of APTs and related security incidents increased rapidly. The main reason for this is that APTs are not focusing on a single vulnerability in a system, which could be detected easily, but they are using a chain of vulnerabilities to reach the high security areas within a company network without noticed.[2]

The APTs stages are approximately similar across many attacks and they differentiate just in the methods that used to pass between stages. Figure (1) shows these stages in order:

a) Reconnaissance: in this stage, the attackers collect the required information about the organization's resources and the employees. Then they build a file for each

employee which contains all the targeted information that obtained from the social networks, e.g. Facebook.

b) Delivery: this stage contains the preparation of spear-phishing email [3] using the information in the previous stage.
c) Exploitation: malware finds its path into the system network then it has been downloaded and activated on the system. Moreover, downloading malware initialized a command and control connection. When the attacker tried to secure this connection, they start to collect information about the security system of the organization.
d) Operation: in this stage, attackers identify the main users which have special privileges in accessing. Also, they identify the servers that will store the information.
e) Data collection: attackers use the data of privileged users that have been got in the previous stages to have the ability of accessing to the targeted data.
f) Ex-filtration: all the information grouped together and transferred over a secure channel to various external servers.

Although, the APT attacks are impossible to prevent permanently but they can be detected in one of the stages as will be shown in the upcoming sections.

Another way to define the APT attack based on the acronym that has always been used is: (A) means that the operation behind the attack includes sophisticated intrusion techniques and the attackers have high specifications in terms of excellent training, progressive skills and ability of fully utilize of the intrusion techniques. (P) indicates that targeted tasks have different priority, where specific task has a high priority than other tasks that have financial or other gain. This targeting is carried through continuous controlling and persistence over a long period of time. (T)refers to the attacker's function in

which they targeted information and caused damage in the system by disrupting the services.

Based on the results that illustrate the vulnerability analysis of APT attacks [4], another important concept has to focus on is the vulnerabilities used by malicious programs. The common thought among organizations is that the zero-day vulnerabilities are crucial to the success of APT attacks. But, as shown in the figure (2), the dependency of APT attacks on the zero-day vulnerabilities is only 19% of the vulnerabilities. While, 70% of these vulnerabilities are public vulnerabilities in the malicious programs.

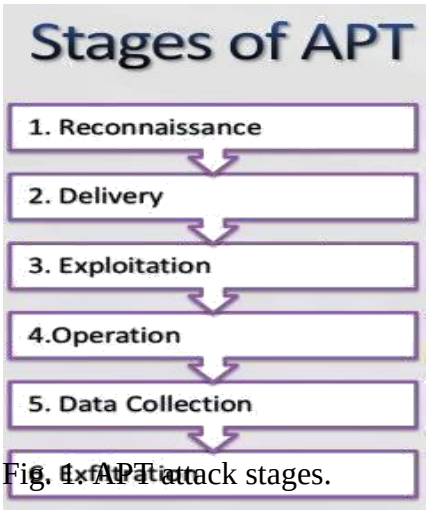


Fig. 1. APT attack stages.

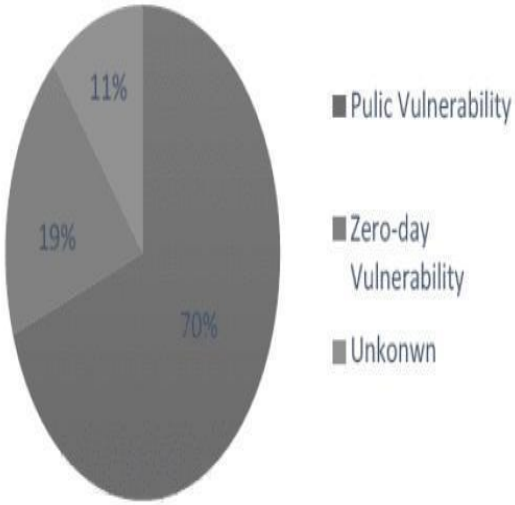


Fig. 2. The vulnerability of APT attack.

The rest of the survey is organized as follow: section II presents the attack models. The APT lifecycle represents in section III. In section IV a detection framework has been proposed and section V presents a comparison between cloud storage defense and APT attack. In section VI some of the related projects have been presented and section VII illustrates the conclusion.

