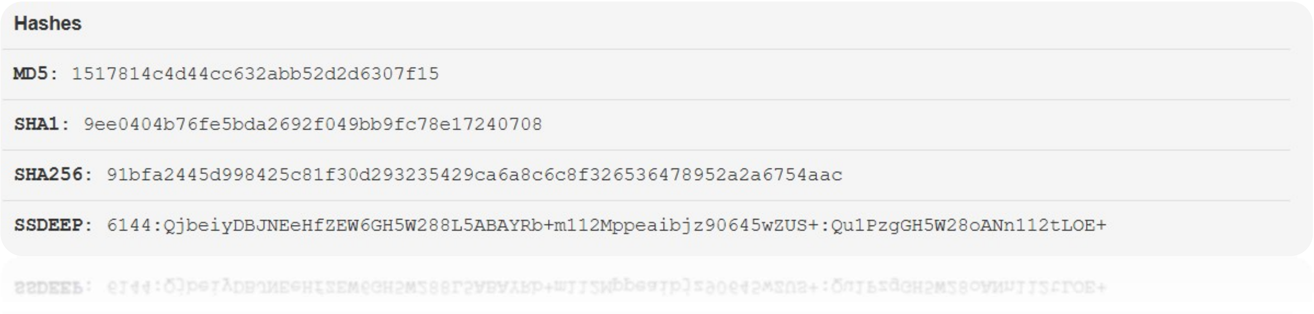
MALWARE ANALYSIS REPORT

1. Basic Information

Field	Value
Malware Name/Hash	91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754aac
Type	Trojan
File Name	WEXTRACT.EXE
File Size	420.00 KB
Date of Analysis	(29-07-2025)
Analyst Name	Suryansh Pandey
Intern Id	110
Platform Targeted	Windows
Sample Source	http://june12.5gbfree.com/fszz/gud.exe



Hashes

MD5: 1517814c4d44cc632abb52d2d6307f15

SHA1: 9ee0404b76fe5bda2692f049bb9fc78e17240708

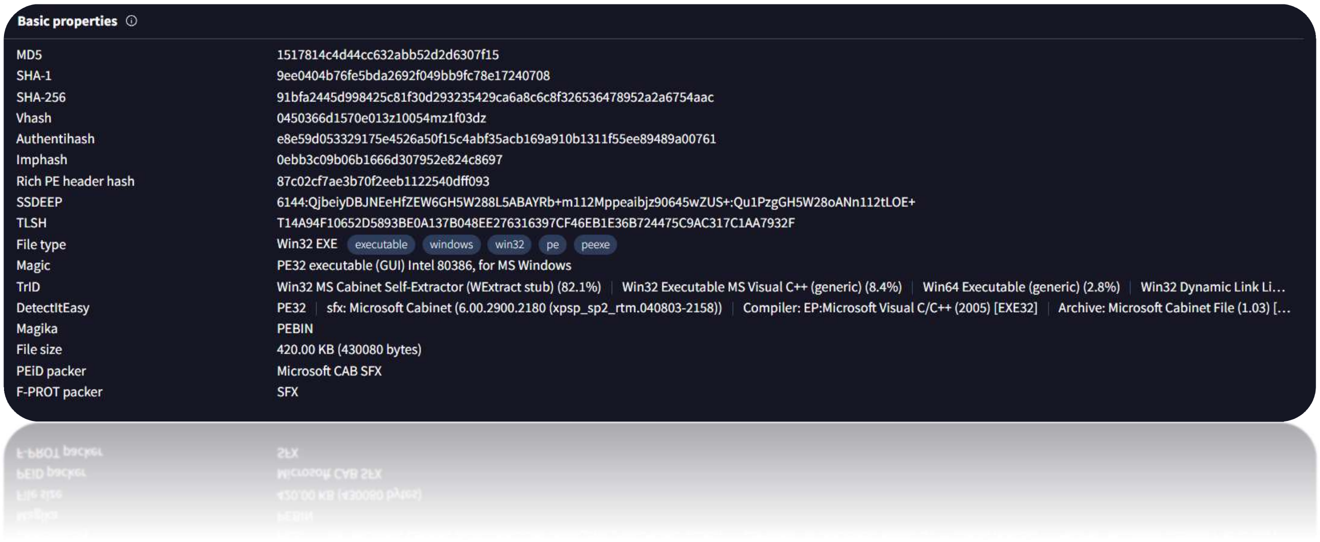
SHA256: 91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754aac

SSDEEP: 6144:QjbeiyDBJNEeHfZEW6GH5W288L5ABAYRb+m112Mppeaibjz90645wZUS+:Qu1PzgGH5W28oANn112tLOE+

