Static Analysis

1. Virus Total Analysis

Hash Analysis

- File Hash: [Insert MD5, SHA-1, SHA-256 hash value]
  - MD5: 1aa4e9631a1ee57420591f855d7cae16
  - SHA-1: 7f1a688ecc4b5f8276e538539c9bb03ade63b9f2
  - SHA-256:e7c1262970690b91483b2ad5ccc69a4718976c932274c82c9c3481efd20a1b9d
- Method of hash acquisition: [Describe process]
  - Found on VirusTotal and confirmed with Detect-It-Easy
- [Link to VirusTotal results]
  - https://www.virustotal.com/gui/file/e7c1262970690b91483b2ad5ccc69a4718976c932274c82c9c3481efd20a1b9d/details

Vendor Analysis

- Number of vendors flagging as malicious: 27/69
- Analysis of vendor results:
  - [Discuss patterns in detection]
    - spreader
    - detect-debug-environment
  - [Common malware names identified]
    - Loader
    - Trojan
    - Dropper
    - Win32
    - Kryptik
  - [Notable vendor disagreements]

File History

- [Discussion of file age]
  - Creation Time: 2020-10-23 10:31:13 UTC
  - First Submission: 2025-04-17 20:50:27 UTC

Community Score

- [Link to your VirusTotal community contribution]
  - https://www.virustotal.com/gui/file/e7c1262970690b91483b2ad5ccc69a4718976c932274c82c9c3481efd20a1b9d/community
- Summary of initial findings posted to the community:

    - This is a highly suspicious and malicious file that uses packing, obfuscation, and steganography to hide its true functionality. The use of suspicious BMP files, API calls associated with system manipulation and file destruction suggest that this malware is designed to deceive users and evade detection. It has the potential to operate as a loader or dropper, delivering additional payloads that may steal data, destroy files, or facilitate remote control.

2. Detect It Easy (DIE) Analysis

File information

- File type:PE32
- Architecture: i386
- Compiler: EP:Microsoft Visual C/C++ (2008-2010) [EXE32]
- File names:
    - Week12.exe
    - 2025-04-18_1aa4e9631a1ee57420591f855d7cae16_amadey_elex_rhadamanthys_smoke-loader

Memory Map Analysis

- Section breakdown:
    - Sections
    - .text
        - Raw size: 748544
        - Entropy: 6.79
        - Permissions:Read, Execute
        - packed
    - .rdata
        - Raw size: 141312
        - Entropy: 4.67
        - Permissions:Read
        - unpacked
    - .data
        - Raw size: 24576
        - Entropy: 4.36
        - Permissions: Read, Write
        - unpacked
    - .rsrc

        - Raw size: 7933440
        - Entropy: 7.32
        - Permissions:Read
        - packed
- Notable findings:
    - [Unusual section permissions]
        - .text has RE permissions and .data has RW permissions
    - [Section size anomalies]
        - .rsrc is very large
        - .text is relatively large

String Analysis

Network Activity/URLs:

- http://s.360safe.com/safei18n/
- ins.htm?mid=%s&ver=%s&lan=%s&os=%s&ch=%s&sch=%s
- uni.htm?mid=%s&ver=%s&lan=%s&os=%s&ch=%s&sch=%s&cpu=%s&ram=%s&protect=%s&ttl=%s&avp=%s&scan=%s&moni=%s
- uni_act.htm?
- feature.htm?id=%d&
- off_vdb.htm?dt=%s&dv=%s&prod=%s&mid=%s&ver=%s&lan=%s&os=%s&ch=%s
- pmode.htm?m=%s&cs=%s&
- err.htm?mod=sp&code=10&mid=%s&ver=%s&lan=%s&os=%s&ch=%s&rn=%s[1]
- checkup.htm?a=%s&
- ws_ff.htm?s=%s&
- account.htm?
- toolbox.htm?id=%d&
- toolbox.htm?id=%d&status=%d&
- wd.htm
- filemon.htm
- src.htm
- bru.htm

Command Lines:

- /elevated
- "%s%s" \elevated
- "%s\%s"
- /shredfilelist="

