Static Analysis
1. Virus Total Analysis
Hash Analysis

- File Hash: [Insert MD5, SHA-1, SHA-256 hash value]
- MD5 - 0d837e8a5a3a981997df60f4bcc9b91b
- SHA-1 - bffb529b93c58a3ed35a0a75d1755d1e1d681ab7
- SHA-256 - b12a5c300a5d436bf62bd088d71dd7a20848072a78a1b99ba5aa2f8258c994b1
- Method of hash acquisition: [Describe process]:
    - Uploaded Week2.exe to VirusTotal and I copied the hash values from there
- [Link to VirusTotal results]
    - https://www.virustotal.com/gui/file/b12a5c300a5d436bf62bd088d71dd7a20848072a78a1b99ba5aa2f8258c994b1/detection

Vendor Analysis

- Number of vendors flagging as malicious: [X/Y]
    - 18/72
- Analysis of vendor results:
    - [Discuss patterns in detection]:
        - Pe, exe, 64bits, upx, persistence, long-sleeps, detect-debug-environment, corrupt
    - [Common malware names identified]:
        - GrayWare/Win32.Wacapew
        - Win/malicious_confidence_60% (W)
        - Exe.trojan.wacapew
        - Unsafe
        - Malicious (score: 100)
        - MALICIOUS
        - Malicious (moderate Confidence)
        - W32/PossibleThreat
        - Detected
        - Trojan-Dropper.Win64.Agent
        - Malware.kb.b.944
        - Trojan.Win32.Generic.4!c
        - Trojan.Malware.300983.susgen
        - Ti!B12A5C300A5D

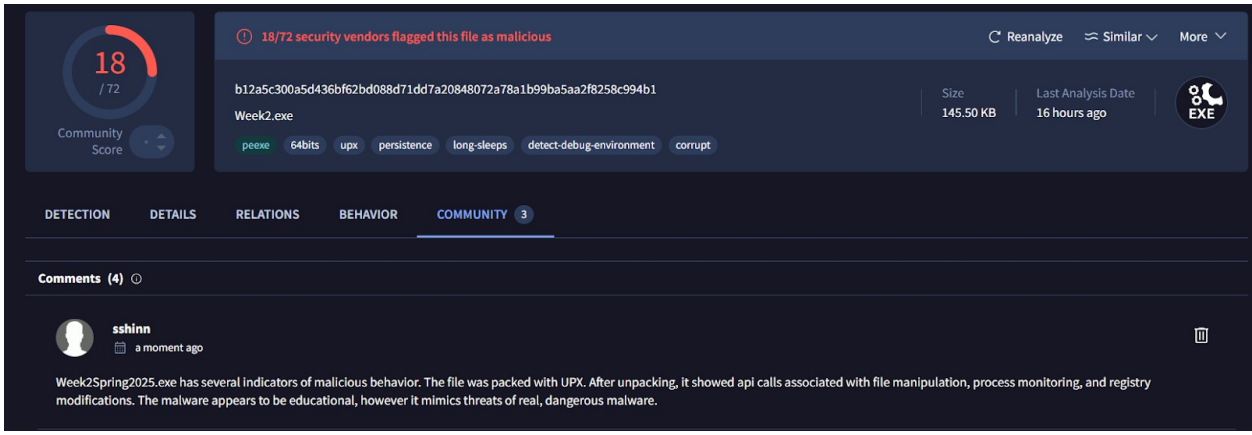
        - Trojan:Win32/Sonbokli.A!cl
        - Malicious
        - Malicious.high.ml.score
        - Artemis!0D837E8A5A3A
    - [Notable vendor disagreements]:
        - One vendor called this GrayWare, another called it Artemis, a few vendors called this a Trojan

File History

- First Submission Date: [Date]
- File Creation Date from Windows: [Date]
    - Creation Time: 2025-01-27 17:50:01 UTC
    - First Submission: 2025-01-29 21:24:54 UTC
- Analysis of submission timeline:
    - [Discussion of file age]: the file is only 2 days old, which means it has only been out "in the wild" for 2 days. This explains why most vendors have not flagged it as malicious.
    - [Notable resubmissions or changes]: I do not have any information to suggest that there have been resubmissions or changes.

Community Score

- [Link to your VirusTotal community contribution]
    - https://www.virustotal.com/gui/file/b12a5c300a5d436bf62bd088d71dd7a20848072a78a1b99ba5aa2f8258c994b1/community



