Static Analysis

1. Virus Total Analysis

Hash Analysis

- File Hash: [Insert MD5, SHA-1, SHA-256 hash value]
  - MD5: 01dba6410fa6bad9c6c45358bca2d1df
  - SHA-1: c22a2402123a5c22d7693f78579c1066e0757cfe
  - SHA-256:8e5a51570b05ca5a93d5ac171b9904660bad5e98cac509a3b129c31621a4741c
- Method of hash acquisition: [Describe process]
  - Found on virustotal
- [Link to VirusTotal results]
  - https://www.virustotal.com/gui/file/8e5a51570b05ca5a93d5ac171b9904660bad5e98cac509a3b129c31621a4741c

Vendor Analysis

- Number of vendors flagging as malicious: [X/Y]
  - 64/72
- Analysis of vendor results:
  - [Discuss patterns in detection]: flagged as pe executable, long sleeps, checks-user-input, detects-debug-environment, nxdomain, definitely a trojan, family labels: lokibot, stealer, agentb
  - [Common malware names identified]: lokibot, stealer, agentb, Trojan.PWS.ZKD, Infostealer, Password-Stealer, PassStealer, Week6.exe
  - [Notable vendor disagreements]: They all agree that this is a trojan. They disagree whether it is an infostealer, passwordstealer, lokibot, agentb, or other malware

File History

- First Submission Date: [Date]
  - First Submission: 2025-02-26 21:21:25 UTC
- File Creation Date from Windows: [Date]
  - Creation Time: 2016-06-23 16:04:21 UTC
- Analysis of submission timeline:
  - [Discussion of file age]: It was created 9 years ago, and it was first submitted a few days ago. That does not make much sense to me, because why would the writer make this malware (Week6.exe by Michael Galde) 9 years ago just to release it now? It does not make sense to me.

    - [Notable resubmissions or changes]: None that is apparent to me

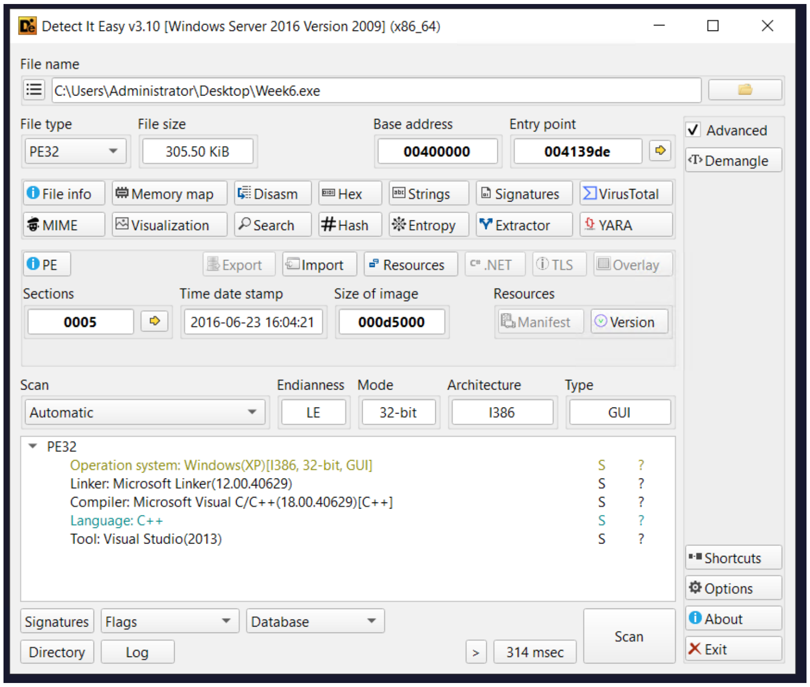
Community Score

- [Link to your VirusTotal community contribution]
    - https://www.virustotal.com/gui/file/8e5a51570b05ca5a93d5ac171b9904660bad5e98cac509a3b129c31621a4741c/community
    - Username sshinn
- Summary of initial findings posted to the community:
    - [Key observations]
    - [Potential indicators of compromise]
    - Week6.exe is a dangerous Trojan, flagged by 64 out of 72 antivirus vendors on VirusTotal. The file was created in 2016 but only recently submitted for analysis. The malware appears to be a credential-stealing Trojan, as it targets login data from various web browsers and email clients. It includes suspicious strings such as "fuckav.ru," suggesting an anti-antivirus or hacker-related connection. The program's structure is also unusual, with an ".x" section and sections with unexpected read, write, and execute permissions.

2. Detect It Easy (DIE) Analysis

File information

- File type: [Type] PE32 executable
- Architecture: [Architecture]: i386
- Compiler: [Compiler information]: Microsoft Visual C/C++
- Additional relevant information:
    - [List notable file characteristics]
        - File size: 305.50 KB (312832 bytes)
        - PE32 Compiler: Microsoft Visual C/C++ (18.00.40629) [C++] Linker: Microsoft Linker (12.00.40629) Tool: Visual Studio (2013)
    - [Unusual headers or structures]
        - .x section is suspicious and unusual
        - File Version Information
            - Copyright © 2025 Professor Michael Galde
            - Product: Week 6 Analysis Sample
            - Description: CYBV 454 Spring 25 Week 6 Malware
            - Original Name: Week6.exe



Detect It Easy v3.10 [Windows Server 2016 Version 2009] (x86_64)

File name: C:\Users\Administrator\Desktop\Week6.exe

File type: PE32 | File size: 305.50 KiB | Base address: 00400000 | Entry point: 004139de

☑ Advanced

Sections: 0005 | Time date stamp: 2016-06-23 16:04:21 | Size of image: 000d5000

Scan: Automatic | Endianness: LE | Mode: 32-bit | Architecture: I386 | Type: GUI

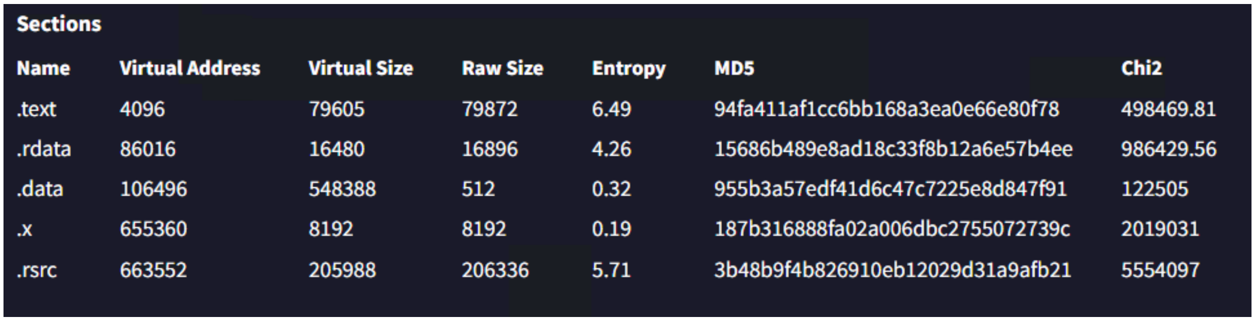
```
PE32
    Operation system: Windows(XP)[I386, 32-bit, GUI]        S   ?
    Linker: Microsoft Linker(12.00.40629)                   S   ?
    Compiler: Microsoft Visual C/C++(18.00.40629)[C++]      S   ?
    Language: C++                                           S   ?
    Tool: Visual Studio(2013)                               S   ?
```