Suspicious API calls

- CreateProcessW
- DeleteFileW
- MoveFileW
- MoveFileA
- RemoveDirectoryW
- SetFileAttributesW
- DeviceIoControl
- AddDllDirectory
- Wow64DisableWow64FsRedirection
- Wow64RevertWow64FsRedirection
- FsForceKill
- BRegDeleteKeyExW
- BRegDeleteKeyEx
- BRegDeleteKeyW
- BRegDeleteKey
- BRegSetValueExW
- BRegSetValueEx
- FSUnlockAll
- FSMoveFileExW
- FSMoveFileExA
- FSMoveFileW
- FSMoveFileA
- FSCopyFileW
- FSCopyFile
- FSDeleteFileW
- FSDeleteFile
- FSWriteFile
- FSReadFile
- SetWindowsHookExW
- UnhookWindowsHookEx
- keybd_event
- SetEnvironmentVariableW
- SetEnvironmentVariableA
- ShellExecuteW
- ShellExecuteExW
- CoCreateInstance
- CoGetClassObject
- VirtualFree
- VirtualAlloc
- CreateThread

- RtlUnwind

Suspicious Strings (General):

- \\.\Scsi%d:
- \\.\%s
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards
- %s:%08x
- GenuineIntel
- GenuineIotel
- Software\360Safe\Liveup
- mid_old
- Mid2Failed
- QHVer.dll
- 360base.dll
- 360conf.dll
- 360NetBase.dll
- sites.dll
- 360TSCommon.dll
- QHFileSmasher.exe
- 360CloudEnterprise
- 360CloudUI
- \config\newui\themes\default
- \config\newui\themes\default\360InternationSafe
- \config\newui\themes\
- FSTurnOffRedirection
- SOFTWARE\360Safe\softmgr
- BypassMetroDesktop
- CFileSmasherLog

Entropy Analysis

- Overall entropy score: 7.35626
- Section-specific entropy:
  - .text
    - Entropy: 6.79
    - Packed
  - .rsrc
    - Entropy: 7.32
    - packed
- Packing analysis:

    - Packed
    - I used Detect-It-Easy extractor to unpack executable and it unpacked to reveal a ZIP file and some images. I unzipped the zip file and I found a very large suspicious .bmp file as well as two empty folders called “image” which is suspicious
    -

4. Disassembly Analysis
    - I analyzed the .bmp file that is 7.3MB, which is very large. I found that it has 3 exports that appear suspicious. These include:
        - IRQ
        - NMS
        - RES
    - I found a lot of very suspicious strings, they were all strings of random letters and numbers and symbols
        - TOOTESUCKTHEFTUBCEG
        - Suck the ?
    - It has a bit depth of 51, which is not standard
    - I used binwalk and found out the following information:
        - `┌──(kali㉿kali)-[~]`
        - `└─$ cd Desktop`
        - `┌──(kali㉿kali)-[~/Desktop]`
        - `└─$ binwalk Week12.exe.0013b430_00730236.bmp`
        -
        - `DECIMAL       HEXADECIMAL     DESCRIPTION`
        - `--------------------------------------------------------------------------------`
        - `0             0x0             PC bitmap, Windows 3.x format,, 942397 x 2 x 51`
        - `4631688       0x46AC88        JBOOT STAG header, image id: 6, timestamp 0x4B432631, image size: 624308758 bytes, image JBOOT checksum: 0x372A, header JBOOT checksum: 0x2031`
        - `5005144       0x4C5F58        JBOOT STAG header, image id: 0, timestamp 0x236D2432, image size: 522780978`

bytes, image JBOOT checksum: 0x333A, header JBOOT checksum: 0x6337

    - 5163789   0x4ECB0D   JBOOT STAG header, image id: 10, timestamp 0x3A562B0F, image size: 1446795789 bytes, image JBOOT checksum: 0x743A, header JBOOT checksum: 0x4A2A
    - 5702051   0x5701A3   LANCOM OEM file
    - 5787184   0x584E30   JBOOT STAG header, image id: 0, timestamp 0x136D2432, image size: 741637220 bytes, image JBOOT checksum: 0x1127, header JBOOT checksum: 0x2609
    - 6274562   0x5FBE02   VMware4 disk image
    - 6409468   0x61CCFC   VMware4 disk image

x32dbg

- I opened Week12.exe in x32dbg
- I found some calls to wininet.dll and other dlls

4. Static Analysis Summary

Key findings from static analysis:

- 27 out of 69 VirusTotal vendors
- Detected as Loader, Trojan, Dropper, Win32, Kryptik, and other malicious types.
- Packed executable: High entropy in .text (6.79) and .rsrc (7.32) sections suggest packing/obfuscation. Overall file entropy is 7.35, reinforcing this.
  Suspicious strings and APIs: Numerous strings related to the 360Safe suite, random unreadable strings, and API calls such as CreateProcessW, ShellExecuteW, VirtualAlloc, CreateThread, and registry manipulation

- Suspicious embedded BMP file: Extracted from unpacked content, bit depth of 51.
- Binwalk results: Identified embedded files such as VMware disk images, JBOOT STAG headers, and a LANCOM OEM file, all hidden within a .bmp.
- Suspicious exports: From the BMP file: IRQ, NMS, and RES appear non-standard and may serve as shellcode or loader entry points.
- String/Command line indicators: Strings like \elevated,

/shredfilelist, and registry key manipulations suggest privilege escalation and system tampering.

