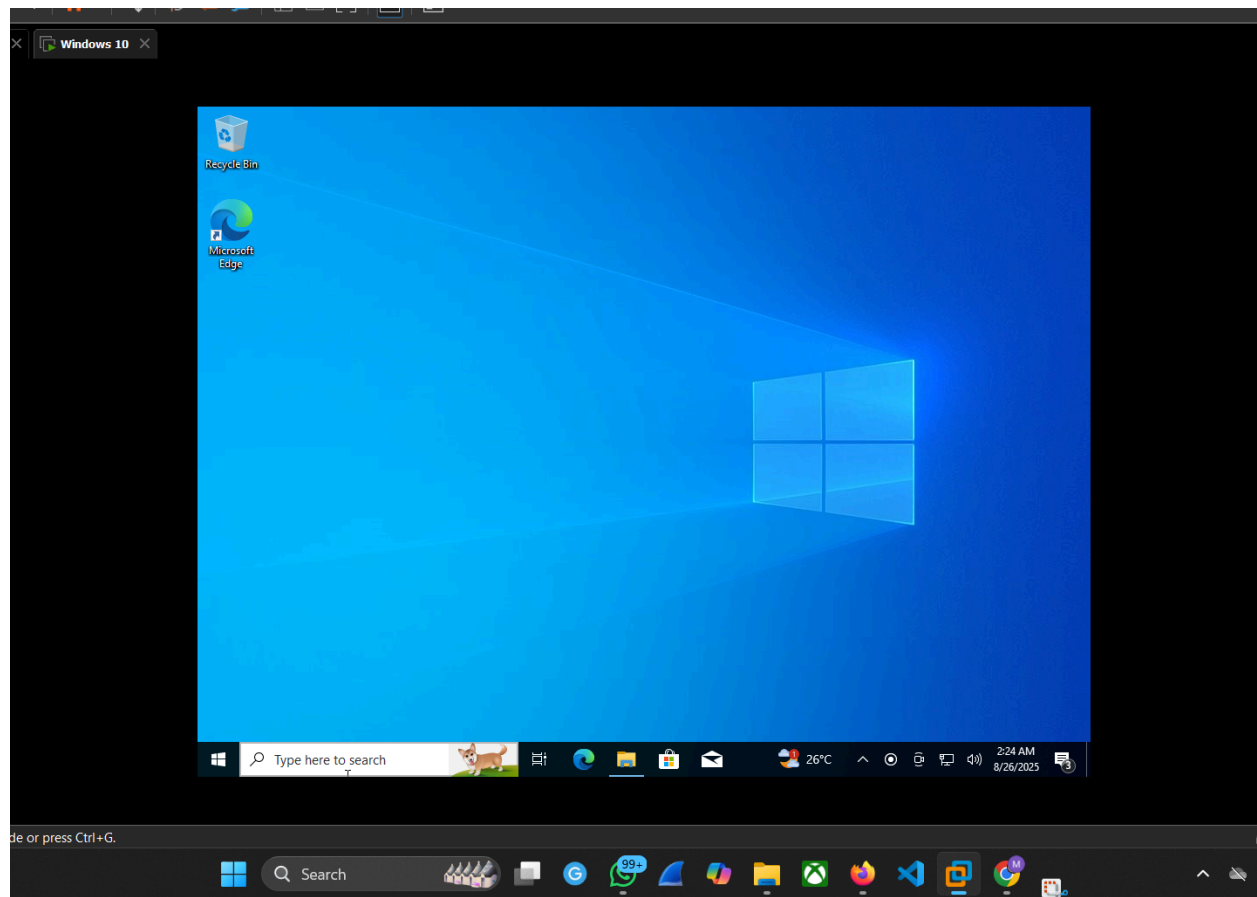
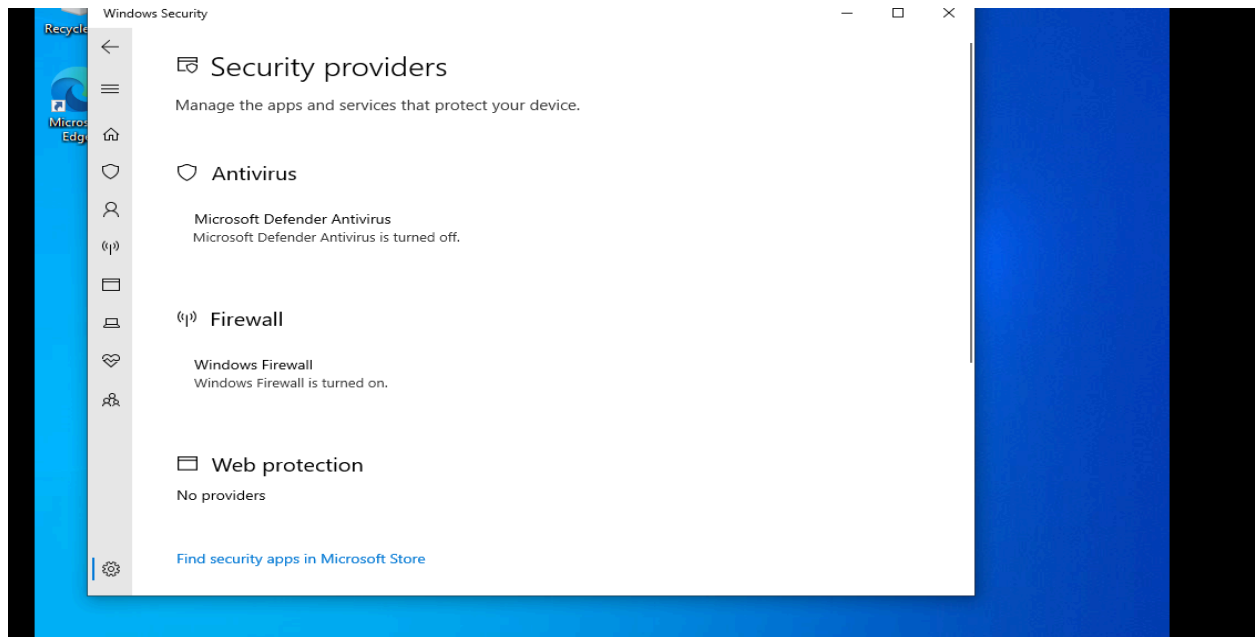


