Advance Persistent Threat Defense Techniques: A Review

MURTAZA AHMED SIDDIQI*, AZIZ MUGHERI AND KANWAL OAD

Department of Computer Science SZABIST Larkana
Corresponding author's email: murtazasiddiqi@lrk.szabist.edu.pk

Abstract

The evolution of internet in the age of information is very rapid. With the rapid development of the internet, significance of privacy and security is also becoming a key concern. This growing security concern is not only limited to multinational organizations and government's high value data, but also for the mass users. During the last few years, there have been a number of network breaches with aims of espionage or sabotage, using an advanced and lethal methodology known as Advanced Persistent Threat. Keeping in view the damage done by such attacks, this paper based on literature review is intended to provide readers with intensive knowledge of an APT attack with its common phases. Later sections of the paper highlights the existing security methods currently in use or proposed by different researchers and security organizations to counter APT attacks. Statistical data on known APT attacks conducted over the last few years is also included in the paper to give the readers a clear idea of devastation caused by APT attacks. At the end of the paper conclusion and future work is emphasized, which include the crucial steps that can be employed to fight against APT attacks. Data analysed in this paper is extracted from annual reports published by well-known security implementation groups and reports released by organizations that have been targeted or victim of APT attacks.

Keywords: Advance Persistent Threats **(**APT), Security, Internet, Hacking, Malware.

INTRODUCTION

The war among the hackers and security experts has been going on since the birth of internet. With the passage of time internet is becoming a necessity of everyone's life for connecting everyone everywhere regardless of the geographical boundaries. But for internet user's, privacy and security has becomes a great concern. With the rapid escalation in sophisticated hacking techniques, even a minor flaw in security can result in a great tragedy. As the industries are moving towards an IT revolution and IT dependency for day-to-day routine is increasing, therefore the security concerns associated with IT are on the rise. Cyber espionage, security breaches and privacy issues are escalating in frequency and are becoming more complex, persistent and difficult to intercept [1]. As per studies such cyber security breaches throughout the globe are costing an estimated cost of nearly $400 billion every year [2].

Keeping in view the recent incidents and financial loss caused due to APT and similar attacks, a number of researchers, government institutions and corporate organizations are questioning about the current security techniques implemented at sensitive data [3]. Studies indicate that cyber attacks conducted at high value targets are highly covert, tenacious and challenging to detect; such attacks are usually initiated with a very stealth approach, to avoid raising any suspicious similar to the Stuxnet [4]and Aurora case [5].

ADVANCED PERSISTENT THREATS

Attack patterns similar to Stuxnet and Aurora are categorized as Advanced Persistent Threats (APT) [6]. Table 1 contains list of some of the well-known APT attacks. An APT attack cannot be preserved casually on any account. Typically, an APT attack can result in costing an organizations nearly $5.5 million in order to counter and investigate the damage done by an APT attack [7]. APT attacks can be separated into number of stages and each stage carries out a specific task, making APT attacks difficult to detect and counter [8]. One of the most common misunderstandings among most of the users is to think that traditional security tools and defence methods are enough to encounter an APT attack. Such attacks are quite persistent, strategically conducted, well funded, sophisticated and are carried out with a stealthy approach. As far as persistency, stealth and thoughtful planning is concerned, researcher's and security experts have come by APT attacks that extended from a month to 28 months in order to maintain stealthy approach to accomplish the desired task [9]. To keep a low profile and avoid suspicion an APT can even change its operational modes from observing or active to sleep mood. APT attackers can also adapt and modify the approach of attack, based on security barriers deployed with in the network [10]. Table 1 highlights the efficiency of APT attacks; showing some of the reported incidents of successful security breaches in some of the most protected networks belonging to both private and government sectors.

Table 1: Known APT attacks from the last few years (2007-2015) [11-14].