- Summary of initial findings posted to the community:
    - [Key observations] Appears to be educational
    - [Potential indicators of compromise] Registry modifications and

malicious api calls

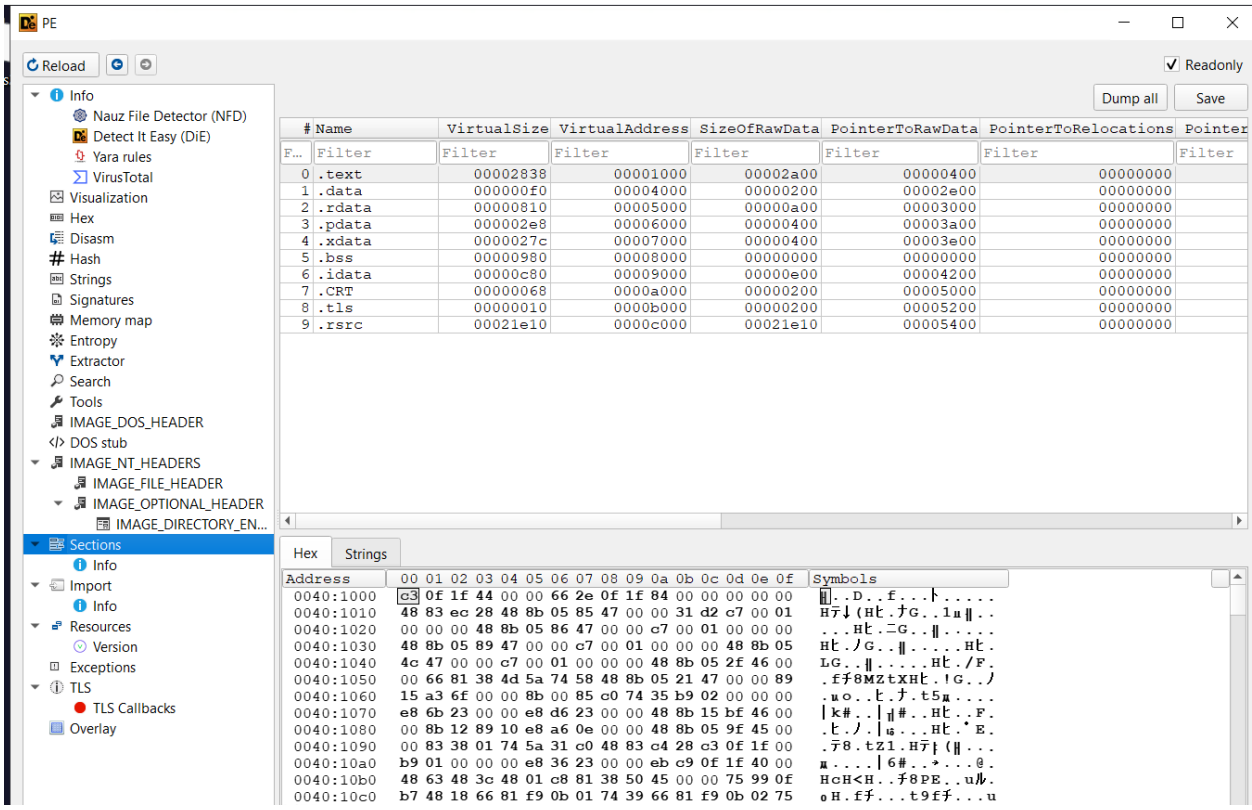
2. Detect It Easy (DIE) Analysis
File Information

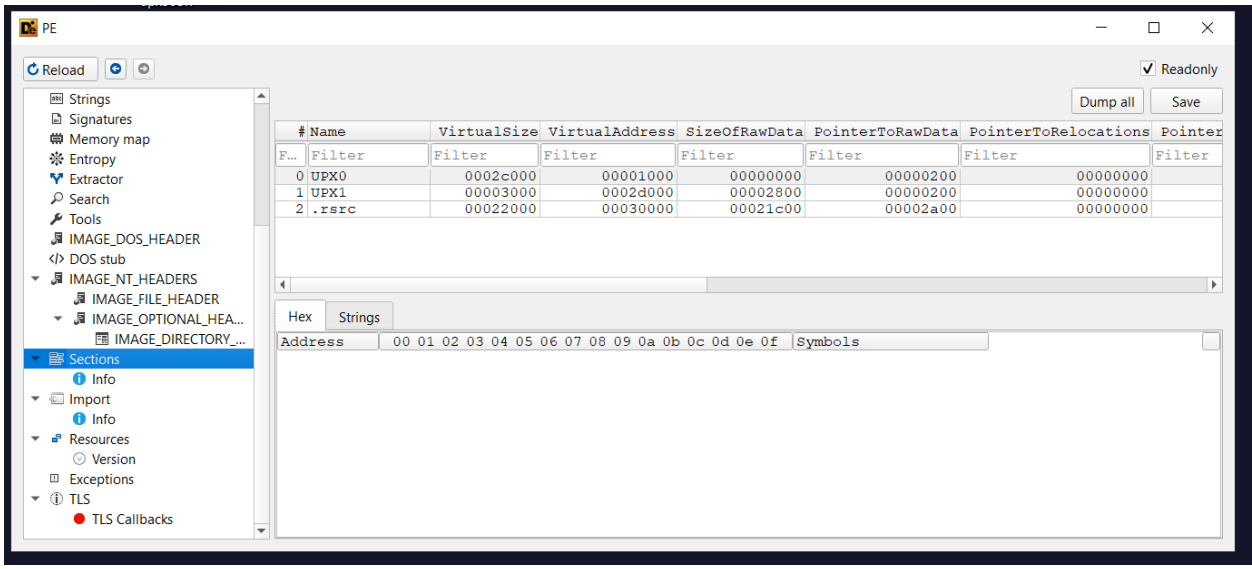
- File type: [Type] PE64
- Architecture: [Architecture] AMD-64
- Compiler: [Compiler information] MinGW
- Additional relevant information:
    - [List notable file characteristics]:
        - Packer: UPX(4.24)[NRV,best]
        - Linker: GNU Linker ld (GNU Binutils)(2.30) [Console64,console]
        - (Heur)Packer: Compressed or packed data[EntryPoint + Imports like UPX (v3.91+) + Sections like UPX + Sections collision ("UPX") + Section 1 ("UPX1") compressed]
    - [Unusual headers or structures]
        - IMAGE_DOS_HEADER
        - IMAGE_FILE_HEADER
        - IMAGE_OPTIONAL_HEADER
        - IMAGE_DIRECTORY_ENTRIES`
        - Before unpacking with UnPacMe: Sections: UPX0, UPX1, .rsrc
        - After unpacking: Sections: .text, .data, .rdata, .pdata, .xdata, .bss, .idata, CRT, .tls, .rsrc

