THINK INDIA JOURNAL

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Technique For Detecting Advanced Persistent Threat By Monitoring Sensitive Files

Nupur Ahluwalia

Asst. Professor , Lovely Professional University

ahluwalianupur@gmail.com

Varun Singla

Computer Science and Engineering

Lovely Professional University

varun.17705@lpu.co.in

***ABSTRACT*- Since when the Internet has been adopted and has evolved, a wide range of cyber attacks have been found to occur, ranging from viruses and worms to malwares and botnets. But in recent years, a new kind of threat has emerged called Advanced Persistent Threat. It is a threat which is most difficult to detect and once it occurs, it stays or persists there for a long period of time. This threat is designed in such a way that it can easily evade the conventional detection mechanisms.The attackers particularly target the employees or people having the high-level access to the most crucial data or the resources of the organization. This paper presents an approach for detecting APT when it has successfully breached into an employee's system and the attacker is now trying to access the sensitive files stored on that system. The proposed approach can monitor the access of these sensitive files in order to detect the anomalous behavior of file access.**

Keywords: Advanced Persistent Threat (APT), Command and Communications (C&C), Social Engineering,

I. INTRODUCTION

The data in the organizations is vulnerable to many different threats.Intruding into the organization's network and stealing the crucial information can provide higher payoffs to the criminals by just a single attack. And when the attacks are targeted at the big data stores, the loss can be even more serious for the targeted organizations.

There are many different cyber attacks, out of which 5 are most severe and most of the organizations are likely to face them: Socially Engineered Trojans, Upatched Software, Phishing Attacks, Network travelling worms and Advanced Persistent Threat. Among these 5 cyber attacks, Advanced Persistent Threat (APT) is most recent and very difficult to detect.

An Advanced Persistent Threat is an attack in which an unauthorized user gains access to a system or

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

network and remains there for an extended period of time without being detected.

The term **Advanced** indicates that the attack is performed by a group of hackers who are very highly skilled and well trained. They work in coordination and are highly resourced both in funds as well as technical perspectives. The attackers are much aware of the modern intrusion techniques.

Persistent means once this threat breaches, it persists in the network undetected for a long period of time. Even if the attempt fails once, the attack will still persist in the network and will keep on making the attempts until its objective is achieved.

Threat means that the attack is not performed just by a piece of malicious code. Rather, it involves human coordination. Hence, it is very well organized and targeted.

The **goal** of APT is not to harm the system directly. The attackers use this attack to get control over the infected machines and to steal the sensitive information of the organizations.

Phases of APT attack:

1. **Reconnaissance:** In this stage, the highly skilled attackers collect the information about the targeted organization. The information about the organization's employees, resources, and network servicesis collected by scanning and monitoring the organization's network.
2. **Delivery:** In this stage, the attacker uses the information gathered in the first stage to deliver the exploit to the target. This delivery can be done by sending a spear phishing mail which the targeted user (employee) can trust. When the targeted employee or person opens the spear phishing mail, it secretly downloads the embedded RAT file.
3. **Initial Intrusion:** Once the exploit in the delivery stage is successful, the attacker gains access to the targeted machine. Now, a backdoor malware is installed in the system. Once it is successfully installed, the Command and Control (C2) mechanisms are used to get the control over the victim computers. Once a C&C connection to the victim's computer has been established, the attackers stealthily keep collecting the information stored on the system.
4. **Operation:** In this stage, the attack maintains its persistence in the network for a long period of time. The lateral movement of the attack takes place in the network. In this stage also, the attacker can send a spear phishing mail from the victim system to the other system in the network and the servers storing the sensitive information are identified.
5. **Data Collection:**In this stage, the data and the targeted information from different machines and servers is gathered. Multiple copies of this collected information can be made and stored in different servers called staging points.
6. **Data Exfiltration:** This is the last and the most critical stage of an APT attack. In this, the data collected and stored in the staging points is transferred to the attackers through different channels. The data is sent to multiple servers called drop points so that the actual destination of the data is not detected. This is the last stage of APT.

According to the phases of APT, the defense mechanisms need to be applied to all the phases, in order to provide a full detection mechanism.

Detection at an early stage of APT can be done by:

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

1. The identification of the domain names and to check if they are malicious
2. Verification of the signatures using the signature database
3. Detection of anomalous behaviors like when the user makes multiple attempts to login and the attempt fails more than a predefined threshold value
4. Detection of malicious code embedded with the email attachments

Detection at a later stage can be done by:

1. Monitoring the applications and managing the requests for application changes.
2. Monitoring the access of sensitive data continuously
3. Using tools to monitor the access attempts and generating logs.
4. Monitoring of the outbound data to identify anomalous usage
5. Identifying the encrypted packets sent outside of the organization network
6. Identifying the destinations of the outbound data

II. PROPOSED METHODOLOGY

The proposed methodology is designed for the detection of threat at a later stage of APT. The detection has been done majorly in the operation phase of APT i.e. when the attacker is trying to access the data stored on the system. The detection mechanism proposed in this paper involves combination of few techniques according to the phases of the APT.