Potential functionality:

- Dropper or loader: The file appears to use extracted payloads
- Use of large BMP with embedded binaries and hidden data evades detection.
- Registry key changes, environmental variable setting, file system alterations, and keyboard hooks (SetWindowsHookExW) establish persistence
- Potential anti-VM or anti-debug techniques: Calls to Wow64DisableWow64FsRedirection, string obfuscation, and debugger/environment checks

Risk indicators:

- Obfuscation and packing
- Anti-analysis behavior
- Hidden disk images and shellcode
- Suspicious HTTP URLs
- Wininet usage for possible C2 communication

Dynamic Analysis

- Network activity summary:
  - 46.8.236.61 - Command and control center
- Processes:
  - Connects to the CnC server
    - Week12.exe (PID: 7492)

Impact Analysis

User Impact Assessment

Home Users

- Potential impact: Infection could result in system slowdowns, unauthorized access, credential theft, and data corruption or deletion.
- Risk level: High – Especially for users who store personal documents, photos, or financial data.
- Data compromise potential: Moderate to high – Strings and API calls suggest capabilities for data exfiltration, credential theft, and surveillance.

Business Users

- Operational impact: deleting critical files
- Data security concerns:sensitive information leakage, especially intellectual property, financial data, and internal communications.
- Financial implications: Costs associated with downtime, incident response, regulatory fines

Government Users

- Security implications:process creation, registry manipulation, and potential data exfiltration over HTTP.
- Data sensitivity concerns: may jeopardize national security or classified information if systems with sensitive access are compromised.
- Operational disruption potential: High — especially in agencies relying on real-time operations, communications, or critical infrastructure systems.

Mitigation Strategy

Immediate Response

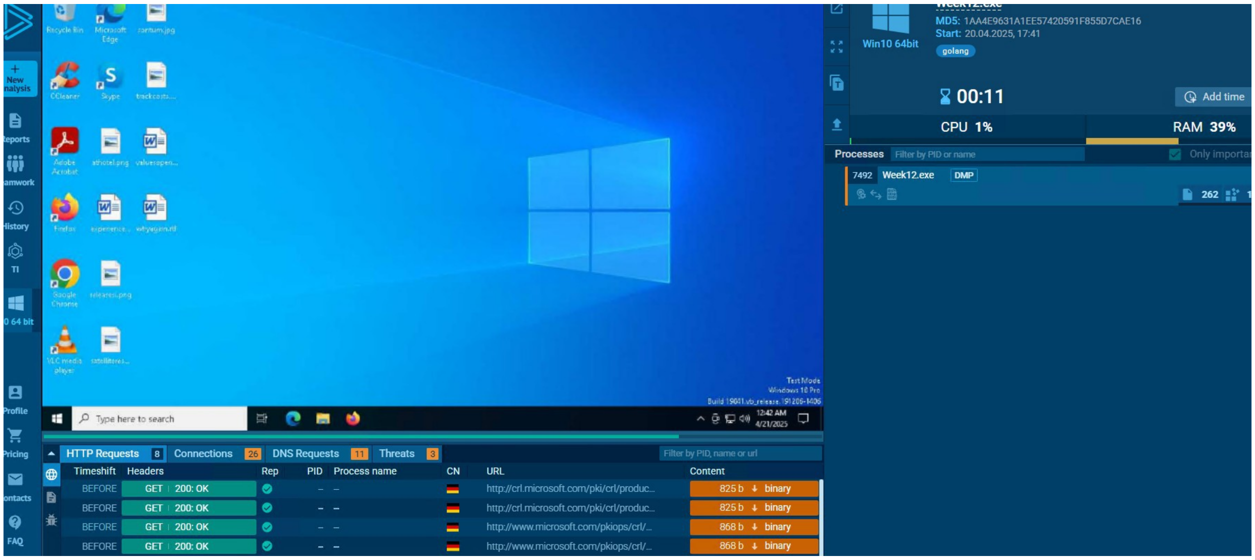
- Initial containment steps:
    - Disconnect infected hosts from all networks
    - Disable shared drives and prevent further data access or leakage.
- System isolation procedures:
    - Create secure backups and prevent backups
- Data preservation methods:
    - Create full disk images for forensic analysis.