314 msec

Memory Map Analysis

- Section breakdown:
    - .text:
        - Virtual Address:4096
        - Raw Size:79872
        - Virtual Size:79605
        - Entropy:6.49
        - MD5 Hash:94fa411af1cc6bb168a3ea0e66e80f78
        - Permissions: Read and Execute
    - .rdata:
        - Virtual Address:86016
        - Raw Size:16896
        - Virtual Size:16480
        - Entropy:4.26
        - MD5 Hash: 94fa411af1cc6bb168a3ea0e66e80f78
        - Permissions: Read
    - .data
        - Virtual Address:106496
        - Raw Size:512
        - Virtual Size:548388
        - Entropy:0.32
        - MD5 Hash:955b3a57edf41d6c47c7225e8d847f91
        - Permissions: Read and Write
    - .x
        - Virtual Address:655360
        - Raw Size:8192
        - Virtual Size:8192

        - Entropy:0.19
        - MD5 Hash:187b316888fa02a006dbc2755072739c
        - Permissions: Read and Write
    - .rsrc
        - Virtual Address:663552
        - Raw Size:206336
        - Virtual Size:205988
        - Entropy:5.71
        - MD5 Hash: 3b43b48b9f4b826910eb12029d31a9afb21
        - Permissions: Read
- Notable findings:
    - [Unusual section permissions]
        - .text has Execute permissions
        - .x and .data have write permissions
        - All sections have read permissions
    - [Section size anomalies]
        - All of the sections have similar virtual size to raw size, except for .data, which has a large virtual size and a very small raw size



Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	79605	79872	6.49	94fa411af1cc6bb168a3ea0e66e80f78	498469.81
.rdata	86016	16480	16896	4.26	15686b489e8ad18c33f8b12a6e57b4ee	986429.56
.data	106496	548388	512	0.32	955b3a57edf41d6c47c7225e8d847f91	122505
.x	655360	8192	8192	0.19	187b316888fa02a006dbc2755072739c	2019031
.rsrc	663552	205988	206336	5.71	3b48b9f4b826910eb12029d31a9afb21	5554097

String Analysis

- Notable strings discovered:

[URLs/IPs]

- Fuckav.ru
    - [File paths]
- SOFTWARE\Microsoft\Cryptography
- %s\%s\User Data\Default\Login Data
- %s\%s\User Data\Default\Web Data
- %s%s\Login Data
- %s%s\Default\Login Data
- Comodo\Dragon
- MapleStudio\ChromePlus
- Google\Chrome
- Yandex\YandexBrowser
- CocCoc\Browser

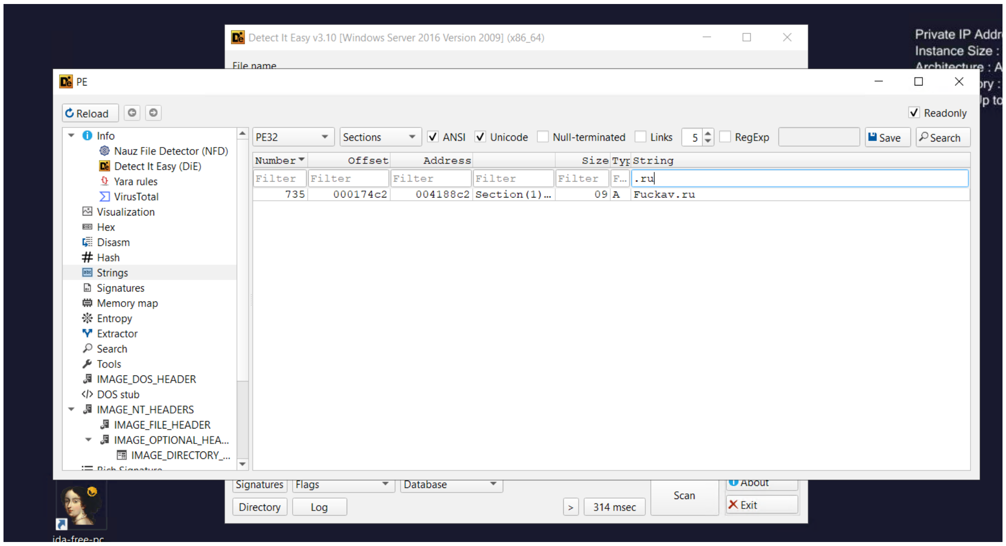
- Comodo\Chromodo
- Coowon\Coowon
- 360Browser\Browser
- CatalinaGroup\Citrio
- Google\Chrome SxS
- tSoftware\Microsoft\Internet Explorer\IntelliForms\Storage2
- Software\Microsoft\Internet Explorer\TypedURLs
- %s\logins.json
- %s\prefs.js
- %s\signons.sqlite
- %s\Mozilla\Firefox\profiles.ini
- %s\Mozilla\Firefox\Profiles\%s
- %s\Mozilla\SeaMonkey\profiles.ini
- %s\Mozilla\SeaMonkey\Profiles\%s
- %s\Flock\Browser\profiles.ini
- %s\Flock\Browser\Profiles\%s
- %s\Thunderbird\profiles.ini
- %s\Thunderbird\Profiles\%s
- %s\K-Meleon\profiles.ini
- %s\K-Meleon\%s
- %s\Comodo\IceDragon\profiles.ini
- %s\Comodo\IceDragon\Profiles\%s
- %s\NETGATE Technologies\BlackHawk\profiles.ini
- %s\NETGATE Technologies\BlackHawk\Profiles\%s
- %s\Postbox\profiles.ini
- %s\Postbox\Profiles\%s
- %s\8pecxstudios\Cyberfox\profiles.ini
- %s\8pecxstudios\Cyberfox\Profiles\%s
- %s\Moonchild Productions\Pale Moon\profiles.ini
- %s\Moonchild Productions\Pale Moon\Profiles\%s
- %s\FossaMail\profiles.ini
- %s\FossaMail\Profiles\%s
- %s\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}\data
- %s\nss3.dll
- SOFTWARE\Mozilla\Mozilla Firefox
- %s\%s\Main
- SOFTWARE\Mozilla\Mozilla Thunderbird
- SOFTWARE\Mozilla\FossaMail
- SOFTWARE\Postbox\Postbox
- SOFTWARE\Mozilla\Flock
- SOFTWARE\Flock\Flock
- %s\NETGATE\Black Hawk
- SOFTWARE\Mozilla\Pale Moon
- %s\Lunascape\Lunascape6\plugins\{9BDD5314-20A6-4d98-AB30-8325A95771EE}
- SOFTWARE\K-Meleon
- SOFTWARE\ComodoGroup\IceDragon\Setup
- SOFTWARE\8pecxstudios\Cyberfox86
- SOFTWARE\8pecxstudios\Cyberfox
- SOFTWARE\mozilla.org\SeaMonkey
- %s\Mozilla\Profiles
- SOFTWARE\Mozilla\SeaMonkey
- SOFTWARE\Mozilla\Waterfox
- %s\Opera
- Software\QtWeb.NET\QtWeb Internet Browser\AutoComplete
- %s\QupZilla\profiles\default\browsedata.db
- %s\Apple Computer\Preferences\keychain.plist
- %s\Apple Application Support\plutil.exe
- %s\Data\AccCfg\Accounts.tdat