II. ATTACK MODEL

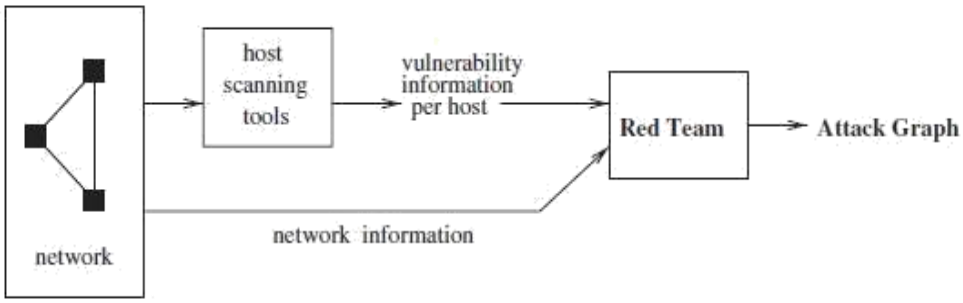
In this section, we describe three attacks model. First, the attack graphs which used to capture changes over time of the total security in the network by capturing interrelations of vulnerabilities. Second, the attack tree and finally we introduce a new APTS model called the attack pyramids.

A. Attack Graph

Attack graph has been produced by the Red team. It used to model the vulnerabilities of the systems and their potential exploits. The exploits, which leading to the partial failure of the systems, are subject of keen security interest. Apparent efforts have been expended in modeling, analyses and detection attacks. One considerable methodology is construction of attack graphs of the system for analysis and response strategies.

To evaluate the security of a network, the effects of interactions of local vulnerabilities must take into account and try to find the security holes introduced by interconnection. Figure (3) shows a typical process for vulnerability analysis of a network to produce an attack graph. First, scanning tools determine vulnerabilities of individual hosts. Then, the local vulnerability information is used along with other information about the network, such as connectivity between hosts.

Topological Vulnerability Analysis (TVA) is a tool for generating attack graphs. TVA monitors the state of network assets maintains models of network vulnerabilities and combines vulnerabilities on overall security posture. Other tools for generating attack graphs are NetSPA (Network Security Planning Architecture) and



MulVAL (Multihost, multistage, Vulnerability Analysis). NetSPA uses readily available source of data to automatically compute network reachability, classify vulnerabilities, build the graph and recommend actions to improve network security. [5]

In general, attack graphs have been used in several functions which used the attack graph as the accurate representation of the network's vulnerability. These uses are: Risk assessment, Network hardening, Intrusion Detection.

Risk Assessment: Risk assessment gets more difficult in evaluation as the networks become bigger in size and the attacks become more advanced. Risk assessments study the impact of vulnerabilities individually and also the possible combination of these vulnerabilities. The role of the attack graph is to model the possibility of all the vulnerabilities to construct attack paths.

Network hardening: in this function, attack graph is used to define the minimum cost for set of actions that must be done to eliminate the attacks against critical resources. The types of these actions include: changing configuration, trying to repair some of the network vulnerabilities at the entry points or adding intrusion detection devices to observe all the network activities.

Fig. 3. Vulnerability Analysis of a Network

Intrusion Detection: Attack graph can improve the alert correlation techniques in several ways, for example: matching intrusion events, defining the attack patterns and predicting attack plans. Attack graph can be used in this function as the correlating alerts.

Despite the many uses of attack graph, it has several difficulties in terms of using in practical security system. These challenges can be classified as follow: [7]

1- The generation of attack graph.
2- Visualization.
3- Analysis graph in order to formulate the security properties and violation detection.
4- Enough representation of system parameters in the graph.

B. Attack Tree

Attacks trees were defined by Bruce Schneier to model threats against computer systems. They provide a methodical way of describing the security of system based on varying attacks. The structure of a tree is used to represent attacks against a system with the goal as the root node and different ways of reach that goal as children nodes. Child node can be a goal and new sub-trees can be built to become as root. The nodes between children can be AND or OR nodes. OR nodes are used to represent alternatives and AND nodes are used to represent different steps toward achieving the same goal.

