

Digital Forensics

2021SM_CS_6419_FRE1A

Final Project: Digital Forensics Report

Prepared by:
Mohammadali Rahnama

Student number:
3709515



TABLE OF CONTENTS

TABLE OF CONTENTS.....	1
LIST OF FIGURES	1
LIST OF TABLES	1
INTRODUCTION	2
BACKGROUND INFORMATION ON THE INFECTION.....	2
HYPOTHESIS.....	4
ANALYSIS	4
NETWORK ANALYSIS	4
MEMORY ANALYSIS	9
DESTRUCTION TYPE.....	11

LIST OF FIGURES

Figure 1. Security warning on excel.	3
Figure 2. The EXE file used to recreate the infection.	3
Figure 3. Traffic from the victim's network filtered in Wireshark.....	5
Figure 4. HTTP request ending with .jpg returned a Windows EXE.	6
Figure 5. Exporting the file from the HTTP traffic in the pcap.	7
Figure 6. Saving the file returned from aromaterapiaclinicabrasil.com.br. ...	8
Figure 7. checking the file type using the "file" command.....	8
Figure 8. Alerts from the infection analysis using VirusTotal.	9
Figure 9. DumpIt command	9
Figure 10. Checking the registry using Volatility.....	10
Figure 11. The added registry information.	10
Figure 12. Alerts from the investigation of the new file using VirusTotal....	11

LIST OF TABLES

Table 1. Data sources and the tools that were used.	4
--	---

INTRODUCTION

Zusy malware is a banking Trojan that uses man-in-the-middle attacks to steal bank information. It is a spin-off of the well-known Zeus banking Trojan and is where Zusy takes its name. Zusy (also known as TinyBanker, Tinba, and Zegost) is a malicious piece of malware that is used to steal not only money but also personal information. Regardless of its name or size, it packs a powerful punch. It is critical to have a dependable endpoint anti-malware solution in place to protect your computer from infections like Zusy.

Zusy malware variants have been around for a long time. Zusy's early incarnations were in the form of adware. According to researchers, later versions of Zusy have been updated with a spyware component used to steal information from businesses.

The original version of Zusy works by injecting itself into Windows processes such as explorer.exe and winver.exe, so that when victims of the malware visit a financial services website, a bogus form appears, tricking them into submitting personal information. The newer Zusy variant, on the other hand, can infect a user's device simply by hovering over a hyperlink in an infected PowerPoint document. The user does not even need to click on the link for the malware to execute – a simple mouse hover over it will suffice. The PowerPoint attachment is frequently distributed via spam emails with subject lines such as "Order Confirmation" or "Purchase Order Number."

In addition, newer versions of Zusy can steal information by spying on webcams and turn your computer into a zombie machine controlled by the cybercriminal. Furthermore, when compared to other malware, Zusy malware is quite small, making it difficult to detect once it has infected a device. However, Zusy's small size has no bearing on the amount of damage it is capable of inflicting.

Office Macros are small pieces of code written in Visual Basic (VBA) that allow you to perform specific repetitive tasks. They are useful in and of themselves, but malware writers frequently exploit this functionality to introduce malware into your computer system.

A Macro virus is a virus that exploits Macros that run in Microsoft Office applications such as Word, PowerPoint, and Excel. Cybercriminals send you a macro-infested payload or a file that will later download a malicious script via email, with a subject line that entices or provokes you to open the document. When you open the document, a macro is launched to carry out whatever task the criminal has set for himself.

BACKGROUND INFORMATION ON THE INFECTION

A malicious Excel spreadsheet was responsible for this infection. A customer involved in a penetration test recently contacted us about a suspicious email message received by one of their employees. The attachment was a Microsoft Excel workbook with a Visual Basic (VBA) macro.

The user had to be enticed into opening it, just like in any other phishing campaign involving Microsoft Office files. In the subject line, the attackers used a classic phishing

lure: "Annual Employee Evaluation Report," so the employee opened the attachment to see how the evaluation went.

The spreadsheet's contents were immediately disappointing. There were no outcomes, no new salaries, no bonus information, and nothing else. The only thing that stood out was Microsoft's bright yellow warning: "SECURITY WARNING Macros have been disabled."

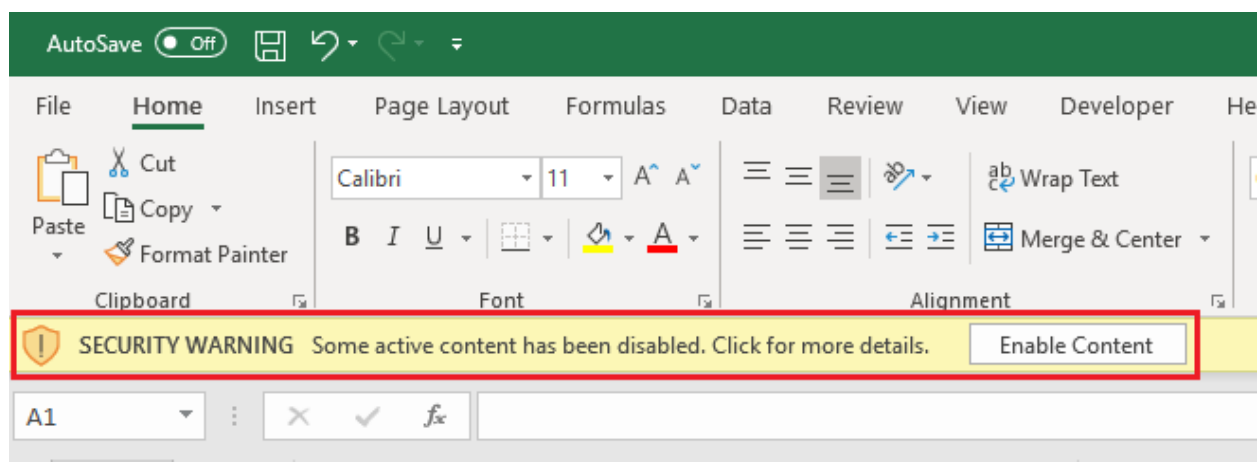


Figure 1. Security warning on excel.