1.Installing windows 10 pro in VMware to set up flare vm	2
2.0 Installing flare VM and setup	4
2.1 Taking two malware file samples :	5
3.0 Fingerprinting the malware :	7
3.1 Using Virustotal	7
4.0 Strings	8
5.0 Packing	9
6.0 Pestudio	10

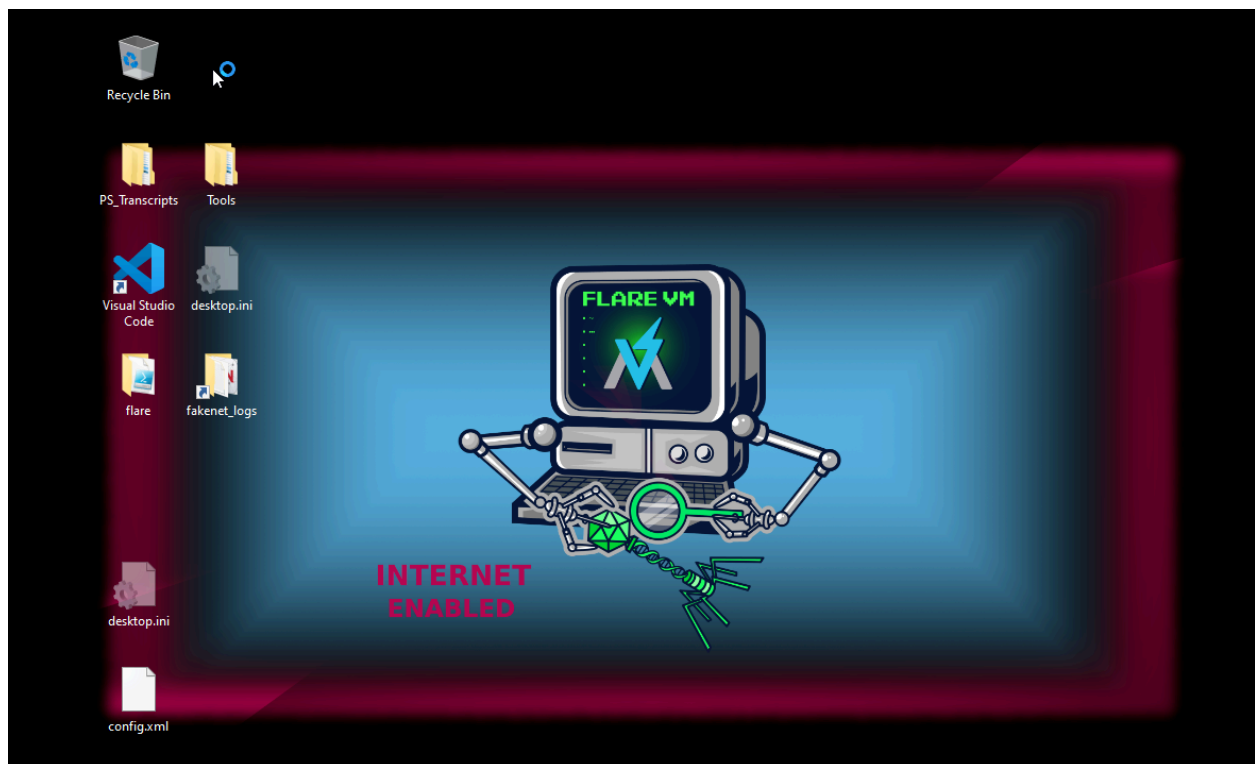
1.Installing windows 10 pro in VMware to set up flare vm



