

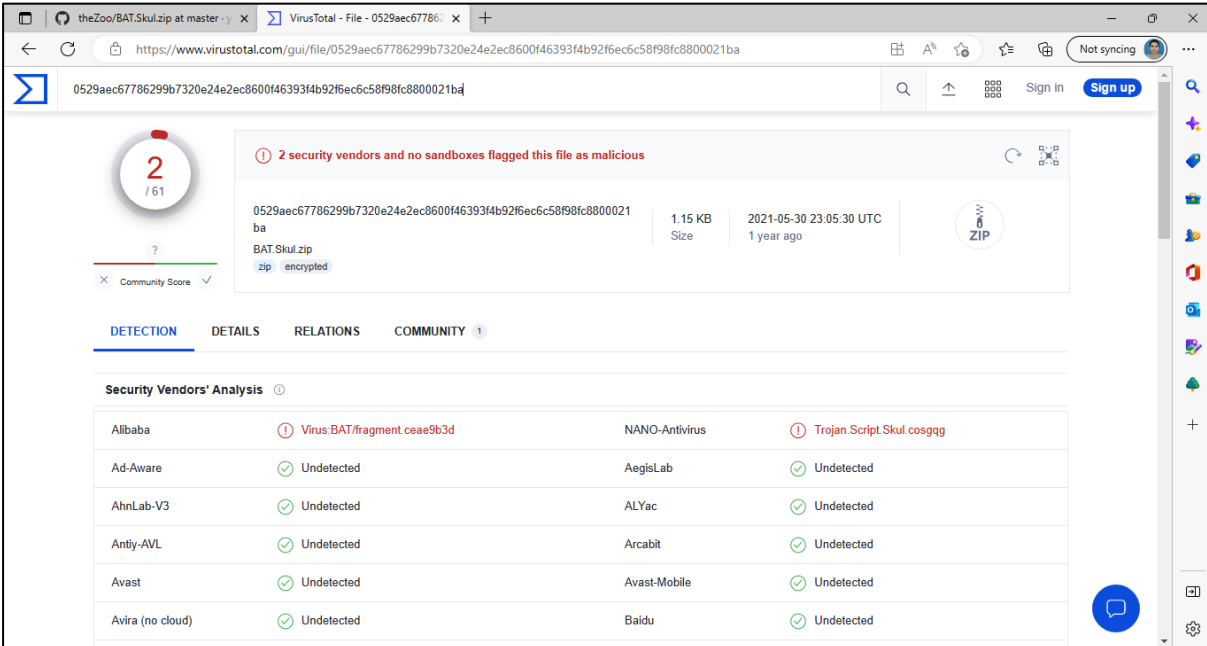
Static Malware Analysis

Basic static analysis can confirm whether a file is malicious, provide information about its functionality, and sometimes provide information that will allow you to produce simple network signatures.

Tools:

1. Virustotal
2. PEstudio
3. WinMD5

• Sample 1



The screenshot shows the VirusTotal web interface for a file analysis. The file is identified as 'BAT.Skul.zip' with a size of 1.15 KB, uploaded on 2021-05-30 23:05:30 UTC. The file is marked as 'zip' and 'encrypted'. A community score of 2/61 is displayed. A warning indicates that 2 security vendors and no sandboxes flagged the file as malicious. The 'DETECTION' tab is active, showing a table of security vendors' analysis results.

Security Vendors' Analysis			
Alibaba	⚠ Virus.BAT/fragment.ceae9b3d	NANO-Antivirus	⚠ Trojan.Script.Skul.cosgqg
Ad-Aware	✅ Undetected	AegisLab	✅ Undetected
AhnLab-V3	✅ Undetected	ALYac	✅ Undetected
Antiy-AVL	✅ Undetected	Arcabit	✅ Undetected
Avast	✅ Undetected	Avast-Mobile	✅ Undetected
Avira (no cloud)	✅ Undetected	Baidu	✅ Undetected

theZoo/BAT.Skul.zip at master · y · VirusTotal - File - 0529aec67786

https://www.virustotal.com/gui/file/0529aec67786299b7320e24e2ec8600f46393f4b92f6ec6c58f98fc8800021ba/details

0529aec67786299b7320e24e2ec8600f46393f4b92f6ec6c58f98fc8800021ba

DETECTIONDETAILSRELATIONSCOMMUNITY 1

Basic Properties

MD5

b46113a11b853c258a5480eb3648cd83

SHA-1

7dc202d0c1eae57fd5ddb9c12c06d599799f3a1e

SHA-256

0529aec67786299b7320e24e2ec8600f46393f4b92f6ec6c58f98fc8800021ba

Vhash

196a163dc177b7f893b255be1f71d1cb

SSDEEP

24:Ap8O/tU5u8Lu3LX0mkAwKheH3Y0JdDf1CSpzveyZ5H:ARU5ut70BghWYwkYfv

TLSH

T13D21937340BBEA00D97B48749ADF19F3AA408C1780154F73E4AD78519DEA4F4CE94AA9

File type

ZIP

Magic

Zip archive data, at least v2.0 to extract

TrID

ZIP compressed archive (80%) PrintFox/Pagefox bitmap (640x800) (20%)

File size

1.15 KB (1181 bytes)

History

First Submission

2019-03-14 07:24:01 UTC

Last Submission

2022-08-10 09:33:53 UTC

Last Analysis

2021-05-30 23:05:30 UTC

Earliest Contents Modification

2004-05-31 23:00:58

Latest Contents Modification

2019-01-09 22:40:54

Names

theZoo/BAT.Skul.zip at master · y · VirusTotal - File - 0529aec67786

https://www.virustotal.com/gui/file/0529aec67786299b7320e24e2ec8600f46393f4b92f6ec6c58f98fc8800021ba/details

