Static Analysis

hpreader.exe
Virus Total Analysis
Hash Analysis

- File Hash: [Insert MD5, SHA-1, SHA-256 hash value]
  - MD5:ec5fabce1aea37883ce92d016c8a8e20
  - SHA-1:c0554c4d746a823e0dfedc23b1d7f823ab7a3840
  - SHA-256:a70ea8f787e6560d48fe90182e9c0e5ebc587d96bea3ab6491ba29ef4727a95f
- Method of hash acquisition:Found on VirusTotal and confirmed using Detect-It-Easy
- [Link to VirusTotal results]
  - https://www.virustotal.com/gui/file/a70ea8f787e6560d48fe90182e9c0e5ebc587d96bea3ab6491ba29ef4727a95f/details

Vendor Analysis

- Number of vendors flagging as malicious: 0/72
- Analysis of vendor results:
  - This file was undetected by every single vendor
  - The digital signature of the file did not verify.
  - This file seems to do everything a pdf viewer would do
  - No antivirus would flag this file as malicious

File History

- First Submission Date: 2025-03-31 20:32:43 UTC
- File Creation Date from Windows: 2017-11-22 08:36:52 UTC
- Analysis of submission timeline:
  - This file was created 7-8 years ago
  - It was first submitted to VirusTotal last week

Community Score

- [Link to your VirusTotal community contribution]
  - https://www.virustotal.com/gui/file/a70ea8f787e6560d48fe90182e9c0e5ebc587d96bea3ab6491ba29ef4727a95f/community
  - sshinn: This is a pdf reader, however it has a suspicious import to msimg32.dll, which drops a malicious payload.

Detect It Easy (DIE) Analysis
File information

- File type: PE32
- Architecture: i386
- Compiler: Microsoft Visual C/C++(15.00.30729)[LTCG/C] [Compiler information]
- Additional relevant information:
  - Operation system: Windows(2000)[I386, 32-bit, GUI]

- Overlay: Binary[Offset=0x00610400,Size=0x1c68]
- File size: 6.17 MiB
- Lists suspicious dll msimg32.dll as an import (found in Ghidra)
  - Import(6)(CRC)['MSIMG32.dll']
  - Packed .text section
  - Packed .rdata section
  - Packed overlay

Memory Map Analysis

- Section breakdown:
  - [.text section analysis]
    - Size: 2914816
    - Entropy:6.52
    - Permissions:RE
  - [.rdata section analysis]
    - Size:2842112
    - Entropy:7.11
    - Permissions:R
  - [.data section analysis]
    - Size:408576
    - Entropy:5.2
    - Permissions:RW
  - [.rsrc]
    - Size:191488
    - Entropy:4.75
    - Permissions:None listed
    - Includes packed overlay
- Notable findings:
  - [Unusual section permissions]
    - .text has read execute permissions
    - .data has read write permissions
  - [Section size anomalies]
  - .rdata and .text sections are very large and both have high entropy

String Analysis

- Notable strings discovered:
  - GdipDeleteBrush
  - GdipFree
  - GdipDeletePen
  - GdipCloneBrush
  - GdipDeleteGraphics
  - GdipSetSmoothingMode
  - GdipCreateSolidFill
  - GdipAlloc
  - GdipSetPageUnit

    - GdipCreateFromHDC
    - GdipSetCompositingQuality
    - GdipFillRectangleI
    - GdipDrawLineI
    - GdipCreatePen1
    - GdipFillEllipseI
    - GdipCreateBitmapromStreamICM
    - GdipGetImageHorizontalResolution
    - GdipCloneBitmapAreaI
    - GdipScaleMatrix
    - GdipGetImageHeight
- String analysis: There were no strings that seemed suspicious. All of the strings appeared to support that this is a legitimate pdf viewer program.

Entropy Analysis

- Overall entropy score: 6.97434
- Section-specific entropy:
    - .text: 6.51549 entropy, packed
    - .rdata: 7.11177 entropy, packed
    - Overlay: 7.39975 entropy, packed

msimg32.dll

Virus Total Analysis

Hash Analysis

- File Hash: [Insert MD5, SHA-1, SHA-256 hash value]
    - MD5: 103d1f6978b25cdef890f96950d64324
    - SHA-1: 690fdd8951f31f464fe4474e2f90b96f4d4ed4e7
    - SHA-256:fe4b2bdd63fc4d2afe0add5931a4f2cfb0b93f3b969028e321153dbfccdac408
- Method of hash acquisition:Found on VirusTotal and confirmed using Detect-It-Easy
- [Link to VirusTotal results]: https://www.virustotal.com/gui/file/fe4b2bdd63fc4d2afe0add5931a4f2cfb0b93f3b969028e321153dbfccdac408/details