Long-term Prevention

- Security control recommendations:
    - Implement application whitelisting
- Policy modifications:
    - Enforce the principle of least privilege for all users and processes.
    - Require multi-factor authentication for critical services.
- Training requirements:
    - Educate employees and users on phishing, suspicious file attachments

Conclusion

The analysis of Week12.exe revealed a highly suspicious and malicious file that uses packing, obfuscation, and steganography to hide its true functionality. The use of suspicious BMP files, API calls associated with system manipulation and file destruction suggest that this malware is designed to deceive users and evade detection. It has the potential to operate as a loader or dropper, delivering additional payloads that may steal data, destroy files, or facilitate remote control.



Week12.exe
MD5: 1AA4E9631A1EE57420591F855D7CAE16
Start: 20.04.2025, 17:41

Win10 64bit

golang

00:11

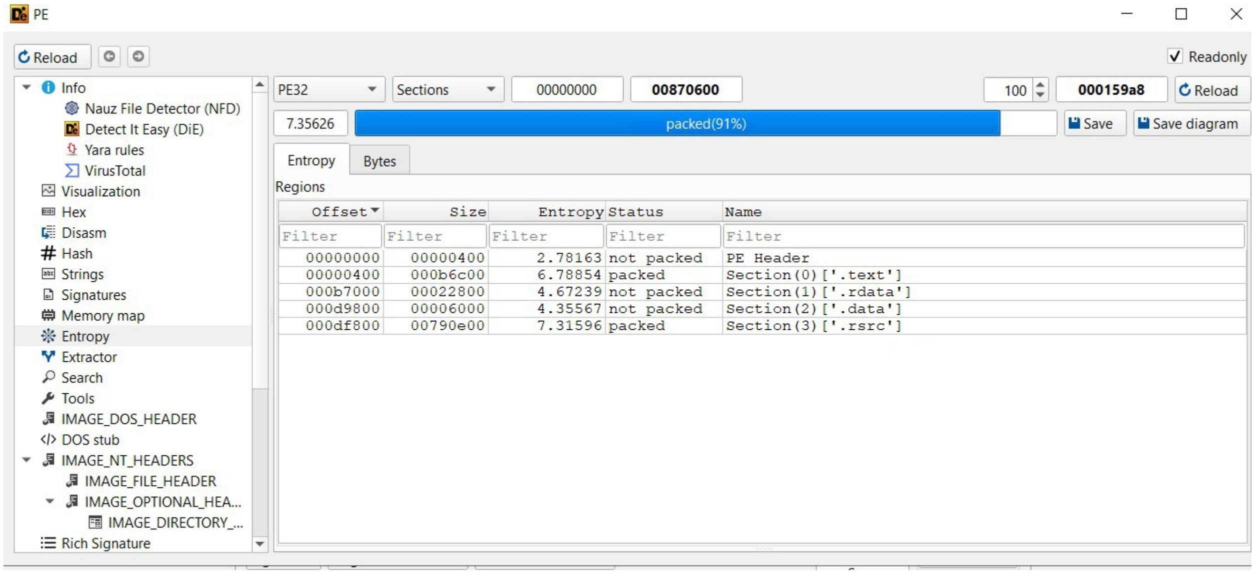
CPU 1%

RAM 39%

PID	Process
7492	Week12.exe

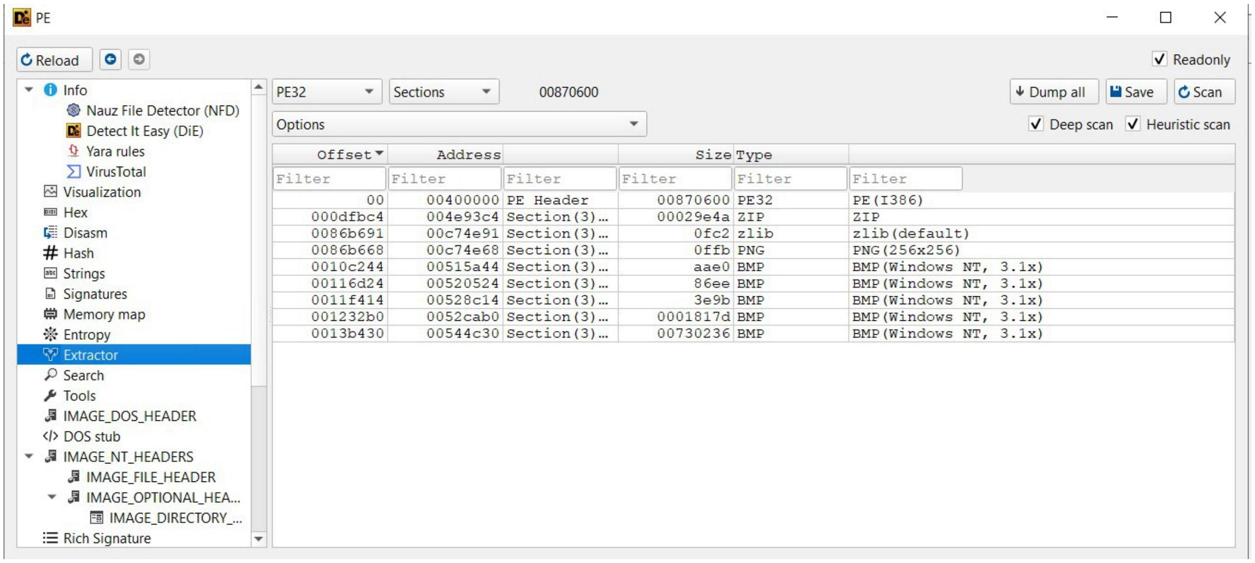
HTTP Requests 8 | Connections 26 | DNS Requests 11 | Threats 3