0529aec67786299b7320e24e2ec8600f46393f4b92f6ec6c58f98fc8800021ba

Not syncing

BAT.Skul.zip

Bundle Info

Contents Metadata

Contained Files

3

Uncompressed Size

6.81 KB

Earliest Content Modification

2004-05-31 23:00:58

Latest Content Modification

2019-01-09 22:40:54

Contained Files By Type

UNKNOWN 3

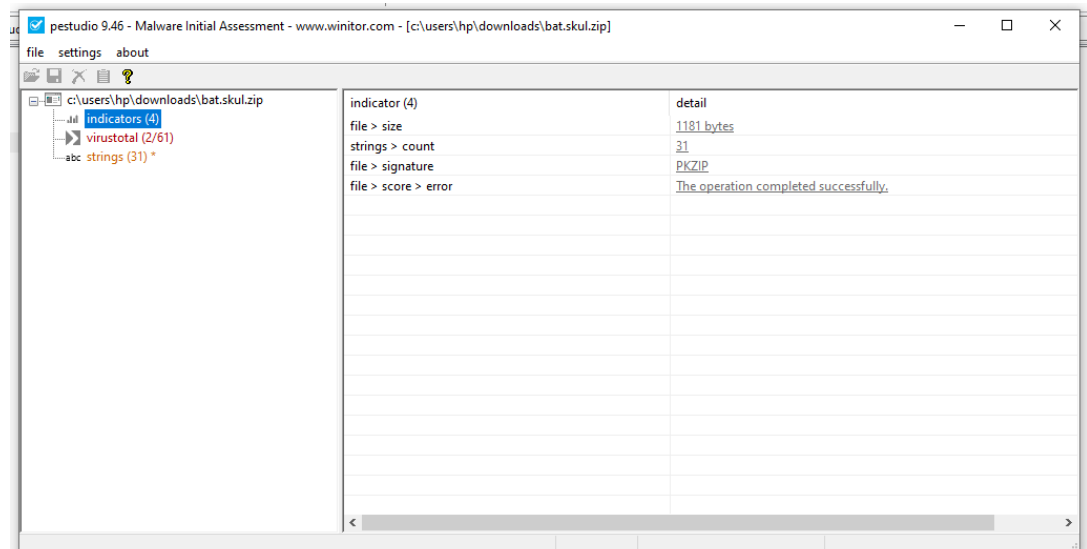
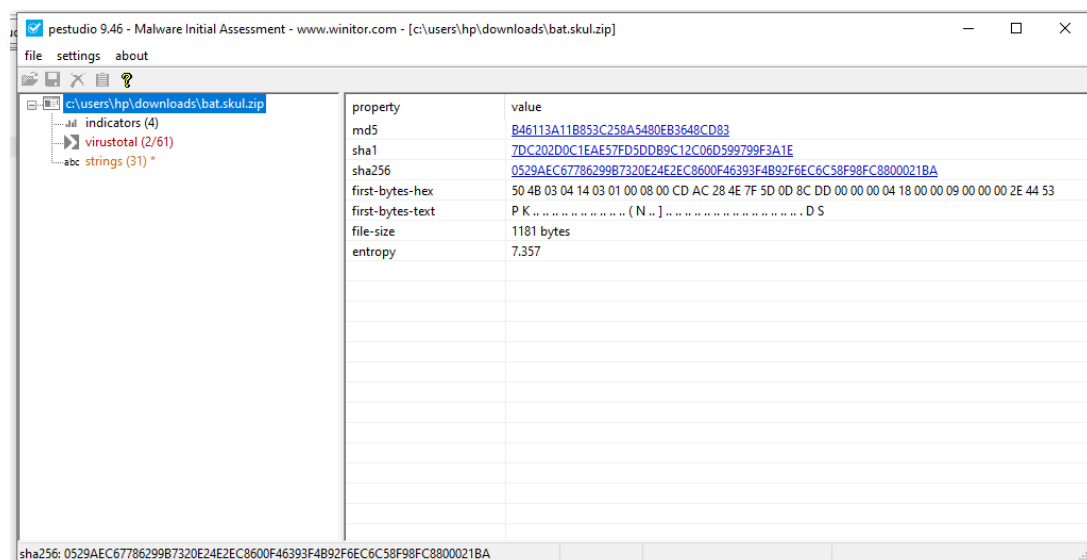
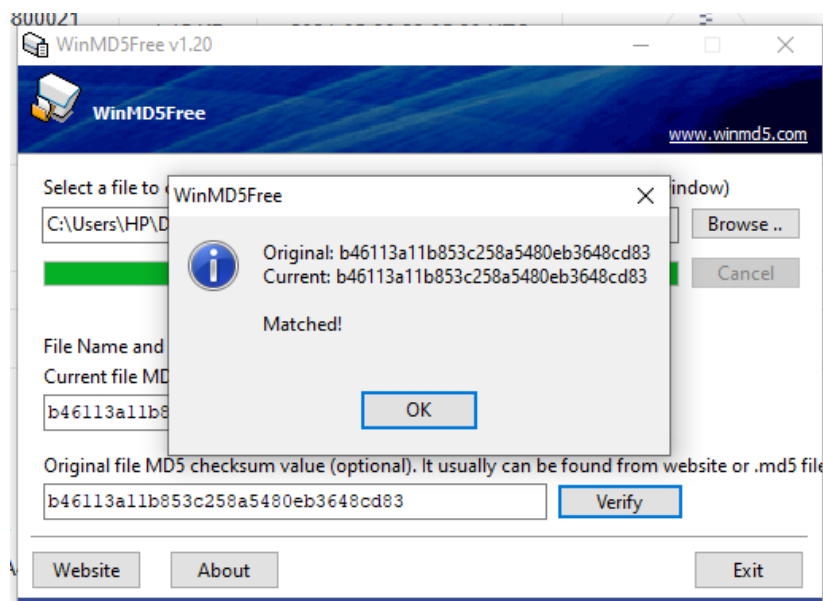
Contained Files By Extension

