Static Analysis

1. Virus Total Analysis

Hash Analysis

- File Hash:
  - MD5: 4ab35d36922cb1eff9ce2a0bd86088ca
  - SHA-1: 0dab981c732975a2bdbbf577cfbd90434b6cfc2b
  - SHA-256:171bebac610031563942c73669f95151c9edbcb2392b2b6cea1493507cf6c7e8
- Method of hash acquisition:
  - Found on VirusTotal and verified with Detect-It-Easy
- [Link to VirusTotal results]
  - https://www.virustotal.com/gui/file/171bebac610031563942c73669f95151c9edbcb2392b2b6cea1493507cf6c7e8/detection

Vendor Analysis

- Number of vendors flagging as malicious: 44/72
- Analysis of vendor results:
  - Discuss patterns in detection
    - peexe
    - detect-debug-environment
    - calls-wmi
    - 64bits
    - upx
    - corrupt
    - persistence
  - [Common malware names identified]
    - stealer
    - gensteal
    - trojanstealer
    - TMPNstealer
    - Win64EvoGen

File History

- First Submission Date: 2025-04-07 19:28:37 UTC
- File Creation Date from Windows: unknown

Community Score

- [Link to your VirusTotal community contribution]
  - https://www.virustotal.com/gui/file/171bebac610031563942c73669f95151c9edbcb2392b2b6cea1493507cf6c7e8/community
- Username:sshinn
  - It bypasses User Account Control using fodhelper.exe to gain admin rights. UAC bypass via fodhelper is a common malware technique to gain admin privileges. It changes the registry to make itself run automatically when the system starts. It uses system tools like cmd.exe, wmic.exe, and attrib.exe to change system settings and hide itself. It checks for the computer’s

external IP address—common behavior in malware that reports to a command-and-control (C2) server. It likely steals sensitive information and modifies system settings for persistence.

2. Detect It Easy (DIE) Analysis

File information

- File type: PE64
- Architecture: AMD64
- Additional relevant information:
    - [List notable file characteristics]
        - File names:
            - FREE AI Homework Helper Week11.exe
            - Week11.exe
            - SecurityHealthSystray.exe
        - Packer: UPX (3.91+) [modified]
        - (Heur)Language: ASMx64
    - [Unusual headers or structures]
        - UPX0
        - UPX1
        - UPX2

Memory Map Analysis

- Section breakdown:
    - UPX0: 4096 8040448
        - Raw size:0
        - Entropy: 0
        - Permissions: RWE
    - UPX1:
        - Raw size: 752844
        - Entropy: 8
        - Permissions: RWE
    - UPX2:
        - Raw size: 512
        - Entropy: 1.37
        - Permissions: RW
    - .rsrc:
        - Raw size:183808
        - Entropy: 5.11
        - Permissions: R
- Notable findings:
    - Read Write Execute Permissions in UPX0 and UPX1 suggest that these sections have full access

String Analysis

- Notable strings discovered:
    - KERNEL32.DLL: can be used by malware for system operations.
    - ExitProcess: commonly used in malware to terminate itself or other processes.

    - LoadLibraryA: used to load DLLs into memory. Malware often uses this to load malicious code into a process's memory, it could indicate that a malicious payload is being injected.
    - VirtualProtect: Malware may use this to inject code into memory by changing permissions
    - 040904E4: This is a locale code, which represents "English - United States (Windows)."
    - University of Arizona Malware Analysis: Created for CYBV454
    - GetProcAddress

Entropy Analysis

- Overall entropy score: 7.99143[
- Section-specific entropy:
    - UPX1: 7.999 Entropy
- Packing analysis:
    - [Packed/Unpacked determination]
        - This file is packed
    - [Packer identified (if applicable)]
        - UPX packer
    - [Unpacking methodology (if attempted)]
        - I used the Detect-It-Easy extractor and it unpacked to a .PNG file and a .zlib file
        - FREE AI Homework Helper Week11.exe.00_0075b600.exe
        - FREE AI Homework Helper Week11.exe.0075623c_4f55.png
        - FREE AI Homework Helper Week11.exe.00756272_4f0f.zlib
        - FREE AI Homework Helper Week11.patch.JSON

4. Disassembly Analysis

- Found entry point in function
- Found some malicious apis such as VirtualProtect and GetProcAddress
- Apphelp.dll which seemed suspicious
- Used Ghidra and x64dbg
- In Ghidra, imports are as follows
    - KERNEL32.DLL
        - ExitProcess
        - GetProcAddress
        - LoadLibraryA
        - VirtualProtect

4. Static Analysis Summary

- Key findings from static analysis:
    - The file appears to be malicious. One of the most significant indicators is that 44 out of 72 antivirus vendors flagged this file as dangerous on VirusTotal. The file has been linked to known types of malware, such as "stealer" and "trojanstealer," which are programs designed to steal personal information. The

file also uses some suspicious system functions, like VirtualProtect and GetProcAddress, which are often used by malware to manipulate or inject malicious code into running programs. These behaviors suggest the file could try to alter other programs or system processes.

- Potential functionality:
    - Based on the analysis, it looks like the file is designed to be malicious once executed. The fact that it is packed using a tool called UPX, which is often used to hide malicious code, means it is trying to avoid detection by security tools. When the file runs, it might try to inject malicious code into other processes or alter system settings to make itself harder to find. The file may also be trying to steal personal data, as indicated by the "stealer" label found in its detection. Additionally, the file seems to have mechanisms that allow it to stay on the computer even after a restart, which is typical of malware that tries to stay hidden and keep running in the background.
- Risk indicators:
    - There are several warning signs that suggest this file is a significant security risk. First, the fact that 44 antivirus vendors flagged it as malicious is a strong indication that it is harmful. The file’s use of UPX to pack and hide its contents is another red flag, as this is often done to prevent security tools from analyzing the file. Furthermore, the file has been identified as a trojanstealer, meaning it is likely designed to steal sensitive information from the user’s computer. The use of system functions like LoadLibraryA, which allows the file to load other harmful code, and ExitProcess, which can terminate or crash programs, are also typical behaviors of malware. These factors all point to the file being a dangerous threat that could cause damage if run on a computer.

Dynamic Analysis
1. Analysis Environment
Environment Setup

- Virtual Machine specifications:
    - [OS version]
    - [Memory allocation]
    - [Network configuration]
- Monitoring tools deployed:
    - [Process monitoring]
        - Ensure you use RegShot, Process Monitor, Process Explorer
    - [Network monitoring]
        - Ensure you use Wireshark
    - [File system monitoring]
- Safety measures implemented:

    - [Network isolation]
        - Try the analysis with and without Fakenet
    - [Snapshot configuration]
    - [Additional protections]

2. Runtime Observations

Initial Execution

- Malicious:
    - Bypass User Account Control (Modify registry)
        - FREE AI Homework Helper Week11.exe (PID: 4756)
    - Bypass User Account Control (fodhelper)
        - fodhelper.exe (PID: 5048)
    - Changes the autorun value in the registry
        - FREE AI Homework Helper Week11.exe (PID: 5892)
- Suspicious:
    - Changes default file association
        - FREE AI Homework Helper Week11.exe (PID: 4756)
    - Starts CMD.EXE for commands execution
        - FREE AI Homework Helper Week11.exe (PID: 4756)
    - Creates or modifies Windows services
        - FREE AI Homework Helper Week11.exe (PID: 5892)
    - Uses ATTRIB.EXE to modify file attributes
        - FREE AI Homework Helper Week11.exe (PID: 5892)
    - Executable content was dropped or overwritten
        - FREE AI Homework Helper Week11.exe (PID: 5892)
    - Adds/modifies Windows certificates
        - FREE AI Homework Helper Week11.exe (PID: 5892)
    - Uses WMIC.EXE to obtain Windows Installer data
        - FREE AI Homework Helper Week11.exe (PID: 5892)
    - Accesses product unique identifier via WMI (SCRIPT)
        - WMIC.exe (PID: 5376)
    - Checks for external IP
        - FREE AI Homework Helper Week11.exe (PID: 5892)
        - svchost.exe (PID: 2196)
- [Process creation]
    - PID: 5048, C:\WINDOWS\system32\fodhelper.exe
    - cmd.exe
    - WMIC.exe
- [Registry modifications]
    - Total events: 5321
    - Read events: 5309
    - Write events: 9
    - Delete events: 3
    - (4756) FREE AI Homework Helper Week11.exe
    - Key: HKEY_CLASSES_ROOT\ms-settings\shell\open\command
    - Operation: DelegateExecute
    - (4756) FREE AI Homework Helper Week11.exe
    - Key: HKEY_CLASSES_ROOT\ms-settings\shell\open\command

        - Operation: delete value
        - Name: DelegateExecute
        - (5048) fodhelper.exe
        - Key:HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
        - Operation: write
        - Name: SlowContextMenuEntries
        - Value:6024B221EA3A6910A2DC08002B30309D0A010000BD0E0C47735D584D9CEDE91E22E23282770100000114020000000000C0000000000000468D0000006078A409B011A54DAFA526D86198A780390100009AD298B2EDA6DE11BA8CA68E55D895936E000000
        - (5048) fodhelper.exe
        - Key:HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Content
        - Operation: write
        - Name: CachePrefix
        - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies
- Network activity summary:
    - ET INFO External IP Address Lookup Domain (ipify .org) in TLS SNI
        - (ip.addr == 104.26.12.205 && tcp.port == 443) && (ip.addr == 192.168.100.10 && tcp.port == 49743)
        - Src IP: 192.168.100.10
        - Dst IP:104.26.12.205
    - ET INFO External IP Lookup Domain (ipify .org) in DNS Lookup
        - Src IP: 192.168.100.10
        - Dst IP: 192.168.100.2
        - Domain: api.ipify.org
    - Device Retrieving External IP Address Detected, ET INFO External IP Lookup ip-api.com
        - Src IP: 192.168.100.10
        - Dst IP: 208.95.112.1
    - INFO [ANY.RUN] External IP Check (ip-api .com)
        - Src IP: 192.168.100.10
        - Dst IP: 192.168.100.2
        - Domain: ip-api.com

Impact Analysis

Home Users

- Potential impact: Personal info like passwords could be stolen
- Risk level: High.
- Data compromise potential: Yes – identity theft or data leaks

Business Users

- Operational impact: Systems may slow down or crash
- Data security concerns: Sensitive company data could be stolen
- Financial implications: Possible financial loss or reputation damage

Government Users

- Security implications: Could lead to leaks of confidential information
- Data sensitivity concerns: National security data might be at risk

- Operational disruption potential: Services could be interrupted

2. Mitigation Strategy

Immediate Response

- Initial containment steps: Stop running the infected file immediately
- System isolation procedures: Disconnect the device from the internet/network
- Data preservation methods: Save memory dumps, logs, and the file for investigation

Long-term Prevention

- Security control recommendations: Use antivirus and endpoint protection; block packed executables.
- Policy modifications: Block unknown programs and restrict admin privileges.
- Training requirements: Teach users not to download strange or unknown files.

Conclusion

1. Analysis Reflection
   - Summary of findings: The file is malware, flagged by 44 antivirus tools. It can steal info, change system settings, and stay hidden.
   - Unusual characteristics: Packed with UPX
   - Learning outcomes: Learned about packing and how malware checks for network access.

2. Evidence Documentation
   - Screenshot descriptions and relevance: Screenshots of VirusTotal results, RegShot registry changes, and Wireshark network logs showing external IP access.
   - Tool output documentation: Logs from DIE (packing info), Process Monitor (PID actions), and RegShot (registry changes).
   - Additional supporting materials: Unpacked .PNG and .zlib files, JSON patch, autorun registry edits, and process tree screenshots.

Your Report Should Answer:

What is this malware doing behind the scenes?

- It bypasses User Account Control using fodhelper.exe to gain admin rights.
  - UAC bypass via fodhelper is a common malware technique to gain admin privileges
- It changes the registry to make itself run automatically when the system starts.
- It uses system tools like cmd.exe, wmic.exe, and attrib.exe to change system settings and hide itself.
- It checks for the computer’s external IP address—common behavior in malware that reports to a command-and-control (C2) server.
- It likely steals sensitive information and modifies system settings for persistence.

What kind of threat does this malware represent (e.g., spyware, info-stealer,

trojan, etc.)?

- Info-Stealer: It's flagged as a stealer and trojanstealer, meaning it's likely trying to steal data like usernames, passwords, and system info.
- Trojan: It acts like a normal program (FREE AI Homework Helper), but secretly performs malicious actions.

What are the options for containment and recovery?

- Containment:
  - Disconnect the infected computer from the network immediately.
  - Kill the process and stop any associated services.
  - Do not delete the file right away—preserve it for investigation.
- Recovery:
  - Restore from a clean backup made before the infection.
  - Reinstall the operating system if necessary.
  - Change all passwords and monitor for suspicious activity.

When during execution do key actions take place (before/after error)?
execution before error

- Gains admin access using fodhelper.exe
- Edits registry keys to run at startup
- Changes default file settings and drops extra payloads

after error

- Connects to the internet to check IP
- May attempt to send stolen data or receive instructions from a C2 server

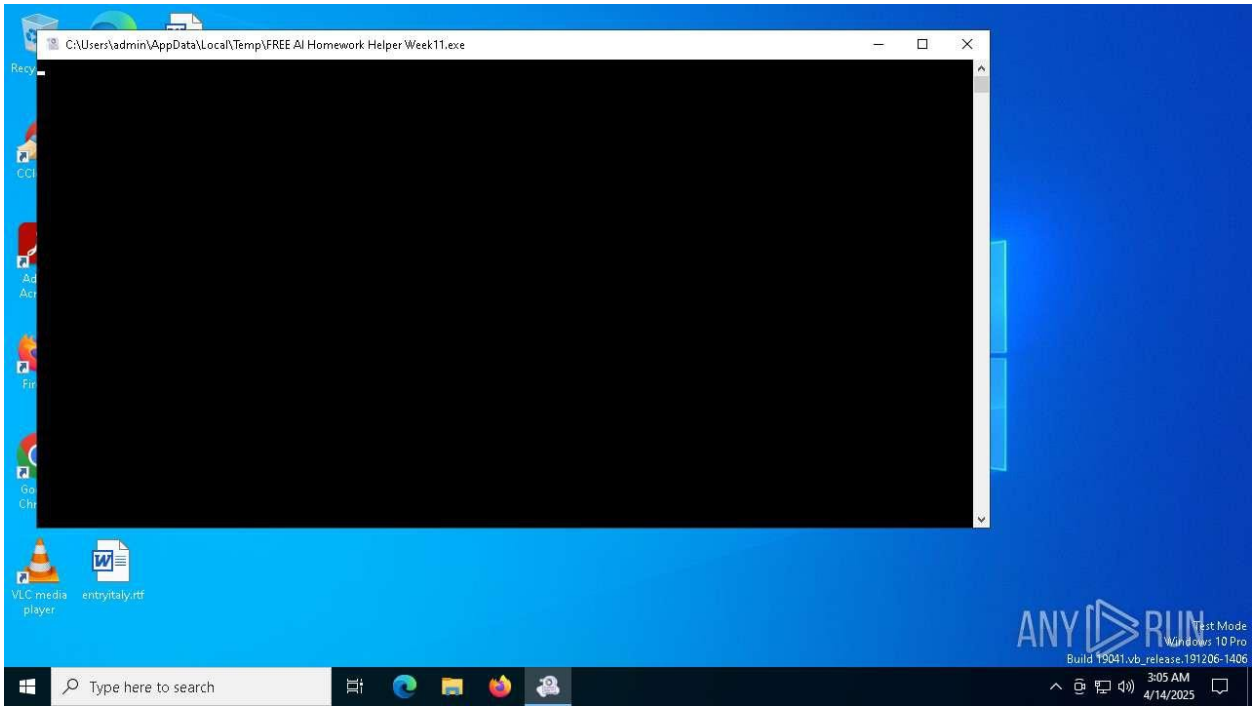
How does this malware attempt to deceive users or avoid detection?

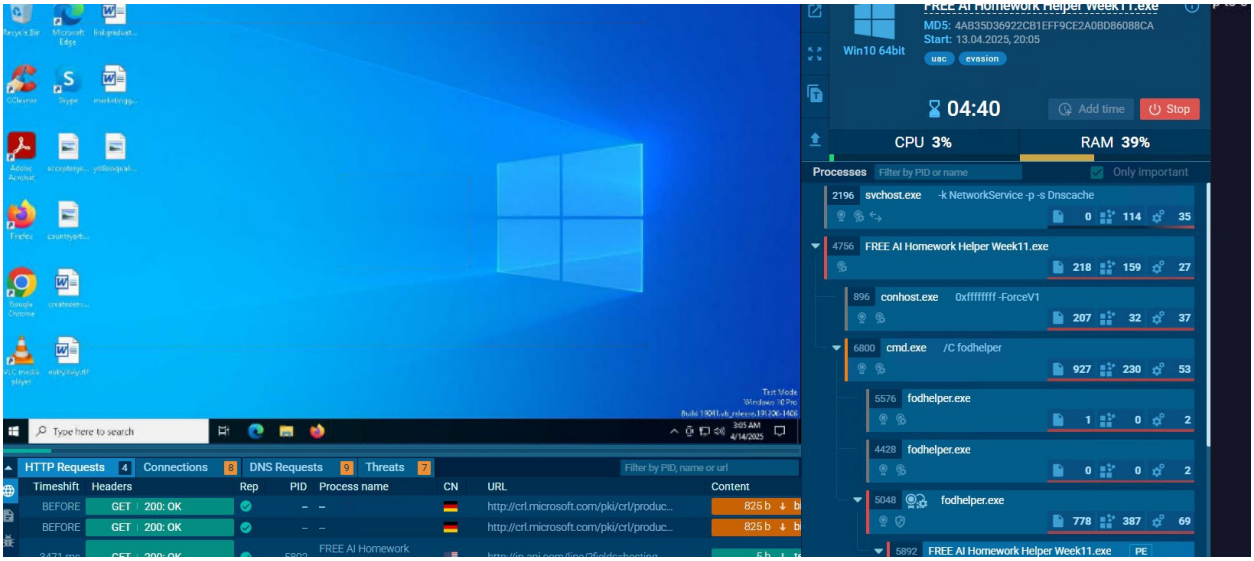
- Packed with UPX to hide its real code and confuse antivirus scanners.
- Uses names like "FREE AI Homework Helper" to trick users into trusting and running it.
- Uses legit system tools (cmd, wmic, attrib) to blend in with normal Windows behavior.
- Alters registry keys (using fodhelper.exe)..

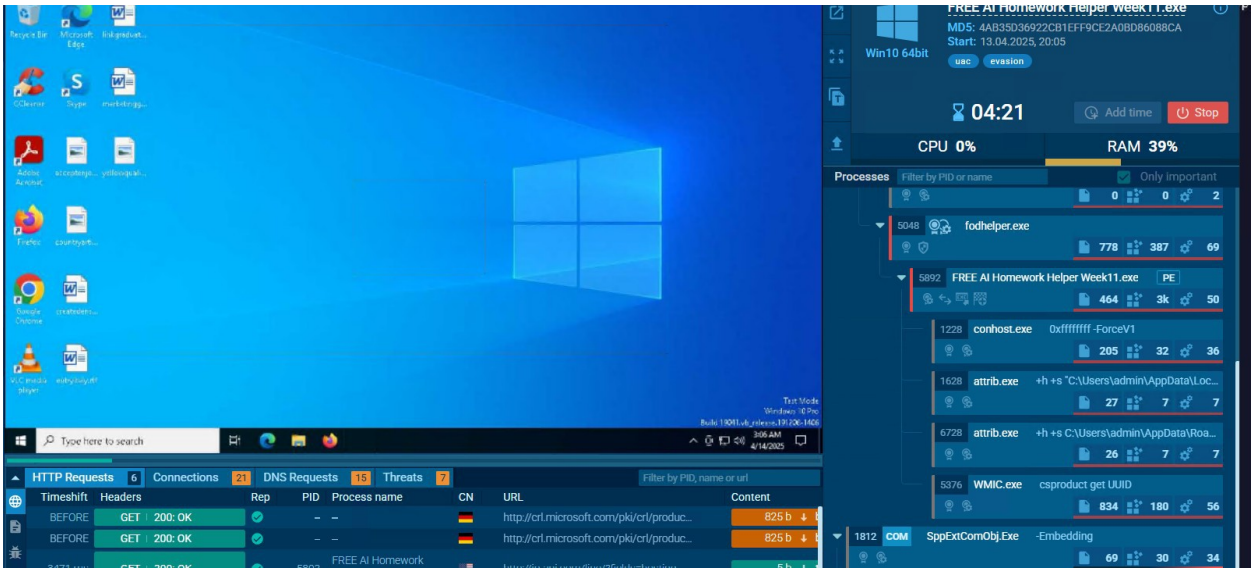
Your report must include:
Evidence from x64dbg/x86dbg shows function calls, memory writes, or suspicious behavior.
At least one disassembly screenshot or analysis from your preferred tool.
Examination of relevant import/export tables, strings, and execution flow.

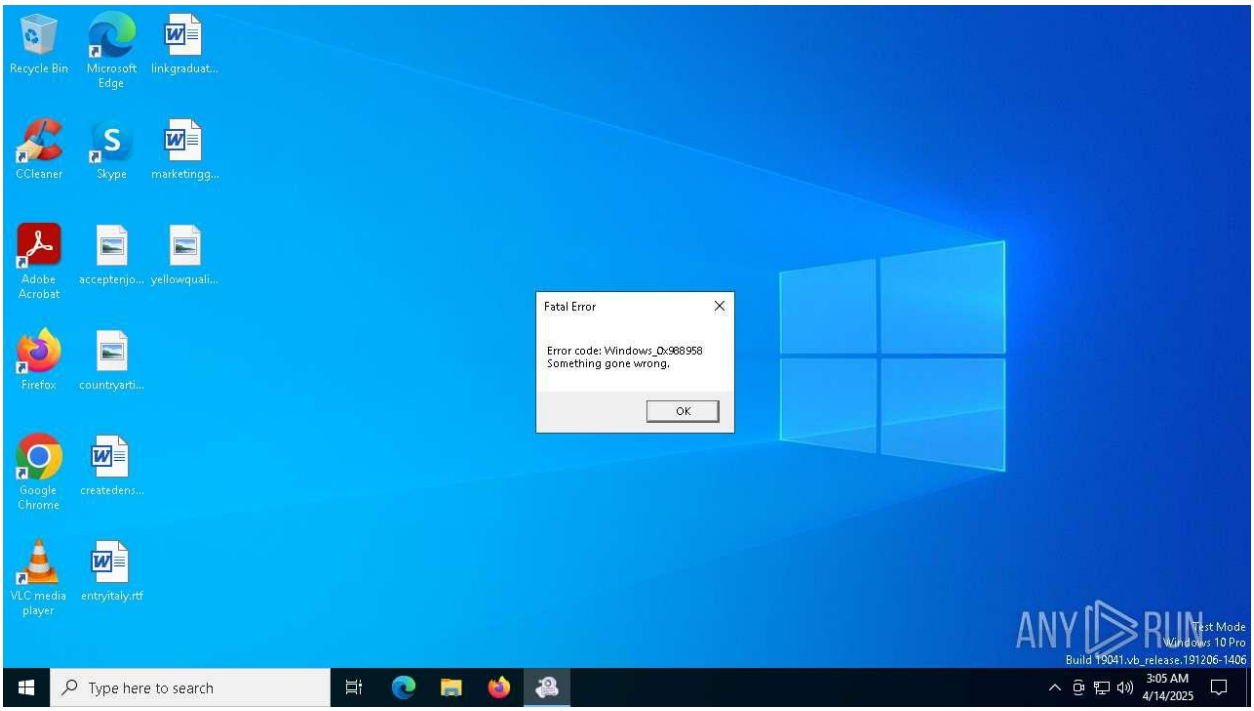
Documentation of at least four Indicators of Compromise (IoCs), including but not limited to:

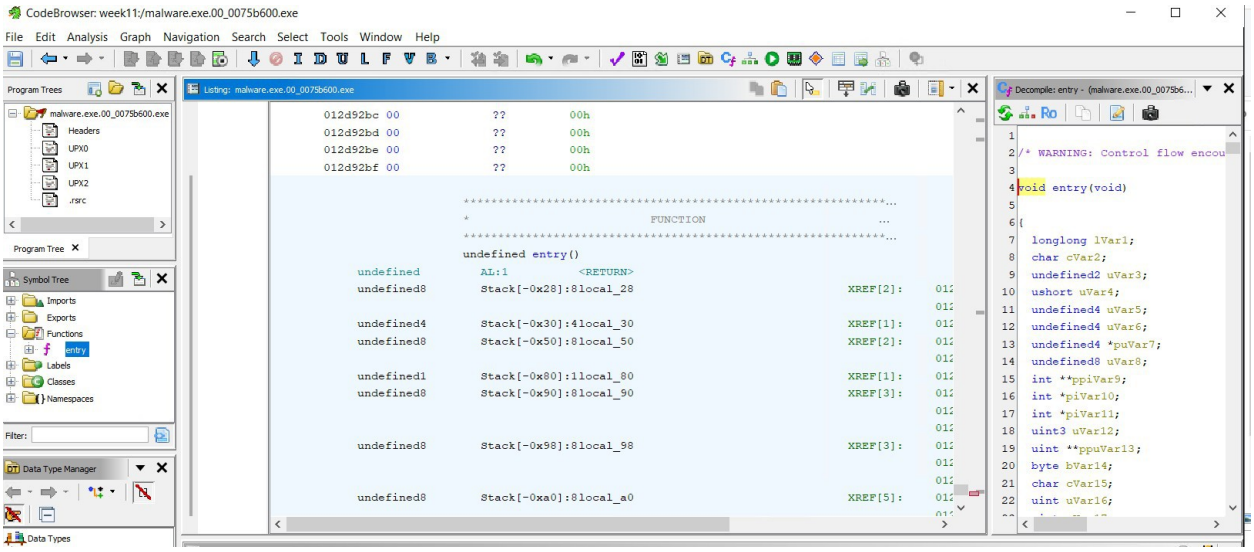
1. The malware modified the HKEY_CLASSES_ROOT\ms-settings\shell\open\command registry key and removed the DelegateExecute value to exploit fodhelper.exe for UAC bypass and gain elevated privileges.
2. The executable altered the autorun registry settings, ensuring it would automatically launch during system startup
3. It spawned multiple suspicious processes such as cmd.exe, wmic.exe, and attrib.exe, and it was heavily packed
4. The malware contacted external IP lookup services like ipify.org and ip-api.com, indicating potential command-and-control (C2) communication

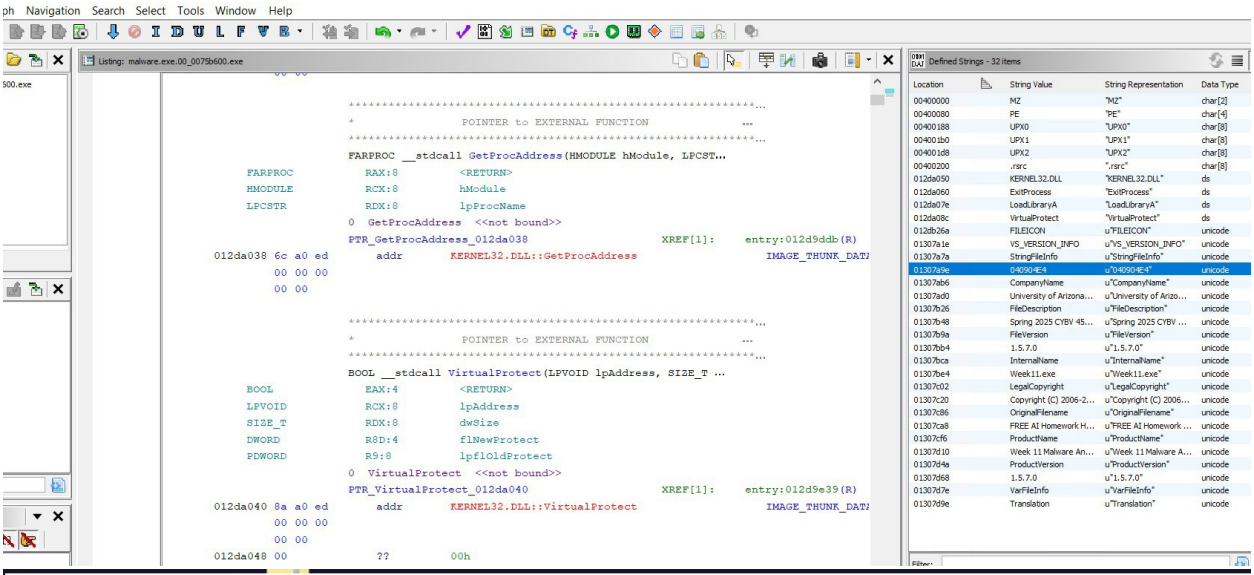

C:\Users\admin\AppData\Local\Temp\FREE AI Homework Helper Week11.exe
VLC media player
entryitaly.rtf
Type here to search
Test Mode
Windows 10 Pro
Build 19041.vb_release.191206-1406
3:05 AM
4/14/2025

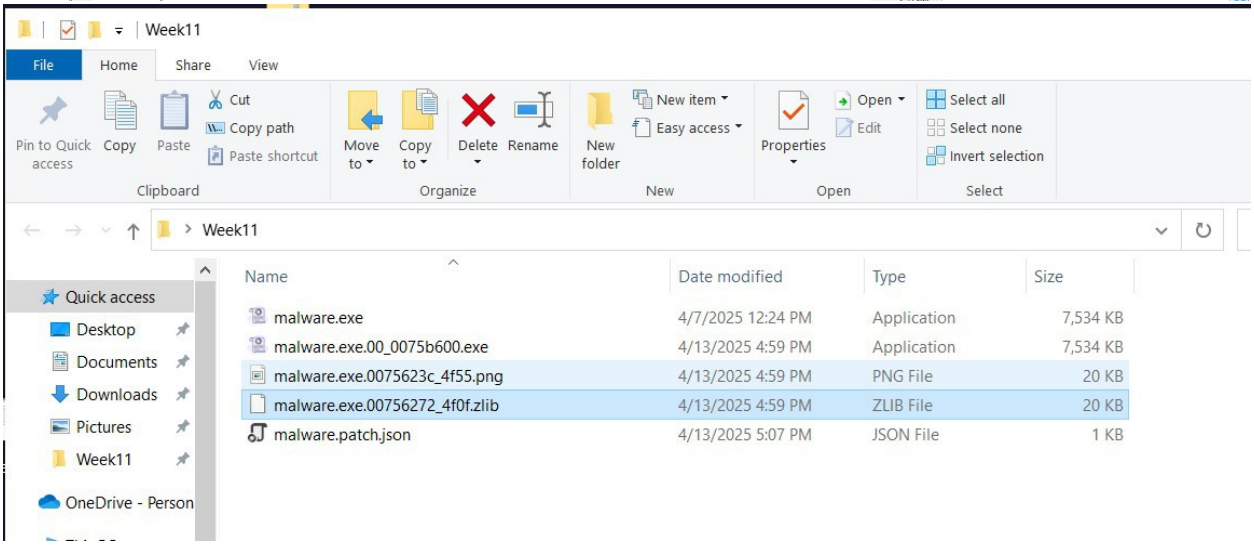

Win10 64bit
MD5: 4AB35D36922CB1EFF9CE2A0BD86088CA
Start: 13.04.2025, 20:05
uac
evasion
04:40
Add time
Stop
CPU 3%
RAM 39%
Processes
Filter by PID or name
Only important
2196 svchost.exe -k NetworkService -p -s Dnscache
4756 FREE AI Homework Helper Week11.exe
896 conhost.exe 0xffffffff -ForceV1
6800 cmd.exe /C fodhelper
5576 fodhelper.exe
4428 fodhelper.exe
5048 fodhelper.exe
5892 FREE AI Homework Helper Week11.exe
HTTP Requests 4
Connections 8
DNS Requests 9
Threats 7
Timeshift
Headers
Rep
PID
Process name
CN
URL
Content
BEFORE GET 200: OK http://crl.microsoft.com/pki/crl/produc... 825 b
BEFORE GET 200: OK http://crl.microsoft.com/pki/crl/produc... 825 b


FREE AI Homework Helper Week11.exe
MD5: 4AB35D36922CB1EFF9CE2A0BD86088CA
Start: 13.04.2025, 20:05
Win10 64bit
uac
evasion
04:21
Add time
Stop
CPU 0%
RAM 39%
Processes
Filter by PID or name
Only important
5048 fodhelper.exe
5892 FREE AI Homework Helper Week11.exe PE
1228 conhost.exe 0xffffffff -ForceV1
1628 attrib.exe +h +s "C:\Users\admin\AppData\Loc...
6728 attrib.exe +h +s C:\Users\admin\AppData\Roa...
5376 WMIC.exe csproduct get UUID
1812 COM SppExtComObj.Exe -Embedding
HTTP Requests 6
Connections 21
DNS Requests 15
Threats 7
Timeshift
Headers
Rep
PID
Process name
CN
URL
Content
BEFORE GET 200: OK
http://crl.microsoft.com/pki/crl/produc...
825 b


Recycle Bin
Microsoft Edge
linkgraduat...
CCleaner
Skype
marketingg...
Adobe Acrobat
acceptenjo...
yellowquali...
Firefox
countryarti...
Google Chrome
createdens...
VLC media player
entryitaly.rtf
Fatal Error
Error code: Windows_0x988958
Something gone wrong.
OK
ANY RUN
Test Mode
Windows 10 Pro
Build 19041.vb_release.191206-1406
Type here to search
3:05 AM
4/14/2025


CodeBrowser: week11:/malware.exe.00_0075b600.exe
File Edit Analysis Graph Navigation Search Select Tools Window Help
Program Trees
malware.exe.00_0075b600.exe
Headers
UPX0
UPX1
UPX2
.rsrc
Symbol Tree
Imports
Exports
Functions
entry
Labels
Classes
Namespaces
Data Type Manager
Data Types
Listing: malware.exe.00_0075b600.exe
012d92bc 00 ?? 00h
012d92bd 00 ?? 00h
012d92be 00 ?? 00h
012d92bf 00 ?? 00h
FUNCTION
undefined entry()
undefined AL:1 <RETURN>
undefined8 Stack[-0x28]:8 local_28 XREF[2]:
undefined4 Stack[-0x30]:4 local_30 XREF[1]:
undefined8 Stack[-0x50]:8 local_50 XREF[2]:
undefined1 Stack[-0x80]:1 local_80 XREF[1]:
undefined8 Stack[-0x90]:8 local_90 XREF[3]:
undefined8 Stack[-0x98]:8 local_98 XREF[3]:
undefined8 Stack[-0xa0]:8 local_a0 XREF[5]:
Decompile: entry - (malware.exe.00_0075b6...
/* WARNING: Control flow encou
void entry(void)
{
longlong lVar1;
char cVar2;
undefined2 uVar3;
ushort uVar4;
undefined4 uVar5;
undefined4 uVar6;
undefined4 *puVar7;
undefined8 uVar8;
int **ppiVar9;
int *piVar10;
int *piVar11;
uint3 uVar12;
uint **ppuVar13;
byte bVar14;
char cVar15;
uint uVar16;