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
BEFORE	GET 200: OK	✓	–	–		http://crl.microsoft.com/pki/crl/produc...	825 b ↓ binary
BEFORE	GET 200: OK	✓	–	–		http://crl.microsoft.com/pki/crl/produc...	825 b ↓ binary
BEFORE	GET 200: OK	✓	–	–		http://www.microsoft.com/pkiops/crl/...	868 b ↓ binary
BEFORE	GET 200: OK	✓	–	–		http://www.microsoft.com/pkiops/crl/...	868 b ↓ binary



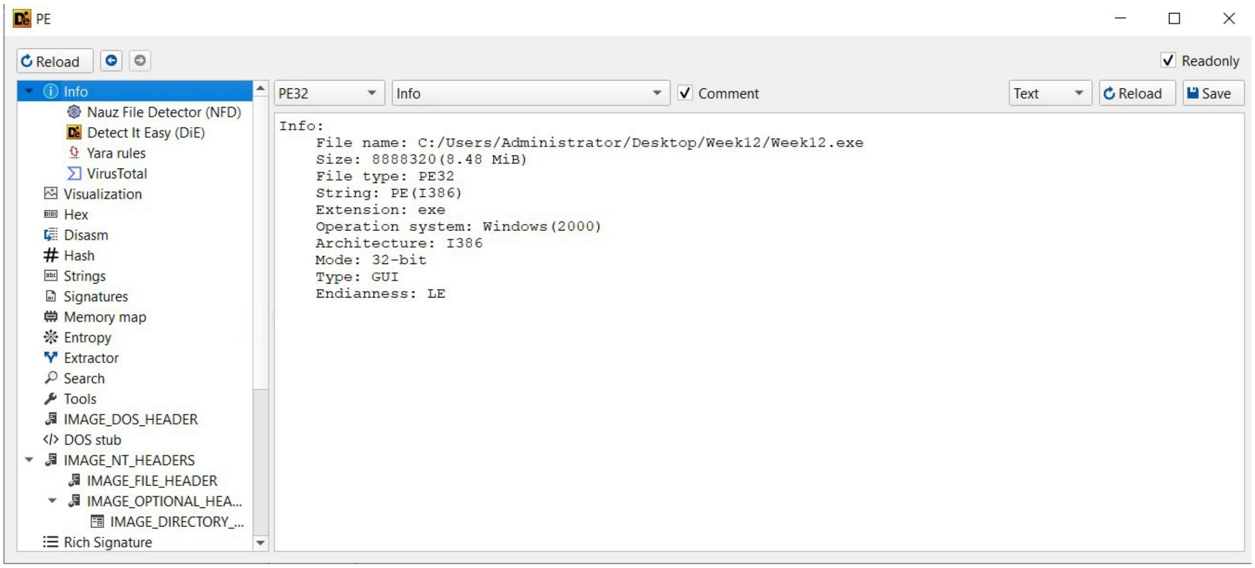
Regions

Offset	Size	Entropy	Status	Name
00000000	00000400	2.78163	not packed	PE Header
00000400	000b6c00	6.78854	packed	Section(0)['.text']
000b7000	00022800	4.67239	not packed	Section(1)['.rdata']
000d9800	00006000	4.35567	not packed	Section(2)['.data']
000df800	00790e00	7.31596	packed	Section(3)['.rsrc']

