Critical Analysis on Advanced Persistent Threats

Murtaza A. Siddiqi
Lecturer
SZABIST – Larkana

Naveed Ghani
Assistant Professor
SZABIST – Larkana

ABSTRACT
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.

General Terms
Security, Hacking, Malware, Cyber Security, APT.

Keywords
APT, Malware, Security, Cyber, Hacking, Internet.

1. INTRODUCTION
In this age of technology, Internet plays a very vital role in almost every field of life. Without any shred of doubt, it can be implied that Internet has a massive impact on professional and personal life. As the use of Internet becomes abandoned, so does the need for privacy and security. Among data such as images and documents there is a clear line between the information what is private and information which can be shared, same applies to organizations either private or public. Then there are banks and financial institutes who nowadays rely solely on Internet for their day-to-day operations, from communication to Electronic commerce (e-commerce). With this much involvement of Internet the most prominent threat comes in the form of security. Security issues over the Internet come with numerous flavors starting from cyber espionage, malware, cyber extortion, identity theft, phishing and so on and so forth. Over the years hackers have devised new more advanced and highly potent methods to do their biddings. Among these advanced methods use for infiltration is Advance Persistent threat or APT.

Aim: This paper highlights how APT attacks are carried out over the last few years and who are the potential targets for such attacks. The information extracted for this paper is based on literature review. Numbers of prestigious cyber security firms have published white papers and case studies on how APT works.

Objective: Main focus of this paper is toward the most common attack pattern and tools. This could assist in defining a base lining model on how an APT can be detected in a network.

1.1 Introduction to APT
To begin with first there must be a clear understand on how these attacks are logically designed. An APT is not a single step attack but it is composed of numerous hacking tools and processes. The attackers behind such assaults possesses high level of knowledge and plenty of resources, making APT an even more prominent threat. Unlike other attacks, APT follows sophisticated pattern to achieve its objective. The APT tracks its target constantly over a long period of time, insertions which could vary from 1 month time to 28 months of time [1]. So that it can adapt to be resilient against new security measures and it keeps a stealthy approach to reach its target [5]. After reading the above APT approach some consider the traditional approach to be the same but there is a difference. Steps followed by an APT starts with a very clear target or goal based attack, as such attacks are conducted on high value targets with potential high value data. Based on attacks reported by Fire Eye 2013 [7] usually the targets are government or organizations with high value data, which can be described as financial institutes, healthcare, telecom, education and list goes on. As mentioned before people behind APT attacks are very formidable they may even be part of government or cyber defense unit [3]. This gives them an edge over traditional hackers who might not be part of the target system. As being part of the target organization helps a great deal in executing of phases such as identifying the target and keeping a low profile (stealth approach). As the following table 1 clearly shows the basic difference between an APT and a traditional attack.

Table 1: Difference between traditional attack and APT

	Classic/traditional attacks	APT
Reason	Personal or financial benefits, showoff	Economic advantages, strategic benefits, stealing sensitive information
Target	Undetermined	Governmental institutions, multinational enterprises and banks.
Approach	Aggressive, very rapid, smash and grab, tactic based on a very limited time based attack.	Repeated attempts using number of methods, stealth approach, adapts to resist defenses, very slow to avoid any suspicions may involve sleep modes before commencing any attack.
Attacker	Usually One person	Highly organized, sophisticated, Determined, highly skilled and no shortage of resources

2. APT ATTACK METHODOLOGY

Normally APT attacks are stage based; usually these stages could be four or five. Despite the number of stages, the general idea of an APT can be described as breaking in, scanning the network, identifying target, making it accessible to accomplish the goal and finally escaping the network without leaving any trace or evidence. Similar patterns were found in a research on assumed Chinese hackers attack using APT tactic between 2004 and 2013 [3] the steps were categorized as; Initial compromise , Establish Foothold, Escalate Privileges, Internal Reconnaissance, Move Laterally, Maintain Presence, Complete Mission.

