International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Technology for Antiforensic Attacks

***S Bhargavi*[1], *Chirag R Rai*[2*]**

Dept. of ECE, SJCIT, Chickaballapur, India
*Email :chandangowda2701@gmail.com

ABSTRACT

Day by day, there is increasing demand for high data rates it causes lack of radio spectrum for the new emerging technologies in the area of wireless communications. So, it must use spectrum efficiently, that is proper spectrum management. Spectrum management is responsible for the spectrum deficiency. In case of spectrum management, it is must to accurate determination of the present licensed users. The Cognitive radio is a type of wireless communication. In this a transceiver can intelligently detect which communication channels are in active and which is inactive. As soon as it detects an unused channel it instantly moves into a vacant channel by avoiding busy channels. This results in optimization of the use of available radio-frequency spectrum with minimization of interference to other users.

Keywords— Compression, Instruction cache, Huffman coding, Arithmetic encoding.

INTRODUCTION

Digital forensics is the process of forensic investigation pertaining to computers and mobile devices. Like any forensic investigation, its goal is to gather all the relevant data for recreating the crime scene and shining light on questions like who committed the crime, when they did it, what their motive was, how they attacked, etc.One of the main objectives of attackers is to remain undetected by digital forensic investigators, both during and after their malicious activities. To achieve this, they perform anti-forensic techniques, in which they invest tremendous efforts.The purpose of anti-forensic techniques is to remove any kind of artifact or evidence that can tie the attacker to the incident. Compared to a real-life crime scene, this would be equivalent to the thief wearing a mask to hide from security cameras, gloves to prevent from leaving fingerprints and making sure no used equipment is left at the scene.In this article, I will cover various anti-forensic techniques that are based on file system, Windows Registry, and Windows event logs. Americans lost over USD 4 billion to cyberattacks in2020 (McCarthy, 2021).

Computer Forensic Tools (CFTs) allow investigators to recover deleted files, reconstruct an intruder's activities, and gain intelligence about a computer's user. Anti-Forensics (AF) tools and techniques frustrate CFTs by erasing or altering information; creating "chaff" that wastes time and hides information; implicating innocent parties by planting fake evidence; exploiting implementation bugs in known tools; and by leaving "tracer" data that causes CFTs to inadvertently reveal their use to the attacker. Traditional AF tools like disk sanitizers were created to protect the privacy of the user. Anti-debugging techniques were designed to protect the intellectual property of compiled code. Rootkits allow attackers to hide their tools fromother programs running on the same computer. But in recent years there has been an emergence of AF that directly target CFTs. This paper categorizes traditional AF techniques such as encrypted file systems and disk sanitization utilities, and presents a survey of recent AF tools including Timestomp and Transmogrify. It discusses approaches for attacking forensic tools by exploiting bugs in those tools, as demonstrated by the "42.zip" compression bomb. Finally, it evaluates the effectiveness of these tools for defeating CFTs, presents strategies for their detection, and discusses countermeasures Along with this rise in internet crime, advances in anti-forensictechniques have added new layers of complexity for digital forensic investigators.

Fig 1: Anti forensic techniques [1].

Anti-forensic techniques are designed to prevent individuals who commit cyberattacks from being discovered. In this article, we'll explain the five anti-forensic techniques that present the most significant challenges for today's digital forensic investigators. The rapid growth and development in technology has made computers a weapon which can cause great loss if used with wrong intentions. Computer forensics aims at collecting, and analyzing evidence from the seized devices in such ways so that they are admissible in court of law. Anti-forensics, on the other hand, is a collection of tricks and techniques that are used and applied with the clear aim of forestalling the forensic investigation. Crime and crime prevention go hand in hand. Once a crime surfaces, then a defense is developed, then a new crime counters the new defense. Hence along with continuous developments in forensics, a thorough study and knowledge of developments in anti-forensics is equally important. This paper focuses on understanding different techniques that can be used for anti-forensic purposes with help of open source tools.Computers have become an integral part of our day to day life. They are being used in every walk of life and have made life convenient for everyone. However, different capabilities of computers have also equipped criminals with technology that can be misused. Now a crime can be surfaced either without leaving any evidence or by removing them such that they are untraceable. Hence, computer crime is any crime which involves usage of a computer or any other digital device making it a subject of investigation [1]. Web definition of forensics explains it as methods and techniques used in investigation of crime [2]. Therefore computer forensics refers to a computer system which has been seized from a crime scene and undergoes forensic analysis in search of substantial evidence.