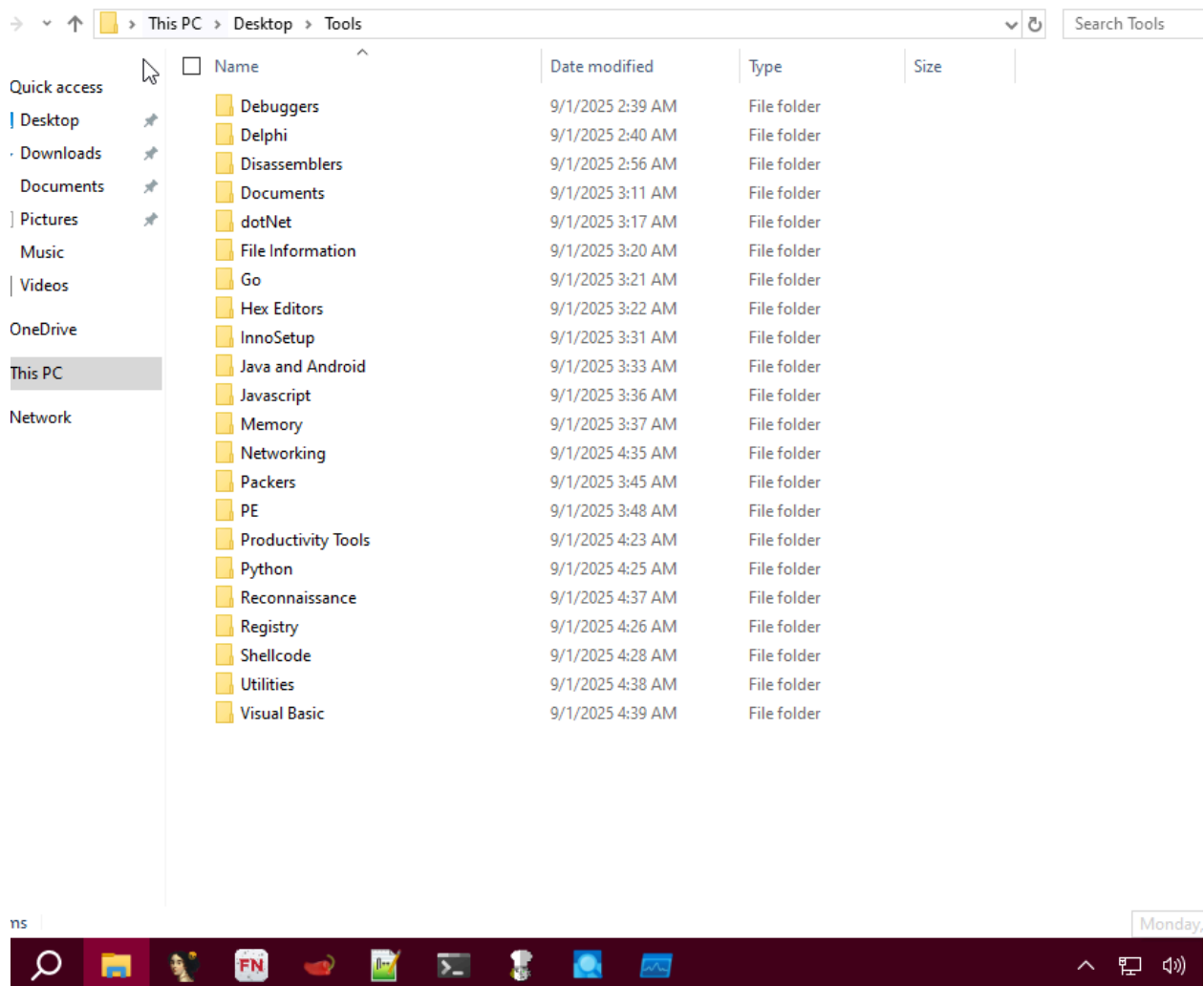
Setting up windows 10 pro by Disabling automatic updates and Windows Defender for a controlled malware analysis environment



