

Static Analysis – Techniques and Tooling

Static analysis covers everything that can obtain information from a sample without actually loading the program into executable memory space and observing its behavior.

Technical requirements

The technical requirements for this chapter are as follows:

- FLARE VM
- An internet connection (connect only when required)
- Tools - **Get-FileHash, Get-ChildItem, VirusTotal, ssdeep, filetype.exe, strings**
- .zip files containing tools and malware samples from the desktop or downloaded from the below link:

[https://github.com/ PacktPublishing/Malware-Analysis-Techniques](https://github.com/PacktPublishing/Malware-Analysis-Techniques)

Text book : Malware Analysis Techniques Tricks for the triage of adversarial software Dylan Barker, 2021

Hashing

- A hashing algorithm is a one-way function that generates a unique checksum for every file, much like a fingerprint of the file.
- Hashing algorithms and their corresponding bits:

Algorithm	Output Bits	Broken
MD5	128	Yes
SHA1	160	Yes
SHA256	256	No
SHA512	512	No

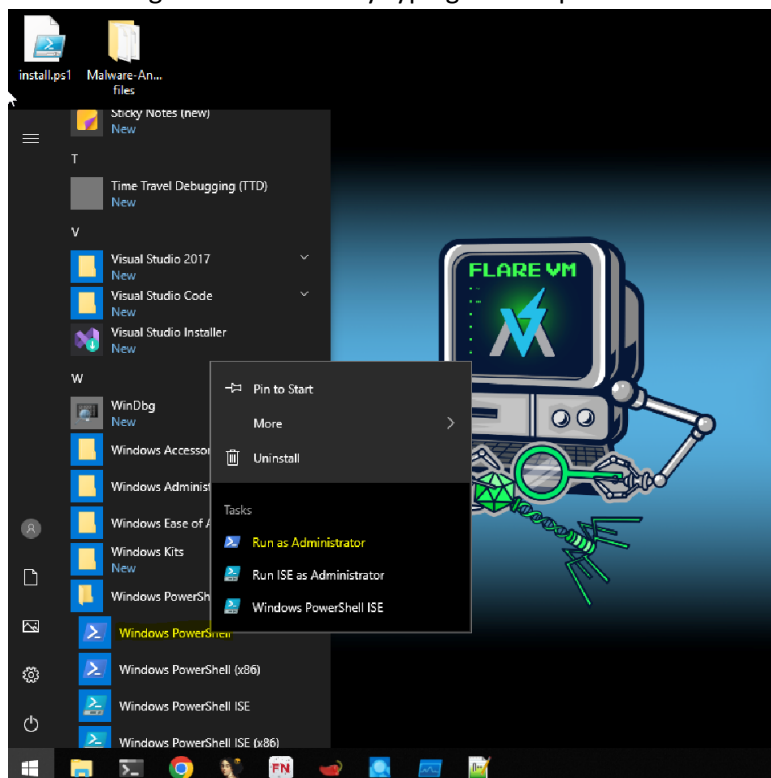
- **Collision** is an occurrence where two different files have identical hashes. When a collision occurs, a hashing algorithm is considered broken and no longer reliable. Examples of such algorithms include MD5 and SHA1.

➤ **Obtaining file hashes**

- Tool built-in into Windows PowerShell - **Get-FileHash** — gets the hash of the file it is provided.
- **Get-ChildItem** and piping the output to Get-FileHash is a great way to get the hashes of files in bulk.
- Modes in Get-ChildItem

```
d - Directory  
a - Archive  
r - Read-only  
h - Hidden  
s - System  
l - Reparse point, symlink, etc.
```

- Usage of the cmdlet by typing Get-Help Get-FileHash



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

FLARE-VM 09/14/2024 11:48:13
PS C:\Windows\system32 > Get-Help Get-Filehash

NAME
    Get-FileHash

SYNTAX
    Get-FileHash [-Path] <string[]> [-Algorithm {SHA1 | SHA256 | SHA384 | SHA512 | MACTripleDES | MD5 | RIPEMD160}]
    [-CommonParameters]

    Get-FileHash -LiteralPath <string[]> [-Algorithm {SHA1 | SHA256 | SHA384 | SHA512 | MACTripleDES | MD5 |
    RIPEMD160}] [-CommonParameters]

    Get-FileHash -InputStream <Stream> [-Algorithm {SHA1 | SHA256 | SHA384 | SHA512 | MACTripleDES | MD5 | RIPEMD160}]
    [-CommonParameters]

ALIASES
    None

REMARKS
    Get-Help cannot find the Help files for this cmdlet on this computer. It is displaying only partial help.
    -- To download and install Help files for the module that includes this cmdlet, use Update-Help.
    -- To view the Help topic for this cmdlet online, type: "Get-Help Get-FileHash -Online" or
    go to https://go.microsoft.com/fwlink/?LinkId=517145.

