

Malware Analysis Project

MSc in Cyber security

ADEOLA DANIEL AJIGINNI

Student ID: 19140002

School of Computing

National College of Ireland

Lecturer: Vikas Sahni

# TABLE OF CONTENTS

Executive summary …………………………………………. ………………..

1. Malware analysis lab setup ………………………… ………………….

Introduction ………………………………………………............

Setting up Virtual Machine ……………………………………….

VM Setup…………………………………….

Network Setup …………………………… …

Lab Testing……………………………. ……

Malware Analysis Tools…………………….

1. Executive Summary………………………………………. ……………

3. Identification ………………... …………………………………………

4. Analysis …………………………………… …………………………..

Code Execution Breakdown ………………..

5. Prevention and Mitigation……………………………………………….

6. Conclusion …...………………………………………………………….

References…………………………………………...

Appendix………………………….. ………………..

Section A: Lab Setup

1: Malware analysis lab setup

Introduction

Analysis of malware requires an isolated environment where we can run malicious files. To be able to see its network communication, what it changes on the (operating system, registry, files) and process creation. All this to be achieved and our environment easily reversed back to its known good state.

Setting up Virtual Machine

Virtual box was picked out of the variety of options available. I chose this because it's not required to restart the system when attempting to run other operating system on your computer, allows copy paste functions within its environment, allows you take snapshots and an excellent GUI console. The malware sample will be executed on the windows machine.

*Victim VM: Windows 10*

* Windows 10 operating system is used as it’s one of the most widely used OS [1].
* Configuration: Windows 10 (64bit) 2.5GB RAM,50GB disk.
* Snapshot is taken of the system at clean state.

*Ubuntu -18.04.1-desktop-amd64 VM*

* This is used to carry out external analysis
* Configuration: Ubuntu (64bit) 2GB RAM,50GB disk, Inetsim used to start DNS and Binding IP address
* Snapshot is taken of system at clean state.
* Virtual network simulation for victim VM used in monitoring network characteristics of the malware.

Network setup [2].

* First, we setup an isolated network by creating a static IP with a specified network adaptor on Ubuntu and Windows 10 VM.
* Isolate the virtual machine from the host machine with the use of a dedicated network.

Lab Testing

* Turn off Firewall and carry out system update before turning it off.
* Ping VM’s within the virtual environment to test connectivity.
* Check iNetsim status from victim’s browser.
* Ensure there isn’t connection between host and VM
* Confirm SSH server is up and running on victim’s Windows VM.

Malware analysis tools (Understanding the behavior of our malware)

Rootkit checkers

* Rootkit Burster: A free tool that scans hidden files, registry entries, system processes, drivers and identifies rootkits with a sensitive detection system [3].
* GMER: This is likened to a sniper trained particularly to find rootkits and will be used to seek a second opinion during analysis [4].

Static Analysis

* Exiftool: This is a command line application for reading, writing and editing meta information in a wide range of file formats [5].
* XXD: This command allows you create a hex dump and carry out the reverse [6].
* JD-GUI: Is a graphical tool that shows java source codes of "class" files. [7]
* Hachoir-subfile: This is used to find subfiles in any binary stream [8].
* Pcregrep: This tool is used for full description of syntax and semantics supported by PCRE [9].

Network analysis

* Wireshark: This is a widely used network protocol analyzer [10].
* TCP dump: A command line utility that allows you to capture and analyze network traffic going through a computer [11].

Memory Forensics

* Volatility: Is an open source memory forensics framework for malware analysis [12].
* TSK: This is a library of Unix and windows utilities and aids the forensic analysis of a computer system.
* Test disk(photorec): This is a free powerful data recovery software [13].

Anti-virus

* Clam V: This is a free antivirus software used to detect malwares.

Packer detection

* PEID: Detects packets, Cryptor and compilers for PE files [14].

Debuggers

* OllyDbg: This debugger is used to carry out binary code analysis and is essential when source code isn't available [15].

Disassemblers and Decompiler

* IDA Pro: This will be used to translate machine language into assembly language.
* Ghidra: It is a software reverse engineering framework used to analyze malware codes.

Change analysis

* Process Explorer: This is a system monitor and task manager application.

