

# Malware Analysis and Enumeration Project

## Introduction

In my role as an ethical hacker with the EC-Council, I conducted an extensive project focused on malware analysis and enumeration techniques. This project was designed to demonstrate my capabilities in identifying, creating, and analyzing malware, as well as extracting critical information from target networks to enhance security measures.

## Objectives

The primary objectives of this project were:

- **Malware Creation and Exploitation:**
  - Creating a Trojan and exploiting a target machine.
  - Developing a virus to infect the target machine.
  - Conducting malware analysis to determine origin, functionality, and potential impact.
  - Detecting malware within a network.
- **Enumeration:**
  - Extracting various pieces of information about the target, such as machine names, ports, operating systems, services, network resources and shares, usernames, user groups, policies, passwords, routing tables, audit settings, and service configurations.

## Tasks and Techniques

This project involved performing a series of tasks using a variety of tools and techniques to achieve thorough malware analysis and enumeration. The tasks included:

1. **Creating and Exploiting Malware:**
  - **Trojan Creation and Exploitation:** Gaining access to and control over victim machines using tools like njRAT and Theef RAT Trojan.
  - **Virus Creation:** Using the JPS Virus Maker Tool to develop a virus and infect target systems.
2. **Static Malware Analysis:**
  - Using tools like Hybrid Analysis, BinText, PeID, Detect It Easy (DIE), PE Explorer, Dependency Walker, IDA, OllyDbg, and Ghidra to perform static analysis of malware samples.
3. **Dynamic Malware Analysis:**
  - Employing tools like TCPView, CurrPorts, Process Monitor, Reg Organizer, Windows Service Manager, Autoruns for Windows, WinPatrol, Mirekrosoft Install Monitor, PA File Sight, DriverView, Driver Reviver, and DNSQuerySniffer to perform dynamic analysis of malware behavior and system interactions.
4. **Enumeration Techniques:**
  - **NetBIOS Enumeration:** Using Windows command line tools and NetBIOS Enumerator.
  - **SNMP Enumeration:** Utilizing tools like snmp-check, SoftPerfect Network Scanner, and snmpwalk.
  - **LDAP Enumeration:** Using Active Directory Explorer, Python (ldap3), and Nmap for LDAP exploration.

- **NFS Enumeration:** Conducting scans using RPCScan and SuperEnum.
- **DNS Enumeration:** Performing DNS zone transfers, DNSSEC zone walking, and service discovery with tools like dig, dnsrecon, and Nmap.
- **SMTP Enumeration:** Listing mail users and open SMTP relays with Nmap.
- **General Enumeration Tools:** Employing Global Network Inventory, Advanced IP Scanner, and Enum4linux for comprehensive network resource enumeration.

## Tools Utilized

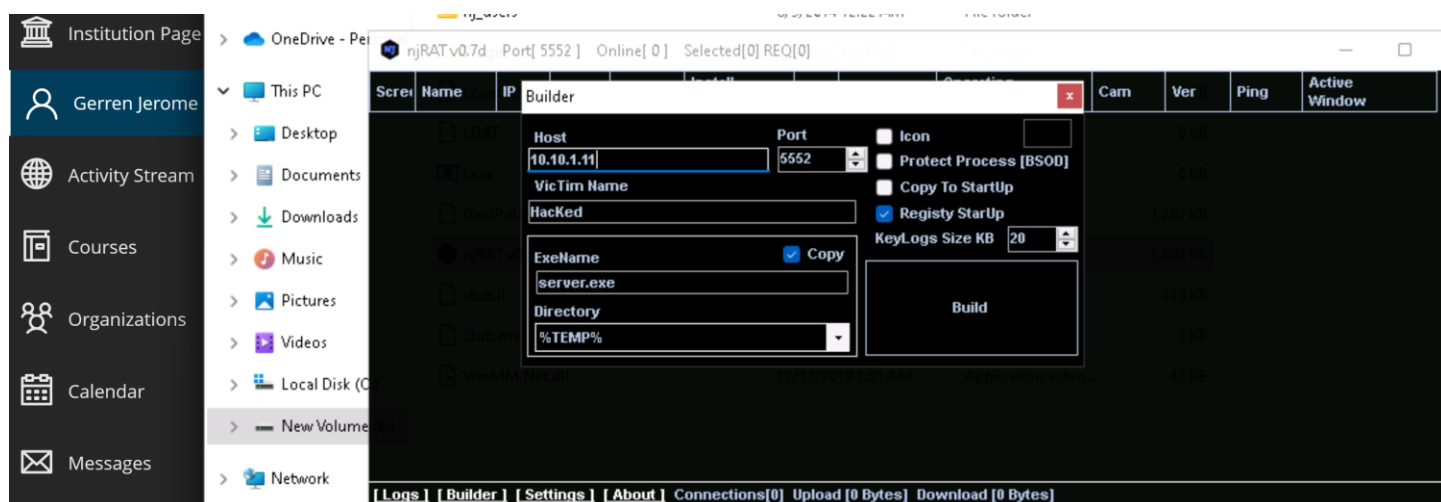
Throughout this project, I utilized several key tools to perform malware analysis and enumeration tasks, including:

- **njRAT and Theef RAT:** For creating and exploiting Trojans.
- **JPS Virus Maker Tool:** For creating viruses.
- Hybrid Analysis, BinText, PeID, DIE, PE Explorer, Dependency Walker, IDA, OllyDbg, Ghidra: For static malware analysis.
- TCPView, CurrPorts, Process Monitor, Reg Organizer, Windows Service Manager, Autoruns, WinPatrol, Mirekrosoft Install Monitor, PA File Sight, DriverView, Driver Reviver, DNSQuerySniffer: For dynamic malware analysis.
- NetBIOS Enumerator, snmp-check, SoftPerfect Network Scanner, snmpwalk, Active Directory Explorer, Nmap, RPCScan, SuperEnum, dig, dnsrecon, Global Network Inventory, Advanced IP Scanner, Enum4linux: For enumeration tasks.

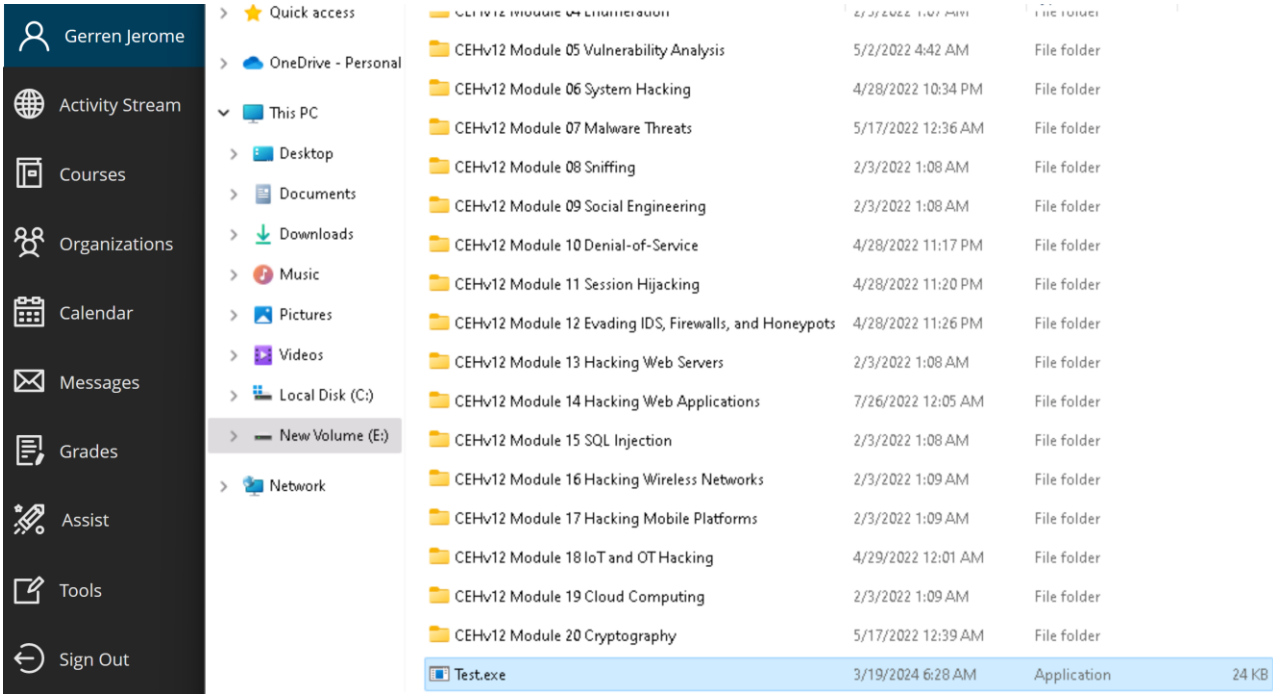
## Gain access to the target system using Trojans.

*Gain control over a victim machine using the njRAT RAT Trojan*

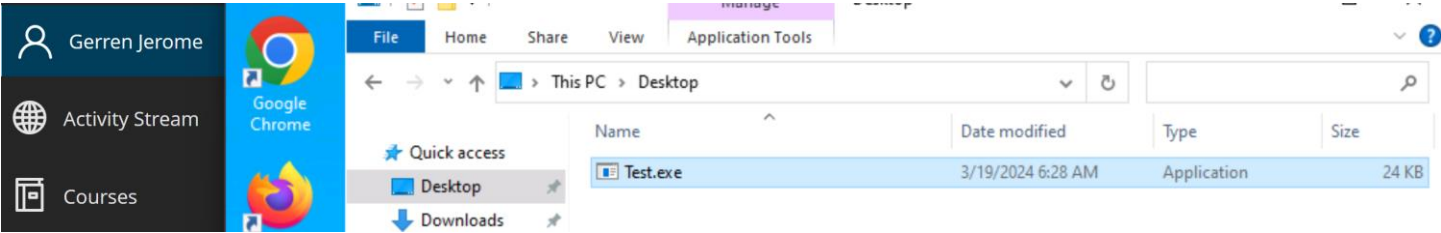
**Confirm install with port (5552) and listener host (WIN\_11; 10.10.1.11)**



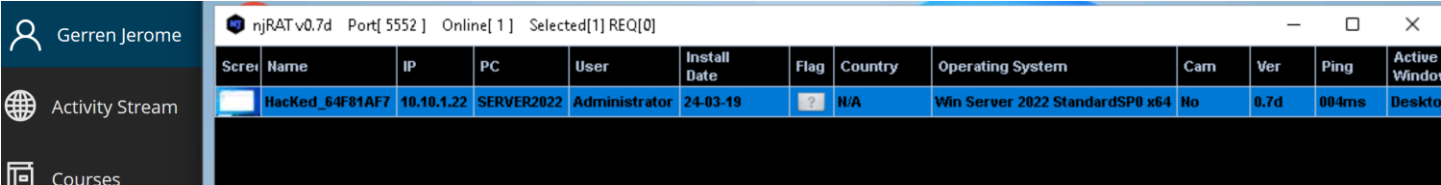
Confirm creation and upload of Test.exe to share folder.



Launch Test.exe on WIN\_SVR\_22



Confirm control session between WIN\_11 and WIN\_SVR\_22



Show Process Manager in njRAT control panel.

The screenshot shows the njRAT control panel interface. On the left is a sidebar with navigation options: Gerren Jerome (user profile), Activity Stream, Courses, Organizations, Calendar, and Messages. The main window title is "[HackEd\_64F81AF7/Administrator/Win Server 2022 StandardSP0 x64]". The top toolbar includes File Manager, Process Manager (highlighted), Connections, Registry, and Remote Shell. Below the toolbar is a "Services" section with a table of running processes.

Name	PID	Directory
AggregatorHost.exe	4428	System32
armsvc.exe	2940	1.0
csrss.exe	504	
csrss.exe	576	
ctfmon.exe	1952	system32
dfsr.exe	3096	system32
dfsrmc.exe	3600	system32
dns.exe	3140	system32
dwm.exe	992	system32
explorer.exe	4592	Windows
fontdrvhost.exe	5064	system32
fontdrvhost.exe	5068	system32

Show network connections.

The screenshot shows the njRAT control panel with the "Connections" tab selected. The main window title is "[HackEd\_64F81AF7/Administrator/Win Server 2022 StandardSP0 x64]". The top toolbar includes File Manager, Process Manager, Connections (highlighted), Registry, and Remote Shell. Below the toolbar is a "Services" section with a table of network connections.

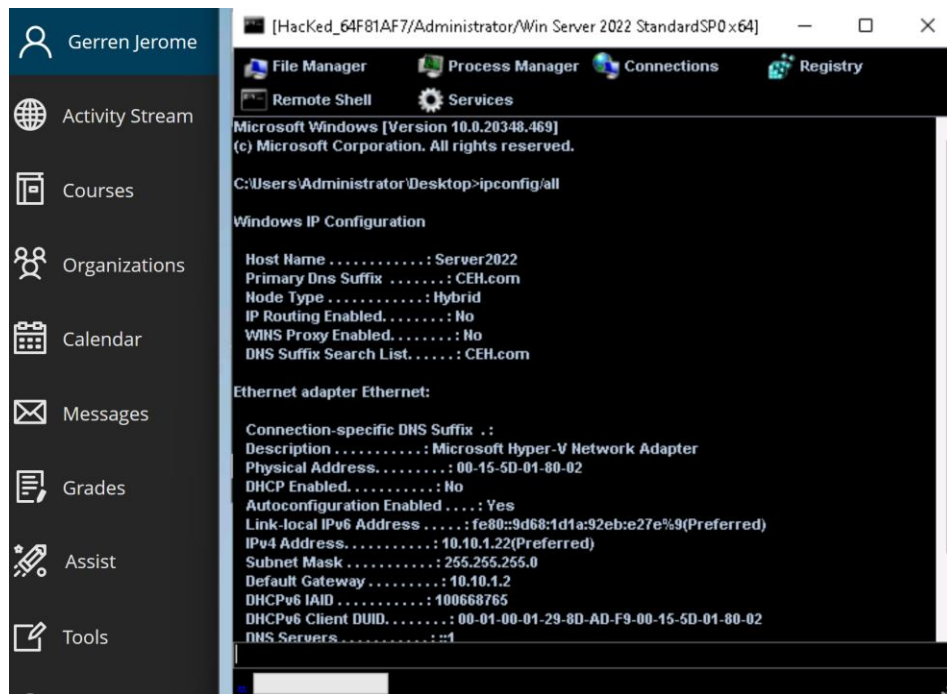
LocalIP	LocalPort	RemoteIP	RemotePort	State	Process
0.0.0.0	80	0.0.0.0	0	Listen	System[4]
0.0.0.0	88	0.0.0.0	0	Listen	lsass[724]
0.0.0.0	135	0.0.0.0	0	Listen	svchost[980]
0.0.0.0	389	0.0.0.0	0	Listen	lsass[724]
0.0.0.0	445	0.0.0.0	0	Listen	System[4]
0.0.0.0	464	0.0.0.0	0	Listen	lsass[724]
0.0.0.0	593	0.0.0.0	0	Listen	svchost[980]
0.0.0.0	636	0.0.0.0	0	Listen	lsass[724]
0.0.0.0	1801	0.0.0.0	0	Listen	mqsvc[3424]
0.0.0.0	2103	0.0.0.0	0	Listen	mqsvc[3424]
0.0.0.0	2105	0.0.0.0	0	Listen	mqsvc[3424]
0.0.0.0	2107	0.0.0.0	0	Listen	mqsvc[3424]
0.0.0.0	3268	0.0.0.0	0	Listen	lsass[724]

Show registry.