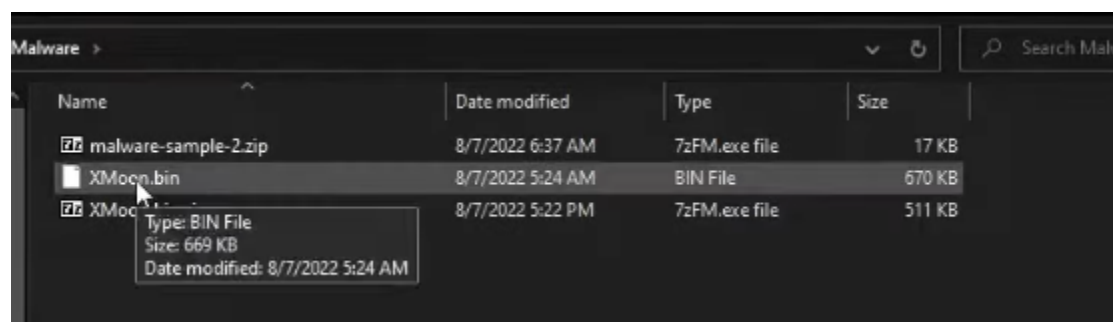
2.0 Installing flare VM and setup



All the tools that needed for Malware Analysis

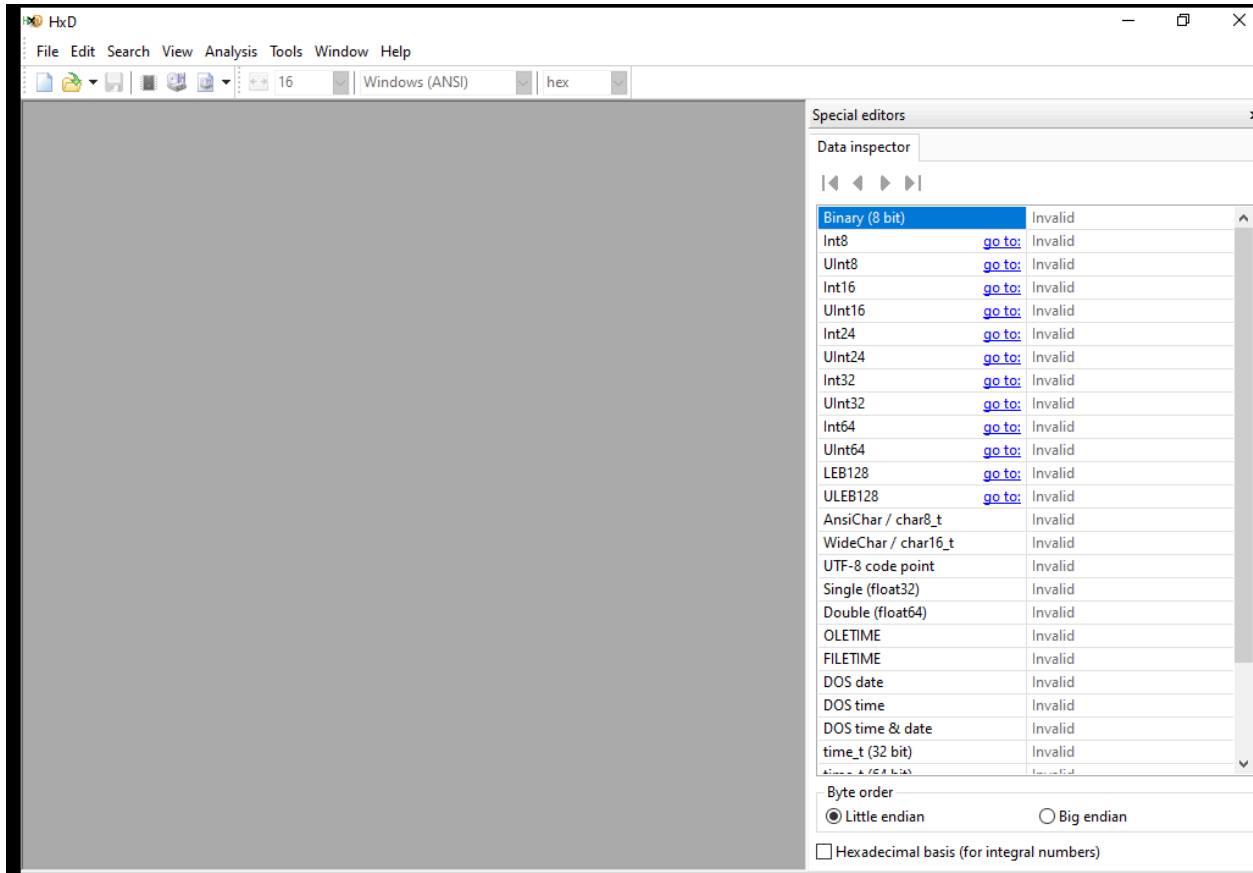


2.1 Taking two malware file samples :

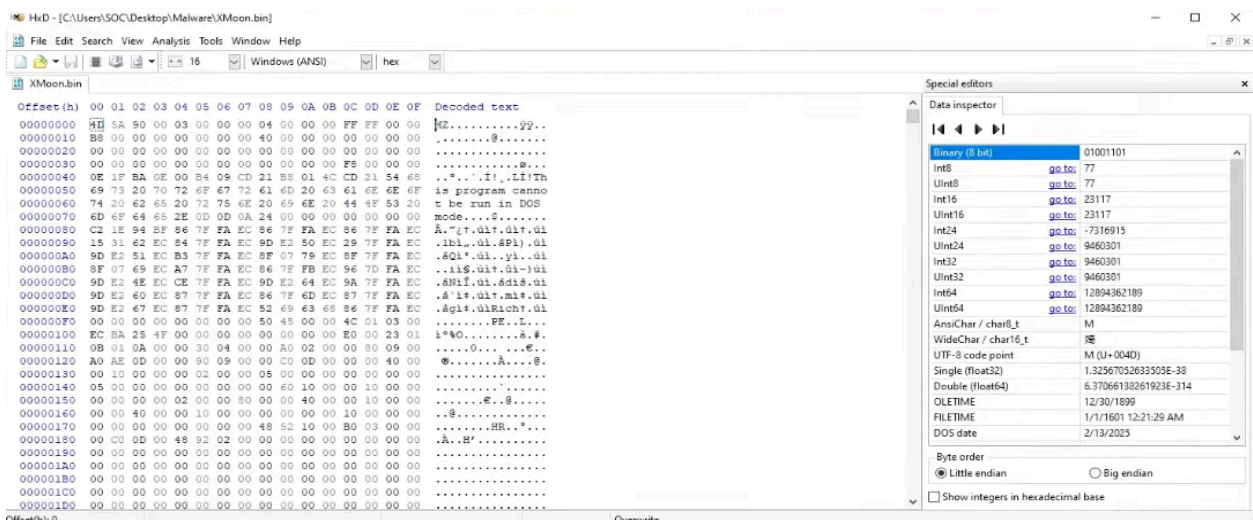


3.0 Filetype of the Malware :

To see the filetype we will use HxD tool



After inserting the file into the tool for find out the filetype



We can see the signature 4D 5A which is an executable file which may contain malware , it can be an image file , so we can use that tool to find the signature and see if it's an executable file

3.0 Fingerprinting the malware :

We will use the hascalc software for identify the malware type

Search instead for **hascalc**



Softonic

<https://hashcalc.en.softonic.com> › Apps › Productivity

HashCalc - Download

15 Dec 2021 — **HashCalc** is a free-of-charge desktop utility that allows you to easily calculate hashes, checksums, and HMAC values for texts, hex strings, and other file ...



People also ask :

3.1 Using Virustotal

After getting the hash number of the malware file as

ea0a5854aa6e91ebe816d256f34f820697a92d86b4f81e8855c84daeed40b9d4 and inserting the hasnumber into the virustotal software we find out that its a trojan malware