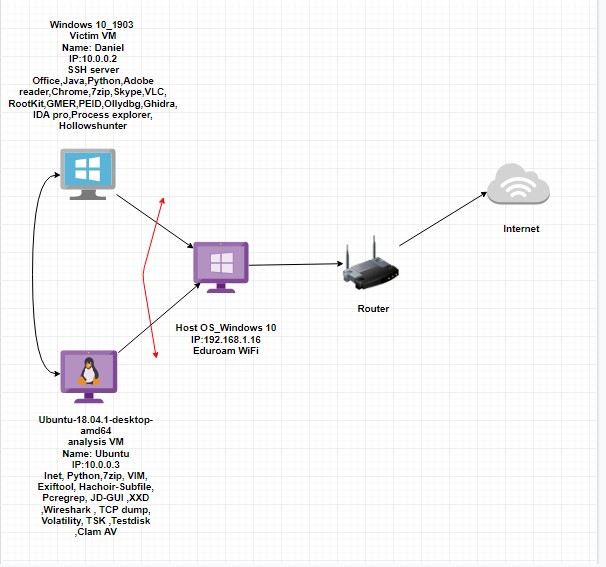
Dynamic Analysis

* Hollows-hunter: This is used to scan all running processes. It recognizes and dumps malicious inputs [16].

Online Tools

* Joe Sandbox, VirusTotal, ThreatMiner.

Sandbox setup



# 2: Executive summary

This malware analysis report is the result of extensive analytic effort on a malicious Trojan variant used by an attacker called Emotet.

Objectives:

* Detailed description of the Trojan Emotet
* In depth analysis with aid of multiple tools to study its malicious behavior
* Suggesting response actions and recommend mitigations

Key findings:

* Information theft
* Rootkit characteristics
* File corruption
* Propagation
* Routine Download

## 3: Malware analysis research topic: Emotet

What is Emotet?

Emotet first documented by Joie Salvio who was in Trend Micro in 2014 was discovered to be a simple banking trojan malware used to steal financial data using various social engineering techniques in form of emails [17]. Over the years it has added a lot of modularity as it has evolved into a botnet, could spread over networks the way worms do.

How it works?

The compromise may arrive as a malicious script, macro-enabled document files or malicious link. Uses C&C servers to receive updates, the same way operating systems update our PC. The first version of Emotet involved corrupting the registry of a targeted machine, this is effectively used to evade detection as any infiltrated data is encrypted then stored in the registry which adds an entry to the startup directory in the windows registry. In turn it grants the attacker persistence on the infected machine due to the difficulty of discovering signs of a compromise/breach. Over the past years Emotet has been discovered to distribute AZORuit, icedID, ZeuS Panda and TrickBot [18].

**The following Antivirus detected Amotet:**

72 ANTIVIRUSES SCANNED BUT ONLY 62 DETECTED EMOTET

|  |  |
| --- | --- |
| Avast | Win32:BankerX-gen [Trj] |
| Arcabit | Trojan.Autoruns.GenericS.D1DED1EA |
| SecureAge APEX | Malicious |
| Antiy-AVL | Trojan[Banker]/Win32.Emotet |
| ALYac | Trojan.Autoruns.GenericKDS.31379946 |
| Alibaba | Trojan:Win32/Emotet.21b382ef |
| AhnLab-V3 | Malware/Win32.Trojanspy.C2880140 |

Table 1: Antivirus detection scan results [19].

Known File Names [19]:

* 0f92b8a6eaed33bd0f339e47953ad3b\_fTAEcKRAdax.ExE
* 10f92b8a6eaed33bd0f339e47953ad3b
* hpmrh7x0J.exe
* PEivBrRZ.exe
* echodep.exe
* sddlpass.exe

Imported File [19]:

