

Week 9 Discussion

Static Analysis

Student identified the type / family of malware.

- Stuxnet, Worm

Student created a Virus Total comment and provided a username.

Comments (13) 



sshinn

a moment ago

week9.dll is a malicious dll file which contains evidence of interacting with and modifying antivirus and security systems. It also contains strings referencing SIEMENS, which is industrial control software associated with Stuxnet.

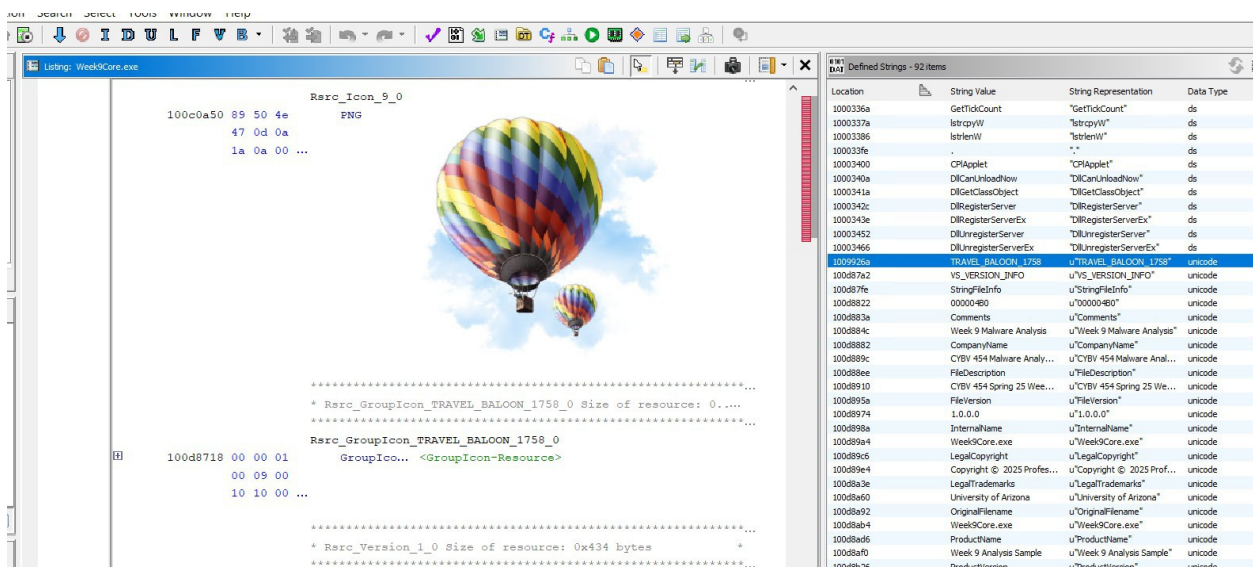
[Show more](#)

Username:sshinn

Comment: week9.dll is a malicious dll file which contains evidence of interacting with and modifying antivirus and security systems. It also contains strings referencing SIEMENS, which is industrial control software associated with Stuxnet.

Student conducted a file analysis and identified what was unique or suspicions of this file. The student additionally found "The Secret"

"The Secret" = hot air balloon images (TRAVEL_BALOON_1758) in packed section (.stub). I disassembled .stub section and found the address for TRAVEL_BALOON_1758 at address 1009926A, which is between .stub Start Address: 10006000 and .stub End Address: 10098FFF



Week9Core.exe

File Information

- MD5: 2044c8cd3f0f14c843908dd057ef582a
- SHA-1: 8a9b99b89d8eaa752156647488586bb0dca0e1c0
- SHA-256:
9b65b76433fb30d1b1f0e41bf5a7556c7fcd596848360f160613e9d0a3110348
- File type: PE32
- Magic: PE32 executable (GUI) Intel 80386, for MS Windows
- Compiler: Microsoft Visual C/C++ (15.00.30729) [LTCG/C] Linker:
Microsoft Linker (9.00.30729) Tool: Visual Studio (2008)
- File size: 852.50 KB (872960 bytes)
- PEiD packer: FASM v1.3x
- VirusTotal: 49/73 flagged as malicious

Memory Map:

- .text: raw size: 6144, entropy: 5.89
- .rdata: raw size: 1536, entropy: 3.97
- .data: raw size: 512, entropy: 0.02
- .reloc: raw size: 512, entropy: 4.02
- .stub: raw size: 602112, entropy: 8
- .rsrc: raw size: 261120, entropy: 7.09