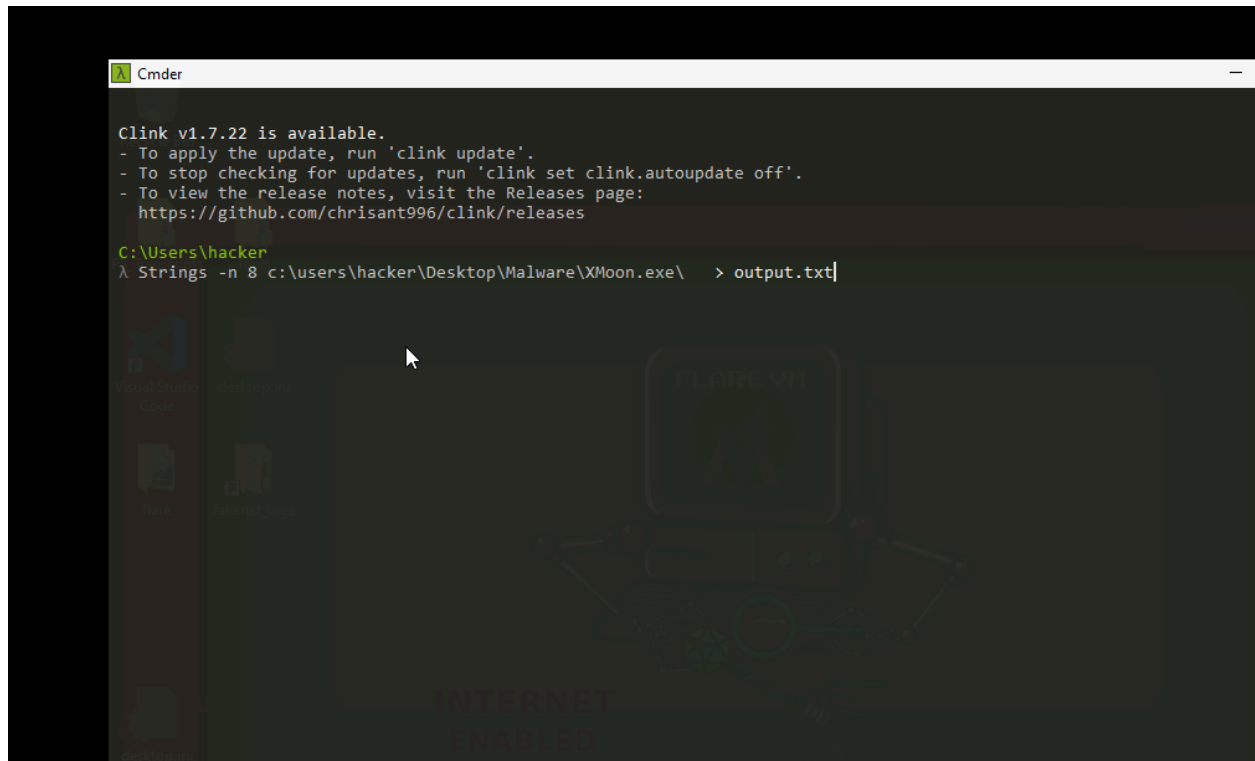
The screenshot shows the VirusTotal analysis page for the file **XMoon.exe** (SHA256: *ea0a5854aa6e91ebe816d256f34f820697a92d86b4f81e8855c84daeed40b9d4*). The file is 669.16 KB and was last analyzed 4 days ago. It has a Community Score of 58/72. The analysis shows that 58/72 security vendors flagged this file as malicious. The file is identified as a trojan, specifically **Trojan:Win32.RL_Agent.R278204**. The security vendors' analysis table is as follows:

Security Vendor	Detection
AhnLab-V3	Trojan/Win32.RL_Agent.R278204
Alibaba	Ransom:Autolt/Lokmwiz.0d4997e0
AliCloud	Ransomware:Win/Crypt888.A
ALYac	Trojan.Ransom.Crypt888
Antiy-AVL	Trojan/Win32.BypassUAC.a
Arcabit	AIT:Trojan.Nymeria.D1AB0 [many]
Arctic Wolf	Unsafe
Avast	Win32:Malware-gen

4.0 Strings

Now we will go through the malware file to know that what's inside the file the urls, the ip , windows API

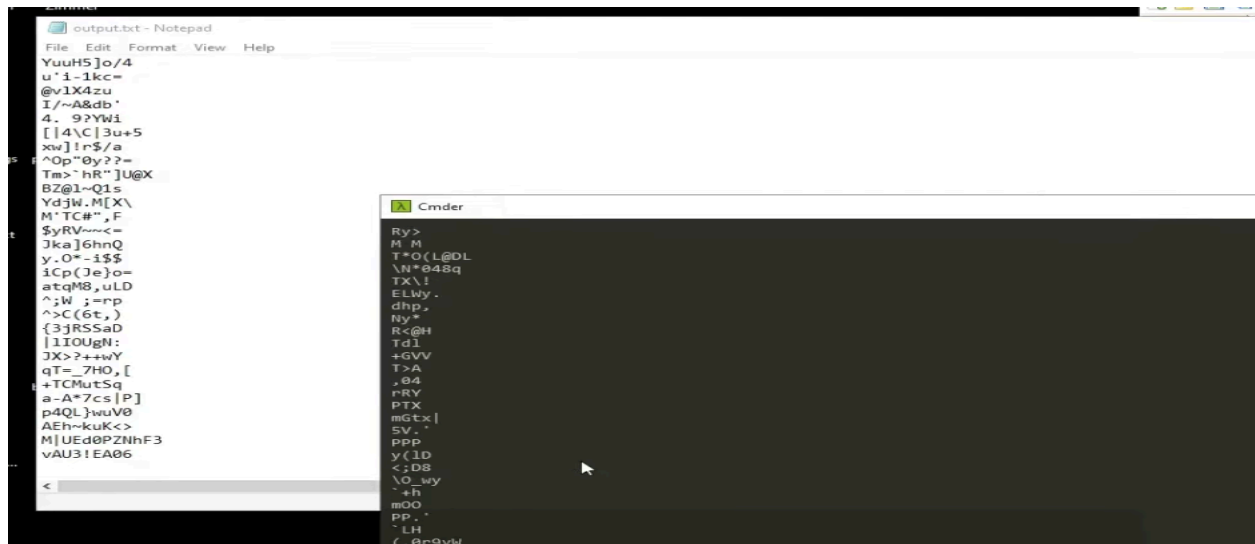
Run this command in cmd tool to find out the string in output.txt



```
Clink v1.7.22 is available.
- To apply the update, run 'clink update'.
- To stop checking for updates, run 'clink set clink.autoupdate off'.
- To view the release notes, visit the Releases page:
  https://github.com/chrisant996/clink/releases

C:\Users\hacker
λ Strings -n 8 c:\users\hacker\Desktop\Malware\XMoon.exe\ > output.txt
```