Figure (4) shows example of attack tree with an expected path that APT can follow. There are four children nodes that illustrate four ways to access the source code: insider, user, repository and steal server with OR nodes connected these four roots. The APT path shown in the figure illustrates six steps: first, getting contact by the spear-fishing email. Second, the malware executes and the attackers control the user machine. This right side steps (1-3) occur in the network plane while the next steps (4-6) occur in the physical plane. Step (4), the attackers initiate a C&C channel to the servers. Source code accessed through repository server and stored data on temporary server.

The approach of detection the APT path that represents in the figure as attack tree model is not usually useful. The reason of this is that the detection may need a short period of

time. So, there is a need of another model of APT to overcome this obstacle and this model is attack pyramid.

C. Attack Pyramid

Attack pyramid is a useful tool used to follow the way that the attack was performed across the system. The goal of this attack is at the top of the pyramid. Each side of the pyramid represents the step that used by attacker to reach the top of pyramid (goal) while each line of this pyramid illustrates the phases of APTs.

This survey proposed to use attack pyramids as a model of APT. Figure (5) shows the relation between the attack pyramid and the stages of APT which mentioned above in the introduction section. The attack pyramid contains of planes which depend on the specifics of the system and each plain contains of events which represent the possible attacks. Events have been divided into three types: (1) Candidate Events: this type represents candidate events even if they don't represent

any type of attack, (2) Suspicious Events: dealing with event that has an abnormal activity, (3) Attack events: events that have to be detected by security system. Also, the planes can be classified into several types. The most popular pyramid planes are the physical plane, the user plane, the network plane and the application plane.

Physical plane: this plane contains events that can construct relations with other events in another plan in case of having the same users and devices. The events in the physical plane can be as evidence that the traffic produced from a device in the working region is generated by the supposed user.

User plane: this plane identified in the initial stages of APTs where the users who have the targeted information and have the possibility of accessing into the APT goals are been monitored. Moreover, all the events that related to the targeted data are been recorded.

Network plane: the network planes contain the largest numbers of events due to the events that have been recorded by flow sensors, firewalls, intrusion detection and prevention systems. These events can correlate with number of events from other planes.

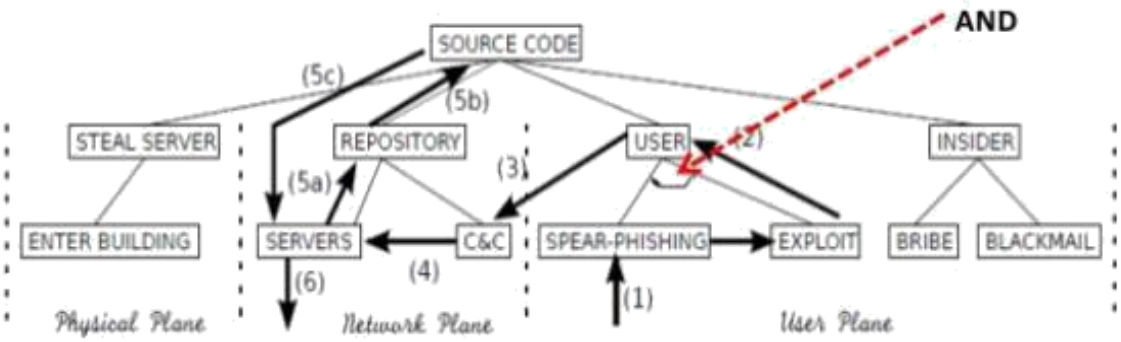
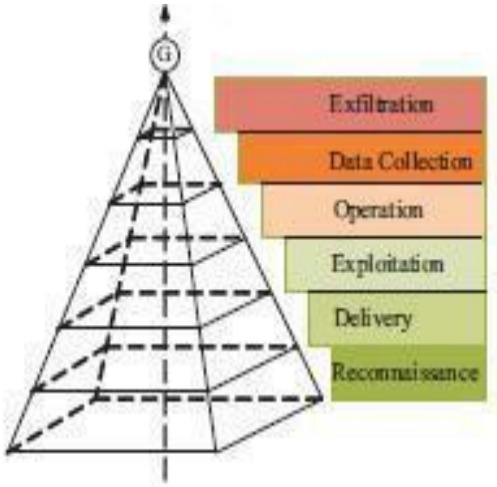


