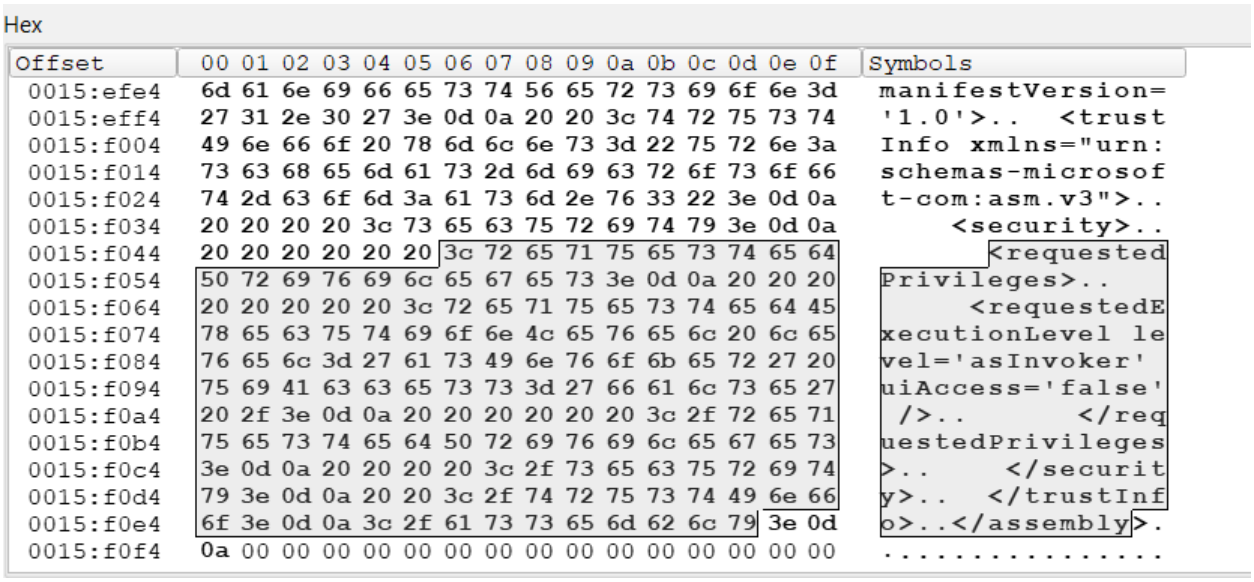
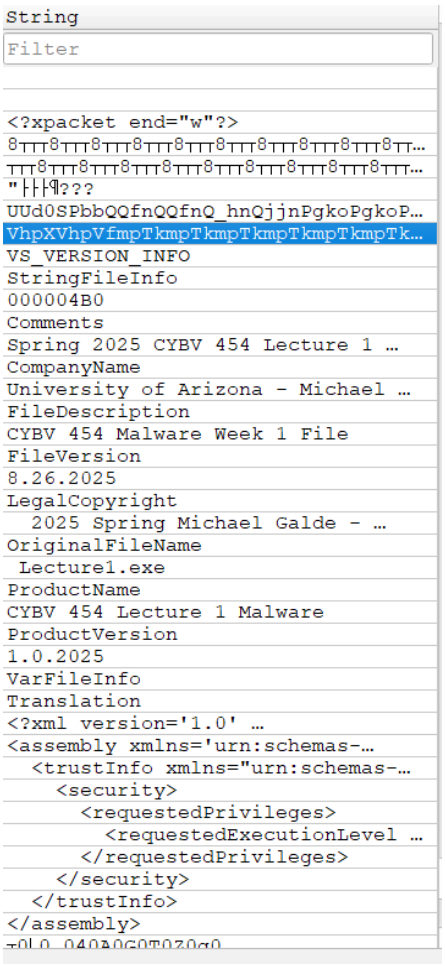
Static Analysis
1. Virus Total Analysis
Hash Analysis
File Hash: MD5[be4208f4729b58e26caee68f0e1eacf9] and SHA256[6c55988009c39eea5d8e1fa552c7db331b0328c5d62527b82f01074e5315f492]
Method of hash acquisition: [Detect-It-Easy]
Link to VirusTotal results:
[https://www.virustotal.com/gui/file/6c55988009c39eea5d8e1fa552c7db331b0328c5d62527b82f01074e5315f492]
Vendor Analysis
Number of vendors flagging as malicious: [54/72]
Analysis of vendor results: Many of the vendors flag this malware as a Trojan, Win32, DiskWriter, KillMBR, ransomware
[Many vendors classify this malware as a Win32 DiskWriter Trojan]
[Lecture1, Week1]
[Some vendors classify this malware as a Lazy Trojan, some say it is a variant of LazyTrojan and some say it is a variant of Win32 DiskWriter Trojan]
File History
First Submission Date: [2025-01-22 21:28:42 UTC]
File Creation Date from Windows: [2021-10-06 13:56:33 UTC]
Analysis of submission timeline:
[This malware was created in October 2021 however it was first submitted to VirusTotal in January 2025]
