Information Cyberwarfare

Malware Analysis

Assignment 1

Student Number: MS19801896

Student Name: Janarthanan Krishnamoorthy

Subject: Information Cyberwarfare

Course: M.Sc. Information Technology (Cyber Security)

Table of Contents

Introduction

Malicious software, or malware, has an impact on most computer interruption and security problems. Any software that accomplishes something that makes hurt a client, computer, or network can be considered malware, including viruses, Trojan horses, worms, rootkits, scareware, and spyware. While the different malware manifestations execute vivid ground of various things as malware analysts, we have a center arrangement of devices and procedures available to us for breaking down malware. Malware analysis is the specialty of dismembering malware to its core structure to see how it functions, how to distinguish it, and how to overcome or dispose of it. With a huge number of malicious projects in the domestic digital platform, and becoming more and more specialized each day, every individual should be in sighted of the malware analysis. Furthermore, with a deficiency of malware analysis experts, the skilled malware analyst is in genuine interest. Our concern is all about the disposal of the malware more efficiently while ensuring the safety of the client's digital assets. We center around malware found on the Windows operating system—by a long shot, the most widely recognized operating system being used today yet the aptitudes you learn will work well for you while dissecting malware on any operating system. We likewise center on executables, since they are the most widely recognized and the most troublesome files that you will experience.

What is Malware analysis

The reason for malware analysis is for the most part to give the information you need to respond to a network intrusion. Your primary objective will be to get an insight into the incident and to ensure the existence of the malware in a system. When investigating suspected malware, your objective will ordinarily be to decide precisely what a specific presume double can do, how to distinguish it on your network, and how to gauge and contain its harm. When you recognize which files require full analysis, it's an ideal opportunity to create signatures to distinguish malware diseases on your network. As you'll learn all through this book, malware analysis can be utilized to create host-based also, network signatures. Host-based signatures, or indicators, are utilized to distinguish malicious code on casualty computers. These indicators frequently identify the files or data generated or manipulated by the malware or transparent alterations that it makes to the library. Not at all like antivirus signatures, malware indicators center around what the malware does to a

system, not on the qualities of the malware itself, has which made them more compelling in recognizing malware that changes the structure or that has been erased from the hard disk.

Network signatures are utilized to recognize malicious code by observing network traffic. Network signatures can be made without malware analysis, yet signatures made with the assistance of malware analysis are for the most part undeniably more successful, offering a higher location rate and less false positives. In the wake of acquiring the signatures, the last target is to make sense of precisely how the malware functions. This is frequently the most posed inquiry by senior management, who needs a full clarification of a significant intrusion.

Malware Analysis Techniques

Obviously, during malware analysis, the malware would be just executable but with more complicated contextual. To understand it, you'll utilize an arsenal of tools and deceives, each noteworthy a modest quantity of information. You will have to utilize the resource of tools to see the full picture. There are two primal principal approaches to malware analysis: static and dynamic. The static analysis includes analyzing the malware without running it. Dynamic analysis includes running the malware. The two techniques are further sorted as basic or advanced.

Basic Static Analysis

The basic static analysis encompasses the examination of the file trespassing the official guidelines comprises inspecting the executable file without review the genuine guidelines. Basic static analysis can ensure whether a file is malicious, give information about its usefulness, and now and then give information that will permit you to deliver basic network signatures. Basic static analysis is clear and can be brisk, yet it's to a great extent insufficient against refined malware, and it can miss significant practices.

Basic Dynamic Analysis

Basic dynamic analysis techniques include running the malware and watching its conduct on the system to evacuate the contamination, produce viable signatures, or both. In any case, before you can run malware securely, you should generate an environment with a viable measure of digital safeguards that will provide you the satisfaction of running. Malware Analysis Primer 3 malware without danger of harm to your system or network. Like basic static analysis techniques, basic

dynamic analysis techniques can be utilized by most individuals without profound programming information, however they won't be successful with all malware and can miss significant usefulness.

Advanced Static Analysis

The advanced static analysis comprises of figuring out the malware's internals by stacking the executable into a disassembler and taking a gander at the program guidelines to find what the program does. The guidelines are executed by the CPU, so advanced static analysis lets you know precisely what the program does. Notwithstanding, advanced static analysis has a more extreme expectation to absorb information than basic static analysis and requires particular information on disassembly, code develops, and Windows operating system ideas, all of which you'll learn in this report

Advanced Dynamic Analysis

The advanced dynamic analysis utilizes a debugger to examine the inward condition of a running malicious executable. Advanced dynamic analysis techniques give another approach to extricate definite information from an executable. These techniques are most helpful when you're attempting to get information that is hard to accumulate with different techniques. In this book, we'll show you instructions to utilize advanced dynamic analysis along with advanced static analysis to break down suspected malware.

What is Malware

"A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim".

Types of malware

Adware	Advertising that is integrated into the software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack Kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanisms that bypass a normal security check; it may allow unauthorized access to functionality in a program, or onto a
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.
Drive-by-Download	An attack using code in a compromised web site that exploits a browser vulnerability to attack a client system when the site is
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.
Macro Virus	A type of virus that uses macro or scripting code, typically embedded in a document and triggered when the document is viewed or edited, to run and replicate itself into other such
Mobile code	Software (e.g., script, macro, or other portable instruction) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Rootkit	Set of hacker tools used after an attacker has broken into a computer system and gained root-level access.

Spammer programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate
Virus	Malware that, when executed, tries to replicate itself into other executable machine or script code; when it succeeds the code is said to be infected. When the infected code is executed, the virus
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, usually by exploiting software vulnerabilities in the
Zombie, bot	The program activated on an infected machine that is activated to launch attacks on other machines.

Classifications of Malware

There is no universally accepted classification

- One classification is based on:
  - How malware first spreads/propagates to reach its target
  - The payloads/actions malware performs on the target
- Other malware classification:
  - Parasitic software that needs a host program (e.g., virus)
  - Self-contained software (e.g., worms, trojans)
  - Malware that does not replicate (trojans, email spam)
  - Malware that replicates (virus, worms)

Propagations:

- By infection - Infecting existing program that spread to other systems (e.g., virus)
- By exploiting vulnerability - Attacking software vulnerabilities that allow malware to be downloaded/spread, e.g., worm
- By social engineering - Tricking users to install the malware (trojan, phishing)

Payloads:

- Corrupting host systems and data
- Stealing system resources/service to make it zombie/botnet
- Stealing system information (login, password, other personal details)
- Stealthing – hiding within the host system to avoid detection

What is a Virus

A computer virus, much like an influenza virus, is intended to spread from host to have and can repeat itself. Additionally, similarly, that influenza virus can't imitate without a host cell, computer viruses can't repeat and spread without programming, for example, a file or document.

In increasingly specialized terms, a computer virus is a kind of malicious code or program written to adjust how a computer works and is intended to spread starting with one computer then onto the next. A virus works by embedding or attaching itself to a legitimate program or document that bolsters macros to execute its code. All the while, a virus can cause surprising or harming impacts, for example, hurting the framework software by corrupting or destroying data.