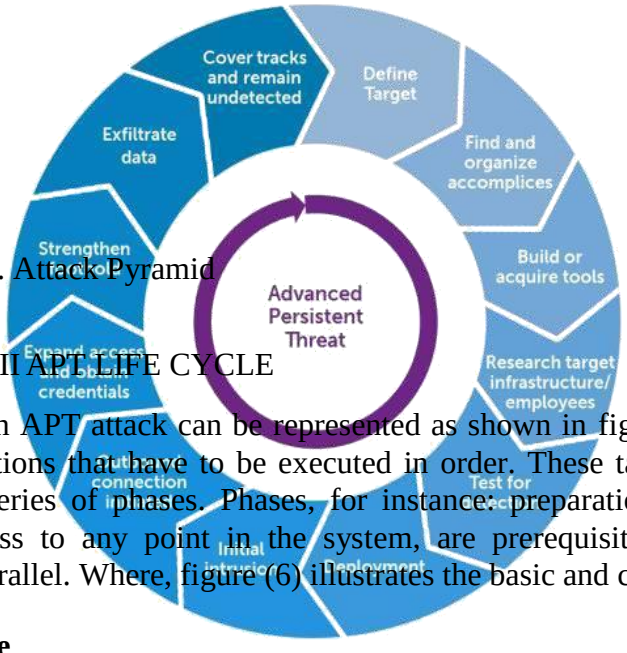
Fig. 4. Attack Tree model

Application plane: application planes list all the applications gateway, ex:SIP, RTP, DNS, email, p2p, .., and servers.

Attackers will use spear phishing on employees in the system to initiate the malware distribution, which might be observed and recorded by the email, or a SMS/MMS message.

- specify target
- search and Find accomplices
- construct or gain tools
- Research target/infrastructure/employees
- evaluate for detection





ig. 5. Attack Pyramid

III APT LIFE CYCLE

The life style of an APT attack can be represented as shown in figure (6). It can be divided into several operations that have to be executed in order. These targeted operations can be analyzes over a series of phases. Phases, for instance: preparation and get the ability of unauthorized access to any point in the system, are prerequisites. Other phases can be implemented in parallel. Where, figure (6) illustrates the basic and common phases.

Preparation phase

Preparation phase consists of the following parts of the APT lifecycle:

All the operations, that required being ready before the execution phase, are belonged to preparation phase. Whereas, APT attack comprises a large sets of preparation. The requirements and components in this phase are collected by attackers initially. These components generally cover infrastructure tools, data, information about the targeted system and other required sets.

Initial intrusion

The Initial Intrusion phase consists of the following aspects of the lifecycle:

- Deployment
- Initial intrusion
- Outbound connection initiated

The step after preparation is to get the ability of accessing to the targeted system. The common way to achieve this unauthorized access is using spear-phishing email which contains attachment for example. The links inside the email used to install the malware programs on the targeted system.

Figure (7) shows a spear-phishing email containing an attachment. Links or attachments are an executable malware, it becomes as archive files contain these malwares. These files become the vulnerabilities of the system. Whereas, if the user tried to open these malicious file, the malware program is completely installed on the system and made a big damage.