Enabling macros on this spreadsheet caused the vulnerable host to download a malicious Windows executable (EXE) and save it as a file on the host where it was first run.

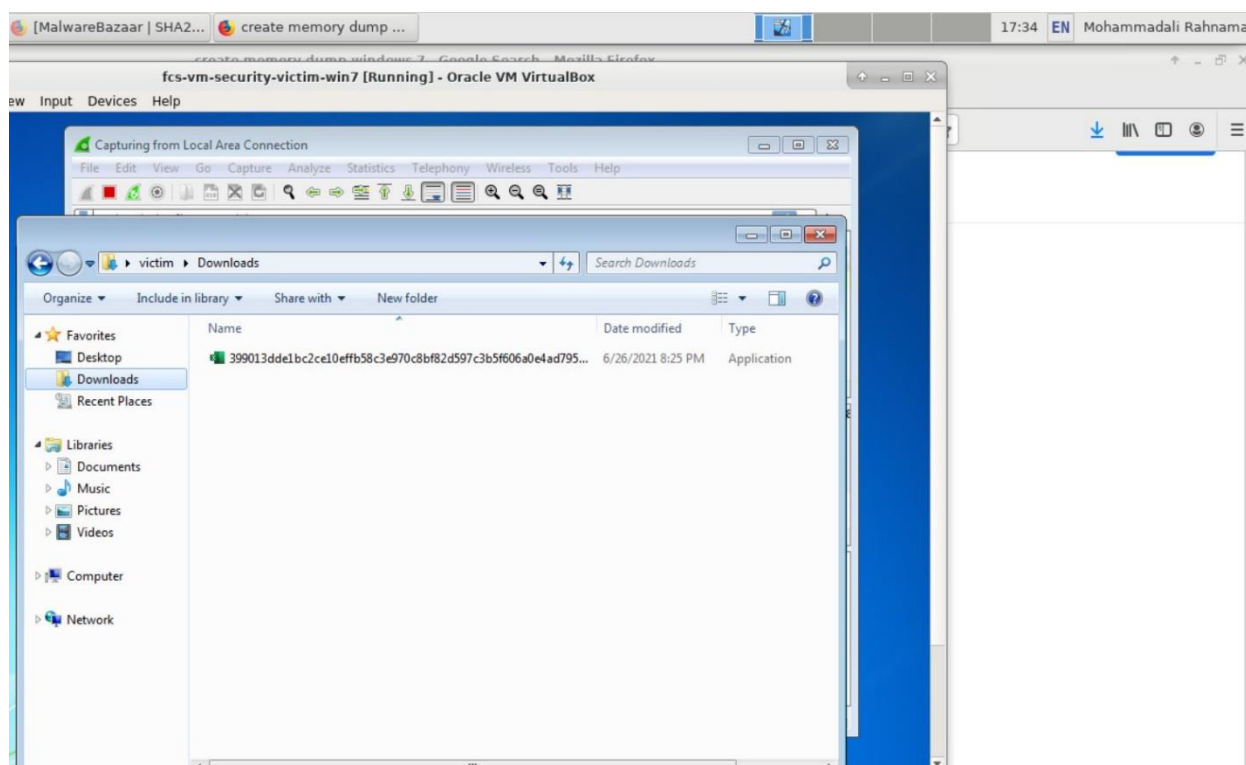


Figure 2. The EXE file used to recreate the infection.

In order to recreate the infection, we executed the malicious Windows executable (EXE) on our computer.

HYPOTHESIS

Based on the description of the case and interview that was conducted with the victim and the fact that a Microsoft Office Macro file was downloaded we can hypothesis that a malware form the Zusy malware family was used to infect the victim's computer, we will investigate the memory and the network traffic of the victim's computer to be able to prove our hypothesis.

ANALYSIS

Two data sources are considered in this case. First, the network traffic and second the memory dump.

Table 1. Data sources and the tools that were used.

Data Source	Tools used for acquisition	Tools used for analysis
Network traffic (Network.pcap)	Wireshark	Wireshark
Memory dump (WIN7VIC-20210627-012754.raw)	Dumplt	Volatility

Wireshark (optimized for web-based malware traffic) is our tool of choice for both capturing and reviewing the network traffic of the infection activity.

Dumplt is our tool of choice to capture a memory dump.

Volatility is our tool of choice to analyze the memory dump.