Then we will find out the output where the string of ip address, api will be included

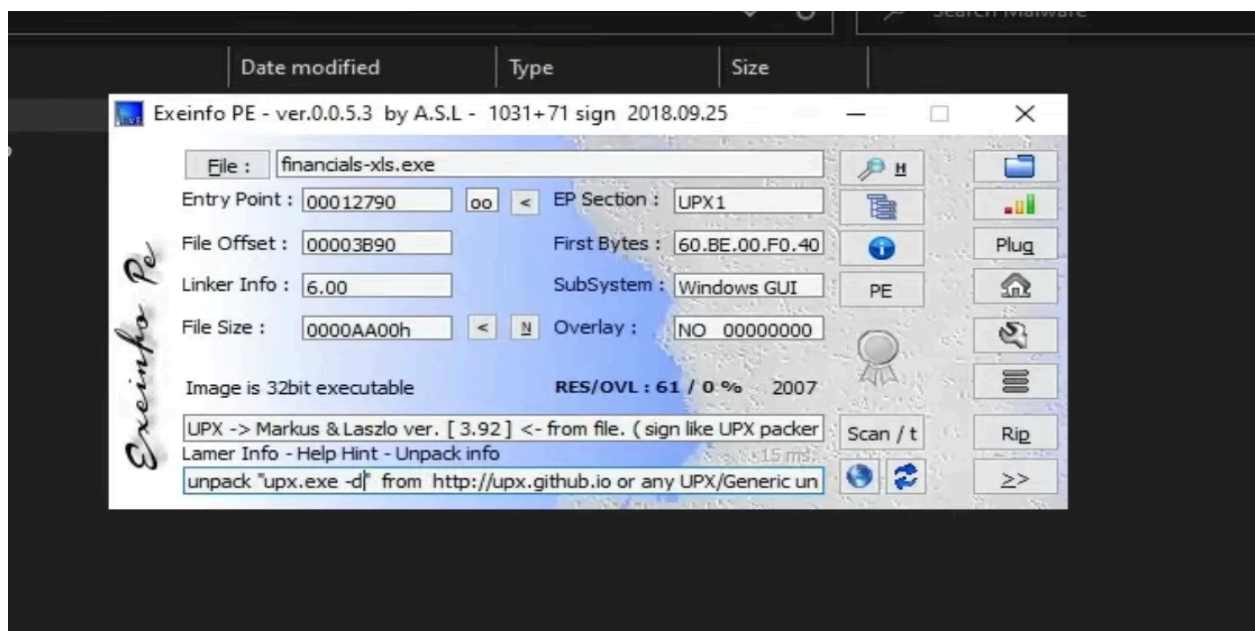
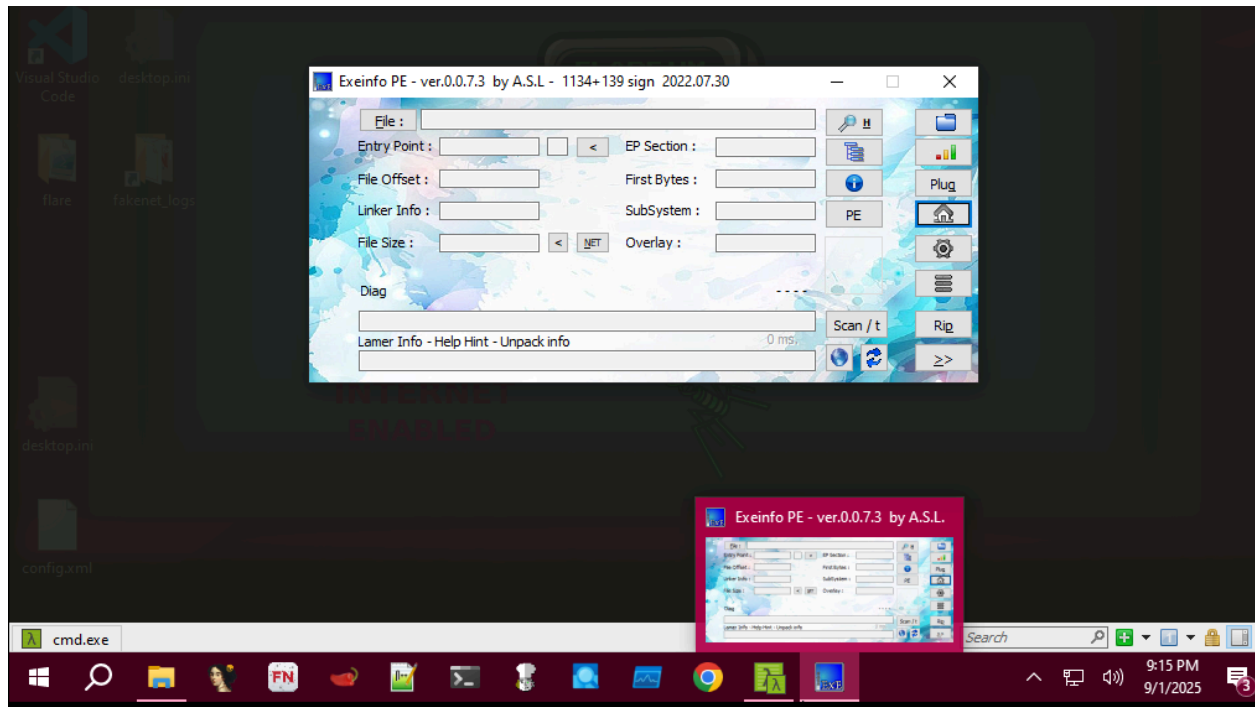


```
output.txt - Notepad
File Edit Format View Help
YuuHS]o/4
u'i-1kc=
@v1X4zu
I/~A&db.
4. 9?YWi
[ [4\C]3u+5
xw]!r$/a
^Op"0y??=
Tm>"hR" ]U@X
BZ@l~Q1s
Vd]W.M[X\
M"TC#",F
$yRV~<=
Jka]6hnQ
y.O*-i$$
iCp(Je)o=
atqM8,uLD
^;W ;=rp
^>C(6t,)
{3jRS5aD
|1IOUgN:
JX>?++wY
qT=_7HO,[
+TCMutSq
a-A*7cs[P]
p4QL}wuV0
AEh~kuK<>
M|UEd0PZNhF3
vAU3!EA06
<
```