Memory Map Analysis

- Section breakdown:
    - [.text section analysis]
        - Read, Execute flags
        - No unusual hex values
    - [.data section analysis]
        - Read, Write flags
        - No unusual hex values
    - [.rsrc section analysis]
        - Read, Write flags
        - No unusual hex values
    - [Other relevant sections]
        - String found in rdata: WARNING: This is a training program for CYBV 454 Malware Analysis Class

- Detect It Easy did not show any notable findings after unpacking the malware and analyzing the sections. Most significant findings were found in Strings and API calls from using Ghidra. The string found in rdata contained critical information about the malware, however.





- Notable findings:
    - [Unusual section permissions]
        - Read Execute permissions in text section
    - [Section size anomalies]
        - 00021e10 is a relatively large size, it is for the .rsrc section

String Analysis
Notable strings discovered:

- Unknown pseudo relocation bit size %d.
- Unknown pseudo relocation protocol version %d.
- VirtualProtect failed with code 0x%x
- VirtualQuery failed for %d bytes at address %p
- %s\%s
- %s\%s_scan.json
- %s*.*
- 040904b0
- 040904b0
- 1.0.0.0
- 1.0.0.0
- 175.45.176.222
- 192.168.100.156
- 210.52.109.111

- __C_specific_handler
- __getmainargs
- __initenv
- __iob_func
- __lconv_init
- __set_app_type
- __setusermatherr
- _acmdln
- _amsg_exit
- _cexit
- _fmode
- _initterm
- _matherr(): %s in %s(%g, %g) (retval=%g)
- _onexit
- _strdup
- _vsnprintf
- abort
- Address %p has no image-section
- ADVAPI32.dll
- Argument domain error (DOMAIN)
- Argument singularity (SIGN)
- Author
- Author
- C:\CYBV454_DISCLAIMER.txt
- calloc
- CloseHandle
- closesocket
- CompanyName
- CompanyName
- ContactInformation
- ContactInformation
- CopyFileA
- Copyright © 2025 Michael Galde. All rights reserved.

- Copyright © 2025 Michael Galde. All rights reserved.
- Created by Professor Galde for educational purposes only.
- CreateFileA
- CreateMutexA
- CryptAcquireContextA
- CryptCreateHash
- CryptDestroyHash
- CryptGetHashParam
- CryptHashData
- CryptReleaseContext
- CYBV 454 Malware Analysis Class Project
- CYBV 454 Malware Analysis Class Project
- CYBV 454 Malware Analysis Week 2 Spring 2025
- CYBV 454 Malware Analysis Week 2 Spring 2025
- CYBV454-BEACON:%s:%s:ANALYSIS-TARGET
- DeleteCriticalSection
- Documents
- Downloads
- Dynamic Analysis Training Module
- EnterCriticalSection
- ERROR_CRYPTO_CONTEXT
- ERROR_HASH_CREATION
- ERROR_OPENING_FILE
- exit
- fclose
- FileDescription
- FileDescription
- FileVersion
- FileVersion
- FindClose
- FindFirstFileA
- FindNextFileA
- fopen

- fprintf
- fputs
- free
- fwrite
- GCC: (x86_64-posix-seh-rev0, Built by MinGW-W64 project) 8.1.0
- GetCurrentProcess
- GetCurrentProcessId
- GetCurrentThreadId
- GetLastError
- GetModuleFileNameA
- GetStartupInfoA
- GetSystemTimeAsFileTime
- GetTickCount
- htons
- If this program was found on your machine outside of the class environment,
- inet_addr
- InitializeCriticalSection
- InternalName
- InternalName
- KERNEL32.DLL
- LastAnalysis
- LeaveCriticalSection
- LegalCopyright
- LegalCopyright
- malloc
- memcpy
- memset
- Michael Galde
- Michael Galde
- michaelgalde@arizona.edu
- michaelgalde@arizona.edu
- Microsoft Security Check
- Microsoft_Security_Plus_Member