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	5710	6144	5.89	736cc165ffc0986a134ea5fb88663ac1	75471.86
.rdata	12288	1148	1536	3.97	960c476c9e0c05eac9db75daa5389c42	89250.46
.data	16384	32	512	0.02	9475a59226943a3ad422e18169989f66	130049
.reloc	20480	370	512	4.02	57cbbc1eb3c7f4081c0b6de97e96a781	31009
.stub	24576	602112	602112	8	3259fb64a6855b8b5a0e413449831925	5397.67
.rsrc	626688	261072	261120	7.09	4f3f4823116304b21aa4720930eb877b	1865466.62

Strings

Suspicious API Calls:

- ZwCreateSection
- ZwOpenFile
- ZwClose
- ZwQueryAttributesFile
- ZwQuerySection
- GetProcAddress
- VirtualProtect
- VirtualQuery

- FlushInstructionCache
- UnmapViewOfFile
- MapViewOfFile
- CreateThread
- WaitForSingleObject
- GetExitCodeThread
- OpenProcessToken
- GetTokenInformation

Suspicious DLLs:

These DLLs are often used in malware for system manipulation, persistence, or privilege escalation.

- ntdll.dll
- kernel32.dll
- KERNEL32.DLL.ASLR.%08x
- USER32.dll (can be used for keylogging)
- ADVAPI32.dll (often used for privilege escalation)

Potentially Malicious Functionality:

- lstrcmpiW / lstrcmpiA (often used in anti-analysis)
- GetCurrentProcess
- GetModuleHandleW / GetModuleHandleA
- GetVersionExW
- GetTickCount (used to detect debugging)
- DeleteFileA (can be used to delete evidence)

Potential Indicators of DLL Hijacking or Persistence:

- DllCanUnloadNow
- DllGetClassObject
- DllRegisterServer
- DllRegisterServerEx
- DllUnregisterServer
- DllUnregisterServerEx

Miscellaneous Suspicious Entries:

- .stub (packed .stub section)
- ExitProcess
- TRAVEL_BALOON_1758 - strange images of a hot air balloon in .stub section
-

These strings suggest that injection, persistence, anti-debugging

Week9Core.exe could use process

week9.exe

File Information:

- MD5: dd2490833dca91a2d6990e8806d6401b
- SHA-1: c12045bc1888b19ef09c2619c1d1bc3ad93e86a9
- SHA-
256:0549801bdd218313da5048beaaf670281dfec198b6696b3a4d7e0d2adc10e595
- File type: PE32
- Magic: PE32 executable (GUI) Intel 80386, for MS Windows
- Compiler: Microsoft Visual C/C++ (15.00.30729) [C] Linker: Microsoft Linker (9.00.30729) Tool: Visual Studio (2008)
- File size: 263.50 KB (269824 bytes)
- VirusTotal 40/72 vendors flagged as malicious

Memory Map:

- .text: raw size: 6656, entropy: 5.98
- .bin: raw size: 512, entropy: 0.08
- .reloc: raw size: 512, entropy: 3.94
- .rsrc: raw size: 261120, entropy: 7.08

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	6322	6656	5.98	d19e3016a66d3a76065ad60deb7238c5	85479.97
.bin	12288	32	512	0.08	c155f6664e261082ce5718a1a87a8753	128522
.reloc	16384	390	512	3.94	16cdfb2ed7beeb7a5c57903faf635a2b	32869
.rsrc	20480	261056	261120	7.08	4d51b930a39a1c3c1f84af9900daada2	1866617.88

Week9.dll

File Information:

- MD5:2f4e30a497ae6183aabfe8ba23068c1b
- SHA-1:1df6ae2a5594ab29a6e60b6d9296128b1f9fd980
- SHA-
256:15de4133ad0be9adf8e694ad7f66dd8b89841f8139456edf6efc9c4e5edfc2c8
- File type: Win32 DLL / PE32
- Magic: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
- Compiler: Microsoft Visual C/C++ (15.00.30729) [LTCG/C++] Linker: Microsoft Linker (9.00.30729) Tool: Visual Studio (2008)
- File size:1.53 MB (1603072 bytes)

- F-PROT packer
- Cyren packer
- Varist packer
- VirusTotal: 57/73 flagged as malicious

Memory Map:

- .text: raw size: 316416, entropy: 6.56
- .rdata: raw size: 50688, entropy: 6.12
- .data: raw size: 12800, entropy: 5.17
- .xdata: raw size: 61952, entropy: 3.39
- .cdata: raw size: 1536, entropy: 2.32
- .rsrc: raw size: 1122304, entropy: 6.53
- .reloc: raw size: 36352, entropy: 4.85