[It has been submitted under two names, Lecture1 and Week1]
Community Score
[https://www.virustotal.com/gui/file/6c55988009c39eea5d8e1fa552c7db331b0328c5d62527b82f01074e5315f492/community]
Summary of initial findings posted to the community:
[Executable makes system inoperable. Included Audio/visual component.]
[Flagged as malicious by over half of the included vendors. Listings including Trojan | Malware | disk writer]
2. Detect It Easy (DIE) Analysis
File Information
File type: [PE32]
Architecture: [I386]
Compiler: [Compiler: Microsoft Visual C/C++(19.16.27045)[LTCG/C]]
Additional relevant information:
[List notable file characteristics: Windows XP OS, Comments:Spring 2025 CYBV 454 Lecture 1 Malware File, CompanyName: University of Arizona - Michael Galde]
[IMAGE_DOS_HEADER, INAGE_NT_HEADERS: IMAGE_FILE_HEADER, IMAGE_OPTIONAL_HEADER:IMAGE_DIRECTOEY_ENTRIES]
Memory Map Analysis
Section breakdown:
[.text section from memory address 00401000 to 0041e200]
[.data section from memory address 0046e000 to 0046e800]
[.rsrc section from memory address 00477000 to 00569600, chinese characters]
[_RDATA: chinese characters and symbols]