Fig. 6. APT Lifecycle

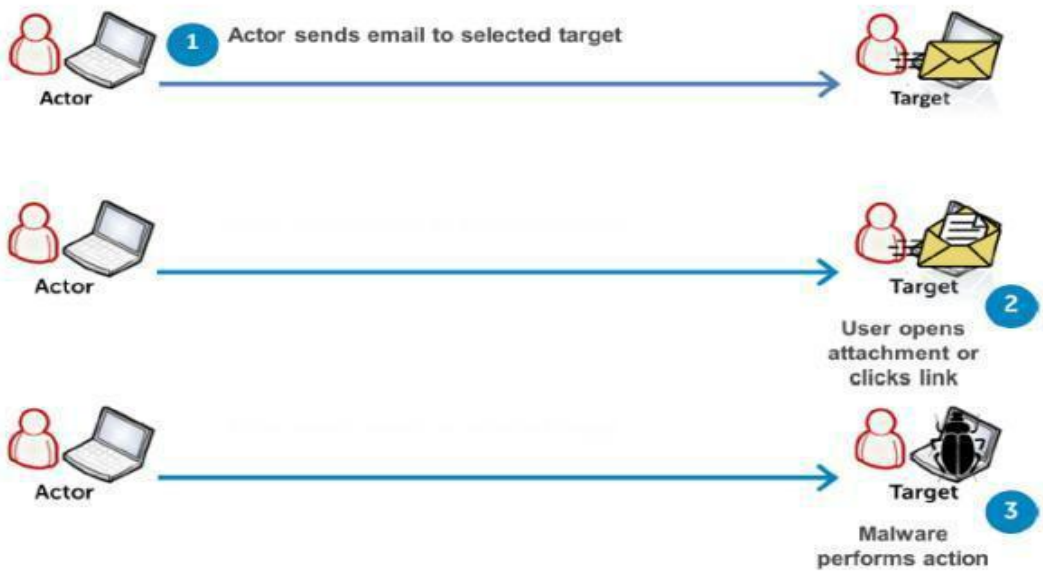


Fig. 7. The operation of sending email with malicious contents by APT attackers.

IV DETECTION FRAMEWORK

The presentation in the figure (8) is the detection framework for advanced attack advanced attack. The collected data box has a group of the information and events F1 to Fn that have been gathered using special techniques into a context and transferred these contexts to alert system box. Using the signature data base, the alert system applied detection approaches for the received contexts to check the risk level of these contexts. Based on the result of alert box, the alarm is trigged in case of high risk level. But in case of raising the alert, the analyst has to investigate the sources of this alert and take necessary steps. Moreover, there is an updated step of the signature database when the alert is upgraded into alarm.

Detection rules based on the source of information are divided into three types. First type, signature based rule, requires checking the behavior of events against attacks so to keep this type effective, it needs to be updated every period of time. In the second type which is the profiling based rule, the behavior of the monitored entity has to be checked with the behavior baselines. The last type is the policy based rules which is the static rules in the organization.

Assuming that the plane Pi is contains a set of events, pi = {ei^1,…,ei^{ki}…}, whereas the format of ei^j is ei^j = (t, id, a1, . . . , ami), where: (j) is the event index in the plane, (t) is the time when the event is listed, (id) is the identifier of event and (a) is the attribute of the event. The correlation rule concept (R) is used to present the relation between events within the plane. It defines as:

$$R = U^n i,j \; Rij$$

Where, Rij indicates the correlation rule between events in both Pi and Pj planes. After define the correlation rules between events, we can gathered the events relevant to an attack context and identified the attack. Attack context is a group of events from multiple planes that have correlations between them. It can be represented as (Aj), with

$$Aj = \{ E,R,W,H,C,L,G\}$$

Where:

E = {$e^{k1}1$, .. , $e^{ki}i$, ..} is the correlated events, R is the correlation rule, W is the time window, H is historical data about attacks, C is the attack confidence indicator, L is the attack's risk level and G is the goal. The attack risk level and the confidence indicator have been used to evaluate the threat to the goal quantitatively.

With the increasing in the number of possible security relative events and also the large set of targeted data that need to be protected, any effective detection method have to be scalable to hundreds of GB of data and thousands of events. Because of this, MapReduce framework has been presented to overcome this challenge. The idea behind this concept is to utilize a large number of clusters machines called workers to implement computation tasks by divide these tasks in parallel using Map and Reduce operations. In the first step, the input

data will split into small chunks, then using the parallel concept, each chunk will be processed by a different worker in the Map phase. While in the Reduce phase, a group of workers will implement the Reduce operation on the data which received from workers who implemented the Map operations.[8]

The steps of MapReduce framework are presented in figure (9). First step represents the collection of all the data from different resources such as: network sensors, systems logging mechanisms, perimeter security systems, etc., then they mapped to a list of goals. The events are stored for a period of time before feed it into the MapReduce operations. After that, reduce (1) takes as input a set with goal and event, and output a set with a goal and the set of all events that belong to the goal context. While the final reduce operation, reduce (2), is applied for each goal and all events in the context and its output is list of goals and all the alerts that found by implement the detection algorithm of the malicious activity. The alert system received the final output of the last reduce operation and decide whether trigger the alarm or not.

