International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Effective Data Erasure and Anti-Forensics Techniques

Anand V[1], Dr. MN Nachappa[2]

[1]MCA Scholar, [2]Academic Head,

[1,2]Department of MCA, School of CS & IT, Jain (Deemed-to-be) University, Bangalore, Karnataka India

ABSTRACT

Deleting sensitive data after usage is just as important as storing of data in a safe location. In the verge of cyber-attacks such as data theft happening, it is best to delete or purge or destroy unwanted sensitive data after its use as soon as possible. Data stored offline, for example in hard disks are just as prone to get stolen as the data stored online. For destroying the data to ensure cybercriminals should not get hold of this, techniques such as Data Wiping and Anti-Forensics are used. A study is done on how these techniques can be used to the advantage of our system and against the cyber criminals.

KEYWORDS: *Data, Windows registry, Anti-Forensics, Data Wiping*

How to cite this paper: Anand V | Dr. MN Nachappa "Effective Data Erasure and Anti-Forensics Techniques" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.708-711, URL: www.ijtsrd.com/papers/ijtsrd38043.pdf

IJTSRD38043

1. INTRODUCTION

Data deleted from the hard disk is technically 'not deleted', means it is being replaced by free space and new data thereof. The deleted data recovery was there since the beginning of 90's itself. And now more advanced methods made data to be recovered more easily. This poses as a security threat because their information which is to be gone for good for the sake of privacy. A normal non techie user deletes with assumption that it is gone forever and his private information will never be leaked or recovered. However, it can be recovered with better hardware, faster processors and efficient software.

Wiping the hard disk is one way to purge/destroy the data in such a way that it never will be recovered. There are many methods to wipe hard disk space. The other term used as synonym of wiping data is called shredding. For shredding, different types of algorithms are used, each of them having their own advantages and disadvantages, a balance of Speed of completion of data shredding and the Security which depicts how hard it is to recover the data.

The latter part that will be discussed will be about various Anti-Forensics methods used by cyber criminals in order to prevent them from being exposed and captured by the police. These techniques can be used against them in such a way that it will secure the information and security of the organization. This study will be an extension to the former part, i.e. Data Wiping method, since that also comes under the purview of Anti-Forensics.

In short, the main types of malicious activities done by cyber criminals are listed below and the solutions, techniques will be discussed further.

- Recovering deleted data from stolen storage devices.
- Finding open ports to plan attack/hacking.
- DDos attack to the specific targeted IP Address

2. BACKGROUND

2.1. Data Wiping Algorithms

The below figure shows comparison for each shredding algorithm.

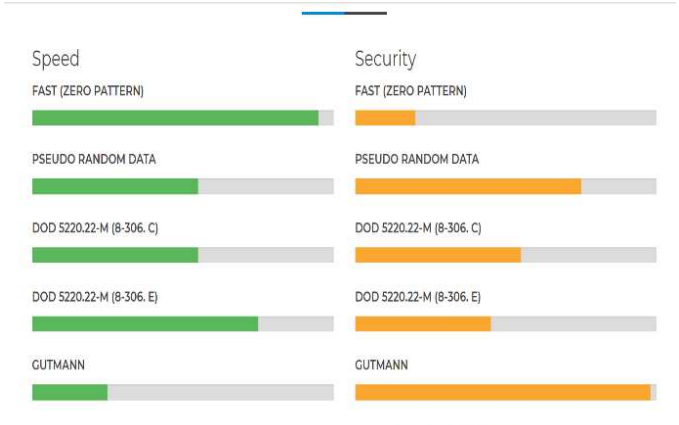

Figure 1: Comparing Data Wiping Algorithms

From this figure, we can assume that Gutmann method is more secure and using this method make the deleted data less recoverable, however Gutmann method takes more time and high toll on the system resources such as processor and

RAM. Aim is to find a way to run Gutmann algorithm on a low scale as a background service the whole time the PC is working it will shred the slack/free space without utilizing much of system resources, because it should not affect the other normal programs of windows. The disadvantage of consumption of time by this algorithm cannot be changed, however it can be extended.