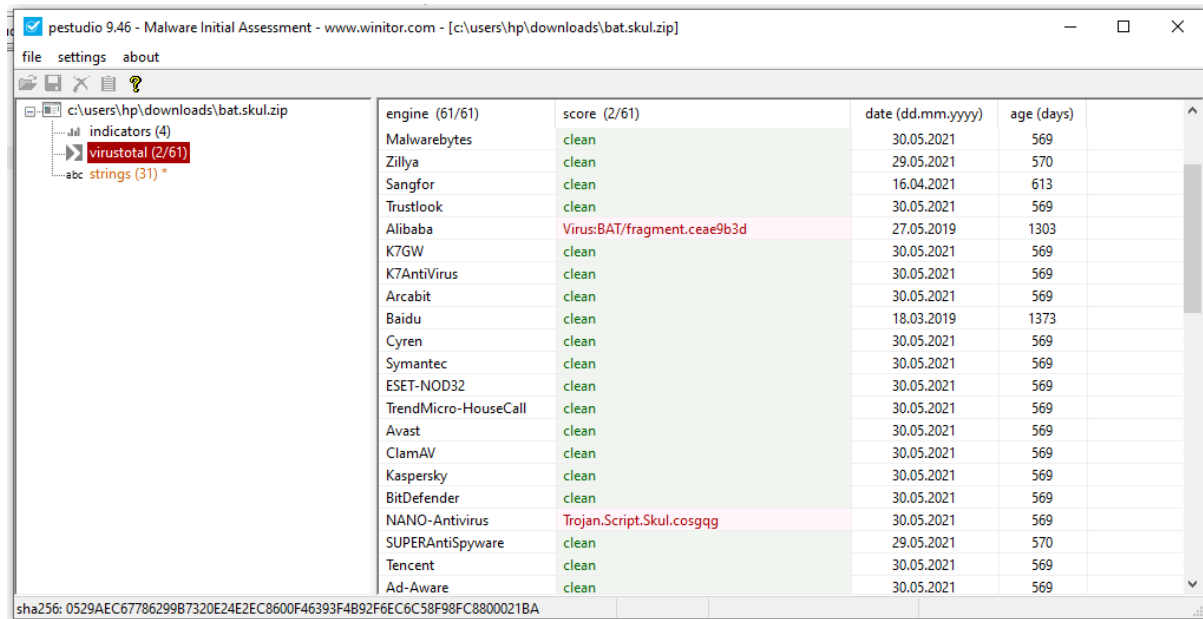
BAT

1

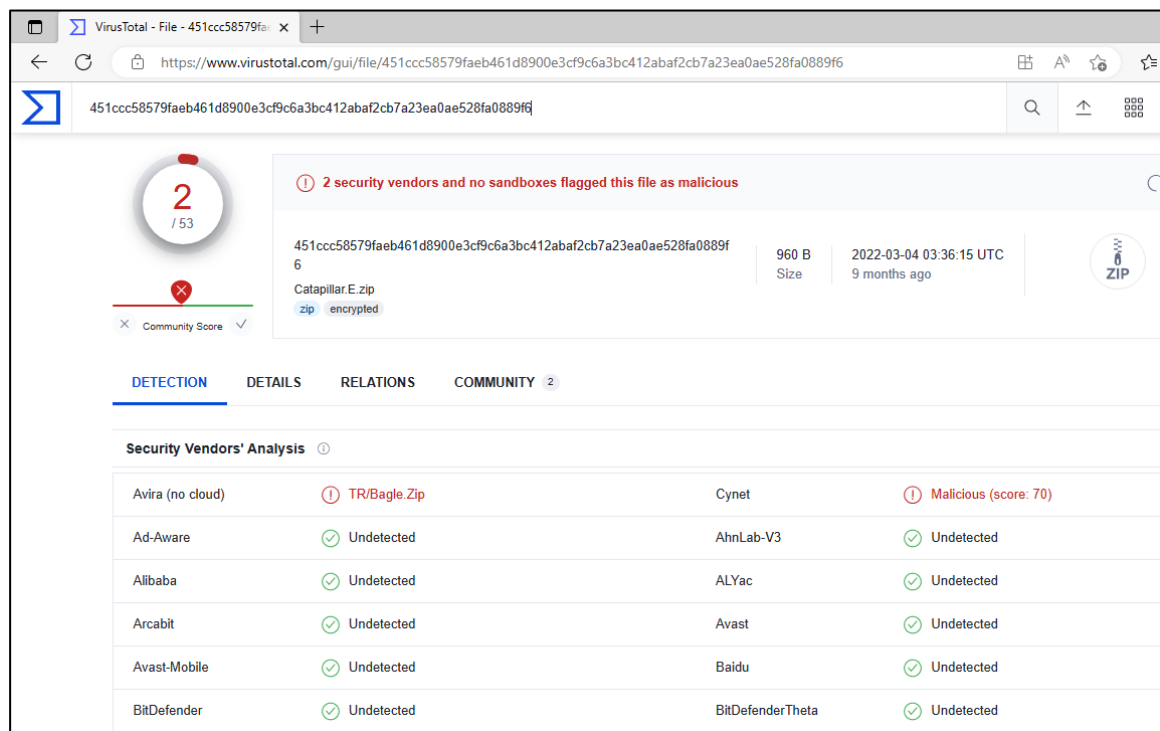
TXT

1





• Sample 2



← ↻ 🔍 https://www.virustotal.com/gui/file/451ccc58579faeb461d8900e3cf9c6a3bc412abaf2cb7a23ea0ae528fa0889f6/details

451ccc58579faeb461d8900e3cf9c6a3bc412abaf2cb7a23ea0ae528fa0889f6

2 / 53

2 security vendors and no sandboxes flagged this file as malicious

451ccc58579faeb461d8900e3cf9c6a3bc412abaf2cb7a23ea0ae528fa0889f6 960 B Size 2022-03-04 03:36:15 UTC 9 months ago

Catapillar.E.zip zip encrypted

Community Score

DETECTION DETAILS RELATIONS COMMUNITY 2

Basic Properties

MD5	910c2d354eff59b037b957f2a7262992
SHA-1	67d66f43911aafec05bd7a8730311a2191bbdc3
SHA-256	451ccc58579faeb461d8900e3cf9c6a3bc412abaf2cb7a23ea0ae528fa0889f6
Vhash	43d37ca2355b37b10b7524b3a8830edc
SSDEEP	24:OIRkKSfIbdac+AuWtvkbUTwRXX3bLmsuSSw1kCTeXV17vbtq:OfDFIN75YLLLmXRw1pojY
TLSH	T1CB115052A806C176C26D09F4FD3E9A859B600ACAC7722EA4829C640BED230B81B58
File type	ZIP
Magic	Zip archive data, at least v2.0 to extract
TrID	ZIP compressed archive (80%) PrintFox/Pagefox bitmap (640x800) (20%)
File size	960 B (960 bytes)

History

WinMD5Free v1.20

WinMD5Free www.winmd5.com

Select a file to compare (or drag and drop)

C:\Users\HP\Documents\WinMD5Free

File Name and Size

Current file MD5

910c2d354eff59b037b957f2a7262992

Original file MD5 checksum value (optional). It usually can be found from website or .md5 file