- Mingw-w64 runtime failure:
- msvcrt.dll
- MZ
- NetworkError
- OriginalFilename
- OriginalFilename
- Overflow range error (OVERFLOW)
- Partial loss of significance (PLOSS)
- PE
- Pictures
- please contact michaelgalde@arizona.edu for recovery assistance.
- ProductName
- ProductName
- QueryPerformanceCounter
- ReadFile
- RegCloseKey
- RegCreateKeyExA
- RegOpenKeyExA
- RegSetValueExA
- RT_MANIFEST
- RtlAddFunctionTable
- RtlCaptureContext
- RtlLookupFunctionEntry
- RtlVirtualUnwind
- sendto
- SetFileAttributesA
- SetUnhandledExceptionFilter
- SHELL32.dll
- SHGetFolderPathA
- signal
- Sleep
- socket
- Software\CYBV454_Malware_Class

- Software\CYBV454_Malware_Class\Errors
- Software\Microsoft\Windows\CurrentVersion\Run
- strcat
- StringFileInfo
- StringFileInfo
- strlen
- strncmp
- TerminateProcess
- The result is too small to be represented (UNDERFLOW)
- TlsGetValue
- Total loss of significance (TLOSS)
- Translation
- Translation
- UnhandledExceptionFilter
- University of Arizona
- University of Arizona
- Unknown error
- VarFileInfo
- VarFileInfo
- vfprintf
- VirtualProtect
- VirtualQuery
- VS_VERSION_INFO
- VS_VERSION_INFO
- VS_VERSION_INFO
- WARNING: This is a training program for CYBV 454 Malware Analysis Class
- Week2Spring2025.exe
- Week2Spring2025.exe
- Week2Spring2025.exe
- Week2Spring2025.exe
- WS2_32.dll
- WSAStartup
- WSAStartup Failed

- {"name":"%s","size":%ld,"md5":"%s

Filter by:

All Posts

|

Clear filters

Show:

Threaded — Newest
First — Oldest
First — Author
First Name A-Z
Author First Name Z-A
Author Last Name A-Z
Author Last Name Z-A
Subject A-Z
Subject Z-A
Attachments First

- View profile card for Sarah Shinn
- 
-
- **Sarah Shinn**
- February 3 at 12:55 AM

-
- Analysis of string findings:

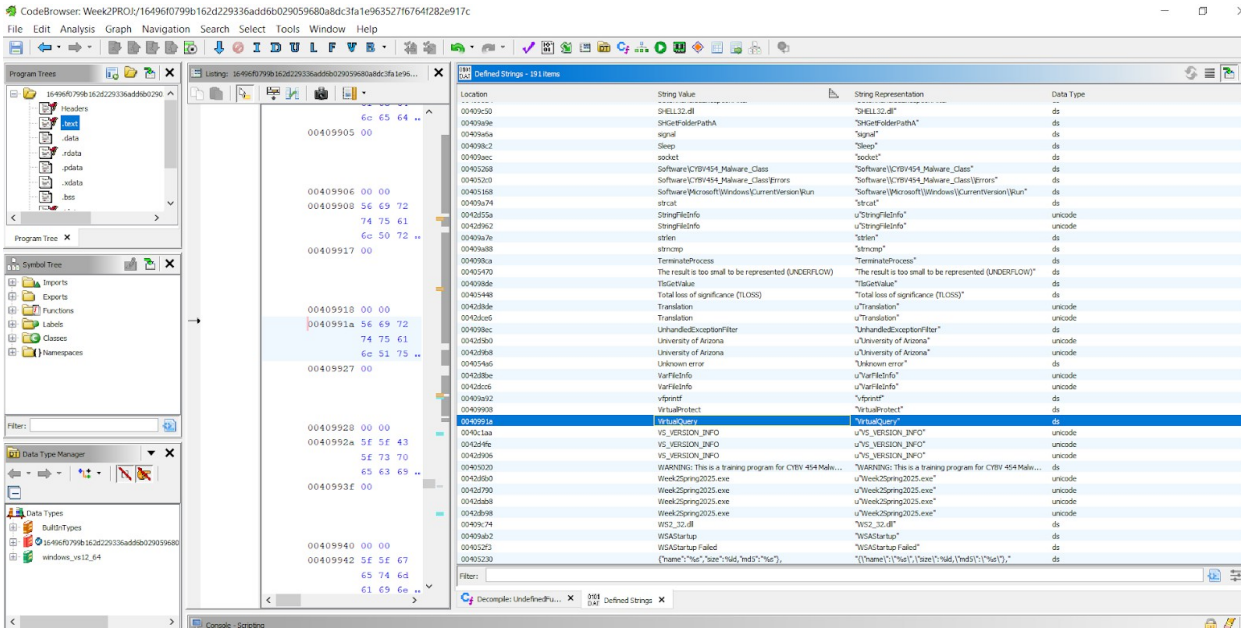
- The extracted strings suggest that this executable is likely engaging in:
- File Operations: The presence of CreateFileA, ReadFile, CopyFileA, FindFirstFileA, FindNextFileA, and SetFileAttributesA suggests that the program interacts with files, potentially for reading, writing, or modifying them.
- Process and Thread Manipulation: API calls like GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, TerminateProcess, and UnhandledExceptionFilter indicate process monitoring or control.
- Registry Modifications: The inclusion of RegCreateKeyExA, RegOpenKeyExA, RegSetValueExA, and RegCloseKey suggests possible

persistence mechanisms by modifying Windows Registry keys.