For example, if 500 GB of free space takes 24 hours to be shredded it takes large amount of RAM memory of a single run. Instead of that if we use a method or technique to shred the same 500 GB free space by limiting resources to the process, the performance of the computer will not slow down in a noticeable manner. The progress is saved on every shutdown and resumed back when pc is turned on. This method will extend the time to days or even weeks, however it will not be noticeable since there is always times when pc is turned on idle and very low RAM-Processor consuming software are used. Little by little, slow and steady the private/confidential/useless data is deleted forever beyond recovery.

2.2. Open Port Vulnerability

In networks security an open port is a number assigned to UDP/TCP to receive packets. All the communication and data exchange are happening through ports. Leaving the port open after use is a dangerous vulnerability, because the attackers can insert malware though it and gain access to the system.

2.3 DDoS Attack

DoS (Denial-of-Service) attack means sending multiple and malicious requests from a device to a server/system/website just to make it overload and slow down or break the functioning of resources. DDoS (Distributed Denial-of-Service) is using multiple devices including maybe even IOT devices too. A main target now a days are the online video gamers had to become victims of this. The DDoS attacks caused the online gamers systems slow down and even crash

Figure 2: DDoS Attack

3. ANTI-FORENSICS

Anti-Forensics is commonly known as the techniques used by cyber criminals to over their malicious activities over internet or in their own computer offline. Deleting the data beyond recovery is one of the main examples of Anti-Forensics. However according to the situation, the term Anti-Forensics can have other meaning also, in a positive way. By wiping sensitive information, we are preventing the potential attackers and infiltrators from accessing those. It is the responsibility of the system administrator to protect each and every bit of data from leaking out. The field of Anti-forensics is a considerably less explored field when considering to other fields of cyber security, so giving education to the employees under the system administrator and dealing with database management, developing and information management.

Thus, some techniques can be implemented on the systems containing deleted sensitive data with the adequate permissions from the upper authority of the organization. The term Anti Forensics is mostly understood in a negative way, i.e. Ways in which cyber-criminals erase their activity so that evidence should not be traced back to them, on the other hand if we see it in such a manner that those techniques which the perpetrators use can be used against them too. Say like "If you want to catch a thief, you need to think like a thief". Let us see how the techniques used can be used against them with the help of two case studies.

4. PROPOSED DESCRIPTION

In this part of two case studies are considered which involves anti-forensics and how it can be implemented more effectively. They can be listed as

1. Data wiping without any interruptions – Wiping the free space/deleted data from slack space by keeping the system in hibernation mode temporarily;
2. Continuous scanning of ports to check forany open ports.
3. 3-IP spoofing for own computer, when a DDos Attack is suspected.
4. Extracting embedded hidden information using steganography.

In order to perform these operations, system administrator privileges are necessary, since it involves changing of registry values. These techniques are recommended only to be performed only once a year or in 6 months, or whenever it may deem necessary and not on a regular basis.

5. TECHNIQUES AND EXECUTION

Step 1: Hibernating the PC

This is a temporary procedure. By using python scripts, disable the options of Shutdown, Restart and Sign out. The reason behind doing this is simple. All these three processes cause the ongoing processes to stop, and once again these processes will start from the beginning. The Algorithms such as Guttman algorithm takes days, maybe even weeks to complete the operation. It is not practicable to do that in just a single day.By hibernating the pc after use for the day, every time, when the PC is turned on, all the background processes happening in the background will be resumed as it was running earlier.

After all the procedures which takes long time to complete, not only data wiping, but also deep vulnerability Anti-Virus Scanning, we can turn back on the Shutdown, Restart and Sign-out options. Note that this is just to make sure that no one should end those processes in between.