Attack	Entry Method	Date	Classification
Aurora Operation	Malware	2007	Espionage
Stuxnet	Malware	2009	Sabotage
Energetic	Malware	2011	Espionage
RAS Breach	0day, Malware	2011	Espionage
DigiNotar	Compromised network access	2011	Sabotage
Luckycat	Spear phishing emails, 0day, malware	2011	Espionage
Flame	Malware	2012	Espionage
Shamoon	Malware	2012	Sabotage
Operation Ke3chang	Malware	2010 2013	Espionage
Operation SnowMan	Water hole attack (weakness in vfw.org)	2014	Unknown (suspected to be Espionage)
Heartbleed	Malware	2014	Espionage
Darkhotel	Malware, spear phishing, 0 day	2014 2015	Espionage

APT Phases

In previous section, it is mentioned that an APT attacks consist of number of phases [8]. These phases can be generally classified in to following:

i. Reconnaissance: To observe and gain as much information as possible about the target network.

ii. Infiltration: Based on the information collected in the first step the assailant attempts to discover a weak link in order to launch the attack in order to gain access to the network.

iii. Discovery: After the target network is successfully breached, network discovering protocols are run by the assailant. To discover target data, to understand security implemented on the network and how the desired task can be achieved without any suspicion.

iv. Capture: Once the desired target and how to reach that target is identified, the assailant initiates the attack phase and tries to accomplish the desired task with maximum stealth to avoid any suspicion and risk of getting caught.

v. Escape: After completing the objective and acquiring the desired data, assailant makes an escape from the network. To make things worse an APT attacker tries not to leave any kind of digital prints on the victim network, in order to make things difficult for the investigation team to recognize the intrusion procedure, objective achieved or harm done and exit method.

EXISTING TOOLS AND METHODS TO ENCOUNTER APT ATTACKS

APT attacks are becoming more sophisticated and stronger with the passage of time. In order to counter APT attacks much more enhanced and stronger defense techniques are required. A number of common techniques such as; Firewall, IDS, IPS, Botnet, Sandboxing, Web & Email protection, Web application firewall and anti viruses are currently among the best available defense against an APT attack. Unfortunately, with the rapid enhancement in APT attacks, the mentioned tools are not too effective and advance techniques are needed, such as layer based defense mechanism [15].

Defense in Depth/Multi-Layer Defense System

Defense in depth is a multi-layer defense method which is originally based on a concept from military discipline. The basic idea is to apply protective system at multiple layers of network making it much more secure as compared to a single layer security

mechanism. Defense in depth not only protects the system from an APT attack but it can also provide valuable information on the attack and the attacker. Such information can not only assist in tracking the attacker but it can also help in minimizing the damage done by an APT attack [16], which is a very useful mechanism as normally it's not only difficult to detect an APT attack but it's quite difficult to track the damage done by an APT attack. Table 2 shows an illustration of layer based logical approach to Defense in Depth System.

Table 2: Defense in Depth against APT [16]

Layers	Defense Methods
Identity and Access	Identity and Access Management
Physical and Environmental	Physical and Environmental Security
Network	1. Intrusion detection and prevention system 2. VOIP security 3. Network segmentation and firewall 4. Web and mail content inspection 5. Secure remote access 6. Data encryption 7. Network access control
Operating System	Operating System Security
Application	Application Firewall
Data Base	Database Security

Since Defense in Depth approach is a combination of security tools as shown in Table 3 therefore, it provides a comprehensive security method against new and emerging APT attacks. Defense in Depth works on general approach to defend all assets, while taking into consideration the interconnections and dependencies of assets, and implements available resources in an effective layer based monitoring and protection system, minimizing the business's exposure to cyber security risks. A comprehensive lay out of tools and techniques used by Defense in Depth are shown in Table 3 [17].