- Cryptographic Functions: The presence of CryptAcquireContextA, CryptCreateHash, CryptHashData, and CryptGetHashParam suggests the use of cryptographic hashing or encryption, possibly for secure data handling or obfuscation.
- Networking: Calls like WSAStartup, sendto, socket, closesocket, htons, and inet_addr indicate networking functionality, possibly for communication with remote servers. The presence of hardcoded IPs (e.g., 175.45.176.222, 192.168.100.156) raises questions about potential remote communication.
- Memory and Exception Handling: The use of VirtualProtect, VirtualQuery, TlsGetValue, and UnhandledExceptionFilter suggests potential anti-analysis techniques, such as memory protection changes and exception handling manipulation.
- Synchronization and Thread Safety: Functions like CreateMutexA, EnterCriticalSection, LeaveCriticalSection, and DeleteCriticalSection suggest concurrency management, possibly to prevent multiple instances from running simultaneously.
- Persistence Mechanisms: The reference to Software\Microsoft\Windows\CurrentVersion\Run suggests that the program may attempt to achieve persistence by adding itself to startup.
    - [Suspicious patterns]:
- Hardcoded IPs: The presence of multiple hardcoded IP addresses (175.45.176.222, 192.168.100.156, 210.52.109.111) raises red flags, as they could be command-and-control (C2) servers.
- Potential Malware Indicators: The presence of VirtualProtect and VirtualQuery suggests the possibility of code injection or memory protection bypass techniques. The use of RegSetValueExA and modification of Software\Microsoft\Windows\CurrentVersion\Run indicates possible persistence methods.
- Potential Beaconing Behavior: The string CYBV454-BEACON:%s:%s:ANALYSIS-TARGET suggests that the program might send signals to a remote system.
- Obfuscation or Encryption: cryptographic functions

(CryptHashData, CryptAcquireContextA) suggests potential data encryption or obfuscation, possibly to hide payloads or communicate securely with a remote server.

- Some strings indicate that this could be an educational malware analysis project (CYBV 454 Malware Analysis Class and Created by Professor Galde for educational purposes only). Potential User Data Collection: The inclusion of SHGetFolderPathA, GetModuleFileNameA, and references to system directories (Documents, Downloads, Pictures) might indicate file enumeration or exfiltration activities.
- I used Ghidra for Strings/API calls analysis. See screenshot.



- Entropy Analysis
  - Overall entropy score: [Score]
    - 4.33897
  - Section-specific entropy:

        - [List sections with unusual entropy]
        - PE Header: Entropy: 2.63667, not packed
        - Section UPX1: Entropy:7.74817, packed
        - Rsrc: Entropy:3.81526, not packed
    - Packing analysis:
        - [Packed/Unpacked determination]
            - It is packed with UPX
        - [Packer identified (if applicable)]
            - UPX
        - [Unpacking methodology (if attempted)]: I unpacked this file with UnPacMe because unpacking with upx.exe did not work
        - [Alternative unpacking approaches (if needed)]: I tried unpacking with UPX and that did not work
- 3. Static Analysis Summary
    - Key findings from static analysis:
        - [Major indicators of malicious behavior]
        - [Potential functionality]
        - [Risk indicators]
            - The API calls and strings yielded a lot of useful information. The malware is creating files, copying files, and reading files. It is also monitoring processes. It is modifying registry keys and trying to gain persistence (when a malware remains on the system after reboot or logoff). There are also cryptographic

hashing APIs. There are hardcoded IP strings, and a string "CYBV454-BEACON:%s:%s:ANALYSIS-TARGET" which suggests that the malware may beacon to a remote system. It contains API calls VirtualProtect and VirtualQuery, which are common in Malware and are used for adjusting permissions on sections of memory. Calls to these APIs suggest code injection. There are also strings that say "CYBV 454 Malware Analysis Class and Created by Professor Galde for educational purposes only" and "University of Arizona" and stuff like that which suggests that this malware was made for educational purposes, which makes sense because it is for a malware analysis class.

- View profile card for Sarah Shinn
- 
-
- **Sarah Shinn**
- February 3 at 12:55 AM
    - Dynamic Analysis
    - 1. Analysis Environment
    - Environment Setup
        - Virtual Machine specifications:
            - [OS version]
                - Windows 10
            - [Memory allocation]
                - 8 GB RAM
            - [Network configuration]
                - FakeNet Deployed, Internet turned off
        - Monitoring tools deployed:
            - [Process monitoring]