FLARE-VM 09/14/2024 11:50:07
PS C:\Windows\system32 >
```

- Use the files - md5-1.exe and md5-2.exe. Copy them to Desktop. Use the tool Get-ChildItem

```
Administrator: Windows PowerShell

FLARE-VM 09/14/2024 12:14:24
PS C:\Users\mare\Desktop > cd test
FLARE-VM 09/14/2024 12:14:30
PS C:\Users\mare\Desktop\test > Get-ChildItem

Directory: C:\Users\mare\Desktop\test

Mode                LastWriteTime         Length Name
----                -
-a----             7/29/2020   3:12 PM           7168 md5-1.exe
-a----             7/29/2020   3:12 PM           7168 md5-2.exe

FLARE-VM 09/14/2024 12:14:34
PS C:\Users\mare\Desktop\test >
```

- Find the hash for both the files

```
PS C:\Users\mare\Desktop\test > Get-ChildItem | Get-FileHash -Algorithm MD5

Algorithm Hash Path
-----
MD5 665FF10D581F97B33AF9B7FB9F695912 C:\Users\mare\Desktop\test\md5-1.exe
MD5 665FF10D581F97B33AF9B7FB9F695912 C:\Users\mare\Desktop\test\md5-2.exe

FLARE-VM 09/14/2024 12:15:03
PS C:\Users\mare\Desktop\test >
```

- **Observation:** the files have the same size, MD5 hash

- Reconfirm with a different hash algorithm

```
PS C:\Users\mare\Desktop\test > Get-ChildItem | Get-FileHash -Algorithm SHA256
```

Algorithm	Hash	Path
SHA256	E16A3E7BEA60AB2AA1E49E31199791648C58B14D1691935F25F3BD4E94F2F348	C:\Users\mare\Desktop\test\md5-1.exe
SHA256	84AF18CFD067DF107B790EDE3D8D23A0379F8F8BD1913AB0CEA74C4378F4569	C:\Users\mare\Desktop\test\md5-2.exe