Table 3: Defense in Depth Strategy Elements [17]

Defense in Depth Strategy Elements	
Risk Management Program	1. Identify Threats 2. Characterize Risk 3. Maintain Asset Inventory
Cyber Security Architecture	1. Standards/ Recommendations 2. Policy 3. Procedures
Physical Security	1. Field Electronics Locked Down 2. Control Centre Access Controls 3. Remote Site Video, Access Controls, Barriers
ICS Network Architecture	1. Common Architectural Zones 2. Demilitarized Zones (DMZ) 3. Virtual LANs
ICS Network Perimeter Security	1. Firewalls/ One-Way Diodes 2. Remote Access & Authentication 3. Jump Servers/ Hosts
Host Security	1. Patch and Vulnerability Management 2. Field Devices 3. Virtual Machines
Security Monitoring	1. Intrusion Detection Systems 2. Security Audit Logging 3. Security Incident and Event Monitoring
Vendor Management	1. Supply Chain Management 2. Managed Services/ Outsourcing 3. Leveraging Cloud Services
The Human Element	1. Policies 2. Procedures 3. Training and Awareness

It is quite clear from Table 2 and Table 3 that Defense in Depth Technique is very similar to an APT attack technique, as an APT attack is also a combination of different tools being utilized at different phases of APT attack making it difficult to detect and encounter. Using similar approach Defense in Depth applies holistic tactic to shield the system against the APT attacks. Defense in Depth is not a single mechanism but it is a group of multiple things like; people, technology, standard security procedures, operations and awareness to organizations on ATP tactics. The main objective of the Defense in Depth technique is to maximize the chances of avoiding an APT attack and providing a comprehensive recovery and tracking method in case an APT has been successful in accessing organizations network [18].

Defense Techniques Proposed in Research Papers and Security Organizations

Layer based approach is not the only measure to counter against APT attacks, security experts and security providing organizations have proposed other comprehensive methods as well. Table 4 contain some of the methods suggested by most prominent security implementation organizations to counter APT attacks.

Table 4: APT defense methods suggested by well-known security organizations.

Paper	Attack Method	Defense method
Advanced Persistent Threats: A Symantec Perspective [19]	As per paper, the method APT attacks are divided in 4 phases, which are intrusion in a network, discovery of target, capture of target data and exit from network. The attacks are initiated through email phishing, malware behind advertising clicks, finding vulnerabilities on network, capturing the desired data and remove the traces.	As per paper such attacks can be prevented by implementing; 1- Heuristics based security tools such as Antivirus and firewalls. 2- Close monitoring and filtering the incoming and outbound traffic 3- Implementing data encryption and use of VPN.
Defending Against Advanced Persistent Threats: Strategies for New Era of Attack [20]	The paper is based on a study conducted by CA Technologies. As per study, the APT attacks are typically conducted on multinational companies with high value data or high value in term of stock market value. In this paper, authors have described an APT attacker as someone who is always looking for vulnerability in order to infiltrate a network, after a successful infiltration the attacker run discovery protocols to learn the details of the network. Such details may include ports information using port scanning or traffic routes. Once such information is collected the attacker searches	The authors of the paper propose following methods in order to counter an APT attack; 1- Block any unused ports. 2- Encrypt Data with at least 128bit, MD5 hash. 3- For auditing purpose log files must be maintained and should be checked time to time for any suspicious activity. 4- End to End antivirus should be implemented to secure sessions. 5- Well defined firewall policies to encounter attacks from

	for its desired data without raising any suspicion. As soon as the target is identified the attacker captures the data and exits the network. In case of a successful APT attack companies with shared account management policies suffer more losses. Further, a network, which is compromised, can provide the attacker with system logs, user's passwords and in some cases, the attacker leaves a backdoor in network that can be a nightmare for the company.	internal and external sources. Studies show that a large number of cyber-attacks are conducted with inside assistance; to avoid such incidents following steps can be very useful: 1- Identities should be securely saved on different virtual networks and user privileges over resources should be assigned very carefully. 2- Accounts belonging to employee who are no longer part of the organization should be deactivated immediately.
Countering the Advanced Persistent Threat Challenge with Deep Discovery[14]	The data used in this paper is collected from Trend Micro; the paper indicates that the APT Attacks in any organization is like destroying the network as well as the organization. Paper also indicates that an APT attack can easily breach traditional defense systems such as firewalls or antivirus. The description of an APT attacker in this paper is quite the same as described in previous papers. Once the attacker acquires the information about the target network and a point of entry, assailant will bombard the network with every arsenal at its disposal in order to establish a communication structure, which can provide information back to the attacker. Once this task is achieved, the infiltrator will search the network for its target data, which is then	The authors of the paper suggest the following methods to prevent such attacks; 1-Using digital certificate (SSL/SSH) to avoid downloading any infected file or browser redirection to harmful sites, 2-Implement Sandbox strategy at server's end, so that files are simulated properly before utilization, updating or implementation. 3-Using heuristics tools and algorithms to black list IP's on suspicious behavior, routines and sub routines. 4-Proper configuration and installation of security devices check points and tools. Such practices play a core role in effective and strong wall between high value data and the attacker. 5-Separate firewalls be implemented on every server.