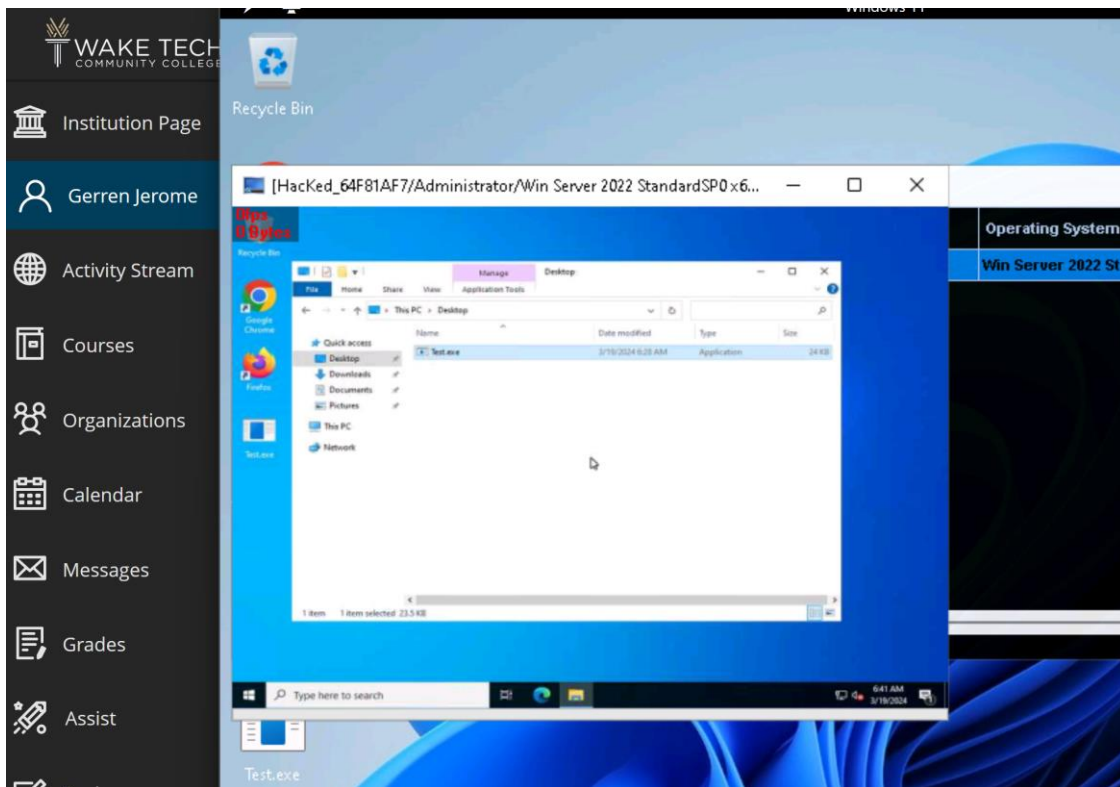
The screenshot shows the njRAT control panel with the "Registry" tab selected. The main window title is "[HackEd\_64F81AF7/Administrator/Win Server 2022 StandardSP0 x64]". The top toolbar includes File Manager, Process Manager, Connections, Registry (highlighted), and Remote Shell. Below the toolbar is a "Services" section with a tree view of the registry.

Name	Type	Value
HKEY_CLASSES_ROOT		
HKEY_CURRENT_USER		
HKEY_LOCAL_MACHINE		
HKEY_USERS		

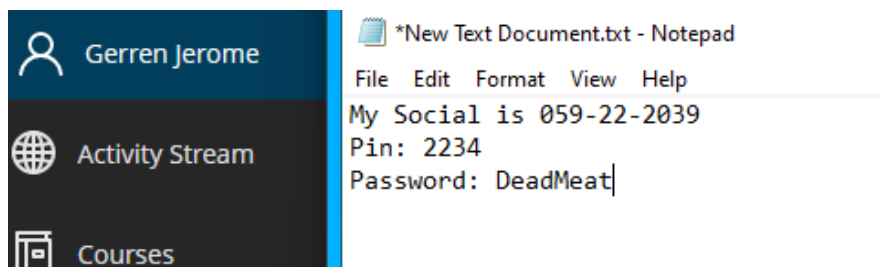
Show remote shell, confirm connection using ipconfig.



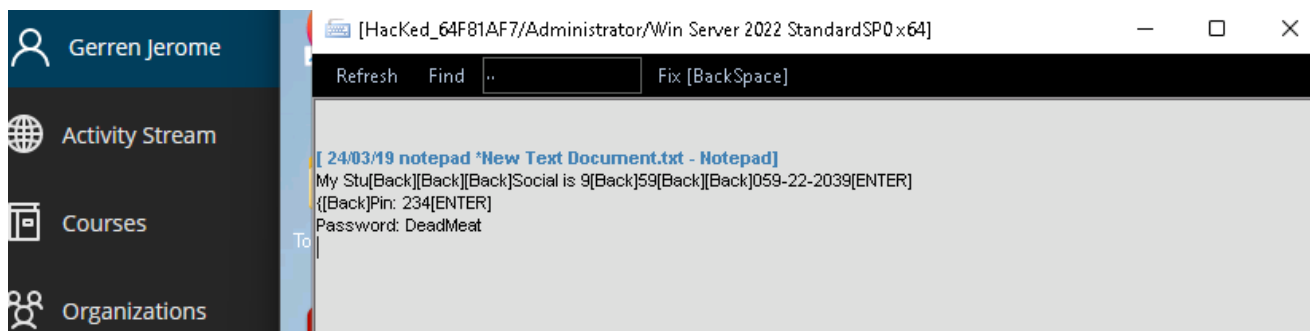
Show remote desktop.



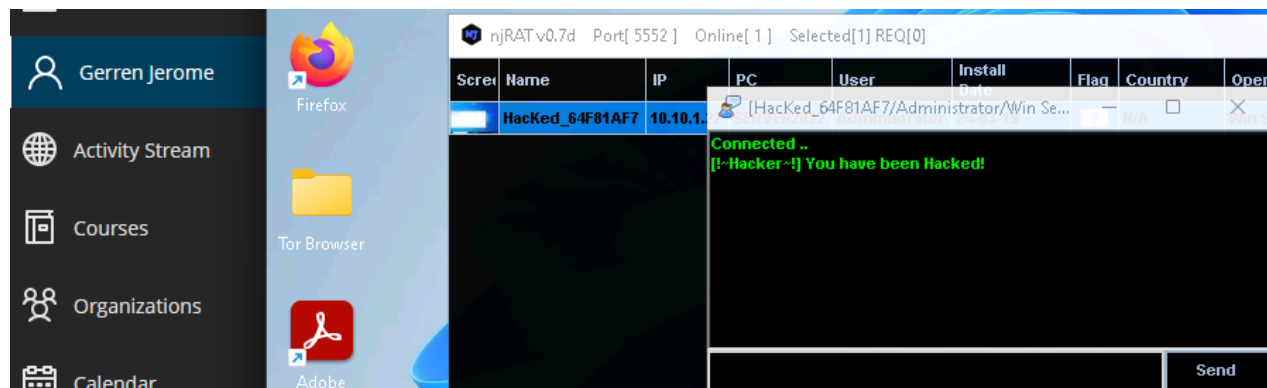
Create dummy text/actions on victim (WIN\_SVR\_22) machine.



Confirm surveillance on WIN\_11 machine in njRAT.



Send chat message (WIN\_11)



Display chat message (WIN\_SVR\_22)



Show automatic recapture of connection with victim.

Gerren Jerome

Activity Stream

Courses

njRAT v0.7d Port[ 5552 ] Online[ 0 ] Selected[0] REQ[0]												
Screen	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window

Gerren Jerome

Activity Stream

njRAT v0.7d Port[ 5552 ] Online[ 1 ] Selected[1] REQ[0]												
Screen	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Ping	Active Window
	HackEd_64F81AF7	10.10.1.22	SERVER2022	Administrator	24-03-19		N/A	Win Server 2022 StandardSP0 x64	No	0.7d	00	

Hide a Trojan using SwayzCryptor and make it undetectable to various anti-virus programs

Results of VirusTotal scan for Test.exe

Institution Page

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

62 / 73

Community Score

62/73 security vendors and no sandboxes flagged this file as malicious

Reanalyze

Similar

More

c81a1db3a5f87e5dddbb81ed6a5989d405ea19d1d2f60b50...

Size 23.50 KB

Last Modification Date a moment ago

EXE

peexe

assembly

DETECTION

DETAILS

BEHAVIOR

TELEMETRY

COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.bladabindi/msil

Threat categories

trojan

dropper

Family labels

bladabindi

msil

bldr

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)

Suspicious

AhnLab-V3

Win-Trojan/Zbot.24064

AliCloud

Backdoor:Win/Bladabindi.N(dyn)

ALYac

Generic.MSIL.Bladabindi.44EE7869

Confirm encryption options in SwayzCryptor

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

This PC

Desktop

Documents

Downloads

Music

Pictures

Videos

Local Disk (C:)

File

Icon

Bind

Extension

Obfuscate

Start up

Mutex

Disable UAC

Require Admin

SWAYZ CRYPTOR

Status: Idle

Encrypt

Minimize

Close



Upload CryptedFile.exe to VirusTotal and compare results

Institution Page

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

46 / 73

Community Score

46/73 security vendors and no sandboxes flagged this file as malicious

Reanalyze

Similar

More

cef4845cc0e43fe833c7ee247dd5ec0c359b6226df385d821...

Size

863.50 KB

Last Modification Date

a moment ago

EXE

CryptedFile.exe

peexe

DETECTION

DETAILS

RELATIONS

BEHAVIOR

TELEMETRY

COMMUNITY

Join the VT Community

and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.autoit.runner

Threat categories

trojan

dropper

Family labels

autoit

runner

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Dropper/Win32.RL_AutoIt.R281176	ALYac	AIT:Trojan.AutoIt.CGX
Arcabit	AIT:Trojan.AutoIt.CGX [many]	Avast	AutoItRunner-AN [Trj]

Upload CryptedFile to the CEH-Tools folder.

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Quick access

Desktop

OneDrive - Perso

This PC

Desktop

Documents

Downloads

Music

This PC > New Volume (E:) > CEH-Tools

Search CEH-Tools

Name	Date modified	Type	Size
CEHv12 Module 15 SQL Injection	2/3/2022 1:08 AM	File folder	
CEHv12 Module 16 Hacking Wireless Networks	2/3/2022 1:09 AM	File folder	
CEHv12 Module 17 Hacking Mobile Platforms	2/3/2022 1:09 AM	File folder	
CEHv12 Module 18 IoT and OT Hacking	4/29/2022 12:01 AM	File folder	
CEHv12 Module 19 Cloud Computing	2/3/2022 1:09 AM	File folder	
CEHv12 Module 20 Cryptography	5/17/2022 12:39 AM	File folder	
CryptedFile.exe	3/19/2024 8:23 AM	Application	864 KB
Test.exe	3/19/2024 8:01 AM	Application	24 KB

22 items | 1 item selected | 863 KB | State: Shared

Copy CryptedFile to Desktop of WIN\_SVR\_22 and run.

Gerren Jerome

Activity Stream

Courses

Organizations

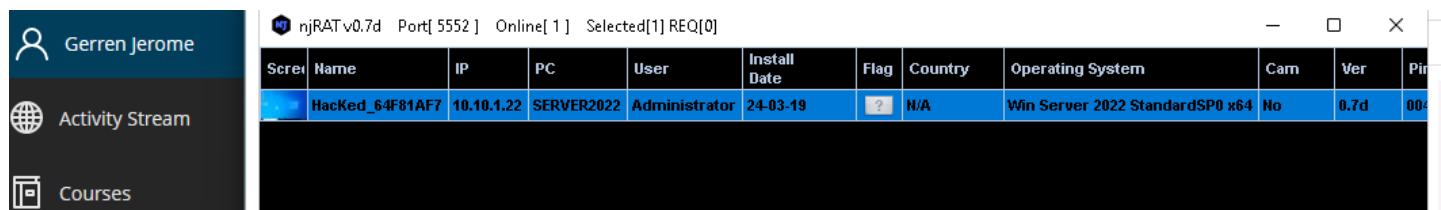
Firefox

Test.exe

CryptedFile.exe



Confirm session in njRAT between WIN\_SVR\_22 and WIN\_11

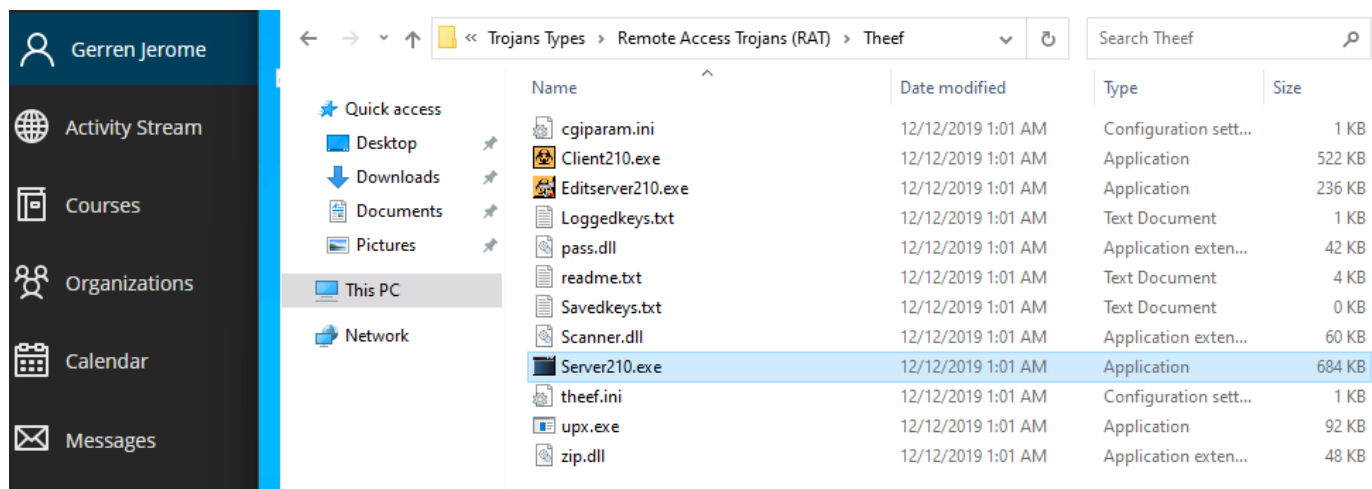


njRAT v0.7d Port[ 5552 ] Online[ 1 ] Selected[1] REQ[0]

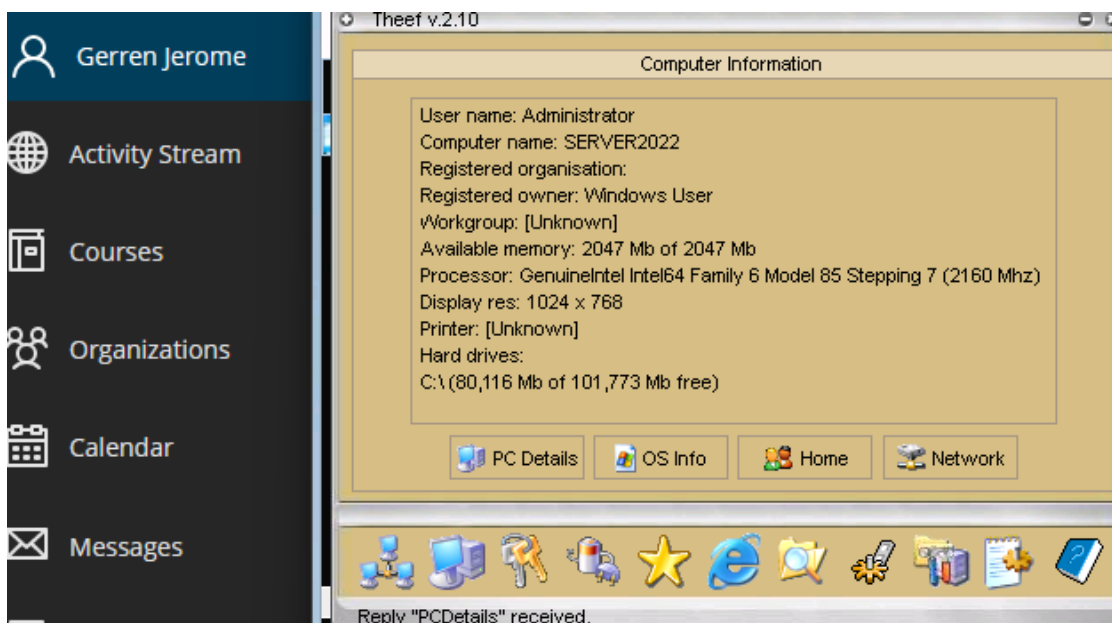
Screen	Name	IP	PC	User	Install Date	Flag	Country	Operating System	Cam	Ver	Pin
	HacKed_64F81AF7	10.10.1.22	SERVER2022	Administrator	24-03-19		N/A	Win Server 2022 StandardSP0 x64	No	0.7d	004