2.1 Exploration

First step to conduct an APT attack is to know the target, gather as much information as possible about the target, so that different loopholes and exploits can be utilized with effect. Such step can be conducted using social engineering techniques, open source intelligence tools (OSINT) or approaching an organization which sell data or information about multinational firms. At the moment there are numerous organizations which provide a wide variety of data about other organizations including information about I.T hardware, security applications utilized or even employee's personal data. In other words the first step of information gathering can be conducted in numerous ways. Defining a security baseline or a model to stop the initial attack is quite a challenge. As there are countless ways to conduct the initial step of infiltrate. Keeping in view the persistent approach in APT, it is only a matter of time for an attacker to find a loophole in security mechanism.

2.2 Infiltrating or breaking in

This phase is comprised of exploiting the weakness and gaining access to the target network. There can be two ways to infiltrate a network one is direct and other is indirect. In direct approach a hacker can compromise any third party working at the organization and use the privilege to gain access to any system or server. In indirect approach hackers employ techniques such as spear phishing, watering hole attack or zero day virus to infiltrate and deploy any remote access tool for further activities. Very common approaches for infiltration include the use of email [8]; targeted user received a link in email from some reliable person or source. The user visits the link website which contains a malicious JavaScript payload; browser downloaded and executed the malicious JavaScript, which contain a built-in a zero-day Internet Explorer exploit. Another most common approach is to send an attachment in the email presuming from a reliable source [9]. Those attachments might seem to be a PDF or an image file but may include zero-day attack code aimed to exploit any earlier unidentified vulnerability within the system. Both the above methods can be categorized as indirect approach, most common direct approach is when a USB is attached to a system. Once an infected USB is attached to a window based system, malware would auto-execute without user interaction, utilizing zero-day vulnerability (in some cases using a modified autorun.inf technique). Such malware are designed to try and utilize Windows Server Service (MS08-067) or Print Spooler Zero-Day (MS10-061) vulnerabilities to exploit any network accessible windows based system and try to acquire higher user privilege, using MS10-073 and MS10 - 092 [10].

2.3 Identifying target

In this phase the attacker tries to search and identify the target data. During this phase the chances of being caught are quite high, as the attacker will be scanning the network for its target. This could result in abnormal traffic behavior or trespassing of data files or access violations on the network.

2.4 Stealing the information

Once the target is identified over the network, attacker must make it accessible or must acquire the appropriate rights to access that particular data. In some cases rootkits [6] can be secretly installed on targeted systems and network access points to monitor or capture data and commands as they stream over the network. Such information captured over the network can be utilized to give invaders the information they need to plan forthcoming attacks or to make target data accessible. Being persistent is also a key feature for this step to be successful.

2.5 Fleeing the network

Like every great thief, robber and hacker the final act plays a very important role. Once the desired target is achieved or data is acquired the infiltrator must make an escape and cover the tracks, so that it becomes more difficult to identify the attacker and to detect the damage done. In some case the attacker uses APT to gain long-term access or to drop a back door so that network can be accessed whenever required. In such reported cases attackers have been able to maintain backdoor access for as much as 660 days [6]. Stolen data can be channeled back webmail wrapped in encrypted packets or similar means.

Table 2 clearly indicates that APT is an approach based on phases, usually 3 to 4 phases. Then most of the organizations are not even aware that an APT attack is being conducted on their network, which is quite a concern for security professionals. Following information clearly highlights the versatility of an APT attacker as they adapt numerous ways to conceal their presence and work persistently to achieve their goals.

Table 2: APT attack methods

Paper	Attack Methods
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 exfiltration. 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 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

	of exfiltration 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.
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 defense' 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 human factor among the vulnerabilities simply makes it very difficult to design a defense 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. However, 93.9% of the people agreed that APTs possess a great threat to national security and economic stability. Among the important findings in this survey paper are that 63% of the people believe that it's just a matter of time before their organization become a victim of an APT attack, while only 60% believe that they are capable enough to stop such an attack. Although a high number of survey responders were using antivirus, anti-malware or traditional network security methods to counter an APT attack. One aspect must be kept in mind that such defense methodologies are good against traditional attacks, but are not suitable for preventing an APT attack.
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. McAfee	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 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.

