International Journal of Advancements in Computer Networks and Its Security– IJCNS
Volume 4 : Issue 4 [ISSN 2250-3757]
Publication Date : 27 December,2014

Advanced Persistent Threat Attack Detection: An Overview

Ibrahim Ghafir and Vaclav Prenosil

***Abstract*—With the webs explosive growth in power and popularity has come a concomitant increase in both the number and impact of cyber criminals. For years businesses have striven to keep malware, spam and unwanted intruders at bay with varying degrees of success. Cyber criminals and spies in turn created more advanced means to breach the security measures. APTs are a new and more sophisticated version of known multistep attack scenarios and they are targeted specifically to achieve a specific goal, most often espionage. The financial loss caused by APT attacks can be very big. Moreover, these APTs form a problem for the current detection methods because these methods depend on known signatures of attacks and APTs make heavy use of unknown security holes for attacks. In this paper we present an overview of the current researches about APT attack detection. In addition, we provide a classification of these researches into three groups which are previous research findings on APT attack, Analyzing already identified of APTs and detect possible APT attack.**

***Keywords*—Advanced Persistent Threat, targeted attacks, intrusion detection, network security, cyber criminals.**

I. Introduction

The Internet is omnipresent with a currently estimated size of approximately 1.37 billion unique pages as indexed by the major search engines [1] and the world wide web has evolved from a system for serving an interconnected set of static documents to what is now a powerful, versatile, and large platform for application delivery and information dissemination and companies have increasingly put critical resources and sensitive data online. Unfortunately, with the web's explosive growth in power and popularity has come a concomitant increase in both the number and impact of cyber criminals. Cybercrime is attractive to criminals because they run a low risk at being caught and prosecuted for their crimes. The result is that a complete industry has evolved aimed at committing cybercrimes and virtually all organizations face increasing threats to their networks and the services they provide. Governments on the other hand have also found that cyberspace can be used to spy on other states and can be an arena for warfare.

At present the cost of cybercrime, criminal activities on cyber infrastructures, is considered to somewhere between 100 billion to 1 trillion US dollars annually worldwide [2]. The magnitude of the problem has prompted much interest within the security community towards researching mechanisms that can mitigate this threat. To this end, intrusion detection systems (IDSs) have been proposed as a potential means of identifying and preventing the successful exploitation of computer networks. As defined in [3], an intrusion is a sequence of related actions performed by a malicious adversary that results in the compromise of a target system. It is assumed that the actions of the intruder violate a given security policy. Intrusion detection (ID) is the process of identifying and responding to malicious activities targeted at computing and network resources.

For years businesses have striven to keep malware, spam and unwanted intruders at bay with varying degrees of success. Much of the protection they have put in place assumes that most of these attacks will be random and that, if an organization's defenses are too hard to breach, the attacker will seek an easier victim. Nowadays, according to technical report by Trend Micro [4], that situation is changing fast with the rise of targeted attacks (or advanced persistent threats/APTs), where both cyber-criminals and hackers are targeting selected organizations and persisting until they achieve their goals.

Virus scanners, firewalls and intrusion detection systems were created with the purpose to reduce the economic damages from cybercrimes. Cyber criminals and spies in turn created more advanced means to breach the security measures. An APT is a form of multistep attack that is executed with more stealth and is targeted specifically to achieve a specific goal, most often espionage. APTs use different steps, just as normal multistep attacks, in order to reach their goal. However, APTs are different in the sense that they are more often based on so-called "zero-day exploits" (not publically known security flaws in software) and advanced means of attack like social engineering [5]. APTs are currently the largest threat to companies and governments [6].

These APTs form a problem for current detection methods because these methods depend on known signatures of attacks and APTs make heavy use of unknown security holes for attacks. The economic damages due to a successful APT attack can be very high. The expected financial impact of attacks is the main influence on investments in security measures [7].

The remainder of this paper is organized as follows. Section II defines APT attack and describes the the life-cycle of this type of multistep attack. In Section III we offer an overview of the current researches about APT attack detection and provide a classification of these researches into three groups. Section IV concludes the paper and suggests future work.