2. Static Analysis

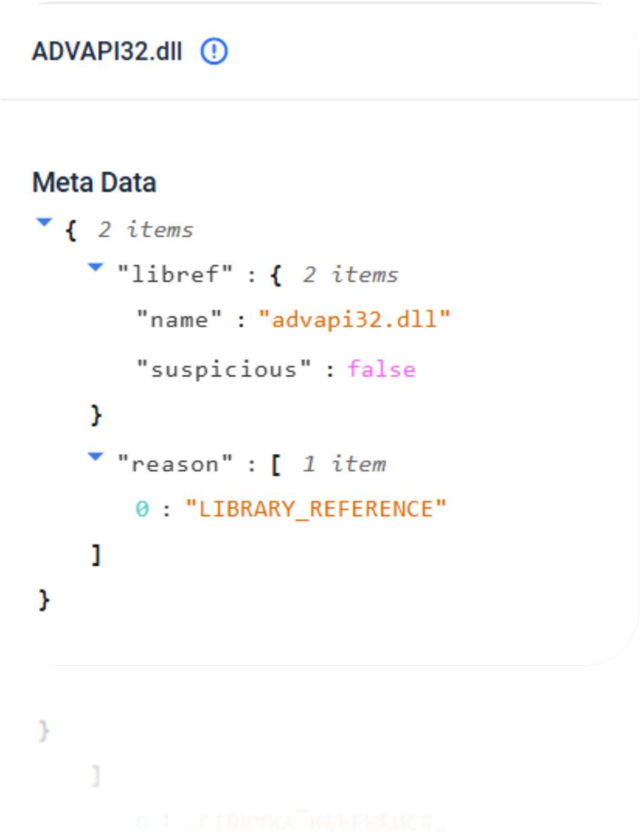
Feature	Details
File Type	Win32 EXE
File Hashes	MD5: 1517814c4d44cc632abb52d2d6307f15 SHA-1: 9ee0404b76fe5bda2692f049bb9fc78e17240708
Strings Found	(offset 00039230: 1A 3B 2A BE 14 42 C5 E7 etc)
PEiD Packer	Microsoft Visual C++ SPx

Feature	Details
Located IPs	3.131.193.27
Sections Info	(.text, .exe, .vir)
Digital Signature	Unsigned
API reference	ExitWindowsEx@USER32.dll
YARA Rules	http://www.hexacorn.com/blog/2012/10/14/random-stats-from-1-2m-samples-pe-section-names/



Basic properties ⓘ

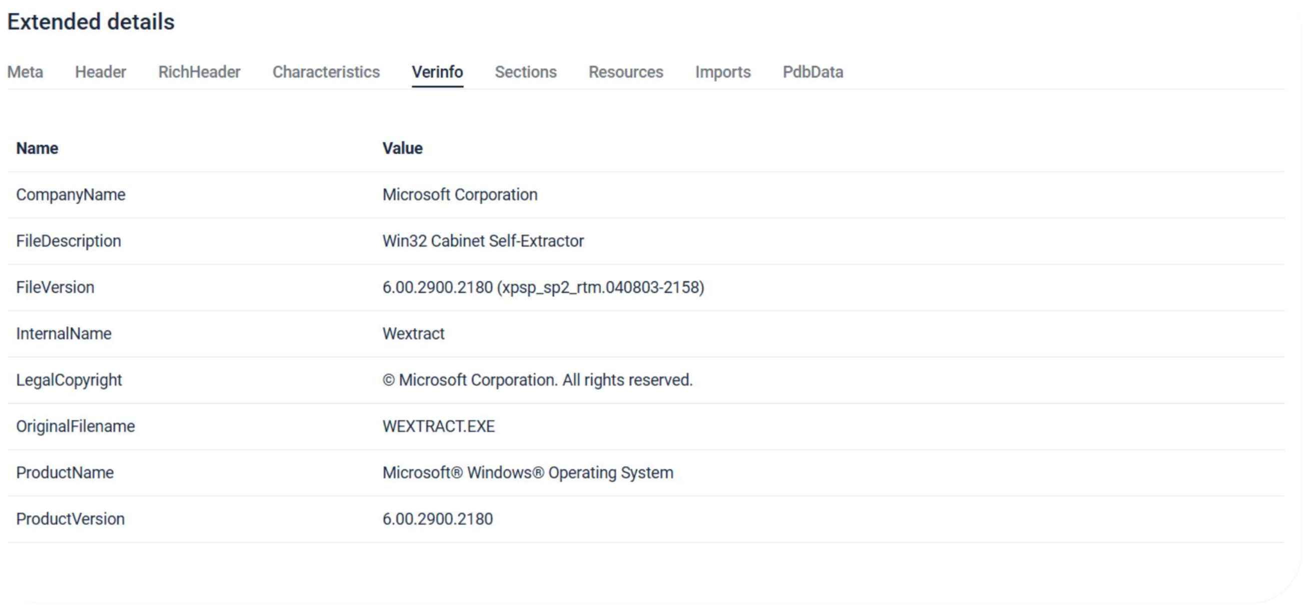
MD5	1517814c4d44cc632abb52d2d6307f15
SHA-1	9ee0404b76fe5bda2692f049bb9fc78e17240708
SHA-256	91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754aac
Vhash	0450366d1570e013z10054mz1f03dz
Authentihash	e8e59d053329175e4526a50f15c4abf35acb169a910b1311f55ee89489a00761
Imphash	0ebb3c09b06b1666d307952e824c8697
Rich PE header hash	87c02cf7ae3b70f2eeb1122540dff093
SSDEEP	6144:QjbeiyDBJNEeHfZEW6GH5W288L5ABAYRb+m112Mppeaibjz90645wZUS+:Qu1PzgGH5W28oANn112tLOE+
TLSH	T14A94F10652D5893BE0A137B048EE276316397CF46EB1E36B724475C9AC317C1AA7932F
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 MS Cabinet Self-Extractor (WExtract stub) (82.1%) | Win32 Executable MS Visual C++ (generic) (8.4%) | Win64 Executable (generic) (2.8%) | Win32 Dynamic Link Li…
DetectItEasy	PE32 | sfx: Microsoft Cabinet (6.00.2900.2180 (xpsp_sp2_rtm.040803-2158)) | Compiler: EP:Microsoft Visual C/C++ (2005) [EXE32] | Archive: Microsoft Cabinet File (1.03) […
Magika	PEBIN
File size	420.00 KB (430080 bytes)
PEiD packer	Microsoft CAB SFX
F-PROT packer	SFX