To hide the Shutdown, Restart, Sign out button

- In the registry editor go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device\Start

- Find the keys HideShutDown, HideRestart and HideSignOut
- Change its values from 0 to 1 respectively.
- Shutdown, SignOut and Restart buttons are hidden

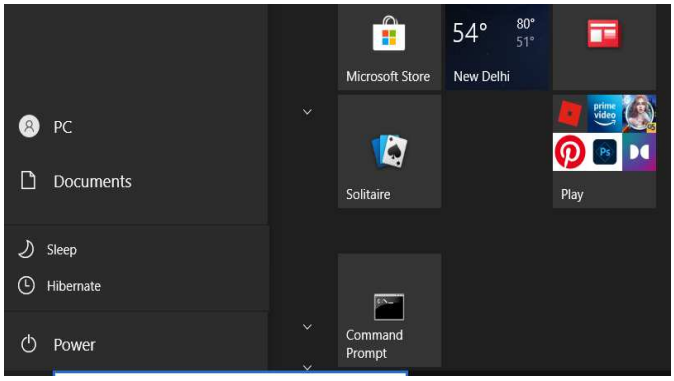

Figure 3: Shutdown, Restart, Sign Out Hidden

Step 2: Perform Data Wiping

We can either use third party application such as Eraser or CCleaner which has 35 pass Guttman pass or use the inbuilt data erasure command of Windows "Cipher" using cmd.

- By using Eraser

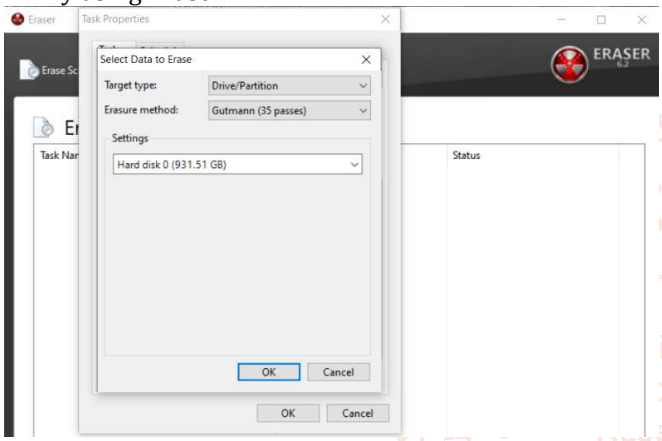

Figure 4: Guttman 35 passes

- By using Cipher

cipher /w:D:\ -- Wipes all the free space/deleted contents in Drive D beyond recovery.

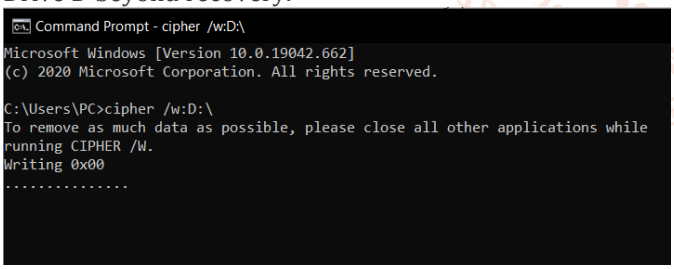

Figure 5: Cipher Command in Windows

Step 3: Port Scanning

A third-party application like Advanced Port Scanner can be used. If the scan is taking longer time, the System can be hibernated. And when it is turned on again, the scan will continue from the port which till then got completed

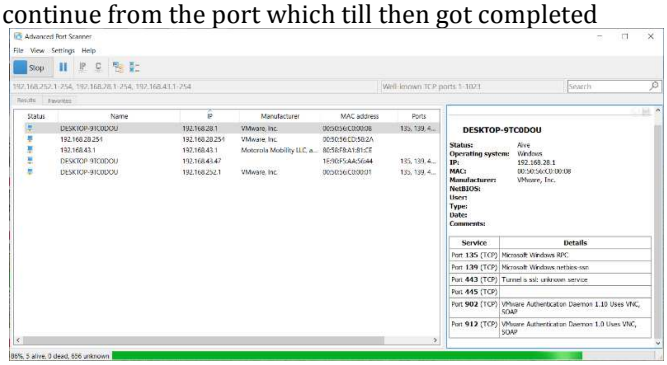

Figure 6: Advanced Port Scanner

Lastly

After performing Data wiping and other time-consuming scanning/anti-forensics operations, we have to unhide the buttons which we hid earlier