Ibrahim Ghafir and Vaclav Prenosil
Faculty of Informatics, Masaryk University
Brno, Czech Republic

II. Advanced Persistent Threats (APTs)

APTs are a cybercrime category directed at business and political targets. APTs require a high degree of stealth over a prolonged duration of operation in order to be successful. The attack objectives typically extend beyond immediate financial gain, and compromised systems continue to be of service even after key systems have been breached and initial goals reached [8]. Figure 1 depicts the steps of APT attack [9].

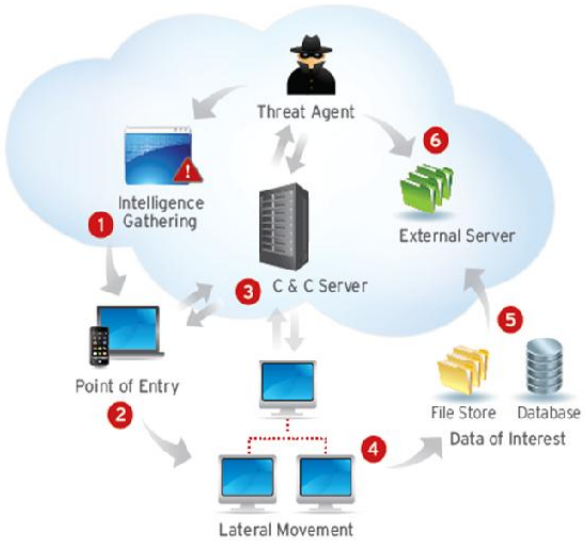

Figure. 1. Typical steps of APT attack.

1- Intelligence Gathering: Identify and research target individuals using public sources (LinkedIn, Facebook, etc) and prepare a customized attack.

2- Point of Entry: The initial compromise is typically from zero-day malware delivered via social engineering (email/IM or drive by download). A backdoor is created and the network can now be infiltrated.

3- Command and Control (C\&C) Communication: Allows the attacker to instruct and control the compromised machines and malware used for all subsequent phases.

4- Lateral Movement and Persistence: Once inside the network, attacker compromises additional machines to harvest credentials, escalate privilege levels and maintain persistent control.

5- Asset/Data Discovery: Several techniques (ex. Port scanning) are used to identify the noteworthy servers and the services that house the data of interest.

6- Data Exfiltration: Once sensitive information is gathered, the data is funneled to an internal staging server where it is chunked, compressed and often encrypted for transmission to external locations.

We can notice from the steps of attack mentioned above that APTs are a new, more sophisticated, version of known multistep attack scenarios. What makes these attacks so much more insidious than those seen in previous years is their sophistication and the use of multiple attack techniques, including social engineering and automated tools [5].

III. Advanced Persistent Threat Attack Detection

In this section we offer an overview of the current researches about APT attack detection. In addition, we provide a classification of these researches into three groups which are previous research findings on APT attack, Analyzing already identified of APTs and detect possible APT attack.

A. *Previous Research Findings on APT Attack*

The first widely reported APT was publicized by Google in January 2010, although it is believed to have begun some six months earlier. Known as Operation Aurora [5], the attack was extremely wide-scale and is believed to have targeted 34 organizations, including Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical, as well as Google itself. Analysis of the Operation Aurora attacks showed that they used extremely sophisticated tactics which, according to the security vendor McAfee, have never before been seen outside of the defense industry. The attacks started by using advanced social engineering techniques and highly targeted emails to selected individuals that contained links to websites. These in turn hosted malicious JavaScript code that was used to exploit a zero-day vulnerability in the Internet Explorer browser.

In total, it is believed that the attack used around a dozen pieces of malware to burrow deep into the network, and several layers of encryption to obfuscate the attack and avoid common detection methods. Once installed on the network, the malware used backdoors to communicate with remote Command and Control (C&C) centers via TCP port 443, which is usually associated with encrypted traffic and which is therefore difficult to inspect. Now with direct access to the network, the hackers were able to use pivoting, which is a method by which hackers exploit the systems they have compromised to attack other systems on the same network and avoid restrictions such as those set by firewalls. This allowed the hackers to explore protected intranets in order to search for intellectual property and other vulnerabilities, and then exfiltrate the information obtained to the C&C servers. Even after the C&C centers were taken down, it is known that the attacks continued for some time

In March 2009, the SecDev group in Canada released findings regarding GhostNet [10]. This study reveals the existence and operational reach of a malware-based cyber espionage network that they call GhostNet. China-based hackers have been targeted the Tibetan organizations in several countries and the research team worked directly with affected Tibetan organizations, including the Private Office of

the Dalai Lama, the Tibetan Government-in-Exile, and several Tibetan NGOs.