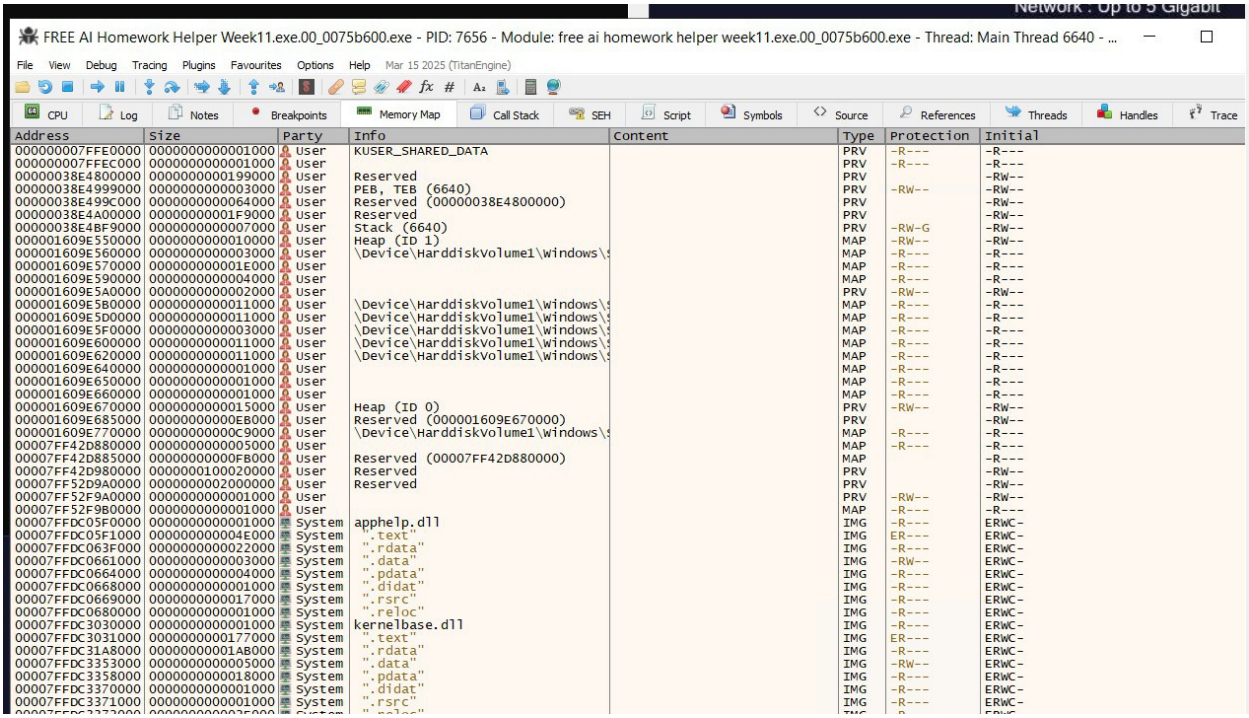

Navigation Search Select Tools Window Help
Listing: malware.exe.00_0075b600.exe
POINTER to EXTERNAL FUNCTION
FARPROC __stdcall GetProcAddress(HMODULE hModule, LPCST...
FARPROC RAX:8 <RETURN>
HMODULE RCX:8 hModule
LPCSTR RDX:8 lpProcName
0 GetProcAddress <<not bound>>
PTR_GetProcAddress_012da038 XREF[1]: entry:012d9ddb(R)
012da038 6c a0 ed 00 00 00 00 00 addr KERNEL32.DLL::GetProcAddress IMAGE_THUNK_DATA
POINTER to EXTERNAL FUNCTION
BOOL __stdcall VirtualProtect(LPVOID lpAddress, SIZE_T ...
BOOL EAX:4 <RETURN>
LPVOID RCX:8 lpAddress
SIZE_T RDX:8 dwSize
DWORD R8D:4 flNewProtect
PDWORD R9:8 lpflOldProtect
0 VirtualProtect <<not bound>>
PTR_VirtualProtect_012da040 XREF[1]: entry:012d9e39(R)
012da040 8a a0 ed 00 00 00 00 00 addr KERNEL32.DLL::VirtualProtect IMAGE_THUNK_DATA
012da048 00 ?? 00h
Defined Strings - 32 items
Location String Value String Representation Data Type
00400000 "MZ" char[2]
00400080 "PE" char[4]
00400188 "UPX0" char[8]
004001b0 "UPX1" char[8]
004001d8 "UPX2" char[8]
00400200 ".rsrc" char[8]
012da050 "KERNEL32.DLL" ds
012da060 "ExitProcess" ds
012da07e "LoadLibraryA" ds
012da08c "VirtualProtect" ds
012db26a "FILEICON" unicode
01307a1e "VS_VERSION_INFO" unicode
01307a7a "StringFileInfo" unicode
01307a9e "040904E4" unicode
01307ab6 "CompanyName" unicode
01307ad0 "University of Arizona..." unicode
01307b26 "FileDescription" unicode
01307b48 "Spring 2025 CYBV 45..." unicode
01307b9a "FileVersion" unicode
01307bb4 "1.5.7.0" unicode
01307bca "InternalName" unicode
01307be4 "Week11.exe" unicode
01307c02 "LegalCopyright" unicode
01307c20 "Copyright (C) 2006-2..." unicode
01307c86 "OriginalFilename" unicode
01307ca8 "FREE AI Homework H..." unicode
01307cf6 "ProductName" unicode
01307d10 "Week 11 Malware An..." unicode
01307d4a "ProductVersion" unicode
01307d68 "1.5.7.0" unicode
01307d7e "VarFileInfo" unicode
01307d9e "Translation" unicode


Week11
File Home Share View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
Open
Select all
Select none
Invert selection
Select
Week11
Quick access
Desktop
Documents
Downloads
Pictures
Week11
OneDrive - Person
Name
Date modified
Type
Size
malware.exe 4/7/2025 12:24 PM Application 7,534 KB
malware.exe.00_0075b600.exe 4/13/2025 4:59 PM Application 7,534 KB
malware.exe.0075623c_4f55.png 4/13/2025 4:59 PM PNG File 20 KB
malware.exe.00756272_4f0f.zlib 4/13/2025 4:59 PM ZLIB File 20 KB
malware.patch.json 4/13/2025 5:07 PM JSON File 1 KB