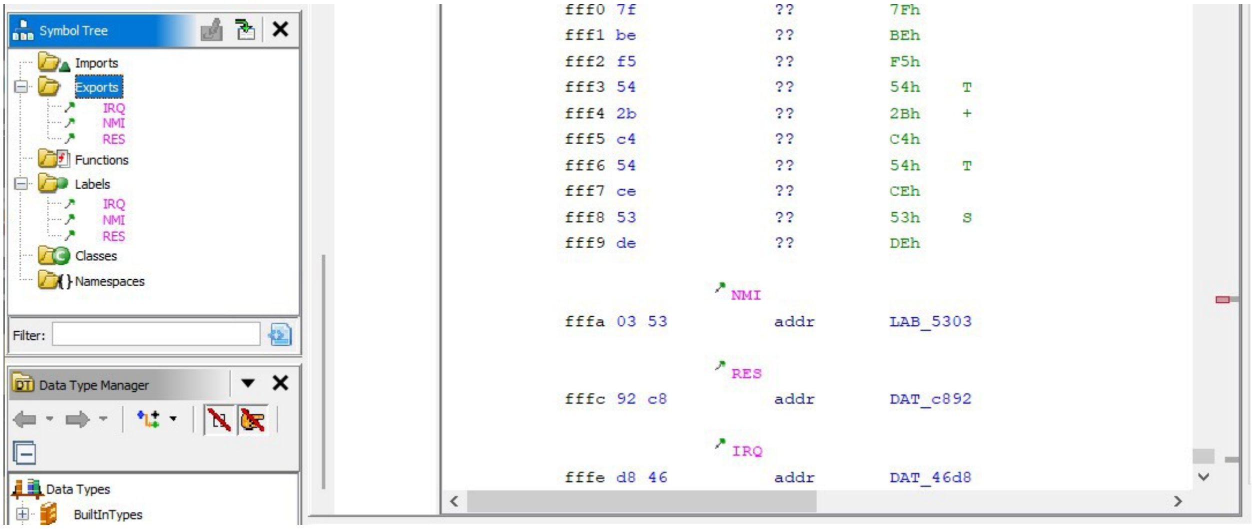


☑ Deep scan ☑ Heuristic scan

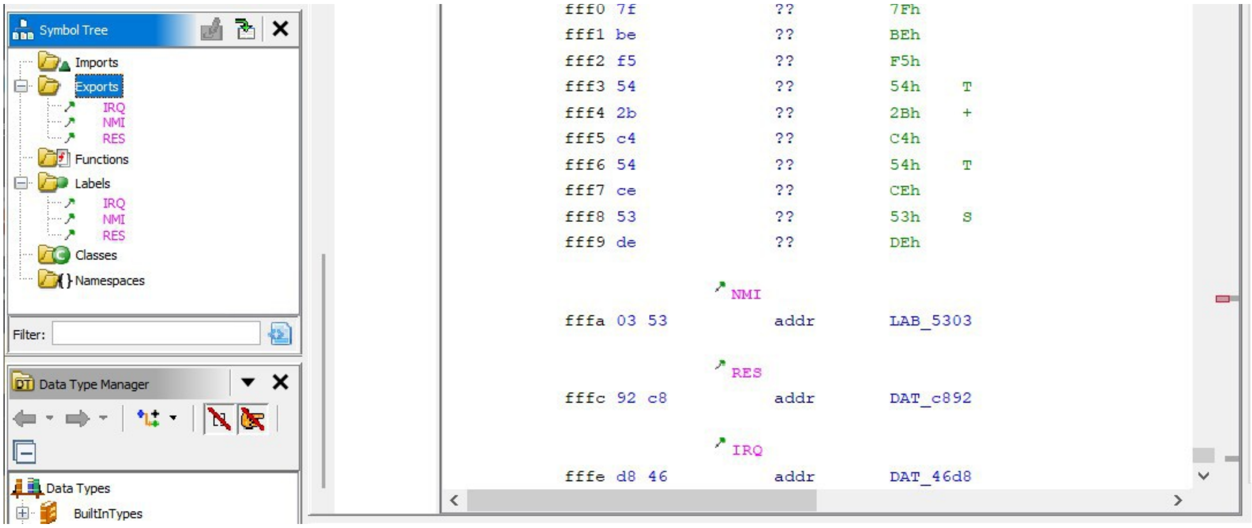
Offset	Address		Size	Type	
00	00400000	PE Header	00870600	PE32	PE(I386)
000dfbc4	004e93c4	Section(3)…	00029e4a	ZIP	ZIP
0086b691	00c74e91	Section(3)…	0fc2	zlib	zlib(default)
0086b668	00c74e68	Section(3)…	0ffb	PNG	PNG(256x256)
0010c244	00515a44	Section(3)…	aae0	BMP	BMP(Windows NT, 3.1x)
00116d24	00520524	Section(3)…	86ee	BMP	BMP(Windows NT, 3.1x)
0011f414	00528c14	Section(3)…	3e9b	BMP	BMP(Windows NT, 3.1x)
001232b0	0052cab0	Section(3)…	0001817d	BMP	BMP(Windows NT, 3.1x)
0013b430	00544c30	Section(3)…	00730236	BMP	BMP(Windows NT, 3.1x)



```
Info:
    File name: C:/Users/Administrator/Desktop/Week12/Week12.exe
    Size: 8888320(8.48 MiB)
    File type: PE32
    String: PE(I386)
    Extension: exe
    Operation system: Windows(2000)
    Architecture: I386
    Mode: 32-bit
    Type: GUI
    Endianness: LE
```



```
fff0 7f          ??      7Fh
fff1 be          ??      BEh
fff2 f5          ??      F5h
fff3 54          ??      54h    T
fff4 2b          ??      2Bh    +
fff5 c4          ??      C4h
fff6 54          ??      54h    T
fff7 ce          ??      CEh
fff8 53          ??      53h    S
fff9 de          ??      DEh

                NMI
fffa 03 53       addr    LAB_5303

                RES
fffc 92 c8       addr    DAT_c892

                IRQ
fffe d8 46       addr    DAT_46d8
```