Create a Trojan server using Theef RAT Trojan

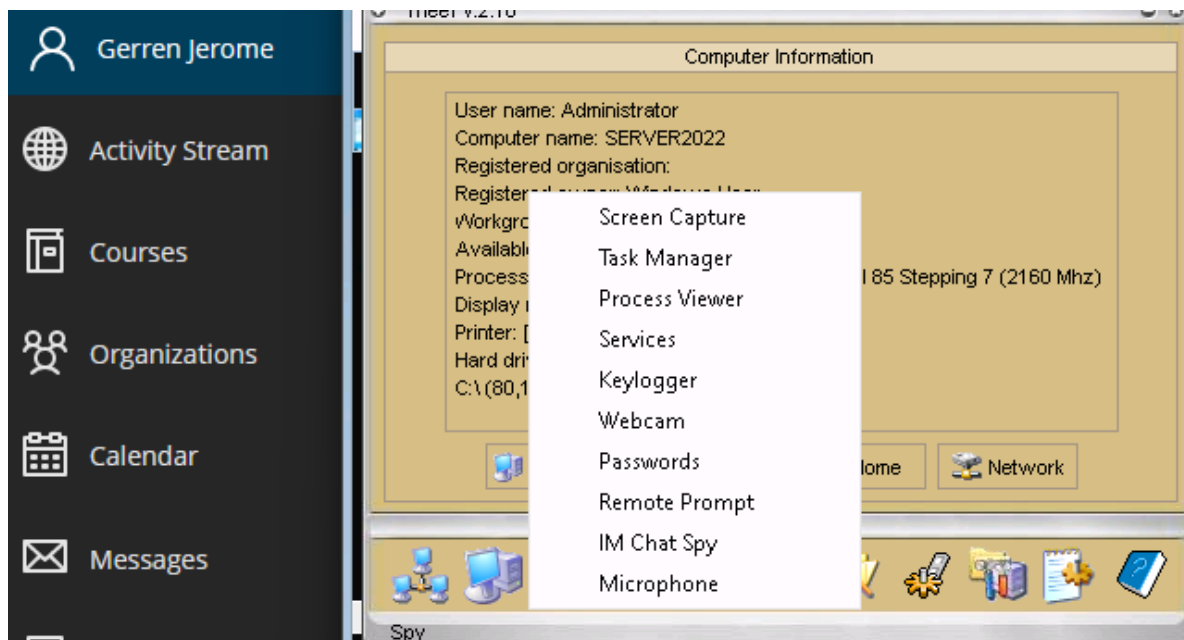
Run Server210 (Theef) on WIN\_SVR\_22



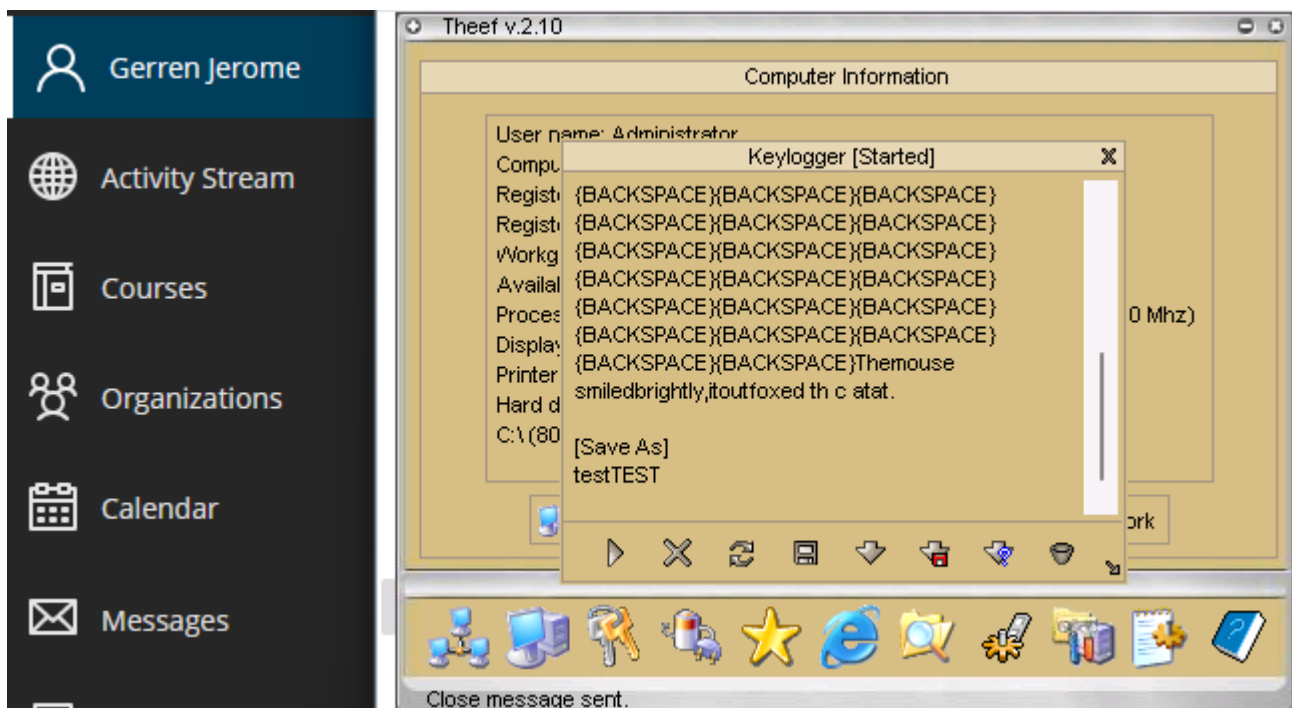
Run Client210 on WIN\_11 and view WIN\_SVR\_22's info in Theef's menu



Show results of Spy screen in Theef



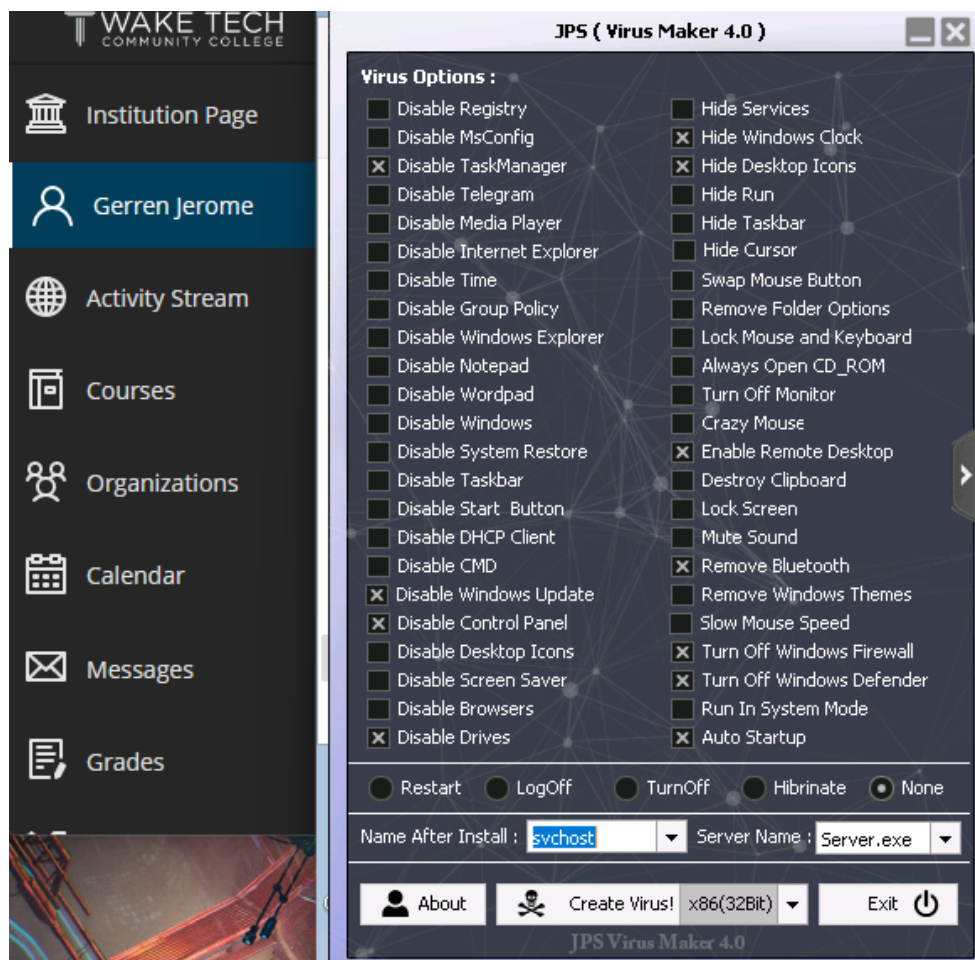
Launch keylogger in Theef, write some stuff on WIN\_SVR\_22, then confirm on WIN\_11



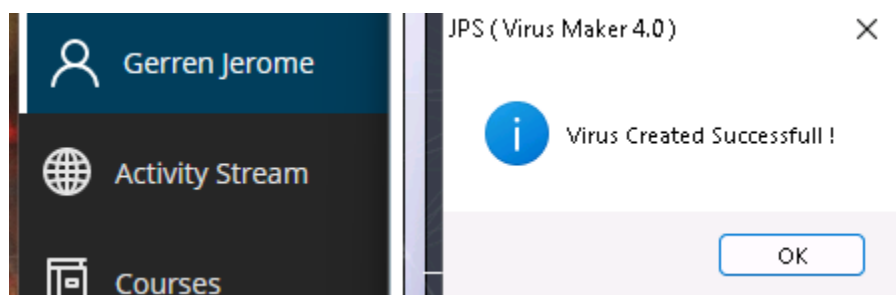
**Infect the target system using a virus.**

*Create a virus using the JPS Virus Maker Tool and infect the target system.*

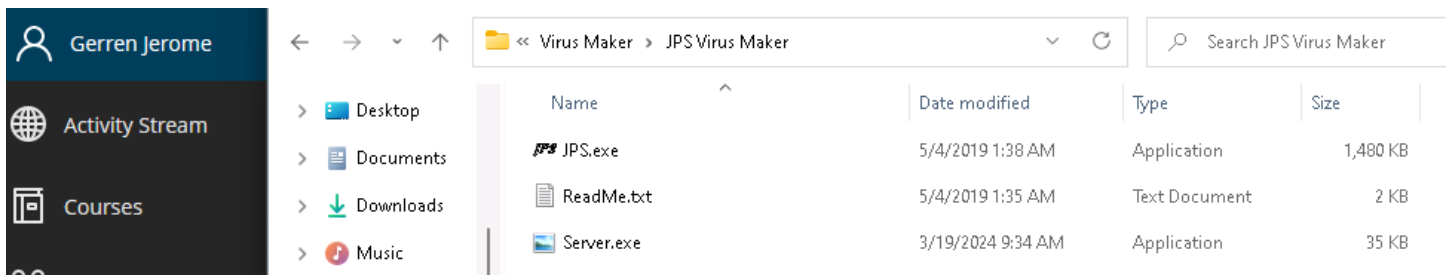
**Create and config virus, part 1 (Virus Options – Left hand menu)**



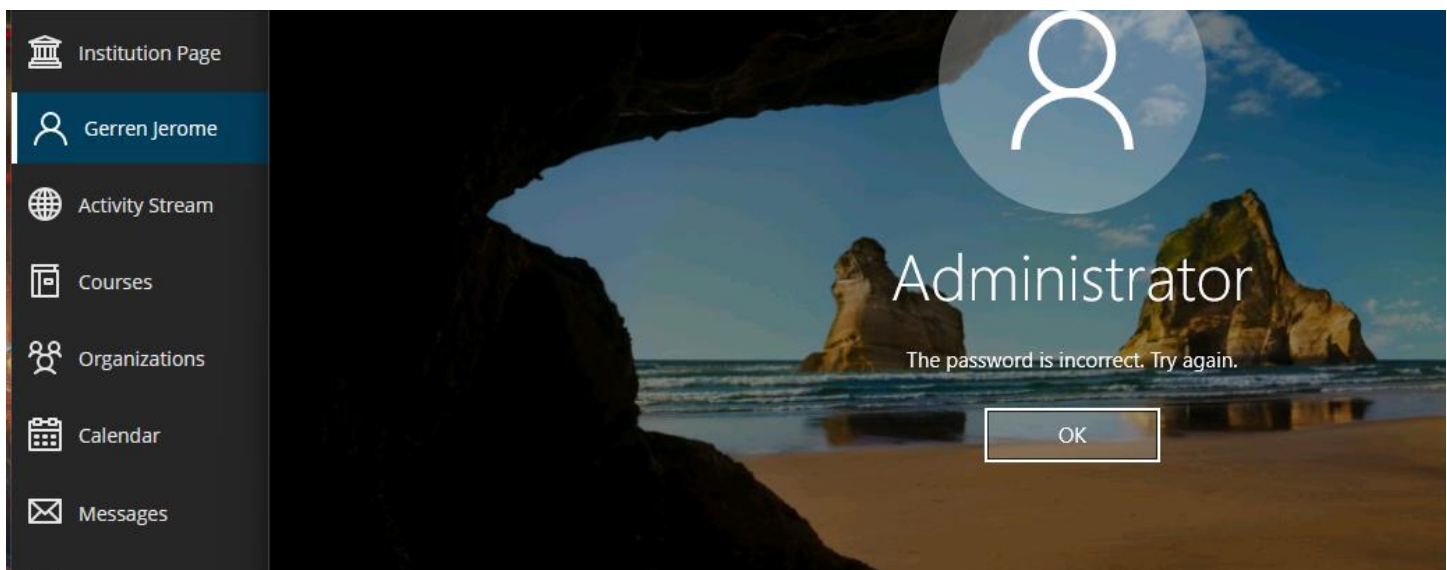
**Create and config virus, part 2 (Virus Options – Right hand menu)**



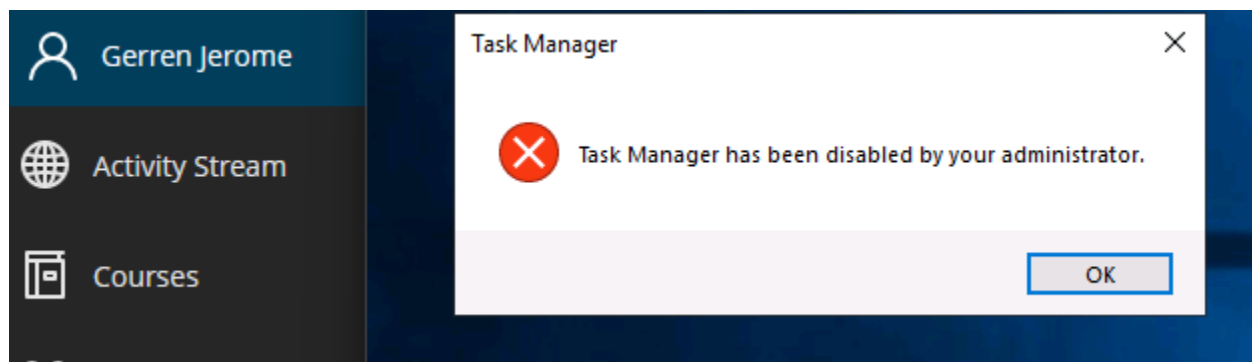
Confirm server.exe is in the JPS Virus Maker folder.



Launch server.exe on WIN\_SVR\_19, attempt to restart and login.



After using new password from Step 9, show Task Manager is disabled.



Perform static malware analysis

Perform malware scanning using Hybrid Analysis

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Anti-Virus Results

Up-to-date

Analysis Overview

Anti-Virus Scanner Results

Related Hashes

Falcon Sandbox Reports (13)

Incident Response

Community (1400)

Back to top

CrowdStrike Falcon

100%

Static Analysis and ML ...

Click here for more information about the product

Visit Vendor: [View](#)

GET STARTED WITH A FREE TRIAL

MetaDefender

95%

Multi Scan Analysis

Last Update: 03/20/2024 01:14:2

View Details: [View](#)

Visit Vendor: [View](#)

Information from Falcon Sandbox Reports

WAKE TECH  
COMMUNITY COLLEGE

Institution Page

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

HYBRID ANALYSIS

Request Info

Falcon Sandbox Reports

MALICIOUS

tini.exe

Analyzed on: 10/19/2020 ...

Environment: Android Sta...

Threat Score: 100/100

AV Detection: 90% Backd...

Indicators: 3 0

Network: (none)

MALICIOUS

tini.exe

Analyzed on: 11/05/2023 ...

Environment: Windows 1...

Threat Score: 100/100

AV Detection: 90% Backd...

Indicators: 3 10

Network: (none)

MALICIOUS

tini.exe

Analyzed on: 10/28/2022 ...

Environment: Windows 1...

Threat Score: 100/100

AV Detection: 86% Backd...

Indicators: 3 19

Network: (none)

MALICIOUS

tini.exe

Analyzed on: 01/11/2023 ...

MALICIOUS

tini.exe

Analyzed on: 01/07/2019 ...