Notable findings:



[Unusual section permissions: 00569444, 00569461]
[.text Virtual Size:0001D1C0, Raw Size:0001D200
.rdata Virtual Size:0004E790, Raw Size:0004E800
.data Virtual Size:0000720C, Raw Size:00000800
_RDATA Virtual Size:000005E0, Raw Size:00000600
.rsrc Virtual Size:000F24F5, Raw Size:000F2600
.reloc Virtual Size:00002378, Raw Size:00002400]

String Analysis
Notable strings discovered: "This program cannot be run in DOS mode"



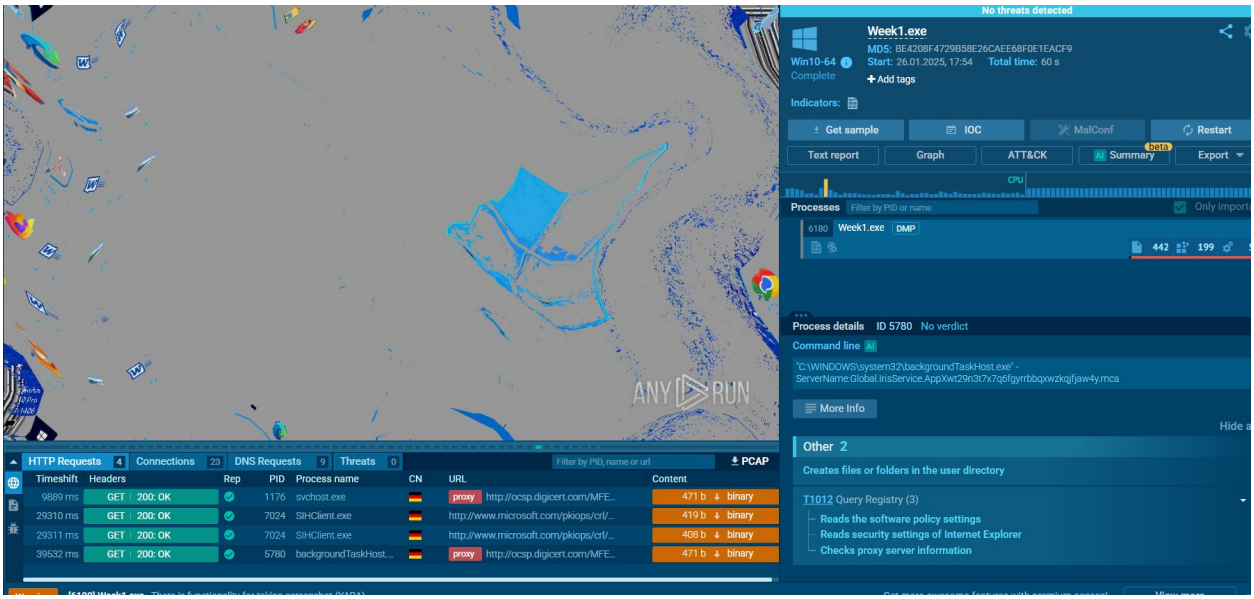
[URLs:xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#",
xmlns:dc="http://purl.org/dc/elements/1.1/">,
No IPs found
[no file paths found]
[no command lines found]

[API calls: FlsAlloc, FlsAlloc, FlsFree, FlsSetValue, FlsSetValue, InitializeCriticalSectionEx, restrict(, delete[]]

Analysis of string findings:[Writer of malware: Michael Galde, for University of Arizona CYBV454, various API calls for memory management]
[Suspicious patterns: the text section is packed]
Entropy Analysis
Overall entropy score: [7.17248]
Section-specific entropy:
[the text section has entropy of 6.68034, it is packed]
Packing analysis:
[Packed/Unpacked determination: the text section is packed]
[Packer identified: __GenericHeuristicAnalysis_By_DosX.7.sg]
[Unpacking methodology (if attempted): I did not attempt]
[Alternative unpacking approaches (if needed)]
3. Static Analysis Summary
Key findings from static analysis: Executable makes system inoperable. Included Audio/visual component. Flagged as malicious by over half of the included vendors. Listings including Trojan | Malware | disk writer. killMBR suggests the virus affects the Master Boot Record.
[flagged by virustotal as malicious, packed text section suggests obfuscation]
[makes system inoperable by affecting master boot record]
[Packed, flagged by antivirus]
Dynamic Analysis
1. Analysis Environment
Environment Setup
Virtual Machine specifications:
[Microsoft Windows XP, Professional Version 2002 Service Pack 3]
[444MB RAM]
[No internet]
Monitoring tools deployed:
[ANYRUN]
[ANYRUN]
[ANYRUN]
Safety measures implemented:
[Network isolation: virtual machine is not connected to internet]
[Snapshot configuration: default cyberapolis Windows XP machine configuration]
[Additional protections: none]
2. Runtime Observations
Initial Execution:
“The task described in the provided JSON is the execution of a file named "Week1.exe" located in the "C:\Users\admin\AppData\Local\Temp\" directory. The process tree shows that the file was executed by another process with the same name, which was located in the same directory. Legitimate programs may use temporary folders to store and execute files. In this case, the execution of the file "Week1.exe" from a temporary folder could be a legitimate action if it is part of a normal program's behavior.” - from AnyRun
[Immediate system changes: Computer is inoperable, screen displays flashing colors and pixelated images, blue screen, icons floating all around screen]
[Process creation: svchost.exe, SIHClient.exe, backgroundTaskHost.exe]
[Network activity:
192.168.100.255 on port 138, 40.127.240.158 on port 443, 23.35.238.131 on