It has four phases in its lifetime. They are,

- Dorman phase: the virus is idle - It will eventually be activated by some events
- Propagation phase: the virus put a copy of itself into other programs or disk. the copy may or may not be identical to avoid detection
- Triggering phase: the virus is activated to perform its intended function

- Execution phase: Where the intended function is being performed. It can be harmless but annoying or damaging

Virus Categories by its targets:

- Boot Sector Infector – infecting the master boot record and spreading when the system is booted
- File Infector – infecting executable files
- Macro virus – infecting macro or scripting files interpreted by the application
- Multipartite virus – infecting files in multiple ways.
- Stealth virus – a form of the virus and its payload that are intentionally designed to hide from detection
- Polymorphic virus – a virus that is hard to detect by its signature since it mutates/changes with every infection
- Metamorphic virus-like polymorphic, it mutates in every infection

How does a computer virus attack

When a virus implant itself to a program, file, or document it stays dormant until it finds it runs it to circumstance or viable conditions to execute its primary. All together for a virus to defect your computer, you need to run the contaminated program, which thusly causes the virus code to be executed.

This implies a virus can stay dormant on your computer, without giving significant indications or side effects. In any case, when the virus taints your computer, the virus can contaminate different computers on a similar system. Stealing passwords or data, logging keystrokes, corrupting files, spamming your email contacts, and in any event, assuming control over your machine are only a portion of the staggering and bothering things a virus can do.

While some viruses can be fun playful in expectation and impact, others can have significant and harming impacts. This incorporates eradicating data or making lasting harm your hard disk. More terrible yet, some viruses are designed for financial profits.

How do computer viruses spread

In a continually associated world, you can get a computer virus from various perspectives, some more clear than others do. Viruses can be spread through email and instant message attachments, Internet file downloads, and web-based life trick joins. Your cell phones and cell phones can get contaminated with portable viruses through obscure app downloads. Viruses can shroud camouflaged as attachments of socially shareable substances, for example, entertaining pictures, welcoming cards, or sound and video files.

To evade contact with a virus, it is essential to practice alert when riding the web, downloading files, and opening connections or attachments. To help remain safe, never download content or email attachments that you are not expecting or files from sites you do not trust.

What are the signs of a computer virus

A computer virus assault can deliver an assortment of manifestations. Here are some of them:

Frequent pop-up windows: Pop-ups may urge you to visit strange sites. Or on the other hand, they may push you to download other software programs or antivirus.

Changes to your homepage: Your standard landing page may change to another site, for example. Besides, you might be not able to reset it.

Mass emails being sent from your email account: A criminal may assume responsibility for your record or send emails in your name from another tainted computer.

Frequent crashes: A virus can cause significant harm to your hard drive. This may make your gadget freeze or crash. It might likewise keep your gadget from returning on.

Unusual slow computer performance: An abrupt difference in processing speed could flag that your computer has a virus.

Unknown programs that startup when you turn on your computer: You may get mindful of the new program when you start your computer or on the other hand, you may see it by checking your computer's rundown of dynamic applications.

Unusual activities like password changes: This could keep you from signing into your computer.

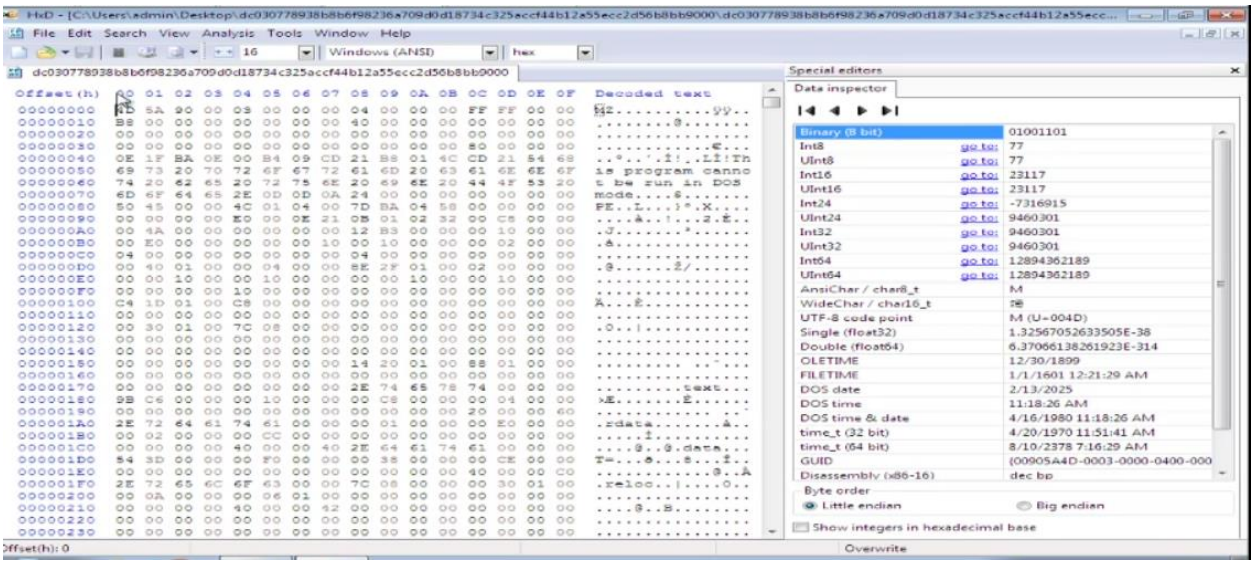
Malware Analysis of Credential Harvester Virus:

Tools required to Analysis malware

- Hex editor
- Exe into PE
- PE studio
- CFF Explorer
- Hash calc
- Virus total
- PE iD