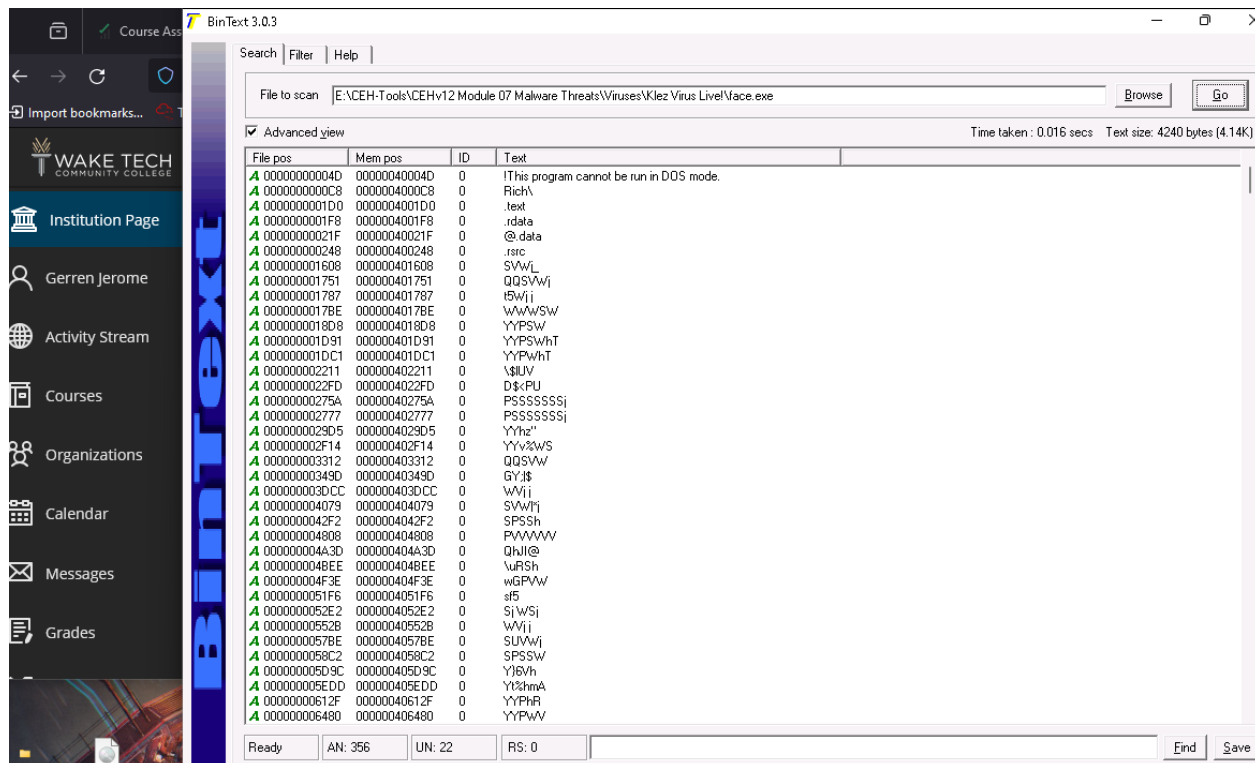
MALICIOUS

tini.exe

Analyzed on: 01/10/2019 ...

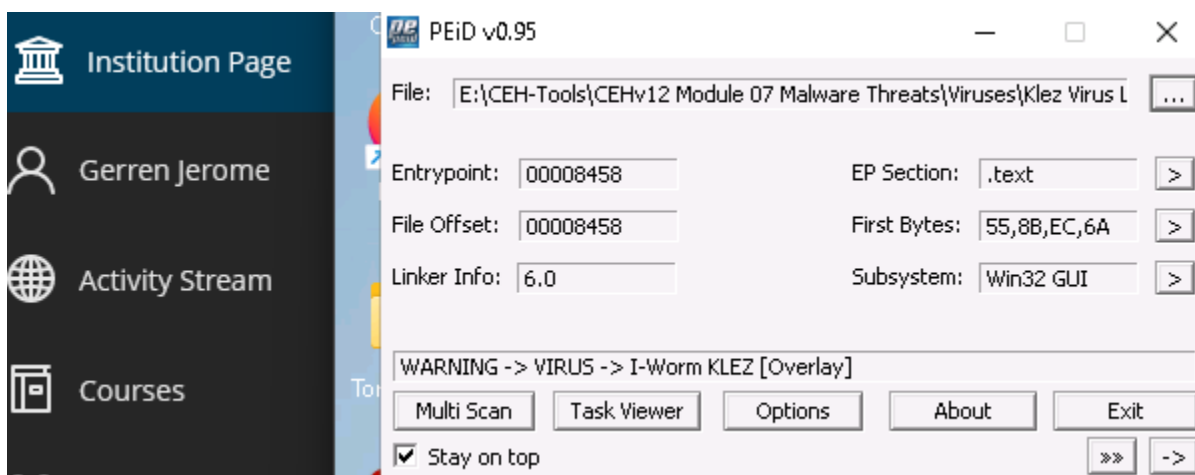
### Perform a strings search using BinText.

#### Extracted information from face.exe in BinText.




### Identify packaging and obfuscation methods using Peid


#### Analysis information from PeID of face.exe





## Analyze ELF executable file using Detect It Easy (DIE)


### File info of ELF test file


 Institution Page


 Gerren Jerome

 Activity Stream

 Courses

 Organizations

 Calendar

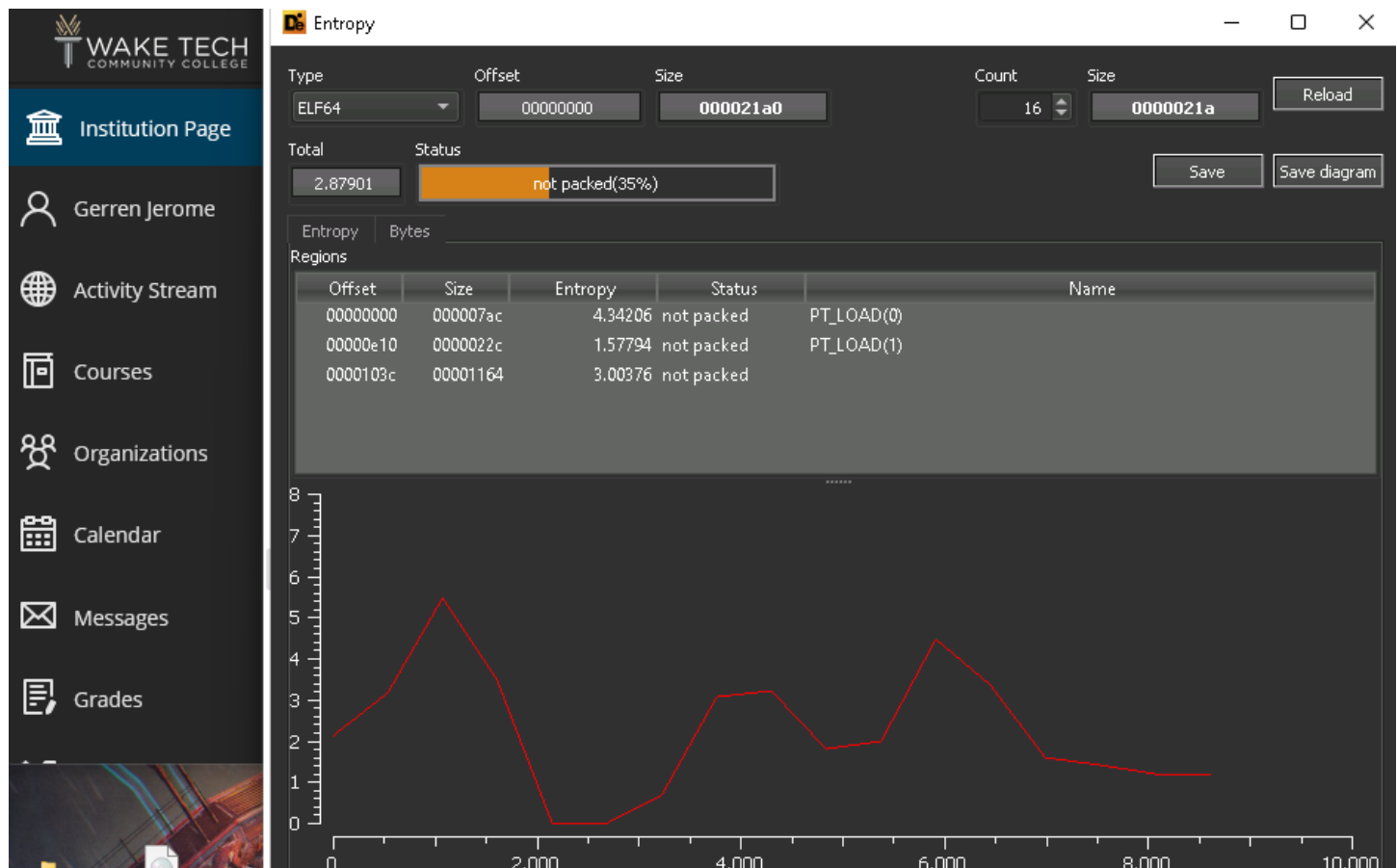
 Messages

Info

Type: ELF64 Offset: 00000000 Size: 000021a0

File name: E:/CEH-Tools/CEHv12 Module 07 Malware Threats/Viruses/ELF Test File  
Size: 8608 (8.41 kB)  
MD5: a7e54a8b83969be7d119c163f78d8c02  
SHA1: ad45d52edb4de4d4b7da11e9cc29bbb973fdebb0  
Entropy: 2.87901(not packed)  
Operation system: Red Hat Linux  
Architecture: AMD64  
Mode: 64-bit  
Type: EXEC  
Endianness: LE  
Entry point (Address): 00400490  
Entry point (Offset): 0490  
Entry point (Relative address): 0490  
Entry point (Bytes): 31ed4989d15e4889e24883e4f0505449c7c02006400048c7c1b005400048c7c77d054000  
Entry point (Signature): 31ed4989d15e4889e24883e4..505449c7c0.....48c7c1.....48c7c7.....  
Entry point (Signature) (Rel): 31ed4989d15e4889e24883e4..505449c7c0.....48c7c1.....48c7c7.....

### Entropy graph of ELF test file





Find the portable executable (PE) info of a malware executable file using PE Explorer

Scan result (Headers Info) for face.exe in PE Explorer

Institution Page

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

PE Explorer - E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live\face.exe

FileViewToolsHelp

HEADERS INFO

Address of Entry Point: 00408458Real Image Checksum: 0001723Bh

Field Name	Data Value	Description
Machine	014Ch	i386
Number of Sections	0004h	
Time Date Stamp	3CB78EB8h	13/04/2002 01:49:44
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	010Fh	
Magic	010Bh	PE32
Linker Version	0006h	6.0
Size of Code	0000C000h	
Size of Initialized Data	00089000h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	00408458h	
Base of Code	00001000h	

Field Name	Data Value	Description
Section Alignment	00001000h	
File Alignment	00001000h	
Operating System Version	00000004h	4.0
Image Version	00000000h	0.0
Subsystem Version	00000004h	4.0
Win32 Version Value	00000000h	Reserved
Size of Image	00096000h	614400 bytes
Size of Headers	00001000h	
Checksum	00000000h	
Subsystem	0002h	Win32 GUI
Dll Characteristics	0000h	
Size of Stack Reserve	00100000h	
Size of Stack Commit	00001000h	
Size of Heap Reserve	00100000h	

Scan result (Section Headers) for face.exe in PE Explorer

Institution Page

Gerren Jerome

Activity Stream

Courses

Organizations

Calendar

Messages

Grades

Assist

PE Explorer - E:\CEH-Tools\CEHv12 Module 07 Malware Threats\Viruses\Klez Virus Live\face.exe

FileViewToolsHelp

SECTION HEADERS

00001000

Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics	Pointing Directories
<input checked="" type="checkbox"/> .text	0000BA4Ah	00401000h	0000C000h	00001000h	60000020h	
<input checked="" type="checkbox"/> .idata	00001022h	0040D000h	00002000h	0000D000h	40000040h	Import Table; Import Address Table
<input checked="" type="checkbox"/> .data	00085E6Ch	0040F000h	00005000h	0000F000h	C0000040h	
<input checked="" type="checkbox"/> .rsrc	00000010h	00495000h	00000010h	00014000h	40000040h	Resource Table

	Size of Raw Data	Pointer to Raw Data
<input checked="" type="checkbox"/> EOF Extra Data	00002800h	00014010h

Legend:

● - Section is pointed to by header (Can't be deleted).

● - Section is pointed to by Data Directories (May be deleted).

● - Section has no reference (May be deleted).

19.03.2024 18:31:13 : EOF Extra Data From: 00014010h (81936)

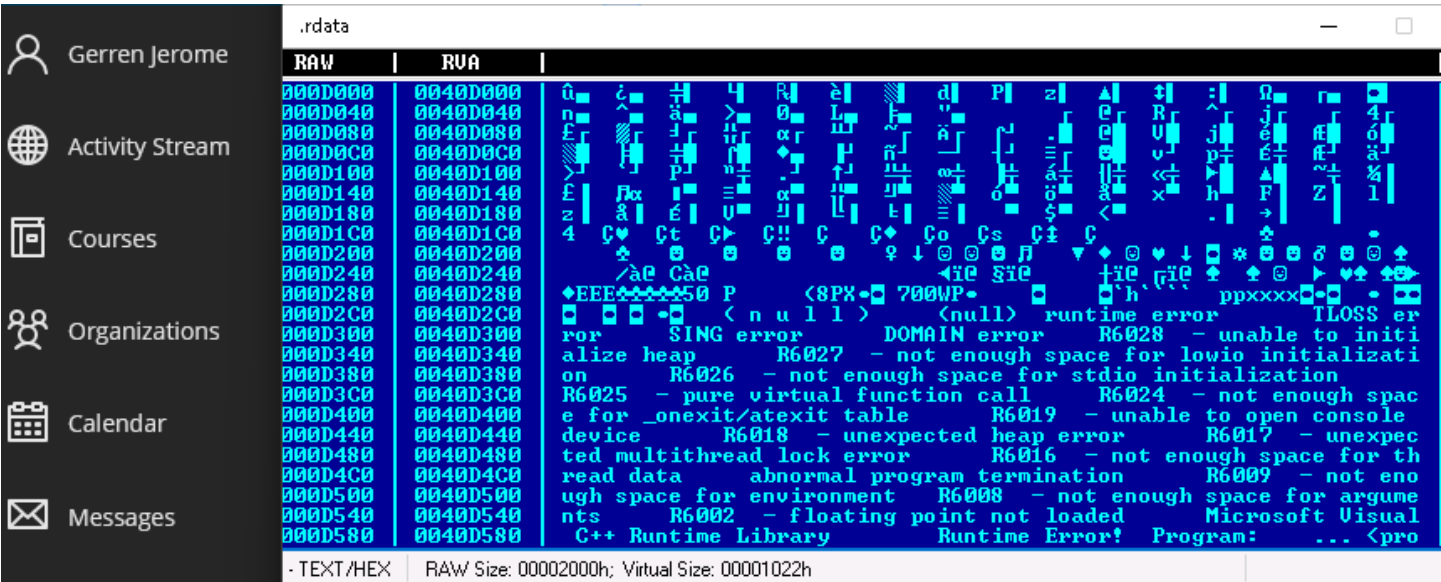
19.03.2024 18:31:13 : Length of EOF Extra Data: 00002800h (10240) bytes.

19.03.2024 18:31:13 : EOF Position: 00016810h (92176)

19.03.2024 18:31:13 : Precompiling Resources...