```
FLARE-VM 09/14/2024 12:17:32  
PS C:\Users\mare\Desktop\test >
```

- **Observation:** SHA256 hashes differ! This indicates without a doubt that these files, while the same size and with the same MD5 hash, are not the same file. The importance of choosing a strong one-way hashing algorithm is demonstrated.
- **VirusTotal** - scanning engine that scans possible malware samples against several antivirus (AV) engines and reports their findings. <https://virustotal.com/>
- Use another sample— 8888888.png. file from chapter 2 folder.

Warning!

888888 .png is live malware—a sample of the **Qakbot (QBot)** banking Trojan threat! Handle this sample with care!

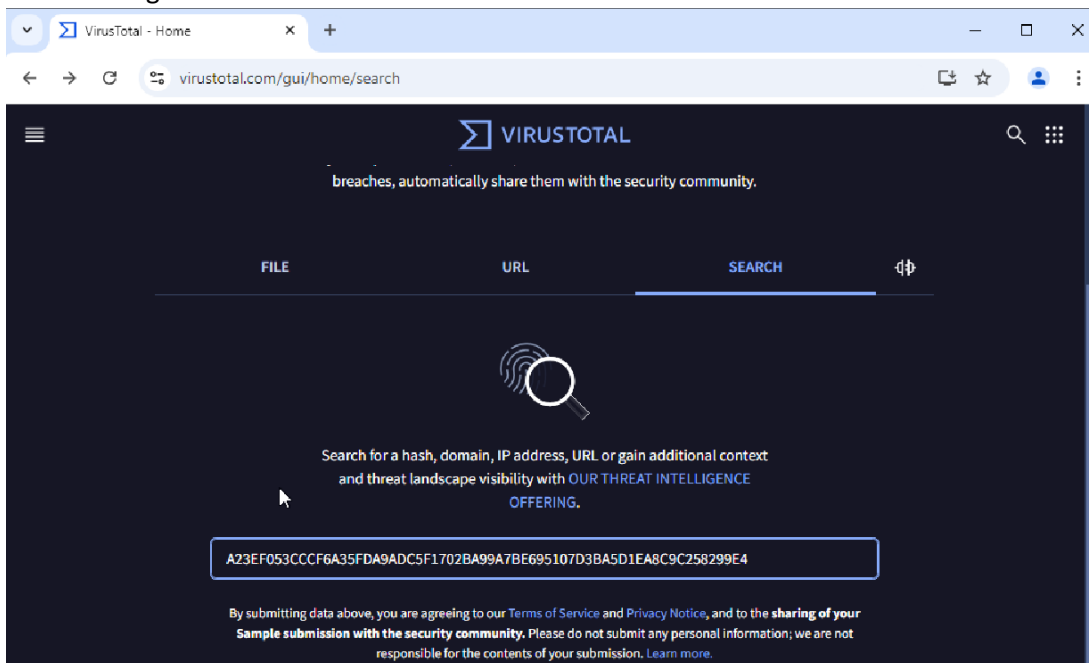
- Find the hash value using the tools Get-ChildItem and Get-Filehash

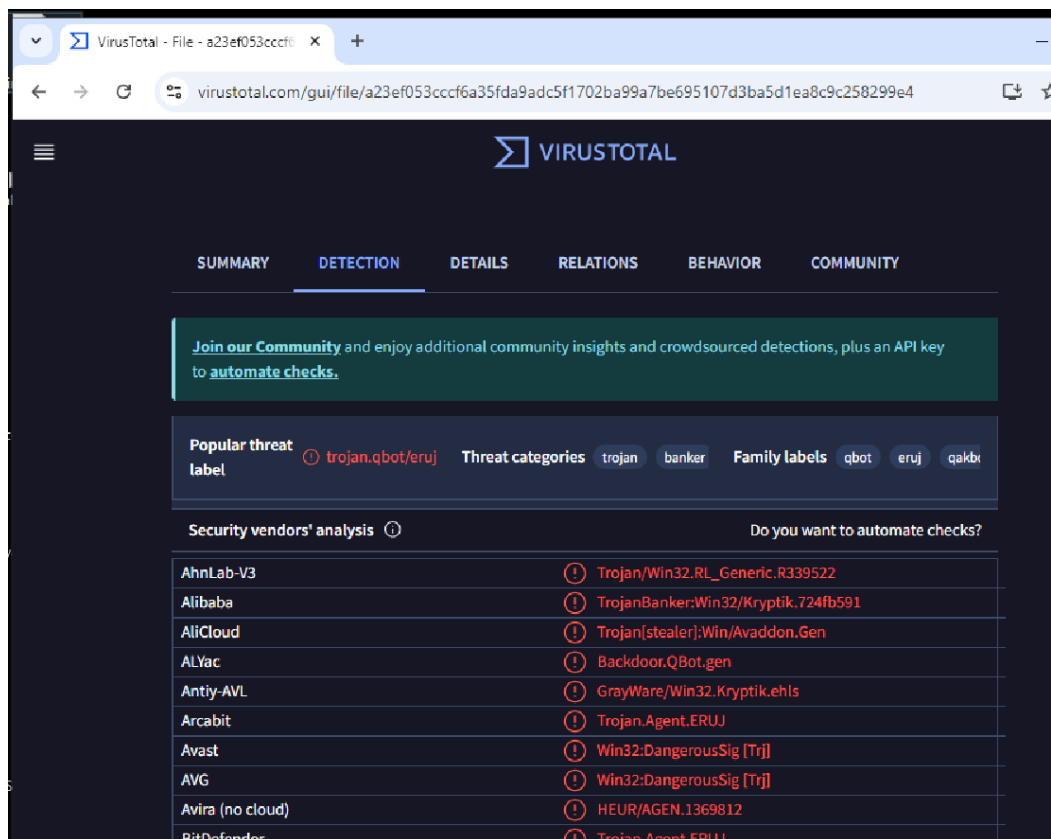
```
PS C:\Users\mare\Desktop\test > Get-ChildItem | Get-FileHash -Algorithm SHA256
```

Algorithm	Hash	Path
SHA256	A23EF053CCCF6A35FDA9ADC5F1702BA99A7BE695107D3BA5D1EA8C9C258299E4	C:\Users\mare\Desktop\test\8888888.png
SHA256	E16A3E7BEA60AB2AA1E49E31199791648C58B14D1691935F25F3BD4E94F2F348	C:\Users\mare\Desktop\test\md5-1.exe