In this layer, firstly all the vulnerable documents are monitored. These are the documents that store sensitive information which the attacker may try to read or steal. So, in the **First detection layer:**

1. The access of the sensitive files is monitored.
2. Whenever a file is accessed, its corresponding logs are generated.
3. An access counter is updated. The counter is used to identify the documents that are frequently read/ accessed.

Second Detection Layer:

1. In the second detection layer:
2. Detection of modification in files is monitored with the help of hash mechanism as shown in Figure 3.1.
3. Addition or deletion of files is monitored.
4. Logs are generated for each action performed.
5. The logs are secretly stored in a file showing the exact date and time of access/ modification.

Algorithm or rules:

Step 1: If the program is run for the first time, then it reads all the files which have to be monitored.

Step 2: Then a hash is generated for each file using the hash key “abcdeabcde123456” and saves it in a file.

Step 3: If now, the attacker tries to access/modify the file and save it, then another hash code for that file is generated using the same hash key.

Step 4: Both the hash codes are matched against each other. If the codes are same, then it means the file has been accessed. If the codes are different, the program detects that the file has been modified.

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

Step 5: The previously stored hash file is updated with the new hash.

Step 6: The access/modification counter for file is updated.

III. RESULTS

The Fig. 1 shows the list of sensitive files stored on user's system which the attacker may try to access.

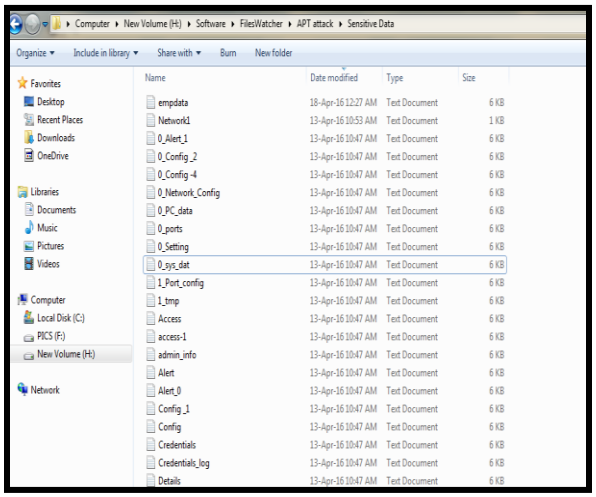

Fig. 1 Sensitive files stored on the victim machine

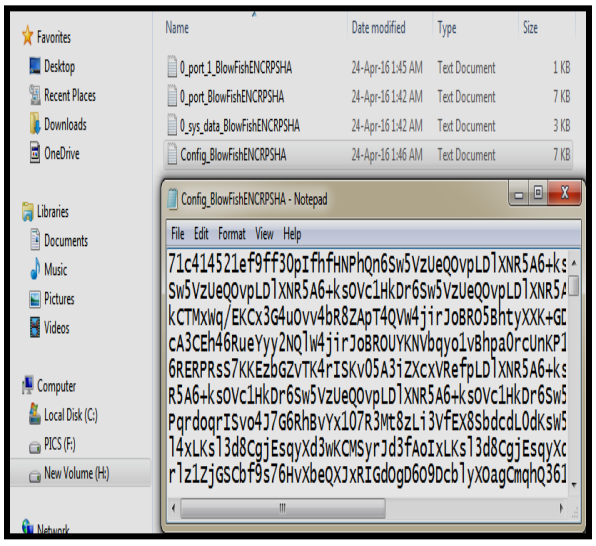

Fig. 2 Hash code generated for each file

Fig. 2 shows hash code generated after running the program.

Fig. 3 illustrates that the logs generated whenever a sensitive file is accessed and the access counter of that file is updated.

Fig. 4 illustrates that the logs of access or modification of files are stored in a file secretly with exact date and time. This log file can be later used for analysis and identification of anomalous behaviors.

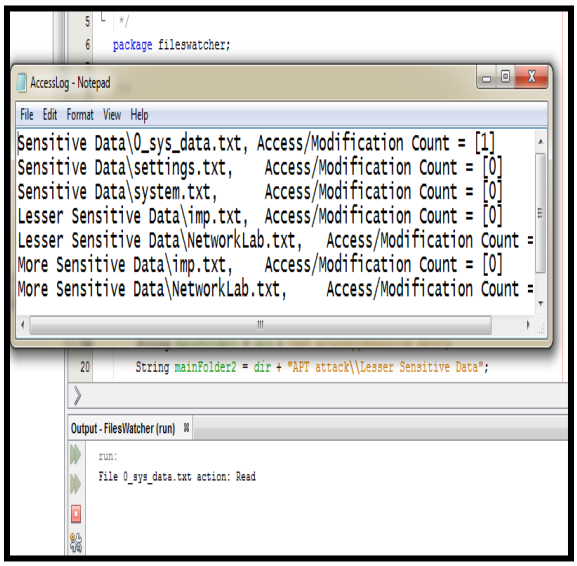

Fig. 3 Logs generated on access of file

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

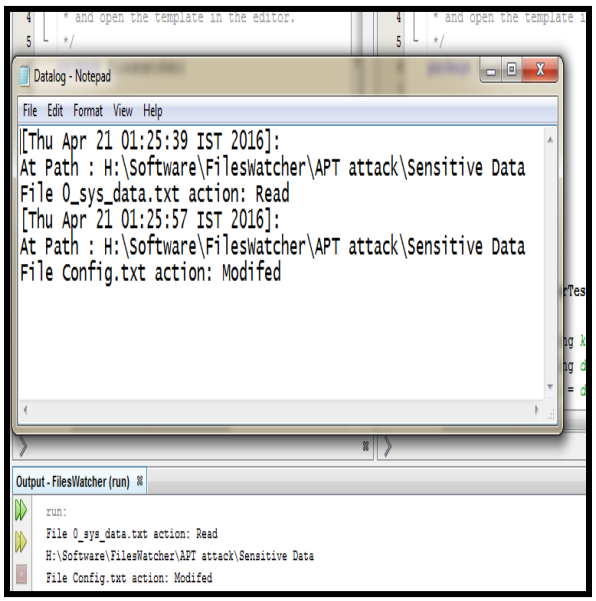

Fig. 4 Logs saved with date and time of access

IV. CONCLUSION AND FUTURE SCOPE

The technique proposed in this paper, works for the second layer of threat, in which the attacker has successfully intruded into the system and tries to access or modify the crucial information stored on the system.

The goal of our technique is to monitor the sensitive files stored on the system. In the proposed technique, the logs are generated for each activity performed by the attacker on the crucial data stored on the victim machine. These logs can further be analyzed for identifying the anomalous patterns or the possibility of threat.

The implementation is done using the java coding which can later be shifted to the bigger platforms and tools like Hadoop for monitoring very large no. of files. Also, the analysis of the logs generated by the program can be easily done by using the tools like Hadoop.

This technique can be combined with the other techniques to form an effective and a complete detection mechanism for Advanced Persistent Threat.

V. REFERENCES

[1] G. Zhao, K. Xu, L. Xu, and B. Wu, "Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis," *Access, IEEE*, 2015, Vol. no. 3, August 2015

[2] Yusuf Simon Enoch, Adebayo Kolawole John and Zirra B. Peter, "Addressing Advanced Persistent Threats using Domainkeys Identified Mail (DKIM) and Sender Policy Framework (SPF)", *Journal of Emerging Trends in Computing and Information Sciences*, Vol. no. 6, January 2015

[3] Paul Giura and Wei Wang, "Using large scale distributed computing to unveil advanced persistent threats", *AT&T Security Research Centre*, New York, 2012

[4] C. Hsieh and K. Lee, "AD 2 : Anomaly Detection on Active Directory Log Data for Insider Threat Monitoring", *49th Annual IEEE International Carnahan Conference on Security Technology*, 2015

[5] P. Hu, H. Li, H. Fu, D. Cansever, and P. Mohapatra, "Dynamic defense strategy against advanced persistent threat with insiders*",* *IEEE Conference on Computer Communications (INFOCOM),* 2015

[6] A.K. Sood and R.J. Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats",*IEEE Security & Privacy*, Vol. no. 11, 2013

[7] https://lirias.kuleuven.be/bitstream/123456789/461050/1/2014-apt-study.pdf

ISSN: 0971-1260
Vol-22-Issue-16-August-2019

[8] http://www.computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation

[9] http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

[10] https://www.lifeboatdistribution.com/content/vendor/sophos/whitepaper-sophos-advanced-persistent-threats-detection-protection-prevention.pdf

[11] https://www.websense.com/assets/white-papers/whitepaper-websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf

[12] http://taosecurity.blogspot.in/2010/01/what-is-apt-and-what-does-it-want.html

[20] http://searchsecurity.techtarget.com/feature/Defend-against-APTs-with-big-data-security-analytics

[21] https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition

[22] https://www.damballa.com/downloads/r_pubs/advanced-persistent-threat.pdf

[23] http://www.mcafee.com/in/resources/white-papers/wp-combat-advanced-persist-threats.pdf