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	316322	316416	6.56	0048d582b7b22dd73e57da168ab55dc0	1548041.75
.rdata	323584	50432	50688	6.12	7ce5b4f1b941de540ff83bb355574f0b	1178331.75
.data	376832	14880	12800	5.17	2e6c77210b50b264bd06c8d923f5ae03	465363.19
.xdata	393216	61916	61952	3.39	ba9061e5c21f086c98c062848ab02fe4	5031309
.cdata	458752	1046	1536	2.32	e0c0871ffc748e692873c471c18f5c50	142661.77
.rsrc	462848	1122040	1122304	6.53	10762d26fd7f1bb3bd2062d58517919d	12777229
.reloc	1585152	36176	36352	4.85	e7cf9ec964d02223248d2250eb0e777f	1624714.5

I decided to do a string analysis on week9.dll because I found so many suspicious findings in Ghidra

Suspicious strings:

- HTTP\SHELL\OPEN\COMMAND
- %SystemRoot%\system32\winlogon.exe
- %SystemRoot%\system32\lsass.exe
- tmpoxy.exe
- InstallPath
- SOFTWARE\TrendMicro\NSC\TmProxy
- ekrn.exe
- %A\ESET\ESET Smart Security\Updfiles*.nup
- ccSvcHst.exe
- rtvscan.exe
- %C\Symantec Shared\VirusDefs\binhub*.dat
- fsdfwd.exe
- UmxCfg.exe

- bdagent.exe
- avguard.exe
- Mcshield.exe
- szInstallDir32
- SOFTWARE\McAfee\VSCore
- %C\McAfee\Engine*.dat
- avp.exe
- SOFTWARE\kasperskyLab\avp6\environment
- SOFTWARE\kasperskyLab\avp7\environment
- SOFTWARE\KasperskyLab\protected\AVP7\environment
- SOFTWARE\KasperskyLab\protected\AVP8\environment
- SOFTWARE\KasperskyLab\protected\AVP9\environment
- *%A\Kaspersky Lab\AVP%v\Bases*.c
- HH:mm:ss
- dddd, MMMM dd, yyyy
- MM/dd/yy
- SunMonTueWedThuFriSat
- JanFebMarAprMayJunJulAugSepOctNovDec
- s7otbxsx.dll
- \s7otbxdx.dll
- \s7otbxdx.dl_
- \s7otbxsx.dll
- \help\winmic.fts
- Global\CscCacheClearEvent
- 85991EC7-5621-4A6F-9453-DC19BAE9C542
- Global\85991EC7-5621-4A6F-9453-DC19BAE9C542
- \inf\oem7i.PNF
- \inf\oem7w.PNF
- s7otbxdx.dll
- %SystemRoot%\inf\oem7A.PNF
- Control Panel\Appearance
- %SystemRoot%\inf*.pnf
- %SystemRoot%\inf\mdmeric3.PNF
- %SystemRoot%\inf\mdmcpq3.PNF
- %SystemRoot%\system32\Drivers\mrxcsl.sys
- %SystemRoot%\system32\Drivers\mrxsmb.sys; %SystemRoot%\system32\Drivers*.sys
- MRxCls
- *SYSTEM\CurrentControlSet\Services*
- ImagePath
- .sys
- *??*
- WkssvcShutdownEvent
- Global\WBM_ESP_OPEN_FOR_BUSINESS
- WBM_ESP_OPEN_FOR_BUSINESS

- %SystemRoot%\inf\oem6C.PNF
- MRXCLS
- Global{62BBECCC-536F-4dc6-A387-8B1A17CF8A75}
- SOFTWARE\Microsoft\Windows Defender\Real-Time Protection
- {A3116B9-3F4E-438a-52C8-D0464A2D72B5}
- Global{A3116B9-3F4E-438a-52C8-D0464A2D72B5}
- AFX64c313
- hOmSave7
- S7EPATDX.CPL
- s7hkimdb.dll
- .mcp
- hOmSave7
- s7hkimdb.dll
- S7EPATDX.CPL
- Step7\Example

Student provided an overall analysis for their static analysis and provided their steps and methodology.

This static analysis is for Week9Core.exe, week9.exe, and Week9.dll, and they are all flagged as malicious. Week9Core.exe showed high entropy in its .stub section, indicating packing, and contained an image (TRAVEL_BALOON_1758) within the .stub section. It also listed suspicious API calls related to process injection (ZwCreateSection, ZwOpenFile, ZwClose, MapViewOfFile), anti-debugging (GetTickCount, lstrcpw), and persistence (CreateThread, VirtualProtect). Additionally, it included suspicious DLLs such as ntdll.dll, kernel32.dll, and ADVAPI32.dll, which could indicate system manipulation and privilege escalation. VirusTotal flagged 49/73 vendors as malicious. Week9.exe, another PE32 executable, had lower entropy with 40/72 detections on VirusTotal.