SHA256	84AF18CFD067DF107B790EDE3D8D23A0379F8F8BD1913AB0CEA74C4378F4569	C:\Users\mare\Desktop\test\md5-2.exe

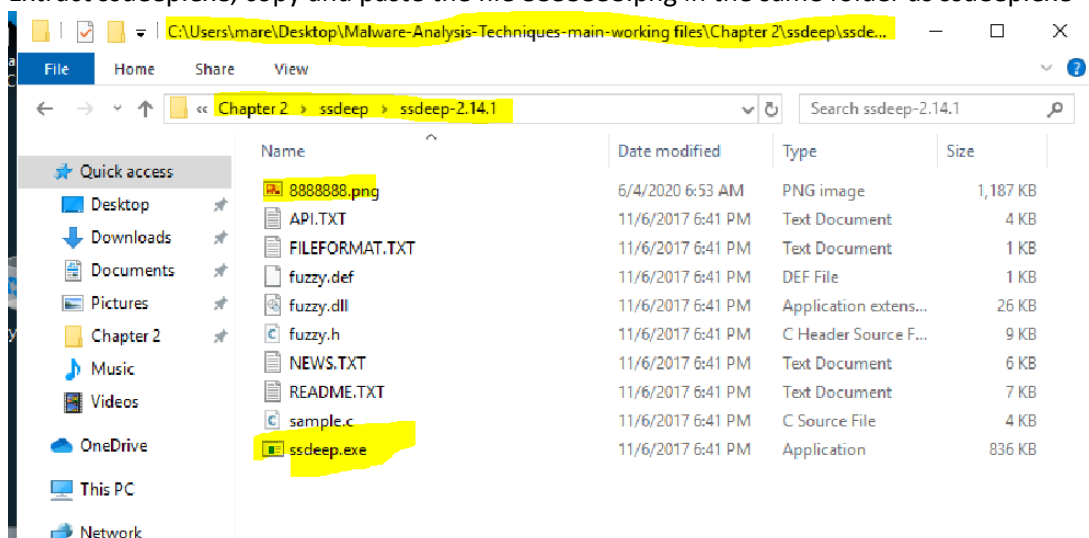
```
FLARE-VM 09/14/2024 12:33:51  
PS C:\Users\mare\Desktop\test >
```

- copy the hash and paste in the VirusTotal web link to check possible match with several antivirus engines.

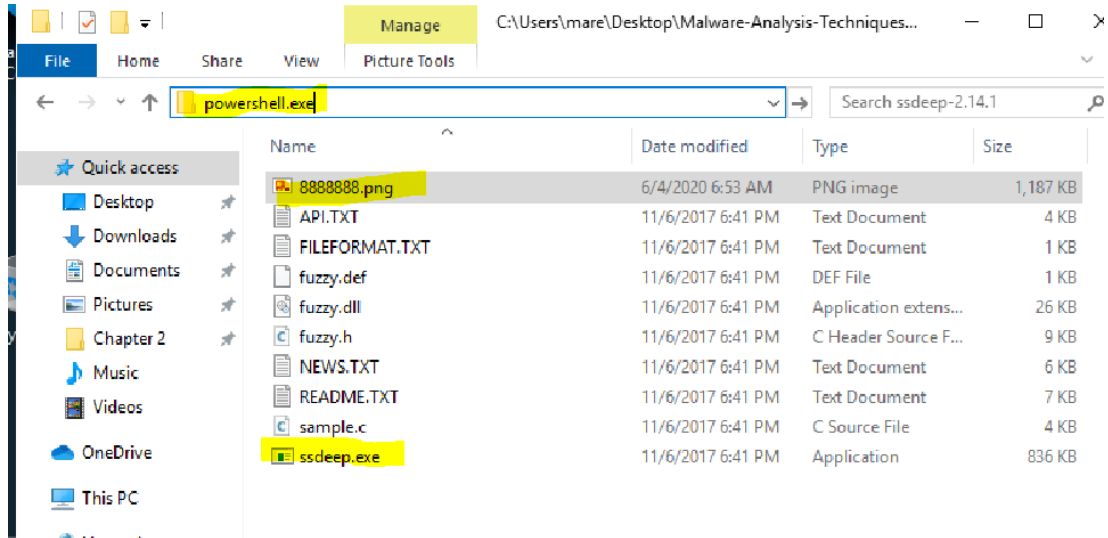




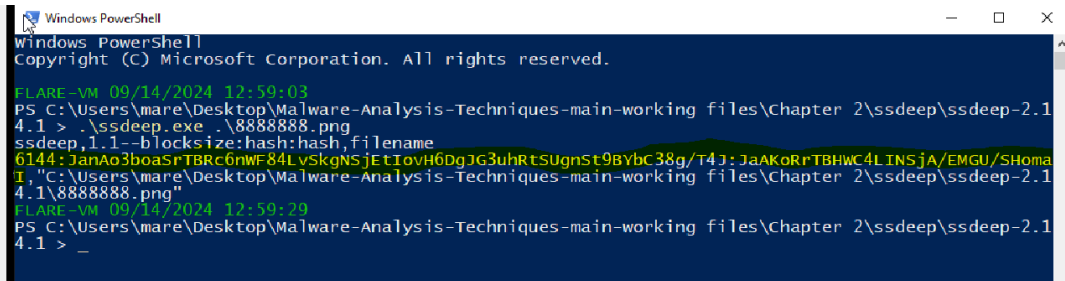
- if no matches found, then **hashbusting** technique (ensures each malware sample has a different static hash!) might be used.
- **fuzzy hashing** – handles hashbusting
- **ssdeep** is a fuzzy hashing algorithm that utilizes a similarity digest in order to create and output representations of files in the following format:
chunksize:chunk:double_chunk
- Extract ssdeep.exe, copy and paste the file 88888888.png in the same folder as ssdeep.exe



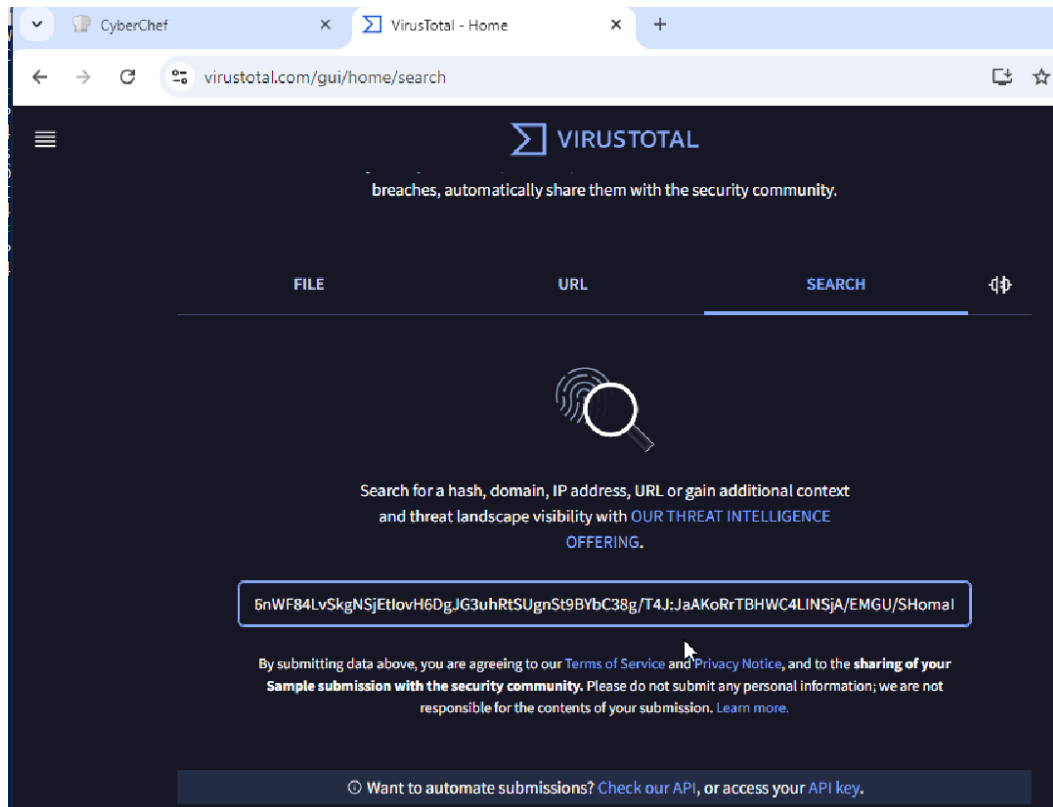
- Open the PowerShell window to the location where ssdeep file is available.

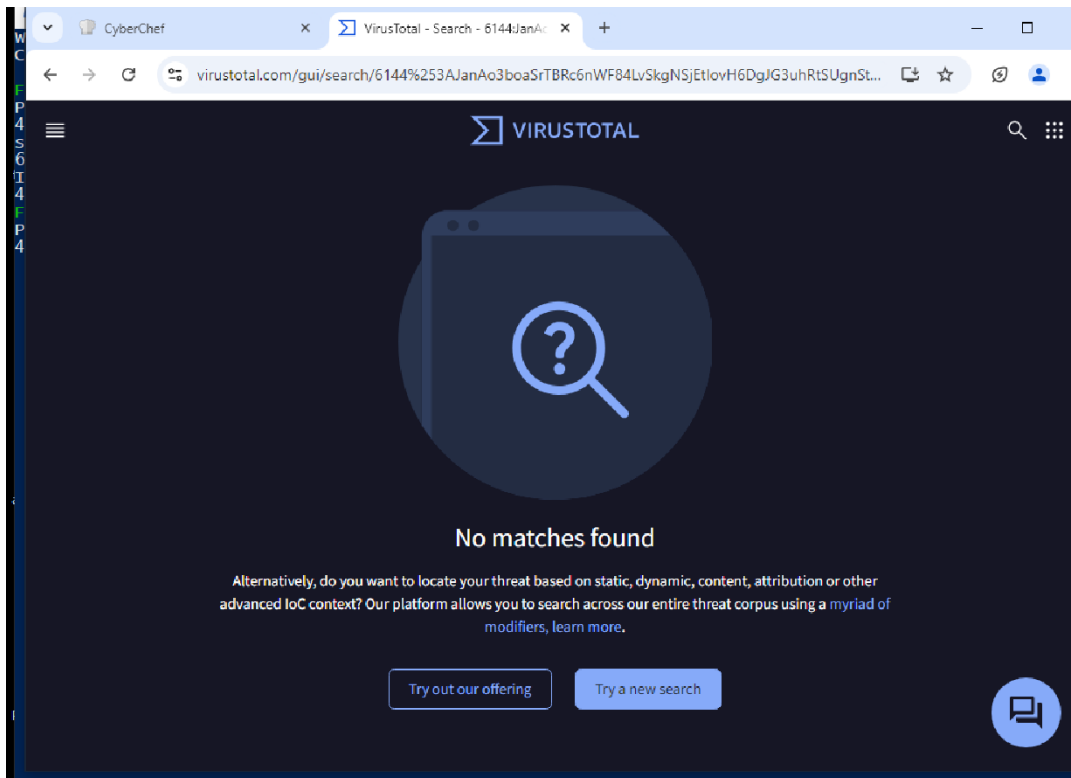


- Obtain ssdeep hash using: `.\ssdeep.exe .\8888888.png`



- Launch VirusTotal.com and find the matches





- ssdeep hashes in VirusTotal, requires an Enterprise membership.