ADVAPI32.dll ⓘ

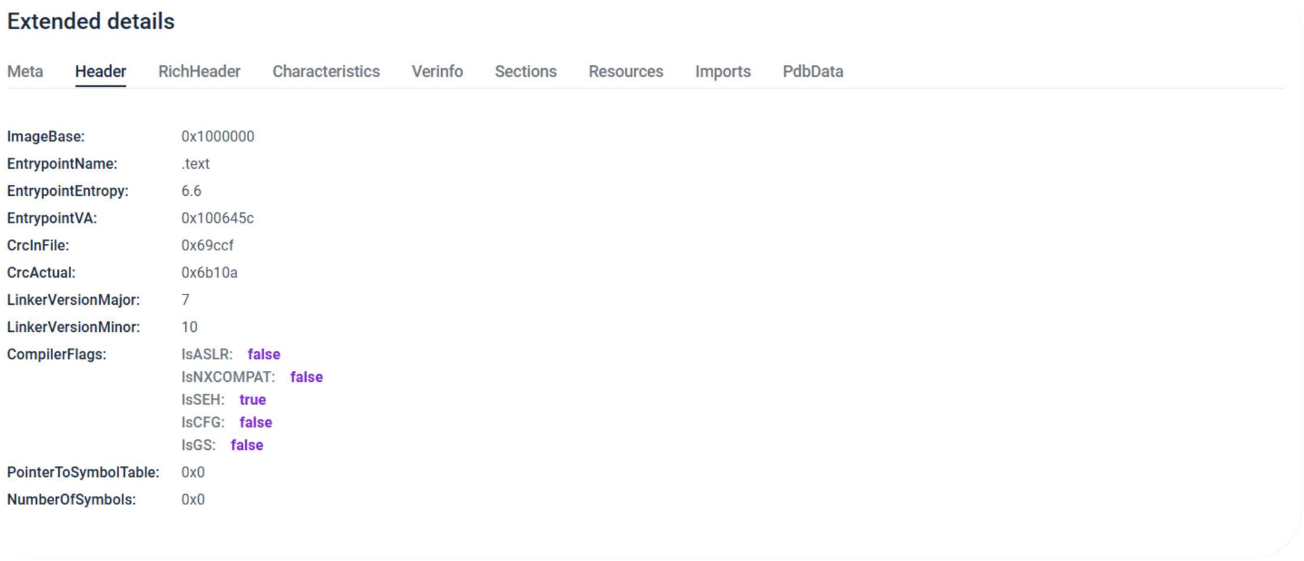
Meta Data

```
{ 2 items
    "libref" : { 2 items
        "name" : "advapi32.dll"
        "suspicious" : false
    }
    "reason" : [ 1 item
        0 : "LIBRARY_REFERENCE"
    ]
}
```



Extended details

Name	Value
CompanyName	Microsoft Corporation
FileDescription	Win32 Cabinet Self-Extractor
FileVersion	6.00.2900.2180 (xpsp_sp2_rtm.040803-2158)
InternalName	Wextract
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	WEXTRACT.EXE
ProductName	Microsoft® Windows® Operating System
ProductVersion	6.00.2900.2180

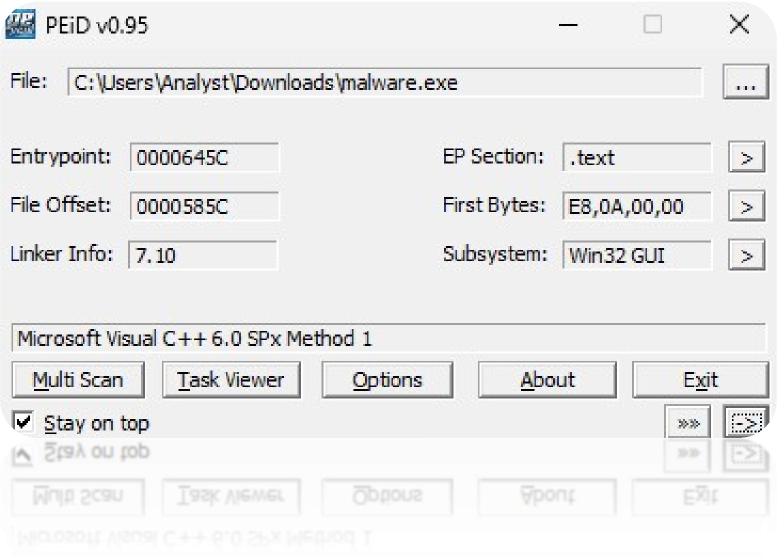


Extended details

ImageBase:	0x1000000
EntrypointName:	.text
EntrypointEntropy:	6.6
EntrypointVA:	0x100645c
CrcInFile:	0x69ccf
CrcActual:	0x6b10a
LinkerVersionMajor:	7
LinkerVersionMinor:	10
CompilerFlags:	IsASLR: **false** IsNXCOMPAT: **false** IsSEH: **true** IsCFG: **false** IsGS: **false**
PointerToSymbolTable:	0x0
NumberOfSymbols:	0x0