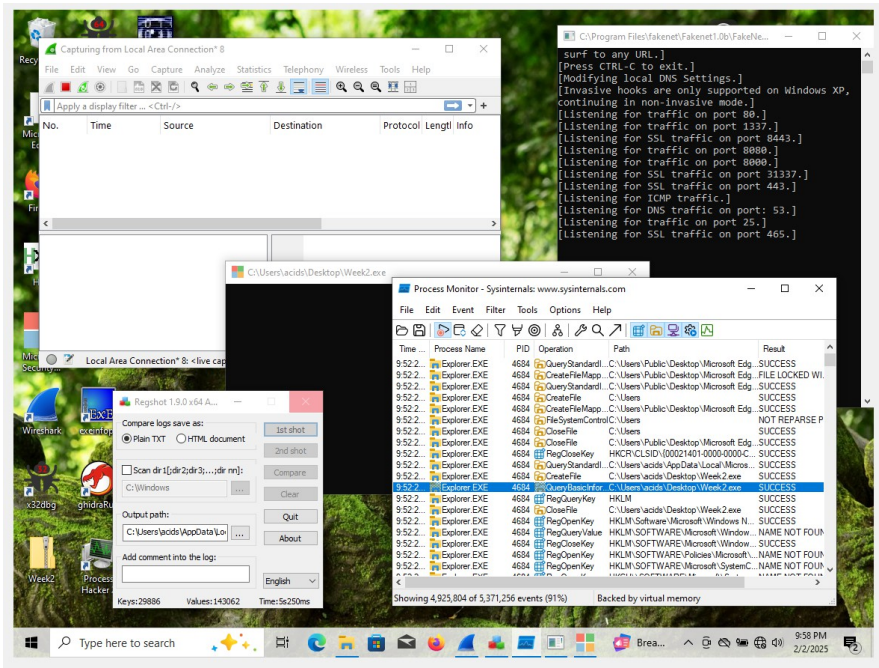
        - Ensure you use RegShot, Process Monitor, Process Explorer
        - I used RegShot, and Process Monitor
    - [Network monitoring]
        - Ensure you use Wireshark
        - I used Wireshark
    - [File system monitoring]
        - I used RegShot
- Safety measures implemented:
    - [Network isolation]
        - Try the analysis with and without Fakenet
        - I used Fakenet and I turned off my network adapter
    - [Snapshot configuration]
        - I am using a Windows 10 machine with Flare VM tools, I took a snapshot
    - [Additional protections]
        - Disabled network adapter and reverted virtual machine to previous snapshot when finished

- 2. Runtime Observations
- Initial Execution
    - [Immediate system changes]

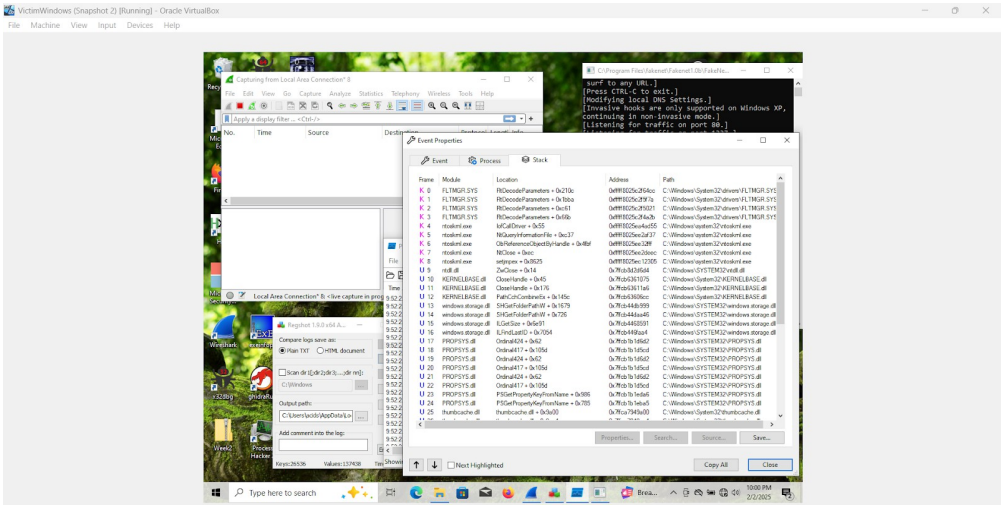
- A blank command prompt showed up

- [Process creation]