- Observe the following screenshot and interpret.

The screenshot displays the VirusTotal file details page. The file is identified by its hash: C59867EC7FA455862478409878E015A42915B318F1D04E8518507940FC0D3E2D. The page lists several detection engines and their results, including 'peexe', 'invalid-signature', 'signed', 'overlay', 'runtime-modules', 'direct-cpu-clock-access', and 'invalid-signature'. Annotations highlight specific details:

- Corresponding cryptographic hash:** Points to the file hash at the top.
- Engines detecting the file as malicious:** Points to the 'Detections' column, which shows 44 out of 72 engines detecting the file as malicious.
- ssdeep similarity:** Points to the 'Similarity' column, which shows 98% similarity for the first two entries.

File Hash	Similarity	Detections	First seen	Last seen	Submitters
C59867EC7FA455862478409878E015A42915B318F1D04E8518507940FC0D3E2D	98%	44 / 72	2020-06-07 10:50:55	2020-06-07 10:50:55	1
2285F8B4C4530E3E3B3A864FCC661811837844598A846CB0ED68954325E657D	98%	44 / 73	2020-06-07 10:52:24	2020-06-07 10:52:24	1
4058C2875E788A36322EAB81155FF2097497818FC4C811F987D33A931FEE	98%	41 / 73	2020-06-07 10:50:54	2020-06-07 10:50:54	1