port 443, 2.17.190.73 on port 80]
[File system changes: other /
Creates files or folders in the user directory
operation:
CREATE device:
DISK_FILE_SYSTEM object:
FILE name:
C:\Users\admin\AppData\Local\Packages\MicrosoftWindows.Client.CBS_cw5n1
h2txyewy\AC\Microsoft\CryptnetUrlCache\Content\E2C6CBAF0AF08CF203BA74BF
0D0AB6D5_363582827213C09529A76F35FB615187
status:0x00000000
created:
CREATED
access:
READ_CONTROL, SYNCHRONIZE, FILE_READ_DATA, FILE_WRITE_DATA,
FILE_APPEND_DATA, FILE_READ_EA, FILE_WRITE_EA, FILE_READ_ATTRIBUTES,
FILE_WRITE_ATTRIBUTES
]
Continued Monitoring
[Persistent changes: files created]
[Scheduled tasks: none]
[Registry modifications: none noted in AnyRun]
[Additional payloads: none noted in AnyRun]
3. Post-Execution Analysis
System state changes:
[Permanent modifications: files created]
[Persistence mechanisms: unknown]
[Data exfiltration evidence: unknown]
Network activity summary:
[Connection attempts: 23 Connections (example: 192.168.100.255 on port 138,
40.127.240.158 on port 443, 23.35.238.131 on port 443, 2.17.190.73 on port
80)]
[Data transfers: no data transfers]
[Command & Control activity: hijack master boot record, takes over whole
system and renders computer inoperable]
Impact Analysis
1. User Impact Assessment
Home Users
[Potential impact: Causes changes to master boot record, creates files, makes
connections]
[Risk level: moderate]
[Data compromise potential: no data was compromised]
Business Users
[Operational impact: Loss of time it takes for program to run, possible
permanent damage]
[Data security concerns: data could be transferred through connections]
[Financial implications: could cause damage to systems]
Government Users
[Security implications: Takes time to run program, data can be transferred

off via connections]
[Data sensitivity concerns: Data can be transferred off machine via connections]
[Operational disruption potential: could disrupt operations]
2. Mitigation Strategy
Immediate Response
[Initial containment steps: wait until program finishes, do fulls system wipe]
[System isolation procedures: turn off connection to internet]
[Data preservation methods: copy all data to backup]
Long-term Prevention
[Security control recommendations: only run malware on a virtual machine]
[Policy modifications: do not run this program unless it is in a virtual machine or sandbox]
[Training requirements: train employees not to run suspicious programs]
Conclusion
1. Analysis Reflection
[Summary of findings: The analyzed file is a PE32 executable compiled with Microsoft Visual C++, was flagged as malicious by 54 out of 72 vendors on VirusTotal.
It is classified as a Trojan (Win32 DiskWriter, KillMBR, ransomware). The malware is packed, with obfuscation in the .text section, and high entropy (7.17 overall). Dynamic analysis confirmed its destructive behavior, including rendering the system inoperable by altering the Master Boot Record (MBR). Displaying visuals and altering system states. Creating new files and attempting network connections.]
[Unusual characteristics: The malware contains metadata referencing "Spring 2025 CYBV 454 Lecture 1 Malware File" and a user (Michael Galde) at the University of Arizona, suggesting it was developed for academic purposes. Packed .text section and the presence of non-standard strings, such as Chinese characters in the .rsrc and _RDATA sections. Network activity involving multiple IPs and ports.]
[Learning outcomes: Understand the behavior and impact of master boot record-modifying malware. Understand the significance of packed sections and entropy in static analysis. Observe the impact of malicious software during dynamic analysis.]
[Additional research needed: Determine the purpose of the network connections made by the malware. Unpack code to analyze obfuscated code within the .text section.]
2. Evidence Documentation
[Screenshot descriptions and relevance:



]

[Tool output documentation: CFF Explorer, VirusTotal, Detect-It-Easy, AnyRun]

[Additional supporting materials]