Computer forensics is necessary not only to collect evidence of crime from computers but also to validate them so that they are admissible to the court of law. With most of the crimes taking place using digital devices, courts of law all around the world are giving equal importance to digital evidence as eyewitnesses [3].Therefore it becomes crucial for both criminals and investigators to handle digital evidence carefully. While investigators take measures to retrieve evidence from digital devices intact, criminals, on the other hand, take countermeasures trying to hide or even destroy the evidence, making investigation even harder. For instance, a case of murder presented as a suicide case. The methods used by the criminal to hide or tamper with the evidence are anti-forensic techniques

METHODOLOGY

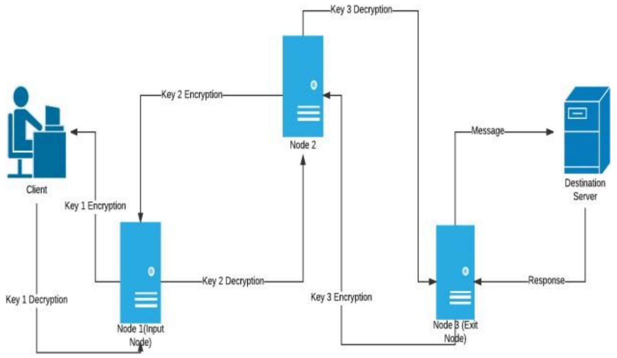

Fig 2: Onion Routing Circuit [4]

The client with access to all the encryption keys i.e key 1, key 2 & key 3 encrypts the message(get request) thrice wrapping it under 3 layers like an onion which have to be peeled one at a time. This triple encrypted message is then sent to the first server i.e. Node 1(Input Node). Node 1 only has the address of Node 2 and Key 1. So it decrypts the message using Key 1 and realizes that it doesn't make any sense since it still has 2 layers of encryption so it passes it on to Node 2. Node 2 has Key 2 and the addresses of the input & exit nodes. So it decrypts the message using Key 2 realizes that it's still encrypted and passes it onto the exit node. Node 3 (exit node) peels off the last layer of encryption and finds a GET request for youtube.com and passes it onto the destination server. The server processes the request and serves up the desired webpage as a response. The response passes through the same nodes in the reverse direction where each node puts on a layer of encryption using their specific key. It finally reaches the client in the form of a triple encrypted response which can be decrypted since the client has access to all the keys.

TECHNOLOGY

Data/File DELETION

Intruders will be a lot concerned about covering the tracks of their prohibited activities across a network or system and try to delete the information contained within the disc as a part of their effort to avert detection. They conjointly attempt to delete foot prints of the files exploitation specialized tools. The method includes elimination of supply files, logs, traces of information from places on the disk drive, and entries on the disc drive (HDD), that embody attributes, orphan files, and dynamic linklibrary DLL files. Intruders may also firmly delete informationor write it to mask the first information. One of the most prominent ways adversaries cover the tracks of their prohibited activities, is deleting artifacts left from the execution of their capabilities in victims' environments.Before diving into the details of deleted files, let's understand how files are stored.Each computer storage device has a file system that organizes the order in which files are arranged and stored. The file system has metadata on each file, including the file name, MACB times, the user who created the file and its location.

DATA/FILE WIPING

Since attackers cannot rely on chance, they need to make sure that the file data and metadata is overwritten and cannot be recovered. There are many tools out there that can do this job,

e.g. “Eraser”, “R-Wipe and Clean” and “File Shredder”. For the ones who love the famous Sysinternals suite – “SDelete” can be used. For the demonstration, I have created a text file called “Wiping_Test.txt”,. You can see that its entry number on the MFT is 853, it is located at “C:\Users\User\Desktop” and its size is 783370 bytes. Pay close attention to its timestamps.