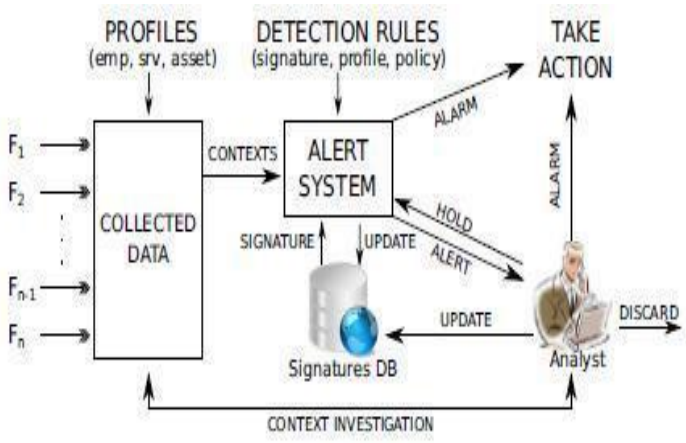


Fig. 8. Advanced Attack Detection Framework

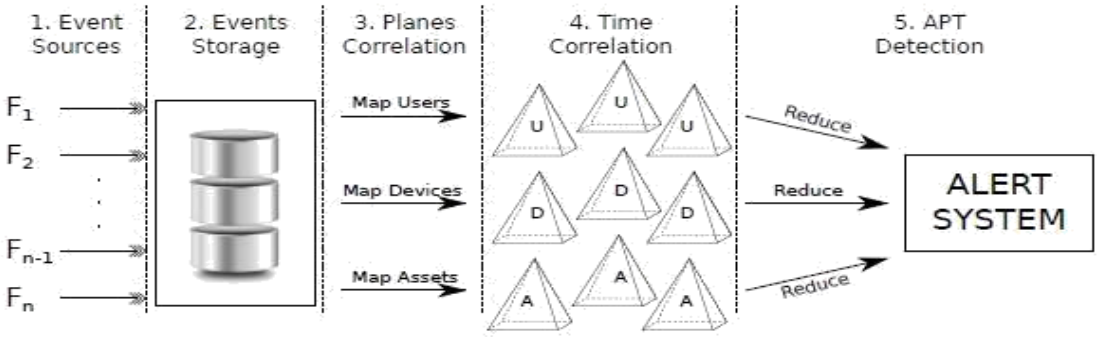


Fig. 9. MapReduce distributed computation.

V Cloud Storage Defense against APT

Cloud storage is one of the vulnerabilities to advanced persistent threats, where the attacker initiates continues and targeted attacks over systems and organizations. As shown in the introduction section, the APT attackers seek to steal the targeted information from the systems including cloud storage without being noticed. In order to make APT detection harder, attackers investigate the defense system plans of the targeted systems.

Prospect theory (PT) is used to illustrate the interaction between the cloud storage defender and the APT attackers. Also, a cloud storage defense game has been proposed in which one of the attackers picks out his time interval to initiate the APT to compromise the cloud storages and on the other hand, one of the defenders picks out its scan interval to retrieve the compromised storage.

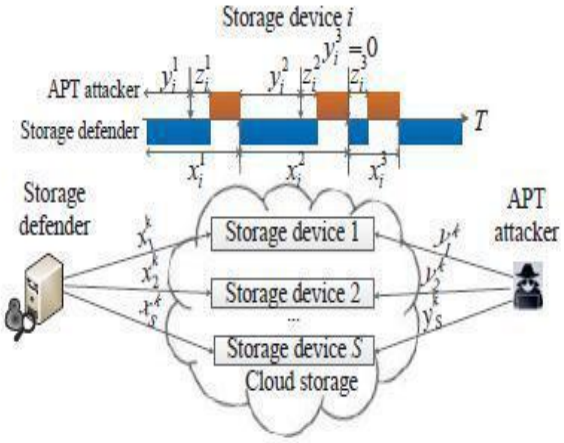


Figure (10) illustrates a cloud storage system containing storage devices (S) that surrounding with threats by the APT attack (A) and protected by the storage defense. The defender choose xk^i interval to scan storage device i, while the APT attacker takes a duration zk^i to perform the k-th attack against device i after attack interval yk^i, with $1 \leq i \leq S$ and $k > 0$.