Vendor Analysis

- Number of vendors flagging as malicious: 36/71
- Analysis of vendor results:
    - Malware Family: Trojan, dllhijack, zusy, injector, win32
    - Malware Features: pedll, idle, detect-debug-environment, overlay, spreader, checks-user-input

File History

- First Submission Date: 2024-10-14 10:19:27 UTC
- File Creation Date from Windows: 2020-12-22 10:54:25 UTC

- Analysis of submission timeline:
    - The file was created 4 years before it was submitted to VirusTotal

Community Score

- [Link to your VirusTotal community contribution]:
- https://www.virustotal.com/gui/file/fe4b2bdd63fc4d2afe0add5931a4f2cfb0b93f3b969028e321153dbfccdac408/community
- Sshinn: this is a search order DLL hijacker which drops a malicious exe when a debugger is being used. hpreader.exe acts as a trojan dropper using DLL hijacking to execute msimg32.dll. msimg32.dll unpacks branding.dll, which drops and executes DLLLoader32_D39F.exe. Malware uses obfuscation, anti-debugging techniques.

- Summary of initial findings posted to the community:
    - This dll file works with hpreader.exe and keeps a connection alive to perform data exfiltration
    - The file hpreader.exe appears to call the .dll and execute it
    - The .dll may be using the .exe file to avoid detection and establish persistence. There is also an X.509 certificate signature found in the analysis. This could be to make a malicious file appear to be legitimate.

Detect It Easy (DIE) Analysis

File information

- File type: PE32
- Architecture: i386
- Compiler: Microsoft Visual C/C++(15.00.30729)[C++]
- Additional relevant information:
    - Operation system: Windows(2000)[I386, 32-bit, DLL]
    - Strange structure: Debug data: Binary[Offset=0x000f8ac0,Size=0x58]
    - Strange overlay: Overlay: Binary[Offset=0x00403400,Size=0x02dfcc00]

Memory Map Analysis

- Section breakdown:[.text section analysis]
    - [.text section analysis]:
        - Size:938496
        - Entropy:6.77
        - Permissions:RE
    - [.data section analysis]:
        - Size:167424
        - Entropy:1.51
        - Permissions:RW
    - [.rdata section analysis]:
        - Size:148480
        - Entropy:5.32
        - Permissions:R

- [.rsrc section analysis]:
  - Size:2952192
  - Entropy:6.87
  - Permissions:R
  - Contains overlay
    - Size of overlay: 02dfcc00

- Notable findings:
  - [Unusual section permissions]
    - Packed .text section
    - Packed .rsrc section
    - Unpacked overlay
    - RE .text section
    - RW .data section
  - [Section size anomalies]
    - .rsrc section is large, large overlay

String Analysis

- Notable strings discovered:
  - No suspicious strings in msimg32.dll

Entropy Analysis

- Overall entropy score: 0.84367
- Section-specific entropy:
  - .text section : 6.76964 entropy
  - .rsrc section: 6.87467 entropy
    - Unpacked overlay: 0.0000 entropy
- I unpacked the file and found a "child" dll file called "branding.dll" using UnPac.Me

Disassembly Analysis

I opened branding.dll in x64dbg. This is what I found:

- dllloader32_d39f.00570000
- I dumped the memory of the dllloader32 into a bin file on my desktop
- When I ran branding.dll in x64dbg or when I dumped the memory, a new file appeared on my desktop: DLLLoader32_D39F.exe
- I looked at the strings, and found a lot of malicious apis

Indicators of Compromise found in DLLLoader32_D39F.exe

- Local\szLibraryName%X – dynamic loading of libraries with obfuscated or hidden paths.
- c:\x64_dbg\bin\x32\loaddll.pdb – The use of a debugger or a reference to a PDB suggest debugging
- USER32.dll – process attempting to interact with the user interface in a suspicious manner
- mscoree.dll – if loaded unexpectedly, this may indicate attempts at running malicious .NET code.
- kernel32.dll, ntdll.dll, KERNEL32.dll
- LoadLibraryW, LoadLibraryExA – Loading DLLs dynamically, code injection or malicious libraries

- FreeLibrary, GetProcAddress, FreeLibraryWhenCallbackReturns – these are called to unload or manipulate DLLs to evade detection
- GetModuleHandleExW, GetModuleHandleW – may be used to manipulate or access system libraries inappropriately.
- CreateThreadpoolTimer, SetThreadpoolTimer, WaitForThreadpoolTimerCallbacks – Threads and timers are often used in malware.
- CreateEventExW, CreateSemaphoreExW – malware may use these to control or manipulate the execution flow.
- MessageBoxW – Often used for UI popups
- IsDebuggerPresent – anti-debugging technique
- TerminateProcess, ExitProcess – avoid detection or terminate other security-related processes.
- SetFileInformationByHandleW, GetFileInformationByHandleExW – used to hide files or manipulate the filesystem.
- RtlGetLastNtStatus, RtlUnwind, RaiseException, UnhandledExceptionFilter – could be used for error handling and exception management, often seen in malware trying to evade detection or analysis.
- IsDebuggerPresent, EncodePointer, DecodePointer – used in anti-debugging techniques
- GetCommandLineA –could be a tactic to manipulate execution based on how it was launched.
- GetLastError, GetCurrentProcessId, GetThreadId –used to gather process information and detect or avoid analysis tools.
- CreateSymbolicLinkW – could be used for hiding files or directories
- SetFilePointerEx, FlushFileBuffers – related to file manipulation and could be used to modify files secretly
- HeapAlloc, HeapReAlloc, HeapFree – memory management functions

Static Analysis Summary

I originally had two files, hpreader.exe and msimg32.dll. hpreader.exe listed msimg32.dll as an import. I unpacked msimg32.dll and was able to get another .dll file, branding.dll. When I debugged branding.dll, it unpacked and dropped DLLLoader32_D39F.exe, which had a lot of malicious apis and strings.

- Key findings from static analysis:
    - This executable exhibited multiple malicious behaviors including anti-debugging techniques, dynamic DLL loading, thread/timer manipulation, file system obfuscation, and potential for code injection or persistence.
    - Acts as a loader for malware (DLLLoader32_D39F.exe), likely to establish persistence and exfiltrate data
    - Evidence of anti-analysis features: IsDebuggerPresent, use of .pdb references, GetCommandLineA, and exception handling routines for evasion.
    - Dynamic file dropping
    - Capable of dynamically loading malicious libraries, hiding execution via overlay and obfuscated strings, and interacting

with the filesystem or UI

Dynamic Analysis
1. Analysis Environment
Environment Setup
Virtual Machine specifications:
- Microsoft Windows XP Version 2002 Service Pack 3
- 444 MB of RAM
- [Network configuration]Disconnected from wireless network

Monitoring tools deployed:
- RegShot, Process Monitor, Process Explorer, Wireshark

Safety measures implemented:
- Used Malware Machine

[Network isolation]
- Disconnected from network, I used AnyRun and downloaded the PCAP to analyze with Wireshark from AnyRun

2. Runtime Observations
Initial Execution
[Immediate system changes]
- I received a pop up message asking me to confirm execution, I confirmed
- Then I got a message that the program closed unexpectedly, in Process Explorer the program shows up as "Suspended"

[Process creation]
- msimg32.dll processes started running on both Process Explorer and Process Monitor

[Registry creation]
- Keys added: 3
- Values added: 6
- Values modified: 24
- Total changes: 33
- A new MUICache entry references \\tsclient\D\Week10\hpreader.exe, identified as “Haihaisoft PDF Reader CYBV 454 Malware Analysis,”. Additionally, the UserAssist key reveals obfuscated (ROT13) execution of the same path. Creation of new ShellNoRoam Bag entries

[Network activity]
- Connects to suspicious IP: 192.168.100.255
- Total Packets:550
- Network Connections:47
- Many UDP queries to desktop-jglljld.local

[File system changes]
- ProcessMonitor showed msimg32.dll opening, closing, and creating files

Post-Execution Analysis
System state changes:
- Permanent modifications:
    - Registry changes include MUICache and UserAssist entries.
    - Creation of ShellNoRoam Bag entries.
    - Dropped DLLLoader32_D39F.exe onto disk.

- Persistence mechanisms:
  - DLL search order hijacking.
  - Use of Threadpool timers and Windows registry modifications.
- Data exfiltration evidence:
  - Network activity (UDP packets, repeated DNS lookups).
  - Suspicious connection attempts to 192.168.100.255.

Network activity summary:

- Connection attempts:
  - Repeated attempts to 192.168.100.255 (potential C2).
  - 47 distinct network connection attempts.
- Data transfers:
  - 550 packets logged in PCAP file..
- Command & Control activity:
  - DNS queries to suspicious desktop-jglljld.local

Impact Analysis

1. User Impact Assessment

Home Users:

- Potential impact:
  - Identity theft, credential harvesting, system compromise.
- Risk level:
  - High.
- Data compromise potential:
  - Browser data, files, personal documents, stored credentials.

Business Users:

- Operational impact:
  - Disruption due to loader execution
  - Credential theft
- Data security concerns:
  - client data, credentials
- Financial implications:
  - Cleanup costs, legal fines for data breaches.

Government Users:

- Security implications:
  - Highly sensitive data at risk.
- Data sensitivity concerns:
  - Classified documents or PII compromise.
- Operational disruption potential:
  - Could disrupt critical infrastructure or defense systems.

2. Mitigation Strategy

Immediate Response:

- Initial containment steps:
  - Isolate infected systems from the network.
  - Kill DLLLoader32_D39F.exe, msimg32.dll
- System isolation procedures:
  - Disconnect from internet
- Data preservation methods:
  - Create backups

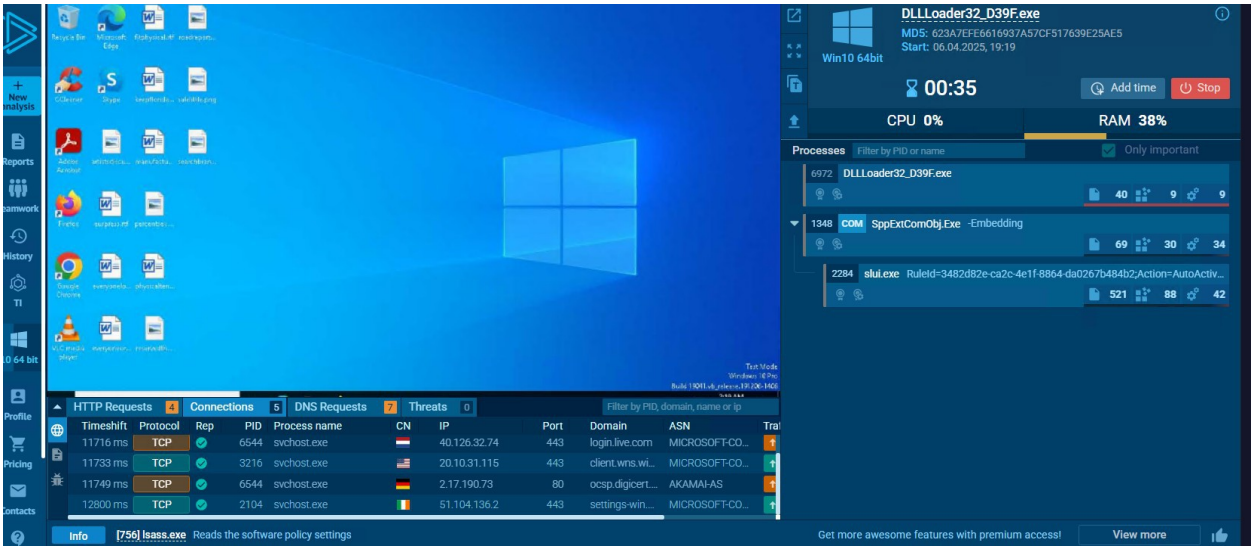
Conclusion

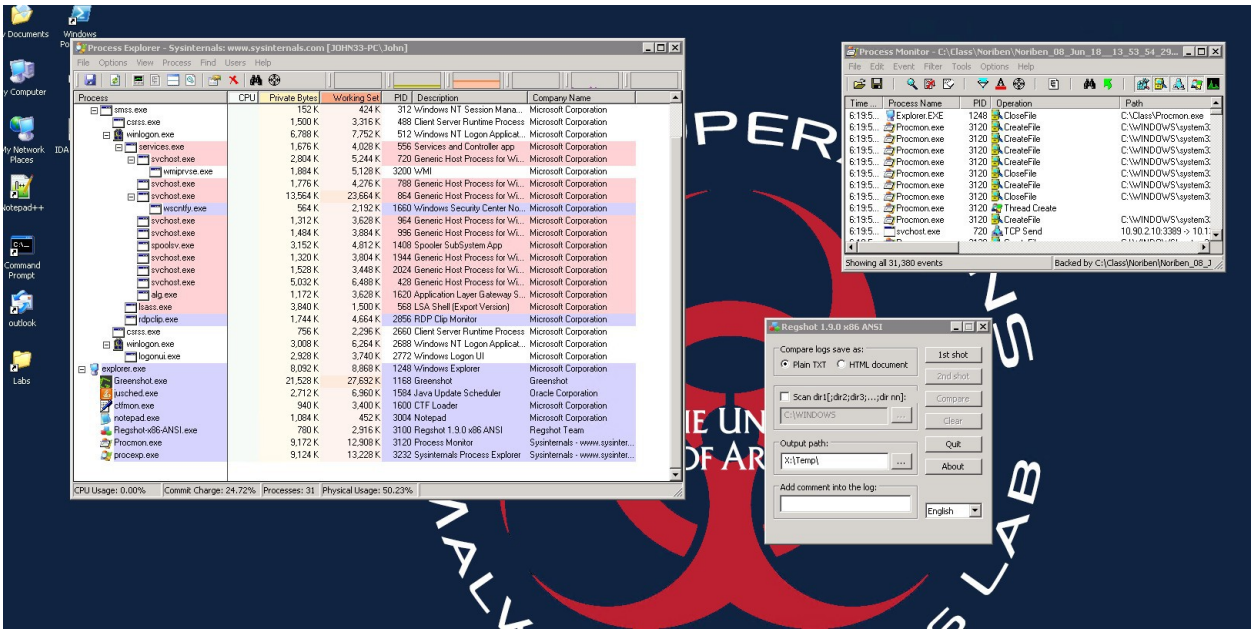
1. Analysis Reflection
   - Summary of findings:
     - hpreader.exe acts as a trojan dropper using DLL hijacking to execute msimg32.dll.
     - msimg32.dll unpacks branding.dll, which drops and executes DLLLoader32_D39F.exe.
     - Malware uses obfuscation, anti-debugging
   - Unusual characteristics:
     - Malicious payload hidden in overlays.
     - Uses anti-debugging techniques that trigger unpacking behavior only while debugging
   - Learning outcomes:
     - DLL imports and overlays.
     - anti-debugging techniques can trigger hidden behaviors.
   - hpreader.exe: A seemingly ordinary PDF viewer.
     - It is ordinary, but it has a suspicious import: msimg32.dll
   - msimg32.dll: A graphics-related library—but is it what it claims?
     - When I unpacked this file I found branding.dll
   - Which file contains the malicious payload, and how is it triggered?
     - branding.dll dropped an executable: DLLLoader32_D39F.exe
     - It was triggered by opening the file in x64dbg
   - How are the files connected?
     - hpreader.exe is a legitimate pdf reader file hiding a trojan
     - It imports msimg32.dll, which unpacks to a file called branding.dll, which drops DLLLoader32_D39F.exe when it is opened in a debugger
   - Is there a persistence mechanism or any evidence of code injection or hijacking?
     - Yes, the malware uses DLL search order hijacking. Strong evidence of code injection includes dynamic API calls like LoadLibraryExA, GetProcAddress, and CreateThreadpoolTimer.
   - What does the malware do, and when does it do it?
     - This malware uses obfuscated strings and malicious APIs to inject code, manipulate memory, and exfiltrate data while evading detection through anti-debugging techniques
   - Determine whether the .exe calls into the .dll—and what the .dll does once loaded.
     - Yes, hpreader.exe imports and calls into the malicious msimg32.dll, triggering its execution. Once loaded, the .dll unpacks and runs a secondary payload (DLLLoader32_D39F.exe), which performs dynamic DLL loading, anti-debugging, thread manipulation, and likely code injection and data exfiltration.
   - Identify at least four Indicators of Compromise (IoCs), including:
     - hpreader.exe acts as a trojan dropper using DLL hijacking to execute msimg32.dll. msimg32.dll unpacks branding.dll, which drops and executes DLLLoader32_D39F.exe..
     - FreeLibrary, GetProcAddress, FreeLibraryWhenCallbackReturns –

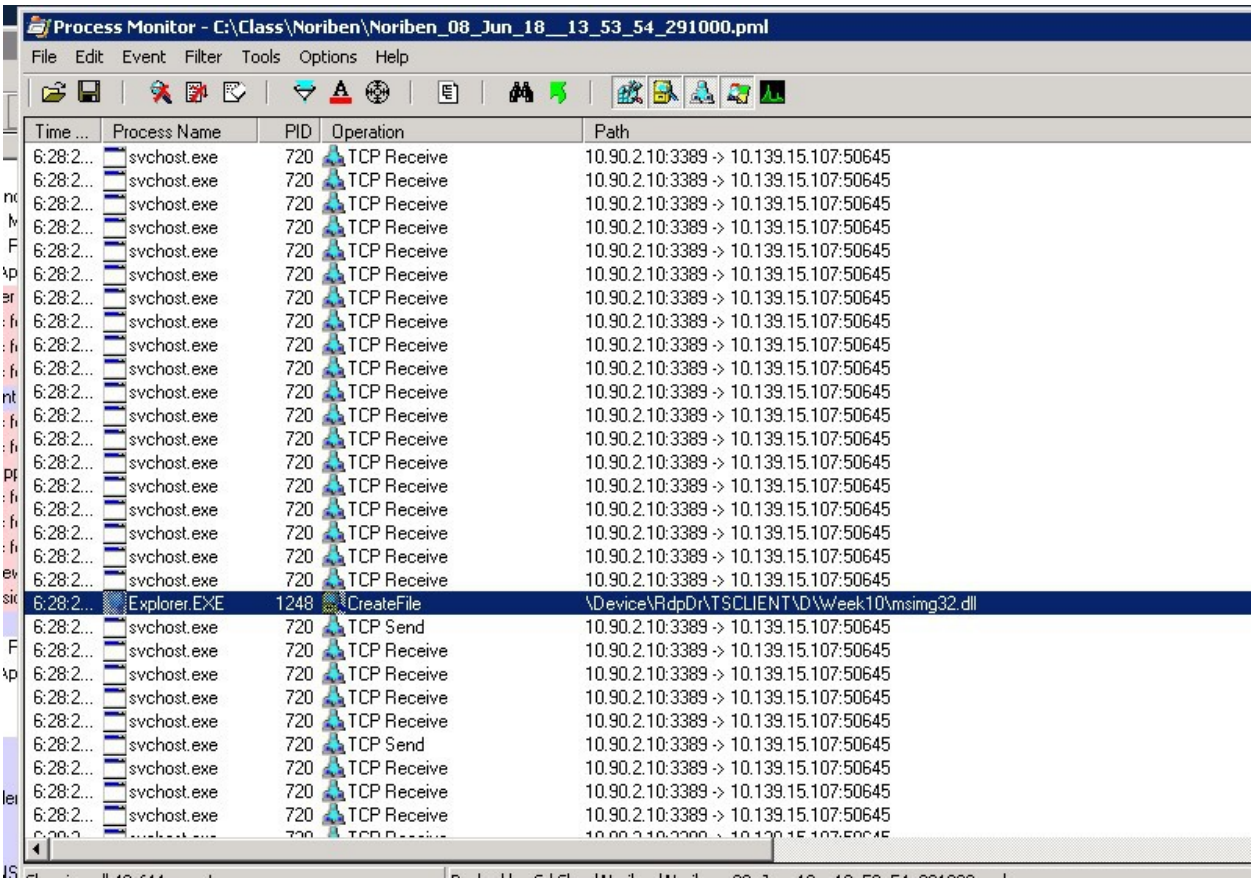
these are called to unload or manipulate DLLs to evade detection

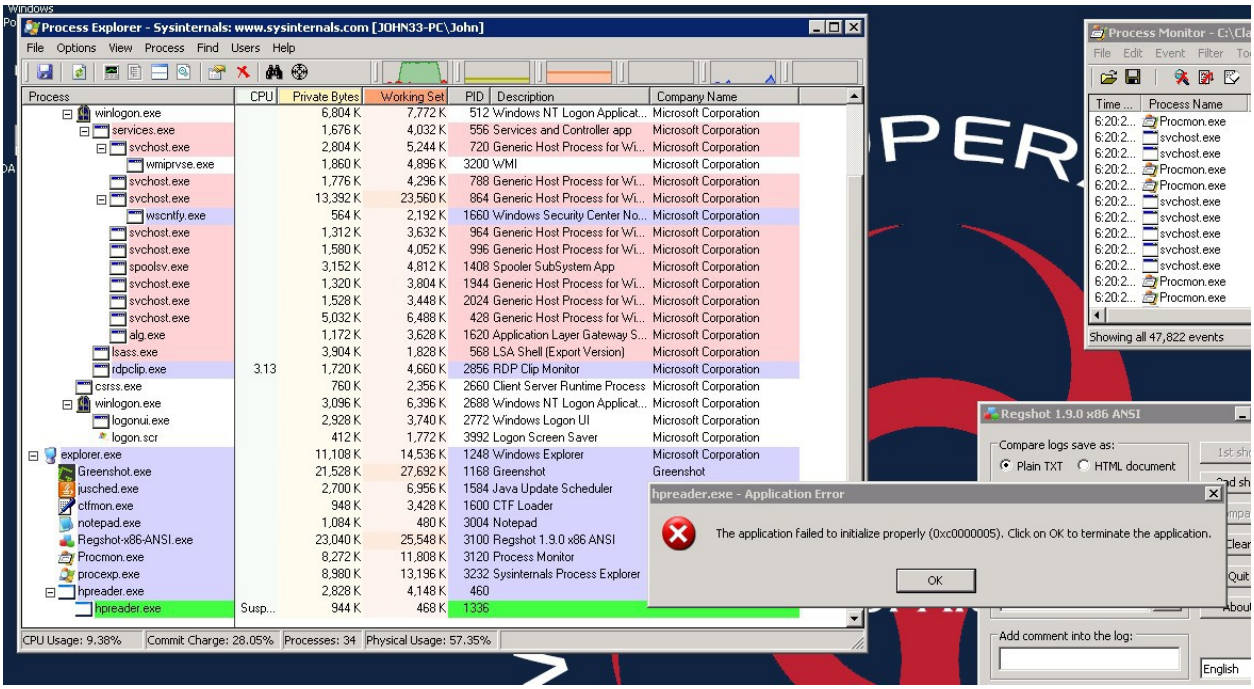
- GetModuleHandleExW, GetModuleHandleW – may be used to manipulate or access system libraries inappropriately.
- CreateThreadpoolTimer, SetThreadpoolTimer, WaitForThreadpoolTimerCallbacks – Threads and timers are often used in malware
- IsDebuggerPresent, EncodePointer, DecodePointer – used in anti-debugging techniques
- Network-based indicators
  - DNS queries to suspicious desktop-jglljld.local
  - Repeated attempts to 192.168.100.255 (potential C2)

I will do a separate static analysis for each file.




Process Explorer - Sysinternals: www.sysinternals.com [JOHN33-PC\John]
Process Monitor - C:\Class\Noriben\Noriben_08_Jun_18__13_53_54_29...
Regshot 1.9.0 x86 ANSI
Compare logs save as:
Plain TXT
HTML document
1st shot
2nd shot
Compare
Clear
Quit
About
Output path:
X:\Temp\
Add comment into the log:
English


Process Monitor - C:\Class\Noriben\Noriben_08_Jun_18__13_53_54_291000.pml
File Edit Event Filter Tools Options Help
Time ... Process Name PID Operation Path
6:28:2... svchost.exe 720 TCP Receive 10.90.2.10:3389 -> 10.139.15.107:50645
6:28:2... Explorer.EXE 1248 CreateFile \Device\RdpDr\TSCLIENT\D\Week10\msimg32.dll
6:28:2... svchost.exe 720 TCP Send 10.90.2.10:3389 -> 10.139.15.107:50645


Process Explorer - Sysinternals: www.sysinternals.com [JOHN33-PC\John]
File Options View Process Find Users Help
Process CPU Private Bytes Working Set PID Description Company Name
winlogon.exe 6,804 K 7,772 K 512 Windows NT Logon Applicat... Microsoft Corporation
services.exe 1,676 K 4,032 K 556 Services and Controller app Microsoft Corporation
svchost.exe 2,804 K 5,244 K 720 Generic Host Process for Wi... Microsoft Corporation
wmiprvse.exe 1,860 K 4,896 K 3200 WMI Microsoft Corporation
svchost.exe 1,776 K 4,296 K 788 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 13,392 K 23,560 K 864 Generic Host Process for Wi... Microsoft Corporation
wscntfy.exe 564 K 2,192 K 1660 Windows Security Center No... Microsoft Corporation
svchost.exe 1,312 K 3,632 K 964 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 1,580 K 4,052 K 996 Generic Host Process for Wi... Microsoft Corporation
spoolsv.exe 3,152 K 4,812 K 1408 Spooler SubSystem App Microsoft Corporation
svchost.exe 1,320 K 3,804 K 1944 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 1,528 K 3,448 K 2024 Generic Host Process for Wi... Microsoft Corporation
svchost.exe 5,032 K 6,488 K 428 Generic Host Process for Wi... Microsoft Corporation
alg.exe 1,172 K 3,628 K 1620 Application Layer Gateway S... Microsoft Corporation
lsass.exe 3,904 K 1,828 K 568 LSA Shell (Export Version) Microsoft Corporation
rdpclip.exe 3.13 1,720 K 4,660 K 2856 RDP Clip Monitor Microsoft Corporation
csrss.exe 760 K 2,356 K 2660 Client Server Runtime Process Microsoft Corporation
winlogon.exe 3,096 K 6,396 K 2688 Windows NT Logon Applicat... Microsoft Corporation
logonui.exe 2,928 K 3,740 K 2772 Windows Logon UI Microsoft Corporation
logon.scr 412 K 1,772 K 3992 Logon Screen Saver Microsoft Corporation
explorer.exe 11,108 K 14,536 K 1248 Windows Explorer Microsoft Corporation
Greenshot.exe 21,528 K 27,692 K 1168 Greenshot Greenshot
jusched.exe 2,700 K 6,956 K 1584 Java Update Scheduler Microsoft Corporation
ctfmon.exe 948 K 3,428 K 1600 CTF Loader Microsoft Corporation
notepad.exe 1,084 K 480 K 3004 Notepad Microsoft Corporation
Regshot-x86-ANSI.exe 23,040 K 25,548 K 3100 Regshot 1.9.0 x86 ANSI
Procmon.exe 8,272 K 11,808 K 3120 Process Monitor Microsoft Corporation
procexp.exe 8,980 K 13,196 K 3232 Sysinternals Process Explorer Microsoft Corporation
hpreader.exe 2,828 K 4,148 K 460
hpreader.exe Susp... 944 K 468 K 1336
CPU Usage: 9.38% Commit Charge: 28.05% Processes: 34 Physical Usage: 57.35%
Process Monitor - C:\Cla
File Edit Event Filter To
Time... Process Name
6:20:2... Procmon.exe
6:20:2... svchost.exe
6:20:2... svchost.exe
6:20:2... Procmon.exe
6:20:2... Procmon.exe
6:20:2... svchost.exe
6:20:2... svchost.exe
6:20:2... svchost.exe
6:20:2... svchost.exe
6:20:2... svchost.exe
6:20:2... Procmon.exe
6:20:2... Procmon.exe
Showing all 47,822 events
Regshot 1.9.0 x86 ANSI
Compare logs save as:
Plain TXT HTML document
hpreader.exe - Application Error
The application failed to initialize properly (0xc0000005). Click on OK to terminate the application.
OK
Add comment into the log:
English


HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HR
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\Shell\Bags\36\Shell\WinPos1920x1080(1).left: 0x00000042
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\Shell\Bags\36\Shell\WinPos1920x1080(1).top: 0x00000042
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\Shell\Bags\36\Shell\WinPos1920x1080(1).top: 0x00000058
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\Shell\Bags\36\Shell\WinPos1920x1080(1).right: 0x00000362
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\Shell\Bags\36\Shell\WinPos1920x1080(1).right: 0x00000378
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\Shell\Bags\36\Shell\WinPos1920x1080(1).bottom: 0x0000029A
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\Shell\Bags\36\Shell\WinPos1920x1080(1).bottom: 0x000002B0
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots: 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\18\MRUListEx: FF FF FF FF
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\0\18\MRUListEx: 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\1\Shell\WinPos1920x1080(1).left: 0x00000042
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\1\Shell\WinPos1920x1080(1).left: 0x00000058
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\1\Shell\WinPos1920x1080(1).top: 0x00000042
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\1\Shell\WinPos1920x1080(1).top: 0x00000058
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\1\Shell\WinPos1920x1080(1).right: 0x00000362
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\1\Shell\WinPos1920x1080(1).right: 0x00000378
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\1\Shell\WinPos1920x1080(1).bottom: 0x0000029A
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\1\Shell\WinPos1920x1080(1).bottom: 0x000002B0
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell\WinPos1920x1080(1).left: 0x00000042
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell\WinPos1920x1080(1).left: 0x00000058
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell\WinPos1920x1080(1).top: 0x00000042
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell\WinPos1920x1080(1).top: 0x00000058
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell\WinPos1920x1080(1).right: 0x00000362
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell\WinPos1920x1080(1).right: 0x00000378
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell\WinPos1920x1080(1).bottom: 0x0000029A
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\10\Shell\WinPos1920x1080(1).bottom: 0x000002B0
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\154\Shell\WinPos1920x1080(1).left: 0x00000042
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\154\Shell\WinPos1920x1080(1).left: 0x00000058
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\154\Shell\WinPos1920x1080(1).top: 0x00000042
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\154\Shell\WinPos1920x1080(1).top: 0x00000058
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\154\Shell\WinPos1920x1080(1).right: 0x00000362
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\154\Shell\WinPos1920x1080(1).right: 0x00000378
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\154\Shell\WinPos1920x1080(1).bottom: 0x0000029A
HKU\S-1-5-21-1547161642-1614895754-1801674531-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\154\Shell\WinPos1920x1080(1).bottom: 0x000002B0
Total changes: 33
Procmon.exe
procexp.exe
hpreader.exe
[Process creation]
msimg32.dll processes started running on both Process Explorer and Process Monitor
[Registry creation]
Keys added: 3