2781C3CAE3F63213C30888EC3EAC5785614E2CC6F8C99598F9ACBE1E96CA53	98%	41 / 73	2020-06-07 10:50:42	2020-06-07 10:50:42	1
64CECA73F1E82F178F23EF08F702F58F51C7E89828EF7818780C8418A23CF	98%	50 / 73	2020-06-12 00:16:06	2020-06-12 00:16:06	1
A6C7272774C043846589768428886F5624A2B6432EA58A7ED1C8AACBC5F79E	92%	42 / 73	2020-06-07 20:45:26	2020-06-07 20:45:26	1
287F8C845AC21628A1E1AA2E970C79662235984E5795A6158C823C9A50BF83D	92%	21 / 73	2020-06-04 18:03:05	2020-06-04 18:03:05	1
795E155672C21662E78233033314E66F91E638B31C716E2E167EBA894927BF9A	92%	41 / 70	2020-06-08 09:46:48	2020-06-08 09:46:48	1

- Clicking one of the highly similar cryptographic hashes will load the VirusTotal scan results for the sample

c59067ec7fa45506247b4d9870e015a42915b310f1dd4e85185d794dfcdd3e2d

Avira (no cloud)	① TR/Kryptik.cvsnd	BitDefender	① Trojan.Agent.ERUJ
BitDefenderTheta	① Gen:NN.ZexaF.34126.kv1@aO@wOdpk	CrowdStrike Falcon	① Win/malicious_confidence_60% (W)
Cybereason	① Malicious.bc1a75	Cylance	① Unsafe
eGambit	① PE.Heur.InvalidSig	Emsisoft	① Trojan.Agent.ERUJ (B)
Endgame	① Malicious (high Confidence)	eScan	① Trojan.Agent.ERUJ
ESET-NOD32	① A Variant Of Win32/GenKryptik.ELVG	F-Secure	① Trojan.TR/Kryptik.cvsnd