# PEid Tools (Screenshots):

1. Basic Information



PEiD v0.95

File: C:\Users\Analyst\Downloads\malware.exe

Entrypoint: 0000645C

EP Section: .text

File Offset: 0000585C

First Bytes: E8,0A,00,00

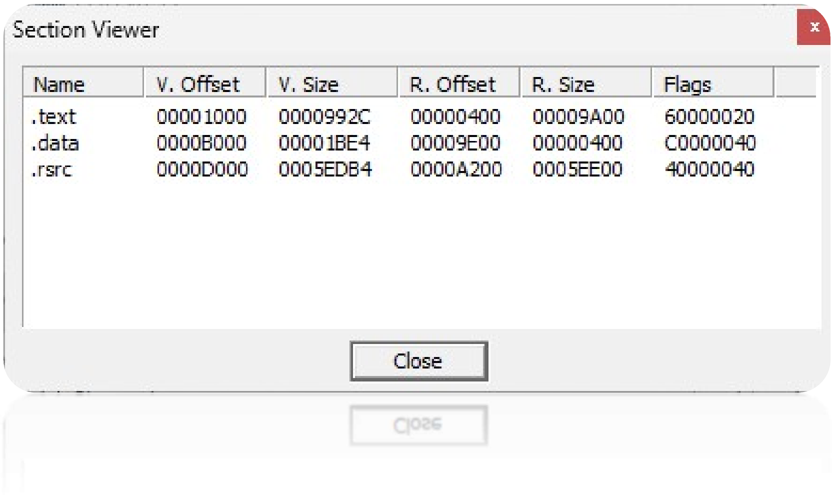
Linker Info: 7.10

Subsystem: Win32 GUI

Microsoft Visual C++ 6.0 SPx Method 1

☑ Stay on top

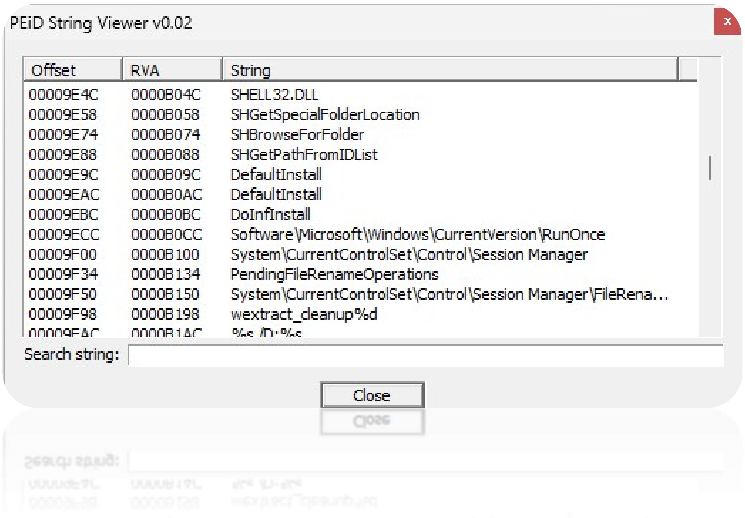
2. EP Section



Section Viewer

Name	V. Offset	V. Size	R. Offset	R. Size	Flags
.text	00001000	0000992C	00000400	00009A00	60000020
.data	0000B000	00001BE4	00009E00	00000400	C0000040
.rsrc	0000D000	0005EDB4	0000A200	0005EE00	40000040

3. Strings

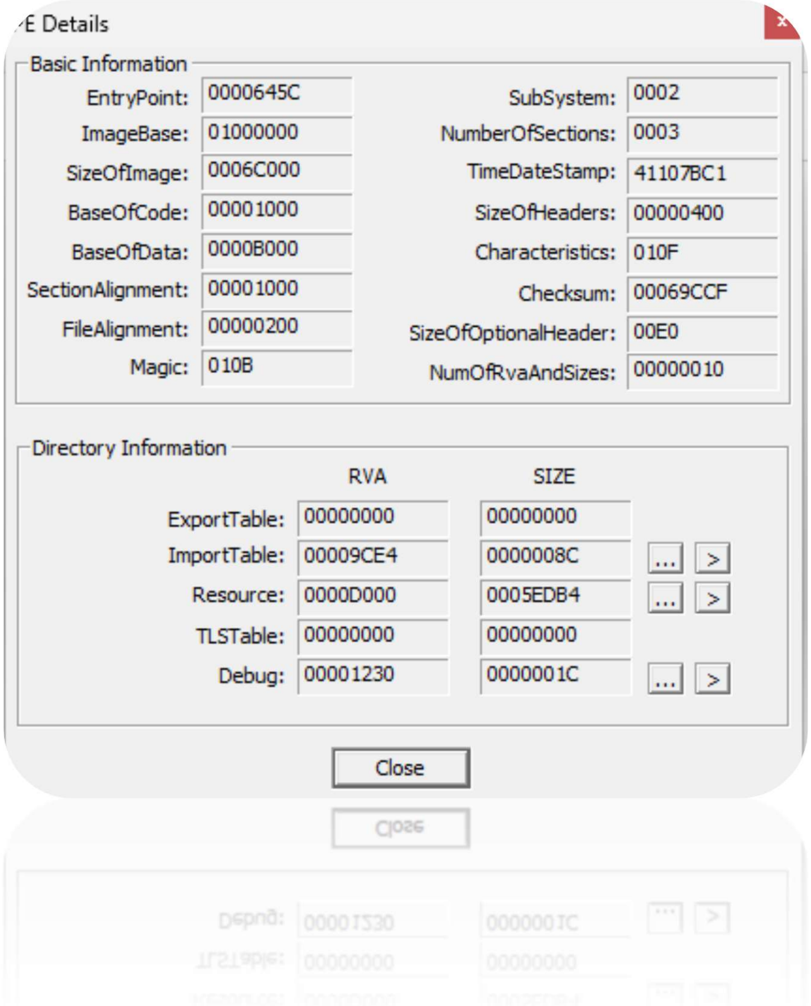


PEiD String Viewer v0.02

Offset	RVA	String
00009E4C	0000B04C	SHELL32.DLL
00009E58	0000B058	SHGetSpecialFolderLocation
00009E74	0000B074	SHBrowseForFolder
00009E88	0000B088	SHGetPathFromIDList
00009E9C	0000B09C	DefaultInstall
00009EAC	0000B0AC	DefaultInstall
00009EBC	0000B0BC	DoInfInstall
00009ECC	0000B0CC	Software\Microsoft\Windows\CurrentVersion\RunOnce
00009F00	0000B100	System\CurrentControlSet\Control\Session Manager
00009F34	0000B134	PendingFileRenameOperations
00009F50	0000B150	System\CurrentControlSet\Control\Session Manager\FileRena...
00009F98	0000B198	wextract_cleanup%d
00009FAC	0000B1AC	%s /D:%s