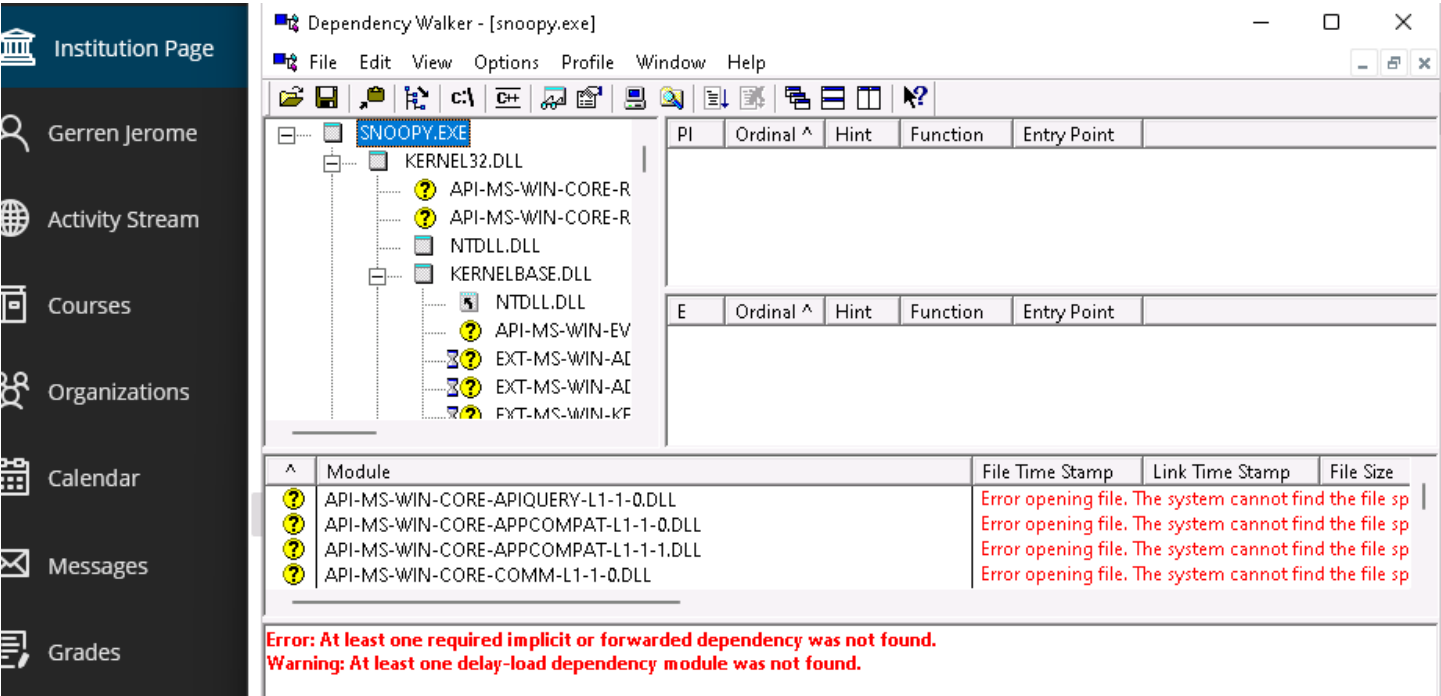
19.03.2024 18:31:13 : Done.

Hex viewer before closing.



Identify file dependencies using Dependency Walker

Confirm import (Snoopy.exe) in DW



## Display DLL details in DW for KERNEL32.dll

The screenshot shows the Dependency Walker (snoopy.exe) window. The left pane shows the tree view with SNOOPY.EXE expanded, showing its dependencies: ADVAPI32.DLL, WS2\_32.DLL, and MPR.DLL. The right pane shows the details for KERNEL32.DLL, including a table of functions and their entry points.

PI	Ordinal ^	Hint	Function	Entry Point
N/A	27 (0x001B)		CloseHandle	Not Bound
N/A	40 (0x0028)		CopyFileA	Not Bound
N/A	52 (0x0034)		CreateFileA	Not Bound
N/A	53 (0x0035)		CreateFileMappingA	Not Bound
N/A	68 (0x0044)		CreateProcessA	Not Bound
N/A	74 (0x004A)		CreateThread	Not Bound
N/A	76 (0x004C)		CreateToolhelp32Snapshot	Not Bound
N/A	87 (0x0057)		DeleteFileA	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
1 (0x0001)	70 (0x0046)		BaseThreadInitThunk	0x00016720
2 (0x0002)	901 (0x0385)		InterlockedPushListSList	NTDLL.RtlInterlockedPushListSList
3 (0x0003)	1569 (0x0621)		Wow64Transition	0x0008209C
4 (0x0004)	0 (0x0000)		AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
5 (0x0005)	1 (0x0001)		AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
6 (0x0006)	2 (0x0002)		ActivateActCtx	0x00021AC0
7 (0x0007)	3 (0x0003)		ActivateActCtxWorker	0x00016E50

Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum
API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. The system cannot find the file specified (2).					
API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. The system cannot find the file specified (2).					
API-MS-WIN-CORE-CONSOLE-L1-2-1.DLL	Error opening file. The system cannot find the file specified (2).					
API-MS-WIN-CORE-CONSOLE-L1-2-2.DLL	Error opening file. The system cannot find the file specified (2).					

Error: At least one required implicit or forwarded dependency was not found.  
Warning: At least one delay-load dependency module was not found.

## Perform malware disassembly using IDA and OllyDbg

## Results of analysis (face.exe) in IDA

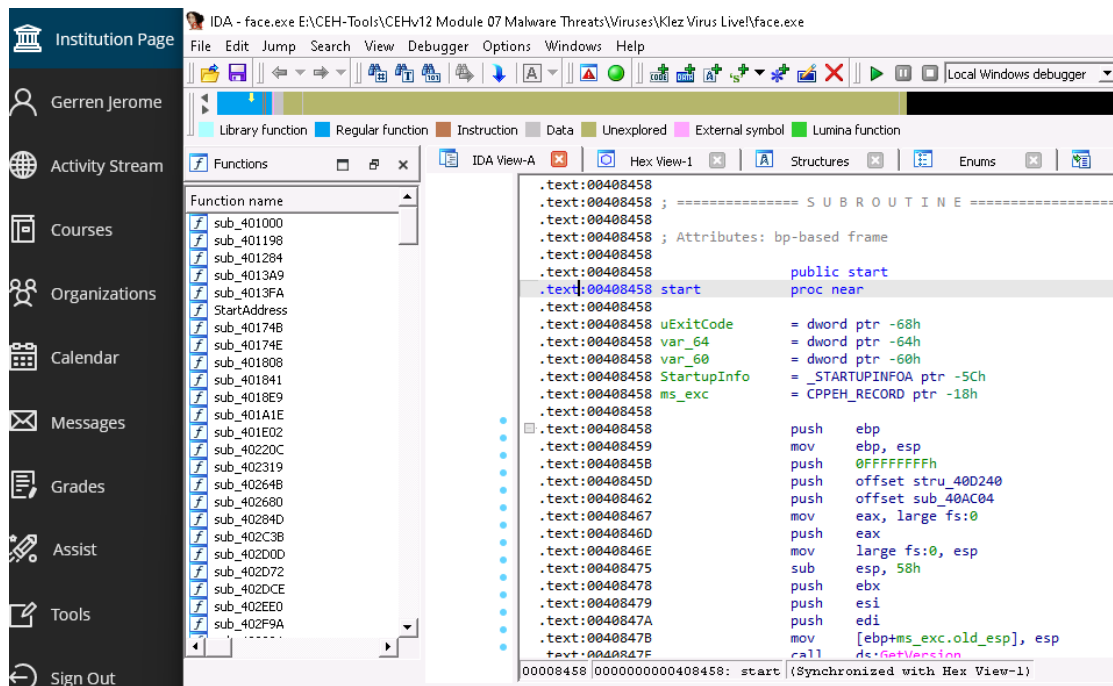
The screenshot shows the IDA Pro interface with the file E:\CEH-Tools\CEHV12 Module 07 Malware Threats\Viruses\Klez Virus Live\face.exe loaded. The Functions list on the left shows various functions, including sub\_401000, sub\_401198, sub\_401284, sub\_4013A9, sub\_4013FA, StartAddress, sub\_401748, sub\_40174E, sub\_401808, sub\_401841, sub\_4018E9, sub\_401A1E, sub\_401E02, sub\_40220C, and sub\_402319. The main window shows the disassembly of the function sub\_402319, which is a public start function. The disassembly code is as follows:

```
loc_408543:
; Attributes: bp-based frame
mov     esp, [ebp+ms_exc.old_esp]
push    [ebp+uExitCode]; uExitCode
call    sub_40A24A
start endp ; sp-analysis failed

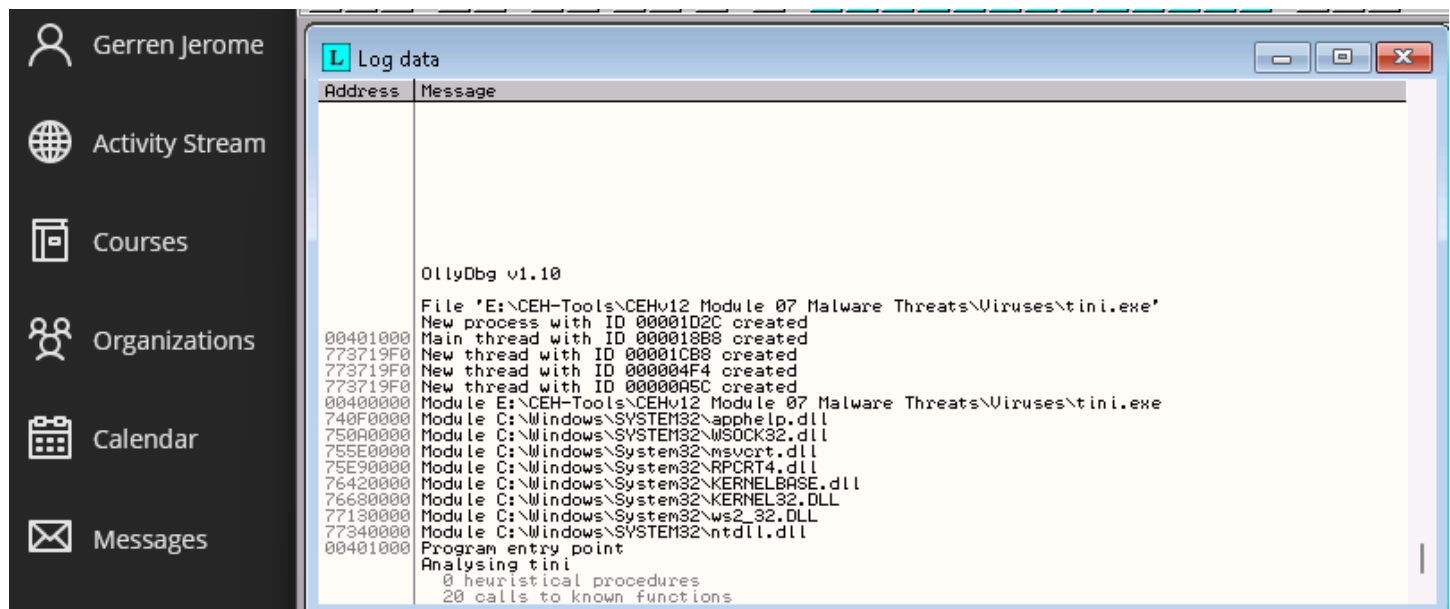
uExitCode= dword ptr -68h
var_64= dword ptr -64h
var_60= dword ptr -60h
StartupInfo= _STARTUPINFOA ptr -5Ch
ms_exc= CPPEH_RECORD ptr -18h

push    ebp
mov     ebp, esp
push    0FFFFFFFh
push    offset stru_40D240
push    offset sub_40AC04
mov     eax, large fs:0
push    eax
mov     large fs:0, esp
sub     esp, 58h
push    ebx
push    esi
push    edi
mov     [ebp+ms_exc.old_esp], esp
call    ds:GetVersion
```

### Text view of face.exe in IDA

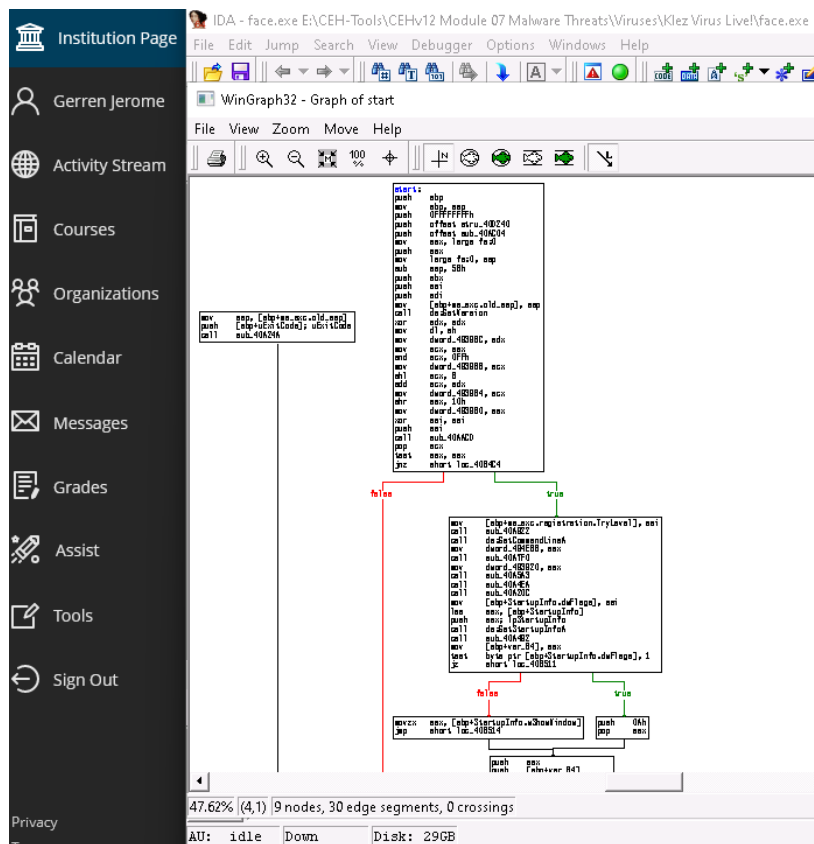


### view log data of tini.exe in OllyDBG

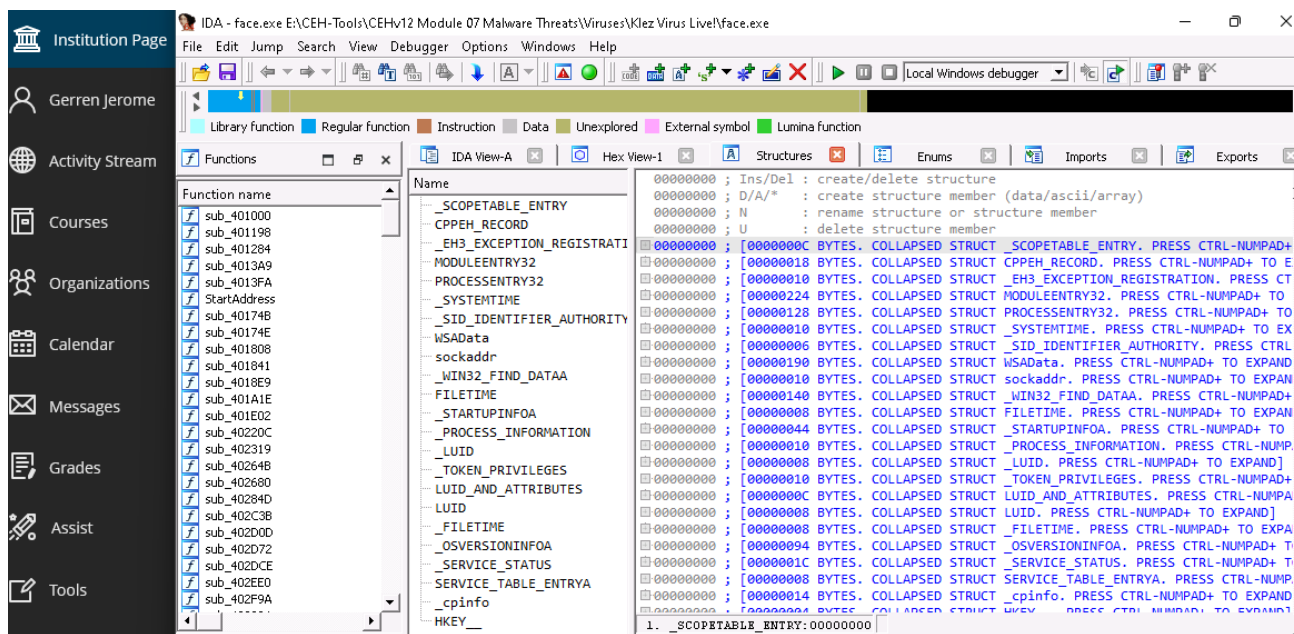


Memory map									
Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as	
00010000	00011000				Map	R	R	\Device\Harddisk0\...	
00030000	00010000				Map	RW	RW		
00040000	0001F000				Map	R	R		
00095000	0000B000				Priv	RW GUA	RW		
0019B000	00002000				Priv	RW GUA	RW	stack of ma	
0019D000	00003000				Priv	RW GUA	RW		
001A0000	00004000				Map	R	R		
001B0000	00002000				Priv	RW	RW		
001C0000	00011000				Map	R	R	\Device\Harddisk0\...	
001E0000	00011000				Map	R	R		
00243000	00004000				Priv	RW	RW		
00247000	00004000				Priv	RW	RW		
0024B000	00004000			data block	Priv	RW	RW	\Device\Harddisk0\...	
0024F000	00004000			data block	Priv	RW	RW		
00253000	00004000			data block	Priv	RW	RW		
00257000	00004000			data block	Priv	RW	RW		
00400000	00001000	tini		PE header	Imag	R	RWE	\Device\Harddisk0\...	
00401000	00001000	tini	.text	code	Imag	R	RWE		
00402000	00001000	tini	.rdata	imports	Imag	R	RWE		
00403000	0000D000	tini	.data	data	Imag	R	RWE		
00410000	00003000				Map	R	R	\Device\Harddisk0\...	
00420000	00011000				Map	R	R		
00440000	00003000				Map	R	R		
00450000	00003000				Map	R	R		
00460000	000CE000				Map	R	R	\Device\Harddisk0\...	
00530000	00011000				Map	R	R		
00550000	00011000				Map	R	R		
005A5000	0000B000				Priv	RW GUA	RW		
005B0000	0000B000				Priv	RW	RW	\Device\Harddisk0\...	
005F5000	0000B000				Priv	RW GUA	RW		
00635000	0000B000				Priv	RW GUA	RW		
00670000	0001A000				Priv	RW	RW		

Graph view in IDA.