910c2d354eff59b037b957f2a7262992

Website About Exit

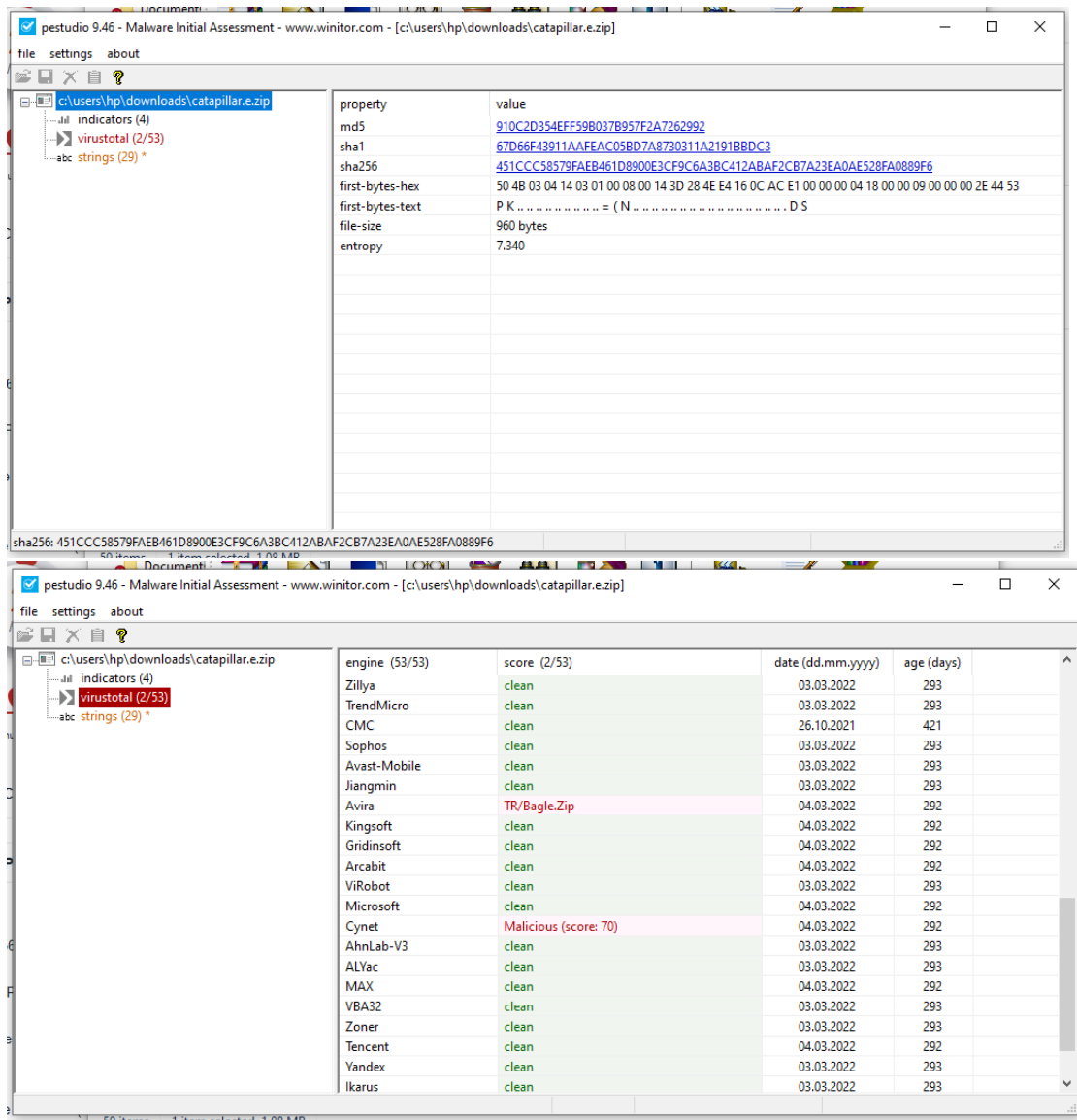
WinMD5Free

Original: 910c2d354eff59b037b957f2a7262992
Current: 910c2d354eff59b037b957f2a7262992

Matched!

OK

Verify



- Sample 3

2

/ 62

?

Community Score

2 security vendors and no sandboxes flagged this file as malicious

72687b3bdb1b51311c94178fa0bc263129ee22310d15e83b4b0540b5bf072649

4.93 MB

2022-03-02 05:07:19 UTC

OSX.HellRaiser.zip

zip

mac-app

ZIP

DETECTION

DETAILS

COMMUNITY

Security Vendors' Analysis

Fortinet	ⓘ Riskware/Brugli.OSX	NANO-Antivirus	ⓘ Trojan.Mac.Hellraiser.bchkmo
Ad-Aware	✔ Undetected	AhnLab-V3	✔ Undetected
Alibaba	✔ Undetected	ALYac	✔ Undetected
Antiy-AVL	✔ Undetected	Arcabit	✔ Undetected
Avast	✔ Undetected	Avast-Mobile	✔ Undetected
Avira (no cloud)	✔ Undetected	Baidu	✔ Undetected

2

/ 62

?