NETWORK ANALYSIS

After applying the web filter and analyzing all the HTTP requests we can see that a malicious request was made to the "aromaterapiaclicabrazil.com.br" on "162.214.51.208":

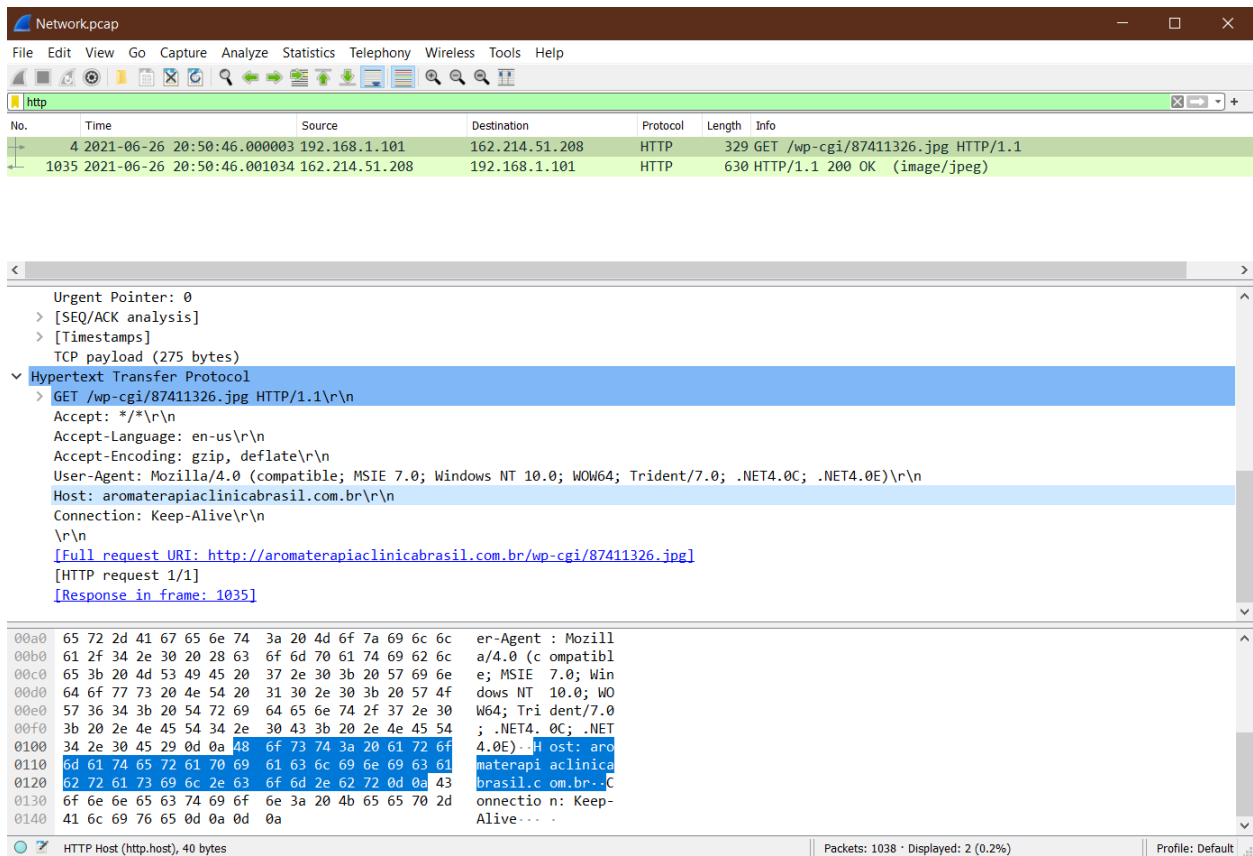


Figure 3. Traffic from the victim's network filtered in Wireshark.

This HTTP request ends with .jpg, but it returned an EXE. When we follow the TCP stream, we can confirm this is, in fact, an EXE.