5.0 Packing

In malware analysis, packing is a technique used by attackers to obfuscate malware code by compressing or encrypting it to evade detection by antivirus software and hinder analysis.

So we gonna check it now with **exeinfo tool**



From here we know that what packing technique the attacker used , its using UPX to hide itself , from the tool we also know that how to decode the pack as Lamer info

Now we gonna unpack it using the command

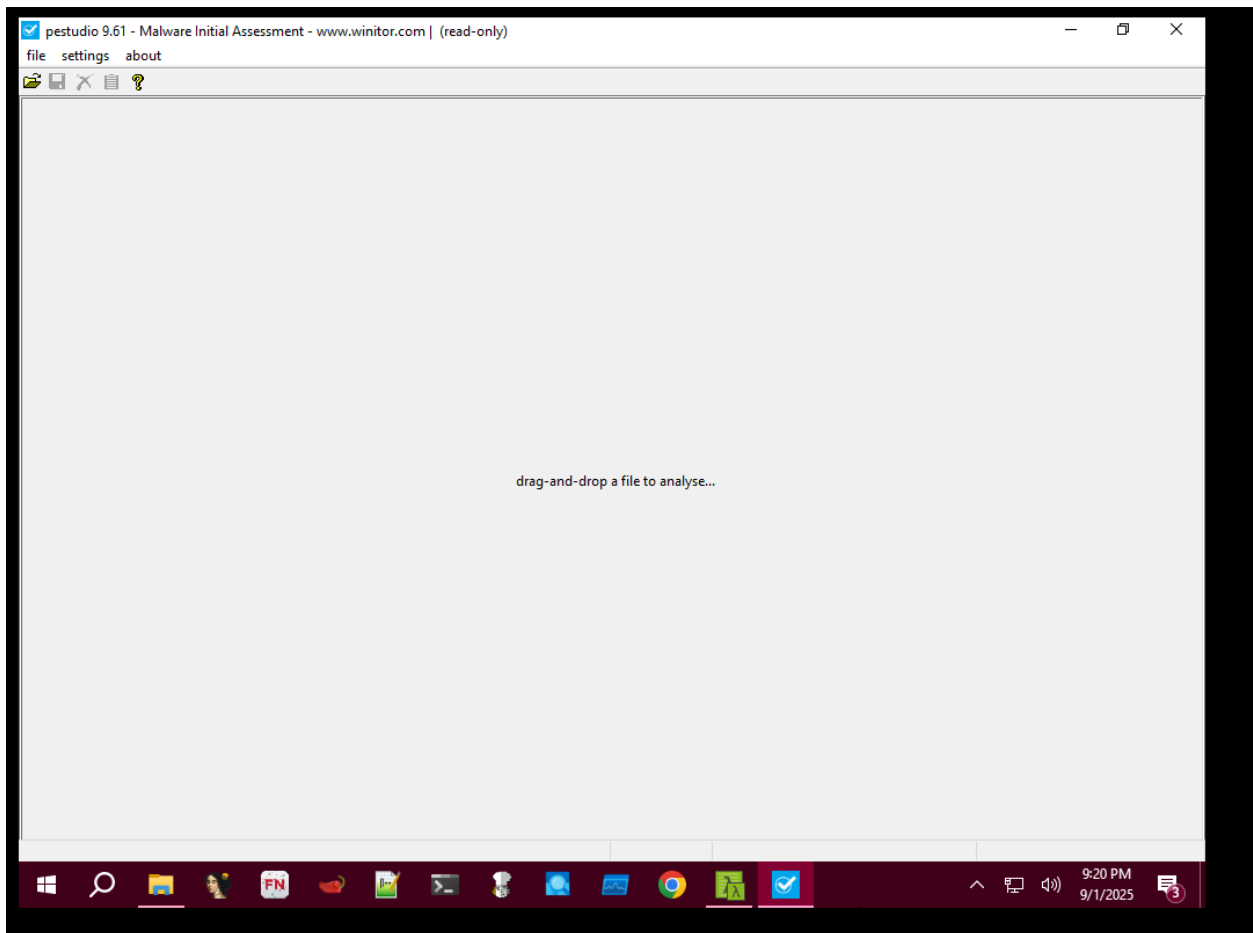
```
λ upx -d -o UnpackedMalware.exe financials-Xls.exe
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX 3.96w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020

File size      Ratio      Format      Name
-----
57344 <- 43520 75.89% win32/pe UnpackedMalware.exe

Unpacked 1 file.
```