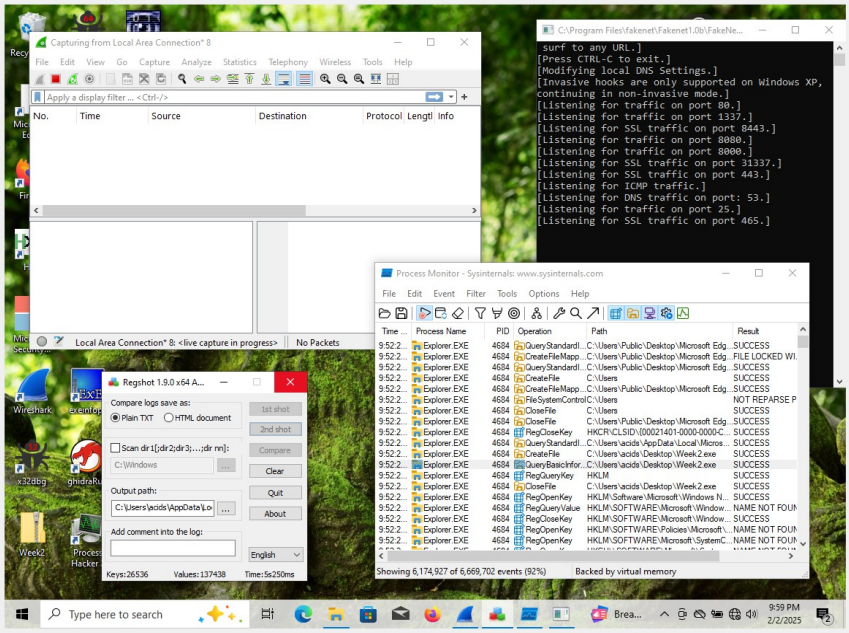
-



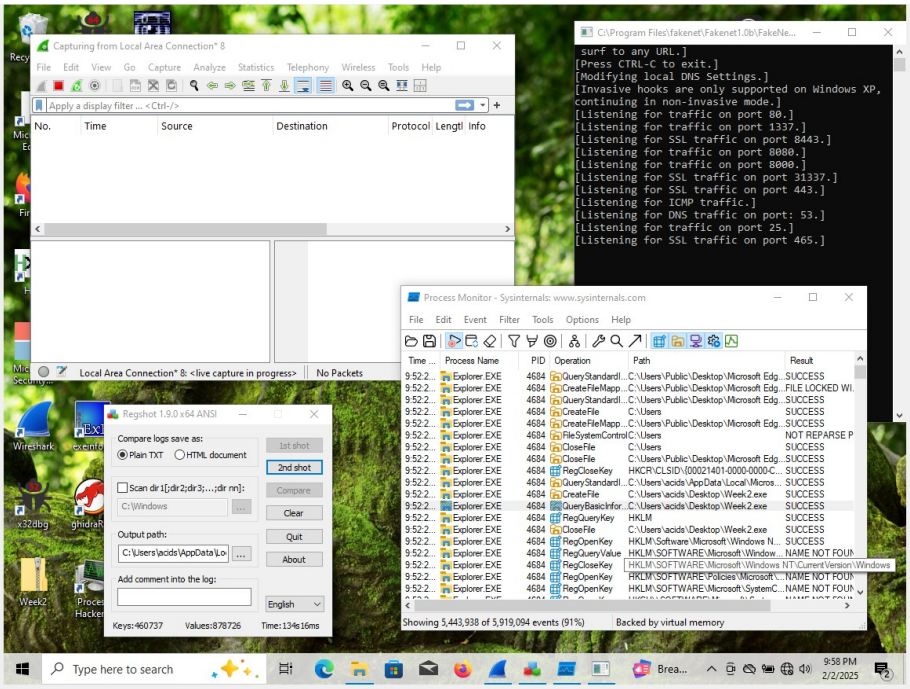
-



- CreateFile, CloseFile, and QueryBasicInformation were operations associated with Week2.exe
- I also looked at the stack when clicking on the QueryBasicInformation process for Week2.exe. I saw some operations called “CloseHandle” which to me could have indicated malicious activity.
    - [Registry creation]
        - Modified keys: 467566
        - Modified values: 893027
        - Total changes: 21247
-



-



- [Network activity]
    - I did not capture a single packet despite running WireShark. I was using FakeNet with my network adapter disabled. I used ANYRUN, and detected some network activity though.
    - SearchApp.exe: 2.19.80.27
    - RUXIMICS.exe: 51.104.136.2
- [File system changes]
    - CreateFile, CloseFile were seen in ProcMon

- Continued Monitoring
    - [Persistent changes]
        - I do not know because I revert the snapshot, but I noted above that many registry changes were made
    - [Scheduled tasks]

        - I did not see any scheduled tasks
    - [Registry modifications]
        - Modified keys: 467566
        - Modified values: 893027
        - Total changes: 21247
    - [Additional payloads]
        - VirtualProtect was used, so there was probably a payload in a memory location pointed to by VirtualProtect, if I were to debug the api call. Many of the vendors on VirusTotal said that this was a Trojan, so that is possible.
- 3. Post-Execution Analysis
    - System state changes:
        - [Permanent modifications]
            - I could not tell if there were permanent modifications, but I assume so because of the registry changes
        - [Persistence mechanisms]
            - I know a handle was closed, maybe it was used to gain access to a running process?
        - [Data exfiltration evidence]
            - Files were created and closed, and some network activity was shown on ANYRUN
    - Network activity summary:
        - [Connection attempts]

        - There are several IP addresses that the malware accessed and seen below in the ANYRUN screenshot