	acquired and sent back to the attacker HQ. In the end, the attacker makes an escape without leaving any trace	6- Using highly effective data encryption techniques. In case if data is even compromised, it will not be an easy task to decipher it
The Study of APT Attack Stage Model [21]	As per paper an APT attack can be divided in to 4 stages, preparation stage, access stage, resident stage and harvest stage. Despite the different names, the concept of stages of an APT attack is same as described in previous papers. Initial stages consist of information gathering (direct or indirect) such as port scanning, vulnerability scanning, search engines along with advanced crawlers and custom developments to get the network information. After getting the information, the infiltration stage is executed based on the gathered information. Accessing the network can be done my numerous ways such as spear phishing emails, social engineering, water hole attack etc. Once inside the network attacker intend to establish command and control mechanism to search the desired data, acquire it and then exit the network. As per studies attacks which are based on social engineering, waterhole and direct approach are highly effective ones. 19% of APT cases use the Zero Day Vulnerabilities and almost 70% has exploit vulnerabilities.	In order to prevent APT attack the authors of this paper suggest the following: 1- First step to counter an APT is educating the staff on how to avoid any internal assistance to an APT attacker. Staff should be aware on how to prevent data leaks through social media or social gathering and not to share authentication information with any one. 2- Proper responsiveness towards the internal network security is very important. 3- To prevent zero day exploits and vulnerabilities (outdated software), user must keep the system and software updated. 4- Firewalls must be configured properly so that only authentic traffic is allowed to access and exit the network. 5- Anti-viruses should be installed not only on the core system (servers) but also on every local host with updated virus definitions. 6- Implementing IDS (Intrusion Detection Systems) that can alerts the authorities under any kind of suspicious activity. 7- Strict I.T. policies as per standards should be implemented for organization's employees. 8- Deployment of tools like honey pots system with in the network in order to detect any suspicious or malicious activity can be very effective. 9- Use of Sandbox to check any suspicious file before allowing it on the network or installing it can also

		be very useful. Security experts must go through risk assessment if an APT attack is successfully conducted or in progress on the network. So that exact awareness of damage done or expected damage can be calculated for recovery and response purposes

Behavior Analysis Tools to Counter APT Attacks

Earlier sections have discussed a comprehensive approach or a complete method, which can be used to safe guard against APT attacks. In this section, tools that can be used to detect an APT attack are being discussed. Table 5 shows a list of tools, which can be used effectively to detect an APT, attack on a network. These tools have two basic analytical methods to detect an abnormality in a network. Mentioned tools can detect an APT based on the behaviour of the network and coding of application running with in the network.

Table 5: Tools to perform coding and behavioural analysis to detect an APT attack [22]

Tool	Description	Analysis Method
Autoruns	Provides a list of auto-start file locations.	Behavioural
Process Monitor	Log changes in any registry, file, process, thread etc.	Behavioural
ListDLLs	Provides a list of DLL files on the system.	Behavioural
TCPview	Monitor or log active end to end TCP/UDP connections	Behavioural
VMMap	Provide details of virtual and physical memory utilized by any program	Behavioural
Capture-Bat	Honey pot services at client end, to log and monitor any attack.	Behavioural
Wireshark	Packet Sniffer and network protocol analyser	Behavioural
REMnux	Utility tool based on Linux to analyse any malware and to reverse-engineer it.	Behavioural/Coding
FileInsight	Utility software to display file in both text and hexadecimal format.	Coding

Such tools can be very effective but in a live and active network, it becomes a great issue to identify any abnormality especially when the network has thousands of nodes and users with huge amount of application data transactions per second.