Community Score

2 security vendors and no sandboxes flagged this file as malicious

72687b3bdb1b51311c94178fa0bc263129ee22310d15e83b4b0540b5bf072649

4.93 MB

2022-03-02 05:07:19 UTC

OSX.HellRaiser.zip

zip

mac-app

ZIP

DETECTION

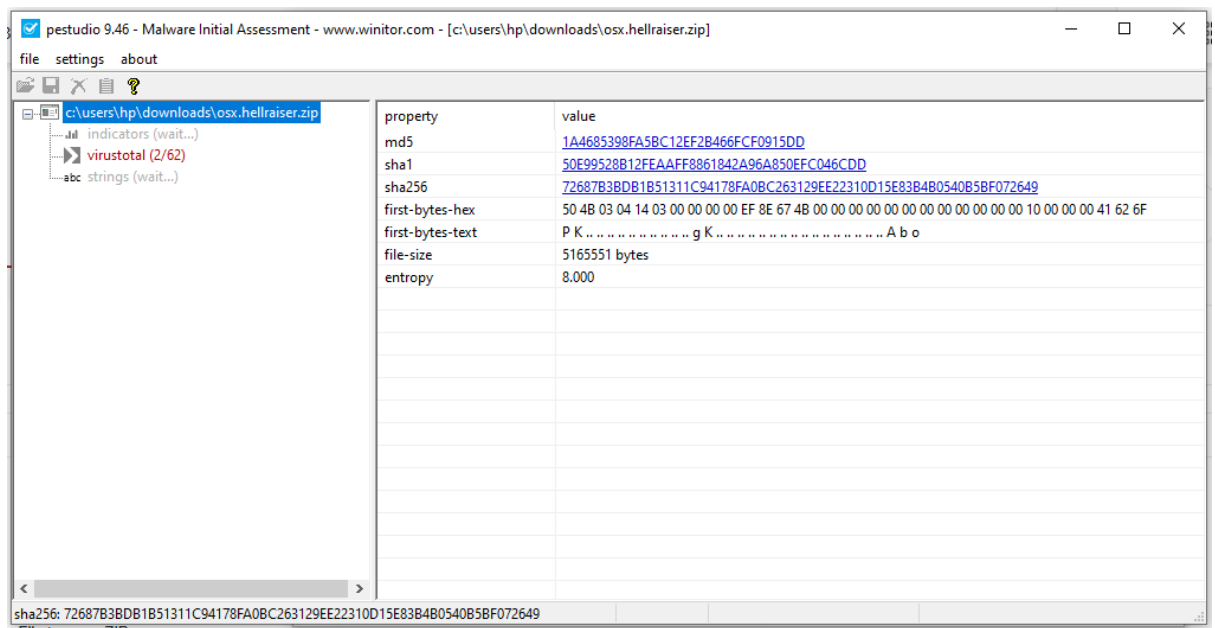
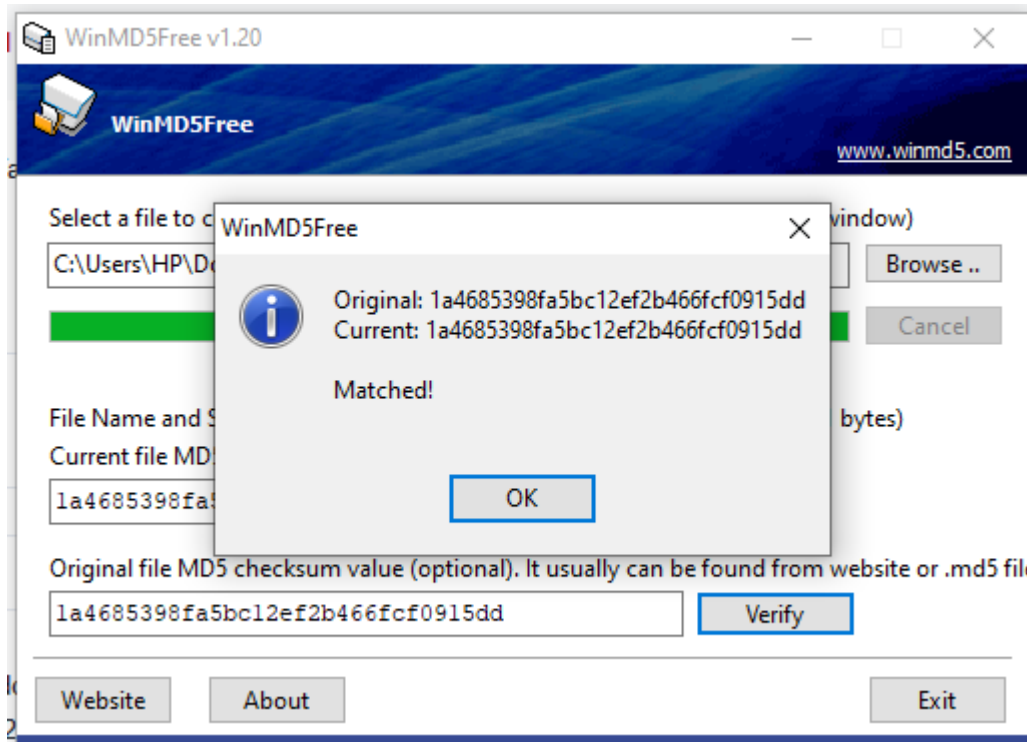
DETAILS

COMMUNITY

Basic Properties

MD5	1a4685398fa5bc12ef2b466fcf0915dd
SHA-1	50e99528b12feaff8861842a96a850efc046cdd
SHA-256	72687b3bdb1b51311c94178fa0bc263129ee22310d15e83b4b0540b5bf072649
Vhash	f9158b37a57080bebf4c38abf84b574b
SSDEEP	98304:JSfd8PbarxH7LFkU2y5X+Dzw2QVvuXlh3QBZB3kP6GTom+O+xDc4IA:JSfdeK7LFks5X+Dc2QVcl6zB32svvA
TLSH	T11A36336E3F10D849C790A67D079CEDD80843A184DC6BEA1251BC716FEEF413BE847AA5
File type	ZIP
Magic	Zip archive data, at least v2.0 to extract
TrID	ZIP compressed archive (80%) PrintFox/Pagefox bitmap (640x800) (20%)
File size	4.93 MB (5165551 bytes)

History



pestudio 9.46 - Malware Initial Assessment - www.winitor.com - [c:\users\hp\downloads\osx.hellraiser.zip]

file settings about

c:\users\hp\downloads\osx.hellraiser.zip

indicators (wait...)

virustotal (2/62)

strings (wait...)

engine (62/62)	score (2/62)	date (dd.mm.yyyy)	age (days)
Avast	clean	02.03.2022	294
ClamAV	clean	01.03.2022	295
Kaspersky	clean	02.03.2022	294
BitDefender	clean	02.03.2022	294
NANO-Antivirus	Trojan.Mac.Hellraiser.bchkmo	02.03.2022	294
SUPERAntiSpyware	clean	26.02.2022	298
Tencent	clean	02.03.2022	294
Ad-Aware	clean	02.03.2022	294
TACHYON	clean	02.03.2022	294
Emsisoft	clean	02.03.2022	294
Comodo	clean	02.03.2022	294
F-Secure	clean	02.03.2022	294
Baidu	clean	18.03.2019	1374
VIPRE	clean	19.01.2022	336
TrendMicro	clean	02.03.2022	294
McAfee-GW-Edition	clean	02.03.2022	294
CMC	clean	26.10.2021	421
Sophos	clean	02.03.2022	294
SentinelOne	clean	01.02.2022	323
Avast-Mobile	clean	01.03.2022	295
Jiangmin	clean	01.03.2022	295

sha256: 72687B3BDB1B51311C94178FA0BC263129EE22310D15E83B4B0540B5BF072649

File type: ZIP

pestudio 9.46 - Malware Initial Assessment - www.winitor.com - [c:\users\hp\downloads\osx.hellraiser.zip]

file settings about

c:\users\hp\downloads\osx.hellraiser.zip

indicators (wait...)

virustotal (2/62)

strings (wait...)