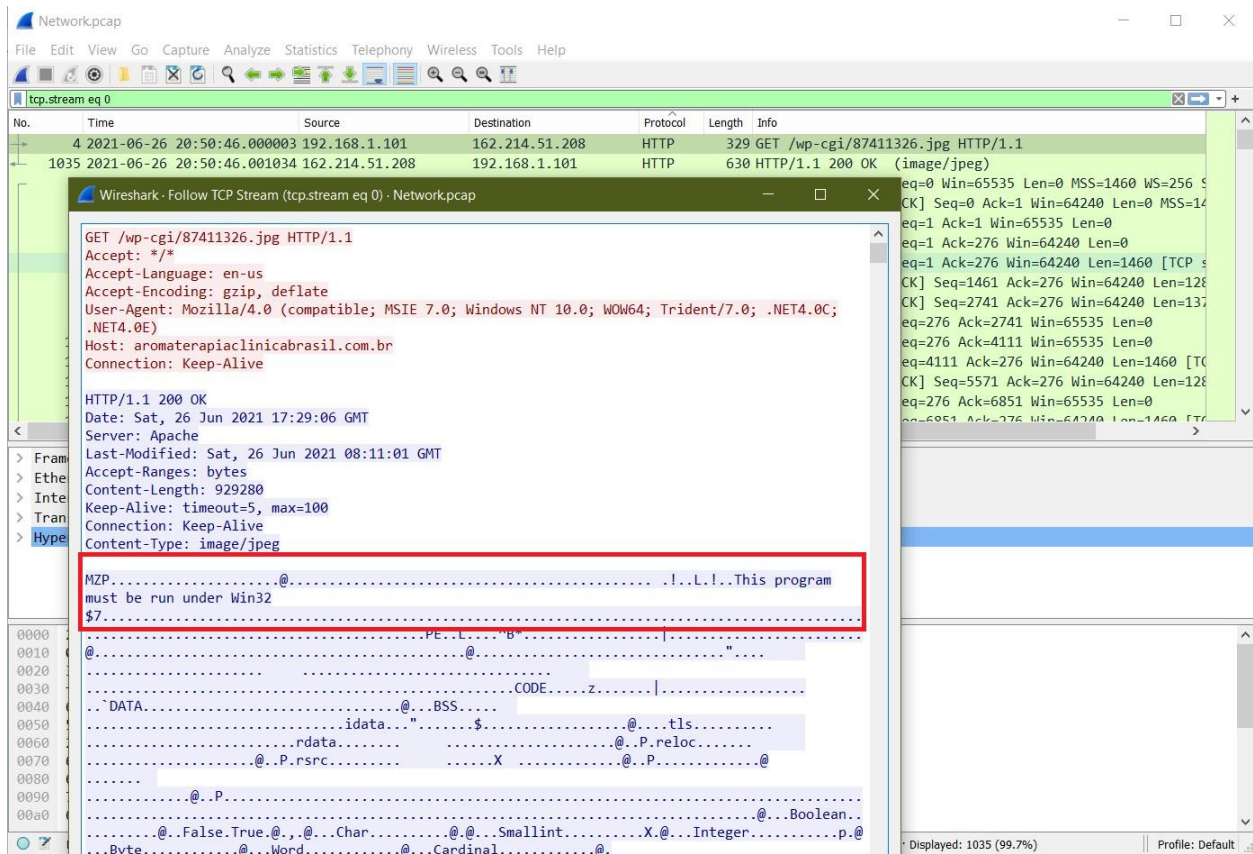


Figure 4. HTTP request ending with .jpg returned a Windows EXE.

Is this an EXE file or a DLL? In a TCP stream, they both look the same. The ASCII characters MZ appear as the first two bytes, and This programme must be run under Win32 and could be used by an EXE or a DLL. We can export the file from the pcap to

get more information about it.

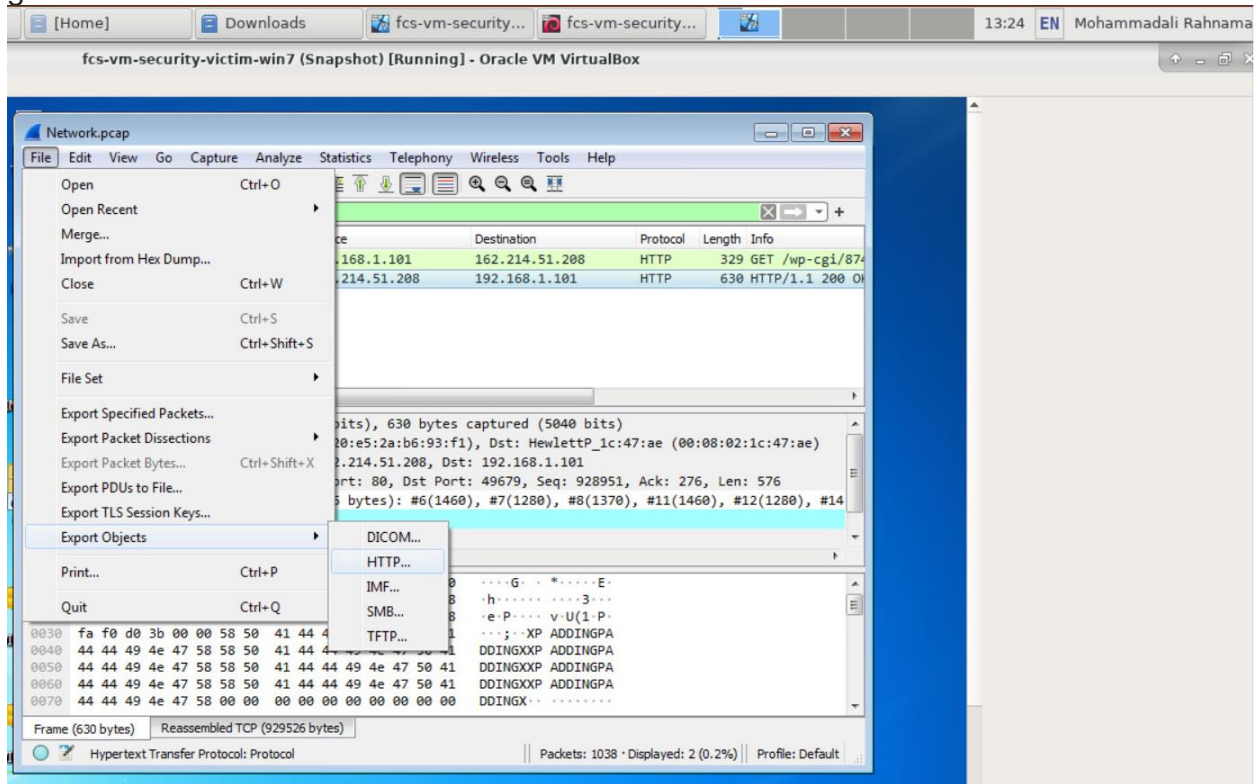


Figure 5. Exporting the file from the HTTP traffic in the pcap.