Week9.dll, a PE32 DLL using multiple packers, showed high entropy in its .text and .rsrc sections. It was flagged by 57/73 vendors.

- %SystemRoot%\system32\winlogon.exe, %SystemRoot%\system32\lsass.exe, tmproxy.exe, ekrn.exe, ccSvcHst.exe, rtvscan.exe, fsdfwd.exe, and others, which may be used to manipulate system processes, evade detection, or provide persistence.
- Strings such as %A\ESET\ESET Smart Security\Updfiles*.nup, avguard.exe, Mcshield.exe, szInstallDir32, and avp.exe could indicate attempts to interact with or evade antivirus programs, potentially using techniques such as DLL hijacking or modifying antivirus definitions.
- Entries like SOFTWARE\TrendMicro\NSC\TmProxy,

SOFTWARE\Microsoft\Windows Defender\Real-Time Protection, and paths related to Kaspersky and McAfee indicate attempts to interact with or disable security tools.

- Strings referring to system services (*SYSTEM\CurrentControlSet\Services*) and drivers (%SystemRoot%\system32\Drivers\mrxcsl.sys, %SystemRoot%\system32\Drivers\mrxsmb.sys) suggest attempts at persistence or driver-level manipulation.
- Filenames like s7otbxsl.dll, s7otbxsl.dll, and s7hkimdb.dll are suspicious

Dynamic Analysis

Provided dynamic analysis using tools to aid in the identify activity.

- For my dynamic analysis I used AnyRun and Wireshark

Week9Core.exe

Processes:

- Week9Core.exe
 - "C:\Users\admin\AppData\Local\Temp\Week9Core.exe" is run
- C:\WINDOWS\system32\SppExtComObj.exe -Embedding is a Windows system file responsible for managing Windows licensing and activation. It runs as a COM object to verify the activation status of Windows. If the file is located outside the C:\WINDOWS\system32\ directory or lacks a valid Microsoft signature, it could indicate potential malware

Registry:

- Week9Core.exe
 - Queries the registry to check supported languages
- slui.exe
 - Reads the software policy settings
 - Checks proxy server information

Network

- activation-v2.sls.microsoft.com
- 192.168.100.255
- login.live.com
 - 40.126.32.74
 - 20.190.160.3
 - 20.190.160.17
 - 20.190.160.4
 - 20.190.160.67
 - 20.190.160.20
 - 20.190.160.5

week9.exe

Overview: very similar dynamic analysis results to Week9Core.exe

- Reads the software policy settings
 - slui.exe (PID: 7420)
- Checks supported languages
 - week9.exe (PID: 7312)

Week9.dll

Overview: Also very similar results to Week9Core.exe and week9.exe

- rundll32.exe
 - "C:\WINDOWS\SysWOW64\rundll32.exe"
 - C:\Users\admin\AppData\Local\Temp\Week9.dll, #1
- Network:
 - 192.168.100.255
 - 40.91.76.224: activation-v2.sls.microsoft.com (unknown reputation score)

40.126.32.7

Student used a disassembler and used their dynamic analysis findings to aid disassembler review of the malicious analysis.

- rundll32.exe (observed in dynamic analysis) is used to launch specific functions within dlls. This caused me to take a closer look at the dll functions in Week9Core.exe and week9.dll.
- DllCanUnloadNow could be used maliciously to ensure the DLL remains in memory, which could be part of a persistence mechanism
- Analyzed week9.dll
 - .?AVMiniZipDuplicateTransformRule@@"
 - SOFTWARE\SIEMENS\STEP7" - this refers to Siemens industrial control software

Provided an analysis comparing the results from your static and dynamic analyses.

The presence of winlogon.exe and lsass.exe, legitimate system processes related to user login and security, indicates the possibility of malware attempting to inject itself into these processes to get persistence and escalate privileges. Antivirus-related executables and paths, such as avguard.exe (AVG), Mcshield.exe (McAfee), and avp.exe (Kaspersky), suggest intent to bypass security defenses.

The SOFTWARE\TrendMicro\NSC\TmProxy and SOFTWARE\Microsoft\Windows Defender\Real-Time Protection registry keys indicate attempts to

interact with or disable security tools.
other suspicious file paths, including %SystemRoot
%\system32\Drivers\mrxcsl.sys and %SystemRoot
%\system32\Drivers\mrxsmb.sys, point to the malware's potential to
manipulate system drivers for persistence or privilege escalation.
The high entropy in sections such as .text, .rsrc, and .stub supports
the hypothesis that Week9.dll and Week9Core.exe use packing for
obfuscation purposes and to make analysis more difficult.
An observation in the dynamic analysis was the use of rundll32.exe to
load Week9.dll. This is a well-known technique for executing code
hidden in DLLs, bypassing traditional execution mechanisms, and making
detection more challenging. The DllCanUnloadNow function could be
exploited to prevent the DLL from being unloaded, thus helping the
malware maintain persistence in memory. Another aspect in both the
static and dynamic analyses was the interaction with the Windows
software activation process, slui.exe, which is responsible for
checking the activation status of Windows.
In static analysis, the string references to various antivirus
processes such as avgguard.exe, Mcshield.exe, rtvscan.exe, Kaspersky,
and ESET suggest the malware's intent to affect or disable security
tools. The static analysis revealed references to persistence
mechanisms through the manipulation of system drivers (e.g.,
mrxcsl.sys and mrxsmb.sys). In dynamic analysis, this persistence was
corroborated by the use of rundll32.exe to execute the malicious DLL.
Both analyses noted suspicious network activity. The dynamic analysis
pointed to connections to external IPs like activation-
v2.sls.microsoft.com. Week9.dll is likely involved in disabling or
bypassing antivirus protections and data exfiltration.

Indicators of Compromise

Student identified Host-based IoC #1 which are indicators that suggest suspicious activity on a specific computer or system.

- Suspicious file paths and filenames such as %SystemRoot
%\system32\winlogon.exe, %SystemRoot%\system32\lsass.exe, and
tmproxy.exe. These files are often used by malware to manipulate
system processes, evade detection, or gain persistence.

Student identified Host-based IoC #2 which are indicators that suggest suspicious activity on a specific computer or system.

- Suspicious registry entries such as
SOFTWARE\TrendMicro\NSC\TmProxy and SOFTWARE\Microsoft\Windows
Defender\Real-Time Protection. These entries could suggest
attempts to interact with or disable antivirus programs

Student identified Host-based IoC #3 which are indicators that suggest suspicious activity on a specific computer or system.

- Student identified Network-Based Indicator which are Indicators associated with a network communication, such as an IP address or domain name. No network activity is a result.

- [illegible]

app.any.run/tasks/24cafe8f-b043-4a3c-84b3-a86b994c3f25

Tools Social Media and O... Recon Additional Recon Email Search Dev OSINT GLTR (glitter) v0.5

win10 64bit

01:06

CPU 0% RAM 38%

Processes

PID	Process name	Mem	CPU	IO
7312	week9.exe	69	9	21
7388	COM SppExtComObj.Exe -Embedding	69	30	34
7420	slui.exe RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2:Actio...	521	88	42

HTTP Requests 5 Connections 19 DNS Requests 12 Threats 0

Timeshift	Headers	Rep	PID	Process name	CN	URL
BEFORE	GET 200: OK	✓	-	-	-	http://cr1.microsoft.com/pki/crl/produc...
BEFORE	GET 200: OK	✓	-	-	-	http://cr1.microsoft.com/pki/crl/produc...
6942 ms	GET 200: OK	✓	6544	svchost.exe	-	http://ocsp.digicert.com/MFEWtZBNM...
29464 ms	GET 200: OK	✓	8000	SIHClient.exe	-	http://www.microsoft.com/pkiops/crl/...
29465 ms	GET 200: OK	✓	8000	SIHClient.exe	-	http://www.microsoft.com/pkiops/crl/...

app.any.run/tasks/24cafe8f-b043-4a3c-84b3-a86b994c3f25

Tools Social Media and O... Recon Additional Recon Email Search Dev OSINT GLTR (glitter) v0.5

win10 64bit

02:51

CPU 10% RAM 38%

Processes

PID	Process name	Mem	CPU	IO
1852	rundll32.exe C:\Users\admin\AppData\Local\Temp\Week9...	261	63	-
5072	COM SppExtComObj.Exe -Embedding	69	30	-
4880	slui.exe RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2:Actio...	524	88	-

HTTP Requests 2 Connections 4 DNS Requests 6 Threats 0

Timeshift	Headers	Rep	PID	Process name	CN	URL
BEFORE	GET 200: OK	✓	-	-	-	http://cr1.microsoft.com/pki/crl/produc...
7476 ms	GET 200: OK	✓	6544	svchost.exe	-	http://ocsp.digicert.com/MFEWtZBNM...