An APT model has been proposed in [9] and show that the APT attacker can apply progressing methods and several types of malware to guess the defense procedure of the target system. Also, the attacker can mark whether the attack has the ability of controlling the target storage device and estimate the size of the stolen data to determine the interval in which the attack is detected and blocked by the defender. The attackers stay a period of time of (y^ki) before start the k-th APT attacks against cloud storage device (i), at the time of detecting these attacks, storage device will be directly restored by the defender. The interval for the entire attacks (k-th attacks) at storage device (i), denoted by z^ki, is commonly a random value which cannot be known by both attacker and defender.

Q-learning technique is based on APT defense and it used for the cloud storage defender who does not have sufficient information about the attack model. The algorithm of Q-learning is appropriate to implement. Also, it can present an optimal policy in the Markov decision process (MDP) [10]. Simulation of Q-learning is used to evaluate the performance based on the APT defense system. These simulations show that it can eliminate the attack motivations of APTs and enhance the usefulness of the defender.

Fig. 10. The illustrative process of cloud storage defense game.

VI Related Work

The first presentation of APT model as the threat tree approach was introduced by Edward Amoroso, later spread by Bruce Schneier as attack tree model. However, the attack pyramid model is considered to be more universally approach and also the only model that gets benefits from correlation rules to correlate the nodes of the tree model.

A flipit game has been presented in [11] to formulate continuous attacks of APT. This type of games, which occurs between the attacker and the defender, is investigated in [12] and displayed that the periodic defense way is the best solution against non-adaptive attackers. The type of defense which based on dynamic programming is proposed in [13], with providing an optimal solution against APT attacks. At first, the prospect theory has been used for studying network security and wireless communications. An example of this is the random access game in [14] which used prospect theory to study the accessing of channel in wireless network. The common APT approaches with multiple storage clouds and multiple levels of attack intervals have proposed in [15].

The researches differed in dividing the APT attack into stages. Where, in [16], JiaXu and Danping Zhou are divided the APT attack into six stages as follow: intelligence gathering, directional invasion, remote control, lateral movement, data mining and system destruction. While, Yiwen Liu is divided APT attack into four stages in [17].

Li, Meicong, et al. in [18] studied and analyzed a large number of APT attack cases which have been disclosed. Also, they proposed all the expected usages and purposes of the APT attacks. These purposes are varied in that paper as follow: stealing information, control, damage ...etc.

In addition, Sheyner et al. presented an example with all details of how the network attacks modals can be analyzed. Whereas, they used these attack models as an input to attack graph tool in order to generate main attack graph that illustrates all the vulnerabilities of the targeted system.

In [19], M. Balazinska et al. present an approach of using all the historical data to apply the concept of enhanced monitoring. Therefore, when the system recorded any event, the database of the historical information is directly queried for the context of this data and for all the similar events.

VII Conclusion

Based on the analysis of the APT attack, this survey summarizes the attack models and proposes the APT attack model as attack pyramids. Meanwhile, the survey presents a detection framework where it becomes possible to detect APT attack in one of its stages and propose the methodology to implement this detection approach. Moreover, a MapReduce framework is presented in this work and it achieved better performance and high flexibility rate since it used a parallel concept of splitting the tasks over multiple workers which reduce the overall load. As the cloud storage is a vulnerability

of APT attack, we proposed a defense system (cloud storage defense) against these attacks and defined the correlation between both defender and attacker based on the prospect theory. Future work deals with more complex and sophisticated attacks, so we need to test and enhance the detection algorithms and study the risk levels of these attacks in addition to use large number of correlation and detection rules. With this clear progress in the spread of these threats, we can use warning signs or key indicators that the system may face an APT attack. Examples of these indicators are: increasing of accesses at times where there is usually no

accessing to the network e.g. night hours. Another example is the observations of an unexpected flow of data from internal to external regions of the system.

REFERENCES

[1] Giura, Paul, and Wei Wang. "Using large scale distributed computing to unveil advanced persistent threats." *Science* 1.3 (2017).

[2] Friedberg, Ivo, et al. "Combating advanced persistent threats: From network event correlation to incident detection." *Computers & Security* 48:: 2015.

[3] RSA, "RSA Security Brief: Mobilizing Intelligent Security Operations for Advanced Persistent Threats," http://www.rsa.com/innovation/docs/11313 APT BRF 0211.pdf, February 2011.