engine (62/62)	score (2/62)	date (dd.mm.yyyy)	age (days)
Avira	clean	02.03.2022	294
Antiy-AVL	clean	02.03.2022	294
Kingsoft	clean	02.03.2022	294
Gridinsoft	clean	02.03.2022	294
Microsoft	clean	01.03.2022	295
ViRobot	clean	02.03.2022	294
ZoneAlarm	clean	02.03.2022	294
GData	clean	02.03.2022	294
Cynet	clean	02.03.2022	294
AhnLab-V3	clean	01.03.2022	295
VBA32	clean	01.03.2022	295
ALYac	clean	02.03.2022	294
MAX	clean	02.03.2022	294
Zoner	clean	01.03.2022	295
Rising	clean	01.03.2022	295
Yandex	clean	01.03.2022	295
Ikarus	clean	01.03.2022	295
MaxSecure	clean	01.03.2022	295
Fortinet	Riskware/BrugilOSX	02.03.2022	294
Panda	clean	01.03.2022	295

sha256: 72687B3BDB1B51311C94178FA0BC263129EE22310D15E83B4B0540B5BF072649

File type: ZIP

- Sample 4

93861a8aa9a4f42489d029c64bc0599c208971891c70a9b2192b60e20c57d3bc

1/61

?

Community Score

1 security vendor and no sandboxes flagged this file as malicious

93861a8aa9a4f42489d029c64bc0599c208971891c70a9b2192b60e20c57d3bc

3.10 KB

2022-08-21 09:38:43 UTC

4 months ago

ZIP

AntiExe.A.zip

zip encrypted

DETECTION

DETAILS

RELATIONS

COMMUNITY 1

Security Vendors' Analysis

NANO-Antivirus	1 Virus.Boot.AntiExe.bbif	Acronis (Static ML)	Undetected
Ad-Aware	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected

93861a8aa9a4f42489d029c64bc0599c208971891c70a9b2192b60e20c57d3bc

1/61

?

Community Score

1 security vendor and no sandboxes flagged this file as malicious

93861a8aa9a4f42489d029c64bc0599c208971891c70a9b2192b60e20c57d3bc

3.10 KB

2022-08-21 09:38:43 UTC

4 months ago

ZIP

AntiExe.A.zip

zip encrypted

DETECTION

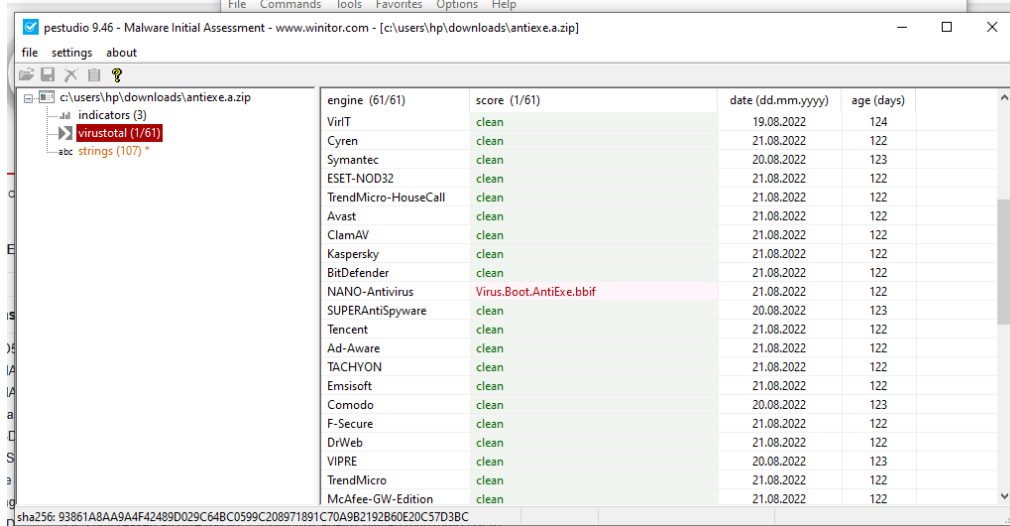
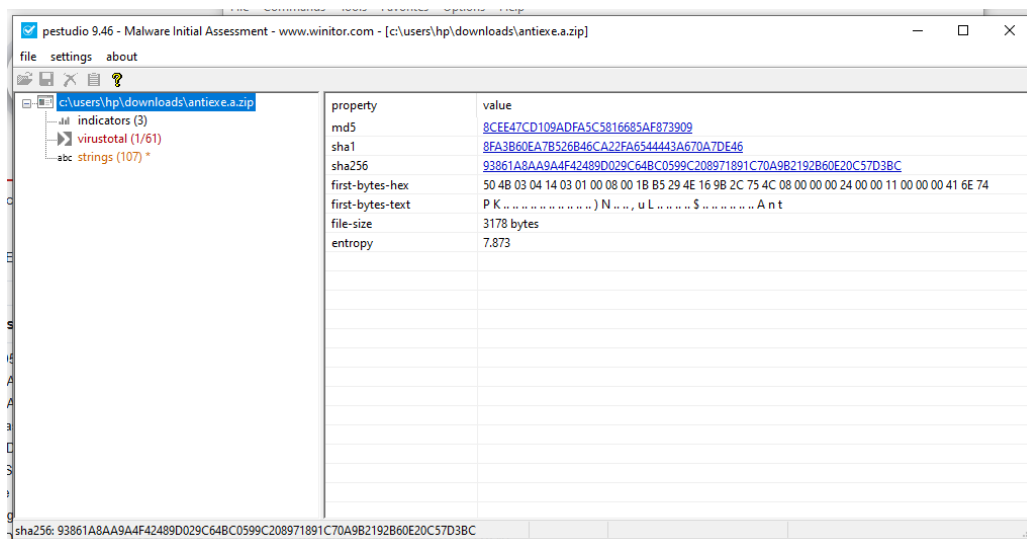
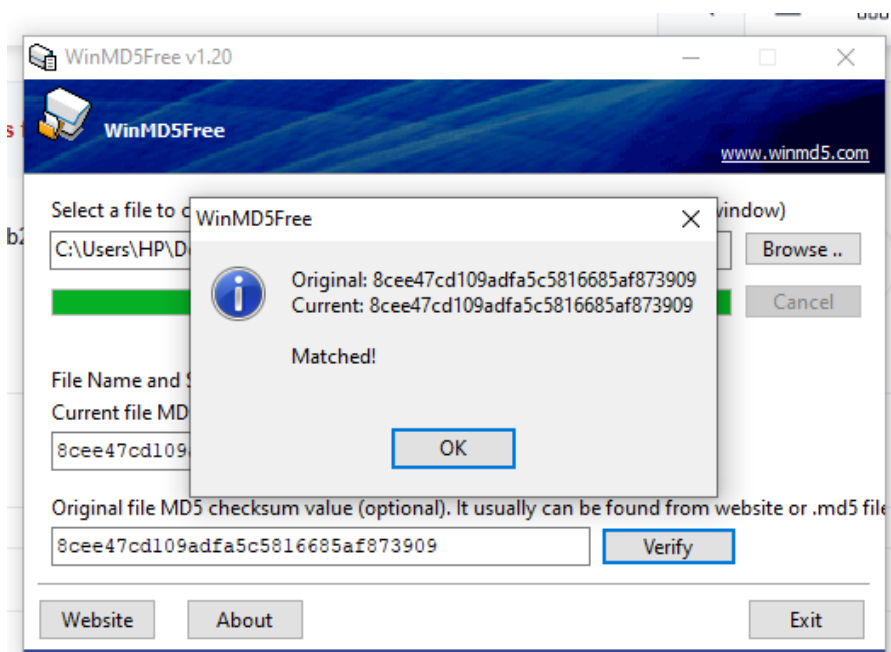
DETAILS