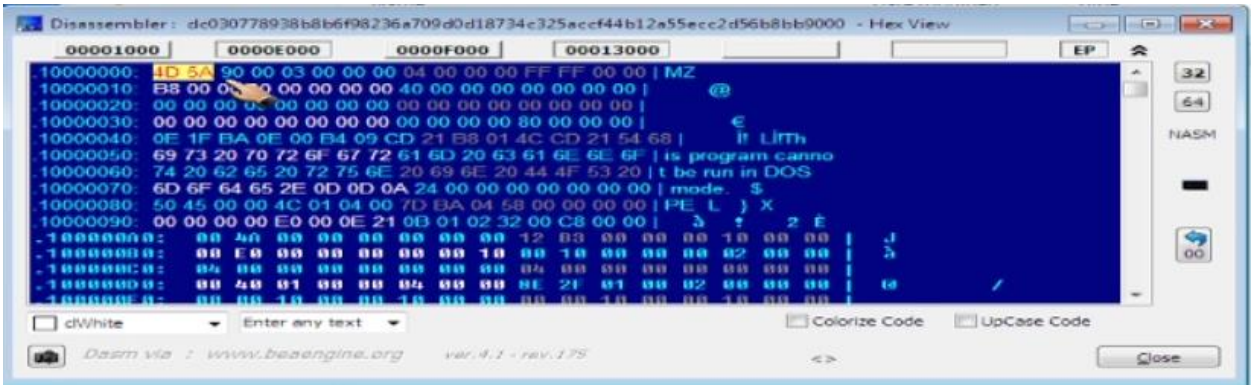
File type identification

Analysis with Hex Editor

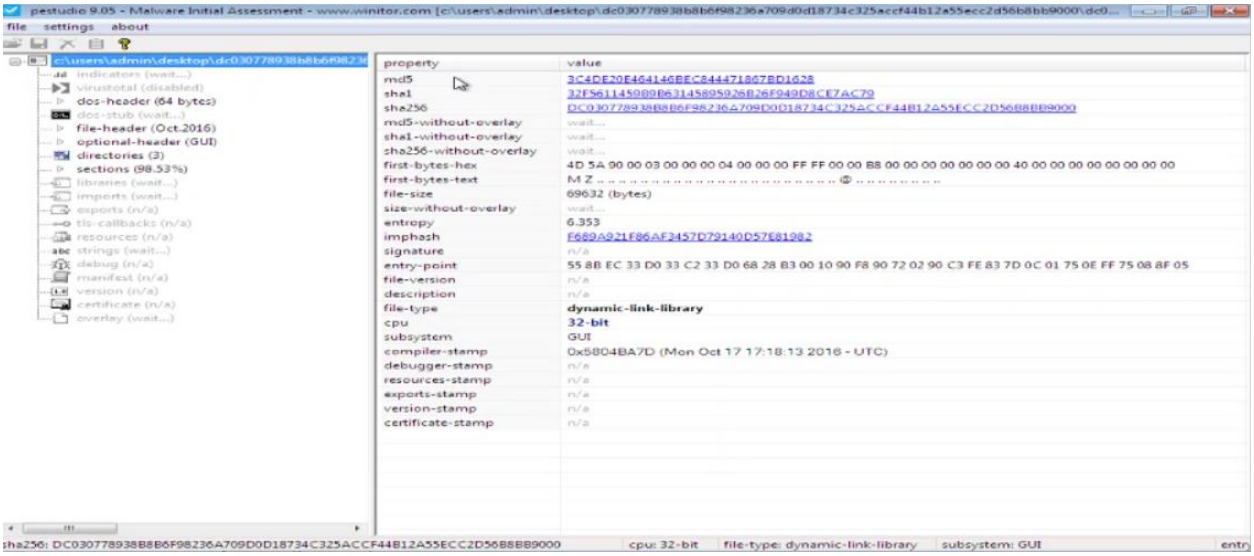


Analyzing the file type by using the Hex Editor. The file type here I found is a 4D 5A – MZ which is a portable executable file.