Search string:

4. PE Details



Basic Information

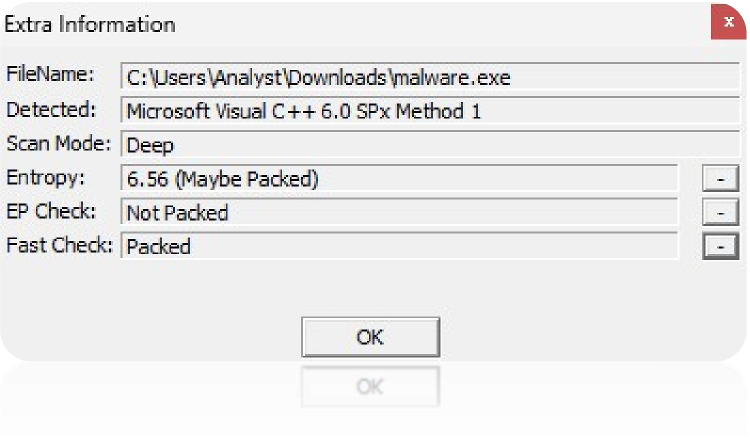
EntryPoint: 0000645C
ImageBase: 01000000
SizeOfImage: 0006C000
BaseOfCode: 00001000
BaseOfData: 0000B000
SectionAlignment: 00001000
FileAlignment: 00000200
Magic: 010B

SubSystem: 0002
NumberOfSections: 0003
TimeDateStamp: 41107BC1
SizeOfHeaders: 00000400
Characteristics: 010F
Checksum: 00069CCF
SizeOfOptionalHeader: 00E0
NumOfRvaAndSizes: 00000010

Directory Information

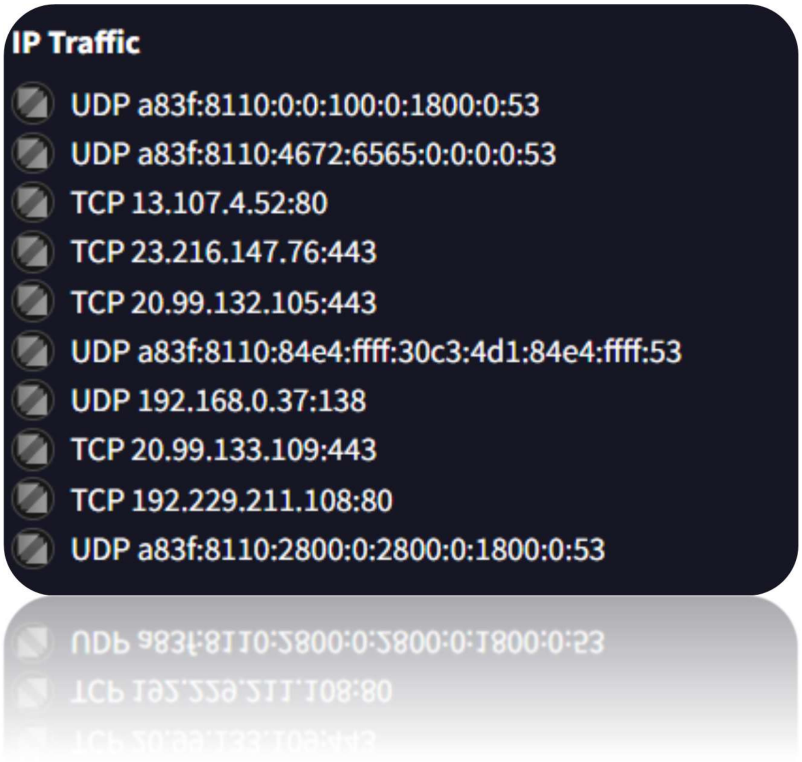
	RVA	SIZE
ExportTable:	00000000	00000000
ImportTable:	00009CE4	0000008C
Resource:	0000D000	0005EDB4
TLSTable:	00000000	00000000
Debug:	00001230	0000001C

5. Extra Information



FileName: C:\Users\Analyst\Downloads\malware.exe
Detected: Microsoft Visual C++ 6.0 SPx Method 1
Scan Mode: Deep
Entropy: 6.56 (Maybe Packed)
EP Check: Not Packed
Fast Check: Packed

