ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Study and Review on Advanced Persistent Threats

Neeshu Sahu, Prof. Shitanshu Jain

Research Scholar, Dept. of Computer Science & Engg, Gyan Ganga Instt. of Technology & Sciences, Jabalpur, India

Professor, Dept. of Computer Science & Engg, Gyan Ganga Instt. of Technology & Sciences, Jabalpur, India

ABSTRACT: Advanced Persistent Threats (APTs) have become a major concern for IT security professionals around the world. Since the birth of Internet, cyber securities have always been an area full of unsolved problems for researchers. Particularly in the age of information, every corporate and government site needs to keep their sensitive data secure from hackers or intruders. With rapid advancement in improved security measures, there always comes along a threat which forces researchers to be on alert. In recent times Advanced Persistent Threat (APT) has been among the most highlighted threat for security experts. At early stages such attacks were dedicated to government or financial organizations, but recent studies based on security breaches indicate that such attacks are now carried out on a much wider domain. In this paper crucial attack stages with the most common methods and tools use by intruders to initiate APTs are discussed, along with recommendation on how a model can be defined to perceive an APT attack being conducted on a network.

KEYWORDS*:* Network Security, Advanced Persistent Threats, Network Security Attack

I. INTRODUCTION

Advanced Persistent Threats (APTs) are a cybercrime category directed at business and political targets. APTs require a high degree of stealithiness over a prolonged duration of operation in order to be successful. The attack objectives therefore 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. Definitions of precisely what an APT is can vary widely, but can best be summarized by their named requirements:
Advanced – Criminal operators behind the threat utilize the full spectrum of computer intrusion technologies and techniques. While individual components of the attack may not be classed as particularly “advanced” (e.g. malware components generated from commonly available DIY construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They combine multiple attack methodologies and tools in order to reach and compromise their target.

Persistent – Criminal operators give priority to a specific task, rather than opportunistically seeking immediate financial gain. This distinction implies that the attackers are guided by external entities. The attack is conducted through continuous monitoring and interaction in order to achieve the defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a “low-and-slow” approach is usually more successful.

Threat – means that there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The criminal operators have a specific objective and are skilled, motivated, organized and well funded.

DOI: 10.15680/IJIRCCE.2016. 0411226

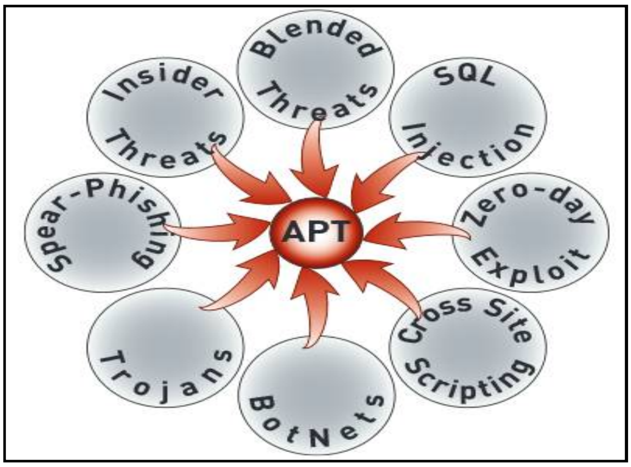

Fig. 1.1 Advanced Persistent Threats

1.1 How Advanced Persistent Threats Breach Enterprises:

APTs breach enterprises through a wide variety of vectors, even in the presence of properly designed and maintained defence-in-depth strategies:

- Internet-based malware infection
- Physical malware infection
- External exploitation

Well funded APT adversaries do not necessarily need to breach perimeter security controls from an external perspective. They can, and often do, leverage “insider threat” and “trusted connection” vectors to access and compromise targeted systems. Abuse and compromise of “trusted connections” is a key ingredient for many APTs. While the targeted organization may employ sophisticated technologies in order to prevent infection and compromise of their digital systems, criminal operators often tunnel in to an organization using the hijacked credentials of employees or business partners, or via less-secured remote offices. As such, almost any organization or remote site may fall victim to an APT and be utilized as a soft entry or information harvesting point. A key requirement for APTs is to remain invisible for as long as possible. As such, the criminal operators of APT technologies tend to focus on low and slow attacks – stealthily moving from one compromised host to the next, without generating regular or predictable network traffic – to hunt for their specific data or system objectives. Tremendous effort is invested to ensure that malicious actions cannot be observed by legitimate operators of the systems.