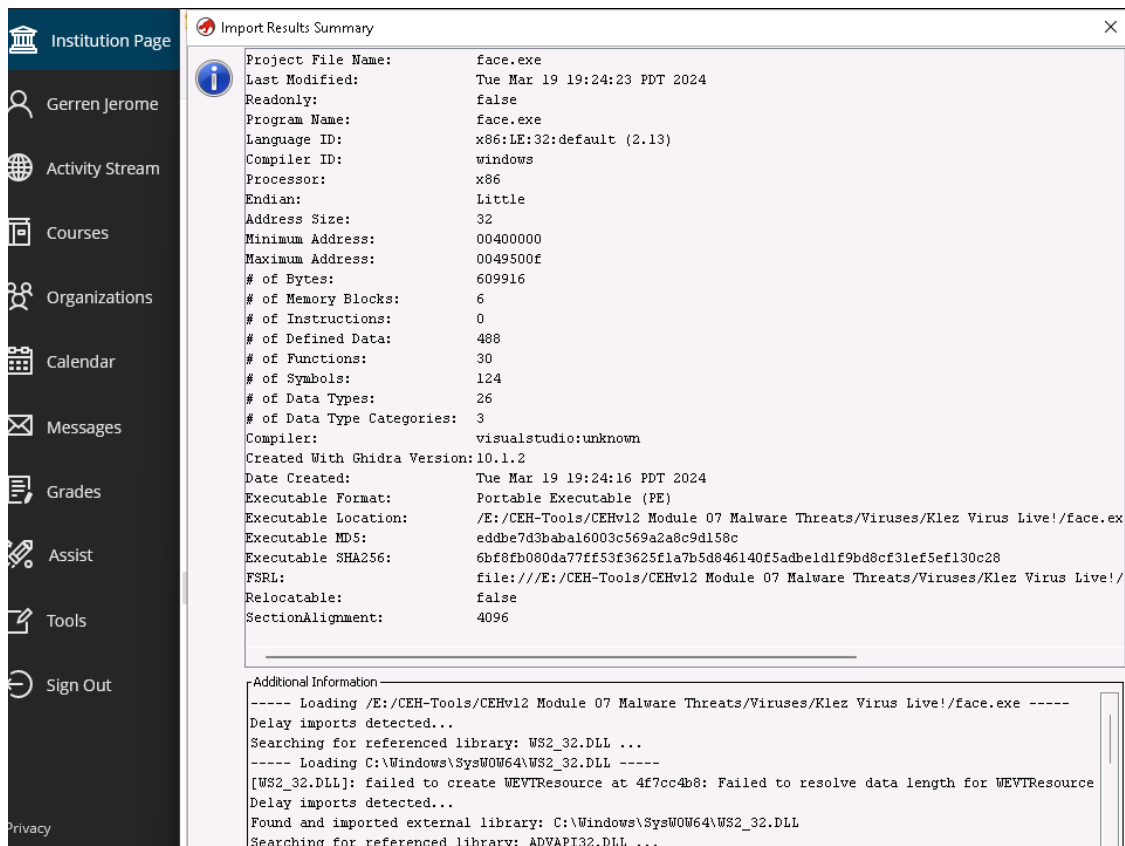


## Structures view in IDA

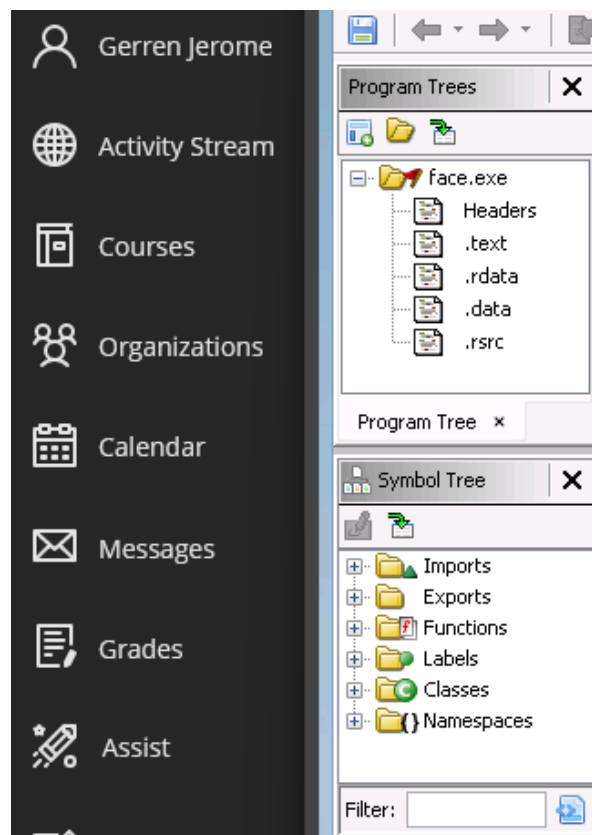


## Perform malware disassembly using Ghidra.

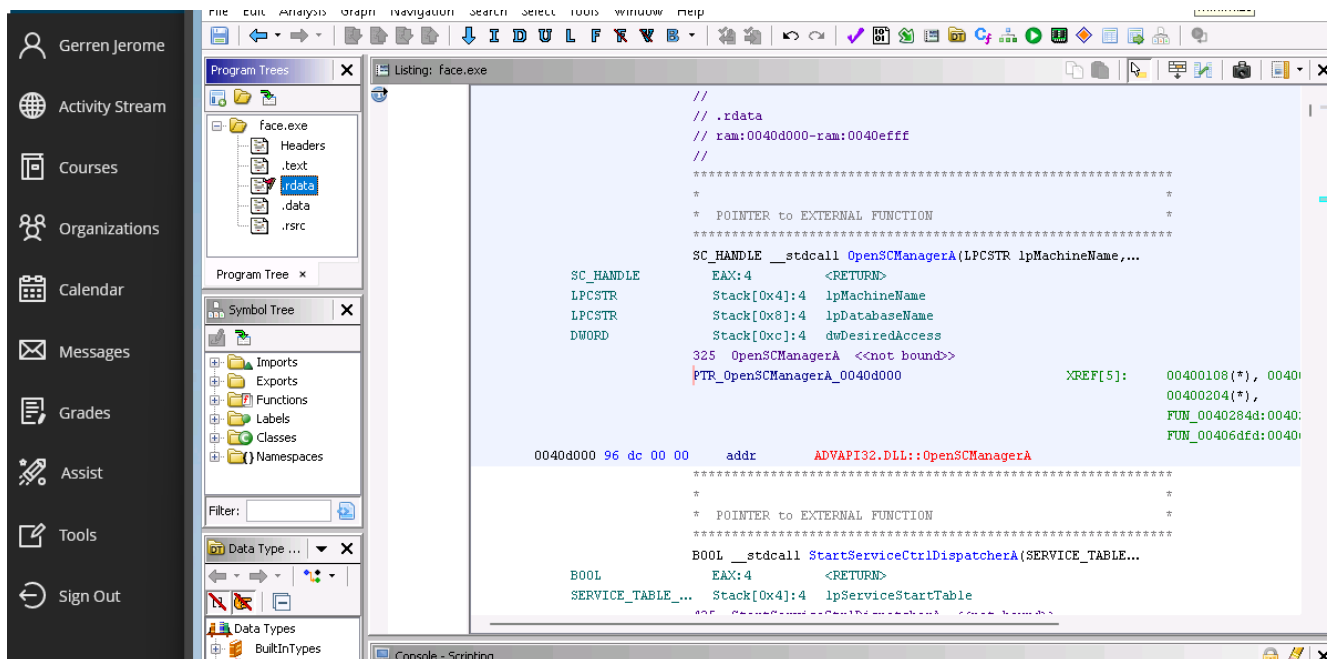
### Import Results Summary window in Ghidra.



## Symbol tree for face.exe in Ghidra



## .rdata node for face.exe in Ghidra

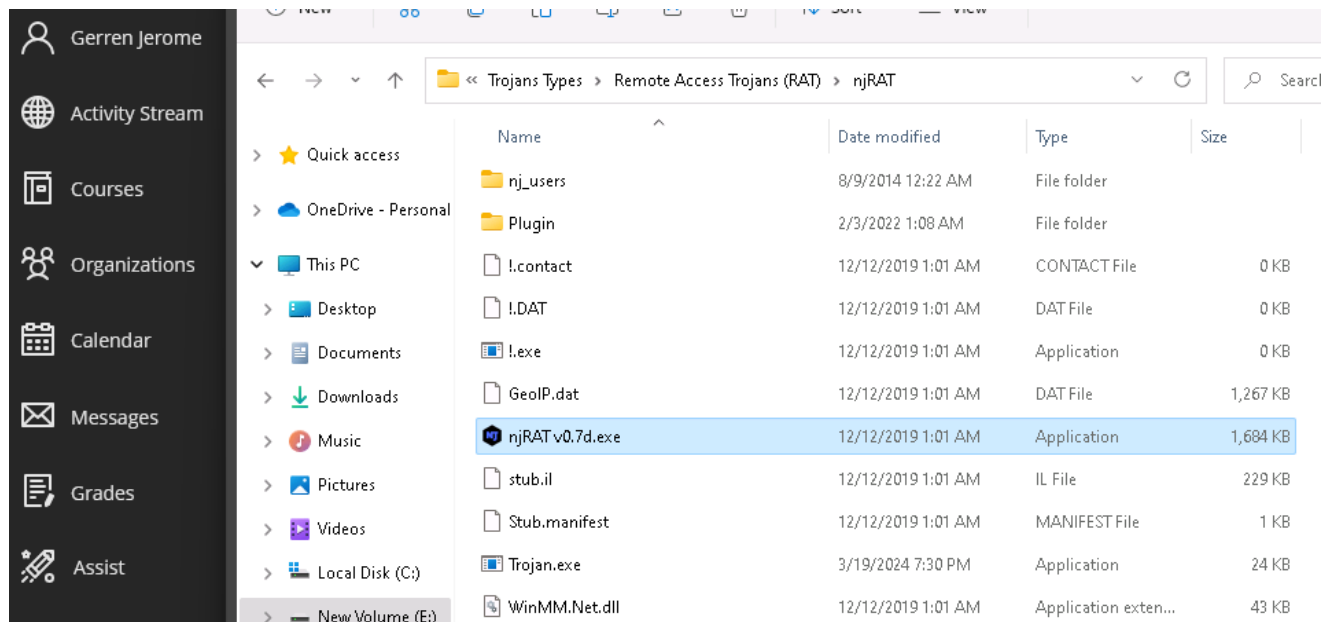




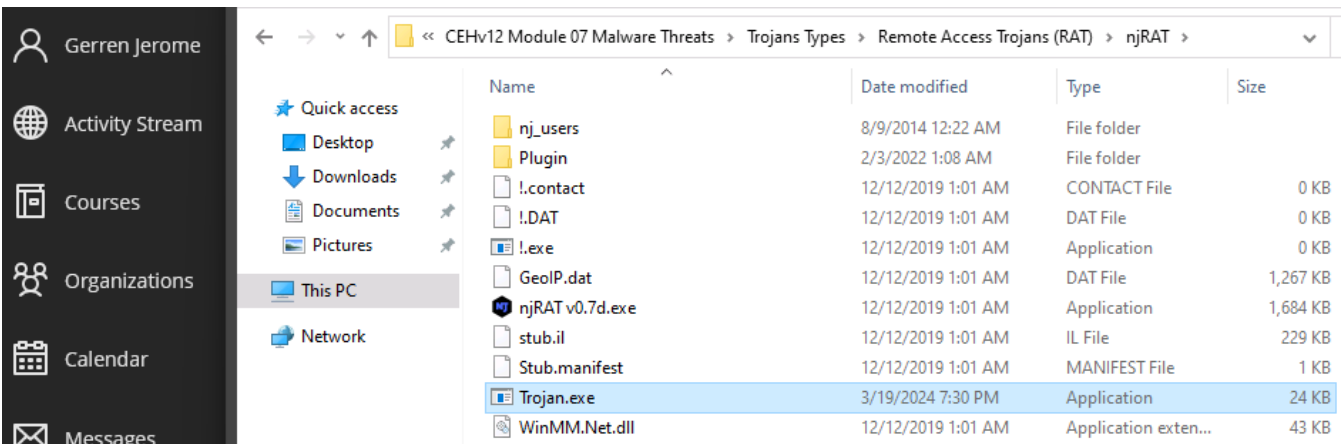
Perform dynamic malware analysis.

Perform port monitoring using TCPView and CurrPorts

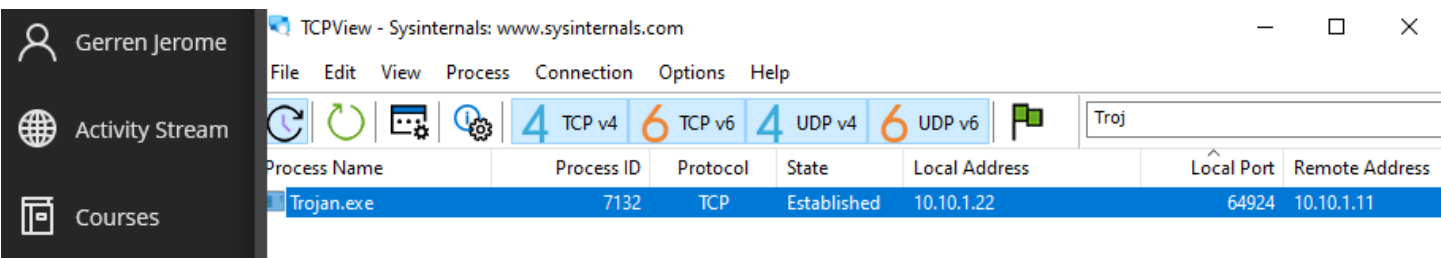
confirm creation of Trojan.exe in CEH-Tools with njRAT



launch Trojan.exe on WIN\_SVR\_22




filter TCPview scan results to find Trojan.exe




Process Name	Process ID	Protocol	Local Port	Local Port Name	Local Address	Remote Port	Remote Port Name	Remote Address	Remote Name
System	4	TCP	64918		10.10.1.22	445	microsof...	10.10.1.11	WII
System	4	TCP	64919		10.10.1.22	445	microsof...	10.10.1.11	WII
System	4	TCP	80	http	0.0.0.0			0.0.0.0	
System	4	TCP	445	microsof...	0.0.0.0			0.0.0.0	
System	4	TCP	5985		0.0.0.0			0.0.0.0	
System	4	TCP	47001		0.0.0.0			0.0.0.0	
System	4	UDP	137	netbios-ns	10.10.1.22				
System	4	UDP	138	netbios-...	10.10.1.22				
System	4	UDP	960		0.0.0.0				
System	4	TCP	80	http	::			::	Ser
System	4	TCP	445	microsof...	::			::	Ser
System	4	TCP	5985		::			::	Ser
System	4	TCP	47001		::			::	Ser
System	4	TCP	64905		fe80::9d68:1d1...	445	microsof...	fe80::709f:40d1...	Wir
System	4	UDP	920		::				Ser
Trojan.exe	6280	TCP	64939		10.10.1.22	5552		10.10.1.11	WII
Unknown	0	TCP	64040		fe80::9d68:1d1...	135	...	fe80::9d68:1d1...	Ser