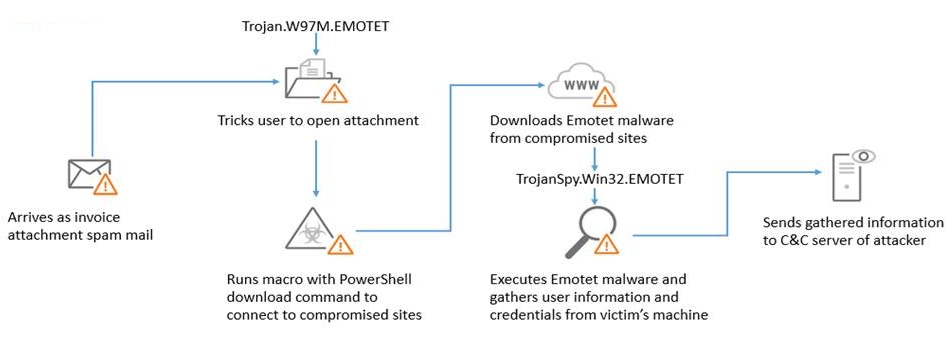
* ESENT.dll
* KERNEL32.dll
* USER32.dll

|  |  |
| --- | --- |
| **MD5** | **SHA 256** |
| 957942f47d28b3623339ea3c3adf20c9 | 368f9cb089d206a8b61251f0c85eeda97ee08a56b33be8579246e964d3af6169 |
| fd2570358cfb650efc03ee9eb6559ede | 0b0e16c38a3d5a85566e67b1d9a7e720e4dee27e163b06099d3d7dfa5dbed9ee |
| c47e82d49d3bc7f0156a4535bb85981a | 652988945185cf5d604d9b48de66288d82d8ed0acdd134398e90d002d2d9fc72 |
| 246598d6f047ca896c55fa385d4dbb5f | f64ccc0582bc7c66af8b40049e485e8e241335261ec95ace909293ba50b2e4a3 |
|  |  |

Table 2: Known MD5 and SHA 256 files [19].

# **4.Analysis**

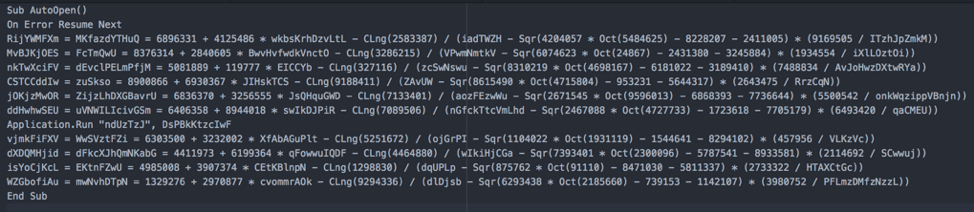
Infection trail [20].

[](https://esupport.trendmicro.com/media/14194578/emotet-infection-chain.jpg)

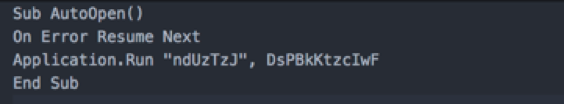
|  |  |
| --- | --- |
| File Name | PAYMENT 225EWF.doc |
| SHA 256 | 707fedfeadbfa4248cfc6711b5a0b98e1684cd37a6e0544e9b7bde4b86096963 |
| MD5 | e8e468710c0a4f0906305c435a761902 |
| File Type | Microsoft word |
| Size | 416.50 KB (426496 bytes) |

Table 3: Sample Analyzed [21].

This version of Emotet ,uses PowerShell to execute final commands .Usually a word document, that prompts the target to enable macros. Once enabled the VBA runs in the background and the payload gets downloaded on the victims machine [21].



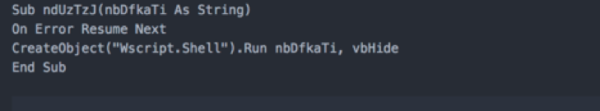
* We will now discard all the useless code that has been included in the sub to complicate analysis.



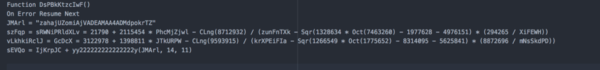
* We can see at the end of the sub procedure, the Application. Run method is called:



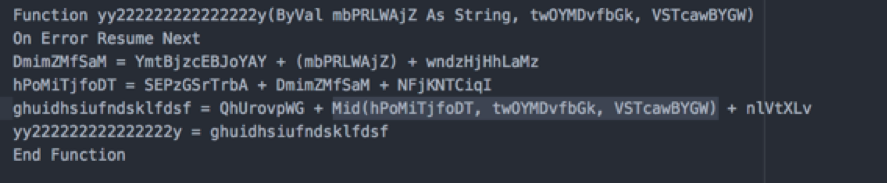
* To execute the method shown above, we can see that the method calls on a sub and a function.



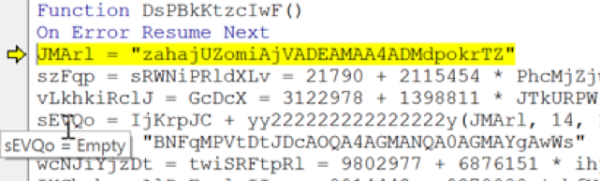
* vbHide will be assigned a value of 0, which means the window is hidden and focus is passed to the hidden window.