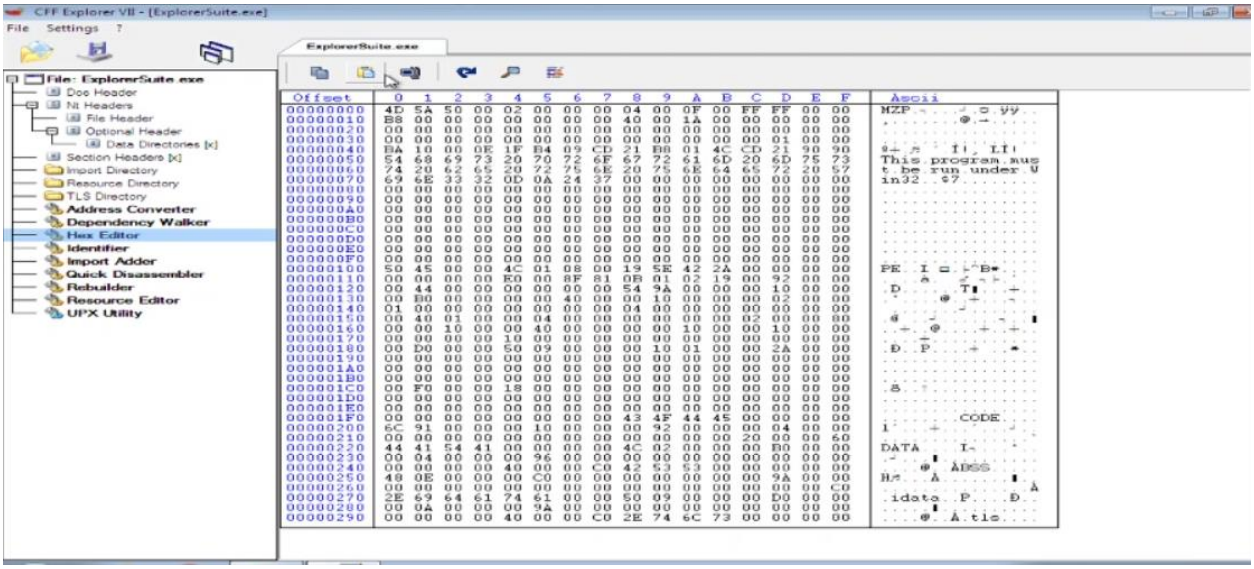
Analysis with Exeinfo PE



Analysis through PE Studio

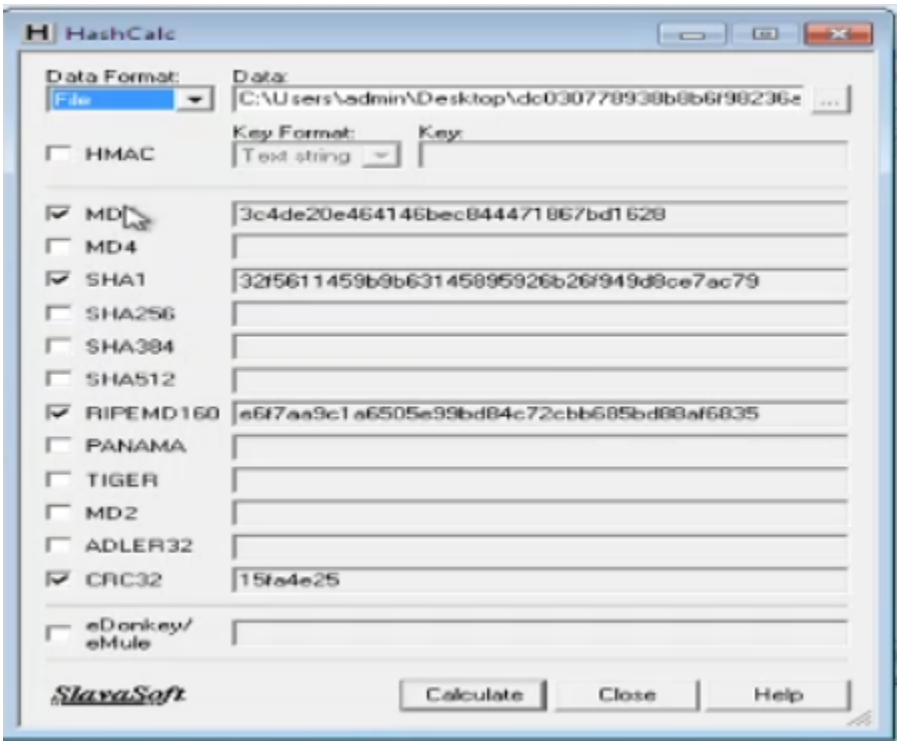


Analysis through CFF Explorer

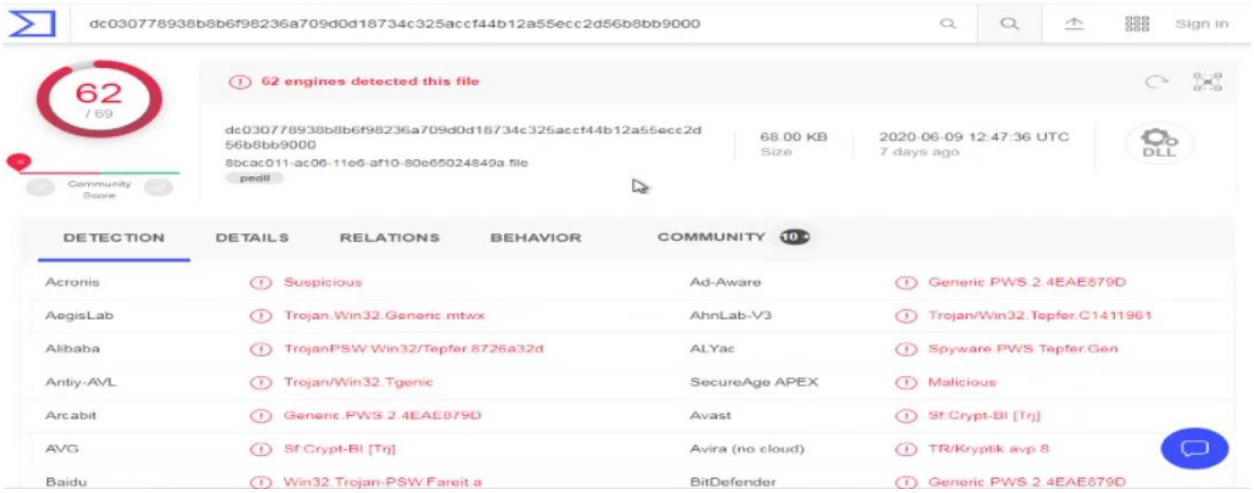


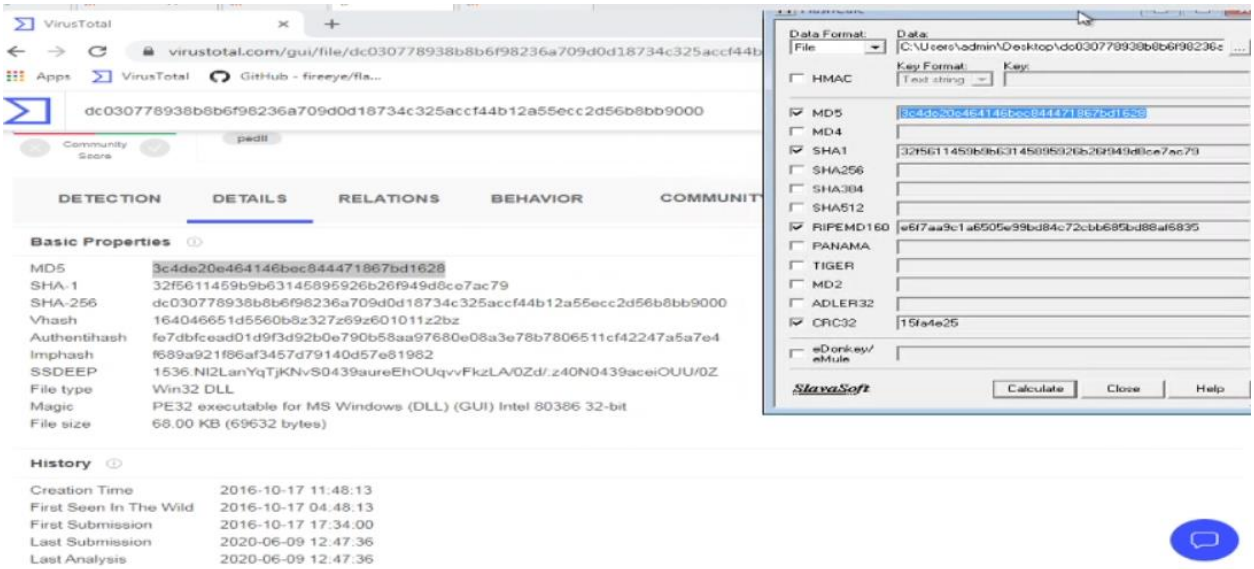
Hash calculation and analysis

Hash calculation through Hash calc application



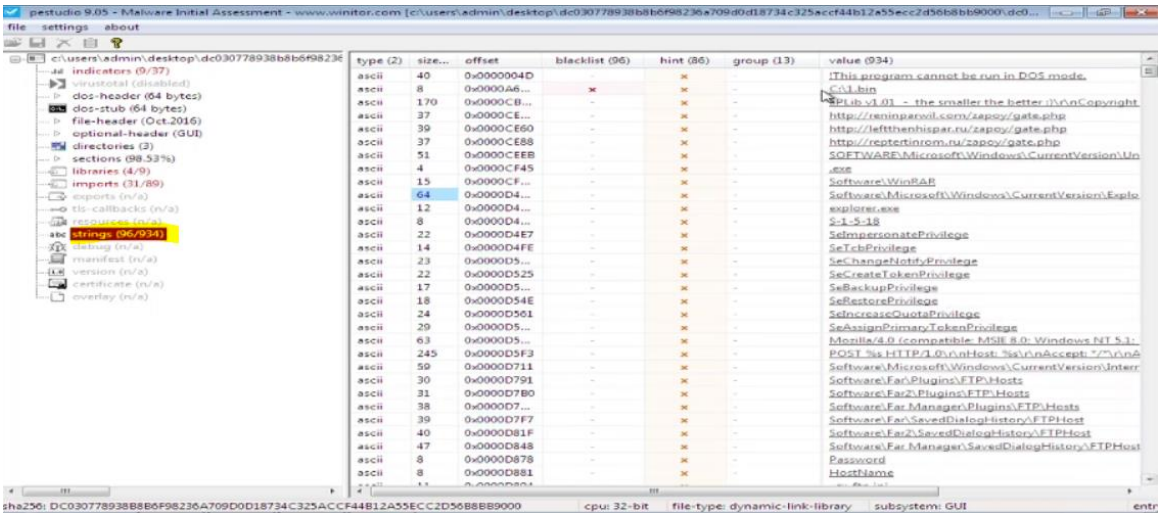
Checking the Hash value in Virus total

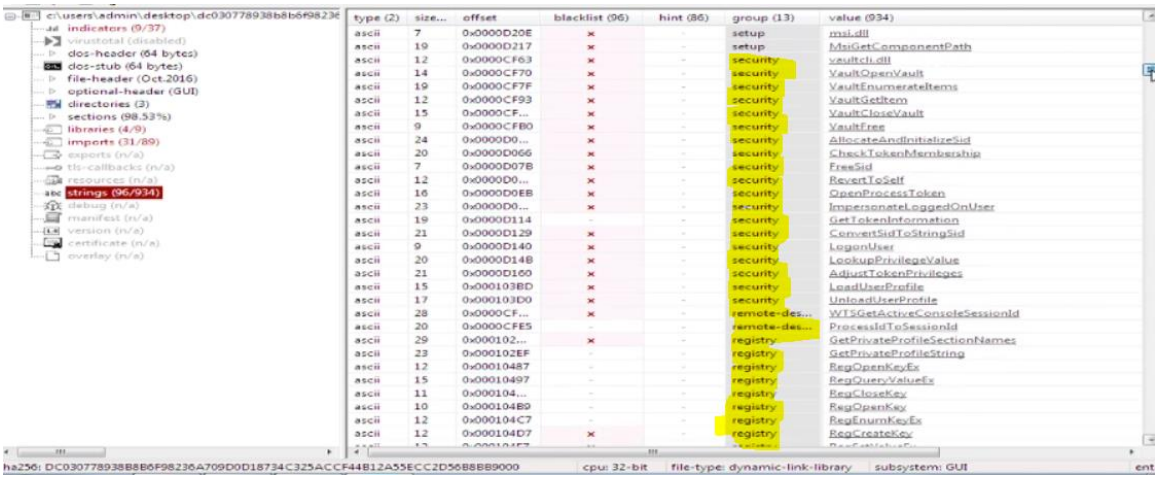




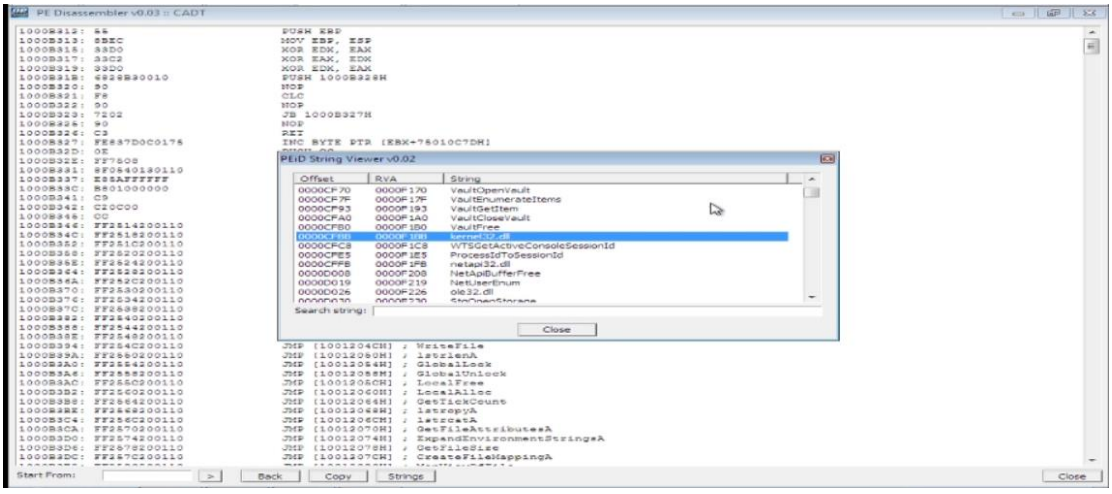
String Analysis