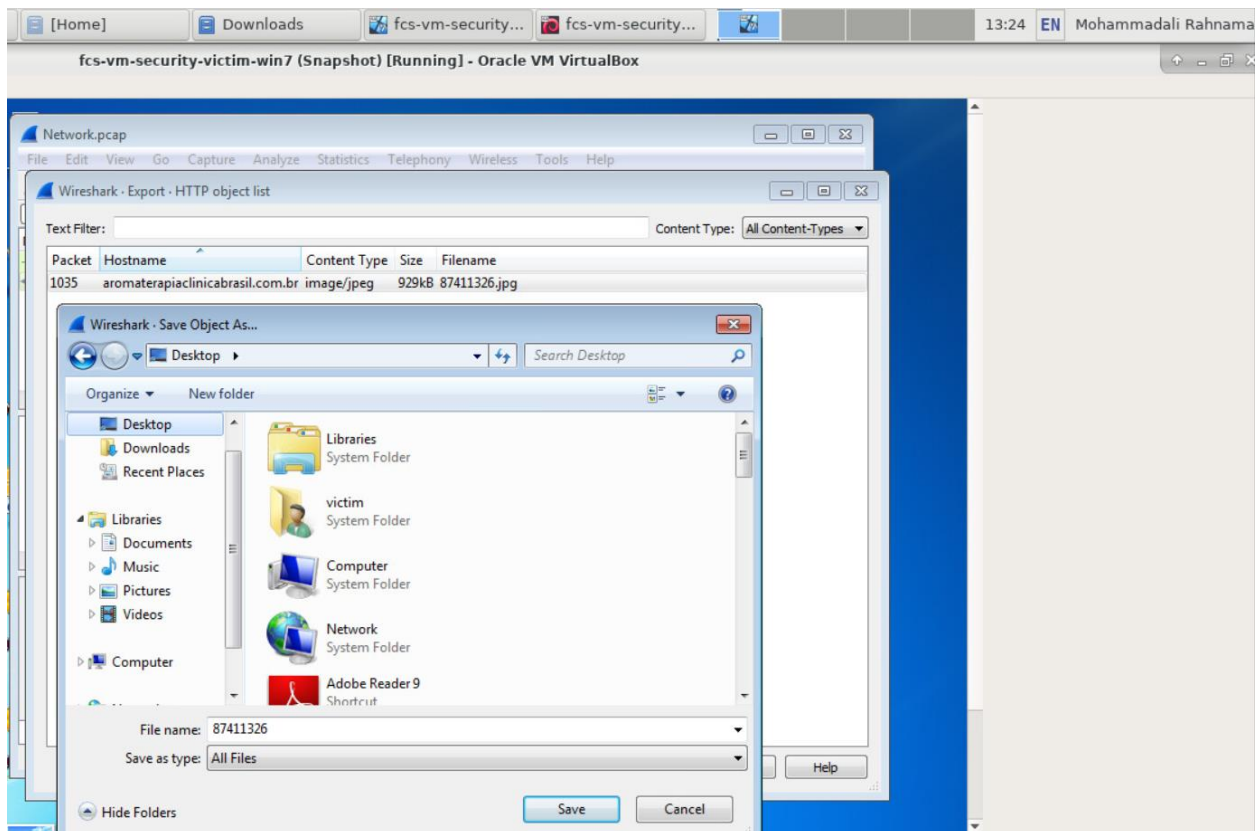


Figure 6. Saving the file returned from aromaterapiaclinikabrasil.com.br.

In a Linux environment, it is easy to confirm what type of file this is. We use the "file" command in a terminal window. We know that the Office document is a delivery mechanism. The actual malware is based on the EXE retrieved after enabling macros.

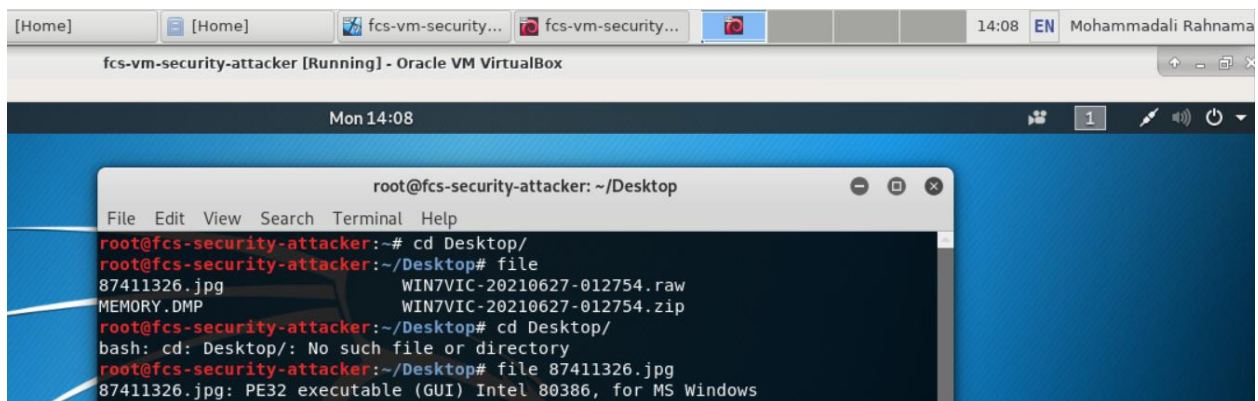


Figure 7. checking the file type using the "file" command.

In order to realize what is the malware family in this case we checked this file by uploading to the Virus Total website and we can see that it is in fact a malware. Different vendors often have their own names for the same type of malware. In this case, alerts from the post-infection traffic revealed that a malware form the Zusy family of malware caused this infection.