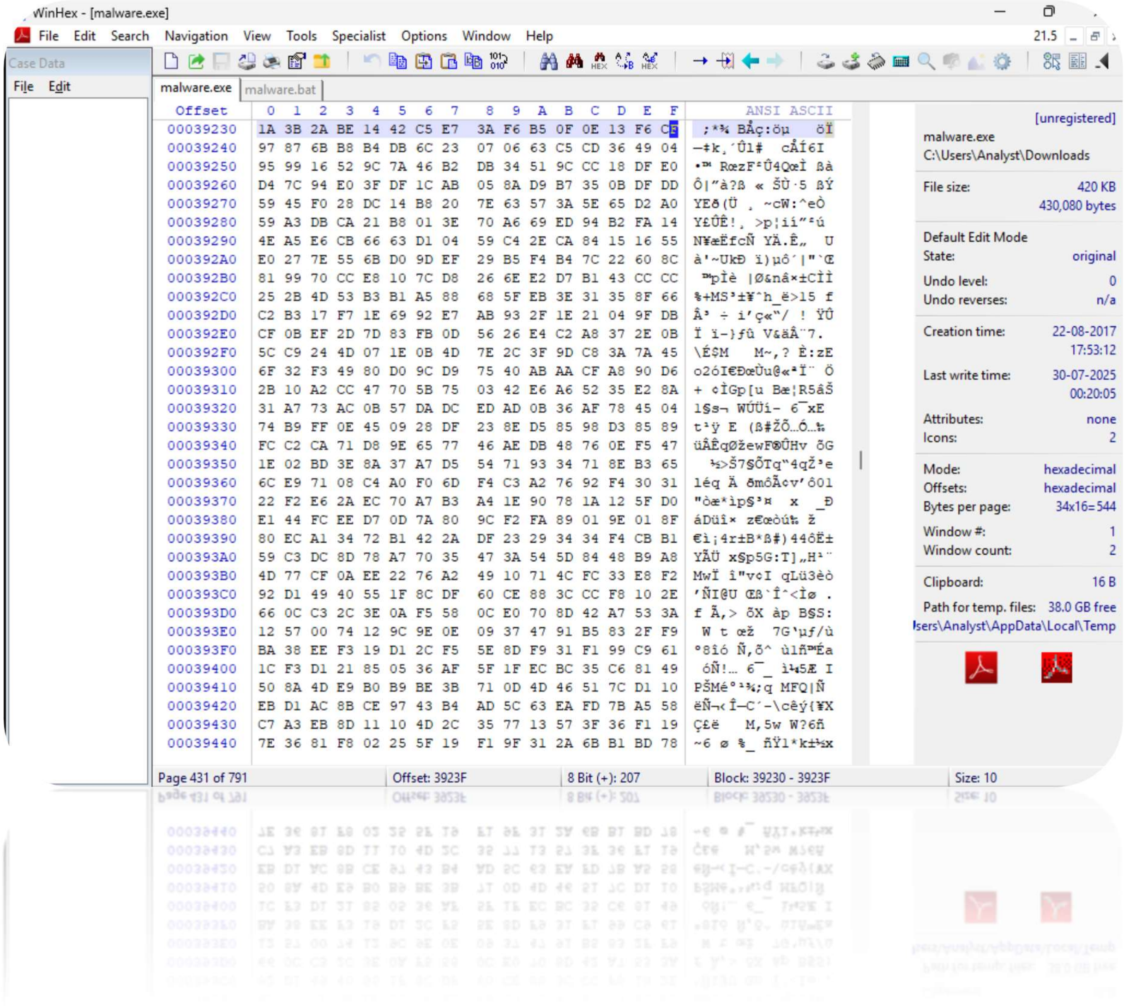
# IP Traffic:



IP Traffic

- UDP a83f:8110:0:0:100:0:1800:0:53
- UDP a83f:8110:4672:6565:0:0:0:0:53
- TCP 13.107.4.52:80
- TCP 23.216.147.76:443
- TCP 20.99.132.105:443
- UDP a83f:8110:84e4:ffff:30c3:4d1:84e4:ffff:53
- UDP 192.168.0.37:138
- TCP 20.99.133.109:443
- TCP 192.229.211.108:80
- UDP a83f:8110:2800:0:2800:0:1800:0:53