Drag and drop the malicious file into the PE studio for analyzing the strings. If we closely see we could see that some files of this application has been already blacklisted due its malicious behavior of the application. In this analysis, we could see what the groups that the application works on are and having control over it. This application took control over the registry, security, network, libraries, and files. These are the critical groups of the system and the attackers mainly targeting on these groups to gather information.

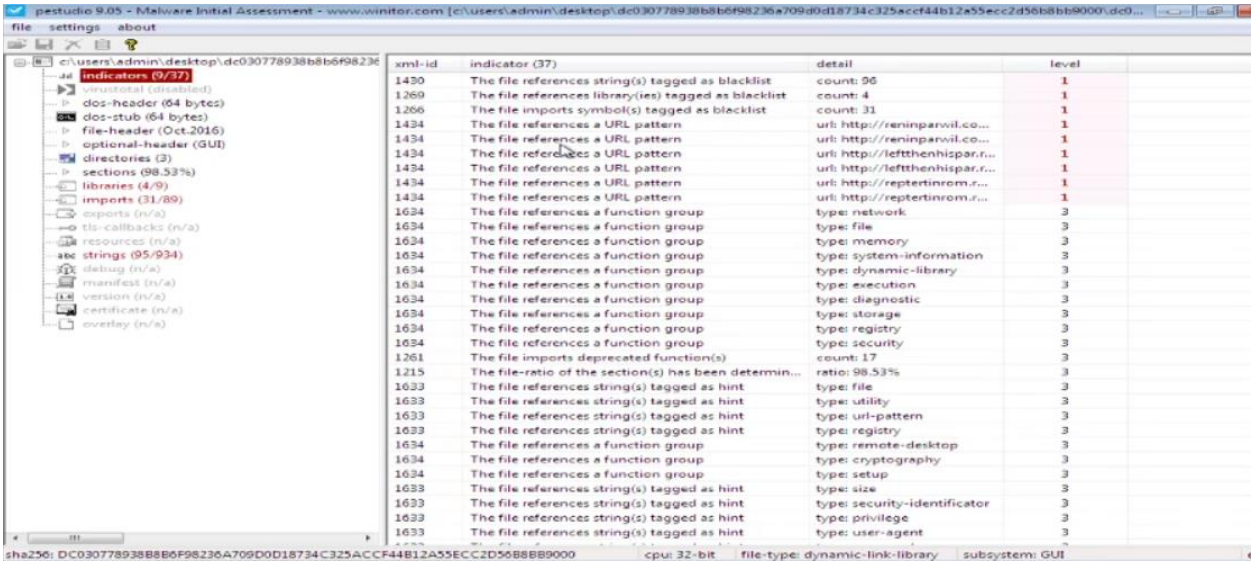




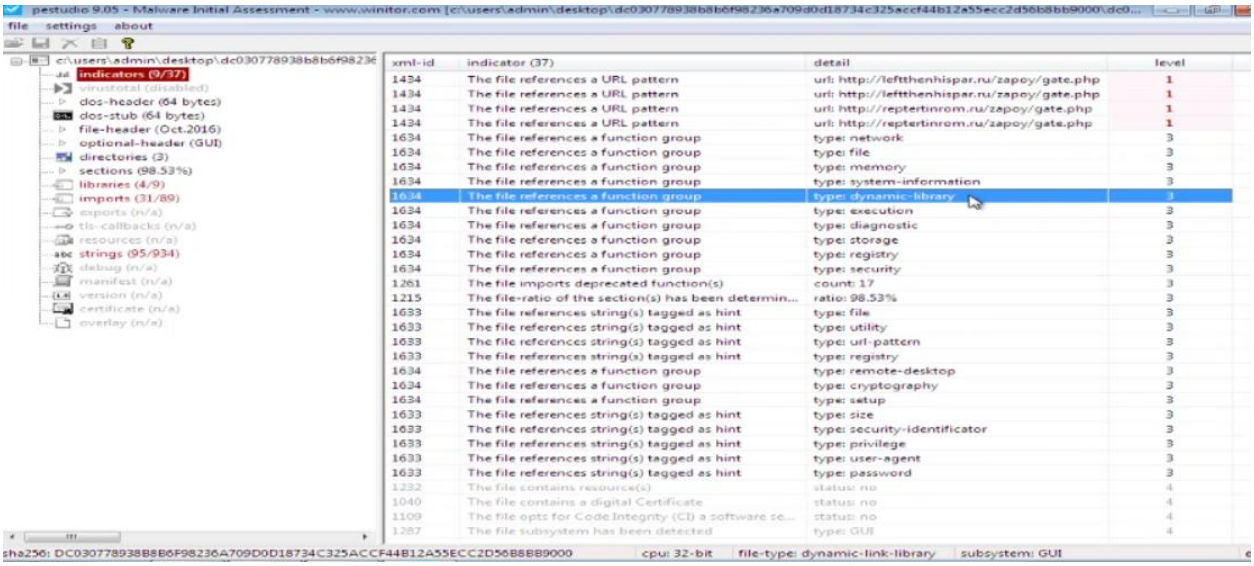
Analisis strings through PE ID application tool.