- %s\Storage
- %s\Foxmail\mail
- Software\IncrediMail\Identities
- Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
- Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook
- Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook
- %s\32BitFtp.TMP
- %s\32BitFtp.ini
- %s\Estsoft\ALFTP\ESTdb2.dat
- %s\site.xml
- %s\BitKinex\bitkinex.ds
- Software\Bitvise\BvSshClient
- %s\BlazeFtp\site.dat
- Software\FlashPeak\BlazeFtp\Settings
- Software\NCH Software\ClassicFTP\FTPAccounts
- %s\Cyberduck
- %s\iterate_GmbH
- %s\EasyFTP\data
- %s\ExpanDrive
- Software\Far\Plugins\FTP\Hosts
- Software\Far2\Plugins\FTP\Hosts
- %s\Far Manager\Profile\PluginsData\42E4AEB1-A230-44F4-B33C-F195BB654931.db
- %s\FileZilla\Filezilla.xml
- %s\FileZilla\filezilla.xml
- %s\FileZilla\recentservers.xml
- %s\FileZilla\sitemanager.xml
- %s\FlashFXP
- Software\NCH Software\Fling\Accounts
- %s\FreshWebmaster\FreshFTP\FtpSites.SMF
- %s\FTPBox\profiles.conf
- %s\FTPGetter\Profile\servers.xml
- %s\FTPGetter\servers.xml
- %s\FTPInfo\ServerList.xml
- %s\FTPInfo\ServerList.cfg
- %s\FTP Navigator\Ftplist.txt
- %s\FTP Now\sites.xml
- %s\FTPShell\ftpshell.fsi
- %s\.config\fullsync\profiles.xml
- %s\DeluxeFTP\sites.xml
- %s\GoFTP\settings\Connections.txt
- %s\%s%i\encPwd.jsd
- %s\%s%i\data\settings\sshProfiles-j.jsd
- %s\%s%i\data\settings\ftpProfiles-j.jsd
- Software\LinasFTP\Site Manager
- %s\oZone3D\MyFTP\myftp.ini
- %s\NetDrive\NDSites.ini
- %s\NetDrive2\drives.dat
- %s\Fastream NETFile\My FTP Links
- %s\NexusFile\userdata\ftpsite.ini
- %s\NexusFile\ftpsite.ini
- %s\INSoftware\NovaFTP\NovaFTP.db
- %s\Notepad++\plugins\config\NppFTP\NppFTP.xml
- %s\Odin Secure FTP Expert\QFDefault.QFQ
- %s\Odin Secure FTP Expert\SiteInfo.QFP
- Software\9bis.com\KiTTY\Sessions
- Software\SimonTatham\PuTTY\Sessions

- %s\Microsoft\Credentials
- Software\VanDyke\SecureFX
- %s\Sessions
- %s\SftpNetDrive
- %s\Sherrod Computers\sherrod FTP\favorites
- %s\SmartFTP
- %s\Staff-FTP\sites.ini
- %s\Steed\bookmarks.txt
- %s\SuperPutty
- %s\Syncovery
- %s\wcx_ftp.ini
- %s\GHISLER\wcx_ftp.ini
- Software\Ghisler\Total Commander
- %s\UltraFXP\sites.xml
- %s\WinFtp Client\Favorites.dat
- Software\Martin Prikryl
- %s\WS_FTP\WS_FTP.INI
- %s\WS_FTP.INI
- %s\Ipswitch
- %s\NetSarang\Xftp\Sessions
- %s\%s\%s.exe
  - [Command lines]
- firefox.exe
- %s\Apple Application Support\plutil.exe
- lsass.exe
- ZwQueryInformationProcess
- ExitProcess
- GetProcessHeap
  - [API calls]
- Foxmail*
- EmailAddress
- Technology
- PopServer
- PopPort
- PopAccount
- PopPassword
- SmtpServer
- SmtpPort
- SmtpAccount
- SmtpPassword
- Software\Incred iMail\Identities
- UserName
- Passwd
- POP3Server
- POP3Port
- Email
- SMTP Email Address
- SMTP Server
- SMTP User Name
- SMTP User
- POP3 Server
- POP3 User Name
- POP3 User
- NNTP Email Address
- NNTP User Name
- NNTP Server
- IMAP Server
- IMAP User Name
- IMAP User
- HTTP User
- HTTP Server URL
- HTTPMail User Name
- HTTPMail Server
- POP3 Port
- SMTP Port
- IMAP Port
- POP3 Password2
- IMAP Password2
- NNTP Password2
- HTTPMail Password2
- SMTP Password2
- POP3 Password
- IMAP Password
- NNTP Password
- HTTP Password
- SMTP Password
- getaddrinfo
- freeaddrinfo
- WS2_32.dll
- GetLastError
- SetLastError
- HeapAlloc

- HeapFree
- GetProcessHeap
- KERNEL32.dll
- CoInitialize
- CoUninitialize
- CoCreateInstance
- ole32.dll
- OLEAUT32.dll
- aPLib v1.01 - the smaller the better :)
- Analysis of string findings:
- [Potential functionality indicated]
  Credential Theft: The presence of paths to browser login data files such as, Chrome, Firefox, Yandex, Opera suggests the malware attempts to steal stored credentials.
- Email & FTP Credential Extraction: The malware targets various email clients (Thunderbird, Outlook, Foxmail, Postbox) and FTP clients (FileZilla, SmartFTP, WinSCP, PuTTY), indicating an intent to steal email and FTP credentials.
- Keylogging & User Input Monitoring: The presence of API calls like GetProcessHeap, ZwQueryInformationProcess, and ExitProcess suggests potential process manipulation, possibly for keylogging or monitoring system interactions.
- Data Exfiltration: References to getaddrinfo, WS2_32.dll, and freeaddrinfo indicate network communication functionality, suggesting that stolen data is exfiltrated to a remote server.
- Persistence Mechanisms: The use of registry keys (SOFTWARE\Microsoft\Cryptography) implies potential persistence tactics, such as auto-starting the malware upon system reboot.
- Debugger & Sandbox Detection: Calls like GetLastError, SetLastError, and HeapAlloc may be used to detect debugging environments and evade analysis.
- [Suspicious patterns]
- References to fuckav.ru: This is a highly suspicious domain that may be associated with command-and-control (C2) communications or payload distribution.
- Unusual File Paths & Browser Targets: The malware attempts to extract sensitive data from multiple browsers and software, including lesser-known ones like Cyberfox, Comodo IceDragon, and QupZilla, showing broad compatibility for data theft.
- Suspicious Section (.x) in PE File: The presence of an .x section with low entropy (0.19) suggests that it might contain encoded or obfuscated data, possibly indicating shellcode or packed content.
- API Calls for Process Manipulation: Calls to functions such as CoCreateInstance, CoInitialize, and HeapFree can be used for executing malicious payloads in memory without leaving traces on disk.
- Encrypted or Packed Data: The presence of aPLib v1.01 - the smaller the better :) suggests that the malware may use compression or packing techniques to evade detection.

- Email & FTP Password Theft Focus: The strings explicitly list email and FTP credential-related keywords such as Passwd, SMTP Password, POP3 Password, IMAP Password, reinforcing its classification as an info-stealer.