## Examine Trojan.exe's Properties (didn't kill process yet)

 Institution Page


---

 Gerren Jerome


---

 Activity Stream


---

 Courses


---

 Organizations


---

 Calendar


---

 Messages


---

 Grades


---

 Assist

---

 Tools

---

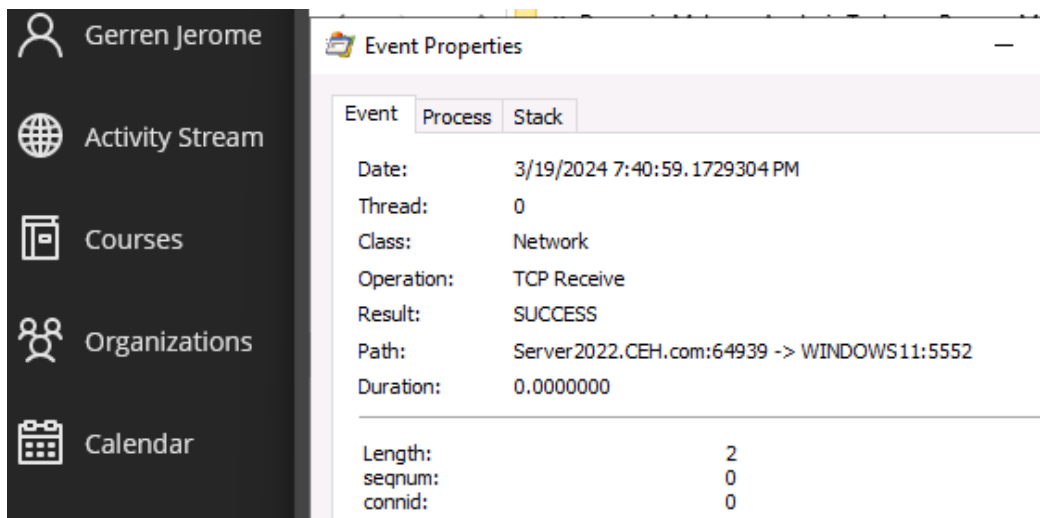
 Sign Out

### Properties

Process Name:	Trojan.exe
Process ID:	6280
Protocol:	TCP
Local Port:	64939
Local Port Name:	
Local Address:	10.10.1.22
Remote Port:	5552
Remote Port Name:	
Remote Address:	10.10.1.11
Remote Host Name:	WINDOWS11
State:	Established
Sent Bytes:	130
Received Bytes:	14
Sent Packets:	11
Received Packets:	7
Process Path:	C:\Users\Administrator\AppData\Local\Temp\1\Trojan.exe
Product Name:	
File Description:	
File Version:	
Company:	
Process Created On:	3/19/2024 7:36:10 PM
User Name:	CEHAdministrator
Process Services:	
Process Attributes:	A

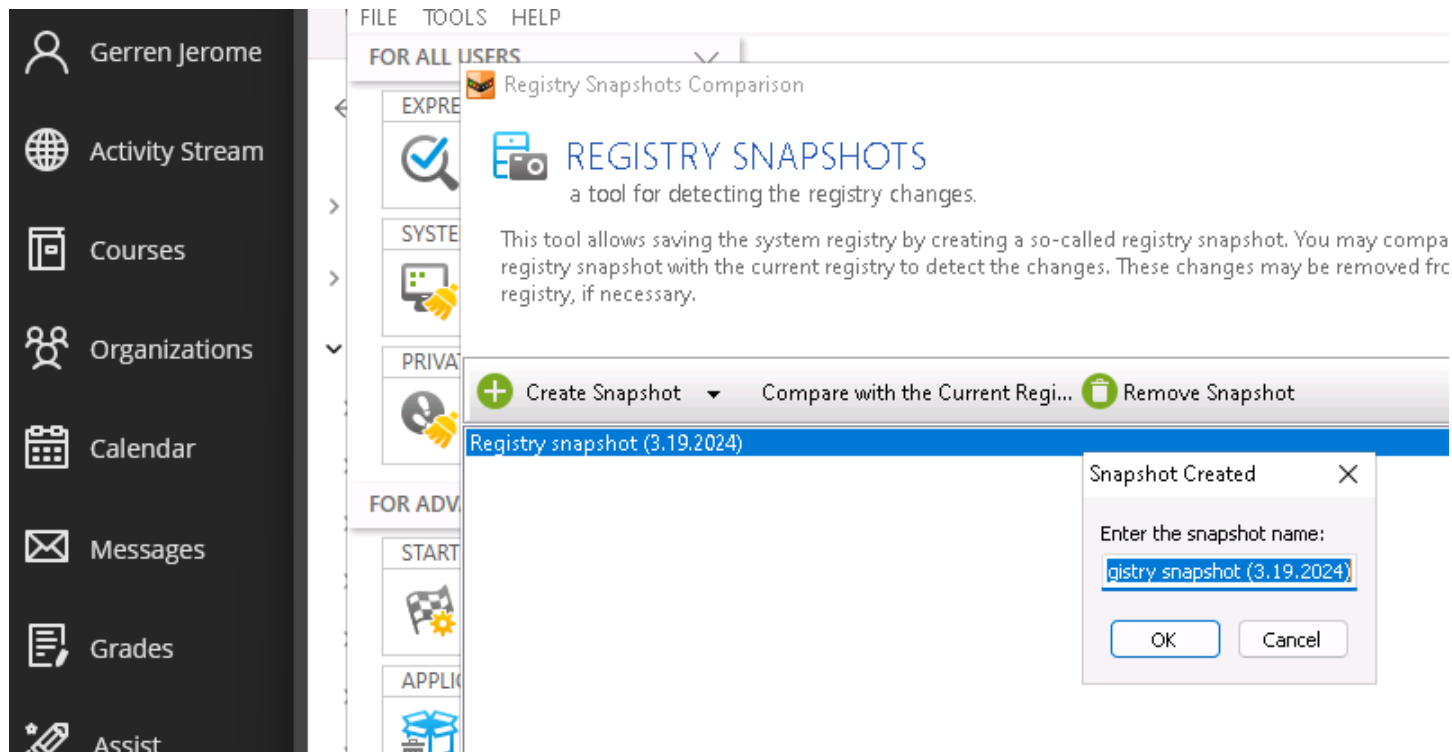
### Perform process monitoring using Process Monitor

#### Identify properties of Trojan.exe from 4a in Process Monitor

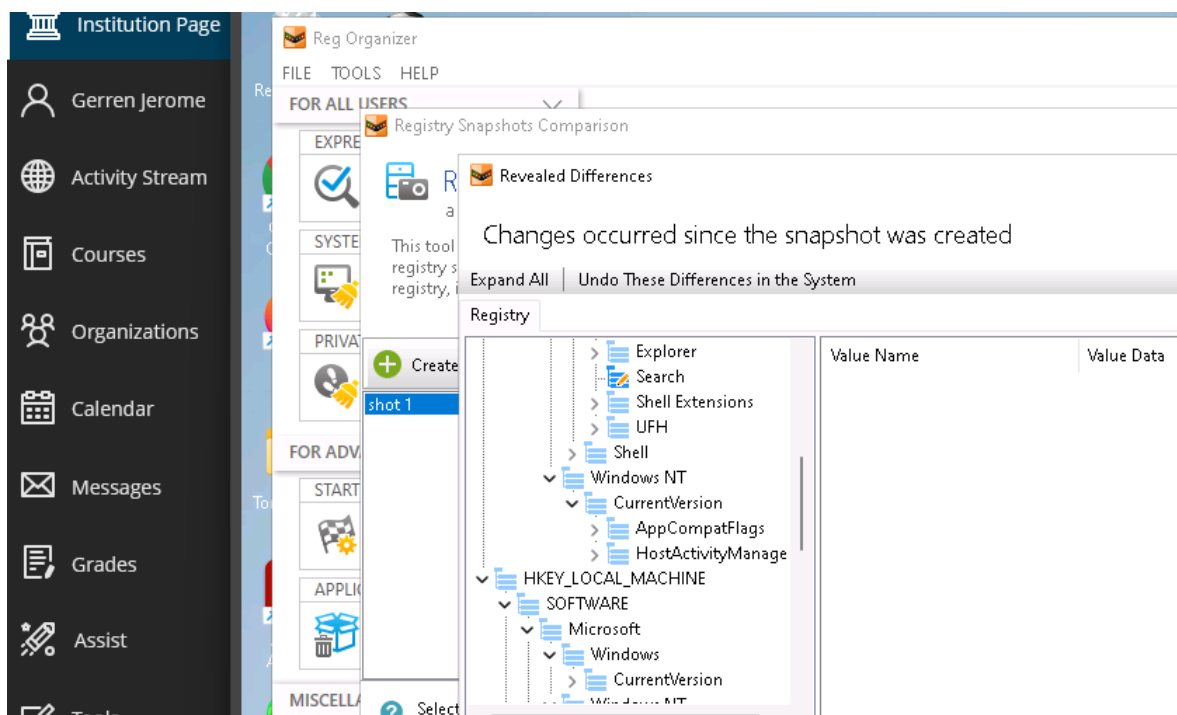


### Perform registry monitoring using Reg Organizer

#### Create snapshot in Reg Organizer

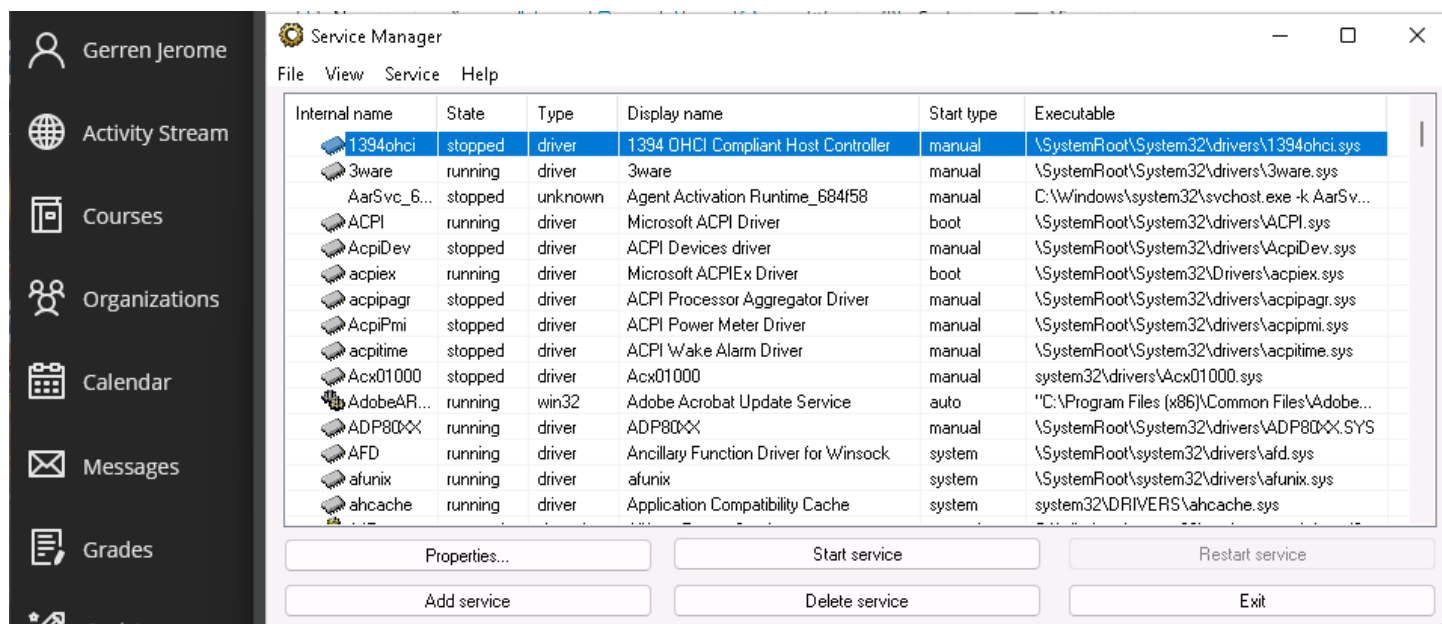


### Identify changes in Registry post-install of SoftPerfect Network Scanner



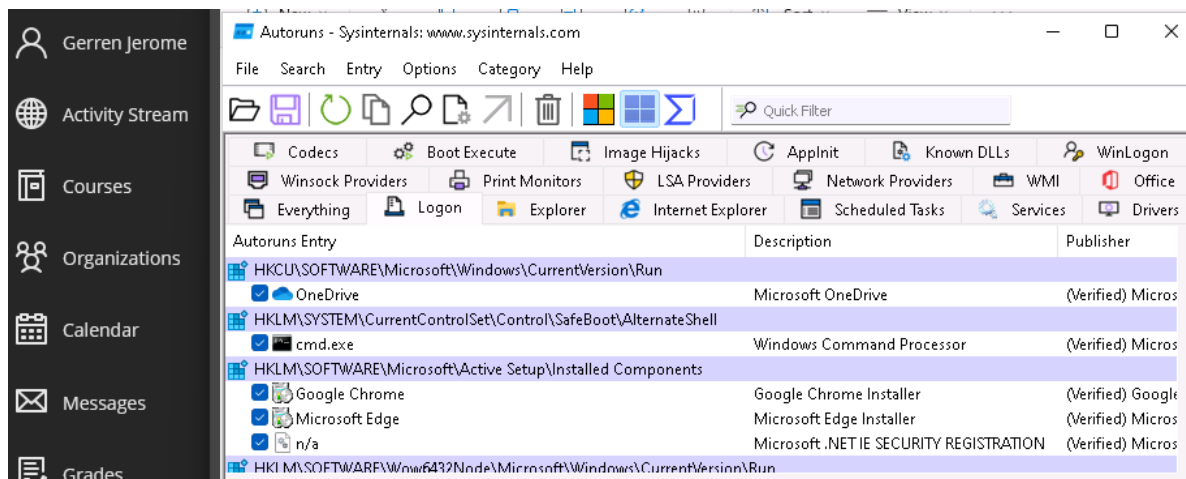
### Perform Windows services monitoring using Windows Service Manager (SrvMan) (1 task)

#### Service Manager main window.

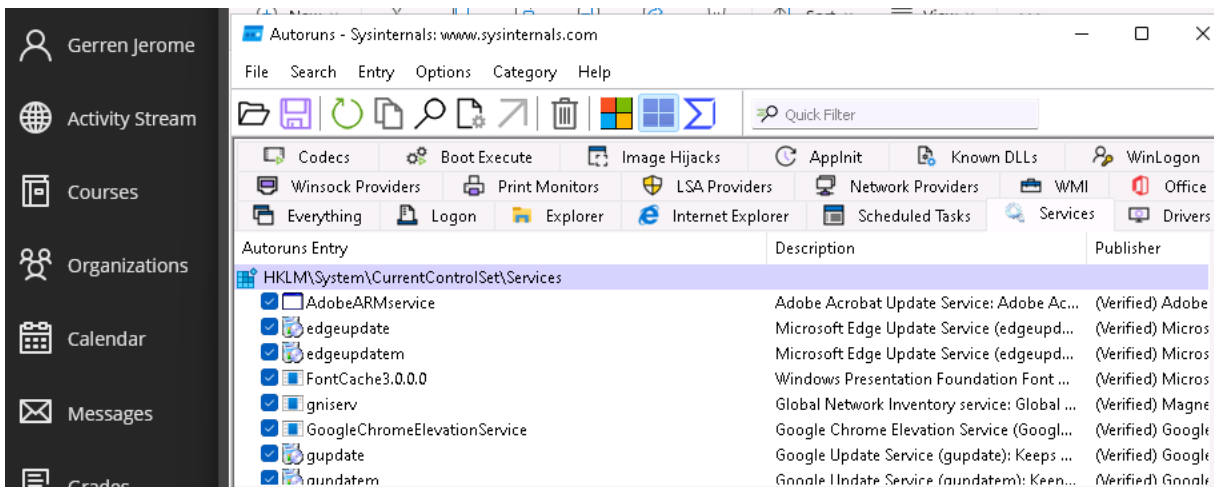


## Perform startup program monitoring using Autoruns for Windows and WinPatrol

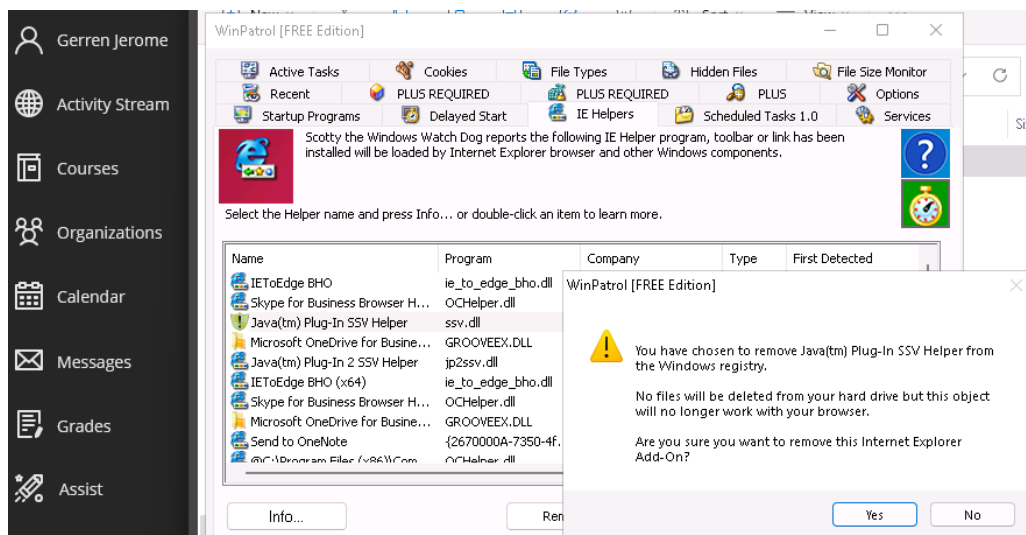
### Identify login processes in Autoruns.