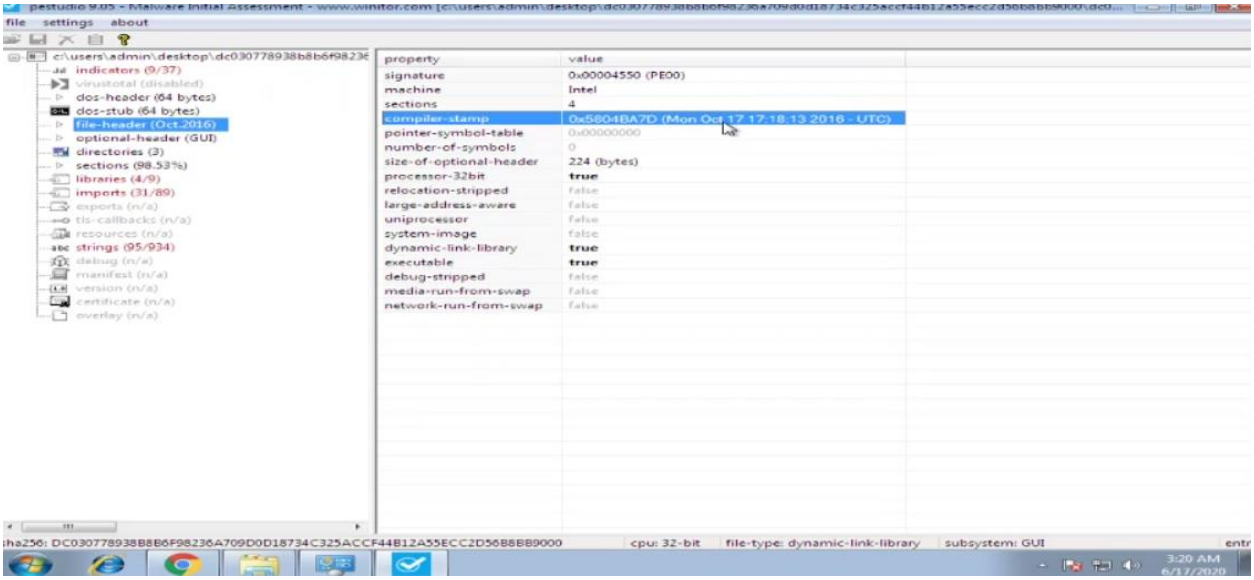


PE Header Analysis

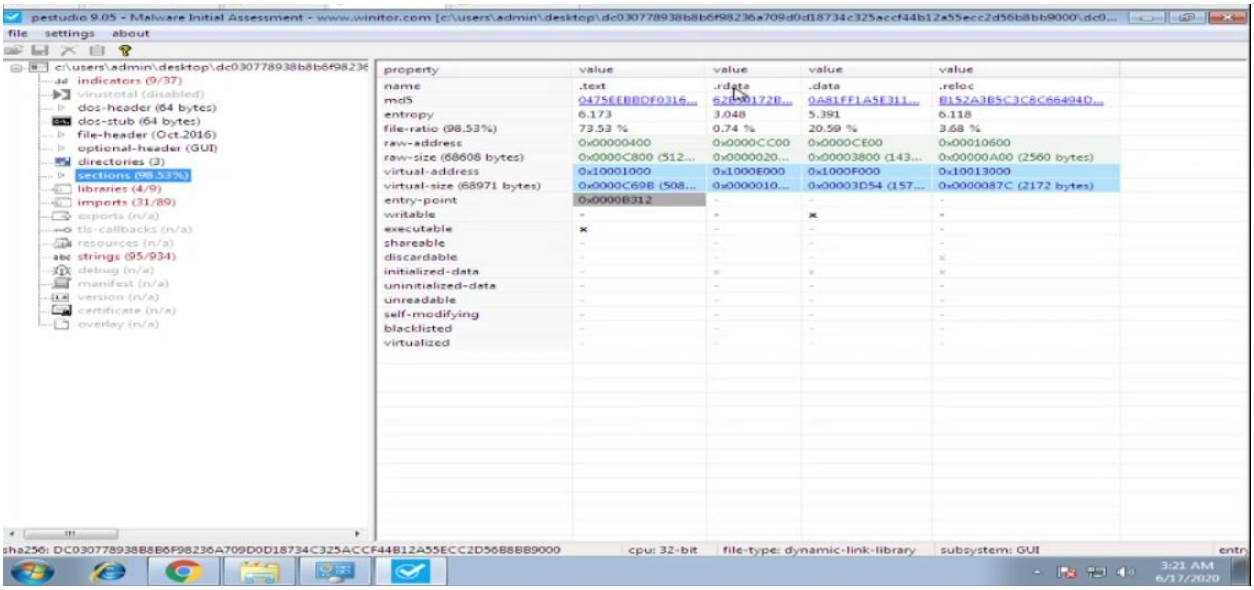


The most critical ones are blacklisted and marked as 1. The risk level has been marked from 1 to 10.if it is 1 its highly risky and if it is 10 it has less risk.

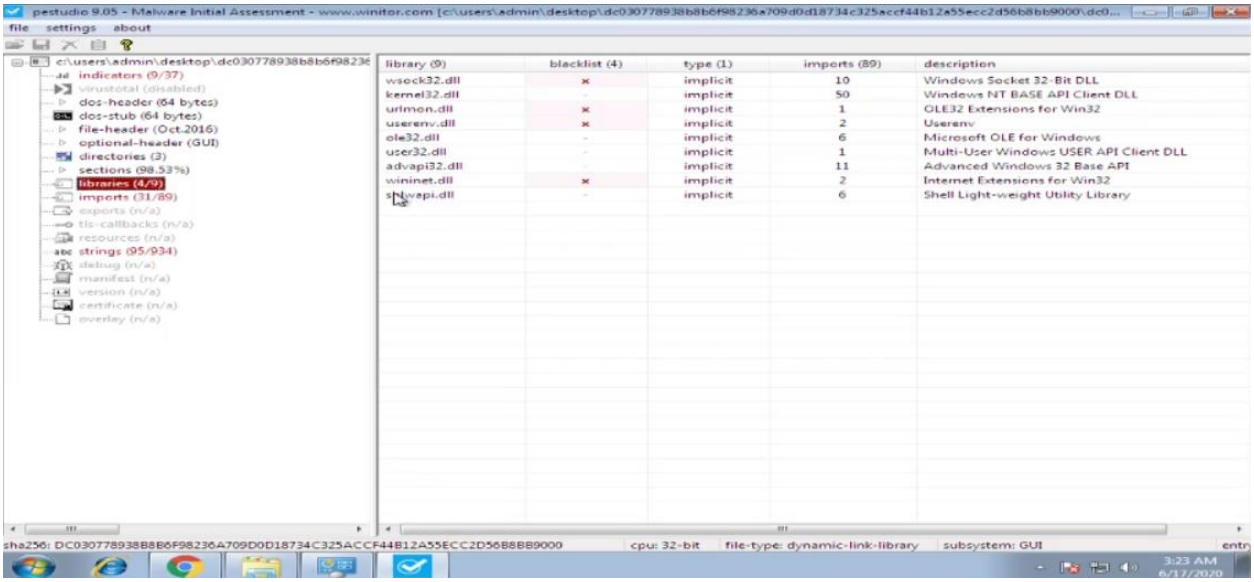




This shows when the malicious code first compiled with the date and time, its signatures, machine type, executable type, dynamic link library, etc.