FireEye	① Generic.mg.2efd9a4f2f4577ee	Fortinet	① W32/GenKryptik.ELTJtr
GData	① Trojan.Agent.ERUJ	Ikarus	① Trojan.Win32.Krypt
K7AntiVirus	① Trojan (005680fc1)	Malwarebytes	① Trojan (005680fc1)
Kaspersky	① Trojan.Win32.Zenpak.aepe	McAfee	① W32/PinkSbot-GUI2EFD9A4F2F45
MAX	① Malware (ai Score=89)	Panda	① Trj/GdSda.A
Microsoft	① Trojan:Win32/Qbot.RA/MTB	Rising	① Trojan.GenKryptik18.AA55 (TFE:dGZIOg...
Qihoo-360	① HEUR/QVM20.1.BEFC.Malware.Gen	SentinelOne (Static ML)	① DFI - Malicious PE
Sangfor Engine Zero	① Malware	Symantec	① ML.Attribute.HighConfidence
Sophos AV	① Troj/Qbot-FS	TrendMicro	① TROJ_GEN.R011C0DF720
Trapmine	① Malicious.moderate.ml.score	VIPRE	① Trojan.Win32.GenericIBT
VBA32	① BScope.Trojan.Inject	ZoneAlarm by Check Point	① Trojan.Win32.Zenpak.aepe
Webroot	① W32.Malware.gen	AegisLab	Undetected
Acronis	Undetected	Avast-Mobile	Undetected
Alibaba	Undetected		

- **Malware serotyping** - Adversaries frequently change the extension of files, sometimes excluding it altogether and sometimes creating double extensions, such as notmalware.doc.exe
- Need a utility for testing file types like **filetype.exe** – a tool within FLARE

