Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 6, 2021, Pages. 1263-1266
Received 25 April 2021; Accepted 08 May 2021.

A Zero-Trust Approach in Digital Forensics

Dr.S.Angel Latha Mary [1], Mukilan N [2], Dr.A.Usha Ruby [3]

[1] Professor and Head, Department of Computer Science and Engineering,
Karpagam College of Engineering, Coimbatore. Email id: xavierangellatha@gmail.com

[2] UG Scholar, Department of Computer Science and Engineering, Karpagam College of Engineering,
Coimbatore. Email id: mukilannarayanamoorthy@gmail.com

[3] Associate Professor, Department of Computer science and Engineering, GITAM School of Technology,
Bangalore Campus,GITAM University, Bengaluru-561203,Karnataka. Email id: uruby@gitam.edu

Abstract:

Today's internet has many applications that make our lives easier. But these applications and the companies that develop them are vulnerable to a plenty of vulnerabilities either unpatched or zero-days that the attackers take advantage of to attack these systems. These companies employ some techniques to investigate these attacks and come to a conclusion. That is where digital forensics plays a major role. Digital forensics involves a series of works and they have to be followed to provide better results. This paper focuses on the zero-trust approach, which could employed to obtain even better results.

Keywords: Digital forensics, zero-trust approach, unpatched vulnerabilities.

Introduction:

Digital forensics is the area or the methodology where the company analyses the attacks it received from the attackers. It could be because of anything, either due to the unpatched vulnerabilities in the software they use or the zero-days in the system itself.

1. Unpatched Vulnerabilities: The vulnerabilities present in some software's they depend on or they use can be exploited and the attackers can use some malware to enter into the system. For example, the application may use some word press plug-in for managing SEO, which may have some vulnerability and the developer might have released some patch to fix this issue. If the company does not update the system, the attacker may take advantage of this unpatched vulnerability to exploit the system using some malware.
2. Zero-day attacks: The products developed by the company are usually deployed within the same server. If the user could manipulate the server in some way, and upload a reverse shell, they could exploit the system by uploading some malwares through the reverse shell uploaded.

These are the main issues for all the attacks targeting the applications and they are analyzed with the help of digital forensics. Thus, digital forensics is nothing but a methodology to analyze attacks and investigate on them to find out where the attack came from, reverse engineers the malwares used, analyzes the damage caused and steps to mitigate them.

Annals of R.S.C.B., ISSN: 1583-6258, Vol. 25, Issue 6, 2021, Pages. 1263-1266
Received 25 April 2021; Accepted 08 May 2021.

Methodology

There are several steps to be followed while analyzing the attacks in order to obtain better results. They are as follows.

1. Identification: In the identification process we completely scan and analyze the system to identify the entities to be investigated. It could be anything ranging from cloud data to memory dumps. Thus, thorough identification mechanisms should be used to find the attacked entity.
2. Preservation of data: It is the most important and the easiest process. When the entity to be analyzed is found, proper mechanisms to be followed to preserve these evidences from getting damaged, For example, if an attack targets the physical memory of the server, then a copy of the memory dump must be taken order to prevent it from becoming erased, since the physical memory is volatile in nature. In other cases, where a hard drives must be investigated, proper preservation equipment like anti-static bags and preventing exposure to UV lights must be ensured.
3. Extract data: Once the data is preserved for the future works, a multiple copies of the data are taken to prevent data loss. Then, the data is extracted to obtain information that is more valuable. This information would be helpful for analysis and investigation in the next steps.
4. Investigation of data: Once all the required information is obtained, the process of investigation starts. In this process, the examiner checks all the possibilities of attacks and how it was executed. If any particular malware is used, a specialized sandbox environment is used for malware analysis. This is can be done with the help of virtualization and reverse engineering. They are also analysed who might have started the attack and how could it be patched.
5. Report generation: It is the last and final process. Since, digital forensics usually involves prosecution and law suits, they have to generate a detailed report of what caused the attacked, which caused the attack and the damage the company had faced. This is the most important process of all as like the preservation of data. Because, even if the examiner finds out everything like who caused the attack and how damaging it was, they had to produce a good write to up to whoever provides the verdict.

The above-mentioned are the important steps involved in digital forensics and malware analysis.

Problem faced in digital forensics

There are multiple problems faced in digital forensics that makes it very difficult to analyze the attacks the company faced. They are as follows.