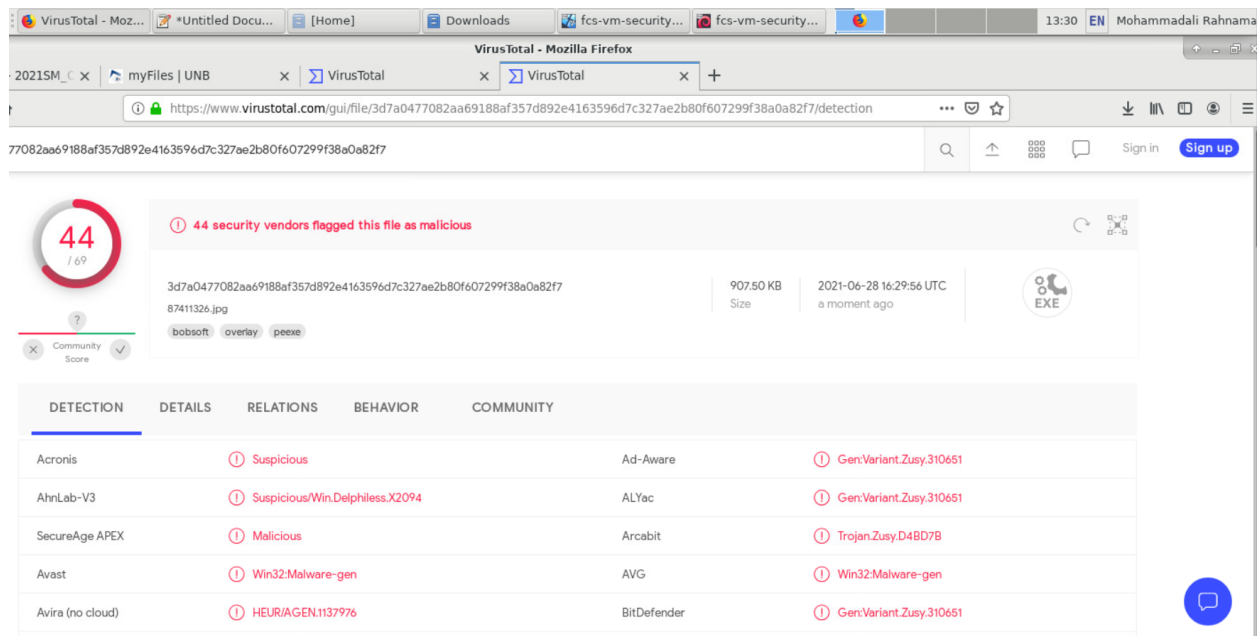


Figure 8. Alerts from the infection analysis using VirusTotal.

MEMORY ANALYSIS

In order to further investigate the case and remove the malware from the system we need to check if the malware was made persistent through an update to the Windows registry.

We first used the DumpIt tool to be able to acquire a full dump of the victim's memory.

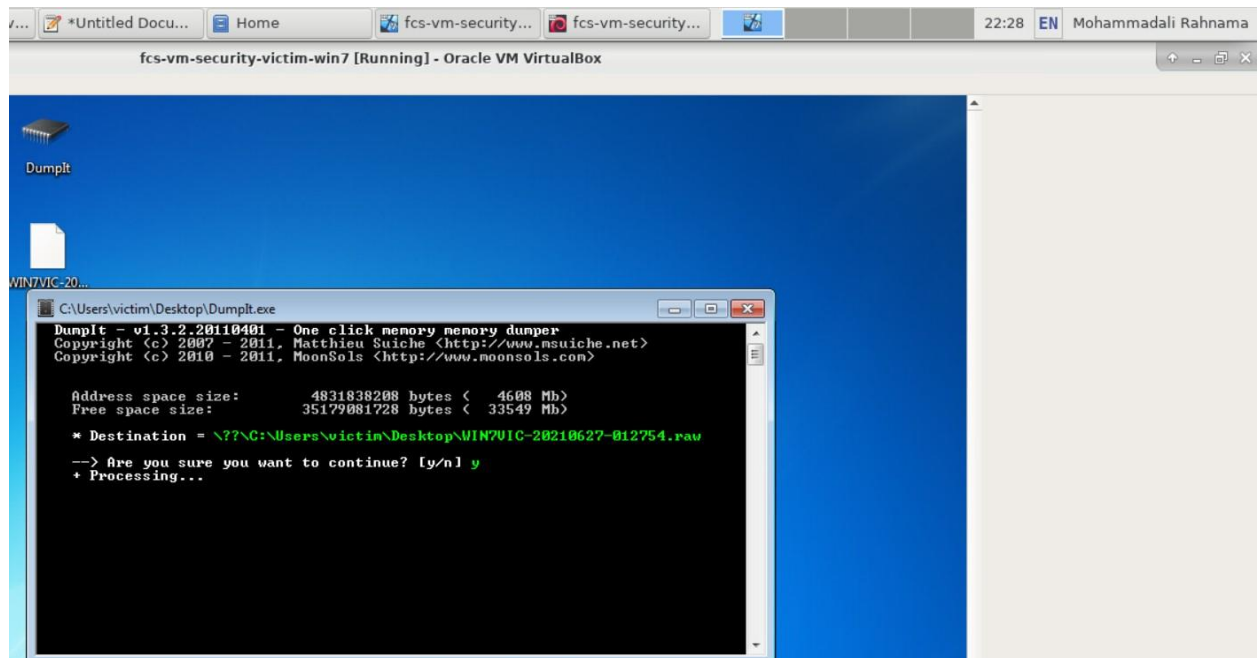
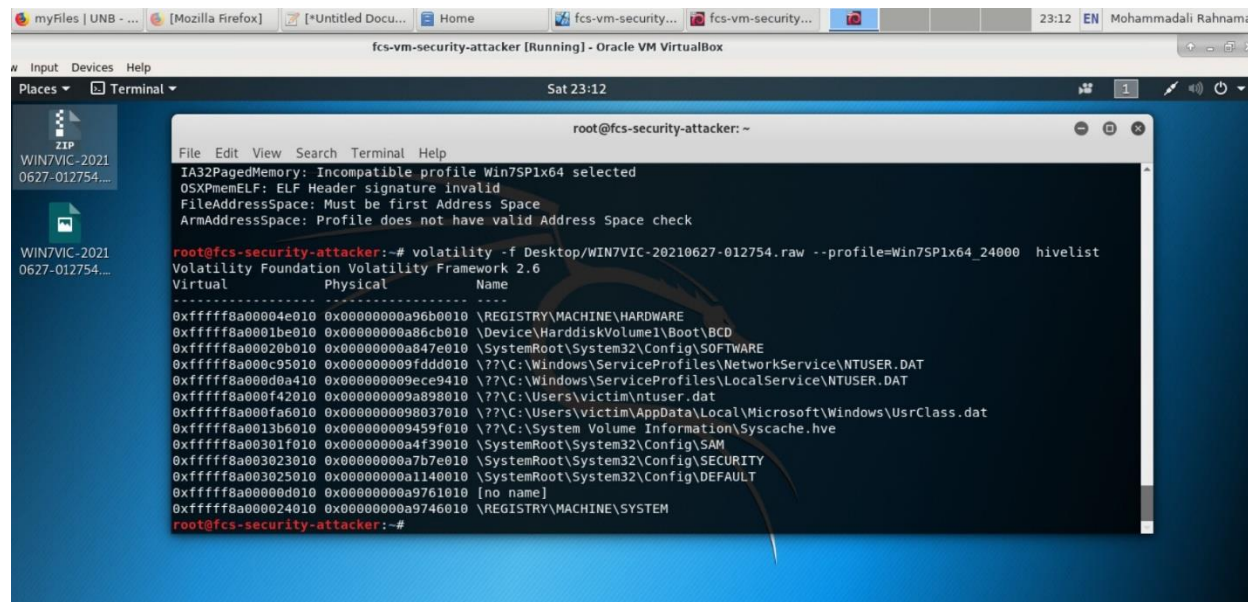