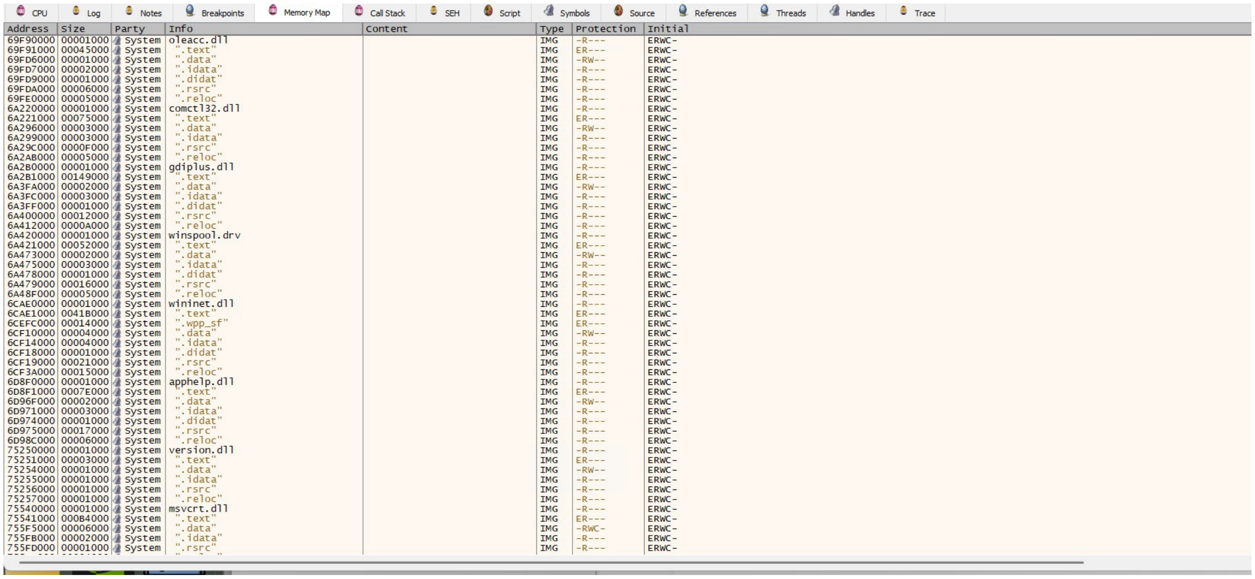
```
fff0 7f          ??       7Fh
fff1 be          ??       BEh
fff2 f5          ??       F5h
fff3 54          ??       54h    T
fff4 2b          ??       2Bh    +
fff5 c4          ??       C4h
fff6 54          ??       54h    T
fff7 ce          ??       CEh
fff8 53          ??       53h    S
fff9 de          ??       DEh

                    NMI
fffa 03 53       addr     LAB_5303

                    RES
fffc 92 c8       addr     DAT_c892

                    IRQ
fffe d8 46       addr     DAT_46d8
```

Comments (5)

sshinn

a moment ago

This is a highly suspicious and malicious file that uses packing, obfuscation, and steganography to hide its true functionality. The use of suspicious BMP files, API calls associated with system manipulation and file destruction suggest that this malware is designed to deceive users and evade detection. It has the potential to operate as a loader or dropper, delivering additional payloads that may steal data, destroy files, or facilitate remote control.



```
Address  Size     Party  Info            Content  Type Protection Initial
69F90000 00001000 System oleacc.dll               IMG  -R---      ERWC-
69F91000 00045000 System  ".text"                 IMG  ER---      ERWC-
69FD6000 00001000 System  ".data"                 IMG  -RW--      ERWC-
69FD7000 00002000 System  ".idata"                IMG  -R---      ERWC-
69FD9000 00001000 System  ".didat"                IMG  -R---      ERWC-
69FDA000 00006000 System  ".rsrc"                 IMG  -R---      ERWC-
69FE0000 00005000 System  ".reloc"                IMG  -R---      ERWC-
6A220000 00001000 System comctl32.dll             IMG  -R---      ERWC-
6A221000 00075000 System  ".text"                 IMG  ER---      ERWC-
6A296000 00003000 System  ".data"                 IMG  -RW--      ERWC-
6A299000 00003000 System  ".idata"                IMG  -R---      ERWC-
6A29C000 0000F000 System  ".rsrc"                 IMG  -R---      ERWC-
6A2AB000 00005000 System  ".reloc"                IMG  -R---      ERWC-
6A2B0000 00001000 System gdiplus.dll              IMG  -R---      ERWC-
6A2B1000 00149000 System  ".text"                 IMG  ER---      ERWC-
6A3FA000 00002000 System  ".data"                 IMG  -RW--      ERWC-
6A3FC000 00003000 System  ".idata"                IMG  -R---      ERWC-
6A3FF000 00001000 System  ".didat"                IMG  -R---      ERWC-
6A400000 00012000 System  ".rsrc"                 IMG  -R---      ERWC-
6A412000 0000A000 System  ".reloc"                IMG  -R---      ERWC-
6A420000 00001000 System winspool.drv             IMG  -R---      ERWC-
6A421000 00052000 System  ".text"                 IMG  ER---      ERWC-
6A473000 00002000 System  ".data"                 IMG  -RW--      ERWC-
6A475000 00003000 System  ".idata"                IMG  -R---      ERWC-
6A478000 00001000 System  ".didat"                IMG  -R---      ERWC-
6A479000 00016000 System  ".rsrc"                 IMG  -R---      ERWC-
6A48F000 00005000 System  ".reloc"                IMG  -R---      ERWC-
6CAE0000 00001000 System wininet.dll              IMG  -R---      ERWC-
6CAE1000 0041B000 System  ".text"                 IMG  ER---      ERWC-
6CEFC000 00014000 System  ".wpp_sf"               IMG  ER---      ERWC-
6CF10000 00004000 System  ".data"                 IMG  -RW--      ERWC-
6CF14000 00004000 System  ".idata"                IMG  -R---      ERWC-
6CF18000 00001000 System  ".didat"                IMG  -R---      ERWC-
6CF19000 00021000 System  ".rsrc"                 IMG  -R---      ERWC-
6CF3A000 00015000 System  ".reloc"                IMG  -R---      ERWC-
6D8F0000 00001000 System apphelp.dll              IMG  -R---      ERWC-
6D8F1000 0007E000 System  ".text"                 IMG  ER---      ERWC-
6D96F000 00002000 System  ".data"                 IMG  -RW--      ERWC-
6D971000 00003000 System  ".idata"                IMG  -R---      ERWC-
6D974000 00001000 System  ".didat"                IMG  -R---      ERWC-
6D975000 00017000 System  ".rsrc"                 IMG  -R---      ERWC-
6D98C000 00006000 System  ".reloc"                IMG  -R---      ERWC-
75250000 00001000 System version.dll              IMG  -R---      ERWC-
75251000 00003000 System  ".text"                 IMG  ER---      ERWC-
75254000 00001000 System  ".data"                 IMG  -RW--      ERWC-
75255000 00001000 System  ".idata"                IMG  -R---      ERWC-
75256000 00001000 System  ".rsrc"                 IMG  -R---      ERWC-
75257000 00001000 System  ".reloc"                IMG  -R---      ERWC-
75540000 00001000 System msvcrt.dll               IMG  -R---      ERWC-
75541000 000B4000 System  ".text"                 IMG  ER---      ERWC-
755F5000 00006000 System  ".data"                 IMG  -RWC-      ERWC-
755FB000 00002000 System  ".idata"                IMG  -R---      ERWC-
755FD000 00001000 System  ".rsrc"                 IMG  -R---      ERWC-
```