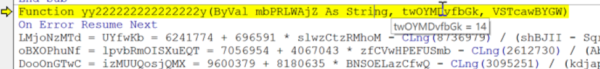
* Notable things can be seen in the code snippet above,



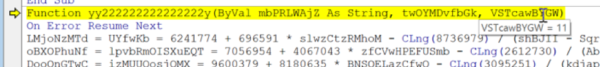
* The function calls on the Mid function, which processes the data for further use. After understanding how the code flow has been structured, we look at how the program executes.



* We can see that the value “14” has been passed on to the function variable “twOYMDvfbGk”:



* Here, we observe the value “11” has been passed on to the function variable “VSTcawBYGW”:



* Finally, the text string will be passed on to the variable mbPRLWAjZ, which was empty previoisly



* Data gets processed using the Mid function, seen above.

Let’s see how that unfolds:

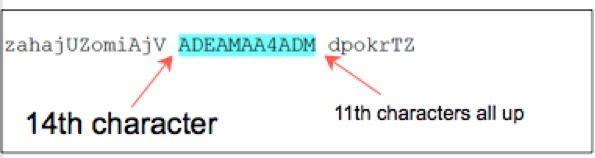
mbPRLWAjZ= zahajUZomiAjVADEAMAA4ADMdpokrTZ

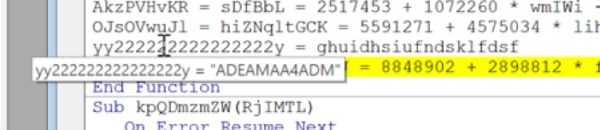
twOYMDvfbGk= 14

VSTcawBYGW= 11

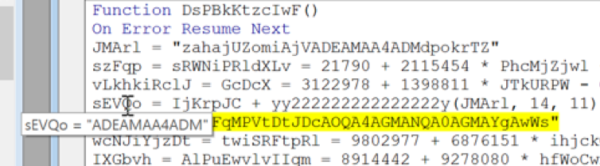
Mid(hPoMiTjfoDT, twOYMDvfbGk, VSTcawBYGW):

Mid(“zahajUZomiAjVADEAMAA4ADMdpokrTZ”, 14, 11)

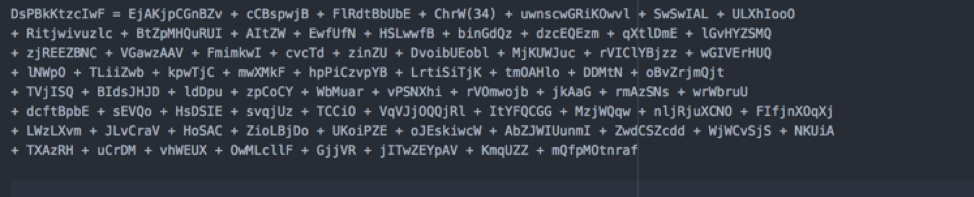




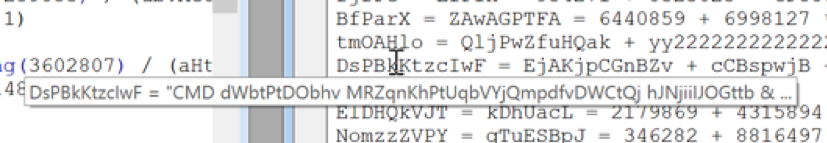
* It gets passed back to the calling variable:



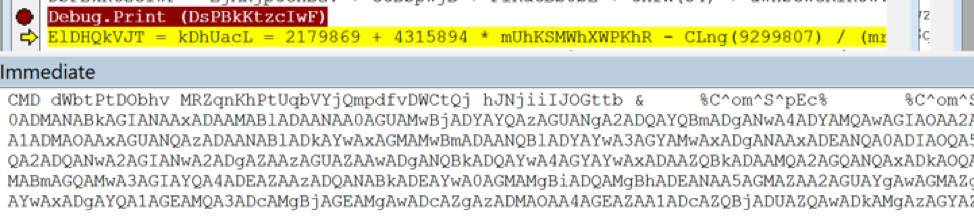
* The variable sEVQo is assigned to **ADEAMAA4AD.**That was a look at one of many variables used in this function.