As the earlier table 2 highlighted attack methods, table 3 lists some of the tools use by APT actors [11]. Mentioned tools are usually use once the initial stage (infiltration) is executed and victim system is accessible. However one thing must not be forget that following list is not the complete list of tools use by APT attackers. As APT attackers tend to keep up with the improvements in defense methods. Most of these attackers design their own tools to fulfill their desired task, but the mentioned tools list can be use a model to identify similar tools and activities over a network to identify APT attack. So if any of the mentioned tools are found, they must be closely monitored to avoid any attack.

Table 3: Common tools use in APT

Tool Name	Description	Typical Phase of Usage
LSB (Least Significant Bit) Steganography	Steganography is the science of hiding information. So, this technique can be used to embed files into images. Which provides a perfect cover to extract data as well as to initiate initial phase of infiltration for an APTs.	Multi-phase (Can be used for Initial stage infiltration as well as Last phase of data extraction)
Netbox	Netbox is a tool that provide RAT services (This tool is also legally use by organizations to provide support to their branch offices)	Multi-phase (For attack purpose, repeatedly trying to gain access to target objective and can also be used for network escape.)
Truesec Lslsass	Lslsass is a useful tool for password cracking (Dump logon sessions). It can also be utilized for pass the hash attack, as once it has the passwords from the logon sessions attacker can move freely over the network without any suspicion.	Mid-phase (This tool can be used for middle stage attack or reconnaissance of the network without raising any red flags)
HUC Packet Transmit Tool / HTran	Htran is a BNC (short for bouncer) tool or reverse proxy server that allows masking or redirecting TCP movement to a desired host, resulting in confusion of host addresses. Attackers who conduct APTs could install this server tool and redirect traffic to the malware CNC server. It allows the attacker to jump through several connections in the target country, making it difficult to trace attacker address.	Multi-phase (For attack purpose, repeatedly trying to gain access to target objective and can also be used for network escape.)
Sdelete (Secure Delete)	Sdelete allows for deleting files in a secure manner overwriting deleted files with patterns of data. Sdelete follows the standard DOD 5220.22-M (Department of Defense) Making recovery very difficult for forensic and complicating event occurrence response protocols.	Final Phase (Covering up the tracks)
GETMAIL	GETMAIL in a tool use for mail retrieval but hackers can modify the tool coding and use it as an escape route or to extract data out of the network.	Final Phase (For escaping with data or simply exiting the network)
LZ77 Data Compression	LZ77 is a data compression algorithm usually use in image compression and in compression suites such as Winzip and Winrar. The focus of LZ77 algorithm is to save space or to hide the original data into an encrypted and compressed format.	Final Phase (For escaping with data or simply exiting the network)

3. CONCLUSION

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 defense 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 behavior, 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 defense methods can be devised to protect network against an APT attack.

4. REFERENCES

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

[2] Protecting Your Critical Assets Lessons Learned from "Operation Aurora" By McAfee Labs and McAfee Found stone Professional Services,2010.

[3] Mandiant. APT1: Exposing One of China's Cyber Espionage Unit.

[4] OPERATION "KE3CHANG": Targeted Attacks Against Ministries of Foreign Affairs Authors: Nart Villeneuve, James T. Bennett, Ned Moran, Thoufique Haq, Mike Scott, and Kenneth Geers. FireEye, White Paper.

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

[6] Advanced Persistent Threats: A Symantec Perspective Preparing the Right Defense for the New Threat Landscape. WHITE PAPER: Cutting Through The Hype(www.symantec.com)

[7] FireEye Labs. Fireeye advanced threat report 2013 (Special Report).

[8] Getting Owned By Malicious PDF – Analysis. GIAC (GPEN) Gold Certification Author: Mahmud Ab Rahman, mahmud@cybersecurity.my. SANS Institute

[9] ADVANCED PERSISTENT THREATS AND OTHER ADVANCED ATTACKS Websense® White Paper.

[10] Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game? Authors: Nikos Virvilis, Dimitris Gritzalis, Theodoros Apostolopoulos Information Security and Critical Infrastructure Protection Research Laboratory Dept. of Informatics, Athens University of Economics & Business (AUEB) 76 Patission Ave., Athens, GR-10434 Greece {nvir, dgrit, tca}@aueb.gr.

[11] In-Depth Look: APT Attack Tools of the Trade. Author: Kyle Wilhoit (Senior Threat Researcher) Trend Micro-TrendLabs Security Intelligence Blog.