Figure 9. DumpIt command

As shown below, after analyzing the memory dump using Volatility and checking the registry, we can see that a new registry has been added to the system:



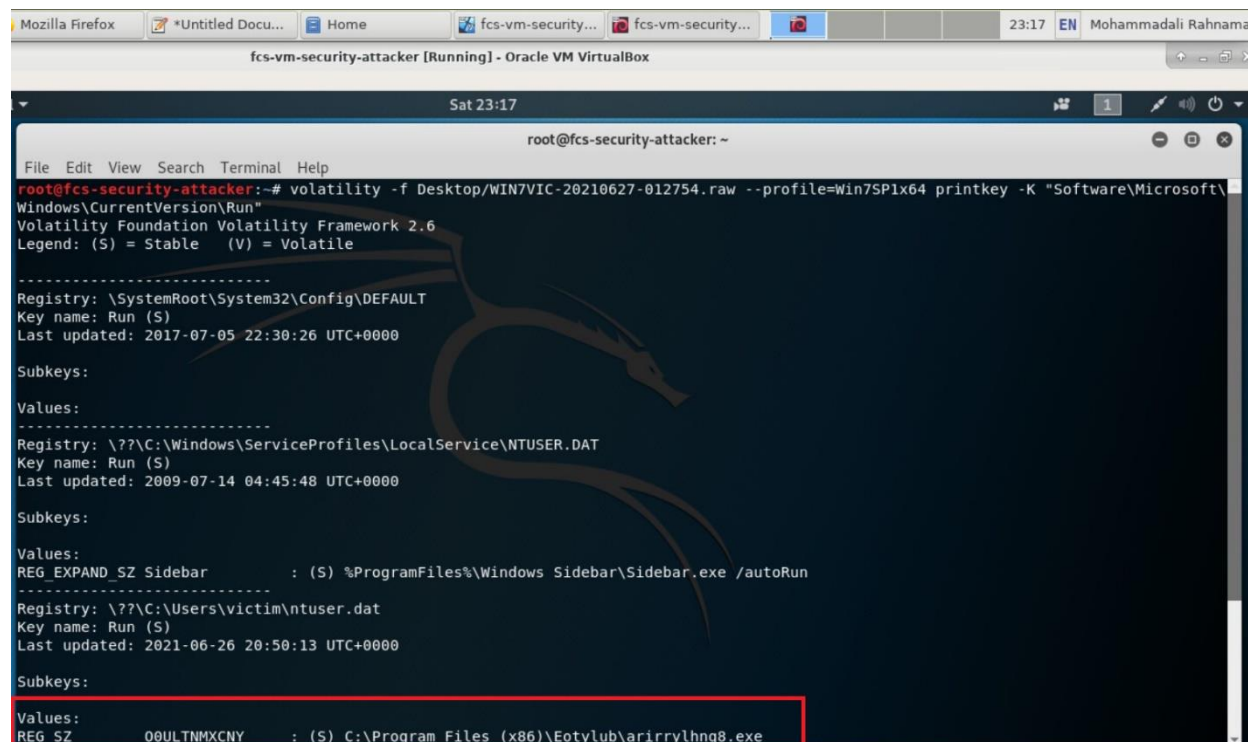
```

root@fcs-security-attacker: ~
File Edit View Search Terminal Help
IA32PagedMemory: Incompatible profile Win7SP1x64 selected
OSXPmemELF: ELF Header signature invalid
FileAddressSpace: Must be first Address Space
ArmAddressSpace: Profile does not have valid Address Space check

root@fcs-security-attacker:~# volatility -f Desktop\WIN7VIC-20210627-012754.raw --profile=Win7SP1x64_24000 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual      Physical      Name
-----
0xfffff8a00004e010 0x00000000a96b0010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0001be010 0x00000000a86cb010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a00020b010 0x00000000a847e010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a000c95010 0x000000009fdd0010 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a000d0a410 0x000000009ece9410 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a000f42010 0x000000009a898010 \??\C:\Users\Victim\ntuser.dat
0xfffff8a000fa6010 0x0000000098037010 \??\C:\Users\Victim\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a0013b6010 0x000000009459f010 \??\C:\System Volume Information\Syscache.hve
0xfffff8a00301f010 0x000000004f39010 \SystemRoot\System32\Config\SAM
0xfffff8a003023010 0x00000000a7b7e010 \SystemRoot\System32\Config\SECURITY
0xfffff8a003025010 0x00000000a1140010 \SystemRoot\System32\Config\DEFAULT
0xfffff8a0000d010 0x00000000a9761010 [no name]
0xfffff8a00024010 0x00000000a9746010 \REGISTRY\MACHINE\SYSTEM
root@fcs-security-attacker:~#