The data was analyzed, and led to the discovery of insecure, web-based interfaces to four control servers. These interfaces allow attacker(s) to send instructions to, and receive data from, compromised computers. The research team successfully scouted these servers, revealing a wide-ranging network of compromised computers. This extensive network consists of at least 1,295 infected computers in 103 countries. Significantly, close to 30% of the infected computers can be considered high-value and include the ministries of foreign affairs and embassies of many countries.

The GhostNet system directs infected computers to download a Trojan known as gh0st RAT that allows attackers to gain complete, real-time control. These instances of gh0st RAT are consistently controlled from commercial Internet access accounts located on the island of Hainan, People's Republic of China. The investigation reveals that GhostNet is capable of taking full control of infected computers, including searching and downloading specific files, and covertly operating attached devices, including microphones and web cameras.

The vector for spreading the GhostNet infection leverages social means. Contextually relevant emails are sent to specific targets with attached documents that are packed with exploit code and Trojan horse programmes designed to take advantage of vulnerabilities in software installed on the target's computer. Once compromised, files located on infected computers may be mined for contact information, and used to spread malware through e-mail and document attachments that appear to come from legitimate sources, and contain legitimate documents and messages. It is therefore possible that the large percentage of high value targets identified in this analysis of the GhostNet are coincidental, spread by contact between individuals who previously communicated through e-mail.

In October 2012, Kaspersky Lab's Global Research and Analysis Team initiated a new threat research after a series of attacks against computer networks of various international diplomatic service agencies [11]. A large scale cyber-espionage network was revealed and analyzed during the investigation, which they called (Red October). The main objective of the attackers was to gather intelligence from the compromised organizations, which included computer systems, personal mobile devices and network equipment.

The attackers have been active for at least several years, focusing on diplomatic and governmental agencies of various countries across the world. Information harvested from infected networks was reused in later attacks. For example, stolen credentials were compiled in a list and used when the attackers needed to guess secret phrase in other locations. To control the network of infected machines, the attackers created more than 60 domain names and several server hosting locations in different countries (mainly Germany and Russia). The C&C infrastructure is actually a chain of servers working as proxies and hiding the location of the "mothership" control server. The attackers created a multi-functional kit which has a capability of quick extension of the features that gather intelligence. The system is resistant to C&C server takeover and allows the attack to recover access to infected machines using alternative communication channels.

Beside traditional attack targets (workstations), the system is capable of stealing data from mobile devices, such as smart phones (iPhone, Nokia, Windows Mobile), enterprise network equipment (Cisco), removable disk drives (including already deleted files via a custom file recovery procedure). The research team mentioned that The samples they managed to find were using exploit code for vulnerabilities in Microsoft Word and Microsoft Excel that were created by other attackers and employed during different cyber attacks and basing on registration data of C&C servers and numerous artifacts left in executables of the malware, they strongly believe that the attackers have Russian-speaking origins.

In February 2013, Mandiant which is an information security company in USA released APT1 report exposing one of China's cyber espionage units. In this report [12] we can summarize the key findings of APT1 as follow:

APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations and has demonstrated the capability and intent to steal from dozens of organizations simultaneously. APT1 compromise 141 companies spanning 20 major industries and once APT1 has established access, they periodically revisit the victim's network over several months or years and steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership. Among other large-scale thefts of intellectual property, they have observed APT1 stealing 6.5 terabytes of compressed data from a single organization over a ten-month time period.

