Advanced Persistent Threat Detection System

Hanu Prasannan[1], Dharani .J[2]

[1]M.Tech Student, Department of Information Technology, SRM University, India
[2]Asst. Professor, Department of Information Technology, SRM University, India

Abstract: ***The Advanced Persistent Threat has quickly risen as a top-level concern for organizations of all types and sizes. Under today's security paradigm, determined attackers will eventually find their way into their target's network, often employing social engineering tactics, phishing techniques and backdoor exploits to steal credentials and obtain access. Persistent intrusions target key users within organizations to gain access to trade secrets, intellectual property, computer source code, and any other valuable information available. In order to combat APTs, it is imperative that organizations should know what is going on within their internal networks to fill in the gaps left by perimeter security solutions. The APT detection system enables organizations to have a defence-in-depth methodology. The APT system designed has a combination of modules like IDS, IPS and UTM, SIEM working together as a grid and correlate rules with each other for complete defence. The firewall provides gateway level protection against attacks. The intrusion detection system detects any sort of anomaly behaviour and threat signatures. Intrusion prevention system detects and prevents vulnerability exploits in the network. In short, the advanced persistent system designed is an incorporation of all security modules working together as a grid to provide a secure defence system as it detects low and slow attacks which do not generate usual alarms and responds real quick to the attack.***

Keywords: Advanced Persistent Threats, Intrusion detection systems, SIEM

1. Introduction

The rise of Advanced Persistent Threats (APTs), a type of targeted attack, has continued to hit corporates and governments to exfiltrating sensitive data. Organizations have found themselves the target of APTs. APTs persistently collect information and data on a specific target using diverse techniques, examine the vulnerabilities of the target, and then carry out attack using the data obtained. An APT is very intelligent, as it selects a clear target and carries out specific attacks, which is unlike the traditional hacking attempts. The attackers employ techniques such as Social engineering and spear phishing to deploy malware into a network which steals all important operation data's of the organization.

The proposed system is developed and designed using open source softwares with high reliability and outcome. Layers of security defence mechanisms are implemented to combat APTs which may trigger an attack inside an organization. The project aims to monitor the inbound and outbound traffic, data integrity and to analyse, detect, scrutinize and prevent the APTs. Real time threat monitoring is enabled to detect anomalies within the organization's internal network. The system designed helps in combating APTs with good success rate reducing false positive alarms.

1.1The 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.

1.1.1 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.

1.1.2 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.

1.1.3 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.

1.1.4 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.

1.1.5 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 exfiltration phase the data can be shipped out.

1.1.6 Exfiltration

The final stage is about exfiltrating 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.

2. Literature Survey

2.1 Intrusion Detection Systems

Intrusion detection systems (IDS) are used for partially automatic over viewing of a corporate network. IDS focus on a company's internal network. There are two types of intrusion detection systems. They are Network IDS (NIDS) and Host-based IDS (HIDS). They are well known for detecting common attacks such as port scans or registering large data transfers. Commonly used IDS are Snort or Dragon. These contain several techniques for detecting anomalies in a network. These countermeasures are useful for detecting APT reconnaissance attempts, such as port scans. SQL injections are also detected with these systems. Although more advanced APT attacks do out-of-box reconnaissance tactics, such as scanning networks for gathering information or social engineering attacks. The benefit of having HIDS installed on each client in a corporate network is the high rate of detecting anomalies such as modification of critical system files. But one of these IDS are not enough to prevent an APT attack from occurring. Combining the two systems can be effective in the detection of APTs.

2.2 Firewalls

Firewalls protect you from denial of service attacks using a policy-based approach that ensures accurate detection. You can deploy Denial of service protection policies based on a combination of elements including type of attack, or by volume, with response options including allow, alert, activate, maximum threshold and drop. Specific types of Denial of service attacks covered include: Flood protection by protecting you against SYN, ICMP, UDP, and other IP-based flooding attacks. Reconnaissance detection by allowing you to detect and block commonly used port scans and IP address sweeps those attackers running to find potential targets. Packet-based attack protects you from large ICMP packets and ICMP fragments. Eventually, advanced persistent threats bypass firewalls and migrate into the network as they are well planned funded attacks, though a firewall stands as an initial barrier for attackers to penetrate. Hence an initial detection might lead to protection of the network and whereby administrators could easily respond to the critical incident.

2.3 Intrusion Prevention System

Intrusion prevention system blocks known and unknown network and application-layer vulnerability exploits from compromising and damaging your enterprise information resources. Vulnerability exploits, buffer overflows, and port scans are detected and blocked by IPS mechanisms. An IPS can fully decode the protocol and then intelligently apply signatures to detect vulnerability exploits. IPS comes integrated with Heuristic-based analysis which detects anomalous packet and traffic patterns such as port scans and host sweeps. Advanced IPS can monitor globally to identify and build protections for domains and infrastructure, and local DNS spoofing. And it re-directs malicious requests to an address of your choosing for discovery and blocking of infected hosts. It also blocks malformed packets, IP defragmentation and TCP reassembly, protecting you against evasion and obfuscation methods used by attackers. An IPS usually blocks signatures sent by the intrusion detection system.

2.4 Common Advanced Persistent Threats

Dark comet is an APT attack which targets organizations which deal with energy and utilities, financial enterprises, governments and telecom. GhostRat targeted organizations leveraging both malware and web traffic. The most famous kind of malware embedded in APT attacks is POISON IVY.APTs use zero day exploits to remain undetected during the attacks. The common types of zero day attacks which attackers target are Java security by making a pointer inactive, or compromising internet browsers, flash, and Readers. APTs also include the wide use of Trojans and worms.

A common example is W32/Rbot-APT also known as APT Aurora, which exploits weak passwords on computers and SQL servers and exploits operating system vulnerabilities. Spear phishing is the technique used in most of the APT attacks which has emails containing attachments of varying file types such as, .XLS, .PDF, .DOC, .DOCX and HWP which accounted for 70% of the total number of spear-phishing email attachments. Other APT attacks are STUXNET, DUQU,FLAME, DARK HOTEL and CLOUD ATLAS.

2.5 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 attackers 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.

3. Design

An Advanced Persistent Threat Detection System when designed should be able to detect any kind of threats that may damage the important resource of the organization. Here the detection system is designed using a collection open source operating systems which include:

- Advanced firewall
- Intrusion detection system
- Intrusion prevention system
- Log collectors
- Security Incident

Event Management (SIEM)

All the modules are configured and managed to detect any slight variations in the network by continuously monitoring the outgoing and incoming traffic. The system designed detects any kind of network scans, port scans, protocol scans, prevents sphere phishing, malwares, side-channel attacks, ftp attacks, SQL injection, cross-site scripting and to prevent any attacks from penetrating inside the network providing fast mitigation techniques. The design offers defence-in-depth methodology by placing security tools layer by layer to employ the required level of security to prevent APTs. The system designed is able to combat zero-day exploits and other vulnerabilities in which APTs rely on to penetrate. The system responds to reconnaissance and social engineering by immediately responding to any initial attacks. Apart from all functionalities the system blocks spam, virus, inspects https, filters web, inspects packets and matches signatures. Thus the main function of the system is to collect, analyse, process and scrutinize.

4. Implementation

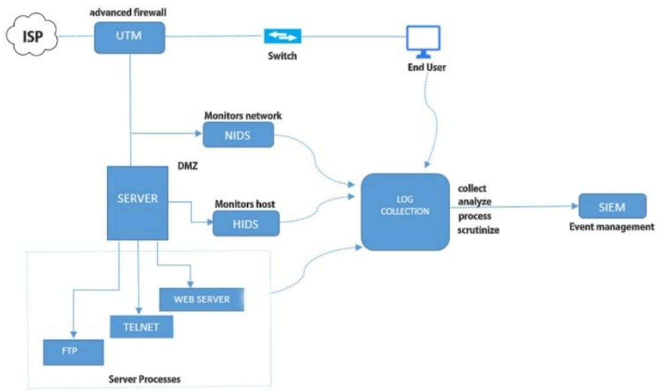

Figure 1: A Basic Implementation of the Concept

As APT depends on remote access and control, the network activity can be disrupted through the analysis of outbound network traffic. Strategies for detection of APT can be implemented through open source software tools and used to implement defence in depth by configuring an advanced Firewall, Intrusion Detection Systems, Anti-virus, Intrusion Prevention Systems, Log collectors and Security incident event management (SIEM).

The system works by the technique of port mirroring, by taking a copy of the network traffic to the Intrusion Detection system where the packets are matched for signatures to a set of rules in the database. The rules are updated periodically with latest signatures to detect any kind of attack or virus signatures. Snort is an open source network-based intrusion prevention and detection system (IDS/IPS) which employs signature and protocol, as well as anomaly-based inspection. Snort looks for a string of bytes for anomaly detection. A snort rule consists of action, protocol, source IP address, destination IP address and message. Intrusion Detection System alerts if any signature is matched. It never drops a packet. A malicious code can be easily detected by an ID. Snort manages network level traffic.

OSSEC is a host-based open source IDS, correlation and analysis engine which provides log analysis, file integrity checking, Windows registry monitoring, rootkit detection, and time-based alerting as well as active response and it is supported by all operating systems. OSSEC prevents insider attacks. Both IDS and OSSEC working together in the server give protection against threats from both internal and external attacks.

The logs collected from IDS, various users, NIDS,HIDS, SERVER are transferred to Security Onion. Security Onion contains software used for installing, configuring, and testing Intrusion Detection Systems. Security Onion contains Snort, Sguil, Snorby, Squert and Elsa for network monitoring and these are very powerful Linux based tools which are effective in the detection and analysis of APTs and other attacks. Security Onion collects, analyses, processes and scrutinizes various logs to get a clear picture of the network traffic. Sguil includes an intuitive GUI that provides access to real time events, APT detection tools and tactics available for varied operating system infrastructure. Squert is a web application used to query and view event data stored in a Sguil database. Through the use of metadata, time series representations, weighted and logically grouped result sets it provides additional context to detect advanced persistent threats.

Security incident event management module is used to collect and analyse the logs from hundreds of systems connected in the organization to study the behaviour of the network and respond if there is any deviation from the normal behaviour of the network. SIEM module is used to combat zero day exploits in which APTs rely on to penetrate into an organization. Alienvault OSSIM (Open Source Security Information Management) is an open source security information and event management system, integrating a selection of tools designed to aid network administrators in security, in intrusion detection and prevention.

5. Conclusion

The project focuses on countermeasures to the advanced persistent threats, a targeted and maliciously intentional attack against specifically targeted victims and data. The system implemented works on defence-in- depth methodology providing security to the organization using approaches which include signature based methodology, statistical and correlation concepts, as well as data leakage prevention.

While there is no ultimate protection against concerted and targeted attacks, a strong framework that includes layered defensive tactics can prove fruitful. Social engineering and failure to patch vulnerabilities in a timely manner lead to persistent attacks. The system designed aims to stop APTs at an early reconnaissance stage. The system is implemented with free, open source tools or supported, commercial platforms, coupled with comprehensive and steady analysis, can help in the early detection of APTs. While targeted attacks are difficult to find, the system designed helps in finding APTs in an initial stage and mitigate them effectively.

References

[1] Combating Advanced Persistent Threats
[2] http://www.mcafee.com/in/resources/white-papers/wp-combat-advanced-persist-threats.pdf
[3] APTs And Advanced Attacks
[4] https://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf
[5] Advanced Persistent Threats Detection
[6] http://www.sans.edu/student-files/projects/JWP-Binde-McRee-OConnor.pdf
[7] Threat handling
[8] https://www.enisa.europa.eu/activities/cert/support/exercise/files/AdvancedPersistentThreatincidenthandlinghandbook.pdf
[9] Network Infrastructure and Advanced APT Attacks
[10] https://www.paloaltonetworks.com/network-infrastructure/advanced-persistent-threat-white-paper.html
[11] Security Incident Event Management
[12] https://community.mcafee.com/community/business/siem/blog/2012/10/26/zero-day-exploits-what-can-a-siem-do