```

Figure 10. Checking the registry using Volatility.



```

root@fcs-security-attacker:~# volatility -f Desktop\WIN7VIC-20210627-012754.raw --profile=Win7SP1x64 printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

-----
Registry: \SystemRoot\System32\Config\DEFAULT
Key name: Run (S)
Last updated: 2017-07-05 22:30:26 UTC+0000

Subkeys:

Values:
-----
Registry: \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
Key name: Run (S)
Last updated: 2009-07-14 04:45:48 UTC+0000

Subkeys:

Values:
REG_EXPAND_SZ Sidebar : (S) %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun
-----
Registry: \??\C:\Users\Victim\ntuser.dat
Key name: Run (S)
Last updated: 2021-06-26 20:50:13 UTC+0000

Subkeys:

Values:
REG_SZ 00ULTNMXCNY : (S) C:\Program Files (x86)\Eotylub\arirrylhq8.exe

```

Figure 11. The added registry information.

This malware worked by deleting the malware from its original address and saving it in a randomly named directory under C:Program Files (x86) Eotylub with a random file

name. As shown above, the malware was made persistent by updating the Windows registry. We checked this new file again by uploading it to the Virus Total website, and we can see that it is indeed a malware from the Zusy family that caused this infection.

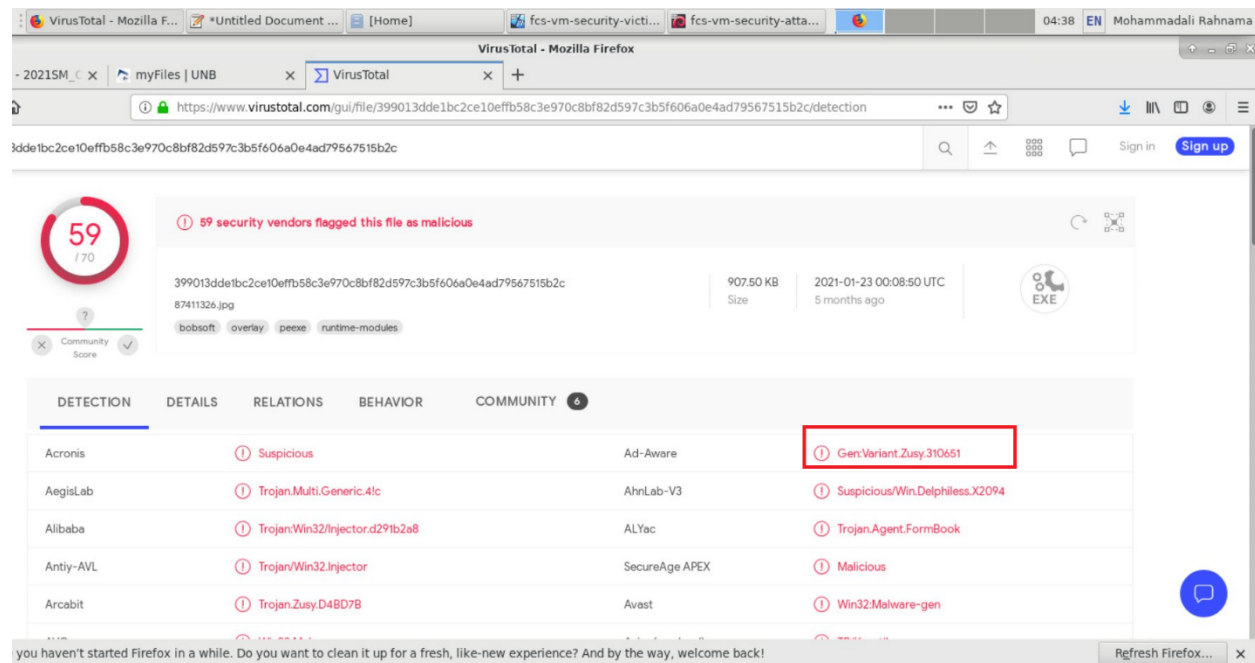


Figure 12. Alerts from the investigation of the new file using VirusTotal.

DESTRUCTION TYPE

The following was the sequence of events and destructions in the case:

- The victim receives a malicious Microsoft Office document (an Excel spreadsheet).
- The victim enables macros on a vulnerable Windows host.
- Through web-based traffic, a vulnerable Windows host retrieves a Windows EXE or DLL.
- The EXE or DLL file is saved to disc.
- The EXE or DLL infects the vulnerable Windows host and is made persistent.