I parsed the $MFT after I wiped the file. As you can see, the same entry number “853” was immediately reused by a different file. Behind the scenes, the NTFS scanned the MFT records and searched for a record with the “unused” flag and then replaced it with another file. There is no longer evidence of “Wiping_Test.txt” in the MFT! Does this mean the attackers can sleep peacefully. The MFT file is the most known forensic evidence used by forensic investigators when they want to prove the existence of a file. Attackers might think that if they clear any evidence from the $MFT, they are completely erasing any evidence that could lead to tracking down the existence of their file.However, there are few more forensic pieces of evidences that still can be used to provide file existence/ Let melist them for you: $J – In case you forgot, this file records file activities so it is worth reviewing.

TIMESTOMPING

Timestomping is the act of changing the timestamp on the metadata of a file, usually to a time prior to the timeframe the incident occurred. The main reason attackers use timestomping, is to delay the detection by as much as they can. If the forensic examiner uses a filter that is based on the timeframe of the initial alert or notification, timestomped files will not show up.

On top of that, timestomped files can stay undetected when performing Threat Hunting on the environment and if a time stamp is part of the detection logic.

STEGNOGRAPHY

Steganography is the process of hiding secret messages or information within an audio, image, video, or text file in a non- suspicious manner. Steganography techniques are often incorporated with encryption to provide an added layer of security. The secret data is extracted by the authenticated person with access to the destination using a steganography tool for decoding the hidden message. Hackers have been using steganography to hide malicious codes and files within legitimate files to bypass security and obfuscate their trails. This anti-forensic technique allows attackers to conduct malicious activities without being detected through threat detection tools and other security parameters. Hackers have been known to hide secret malicious payloads or suspicious messages with invisible ink within news articles, advertisements,

APPLICATIONS

1. Security event monitoring.
2. Establishing the identity of the criminal and victim.
3. Securing and recording the scene of the crime.
4. Collection and preservation of potential pieces ofevidence.
5. DNA Phenotyping.

ADVANTAGES

- Forensics provide accurate and consistent data for theinvestigation.
- It collects all the data of the crime.
- It helps to identify how the crime has happened.

CONCLUSION

The forensic attacks have increased and many new techniques are coming up to protect the data. These techniques will not allow the hacker to access the data or change the data easily andthe crime will cyber-forensic crime will decrease.

REFERENCES

[1] M. Geiger, “Evaluating commercial counter-forensic tools,” Proc. 5th Annu. Digit. Forensic,2015.

[2] D. K and M. B., “Toward understanding the challenges and countermeasures in computer anti-forensics.,” Int. J. Cloud Appl. Compute., 2017.

[3] A. Joshi and D. Bhilare, “Emerging trends and research in digital forensics,” Oiirj.Org, 2014.

[4] Simson L. Garfinkel, " Anti-Forensics: Techniques, Detection and Countermeasures ", Naval Postgraduate School, Monterey, CA, USA, 2017.

[5] Gurpal Singh Chhabra and Anu Jain, " Anti-Forensics Techniques: An Analytical Review", Thapar University Patiala, 2016.

[6] Emin Kugu, " A Survey on Anti-Forensics Techniques ", Hezarfen Aeronautics and Space Technologies Institute, National Defense University Yeşilyurt, 2019.

[7] S. Hilley, "Anti-Forensics with a small army of exploits", Elsevier - Digital Investigation, 2018.

[8] Geiger, "Counter-Forensic Tools: Analysis and Data Recovery" , 18th Annual FIRST Conference, Jun 25-3-2016.

[9] Adv. Prashant Mali, "Electronic Evidence and Cyber Law", CSICommunications, Sep 2018.

[10] H. Jahankhani and E. Beqiri, Handbook of Electronic Security and DigitalForensics, 2010.