PE32 | Sections | ☑ ANSI | ☑ Unicode | □ Null-terminated | □ Links | 5 | □ RegExp

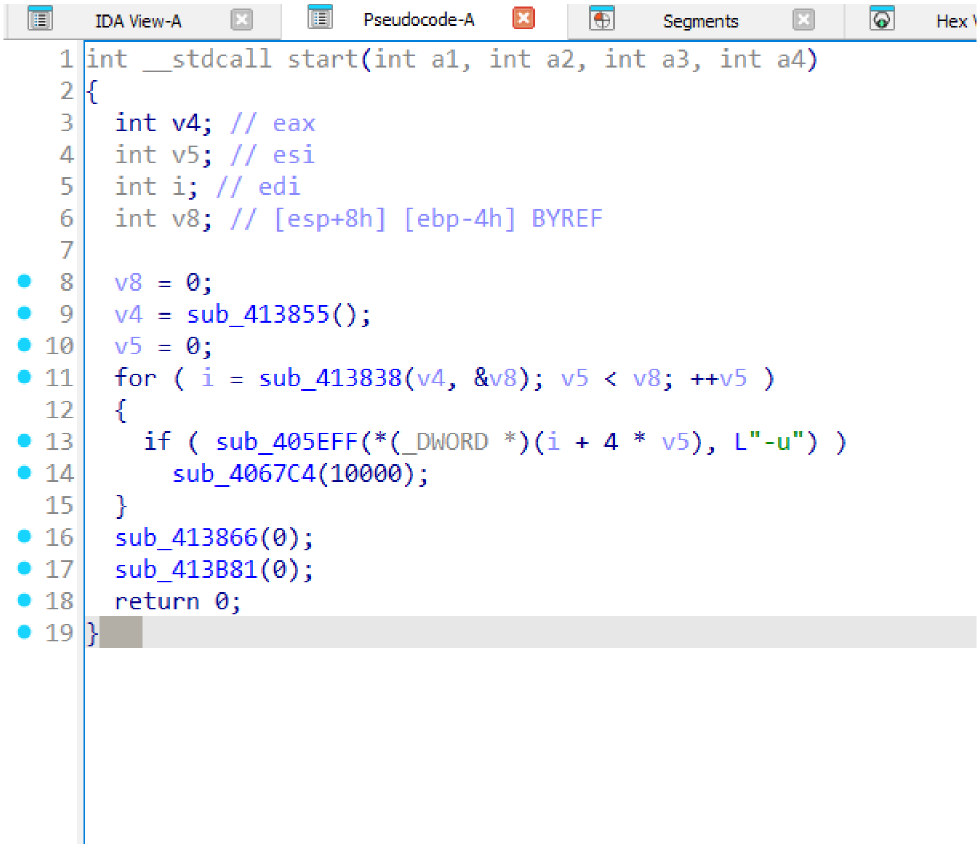
Number	Offset	Address		Size	Typ	String
Filter	Filter	Filter	Filter	Filter	F...	.ru
735	000174c2	004188c2	Section(1)...	09	A	Fuckav.ru

Entropy Analysis

- Overall entropy score: [Score]
  - 6.00469
- Section-specific entropy:
  - [List sections with unusual entropy]
  - .text: 6.49207 is relatively high
  - .x is 0.18850 is relatively low
- Packing analysis:
  - [Packed/Unpacked determination]
    - Detect-It-Easy says it is not packed, but there was a string referencing aPLib which is a file compressor/packer
  - [Packer identified (if applicable)]
    - aPLib possibly, if it is at all packed
  - [Unpacking methodology (if attempted)]
    - Use IDA and x32dbg to unpack manually
  - [Alternative unpacking approaches (if needed)]
    - None

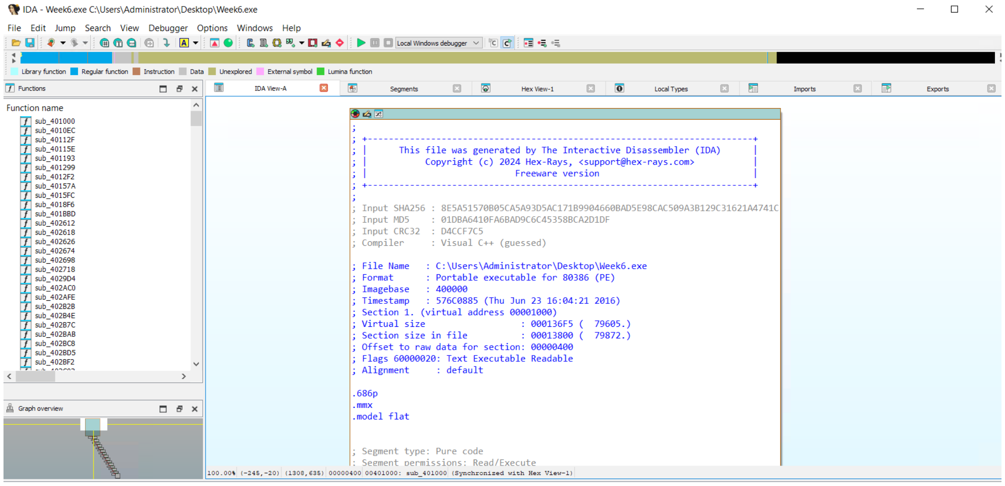
IDA SECTION
Provided analysis of the application Start Point

- Identified start of .text section at Imagebase 400000
- Segment permissions: Read/Execute
- Start Point: .text:004139DE
- Decompiled start function initializes 4 int variables, then has a for loop



```
int __stdcall start(int a1, int a2, int a3, int a4)
{
  int v4; // eax
  int v5; // esi
  int i; // edi
  int v8; // [esp+8h] [ebp-4h] BYREF

  v8 = 0;
  v4 = sub_413855();
  v5 = 0;
  for ( i = sub_413838(v4, &v8); v5 < v8; ++v5 )
  {
    if ( sub_405EFF(*(_DWORD *)(i + 4 * v5), L"-u") )
      sub_4067C4(10000);
  }
  sub_413866(0);
  sub_413B81(0);
  return 0;
}
```



```
sub_401000
sub_4010EC
sub_40112F
sub_40115E
sub_401193
sub_401299
sub_4012F2
sub_40157A
sub_4015FC
sub_4018F6
sub_401BBD
sub_402612
sub_402618
sub_402626
sub_402674
sub_402698
sub_402718
sub_4029D4
sub_402AC0
sub_402AFE
sub_402B2B
sub_402B4E
sub_402B7C
sub_402BAB
sub_402BC8
sub_402BD5
sub_402BF2
```