This shows what are the actions/properties that the malicious have and it can perform. It malicious file has access to read file, write file, delete file etc. it also shows the MD5 hash value of each files.

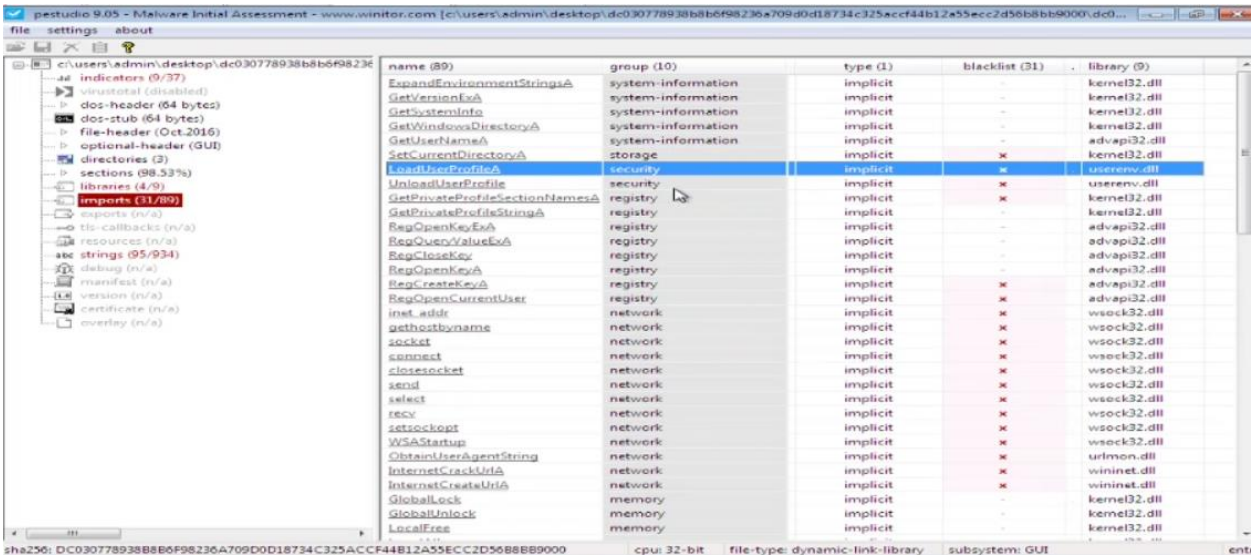


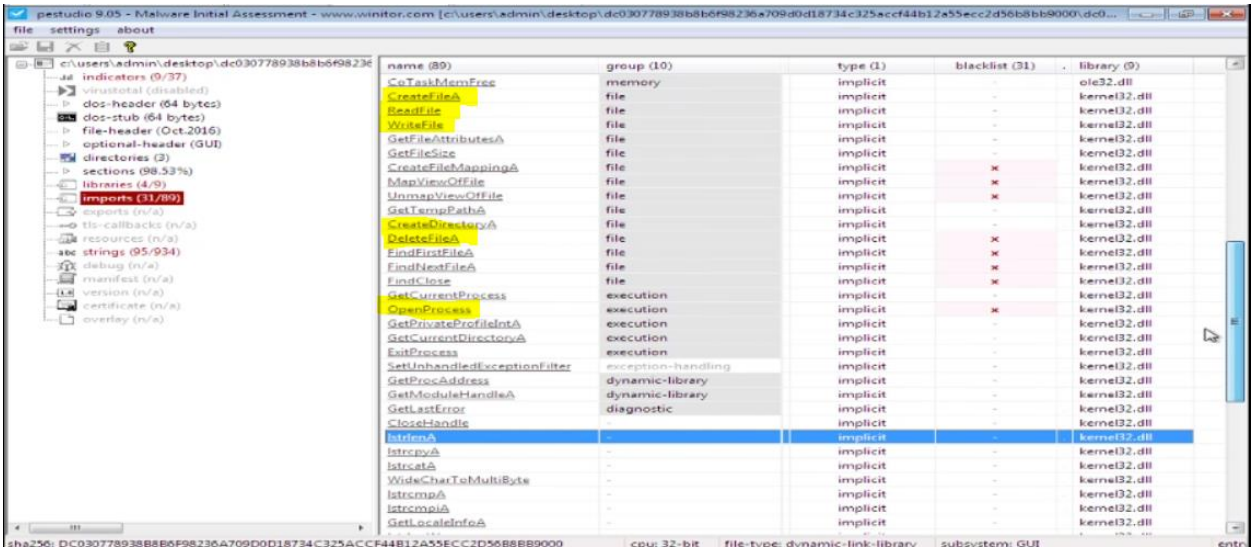
Kernal32.dll - all executable use to interact with system.

Advap32.dll – used to interact with registry.

Wininet.dll – uses internet connection to send data to Command and control server

Wsock32.dll - it creates a socket connection between the system and the command & control server, where the attacker can easily access to the system.