[4] Q. Mi, J. Zhu, C. Xu, J. J. Zong, "Study on APT Network Attack Technology", *Computer and Modernization*, pp. 92-94, October 2014.

[5] S.Kumar, A.Negi and An.Mahanti: Generation and Risk Analysis of Network Attack Graph. Oct.2018.

[6] Yang, Yang. "On the Density and Subsequent Utility of Attack Graphs in Realistic Environments." (2017).

[7] Shandilya, Vivek, Chris B. Simmons, and Sajjan Shiva. "Use of attack graphs in security systems." Journal of Computer Networks and Communications 2014 (2014).

[8] Giura, Paul, and Wei Wang. "Using large scale distributed computing to unveil advanced persistent threats." Science 1.3 (2013): pp-93.

[9] M. Zhang, Z. Zheng, and N. B. Shroff, "A game theoretic model for defending against stealthy attacks with limited resources," in Decision and Game Theory for Security, vol. 9406, pp. 93–112, Nov. 2015.

[10] Xiao, Liang, et al. "Cloud Storage Defense Against Advanced Persistent Threats: A Prospect Theoretic Study." IEEE Journal on Selected Areas in Communications 35.3 (2017).

[11] M. van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "Flipit: The game of stealthy takeover," J.Cryptology, vol. 26, no. 4, pp. 655–713, Oct. 2013

[12] M. Zhang, Z. Zheng, and N. B. Shroff, "Stealthy attacks and observable defenses: A game theoretic model under strict resource constraints," in Proc. IEEE Global Conf. Signal Inf. Process (GlobalSIP), pp. 813–817, Atlanta, GA, Dec. 2018.

[13] M. Zhang, Z. Zheng, and N. B. Shroff, "A game theoretic model for defending against stealthy attacks with limited resources," in Decision and Game Theory for Security, vol. 9406, pp. 93–112, Nov. 2015.

[14] T. Li and N. B. Mandayam, "Prospects in a wireless random access game," in Proc. Annu. Conf. Inf. Sci. Syst., pp. 1–6, Princeton, NJ, Mar.2018

[15]] D. Xu, Y. Li, L. Xiao, N. B. Mandayam, and H. V. Poor, "Prospect theoretic study of cloud storage defense against advanced persistent threats," in Proc. IEEE Global Commun. Conf., Washington, DC, Dec.2016.

[16] .xu, D. P. Zhou, H. and D. Gu, “Review on APT attacks and detection technologies” Secrecy Science and Technology, pp. 009, 2014.

[17] Y. W. Liu, Q Huang, J Yu, and Z. L. Zhang, “The Study of APT Security Detection Architecture and Key Technologies” Journal of

[18] Security and Safety Technolog, pp. 24-29, March 2018.

[19] Li, Meicong, et al. "The study of APT attack stage model." Computer and Information Science (ICIS), 2016 IEEE/ACIS 15th International Conference on.IEEE, 2016.

[20] M. Balazinska, Y. Kwon, N. Kuchta, and D. Lee, “Moirae: History-Enhanced Monitoring, ” in CIDR, 2017.

[21] Barik, MridulSankar, AnirbanSengupta, and ChandanMazumdar. "Attack Graph Generation and Analysis Techniques." Defence Science Journal 66.6 (2016).

[22] Abraham, Subil, and Suku Nair. "A predictive framework for cyber

[23] security analytics using attack graphs." arXiv preprint arXiv:1502.01240 (2015).

[24] Friedberg, Ivo, et al. "Combating advanced persistent threats: From network event correlation to incident detection." Computers & Security 2015.

[25] Y. W. Liu, Q Huang, J Yu, and Z. L. Zhang, “The Study of APT
[26] Security Detection Architecture and Key Technologies” Journal of
[27] Security and Safety Technolog, pp. 24-29, March 2018

[28] Niu, Weina, et al. "Modeling Attack Process of Advanced Persistent Threat." Security, Privacy, and Anonymity in Computation, Communication, and Storage: 9th International Conference, SpaCCS 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings 9. Springer International Publishing, 2016.

[29] ABASS, AHMED ALABDEL, et al. "Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage." IEEE Access (2017).