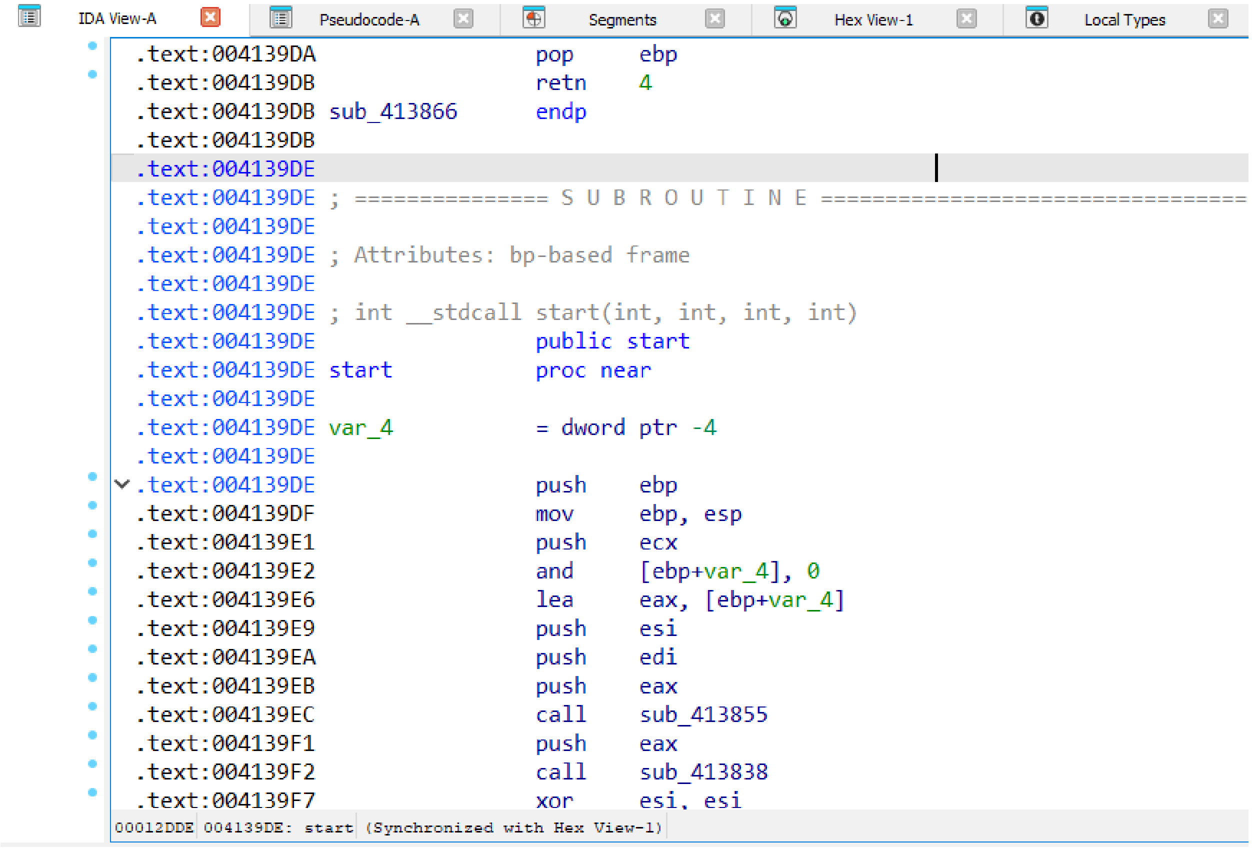
```
;
; +-------------------------------------------------------------------------+
; |      This file was generated by The Interactive Disassembler (IDA)      |
; |           Copyright (c) 2024 Hex-Rays, <support@hex-rays.com>           |
; |                            Freeware version                             |
; +-------------------------------------------------------------------------+
;
; Input SHA256 : 8E5A51570B05CA5A93D5AC171B9904660BAD5E98CAC509A3B129C31621A4741C
; Input MD5    : 01DBA6410FA6BAD9C6C45358BCA2D1DF
; Input CRC32  : D4CCF7C5
; Compiler     : Visual C++ (guessed)

; File Name   : C:\Users\Administrator\Desktop\Week6.exe
; Format      : Portable executable for 80386 (PE)
; Imagebase   : 400000
; Timestamp   : 576C0885 (Thu Jun 23 16:04:21 2016)
; Section 1. (virtual address 00001000)
; Virtual size                  : 000136F5 (  79605.)
; Section size in file          : 00013800 (  79872.)
; Offset to raw data for section: 00000400
; Flags 60000020: Text Executable Readable
; Alignment     : default

.686p
.mmx
.model flat


; Segment type: Pure code
; Segment permissions: Read/Execute
```

```
100.00% (-245,-20) (1308,635) 00000400 00401000: sub_401000 (Synchronized with Hex View-1)
```



```
.text:004139DA                 pop     ebp
.text:004139DB                 retn    4
.text:004139DB sub_413866      endp
.text:004139DB
.text:004139DE
.text:004139DE ; =============== S U B R O U T I N E ================================
.text:004139DE
.text:004139DE ; Attributes: bp-based frame
.text:004139DE
.text:004139DE ; int __stdcall start(int, int, int, int)
.text:004139DE                 public start
.text:004139DE start           proc near
.text:004139DE
.text:004139DE var_4           = dword ptr -4
.text:004139DE
.text:004139DE                 push    ebp
.text:004139DF                 mov     ebp, esp
.text:004139E1                 push    ecx
.text:004139E2                 and     [ebp+var_4], 0
.text:004139E6                 lea     eax, [ebp+var_4]
.text:004139E9                 push    esi
.text:004139EA                 push    edi
.text:004139EB                 push    eax
.text:004139EC                 call    sub_413855
.text:004139F1                 push    eax
.text:004139F2                 call    sub_413838
.text:004139F7                 xor     esi, esi
```

```
00012DDE 004139DE: start (Synchronized with Hex View-1)
```

Provided static analysis of the applications function graph and IDA Pro analysis:

- Networking (getaddrinfo, freeaddrinfo, WS2_32.dll)
- Encryption & Cryptography (CryptStringToBinaryA, LsaICryptUnprotectData, PK11SDR_Decrypt, PK11_Authenticate)
- Process Injection & Memory Manipulation (ZwAllocateVirtualMemory, NtWriteVirtualMemory, ZwReadVirtualMemory, RtlCreateUserThread)
- Credential Theft (Vault API functions: VaultEnumerateItems, VaultGetItem, PK11SDR_Decrypt)
- Persistence Mechanism / Data Theft (SQLite function calls: sqlite3_open16, sqlite3_column_text, SELECT encryptedUsername, encryptedPassword)

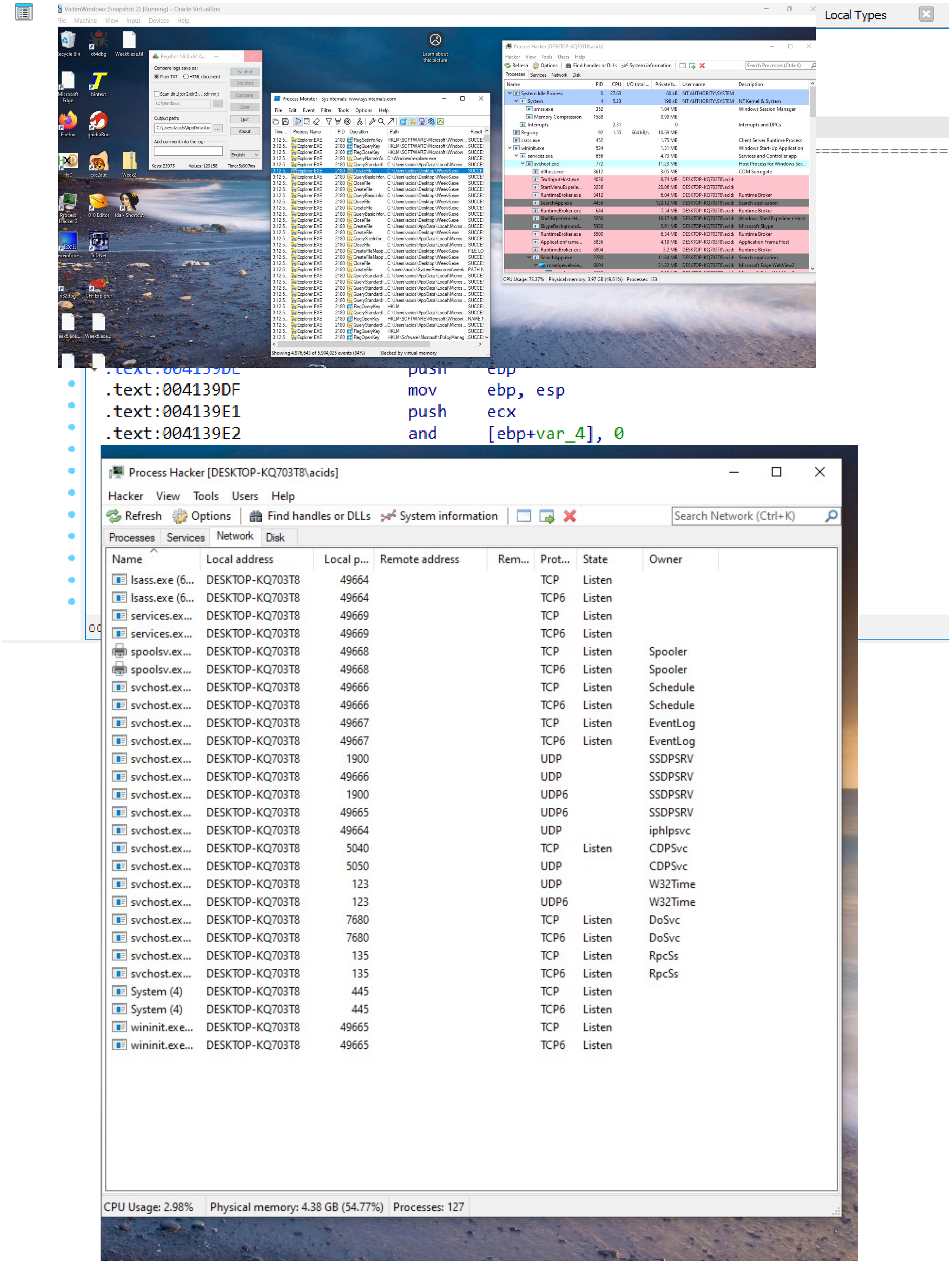
Provided analysis Using IdaPro identifying a function from Dynamic analysis