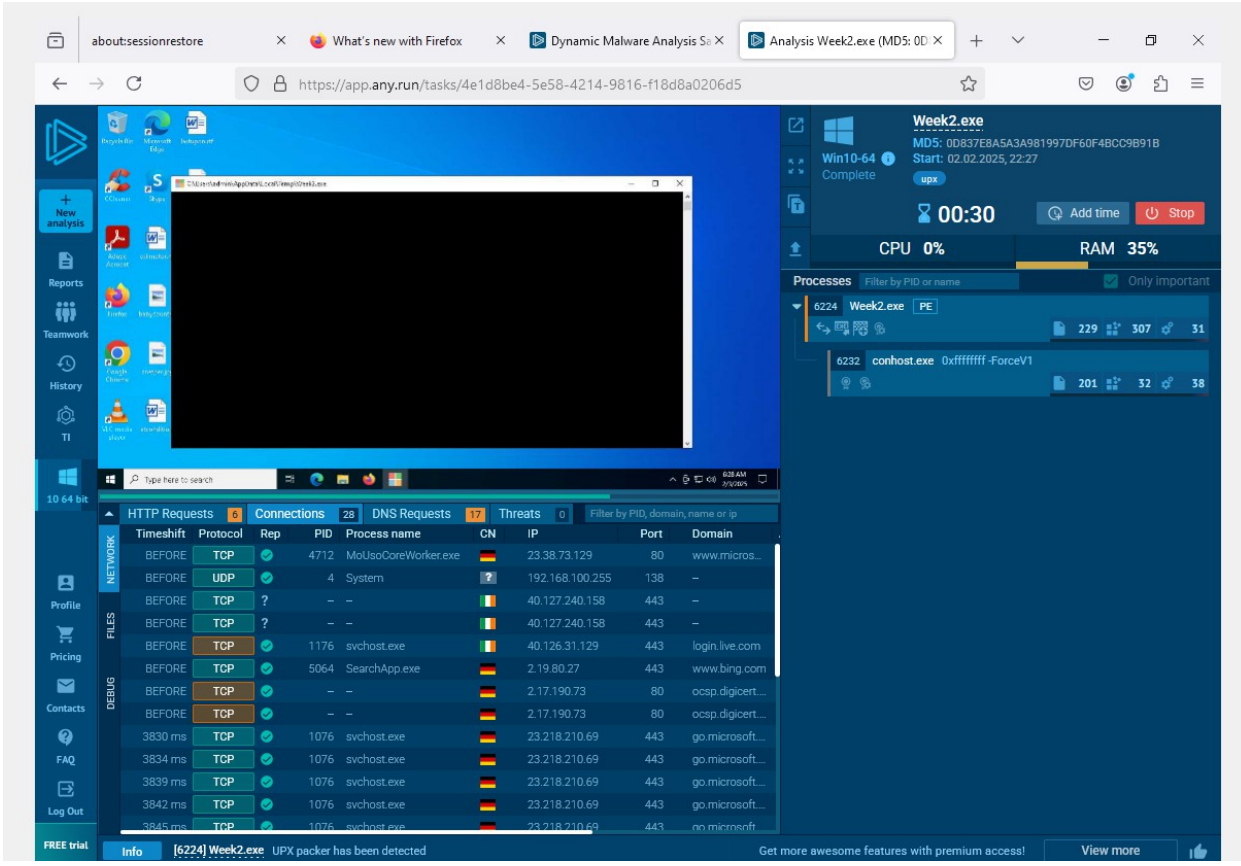
    - [Data transfers]

        - I do not know if data was transferred, I do not see evidence of that, but a file was created with CreateFile

    - [Command & Control activity]

        - There was a beacon call in the static analysis that indicated there may be a command and control center

- Impact Analysis



- 1. User Impact Assessment
- Home Users
  - [Potential impact]
    - There were a ton of registry changes, but I did not see the malware as super harmful
  - [Risk level]
    - Moderate risk to a home user
  - [Data compromise potential]
    - On ANYRUN, there were many network connections, so data could have been compromised
- Business Users
  - [Operational impact]

        - Definitely a risk to confidentiality and integrity

    - [Data security concerns]

        - Data is not completely secure following infection with this malware

    - [Financial implications]

        - There could be financial losses caused by damages to confidentiality and integrity of data

- Government Users

    - [Security implications]

        - Data is not secured after running this malware

    - [Data sensitivity concerns]

        - Sensitive data could be accessed or modified

    - [Operational disruption potential]

        - This is a serious risk to data security simply because a lot of registry changes are made and it is not certain what the malware is doing

- 2. Mitigation Strategy

- Immediate Response

    - [Initial containment steps]

        - Create backups of data

    - [System isolation procedures]

        - Reinstall OS

- [Data preservation methods]
    - Revert system to a previous restoration point or revert to previous snapshot. Keep frequent backups always.

- Long-term Prevention
    - [Security control recommendations]
        - Always keep frequent backups
    - [Policy modifications]
        - Do not run suspicious files, upload file to VirusTotal before running it
    - [Training requirements]
        - Do not run suspicious files, keep regular backups

- Conclusion
- 1. Analysis Reflection
    - [Summary of findings]
        - Week2Spring2025.exe has several indicators of malicious behavior. The file was packed with UPX, and unpacked with UnPacMe. After unpacking, it showed api calls associated with file manipulation, process monitoring, and registry modifications. The malware appears to be educational, however it mimics threats of real, dangerous malware.
    - [Unusual characteristics]
        - There was a Beacon call, found in strings on Ghidra. Could the malware be beaconing to a command and control center
    - [Learning outcomes]

        - Dynamic Analysis, as well as static analysis. I used Ghidra, Detect It Easy, UnPacMe, regshot, procmon, fakenet

    - [Additional research needed]

- 2. Evidence Documentation
    - [Screenshot descriptions and relevance]
        - See screenshots above
    - [Tool output documentation]
        - I used Ghidra, Detect It Easy, UnPacMe, regshot, procmon, fakenet
    - [Additional supporting materials]
        - VirusTotal called this a trojan, and the api call VirtualProtect supports that