RECENT APT ATTACKS

APT attacks are still escalating, despite of all the research and security measures that are being implemented. As per recent report by Symantec [23] and Kaspersky Security [24, 25] McAfee [26-28].

Table 6: Reported attacks during last few years

Symantec [23]			
Year	**2013**	**2014**	**2015**
Total Breaches	253	312	318
Mobile Vulnerabilities	127	168	528
Zero-Day Vulnerabilities	23	24	54
Kaspersky Security [24, 25]			
Year	**2014**	**2015**	**2016**
Attempts to launch malware capable of stealing money	1,911,266	1,966,324 (2.8% higher than in 2014)	1,198,264
Number of users attacked by Trojan-Ransom malware	1,28,132 (Oct to Dec 2014)	3,37,205 (July to Sept 2015)	Not available
Number of users attacked by encryptors (Trojan-Ransom encryptor malware)	1,20,840	1,79,209	821,865

McAfee [26-28]				
Year	**2013**	**2014**	**2015**	**2016**
Total malware attacks	190,000,000	340,000,000	430,000,000	650,000,000
Total ransom ware	1,500,000	2,200,000	4,900,000	8,700,000
Total rootkits malware	1,220,000	1,500,000	1,700,000	Not available

CONCLUSION

Despite availability of defense methods against an APT, the high percentage of successful APT attacks clearly indicates that much is needed to be done for fighting against APT attacks. As this paper is intended to highlight the basic attack patterns of an APT and defense methods being deployed to counter APT attacks, therefore readers will find it evident that current defense methods are not fully equipped to encounter such highly organized attacks. Among the APT defense methods discussed in the paper, some can be quite effective in near future. For example, if organizations report network breaches with complete analysis on the attack, it could help the security experts in proposing a much better defense mechanism to counter such attacks in future. But there are number of reasons why most of the organizations fail to report security breaches. Reasons may include reputational concern of an organization or at times organizations are not even aware that their network is being compromised, which is quite alarming. Layer based defense methods and security systems with automated capabilities to identify false flag or to detect, analyze and encounter malicious activity can play a vital role in approaching times. But a lot of work is needed to be done in order for such system to be highly efficient; as such system with high level of check and balance might result in degrading overall performance of a network. As the world is moving towards Internet of Things (IoT), the importance of security is a very important area, which cannot be neglected.

REFERENCES

[1] Symantec, "Internet Security Threat Report," 2014, Available: http://www. symantec.com/security_response/publications/threatreport.jsp., Accessed on: May 2015

[2] MacAfee, "Net losses: Estimating the global cost of cybercrime," 2014, Available: http://csis.org/files/attachments/140609_rp economic impact cybercrime report.pdf, Accessed on: May, 2015

[3] Crashing the system. (2014, July 12) The Economist. Available: http://www. economist.com/news/special-report/21606419-howprotect-critical-infrastructure-cyber-attacks-crashing-system

[4] M. Kenney, "Cyber-terrorism in a post-stuxnet world," *Orbis*, vol. 59, no. 1, pp. 111-128, 2015. doi: 10.1016/S1353-4858(11)70086-1

[5] M. Zeller, "Myth or reality -Does the Aurora vulnerability pose a risk to my generator?," in 64th Annual Conference for Protective Relay Engineers, 2011, pp. 130-136. doi: 10.1109/CPRE.2011.6035612

[6] C. Tankard, "Advanced Persistent threats and how to monitor and deter them," *Network Security*, vol. 2011, no. 8, pp. 16-19, 2011.

[7] Ponemon Institute, "2011 Cost of Data Breach Study: United States," 2012, Available: http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf

[8] M. A. Siddiqi and N. Ghani, "Critical Analysis on Advanced Persistent Threats," *Int. J. Comput. Appl.*, vol. 141, no. 13, pp. 46-50 Available: www.ijcaonline.org/archives/volume141/number13/siddiqi-2016-ijca-909784.pdf

[9] D. Alperovitch, "Revealed: Operation Shady RAT," 2011, Available: https://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

[10] NIST, "Managing Information Security Risk Organization, Mission, and Information System View " Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology 2011, doi: 10.6028/NIST.SP.800-39.