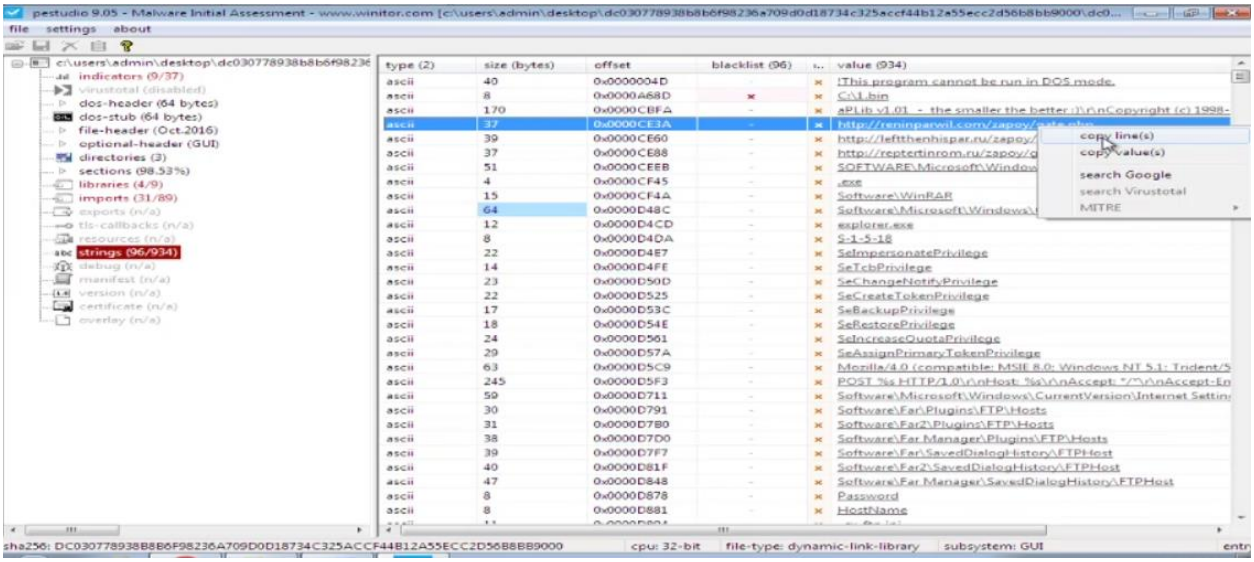




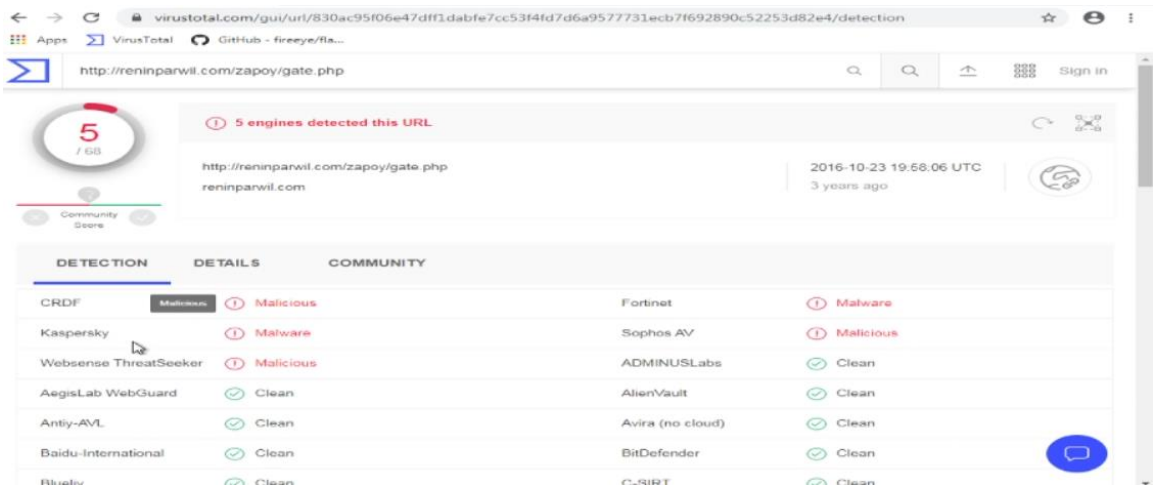
These are the major access needed by the attacker to get the information that stored in the system. Read, write, create, and delete file systems. It also can access the system process.

Checking the url with Virus toltal:

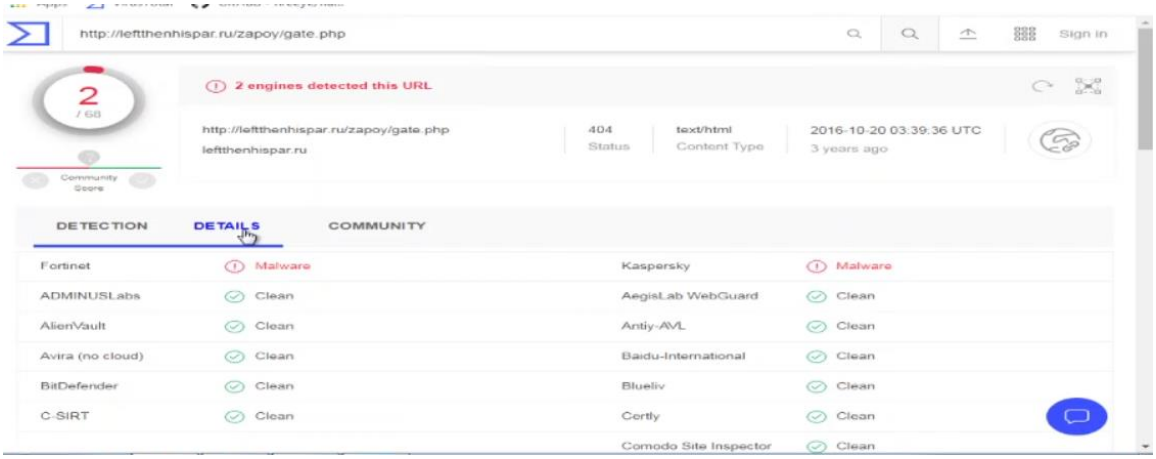
This tool is used to verify whether the url is legitimate one or attackers urls.

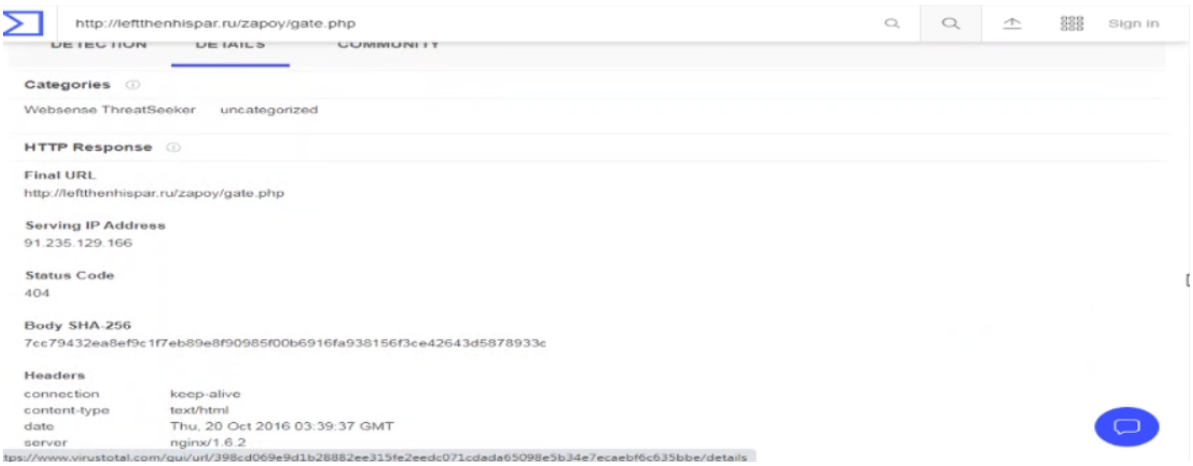


Copy and paste the url from PE studio and paste it in the virus total application.



While checking I found that it's a malicious url of the attacker where the attacker used this url to communicate with the system to send and receive data.





This also shows all information of that particular url.

Conclusion:

This report clearly shows how to perform a malware analysis in static method and it shows different tools to analyze the malware application. The attackers are always more intelligent and always tries to break the security of the system. Now days many malwares are not been identified based on modern analysis technique. So it always advisable to use the secured internet protection like antivirus and keep them up to date and have the system with proper patches and mitigate the malware attack by the attackers.

References

[1] [Online]. Available: https://www.virustotal.com/gui/. [Accessed Thursday June 2020].

[2] [Online]. Available: https://mh-nexus.de/en/hxd/. [Accessed 04 June 2020].

[3] [Online]. Available: https://www.winitor.com/. [Accessed 04 June 2020].

[4] [Online]. Available: https://exeinfo-pe.en.uptodown.com/. [Accessed Thursday June 2020].

[5] [Online]. Available: https://download.cnet.com/CFF-Explorer/3000-2383_4-10431156.html. [Accessed Thursday June 2020].

[6] [Online]. Available: https://www.aldeid.com/wiki/PEiD. [Accessed Thursday June 2020].

Note: The demonstration video of malware analysis is uploaded to drive and the link is shared in the Github. https://github.com/JanarthananKrishna/Malware-Analysis