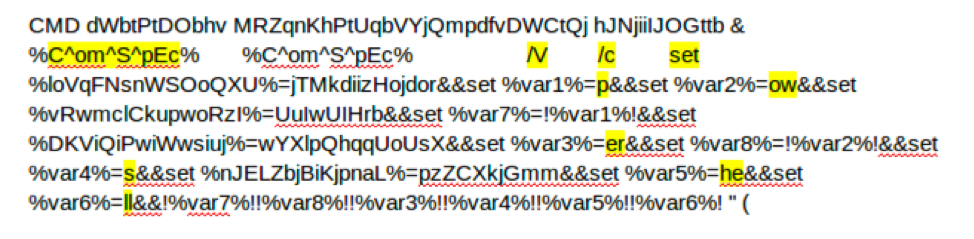
* The value assigned to DsPBkKtzcIwF after the above line of code is executed is the command that will be executed by sub ndUzTzJ:



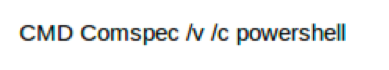
* Now we print the output to screen with the help of MsgBox to have a look or to the immediate window using Debug.Print for a more in-depth result.



* This part of the command above invokes PowerShell:



* Which should translate the above highlighted text to [21]



# **5: Prevention and Mitigation**

* Block email attachments that can't be scanned by antivirus software
* proper employee training
* Filters placed at the email gateway and the creation of a whitelist or blacklist on IP addresses.
* Principles of least privilege should be strictly followed
* Segregate and Segmenting networks
* Have a security awareness program as Emotet mostly targets end users via mails

**6: Conclusions**

Emotet a quite complex and well executed malware, with high level of code obfuscation and encryption used to hide its code. Its impact has been greatly felt by compromised system security, with backdoor capabilities that can execute malicious commands. Violation of user privacy gathers and steals users’ credentials of various applications. Continuous analysis of code variations and other changes in the future as witnessed in recent Emotet variants will not pose any major threat challenge to analysts. The more you know, the more you can mitigate against the form of attacks.

**References**

[1] C. Software, S. Help and C. Hope, "What is the most popular operating system?", *Computerhope.com*, 2020. [Online]. Available: <https://www.computerhope.com/issues/ch001777.htm>

[2] VirtualBox Network Settings: All You Need to Know", *Official NAKIVO Blog*, 2020. [Online]. Available: <https://www.nakivo.com/blog/virtualbox-network-setting-guide/>

[3]RootkitBuster | Trend Micro", *Trend Micro*, 2020. [Online]. Available: <https://www.trendmicro.com/en_ie/forHome/products/free-tools/rootkitbuster.html>

[4] T. Bradley, "Detect and remove rootkits with GMER", *PCWorld*, 2020. [Online]. Available: <https://www.pcworld.com/article/2023718/detect-and-remove-rootkits-with-gmer.html>

[5] "ExifTool by Phil Harvey", *Exiftool.org*, 2020. [Online]. Available: <https://exiftool.org/>

[6] H. Arora, "Linux xxd Command Tutorial for Beginners (with Examples)", *HowtoForge*, 2020. [Online]. Available: <https://www.howtoforge.com/linux-xxd-command/>

[8] "hachoir-subfile program — Hachoir 3.1.2 documentation", *Hachoir.readthedocs.io*, 2020. [Online]. Available: <https://hachoir.readthedocs.io/en/latest/subfile.html>

[9] "pcregrep(1): grep with Perl-compatible regex - Linux man page", *Linux.die.net*, 2020. [Online]. Available: <https://linux.die.net/man/1/pcregrep>

[10]"Wireshark · Go Deep.", *Wireshark.org*, 2020. [Online]. Available: https://www.wireshark.org/. [Accessed: 01- Mar- 2020].