APT1 focuses on compromising organizations across a broad range of industries in English-speaking countries. Of the 141 APT1 victims, 87% of them are headquartered in countries where English is the native language. APT1 maintains an extensive infrastructure of computer systems around the world. They have observed APT1 establish a minimum of 937 Command and Control (C2) servers hosted on 849 distinct IP addresses in 13 countries. In over 97% of the 1,905 times Mandiant observed APT1 intruders connecting to their attack infrastructure, APT1 used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language.

B. *Analyzing Already Identified of APTs*

In [13], the authors show how to determine, from a known targeted attack, the N most likely victims of the attack, they develop a search engine for APT investigators to quickly uncover the potential victims based on the attributes of a known APT victim, by improving the performance in terms of detection rate and false positives with regards to N-gram based approaches.

In [14], the authors provide an in-depth analysis of a large corpus of targeted attacks identified by Symantec during the year 2011. Using advanced TRIAGE data analytics, they are able to attribute series of targeted attacks to attack campaigns

quite likely performed by the same individuals. By analyzing the characteristics and dynamics of those campaigns, they provide new insights into the modus operandi of attackers involved in those campaigns. They evaluate the prevalence and sophistication level of those targeted attacks by analyzing the malicious attachments used as droppers. While a majority of the observed attacks rely mostly on social engineering, have a low level of malware sophistication and use little obfuscation, their malware analysis also shows that at least eight attack campaigns started about two weeks before the disclosure date of the exploited vulnerabilities, and therefore were probably using zero-day attacks at that time.

In [15], they show that it is possible, by using an undirected graph, to associate attacks according to the targets shared between separate attacks and it is possible to build a map of APT activity and identify clusters that may represent the activities of single team of malware writers.

C. *Detect Possible APT Attack*

In [16], they propose a novel system that processes threat information collected on the users' side to detect potential targeted attacks (APT attacks) and by using their approach they are able to reduce the millions of normal malicious events down to a more manageable amount for further in-deep analysis.

They use a combination of clustering techniques to identify groups of machines that share a similar behavior with respect to the malicious resources they request (e.g., exploit kits, drive-by downloads or C&C servers). They correlate the location and industry information in which these machines operate (e.g., oil & gas or government) to discover interesting attack operations and they implemented their system in a working prototype that they called SPuNge.

Their approach consists of two phases. In first stage, they analyze the malicious URLs that regular users machines access over HTTP(S) with an Internet browser, another HTTP client or because infected by a malware. They identify those machines that present a similar network behavior, e.g., accessing web pages used within the same phishing campaign or malware infection. They apply a combination of clustering techniques to group together similar malicious URLs, and they "organize" the machines based on the clusters of URLs that they requested.

In the second phase, they correlate the clusters of machines presenting a similar behavior, and they identify those machines, networks or organizations that are more likely to be involved in a targeted attack. For example, because operating in the same industry (e.g., oil & gas). They developed an analysis framework to analyze the results of the processing and to automatically generate a report for the security analyst.

Although they claim that their empirical results show that their approach works well in practice and is helpful in assisting security analysts in cybercrime investigations, but they depend on their analysis for APT detection on one vector which is malicious URLs and don't take into consideration the other vectors involved in APT lifecycle. Besides this approach is not independent because they based their analysis on a data feed that collected and provided by an antivirus vendor, which also means that it is not real time detection and they should wait for that data.

In [17], they present an abridged version of their initial Duqu analysis, which is a new malware involved in APT attack against a European company aiming at stealing the information. They also describe the Duqu detector toolkit, a set of heuristic tools that they developed to detect Duqu and its variants.

They provide six tools to heuristically detect Duqu variants and their tools can be broadly categorized into three areas: detecting file existence anomalies (FindDuquSys, FindDuquTmp, FindPNFnoINF), detecting properties of files and registry entries (CalcPNFEntropy, FindDuquReg) and analyzing code injection into running processes (GetProcMem). The output of these tools are stored in a log file, where suspicious files, memory regions, registry entries are indicated together with their corresponding hashes.

The authors mentioned themselves that there is a potential impact of false negatives and their tools require a careful investigation of results by security experts. In addition, we can notice that some of these tools are rather simple and would be easy to defeat by changing the malware, so they can only be used to detect existing infections.

IV. Conclusion

In this paper we present an overview of the current researches about APT attack detection. In addition, we provide a classification of these researches into three groups which are previous research findings on APT attack, Analyzing already identified of APTs and detect possible APT attack.