RELATIONS

COMMUNITY 1

Basic Properties

MD5	8cee47cd109adfa5c5816685af873909
SHA-1	8fa3b60ea7b526b46ca22fa654443a670a7de46
SHA-256	93861a8aa9a4f42489d029c64bc0599c208971891c70a9b2192b60e20c57d3bc
Vhash	81d0e3262f6c7b8b87bfaa5cbb12a737
SSDEEP	48:gl/WmtHjJP3dujAwZAJ4S66pMpIX8b/xd8AVXo4SPFD5IK7K3t9U:rHj0CAwZAJG6b/xdN1MD5lx7K3t6
TLSH	T1CD613B26898991A0DC697DF493EF0433E174E111AB55B14813FB3311B6BDB9C4CA9A9
File type	ZIP
Magic	Zip archive data, at least v2.0 to extract
TrID	ZIP compressed archive (80%) PrintFox/Pagefox bitmap (640x800) (20%)
File size	3.10 KB (3178 bytes)



- Sample 5

2

/ 61

Community Score

1

2 security vendors and no sandboxes flagged this file as malicious

c40d4c8da41f0f831d5f3987c9a819949586090e372e1749200c1ec42037f726

6.79 MB

2021-09-01 04:07:20 UTC

726

Neurevt.1.7.0.1.zip

zip

DETECTION

DETAILS

RELATIONS

COMMUNITY 1

Security Vendors' Analysis

Elastic	1 Malicious (high Confidence)	NANO-Antivirus	1 Trojan.Win32.Pincav.cqslmo
Ad-Aware	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected

2

/ 61

Community Score

1

2 security vendors and no sandboxes flagged this file as malicious

c40d4c8da41f0f831d5f3987c9a819949586090e372e1749200c1ec42037f726

6.79 MB

2021-09-01 04:07:20 UTC

726

Neurevt.1.7.0.1.zip

zip

DETECTION

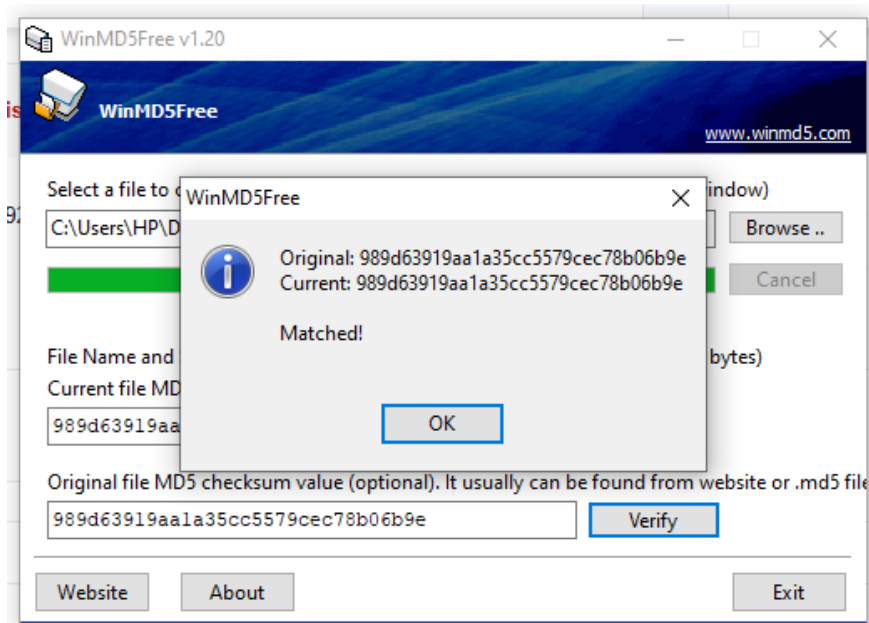
DETAILS

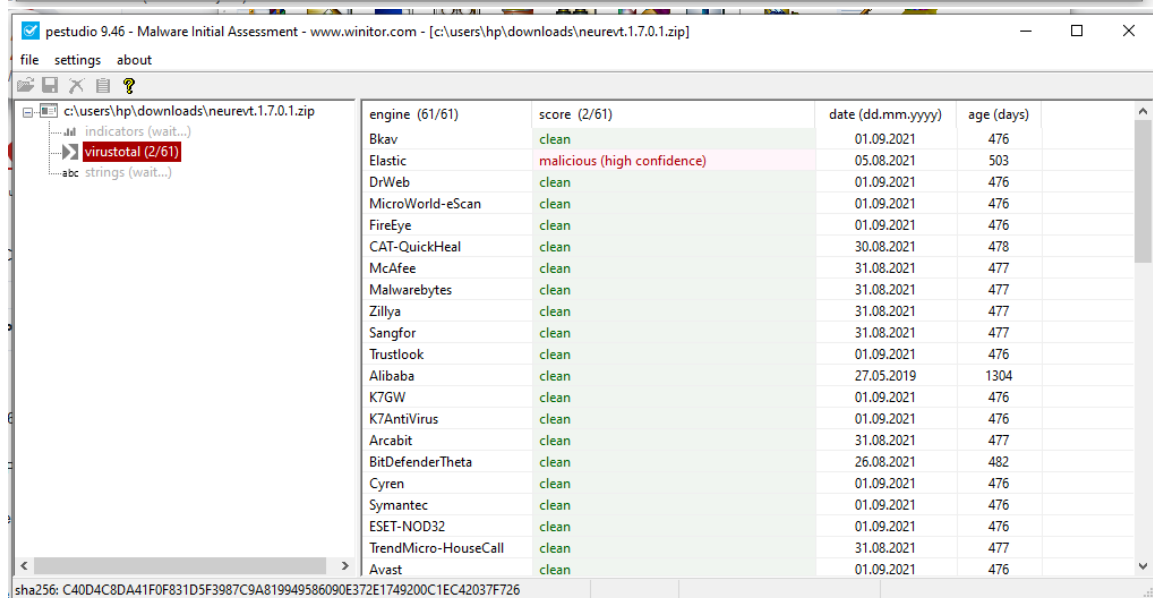
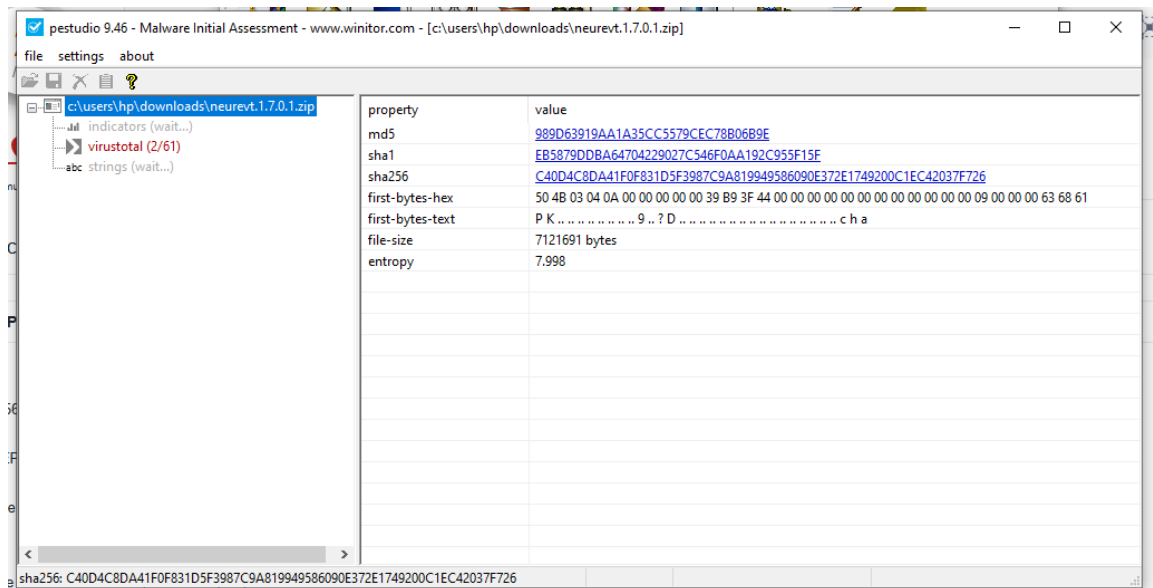
RELATIONS

COMMUNITY 1

Basic Properties

MD5	989d63919aa1a35cc5579cec78b06b9e
SHA-1	eb5879ddba64704229027c546f0aa192c955f15f
SHA-256	c40d4c8da41f0f831d5f3987c9a819949586090e372e1749200c1ec42037f726
Vhash	e2a161613f99935bf452147ee1bb9b51
SSDEEP	196608:6m9ec6PrH7sf553+soZ/FNhw3/CPiH0BuRu6hU8gA:b9eDrg5dIotFistUBwuluA
TLSH	T13076238DFAC205C9E5D71735783D4A1282E8F34486AD7935323F06ABBC91DD12B26B27
File type	ZIP
Magic	Zip archive data, at least v1.0 to extract
TrID	Mozilla Firefox browser extension (40%) Mozilla Archive Format (gen) (35%) ZIP compressed archive (20%) PrintFox/Pagefox bitmap (640x800) (5%)
File size	6.79 MB (7121691 bytes)
F-PROT packer	UTF-8, appended, docwrite, UTF-8, maxorder, eval





- Sample 6

44b7379c84733428bb4c6ee78af2537ffc1fc5ac7cd44373e9c8f349a1da6358

1 / 60

Community Score

1 security vendor and no sandboxes flagged this file as malicious

44b7379c84733428bb4c6ee78af2537ffc1fc5ac7cd44373e9c8f349a1da6358

12.80 KB

2021-08-30 12:49:55 UTC

Junkie.zip

zip encrypted

ZIP

DETECTION

DETAILS

RELATIONS

COMMUNITY 2

Security Vendors' Analysis

Alibaba	Virus:Win32/Junkie.39cfb542	Ad-Aware	Undetected
AhnLab-V3	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected
Avast	Undetected	Avast-Mobile	Undetected
Avira (no cloud)	Undetected	Baidu	Undetected
BitDefender	Undetected	BitDefenderTheta	Undetected

44b7379c84733428bb4c6ee78af2537ffc1fc5ac7cd44373e9c8f349a1da6358

1 / 60

Community Score

1 security vendor and no sandboxes flagged this file as malicious

44b7379c84733428bb4c6ee78af2537ffc1fc5ac7cd44373e9c8f349a1da6358

12.80 KB

2021-08-30 12:49:55 UTC

Junkie.zip

zip encrypted

DETECTION

DETAILS

RELATIONS

COMMUNITY 2

Basic Properties

MD5	b2736c97ab0b3bc23cbfa9e7d073e16d
SHA-1	1e9917c9a598e47220ae0439922de4456a986ea1
SHA-256	44b7379c84733428bb4c6ee78af2537ffc1fc5ac7cd44373e9c8f349a1da6358
Vhash	72f5d26de538edc42439908474edd99b
SSDEEP	384:ZDD9STniPcHJyMq0pXqXmOhJtOXiY6CF:pwWpO2OaraLvF
TLSH	T17C42AF92967C6D1AD8858BB8CBF9837630DC619B1503067384028DF98D8ED677A9C2DA
File type	ZIP
Magic	Zip archive data, at least v2.0 to extract
TrID	ZIP compressed archive (80%) PrintFox/Pagefox bitmap (640x800) (20%)
File size	12.80 KB (13104 bytes)