[11] GreAt. Darkhotel's attacks in 2015. Available: https://securelist.com/blog/research/71713/darkhotels-attacks-in-2015/

[12] A. Redondo-Hernández *et al.*, "Detection of Advanced Persistent Threats Using System and Attack Intelligence," in EMERGING 2015: The Seventh International Conference on Emerging Networks and Systems Intelligence, 2015, pp. 91-94

[13] P. Chen *et al.*, "A Study on Advanced Persistent Threats," vol. 8735, Communications and Multimedia Security. CMS 2014. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg, 2014, pp. 63-72. [Online]. doi: 10.1007/978-3-662-44885-4_5

[14] Trend Micro, "Countering the Advanced Persistent Threat Challenge with Deep Discovery," April 2013, Available: https://www.trendmicro.de/cloud-content/us/pdfs/business/white-papers/wp_deepdiscovery.pdf

[15] B. Hudson, "Advanced Persistent Threats: Detection, Protection and Prevention," Sophos Ltd., US February 2014, Available: http://resources.idgenterprise.com/original/AST-0112935_sophos-advanced-persistent-threats-detection-protection-prevention.pdf

[16] J. V. Chandra *et al.*, "Intelligence Based Defense System to Protect from Advanced Persistent Threat by Means of Social Engineering on Social Cloud Platform," *Indian J. Sci. Technol.*, vol. 8, no. 28, p. 1, 2015.

[17] A. Shamim *et al.*, "Layered defense in depth model for it organizations," in ICCET' 2014: 2nd International Conference on Innovations in Engineering and Technology, 2014, Penang, Malaysia

[18] Industrial Control Systems Cyber Emergency Response Team, "Recommended practise: Improving industrial control systems cybersecurity with defense-in-depth strategies," Department of Homeland Security, Control Systems Security Program, National Cyber Security Division 2009, Available: https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[19] Symantec, "Advanced Persistent Threats: A Symantec Perspective," Symantec Corporation 2011, Available: https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

[20] CA Technologies, "Defending Against Advanced Persistent Threats : Strategies for a New Era of Attacks Security Threats As We Know Them Are Changing," 2014, Available: http://www.valleytalk.org/wp-content/uploads/2015/05/defending-against-advanced-persistent-threats.pdf

[21] M. Li *et al.*, "The study of APT Attack Stage Model: 978-1-5090-0806-3/16/$31.00," in IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama, Japan, 2016, pp. 1-5

[22] F. Li, "A Detailed Analysis of an Advanced Persistent Threat Malware," The Sans Institute 2011, Available: https://www.sans.org/reading-room/whitepapers/malicious/detailed-analysis-advanced-persistent-threat-malware-33814

[23] Symantec, "Internet Security Threat Report," April 2016, vol. 21 Available: https://resource.elq.symantec.com/LP=2899, Accessed on: May 2015

[24] M. Garnaeva, J. V. D. Wiel, D. Makrushin, A. Ivanov, Y. Namestnikov, "Kaspersky Security Bulletin," in "Overall statistics for 2015," Kaspersky Lab. December 15, 2015, Available: https://securelist.com/files/2015/12/Kaspersky-Security-Bulletin-2015_FINAL_EN.pdf

[25] D. Emm *et al.*, "IT Threat Evolution in Q3 2016," Kaspersky 2016, Available: https://cdn.press.kaspersky.com/files/2015/10/IT_threat_evolution_Q2_2015_ENG.pdf

[26] McAfee Labs, "Threats Report," September 2016, Available: https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-sep-2016.pdf

[27] McAfee Labs, "Threats Report," August 2015, Available: https://www.mcafee.com/hk/resources/reports/rp-quarterly-threats-aug-2015.pdf

[28] McAfee Labs, "Threats Report," August 2017, Available: https://www.mcafee.com/hk/resources/reports/rp-quarterly-threats-aug-2015.pdf