### Identify services at startup in Autoruns.



### View IE Helpers tab in WinPatrol

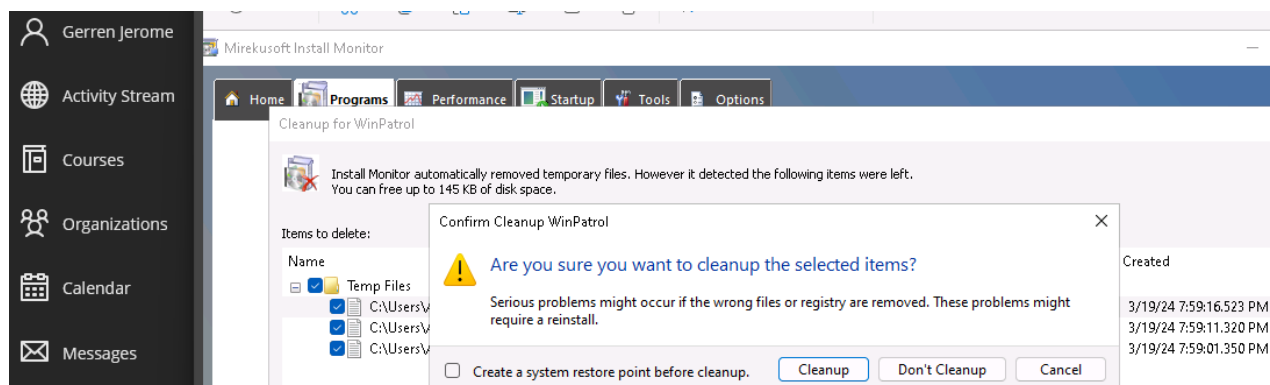


### Show expanded view of Windows Batch File information.



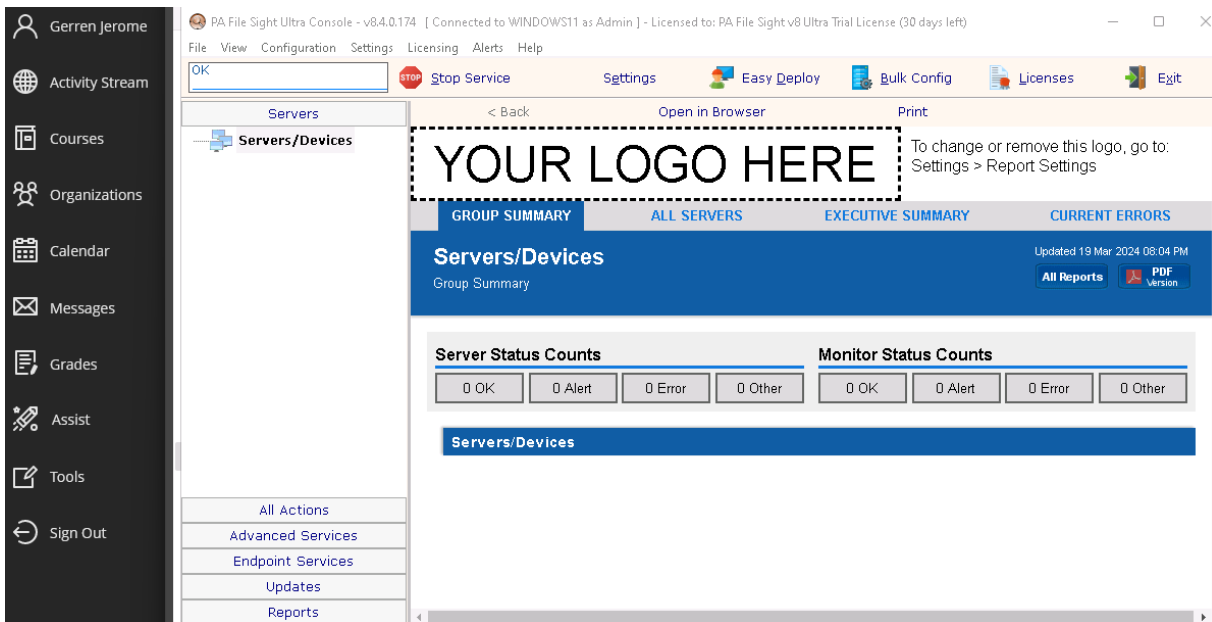
### Perform installation monitoring using Mirekusoft Install Monitor

### confirm cleanup of WinPatrol

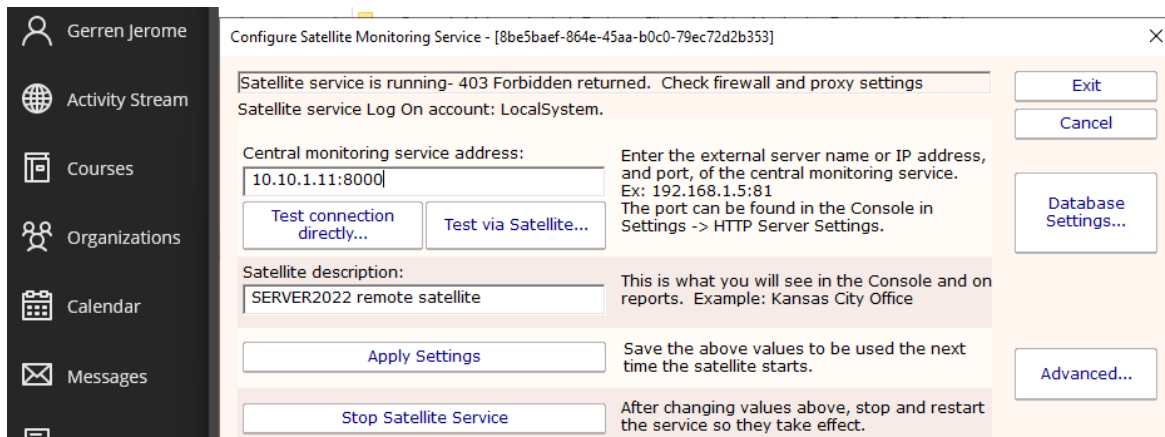


## Perform files and folder monitoring using PA File Sight

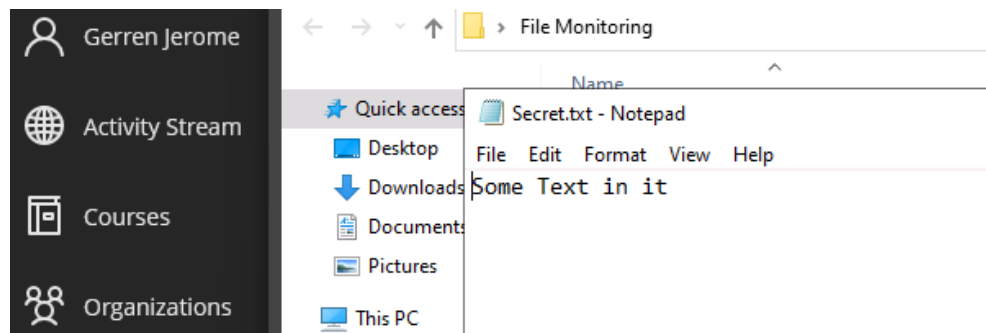
Install and load up PA File Sight Ultra's console.



Configure satellite monitoring service.



i) **Screengrab: Step 21** – Create secret.txt on WIN\_SVR\_22





## Confirm remote monitoring on Server2022.

PA File Sight Ultra Console - v8.4.0.174 [ Connected to WINDOWS11 as Admin ] - Licensed to: PA File Sight v8 Ultra Trial License (30 days left)

File View Configuration Settings Licensing Alerts Help

OK Stop Service Settings Easy Deploy Bulk Config Licenses Exit

Servers < Back Open in Browser Print

File I/O not being monitored. Add a File Sight Monitor to this server (right-click, choose Add New Monitor)

YOUR LOGO HERE

To change or remove this logo, go to: Settings > Report Settings

SERVER2022  
SERVER2022 remote satellite

Updated 19 Mar 2024 08:11:06 PM

Group Reports All Reports PDF Version

System Information

## Create ruleset and instantiate Monitoring File action in Monitor Actions

PA File Sight Configuration

Monitor Actions

This monitor is an Event monitor, which means it fires the configured actions every time a problem is detected.

Error Actions (run in the order shown)

Do Immediately:  
Monitoring File

Global Action List  
Select actions from this list and assign to the monitor

New... Edit...

Add to Blocked User List - 3h 0m  
Add to Blocked User List - TESTING - 3h 0m  
Message Box  
Monitoring File

## View Server2022 dashboard

PA File Sight Ultra Console - v8.4.0.174 [ Connected to WINDOWS11 as Admin ] - Licensed to: PA File Sight v8 Ultra Trial License (30 days left)

File View Configuration Settings Licensing Alerts Help

OK - 3 monitors run Stop Service Settings Easy Deploy Bulk Config Licenses Exit

Servers < Back Open in Browser Print

Devices

SERVER2022

Watch C:\Users\Administrator\Desktop\Inventory Collector

Inventory Collector

System Details

Uptime  
0 days, 3 hours, 0 minutes

CPU  
Intel(R) Xeon(R) Gold 6230 CPU @ 2.10GHz

Model  
Microsoft CorporationVirtual Machine

Operating System  
Microsoft Windows Server 2022 Standard 10.0.20348

CPU: Core Count  
CPU0: 1

Memory  
Physical: 8,191 MB  
Page File: 1,280 MB

Monitor Status

Monitor	Last Status	Last Checked
Inventory Collector Probe methods: WMI, System Details program	OK	3/19/2024 8:11:07 PM
Watch C:\Users\Administrator\Desktop\File Monitoring\	OK	3/19/2024 8:16:55 PM

Confirm monitor is capturing correctly (activity in Secret.txt)

PA File Sight Ultra Console - v8.4.0.174 [ Connected to WINDOWS11 as Admin ] - Licensed to: PA File Sight v8 Ultra Trial License (30 days left)

File View Configuration Settings Licensing Alerts Help

User Account added to Blocked User List

STOP Stop Service Settings Easy Deploy Bulk Config Licenses

Servers < Back Open in Browser Print

YOUR LOGO HERE

To change or remove this logo, go to: Settings > Report Settings

SERVER: SERVER2022 re

System Information

CEH\Administrator [[notepad.exe]]

Time	Operation	File
8:20:40 PM	Written	C:\Users\Administrator\Desktop\File Monitoring\Secret.txt
8:20:10 PM	Read	C:\Windows\Fonts\StaticCache.dat
8:20:10 PM	Read	C:\Windows\SystemResources\notepad.exe.mun
8:20:10 PM	Read	C:\Windows\System32\en-US\notepad.exe.mui
8:20:10 PM	Read	C:\Windows\System32\en-US\propsys.dll.mui
8:20:10 PM	Read	C:\Users\Administrator\Desktop\desktop.ini
8:20:10 PM	Read	C:\Users\desktop.ini

Perform device driver monitoring using DriverView and Driver Reviver

Display driver properties (not afunix.sys)

Properties

Driver Name: afunix.sys

Address: FFFFF804`42630000

End Address: FFFFF804`42643000

Size: 0x00013000

Load Count: 1

Index: 150

File Type: System Driver

Description: AF\_UNIX socket provider

Version: 10.0.22000.348

Company: Microsoft Corporation

Product Name: Microsoft® Windows® Operating System

Modified Date: 12/7/2021 2:50:31 PM

Created Date: 12/7/2021 2:50:31 PM

Filename: C:\Windows\system32\drivers\afunix.sys

File Attributes: A

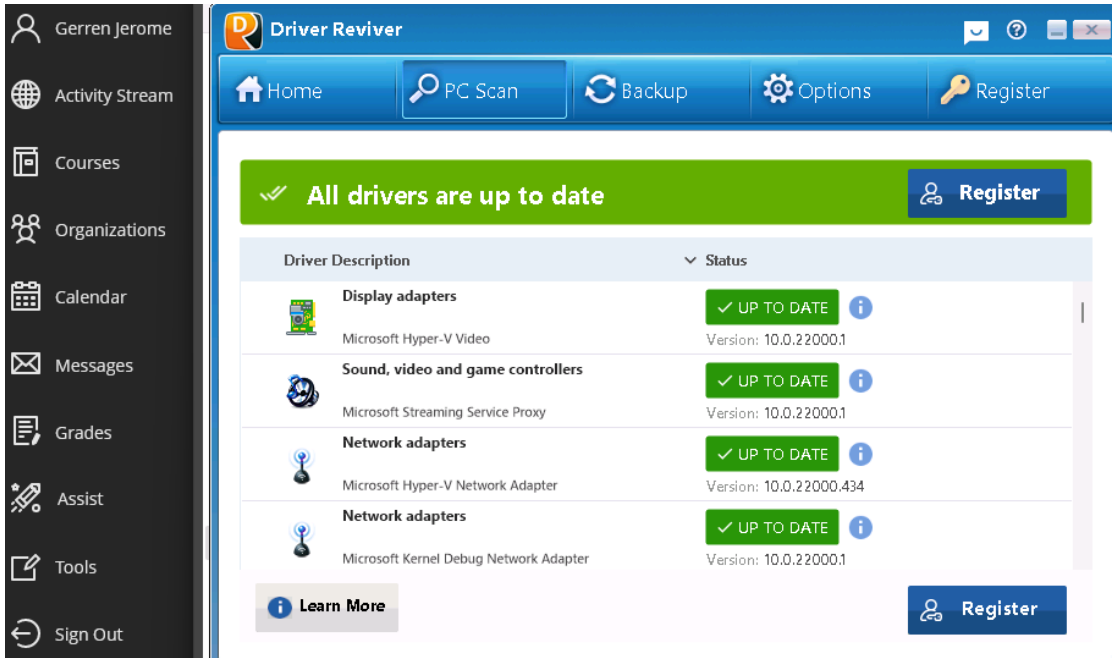
Service Name: afunix

Service Display Name: afunix

Digital Signature:

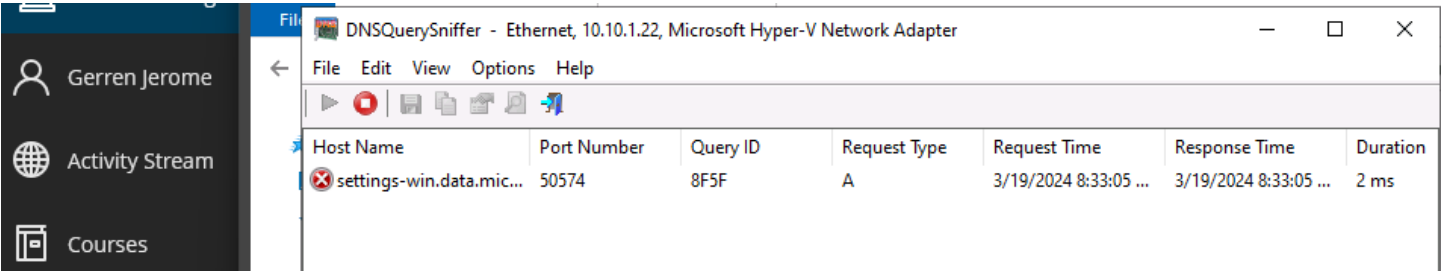
OK

Status Driver Reviver scan



Perform DNS monitoring using DNSQuerySniffer.

Start sniffer.



Observe logged changes to DNS.