6.0 Pestudio

PeStudio is used for the static analysis of Windows executable files (like .exe, .dll) to identify potential malware and suspicious artifacts without actually running the file, its like all in one



Let's use the tool by dropping the malware file here

pestudio 9.39 - Malware Initial Assessment - www.winitor.com [c:\users\soc\desktop\malware\pack\financials.xls.exe]

file settings about

	indicator (39)	detail	level
libraries > flag	count: 1		1
functions > flag	count: 2		1
sections > writable > executable	count: 2		1
strings > flag	count: 3		1
resource > language > flag	name: Russian		1
section > self-modifying	name: UPX4		1
section > self-modifying	name: UPX1		1
section > flag	section: UPX0		1
section > first > writable	section: UPX0		1
section > flag	section: UPX1		1
file > entry-point > suspicious	section: UPX1 > 0x00012790		1
file > score > virustotal	value: 51/66		1
functions > anonymous	count: 1		2
file > checksum > invalid	expected: 0x00014FC4		2
section > virtualized	section: UPX0		2
resources > file-ratio	value: 61.48%		2
resources > instances > standard	count: 3		3
file > signature	name: UPX > www.upx.sourceforge.net		3
file > os > target	name: Windows.NT.4.0		3
function > group	name: dynamic-library		3
function > group	name: execution		3
function > group	name: memory		3
function > group	name: network		3
function > group	name: registry		3
strings > unicode	count: 1		4
strings > ascii	count: 2810		4
file > subsystem > type	name: GUI		4
file > tooling	name: Visual Studio 6.0		4
security > protection	name: address-space-layout-randomization (ASLR) > OFF		4
security > protection	name: code-integrity (CI) > OFF		4
security > protection	name: control-flow-guard (CFG) > OFF		4
security > protection	name: data-execution-prevention (DEP) > OFF		4
file > type	name: executable		4
security > protection	name: stack-buffer-overrun-detection (GS) > OFF		4
resources > manifest > availability	status: no		4
rich-header > checksum	status: valid		4

file settings about

	engine (66/66)	score (51/66)	date (dd.mm.yyyy)	age (days)
indicators (39) *	Lionic	Hacktool.Win32.Renos.3/c	23.05.2022	76
virustotal (51/66)	Elastic	malicious (moderate confidence)	20.05.2022	79
dos-header (64 bytes)	MicroWorld-eScan	Trojan.FakeAlert.RS	22.05.2022	77
dos-stub (152 bytes)	McAfee	Generic.RXAAA-AA127599C22E0EB	22.05.2022	77
rich-header (Visual Studio)	Cylance	Unsafe	23.05.2022	76
file-header (May.2007)	Sangfor	Suspicious.Win32.Save.a	20.05.2022	79
optional-header (GUI)	BitDefender	Trojan.FakeAlert.RS	22.05.2022	77
directories (2)	CrowdStrike	win/malicious_confidence_60% (W)	18.04.2022	111
sections (entry-point)	Arcabit	Trojan.FakeAlert.RS	22.05.2022	77
libraries (7) *	VirIT	Trojan.Win32.FakeAlert.JN	20.05.2022	79
functions (10)	Cyren	W32/FakeAlert.G.gen/Eldorado	23.05.2022	76
exports (n/a)	Symantec	SpySheriff	22.05.2022	77
tlc-callback (n/a)	ESET-NOD32	Win32/Adware.SpySheriff	22.05.2022	77
.NET (n/a)	APEX	Malicious	22.05.2022	77
resources (61.48%)	Paloalto	generic.mli	23.05.2022	76
strings (2811)	ClamAV	Win.Trojan.FakeAlert-33	22.05.2022	77
debug (n/a)	Kaspersky	UDS:Trojan.Win32.Generic	23.05.2022	76
manifest (n/a)	Alibaba	Trojan:Win32/Renos.2bdcbb21c	27.05.2019	1168
version (n/a)	NANO-Antivirus	Virus.Win32.Gen.ccmw	23.05.2022	76
overlay (n/a)	Rising	Downloader.Renos!B.1D0 (CLOUD)	22.05.2022	77
	Ad-Aware	Trojan.FakeAlert.RS	22.05.2022	77
	Sophos	Mal/Generic-S	22.05.2022	77
	Comodo	Application.Win32.Adware.SpySheriff@oso	22.05.2022	77
	DrWeb	Trojan.FakeAlert	22.05.2022	77
	Zillya	Tool.Renos.Win32.1146	19.05.2022	80
	TrendMicro	TROJ_RENOS.SZ	22.05.2022	77
	McAfee-GW-Edition	BehavesLike.Win32.Mydoom.pm	22.05.2022	77
	FireEye	Generic.mg.27599c22e0eba42f	22.05.2022	77
	Emsisoft	Trojan.FakeAlert.RS (B)	23.05.2022	76
	Jiangmin	Trojan.Agent.fmv	22.05.2022	77
	Webroot	W32.Trojan.FakeAlert	23.05.2022	76
	Avira	TR/Dldr.Zlob.Gen	22.05.2022	77
	MAX	malware (ai score=100)	23.05.2022	76
	Gridinsoft	Trojan.Win32.Renos.zvls2	23.05.2022	76
	Microsoft	TrojanDownloader/Win32/Renos	22.05.2022	77
	GData	Trojan.FakeAlert.RS	22.05.2022	77
	Cynet	Malicious (score: 100)	23.05.2022	76
	AhnLab-V3	Win-AppCare/Renos.30720.D	22.05.2022	77
	BitDefenderTheta	Gen:NN.ZexEf.34682.cmGlamRy9il	18.05.2022	81