3. Static Analysis Summary

- Key findings from static analysis:
  - [Major indicators of malicious behavior]
  - [Potential functionality]
  - [Risk indicators]
- The static analysis of the malware sample "Week6.exe" reveals that it is a dangerous Trojan, flagged by 64 out of 72 antivirus vendors on VirusTotal. The file was created in 2016 but only recently submitted for analysis. The malware appears to be a credential-stealing Trojan, as it targets login data from various web browsers and email clients. It includes suspicious strings such as "fuckav.ru," suggesting an anti-antivirus or hacker-related connection. The program’s structure is also unusual, with an ".x" section and sections with unexpected read, write, and execute permissions, which could indicate hidden or obfuscated code.
- Further analysis in IDA Pro reveals that the malware heavily relies on API calls such as getaddrinfo and CoCreateInstance, which allow it to communicate over the internet and interact with Windows services. The presence of functions like HeapAlloc and HeapFree suggests that it dynamically manages memory, possibly to avoid detection. Additionally, the malware references key Windows Registry locations related to browser and email account credentials, proving its intent to steal sensitive user information.

Credential Theft Targets:

- Browsers: Chrome, Firefox, Yandex, Opera, SeaMonkey, Pale Moon, Thunderbird, etc.
- Email Clients: Outlook, Postbox, FossaMail, IncrediMail.
- FTP Clients: FileZilla, WinSCP, Cyberduck, FlashFXP.



Regshot 1.9.0 x64 A...

Compare logs save as:
● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows

Output path:
C:\Users\acids\AppData\Lo

Add comment into the log:

Keys:23975 Values:129158 Time:5s907ms

Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result
3:12:5...	Explorer.EXE	2180	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCE
3:12:5...	Explorer.EXE	2180	RegQueryKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCE
3:12:5...	Explorer.EXE	2180	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCE
3:12:5...	Explorer.EXE	2180	QueryNameInfo...	C:\Windows\explorer.exe	SUCCE
3:12:5...	Explorer.EXE	2180	QueryStandardI...	C:\Users\acids\AppData\Local\Micros...	SUCCE
3:12:5...	Explorer.EXE	2180	CreateFile	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	QueryBasicInfor...	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	CloseFile	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	CreateFile	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	QueryBasicInfor...	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	CloseFile	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	CreateFile	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	QueryBasicInfor...	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	CloseFile	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	CreateFile	C:\Users\acids\AppData\Local\Micros...	SUCCE
3:12:5...	Explorer.EXE	2180	CreateFile	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	QuerySizeInfor...	C:\Users\acids\AppData\Local\Micros...	SUCCE
3:12:5...	Explorer.EXE	2180	CloseFile	C:\Users\acids\AppData\Local\Micros...	SUCCE
3:12:5...	Explorer.EXE	2180	CreateFileMapp...	C:\Users\acids\Desktop\Week6.exe	FILE LO
3:12:5...	Explorer.EXE	2180	CreateFileMapp...	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	CloseFile	C:\Users\acids\Desktop\Week6.exe	SUCCE
3:12:5...	Explorer.EXE	2180	CreateFile	C:\users\acids\SystemResources\week...	PATH N
3:12:5...	Explorer.EXE	2180	QueryStandardI...	C:\Users\acids\AppData\Local\Micros...	SUCCE
3:12:5...	Explorer.EXE	2180	QueryStandardI...	C:\Users\acids\AppData\Local\Micros...	SUCCE
3:12:5...	Explorer.EXE	2180	QueryStandardI...	C:\Users\acids\AppData\Local\Micros...	SUCCE
3:12:5...	Explorer.EXE	2180	QueryStandardI...	C:\Users\acids\AppData\Local\Micros...	SUCCE
3:12:5...	Explorer.EXE	2180	QueryStandardI...	C:\Users\acids\AppData\Local\Micros...	SUCCE
3:12:5...	Explorer.EXE	2180	RegQueryKey	HKLM	SUCCE
3:12:5...	Explorer.EXE	2180	QueryStandardI...	C:\Users\acids\AppData\Local\Micros...	SUCCE
3:12:5...	Explorer.EXE	2180	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	NAME N
3:12:5...	Explorer.EXE	2180	QueryStandardI...	C:\Users\acids\AppData\Local\Micros...	SUCCE
3:12:5...	Explorer.EXE	2180	RegQueryKey	HKLM	SUCCE
3:12:5...	Explorer.EXE	2180	RegOpenKey	HKLM\Software\Microsoft\PolicyManag...	SUCCE

Showing 4,976,643 of 5,904,025 events (84%) Backed by virtual memory

Process Hacker [DESKTOP-KQ703T8\acids]

Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk

Name	PID	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0	27.63		60 kB	NT AUTHORITY\SYSTEM	
System	4	5.23		196 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	352			1.04 MB		Windows Session Manager
Memory Compression	1588			0.99 MB		
Interrupts		2.31		0		Interrupts and DPCs
Registry	92	1.55	664 kB/s	10.69 MB		
csrss.exe	452			1.75 MB		Client Server Runtime Process
wininit.exe	524			1.31 MB		Windows Start-Up Application
services.exe	656			4.73 MB		Services and Controller app
svchost.exe	772			11.23 MB		Host Process for Windows Ser...
dllhost.exe	3612			3.05 MB		COM Surrogate
TextInputHost.exe	4036			8.74 MB	DESKTOP-KQ703T8\acid:	
StartMenuExperie...	3236			20.06 MB	DESKTOP-KQ703T8\acid:	
RuntimeBroker.exe	3412			6.04 MB	DESKTOP-KQ703T8\acid:	Runtime Broker
SearchApp.exe	4456			123.12 MB	DESKTOP-KQ703T8\acid:	Search application
RuntimeBroker.exe	644			7.54 MB	DESKTOP-KQ703T8\acid:	Runtime Broker
ShellExperienceH...	5260			18.17 MB	DESKTOP-KQ703T8\acid:	Windows Shell Experience Host
SkypeBackground...	5380			2.01 MB	DESKTOP-KQ703T8\acid:	Microsoft Skype
RuntimeBroker.exe	5500			6.34 MB	DESKTOP-KQ703T8\acid:	Runtime Broker
ApplicationFrame...	5836			4.19 MB	DESKTOP-KQ703T8\acid:	Application Frame Host
RuntimeBroker.exe	6804			3.2 MB	DESKTOP-KQ703T8\acid:	Runtime Broker
SearchApp.exe	2280			11.84 MB	DESKTOP-KQ703T8\acid:	Search application
msedgewebvie...	6004			31.22 MB	DESKTOP-KQ703T8\acid:	Microsoft Edge WebView2