```
Windows PowerShell
FLARE-VM 09/14/2024 13:21:13
PS C:\Users\mare\Desktop\MAT-working files\Chapter 2 > .\filetype -i .\8888888.png
.\8888888.png (.exe) "Executable File"
FLARE-VM 09/14/2024 13:21:25
PS C:\Users\mare\Desktop\MAT-working files\Chapter 2 > _
```

- **Observation** : adversary has intentionally changed the file type from .exe to .png

- **Collecting strings**- When an executable is compiled, certain ASCII- or Unicode-encoded strings used during development may be included in the binary
- **strings** - a tool from Microsoft's Windows Sysinternals can be utilized to extract any strings located within the binary
- Launch the command prompt and type **strings -n 5 88888888.png > output.txt**
-n, the minimum string length to return

```
C:\Windows\system32\cmd.exe

FLARE-VM Sat 09/14/2024 13:46:09.32
C:\Users\mare\Desktop\MAT-working files\Chapter 2>strings -n 5 88888888.png > out.txt

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com

FLARE-VM Sat 09/14/2024 13:46:17.34
C:\Users\mare\Desktop\MAT-working files\Chapter 2>dir
Volume in drive C has no label.
Volume Serial Number is D42E-325A

Directory of C:\Users\mare\Desktop\MAT-working files\Chapter 2

09/14/2024 01:45 PM <DIR>      .
09/14/2024 01:45 PM <DIR>      ..
06/04/2020 06:53 AM          1,214,992 88888888.png
02/27/2021 08:27 AM          184,320 Challenge_1.dll
07/18/2021 01:52 PM          3,723,264 Challenge_2.bin
09/03/2004 07:39 AM           45,056 filetype.exe
09/03/2004 07:29 AM           4,372 filetypes.dat
07/29/2020 03:12 PM           7,168 md5-1.exe
07/29/2020 03:12 PM           7,168 md5-2.exe
09/14/2024 01:46 PM           40,752 out.txt
09/14/2024 12:55 PM <DIR>      ssdeep
07/18/2021 01:55 PM          331,210 ssdeep.zip
               9 File(s)      5,558,302 bytes
               3 Dir(s)      36,129,927,168 bytes free

FLARE-VM Sat 09/14/2024 13:46:35.15
C:\Users\mare\Desktop\MAT-working files\Chapter 2>_
```

- There are several strings have been returned, including some of the **Windows application programming interface (API)** modules that are imported by this binary.

```
out.txt - Notepad
File Edit Format View Help
GetLastError
Sleep
LoadLibraryA
GetProcAddress
GetModuleHandleW
IsValidLocale
GetOverlappedResult
CommConfigDialogW
lstrcpmA
WriteConsoleOutputA
DeleteTimerQueueTimer
SetHandleCount
GetSystemTimeAsFileTime
GlobalGetAtomNameW
EnumSystemCodePagesA
GetNamedPipeHandleStateA
CompareStringW
GetProcessAffinityMask
ReadConsoleOutputCharacterW
SetMessageWaitingIndicator
GetProfileIntA
Process32FirstW
GetPrivateProfileSectionA
FlushConsoleInputBuffer
<
Windows (CRLF) Ln 1169, Col 10 100%
```

- We can gain some information on which executable was **backdoored** or what the binary is **masquerading as**! This may prove useful both in tracking the operations of the campaign and tracking **indicators of compromise (IOCs)** for internal outbreaks.



```
out.txt - Notepad
File Edit Format View Help
clFuchsia
DrawingStyle
dsTransparent
Masked
Bitmap
VS_VERSION_INFO
StringFileInfo
040904E4
CompanyName
Lovelysoft
FileDescription
Remote Performance Expert Helper Object
FileVersion
1.8.0.1800
InternalName
LegalCopyright
Copyright
2008-2013 Lovelysoft. All rights reserved
LegalTrademarks
All trademarks are the property of their respective owners.
OriginalFilename
ProductName
AdminToys Suite
ProductVersion
<
Windows (CRLF) Ln 3040, Col 1 100%
```