At the very heart of every APT lies remote control functionality. Criminal operators rely upon this capability in order to navigate to specific hosts within target organizations, exploit and manipulate local systems, and gain continuous access to critical information. If an APT cannot connect with its criminal operators, then it cannot transmit any intelligence it may have captured. In effect, it has been neutered. This characteristic makes APTs appear as a sub-category of botnets. While APT malware can remain stealthy at the host level, the network activity associated with remote control is more easily identified. As such, APT’s are most effectively identified, contained and disrupted at the network level.

II. APT CHARACTERISTICS

Targeted: APTs target specific organizations with the purpose of stealing specific data or causing specific damage. This stands in direct contrast to most historical malware, which wreaks havoc on any randomly infected system. The RSA attack targeted intellectual property. These were not opportunistic attacks victimizing just any organization with vulnerability to a given exploit. These were focused campaigns. y perpetrators willing to invest time and money to achieve specific objectives. There are two conclusions here. First, any organization, large or small, with valuable data is subject to APT methods. Second, the more valuable your data, the more likely you are to be targeted. The cybercrime economy is well organized and funded, with attackers investing more to achieve bigger paybacks.

Persistent: APTs play out in multiple phases over a long period of time. Prior to the actual attack, attackers only know the target organization and objective. They do not know where their target data resides, what security controls are in place, or what vulnerabilities exist that might be exploited. To steal the data, the attacker must identify vulnerabilities, evaluate existing security controls, gain access to privileged hosts within the target network, find target data, and finally, extract data from the network. The entire process may take months or even years. The lesson here is that attack detection cannot rely on any single event, but should look for patterns of events that are characteristic of APT methodologies.

Evasive: APTs are systematically designed to evade the traditional security products that most organizations have relied on for years. For example:

- To gain access to hosts within the target network while avoiding network firewalls, the attacker delivers threats within content carried over commonly allowed protocols (http, https, smtp, etc.).
- To install malware on privileged hosts while avoiding antivirus programs, the attacker writes code designed for the specific target environment. This code has never been seen before and therefore, no AV signatures exist to provide protection.
- To send data out of the target network, while again avoiding firewalls, the attacker uses custom encryption and tunnels content within protocols that are allowed outbound by the firewall.

Complex: APTs apply a complex mix of attack methods targeting multiple vulnerabilities identified within the organization. A given APT may involve
1) Telephone-based social engineering to identify key individuals within the target organization,
2) Phishing emails sent to those key individuals with links to a website that executes custom JavaScript code to install a remote access tool,
3) Binary command-and control code (either custom code or code generated by commonly available malware kits) and,
4) Custom encryption technology. Clearly, no single security control provides coverage against all of these vectors.

Any successful APT defence strategy must take a multi-layered approach in which multiple detection mechanisms work together to identify complex patterns of evasive behaviour.