[11]"An introduction to using tcpdump at the Linux command line", *Opensource.com*, 2020. [Online]. Available: <https://opensource.com/article/18/10/introduction-tcpdump>

[12]"Volatility (memory forensics)", *En.wikipedia.org*, 2020. [Online]. Available: <https://en.wikipedia.org/wiki/Volatility_(memory_forensics>

[13]"TestDisk - CGSecurity", *CGSecurity*, 2020. [Online]. Available: <https://www.cgsecurity.org/wiki/TestDisk>

[14]"PEiD - aldeid", *Aldeid.com*, 2020. [Online]. Available: <https://www.aldeid.com/wiki/PEiD>

[15]"OllyDbg", *En.wikipedia.org*, 2020. [Online]. Available: <https://en.wikipedia.org/wiki/OllyDbg>

[16]"hasherezade/hollows\_hunter", *GitHub*, 2020. [Online]. Available: <https://github.com/hasherezade/hollows_hunter>

[17]"New Emotet Report Details Threats From One of the World’s Most Successful Malware Operations", *Fortinet Blog*, 2020. [Online]. Available: <https://www.fortinet.com/blog/threat-research/emotet-playbook-banking-trojan.html>

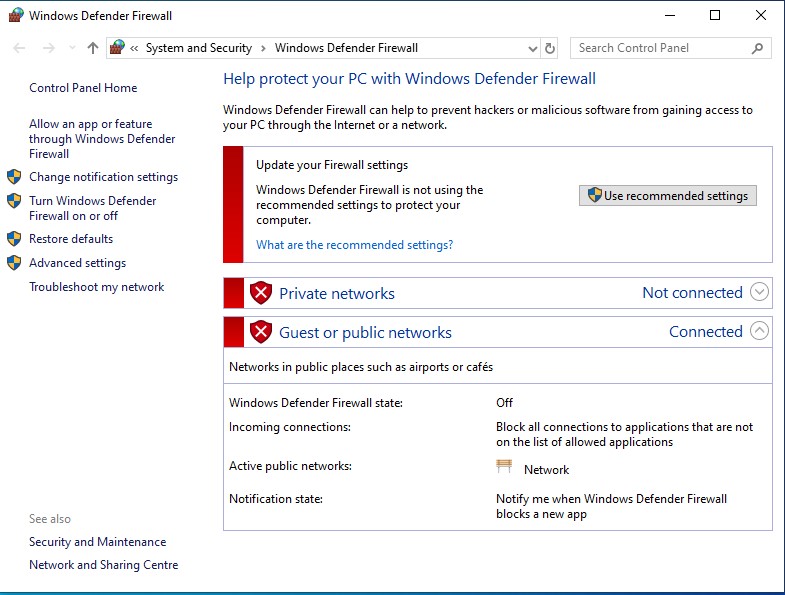
[18]A. Shulmin, "The Banking Trojan Emotet: Detailed Analysis", *Securelist.com*, 2020. [Online]. Available: <https://securelist.com/the-banking-trojan-emotet-detailed-analysis/69560/>

[19]"VirusTotal", *Virustotal.com*, 2020. [Online]. Available: <https://www.virustotal.com/gui/file/7d42a037f8c824724e3525e40f09ae6b3f0eaca4278e4f0b95bb5ca50f008f7b/detection>

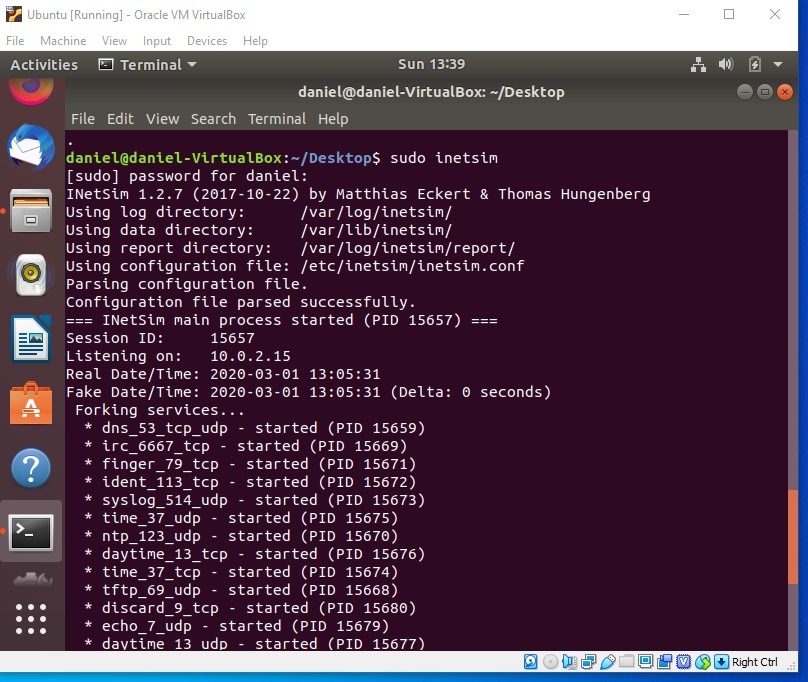
[20]"Resurgence of EMOTET Malware", *Success.trendmicro.com*, 2020. [Online]. Available: <https://success.trendmicro.com/solution/1118391-malware-awareness-emotet-resurgence>