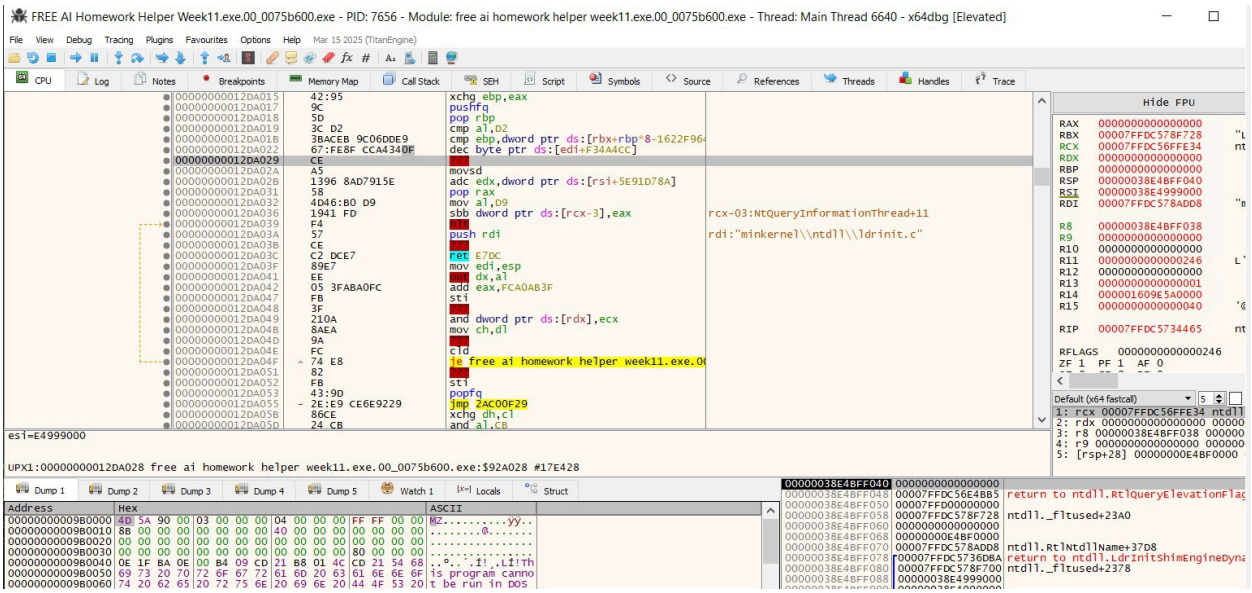
sshinn

a moment ago

It bypasses User Account Control using fodhelper.exe to gain admin rights. UAC bypass via fodhelper is a common malware technique to gain admin privileges. It changes the registry to make itself run automatically when the system starts. It uses system tools like cmd.exe, wmic.exe, and attrib.exe to change system settings and hide itself. It checks for the computer's external IP address—common behavior in malware that reports to a command-and-control (C2) server. It likely steals sensitive information and modifies system settings for persistence.



Address	Size	Party	Info	Content	Type	Protection	Initial
000000007FFE0000	0000000000001000	User	KUSER_SHARED_DATA		PRV	-R---	-R---
000000007FFEC000	0000000000001000	User			PRV	-R---	-R---
00000038E4800000	0000000000199000	User	Reserved		PRV		-RW--
00000038E4999000	0000000000003000	User	PEB, TEB (6640)		PRV	-RW--	-RW--
00000038E499C000	0000000000064000	User	Reserved (00000038E4800000)		PRV		-RW--
00000038E4A00000	00000000001F9000	User	Reserved		PRV		-RW--
00000038E4BF9000	0000000000007000	User	Stack (6640)		PRV	-RW-G	-RW--
000001609E550000	0000000000010000	User	Heap (ID 1)		MAP	-RW--	-RW--
000001609E560000	0000000000003000	User	\Device\Harddiskvolume1\Windows\S		MAP	-R---	-R---
000001609E570000	000000000001E000	User			MAP	-R---	-R---
000001609E590000	0000000000004000	User			MAP	-R---	-R---
000001609E5A0000	0000000000002000	User			PRV	-RW--	-RW--
000001609E5B0000	0000000000011000	User	\Device\Harddiskvolume1\Windows\S		MAP	-R---	-R---
000001609E5D0000	0000000000011000	User	\Device\Harddiskvolume1\Windows\S		MAP	-R---	-R---
000001609E5F0000	0000000000003000	User	\Device\Harddiskvolume1\Windows\S		MAP	-R---	-R---
000001609E600000	0000000000011000	User	\Device\Harddiskvolume1\Windows\S		MAP	-R---	-R---
000001609E620000	0000000000011000	User	\Device\Harddiskvolume1\Windows\S		MAP	-R---	-R---
000001609E640000	0000000000001000	User			MAP	-R---	-R---
000001609E650000	0000000000001000	User			MAP	-R---	-R---
000001609E660000	0000000000001000	User			MAP	-R---	-R---
000001609E670000	0000000000015000	User	Heap (ID 0)		PRV	-RW--	-RW--
000001609E685000	00000000000EB000	User	Reserved (000001609E670000)		PRV		-RW--
000001609E770000	00000000000C9000	User	\Device\Harddiskvolume1\Windows\S		MAP	-R---	-R---
00007FF42D880000	0000000000005000	User			MAP	-R---	-R---
00007FF42D885000	00000000000FB000	User	Reserved (00007FF42D880000)		MAP		-R---
00007FF42D980000	0000000100020000	User	Reserved		PRV		-RW--
00007FF52D9A0000	0000000002000000	User	Reserved		PRV		-RW--
00007FF52F9A0000	0000000000001000	User			PRV	-RW--	-RW--
00007FF52F9B0000	0000000000001000	User			MAP	-R---	-R---
00007FFDC05F0000	0000000000001000	System	apphelp.dll		IMG	-R---	ERWC-
00007FFDC05F1000	000000000004E000	System	".text"		IMG	ER---	ERWC-
00007FFDC063F000	0000000000022000	System	".rdata"		IMG	-R---	ERWC-
00007FFDC0661000	0000000000003000	System	".data"		IMG	-RW--	ERWC-
00007FFDC0664000	0000000000004000	System	".pdata"		IMG	-R---	ERWC-
00007FFDC0668000	0000000000001000	System	".didat"		IMG	-R---	ERWC-
00007FFDC0669000	0000000000017000	System	".rsrc"		IMG	-R---	ERWC-
00007FFDC0680000	0000000000001000	System	".reloc"		IMG	-R---	ERWC-
00007FFDC3030000	0000000000001000	System	kernelbase.dll		IMG	-R---	ERWC-
00007FFDC3031000	0000000000177000	System	".text"		IMG	ER---	ERWC-
00007FFDC31A8000	00000000001AB000	System	".rdata"		IMG	-R---	ERWC-
00007FFDC3353000	0000000000005000	System	".data"		IMG	-RW--	ERWC-
00007FFDC3358000	0000000000018000	System	".pdata"		IMG	-R---	ERWC-
00007FFDC3370000	0000000000001000	System	".didat"		IMG	-R---	ERWC-
00007FFDC3371000	0000000000001000	System	".rsrc"		IMG	-R---	ERWC-


FREE AI Homework Helper Week11.exe.00_0075b600.exe - PID: 7656 - Module: free ai homework helper week11.exe.00_0075b600.exe - Thread: Main Thread 6640 - x64dbg [Elevated]
File View Debug Tracing Plugins Favourites Options Help Mar 15 2025 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Hide FPU
esi=E4999000
UPX1:00000000012DA028 free ai homework helper week11.exe.00_0075b600.exe:$92A028 #17E428
Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Address Hex ASCII