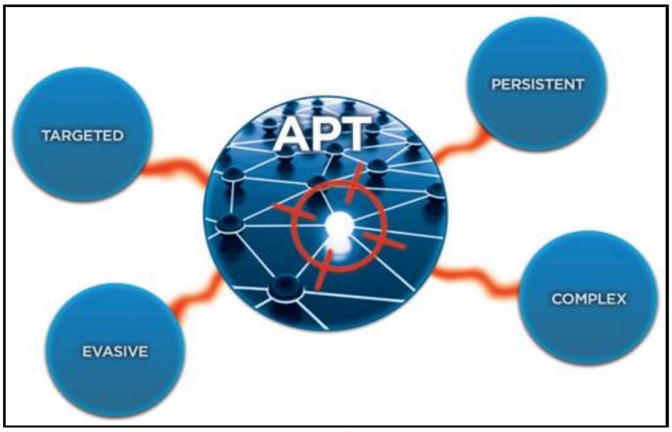

Fig. 1.2 APT Characteristics

III THE PHASES OF AN APT

All Advanced Persistent Threats share the same characteristics as they go through the attack process, for they exhibit certain phases which the attack goes through before the final goal is reached from the adversary perspective. This fact applies to all APT attacks that currently exist. The following phases describe how an APT attack is performed.

A. RECONNAISSANCE

This phase involves getting as much information as possible on the designated target at hand. Therefore besides the actual target, other information sources are commonly exploited, e.g., social networks, Internet services, or dust bins of

employees. The attackers will try and find out as much as possible about the employees of a company and create profiles
of them in order to establish an organizational topology of the company. Furthermore, they tend to use common network scan techniques like port scans to detect potential vulnerable web services for infection later on.

B. *DELIVERY*

The delivery phase tends to lure potential intermediate targets into the exploitation phase. This could be done through spear-phishing techniques or through side channel attacks. Spear Phishing is sending a specific email to a designated target which sounds legitimate for the target user in order to open up an attachment or web link.

C. EXPLOITATION

Once the user clicks on the malicious link or opens the malicious attachment, the exploitation phase starts. The user's machine gets infected with malware, more specifically; it gets infected by a root kit. This is an example of an automated approach in order to exploit a system. Other existing manual methods are SQL Injection and Cross Site Scripting. This malware is able to control the user's machine entirely. It can monitor screen output or log keystrokes. Furthermore it is able to propagate through scanning the local network for potential vulnerabilities for infecting them. All these actions are hidden from the user's machine, because the rootkit tends to hide itself. The Malware will try and set up a Command and Control connection to the attacker’s server in order to receive more specific commands.

D. *OPERATION*

In this phase the attackers scan the internal network, looking for the targeted information they want to ex-filtrate. Again they create profiles of how the internal network is structured. If they realize that the targeted information is not reachable due to tightened security measures, they escalate their privileges by sending out new spear-phishing emails in order to gain higher credentials, until they have the correct security level.

E. DATA COLLECTION

The data collection phase is all about retrieving the target information. Examples of targeted information could be insider knowledge from political emails or a closed-source code from a company. Here the sensitive data is being encrypted and compressed, so that in the exhilaration phase the data can be shipped out.

F. EXFILTRATION

The final stage is about exhilarating the target information to the drop servers. The attackers could be using certain evasive measures in order to avoid detection and tracking. One of these evasive measures is the fast-flux technique. If this phase
is successful, the attackers have succeeded in their attack and the target data is compromised and stolen. They hide their traces, which makes for forensic investigators extremely hard to detect their tracks.

IV. WORKING OF AN ADVANCED PERSISTENT THREAT

In a simple attack, the intruder tries to get in and out as quickly as possible in order to avoid detection by the network's intrusion detection system (IDS). In an APT attack, however, the goal is not to get in and out but to achieve ongoing access. To maintain access without discovery, the intruder must continuously rewrite code and employ sophisticated evasion techniques. Some APTs are so complex that they require a full time administrator. An APT attacker often uses spear phishing, a type of social engineering, to gain access to the network through legitimate means. Once access has been achieved, the attacker establishes a back door. The next step is to gather valid user credentials (especially administrative ones) and move laterally across the network, installing more back doors. The back doors allow the attacker
to install utilities and create a "ghost infrastructure" for distributing malware that remains hidden in plain sight. This malware establishes a connection with the attacker’s compromised server or a botnet to exchange information. The malware installed commonly is a Remote Administration Tool (RAT), through which the attacker can monitor and compromise the organizations network.

V. A STUDY OF APT ATTACK METHODS [12]

Paper	Attack Method
Advanced Persistent Threats: A Symantec Perspective (White Paper)	In this paper APT attack methods are broken down in to four Steps, which are incursion, discovery, capture, and exhilaration. Incursion can be performed using number of typical hacking techniques such as zero-day vulnerabilities, social engineering, SQL injection or malware. The only difference while using such techniques in APT is the approach method. Usually such attacks follow smash and grab techniques, which is ok in short term targets. But in APT such methods are used following long term exploration so that it becomes difficult to identify or to evade the attack. Once the network is accessed comes the discovery part, in which attacker silently discovers the network look for exploits, access points, security implementations and such information. So that network can be of exhilaration gets started. While making an escape, attacker tries to cover their tracks and hide the activity they performed during the attack. Such measures make it difficult for the victim organization to track back the attacker and to identify the damage done by the attack properly analyzed before planning the remaining moves. After analyzing the network and identifying the target comes the phase to steal the data. Once the required data is obtained, the final step
Advanced Persistent Threat Awareness by ISACA Sponsored By TREND micro	This study was conducted by ISACA on APTs in 2012. An APT attack is usually conducted by foes that have high end expertise and no shortage of funds. This enables them to create openings in order to achieve their objectives. As an APT attack pursues its objectives repeatedly over a prolonged time; it adapts to defence' efforts employed to resist it; and it operates at a very low interactive manner to avoid any suspensions. The above approach can be broken down into three segments persistence, adaptability and stealth. As per studies, spear phishing is the most common attack method to launching an APT, to gain initial access to the targeted enterprise. All it takes is a single click from a user that click could be on a link or to open an attachment, for an APT to initiate its first phase of attack. Adding

DOI: 10.15680/IJIRCCE.2016. 0411226

	human factor among the vulnerabilities simply makes it very difficult to design a defence mechanism against initial attacks. More importantly during the research and surveys, it came in to notice that 53.4% of the people believe APT is not so different from traditional attacking methods.
FireEye Advanced Threat Report	The Data used in this report is collected from the Dynamic Threat Intelligence™ (DTI) cloud of FireEye®. The cloud contains attack metrics data collected from FireEye®. clients throughout the globe. The data indicates that malware presences within organizations are on an alarming level. It also indicates that advanced attackers can easily breach traditional defenses including firewalls, anti-malware and anti-virus (AV) with ease. Such advance attacks are based on many different patterns; some 159 different APT-based malware families were identified. Hacking tools such as Poison Ivy, Gh0stRAT, LV and Dark Comet were among the most used by APTs. Studies also revealed command and conquer based APT infrastructure in almost 206 countries and territories. After analyzing the data it was highlighted that Web-derived attack alerts were five times more than that of email-derived attack alerts, reasons could include better awareness of spear phishing among the users. Zero-day attacks are among the most significant weapons for APT attacker. It was discovered the java was the most common zero-day focus for attackers. Alongside Internet Explorer (IE) zero-days attack which is used in watering hole attacks. Crimeware groups are now proficient in developing Java exploits. APTs targeted U.S. government websites in “watering hole” attacks. Attackers regularly find creative ways to bypass malware sandboxes, it is being predicted that Java zero-day attacks may become less in coming days, but the browser based vulnerabilities will be among the most used by attackers to infiltrate a network
Combating Advanced Persistent Threats. How to prevent, detect, and remediate	APTs can be best described as stealth aircraft. As stealth aircrafts are designed to avoid traditional air monitoring system, similarly APTs are design to avoid traditional detection methods. Once APTs infiltrated a network it can disguise itself as legitimate traffic and establish its hold within

DOI: 10.15680/IJIRCCE.2016. 0411226

APTs. McAfee	a network. With this approach long term goals can easily be achieved or one can easily keep an eye on your network with you even knowing it. In this study APTs are defined in five phase approach. First stage is social engineering methods, which are target specific. Using spear-phishing or luring target users into downloading initial-stage malware. Second stage is to create a foothold, once preliminary stage malware initiates and execute its code; request is generated to the APTs creator for further directives. Third stage involves remote commands to be implemented as per attacker's aims. Fourth stage of the attack requires a lot of patience; attackers delay the attack in order to find the right opportune. "Sleep" instructions are usually executed before any other activity so that APTs can avoid any suspicion. The fifth or final stage comes when desired aim is achieved and remote directives are issued to as per requirement if data needs to be extracted or network is to be sabotaged.

VI. Conclusions

An APT can be considered as one of the most threatening security concern, as the world advance towards IoT (Internet of things) curtain measures need to be taken so that APT attacks can be handled with ease. In this research a number of attack methods and tools are being discussed and how traditional security models are not suitable to handle an APT attack. Despite APTs evolving approach, some baselines or models can still be define to detect or identify such attacks. As the research indicates that defining a defence method against initial attack or initial infiltration is difficult, as there are countless ways to conduct the initial phase of attack. But with knowledge of network behaviour, one can at least monitor the network for suspicious activities and act before it's too late. That has been the focus of this research; to identify the common attack methods and tools use by APT attackers so as to maximize on prevention of such instances. For future work this research can extend on defining how defence methods can be devised to protect network against an APT attack.

REFERENCES

[1] Revealed: Operation Shady RAT By Dmitri Alperovitch, Vice President, and Threat Research McAfee, 2011.

[2] Daesung Moon, Hyungjin Im, Jae Dong Lee and Jong Hyuk Park, "MLDS: Multi-Layer Defense System for Preventing Advanced Persistent Threats", *Symmetry* 2014, *6*, 997-1010; doi:10.3390/sym6040997, ISSN 2073-8994.

[3] Byungik Kim Hyeisun Cho Taijin Lee, "Intelligent Network Surveillance Technology for APT Attack Detections", (IJIRIS) ISSN: 2349-7017(O) Issue 1, Volume 2 (January 2015) ISSN: 2349-7009(P).

[4] Edgar Toshiro Yano, Per M. Gustavsson, "Towards a Framework to Detect Multi-stage Advanced Persistent Threats Attacks", Available from: Per M. Gustavsson Retrieved on: 10 February 2016

[5] National Institute of Standards and Technology (NIST), Special Publication 800-39, Managing Information Security Risk, Organization, Mission, and Information System View, USA, 2011

[7] J.Vijaya Chandra Dr. Narasimham Challa and Dr. Mohammed Ali Hussain, "Data and Information Storage Security from Advanced Persistent Attack in Cloud Computing" International Journal of Applied Engineering Research ISSN 0973-4562 Volume 9, Number 20 (2014) pp. 7755-7768.

[8] Kai-Fong Hong, Chien-Chih Chen, Yu-Ting Chiu, and Kuo-Sen Chou, "Ctracer: Uncover C&C in Advanced Persistent Threats based on Scalable Framework for Enterprise Log Data", IEEE International Congress on Big Data, 978-1-4673-7278-7/15 $31.00 © 2015 IEEE.

[9] Barbara Hudson, "Advanced Persistent Threats: Detection, Protection and Prevention", Whitepaper February 2014.

[10] Nikos Virvilis, Dimitris Gritzalis, Theodoros Apostolopoulos, “Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game” (AUEB) 76 Patission Ave., Athens, GR-10434 Greece {nvir, dgrit, tca}@aueb.gr.

[11] Xiaomei Liu, “Research on Prevention Solution of Advanced Persistent Threat” 2nd International Conference on Software Engineering, Knowledge Engineering and Information Engineering (SEKEIE 2014).

[12] Murtaza A. Siddiqi, Naveed Ghani, “ Critical Analysis on Advanced Persistent Threats”, International Journal of Computer Applications (0975 – 8887) Volume 141 – No.13, May 2016