# WinHex Tool (Screenshot):



```
  Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F        ANSI ASCII
00039230   1A 3B 2A BE 14 42 C5 E7  3A F6 B5 0F 0E 13 F6 CF    ;*¾ BÅç:öµ   öÏ
00039240   97 87 6B B8 B4 DB 6C 23  07 06 63 C5 CD 36 49 04   —‡k¸´Û1#  cÅÍ6I
00039250   95 99 16 52 9C 7A 46 B2  DB 34 51 9C CC 18 DF E0   •™ RœzF²Û4QœÌ ßà
00039260   D4 7C 94 E0 3F DF 1C AB  05 8A D9 B7 35 0B DF DD   Ô|"à?ß « ŠÙ·5 ßÝ
00039270   59 45 F0 28 DC 14 B8 20  7E 63 57 3A 5E 65 D2 A0   YEð(Ü ¸ ~cW:^eÒ
00039280   59 A3 DB CA 21 B8 01 3E  70 A6 69 ED 94 B2 FA 14   Y£ÛÊ!¸ >p¦ií"²ú
00039290   4E A5 E6 CB 66 63 D1 04  59 C4 2E CA 84 15 16 55   N¥æËfcÑ YÄ.Ê„  U
000392A0   E0 27 7E 55 6B D0 9D EF  29 B5 F4 B4 7C 22 60 8C   à'~UkÐ ï)µô´|"`Œ
000392B0   81 99 70 CC E8 10 7C D8  26 6E E2 D7 B1 43 CC CC    ™pÌè |Ø&nâ×±CÌÌ
000392C0   25 2B 4D 53 B3 B1 A5 88  68 5F EB 3E 31 35 8F 66   %+MS³±¥ˆh_ë>15 f
000392D0   C2 B3 17 F7 1E 69 92 E7  AB 93 2F 1E 21 04 9F DB   Â³ ÷ i'ç«"/ ! ŸÛ
000392E0   CF 0B EF 2D 7D 83 FB 0D  56 26 E4 C2 A8 37 2E 0B   Ï ï-}fû V&äÂ¨7.
000392F0   5C C9 24 4D 07 1E 0B 4D  7E 2C 3F 9D C8 3A 7A 45   \É$M   M~,? È:zE
00039300   6F 32 F3 49 80 D0 9C D9  75 40 AB AA CF A8 90 D6   o2óI€ÐœÙu@«ªÏ¨ Ö
00039310   2B 10 A2 CC 47 70 5B 75  03 42 E6 A6 52 35 E2 8A   + ¢ÌGp[u Bæ¦R5âŠ
00039320   31 A7 73 AC 0B 57 DA DC  ED AD 0B 36 AF 78 45 04   1§s¬ WÚÜí- 6¯xE
00039330   74 B9 FF 0E 45 09 28 DF  23 8E D5 85 98 D3 85 89   t¹ÿ E (ß#ŽÕ…Ó…‰
00039340   FC C2 CA 71 D8 9E 65 77  46 AE DB 48 76 0E F5 47   üÂÊqØžewF®ÛHv õG
00039350   1E 02 BD 3E 8A 37 A7 D5  54 71 93 34 71 8E B3 65     ½>Š7§ÕTq"4qŽ³e
00039360   6C E9 71 08 C4 A0 F0 6D  F4 C3 A2 76 92 F4 30 31   léq Ä ðmôÃ¢v'ô01
00039370   22 F2 E6 2A EC 70 A7 B3  A4 1E 90 78 1A 12 5F D0   "òæ*ìp§³¤  x  _Ð
00039380   E1 44 FC EE D7 0D 7A 80  9C F2 FA 89 01 9E 01 8F   áDüî× z€œòú‰ ž
00039390   80 EC A1 34 72 B1 42 2A  DF 23 29 34 34 F4 CB B1   €ì¡4r±B*ß#)44ôË±
000393A0   59 C3 DC 8D 78 A7 70 35  47 3A 54 5D 84 48 B9 A8   YÃÜ x§p5G:T]„H¹¨
000393B0   4D 77 CF 0A EE 22 76 A2  49 10 71 4C FC 33 E8 F2   MwÏ î"v¢I qLü3èò
000393C0   92 D1 49 40 55 1F 8C DF  60 CE 88 3C CC F8 10 2E   'ÑI@U Œß`Î^<Ìø .
000393D0   66 0C C3 2C 3E 0A F5 58  0C E0 70 8D 42 A7 53 3A   f Ã,> õX àp B§S:
000393E0   12 57 00 74 12 9C 9E 0E  09 37 47 91 B5 83 2F F9    W t œž  7G'µf/ù
000393F0   BA 38 EE F3 19 D1 2C F5  5E 8D F9 31 F1 99 C9 61   º8îó Ñ,õ^ ù1ñ™Éa
00039400   1C F3 D1 21 85 05 36 AF  5F 1F EC BC 35 C6 81 49    óÑ!… 6¯_ ì¼5Æ I
00039410   50 8A 4D E9 B0 B9 BE 3B  71 0D 4D 46 51 7C D1 10   PŠMé°¹¾;q MFQ|Ñ
00039420   EB D1 AC 8B CE 97 43 B4  AD 5C 63 EA FD 7B A5 58   ëÑ¬‹Î—C´-\cêý{¥X
00039430   C7 A3 EB 8D 11 10 4D 2C  35 77 13 57 3F 36 F1 19   Ç£ë   M,5w W?6ñ
00039440   7E 36 81 F8 02 25 5F 19  F1 9F 31 2A 6B B1 BD 78   ~6 ø %_ ñŸ1*k±½x
```

[unregistered]

malware.exe
C:\Users\Analyst\Downloads

File size: 420 KB
430,080 bytes

Default Edit Mode
State: original

Undo level: 0
Undo reverses: n/a

Creation time: 22-08-2017
17:53:12

Last write time: 30-07-2025
00:20:05

Attributes: none
Icons: 2

Mode: hexadecimal
Offsets: hexadecimal
Bytes per page: 34x16=544

Window #: 1
Window count: 2

Clipboard: 16 B

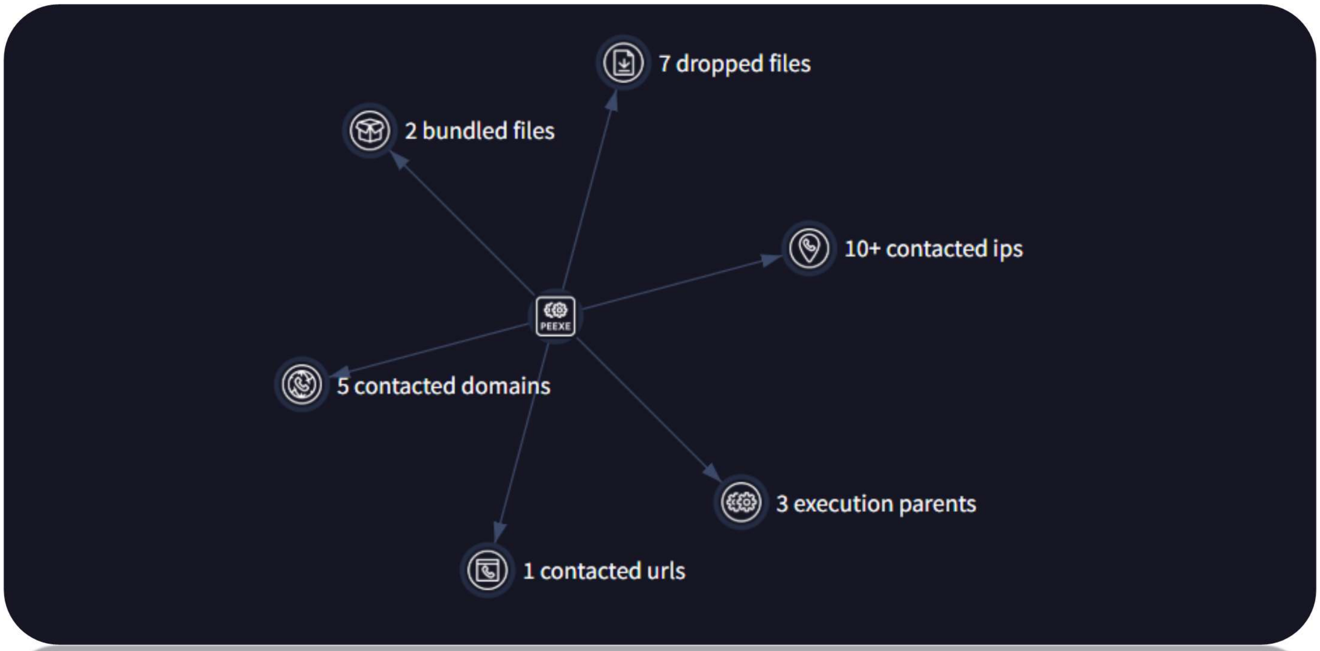
Path for temp. files: 38.0 GB free
Isers\Analyst\AppData\Local\Temp

Page 431 of 791 | Offset: 3923F | 8 Bit (+): 207 | Block: 39230 - 3923F | Size: 10

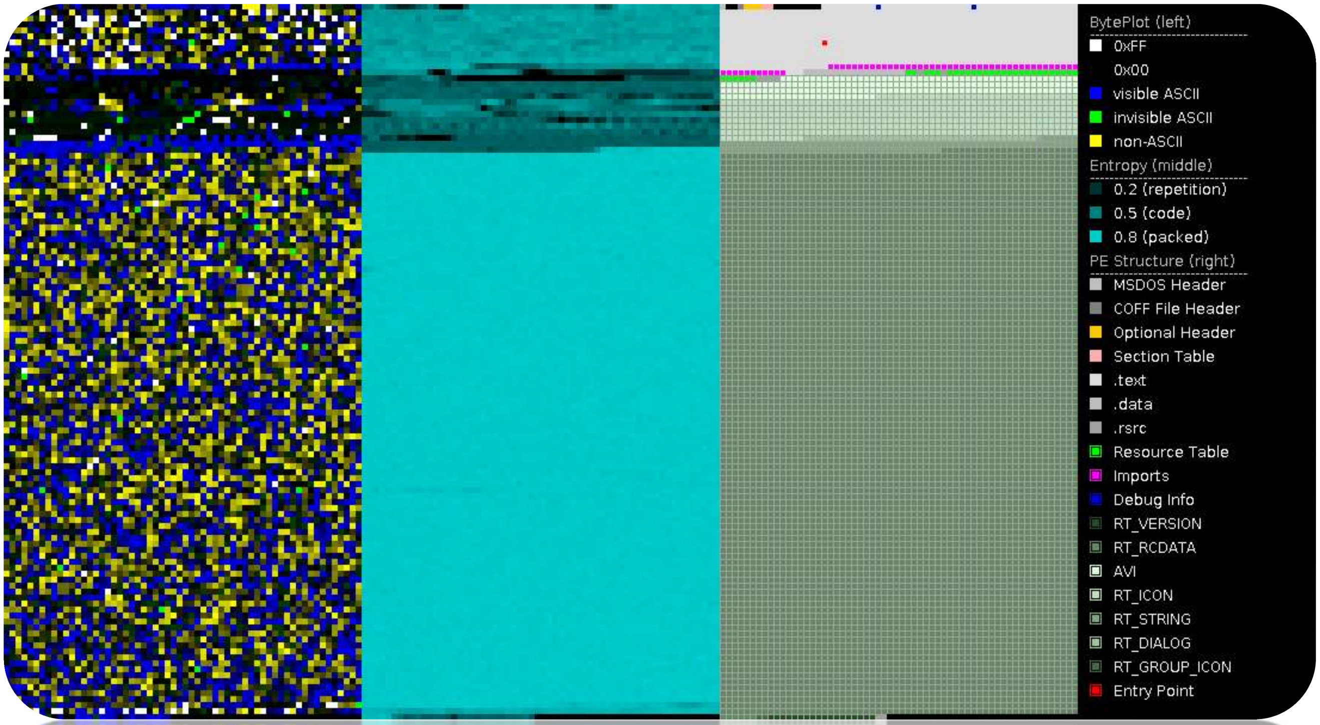
Capabilities:

Executable	packaged as an IExpress self-extracting archive extract resource via kernel32 functions
Data-Manipulation	encode data using XOR
Linking	link function at runtime on Windows
Persistence	persist via Run registry key
Host-Interaction	get file version info create process on Windows set registry value shutdown system delete registry value set file attributes get system information on Windows compare security identifiers query or enumerate registry key enumerate files recursively set current directory terminate process get disk size get disk information delete file etc.

# Graph:



Visualization Input File (PortEx):


BytePlot (left)
0xFF
0x00
visible ASCII
invisible ASCII
non-ASCII
Entropy (middle)
0.2 (repetition)
0.5 (code)
0.8 (packed)
PE Structure (right)
MSDOS Header
COFF File Header
Optional Header
Section Table
.text
.data
.rsrc
Resource Table
Imports
Debug Info
RT_VERSION
RT_RCDATA
AVI
RT_ICON
RT_STRING
RT_DIALOG
RT_GROUP_ICON
Entry Point