APTs are a new and more sophisticated version of known multistep attack scenarios. The financial loss caused by APT attacks can be very big. Moreover, these APTs form a problem for the current detection methods because these methods depend on known signatures of attacks and APTs make heavy use of unknown security holes for attacks. Based on the fact that antivirus and network intrusion detection products, two of the most widely used security technologies, face serious shortcoming in the detection of APT, we consider that there is need for a change in their architecture and detection strategies.

Given the related works presented in this paper, most of the above works focus on analyzing already identified campaigns. In addition, none of the related works address explicitly the problem of detecting potential APT attacks by means of malicious traffic aggregation and correlation between detection methods. Our future work aims at detecting APT attack based on the correlation between the detection methods of some techniques used by the attacker through the life cycle of APT attack. We believe that the opportunity for using this approach in APTs detection is big and, to the best of our knowledge, still unexplored.

References

[1] M. de Kunder, "The size of the world wide web," http://www.worldwidewebsize.com/, accessed: 2014-01-07.

[2] N. Kshetri, The global cybercrime industry: economic, institutional and strategic perspectives. Springer, 2010.

[3] F. Valeur and G. Vigna, Intrusion detection and correlation: challenges and solutions. Springer, 2005, vol. 14.

[4] T. M. technical report, "Targeted attacks and how to defend against them," http://www.trendmicro.co.uk/media/misc/targeted-attacks-and-how-to-defend-against-them-en.pdf, accessed: 2013-12-20.

[5] C. Tankard, "Advanced persistent threats and how to monitor and deter them," Network security, vol. 2011, no. 8, pp. 16–19, 2011.

[6] P. Wood, M. Nisbet, G. Egan, N. Johnston, K. Haley, B. Krishnappa, T.K. Tran, I. Asrar, O. Cox, S. Hittel et al., "Symantec internet security threat report trends for 2011," Volume XVII, 2012.

[7] T. R. Rakes, J. K. Deane, and L. Paul Rees, "It security planning under uncertainty for high-impact events," Omega, vol. 40, no. 1, pp. 79–88, 2012.

[8] Damballa, "Advanced persistent threats (apt)," https://www.damballa.com/knowledge/advanced-persistent-threats.php, accessed: 2013-12-26.

[9] T. M. white paper, "The custom defense against targeted attacks," http://www.trendmicro.fr/media/wp/custom-defense-against-targeted-attacks-whitepaper-en.pdf, accessed: 2013-12-25.

[10] R. Deibert and R. Rohozinski, "Tracking ghostnet: Investigating a cyber espionage network," Information Warfare Monitor, p. 6, 2009.

[11] K. L. ZAO, "Red october diplomatic cyber attacks investigation," http://www.securelist.com/en/analysis/204792262/RedOctober Diplomatic Cyber Attacks Investigation, accessed: 2013-12-27.

[12] M. I. Center, "Apt1: Exposing one of china's cyber espionage units," Mandiant, Tech. Rep, Tech. Rep., 2013.

[13] S.-T. Liu, Y.-M. Chen, and S.-J. Lin, "A novel search engine to uncover potential victims for apt investigations," in Network and Parallel Computing. Springer, 2013, pp. 405–416.

[14] O. Thonnard, L. Bilge, G. O'Gorman, S. Kiernan, and M. Lee, "Industrial espionage and targeted attacks: Understanding the characteristics of an escalating threat," in Research in Attacks, Intrusions, and Defenses. Springer, 2012, pp. 64–85.

[15] M. Lee and D. Lewis, "Clustering disparate attacks: Mapping the activities of the advanced persistent threat." in Proceedings of the 21st Virus Bulletin International Conference.(October 2011) pp, pp. 122–127.

[16] M. Balduzzi, V. Ciangaglini, and R. McArdle, "Targeted attacks detection with spunge," 2013.

[17] B. Bencs´ath, G. P´ek, L. Butty´an, and M. F´elegyh´azi, "Duqu: Analysis, detection, and lessons learned," in ACM European Workshop on System Security (EuroSec), vol. 2012, 2012.