To unhide the Shutdown, Restart, Sign out button

- In the registry editor go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PolicyManager\current\device\Start

- Find the keys HideShutDown, HideRestart and HideSignOut
- Change its values from 1 to respectively.
- Shutdown, SignOut and Restart buttons are no longer hidden

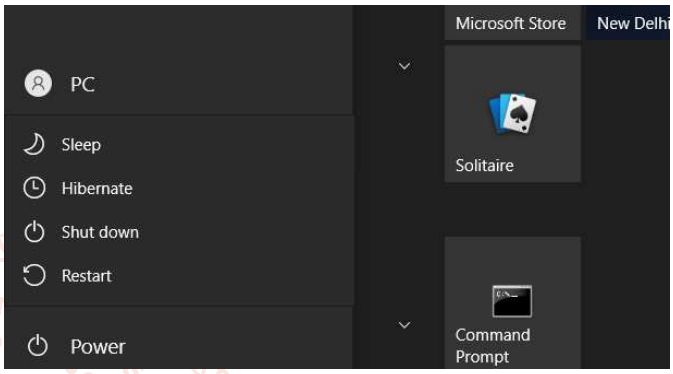

Figure 6: Shutdown, Sign Out and Restart buttons restored

6. FUTURE SCOPE

Like said earlier, in order to beat a criminal, we may have to think like the criminal. These Techniques may not be as fully effective towards the new and upcoming cyber-attacks, but it surely can be used to integrate when making a bigger software solely for the purpose of stopping cyber-criminal activities. We are utilizing the idle time of the computer and securing the data.

Even though tampering of windows registryis not recommended, for the better security of information in the organization, these techniques will come in handy.

7. CONCLUSION

Data wiping and Forensics procedures are long and time-consuming works. It may not be able to complete all in one day. Through this project solution by division of work was seen possible. One every while applying these techniques, the deleted data, which may be sensitive or not will not reach at the hands of the cybercriminal, and counter measures can be taken for Anti-Forensics.

REFERENCES

[1] (CISA), T. C. (2009). *Understanding Denial-of-Service Attacks.* US-CERT.

[2] Gutmann, P. (July 22-25, 1996). Secure Deletion of Data from Magnetic and Solid-State Memory. *Sixth USENIX Security Symposium Proceedings, San Jose, California*.

[3] How to Choose a Secure Data Destruction Method. (2006, Jan 6).

[4] Kissel, R., Regenscheid, A., & Scholl, M. (2014). Guidelines for Media Sanitization. *NIST Special Publication 800-88*.

[5] *Microsoft Docs*. (n.d.). Retrieved from Microsoft: https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cipher

[6] Noblett, M. G., Pollitt, M. M., & Presley, L. A. (2000). Recovering and examining computer forensic evidence. *Forensic Science Communications*.

[7] Pereira, M., José, D., & Santana,, L. (2019, September). *Forensics and Anti-Forensics a Case Study with Port Scan Intrusion and Data Wipe.* Retrieved from ResearchGate: https://www.researchgate.net/publication/337010973_Forensics_and_Anti-Forensics_a_Case_Study_with_Port_Scan_Intrusion_and_Data_Wipe

[8] Roy, S., Bedi, H., & S, S. (n.d.). Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows.

[9] Wei, M., Grupp, L., E. Spada, F., & Swanson, S. (n.d.). Reliably Erasing Data From Flash-Based Solid State Drives. 13.