[21]V. Thakur, "Malware analysis: decoding Emotet, part 1 - Malwarebytes Labs", *Malwarebytes Labs*, 2020. [Online]. Available: <https://blog.malwarebytes.com/threat-analysis/2018/05/malware-analysis-decoding-emotet-part-1/>

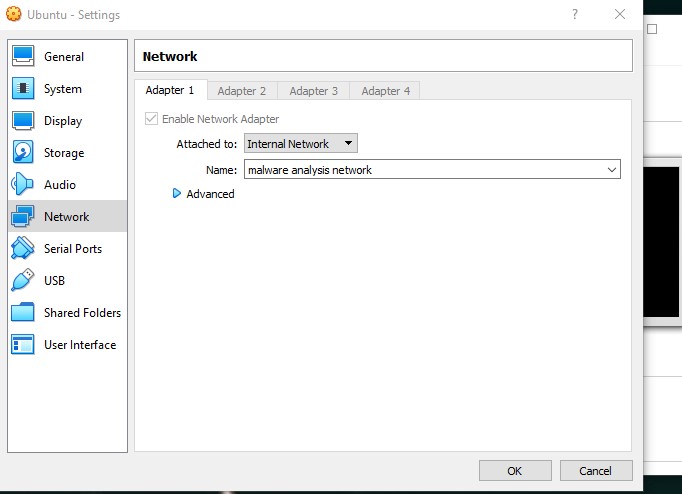
##### **Appendix**



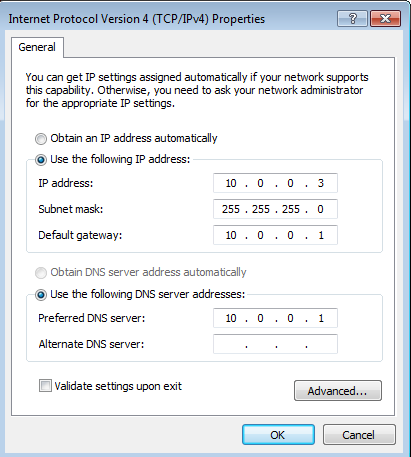
Firewall, auto update is turned off



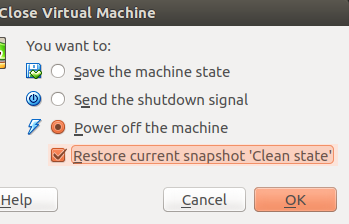
Inetsim server started up



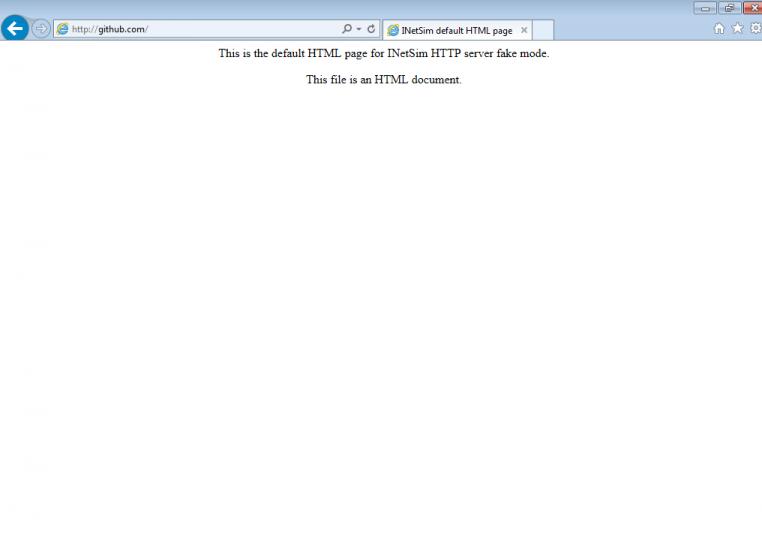
Network Adapter settings cutting off connection with host machine



Victim Windows VM network configuration



Snapshots taken of VM’s at clean state



Windows accessing our Inetsim fake server successfully