CPU Usage: 72.37% Physical memory: 3.97 GB (49.61%) Processes: 133

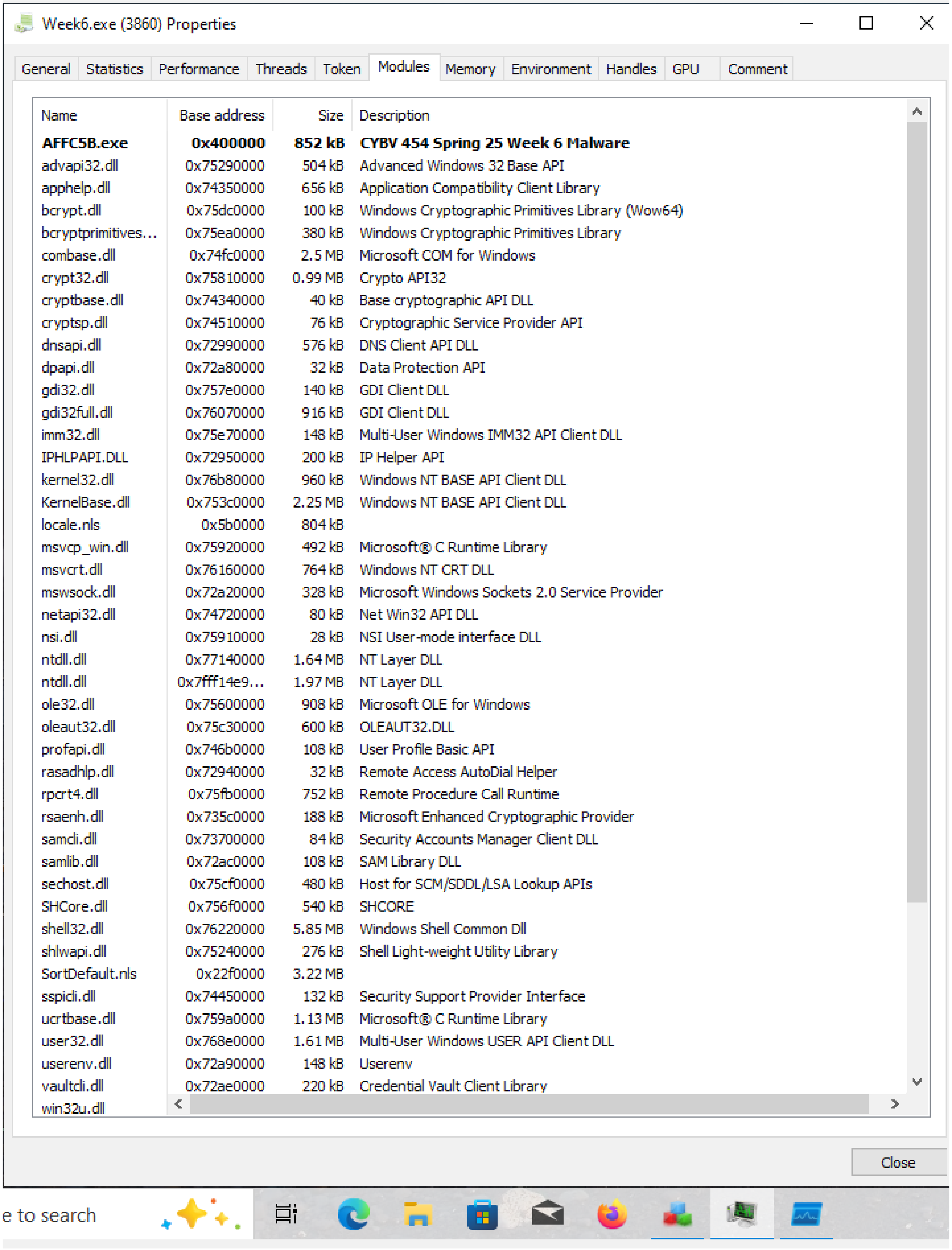
```
.text:004139DE                 push    ebp
.text:004139DF                 mov     ebp, esp
.text:004139E1                 push    ecx
.text:004139E2                 and     [ebp+var_4], 0
```

Process Hacker [DESKTOP-KQ703T8\acids]

Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Network (Ctrl+K)
Processes Services Network Disk

Name	Local address	Local p...	Remote address	Rem...	Prot...	State	Owner
lsass.exe (6...	DESKTOP-KQ703T8	49664			TCP	Listen	
lsass.exe (6...	DESKTOP-KQ703T8	49664			TCP6	Listen	
services.ex...	DESKTOP-KQ703T8	49669			TCP	Listen	
services.ex...	DESKTOP-KQ703T8	49669			TCP6	Listen	
spoolsv.ex...	DESKTOP-KQ703T8	49668			TCP	Listen	Spooler
spoolsv.ex...	DESKTOP-KQ703T8	49668			TCP6	Listen	Spooler
svchost.ex...	DESKTOP-KQ703T8	49666			TCP	Listen	Schedule
svchost.ex...	DESKTOP-KQ703T8	49666			TCP6	Listen	Schedule
svchost.ex...	DESKTOP-KQ703T8	49667			TCP	Listen	EventLog
svchost.ex...	DESKTOP-KQ703T8	49667			TCP6	Listen	EventLog
svchost.ex...	DESKTOP-KQ703T8	1900			UDP		SSDPSRV
svchost.ex...	DESKTOP-KQ703T8	49666			UDP		SSDPSRV
svchost.ex...	DESKTOP-KQ703T8	1900			UDP6		SSDPSRV
svchost.ex...	DESKTOP-KQ703T8	49665			UDP6		SSDPSRV
svchost.ex...	DESKTOP-KQ703T8	49664			UDP		iphlpsvc
svchost.ex...	DESKTOP-KQ703T8	5040			TCP	Listen	CDPSvc
svchost.ex...	DESKTOP-KQ703T8	5050			UDP		CDPSvc
svchost.ex...	DESKTOP-KQ703T8	123			UDP		W32Time
svchost.ex...	DESKTOP-KQ703T8	123			UDP6		W32Time
svchost.ex...	DESKTOP-KQ703T8	7680			TCP	Listen	DoSvc
svchost.ex...	DESKTOP-KQ703T8	7680			TCP6	Listen	DoSvc
svchost.ex...	DESKTOP-KQ703T8	135			TCP	Listen	RpcSs
svchost.ex...	DESKTOP-KQ703T8	135			TCP6	Listen	RpcSs
System (4)	DESKTOP-KQ703T8	445			TCP	Listen	
System (4)	DESKTOP-KQ703T8	445			TCP6	Listen	
wininit.exe...	DESKTOP-KQ703T8	49665			TCP	Listen	
wininit.exe...	DESKTOP-KQ703T8	49665			TCP6	Listen	