1. Encryption: When the data is encrypted as in ransom ware, it makes it highly difficult and nearly impossible to decrypt the data for further analysis. This is because, if the data is encrypted, we need the decryption key to decrypt it. It becomes even worse in the case of asymmetric encryptions.
2. Steganography: The problems of encryption are also faced when steganographic techniques are used. For example, the malicious code may be embedded in an image or an audio file. When this file is downloaded to the system, a series of commands may be executed and malware can be injected. It is not so easy to extract the data from the image or any other media file even using the modern standards of steganalysis.
3. Covert channel: This is similar to the working of proxy systems or tunneling. The attacker usually drives the traffic through a secure network system, thereby evading the intrusion detection system like a legitimate file. If this kind of networks are used, it would be difficult for the examiners to find the secure channel and analyze the traffic.

4. False positives: Here, the attacker may leave some unwanted information to false lead the investigator from obtaining useful information or obtaining legitimate information for the investigation purpose.

Zero-Trust approach

The zero-trust approach is something where the companies applies some policies where anything inside and outside the organization is not trusted immediately. Instead, they are analyzed and then allowed inside the organization. This approach can be applied to the digital forensics as well. This helps to prevent the false positives.

Some measures that can be taken in accordance to the zero-trust approach is as follows.

1. Never expect the attacks to be originated only from outside the organization
2. Analyze the data for classification of legitimate data and false positives
3. Use manual approach instead of automating the malware analysis process
4. Take multiple instances of data for analysis
5. When an attack occurs, immediately have an memory dump of the physical memory to have more insights about the attack
6. Completely analyze the systems to check for the spoofed IP
7. After completion of the report, check the attacked machine or the server again to find the hidden malwares
8. Check for parent processes that allowed the malware to be injected

Advantages of zero-trust approach

1. Reduce the time delays caused by false positives:
   In some cases as mention before, the attacker may use some techniques to deliberately leave out some false positives to cause a delay or false lead the investigator to prevent from getting prosecuted. This may cause some delays in the process of investigation. This can lead to overwriting of data, loss of data, or even theft of integrity of the data. Therefore when a zero-trust is followed, legitimate information can be gathering for further proceedings.
2. Gain greater control of the attack environment:
   When manual methods of malware analysis is carried out or when multiple instances of same data is taken to prevent the data loss, there creates greater control of the attack vector and have a better result.
3. Reduce the risk of ignoring malwares:
   When the process of scanning of malwares is done even after reporting the issue, we can get to know about the other malwares that are hidden in the system. Some malwares could spoof the system as a legitimate and an important file for the system. When analyzed it could be a malware and may cause even more damage the previously discovered one.
4. Reduce the loss of data:
   When multiple instances of data are taken, there creates a trust of data. Because, even when any one of the preservation methods fail, all other data would be safe for analysis. In some cases, the examiner may accidentally modify the data. Thus, multiple instances of data can eradicate this problem.
5. Reduce the issues of incorrect verdicts
   In some cases, the attacker might perform a DDoS attack with several hundreds of zombie computers forming botnets. If this IPs is used, then it may lead to false verdicts. Thus better analysis must be done in order to find the control and command server controlling this botnet.

Conclusion

Thus, digital forensics proves to be an inseparable operation in any organization. In the world of increased number of technology usage, there are multiple ways to attack a system either through unpatched vulnerabilities or through the zero-days bug's presents in the application itself. With the help of digital forensics, it is possible to collect information about the attacks, the loss or the damage it had created to the system or the application or the whole organization itself, where it originated from and much more. Though they follow some systematic processes, they might also be false or some difficulties might be faced as discussed. With the help of suggested zero-trust approach, those difficulties can be removed and they will to obtain better results.

References:

[1] Gilman E., Barth D.: Zero Trust Networks, O'Reilly, (2017)
[2] Sivaraman R.: "Zero Trust Security Model". S3tel Inc, White Paper (2015)
[3] Williams C.: Zero Trust Security, Centrify Special Edition. John Wiley & Sons, Inc., Hoboken, New Jersey (2019)
[4] Osorio de Barros G.: "A Economia da Cibersegurança", Gabinete de Estratégia e Estudos, Ministério da Economia(2018)
[5] Morgan S.: "Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020", Forbes (2015)
[6] Kindervag J.: Build Security Into Your Network's DNA: The Zero Trust Network Architecture, Forrester (2010)
[7] Kindervag J.: Clarifying What Zero Trust Is and Is Not (2018)
[8] Akamai: "The 6 Businesses and Security Benefits of Zero Trust." White Paper (2018)
[9] Ward R., Beyer B,: "BeyondCorp A New Approach to Enterprise Security". Usenix, vol. 39:6 (2014)