CPU Usage: 2.98% Physical memory: 4.38 GB (54.77%) Processes: 127



Name	Base address	Size	Description
AFFC5B.exe	**0x400000**	**852 kB**	**CYBV 454 Spring 25 Week 6 Malware**
advapi32.dll	0x75290000	504 kB	Advanced Windows 32 Base API
apphelp.dll	0x74350000	656 kB	Application Compatibility Client Library
bcrypt.dll	0x75dc0000	100 kB	Windows Cryptographic Primitives Library (Wow64)
bcryptprimitives...	0x75ea0000	380 kB	Windows Cryptographic Primitives Library
combase.dll	0x74fc0000	2.5 MB	Microsoft COM for Windows
crypt32.dll	0x75810000	0.99 MB	Crypto API32
cryptbase.dll	0x74340000	40 kB	Base cryptographic API DLL
cryptsp.dll	0x74510000	76 kB	Cryptographic Service Provider API
dnsapi.dll	0x72990000	576 kB	DNS Client API DLL
dpapi.dll	0x72a80000	32 kB	Data Protection API
gdi32.dll	0x757e0000	140 kB	GDI Client DLL
gdi32full.dll	0x76070000	916 kB	GDI Client DLL
imm32.dll	0x75e70000	148 kB	Multi-User Windows IMM32 API Client DLL
IPHLPAPI.DLL	0x72950000	200 kB	IP Helper API
kernel32.dll	0x76b80000	960 kB	Windows NT BASE API Client DLL
KernelBase.dll	0x753c0000	2.25 MB	Windows NT BASE API Client DLL
locale.nls	0x5b0000	804 kB	
msvcp_win.dll	0x75920000	492 kB	Microsoft® C Runtime Library
msvcrt.dll	0x76160000	764 kB	Windows NT CRT DLL
mswsock.dll	0x72a20000	328 kB	Microsoft Windows Sockets 2.0 Service Provider
netapi32.dll	0x74720000	80 kB	Net Win32 API DLL
nsi.dll	0x75910000	28 kB	NSI User-mode interface DLL
ntdll.dll	0x77140000	1.64 MB	NT Layer DLL
ntdll.dll	0x7fff14e9...	1.97 MB	NT Layer DLL
ole32.dll	0x75600000	908 kB	Microsoft OLE for Windows
oleaut32.dll	0x75c30000	600 kB	OLEAUT32.DLL
profapi.dll	0x746b0000	108 kB	User Profile Basic API
rasadhlp.dll	0x72940000	32 kB	Remote Access AutoDial Helper
rpcrt4.dll	0x75fb0000	752 kB	Remote Procedure Call Runtime
rsaenh.dll	0x735c0000	188 kB	Microsoft Enhanced Cryptographic Provider
samcli.dll	0x73700000	84 kB	Security Accounts Manager Client DLL
samlib.dll	0x72ac0000	108 kB	SAM Library DLL
sechost.dll	0x75cf0000	480 kB	Host for SCM/SDDL/LSA Lookup APIs
SHCore.dll	0x756f0000	540 kB	SHCORE
shell32.dll	0x76220000	5.85 MB	Windows Shell Common Dll
shlwapi.dll	0x75240000	276 kB	Shell Light-weight Utility Library
SortDefault.nls	0x22f0000	3.22 MB	
sspicli.dll	0x74450000	132 kB	Security Support Provider Interface
ucrtbase.dll	0x759a0000	1.13 MB	Microsoft® C Runtime Library
user32.dll	0x768e0000	1.61 MB	Multi-User Windows USER API Client DLL
userenv.dll	0x72a90000	148 kB	Userenv
vaultcli.dll	0x72ae0000	220 kB	Credential Vault Client Library
win32u.dll			

Dynamic Analysis

1. Analysis Environment

Environment Setup

- Virtual Machine specifications:
  - [OS version] WIndows 10
  - [Memory allocation]: 8GB
  - [Network configuration]: Not attached
- Monitoring tools deployed:
  - [Process monitoring]
    - Ensure you use RegShot, Process Monitor, Process Explorer
    - I used regshot, process monitor, and process hacker
  - [Network monitoring]
    - Ensure you use Wireshark
  - [File system monitoring]
- Safety measures implemented:
  - [Network isolation]
    - Try the analysis with and without Fakenet
    - Network not attached, I do not want the malware to spread on my network
  - [Snapshot configuration] clean snapshot set with tools installed
  - [Additional protections]: none

2. Runtime Observations

Initial Execution:

- [Immediate system changes]
  - No windows popped up, but I observed running processes in processhacker and procmon
- [Process creation]
  - AFFC5B.exe
  - crypt32.dll
  - oleaut132.dll
  - CloseFile
  - CreateFile
  - QuerySIzeInformationVolume
  - RegOpenKey
  - RegQueryKey
  - RegCloseKey
- [Registry creation]
  - Keys added: 1

    - Values deleted: 1
    - Values added: 3
        - HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1944\Terminator: "HAM"
    - Total changes: 16
- [Network activity]
    - Lsass.exe
    - Tcp activity on port 49664
    - Activity on port 445, 135, 7680, 123, 5040, 5050, 1900
- [File system changes]
    - CreateFile
    - CloseFIle

1. User Impact Assessment

Home Users

- Potential impact:
    - Loss of personal email credentials
    - Potential for further malware infections through stolen credentials.
    - Potential for personal files to be stolen.
- Risk level: High.
- Data compromise potential: Very high, given the malware's focus on credential theft.

Business Users

- Operational impact:
    - Compromised business email accounts leading to data breaches. Loss of sensitive customer data. Disruption of business operations due to compromised FTP or other access credentials. Potential for Ransomware or other malware to be installed via the initial infection.
- Data security concerns:
    - Exposure of confidential business data (financial records, customer information, intellectual property). Potential for regulatory fines due to data breaches. Loss of trust from customers.
- Financial implications:
    - Costs associated with incident response and data recovery. Potential legal and regulatory fines. Loss of revenue due to downtime and reputational damage.

Government Users

- Security implications:
    - Compromised government systems and networks.
    - Potential for espionage and data exfiltration of sensitive government information.
    - Disruption of critical government services.
    - Potential for the malware to be used as a foothold for a larger attack.

- Data sensitivity concerns:
  - Exposure of classified information.
  - Compromise of citizen data and government databases.
- Operational disruption potential: High, especially if critical infrastructure is targeted.

2. Mitigation Strategy

Immediate Response

- Initial containment steps:
  - Disconnect affected systems from the network immediately.
  - Isolate the infected machine
  - Perform a full system antivirus scan
  - Change all potentially compromised passwords.
- System isolation procedures:
  - Disable network adapters.
  - Use a bootable rescue disk to scan and clean the system.
  - Restore the affected system from a clean backup if available.
- Data preservation methods:
  - Back up critical data

Long-term Prevention

- Security control recommendations:
  - Implement strong password policies and multi-factor authentication.
  - Regularly update antivirus and anti-malware software.
  - Regularly perform vulnerability scans and penetration testing.
- Policy modifications:
  - Develop and enforce a robust incident response plan.
  - Create and enforce a strict password policy.
- Training requirements:
  - Conduct regular security awareness training for all users.
  - Educate users on phishing and social engineering tactics.
  - Train users on safe browsing habits.

Conclusion

1. Analysis Reflection

- Summary of findings:
  - The malware is a credential-stealing Trojan with capabilities to steal data from browsers, email clients, and FTP clients. It exhibits suspicious behavior, including unusual file sections, network communication, and process manipulation. The malware targets a wide range of applications, indicating a broad scope of data theft.
- Unusual characteristics:
  - The discrepancy between the file creation date and the first submission date.
  - The presence of the ".x" section with low entropy.
  - The string "fuckav.ru".

- Learning outcomes:
    - The importance of thorough static and dynamic analysis in malware analysis and using multiple tools and techniques to identify malicious behavior.
- Additional research needed:
    - Further analysis of the malware's command-and-control connections
    - Reverse engineering the malware's payload to understand its full capabilities.

2. Evidence Documentation

- Screenshot descriptions and relevance:
- Tool output documentation:
    - VirusTotal reports.
    - DIE reports.
    - Process Monitor logs.
    - Process Hacker logs.
    - IDA Pro disassembly and function graphs.
- Additional supporting materials: