

NSSECU3 Capture-The-Flag Challenge: don't Fall and don't shed a Tear

Money is not a Problem: Attacking or Defending

Student 2		You Passed	Yes
-----------	--	------------	-----

Sophia Elen Perez
July 3, 2023

I. Challenge Description

This challenge aims to investigate a ransomware attack targeting Jacque-Kween Luxury to identify the point of entry, the exfiltrated data, the system's vulnerability, the specific ransomware employed, and the recovery of encrypted files. Additionally, this challenge aims to identify any compromised files containing the company's Intellectual Property, which would be considered an egregious breach by the board of directors. The investigation will utilize a memory image, disk image, and PCAP file as primary sources of evidence.

II. Answering the Flags

The explanations are arranged in the order of when the questions were answered.

A. Payload (Question 6)

■ **Worth:** 10 points

■ **Question:**

A ransomware was executed on the system, encrypting important files and demanding payment. Investigate and identify the process that was used to execute the ransomware, as well as the time it was executed.

What was the name of the file that was used to execute the ransomware on the system?

Format: <File name>.<File Extension>

■ **Answer:** **Salary-2019.exe**

■ **Thought Process & Analysis**

Upon initial observation of the files and challenge questions, the first question mentioned '*an attachment being opened and downloaded.*' This prompted me to examine the downloaded files in the disk image file named "ctf20230327" using FTK Imager.

AccessData FTK Imager 4.7.1.2

File View Mode Help

Disk Tree

Name	Type	Date Modified
WireSharkPortable64	Directory	3/21/2023 6:15:06 AM
\$I0	NTFS Index All...	3/21/2023 6:41:22 AM
AccessData_FTK_Imager_4.7.1.exe	Regular File	3/20/2023 3:49:08 AM
configuration-Office2019Enterprise.xml	Regular File	2/27/2023 12:32:02 AM
configuration-Office2021Enterprise.xml	Regular File	2/27/2023 12:32:02 AM
configuration-Office365-x64.xml	Regular File	2/27/2023 12:32:02 AM
configuration-Office365-x86.xml	Regular File	2/27/2023 12:32:02 AM
desktop.ini	Regular File	2/23/2022 6:27:02 AM
officedeploymenttool_16130-20218.exe	Regular File	3/17/2023 6:45:28 AM
OfficeSetup.exe	Regular File	3/17/2023 6:51:56 AM
resume-20230327.doc	Regular File	3/2/2023 6:23:47 AM
Salary-2019.exe	Regular File	3/2/2023 6:41:22 AM
sdl-memroy.zip	Regular File	3/20/2023 3:54:27 AM
setup.exe	Regular File	2/27/2023 12:32:02 AM
SysinternalsSuite.zip	Regular File	3/20/2023 3:46:14 AM
Thunderbird Setup 102.9.0.exe	Regular File	5/16/2023 1:35:47 AM
Thunderbird Setup 102.9.0.exe	Regular File	5/16/2023 6:23:22 AM
Windows10-kb5013945-x64_6572e52ed97e1a5f5331875250487e914...	Regular File	6/5/2024 3:16:59 AM
WireSharkPortable64	Regular File	3/24/2023 6:16:23 AM
WireSharkPortable64_4.0.4.paf.exe	Regular File	4/4/2023 4:44:12 AM
WireShark-win64-4.0.4.exe	Regular File	3/17/2023 8:21:45 AM
Spika.doc	Regular File	

Evidence Tree Sources

Evidence: File System [Path: File] Options

Properties Hex Value Interpreter Custom Content Sources Cursor pos = 0

isted: 21 Selected: 0 c:\20230327.001\NONAME [NTFS]\[root]\Users\ORN-JEG\Downloads

In the process of examining the downloaded files, a Windows Defender alert was triggered, indicating the detection of a ransomware threat. The file "Salary-2019.exe" specifically triggered this alert and was then identified as the one matching the format of Question 6.

Windows Security

Ransomware found

Microsoft Defender Antivirus has detected threats.

See details.

Dismiss

Threat quarantined

7/9/2023 10:12 AM

Severity: Severe

Detected: Ransom:MSIL/Ryzerlo.A

Status: Quarantined

Quarantined files are in a restricted area where they can't harm your device. They will be removed automatically.

B. Arrival Vector (Question 1)

- **Worth:** 10 points
- **Question:**

John, a new employee in the HR department of Company JKL, received an email with an attachment from an unknown sender. The email was opened and the attachment downloaded. Investigate the email to determine the URI that the suspicious file was downloaded from.

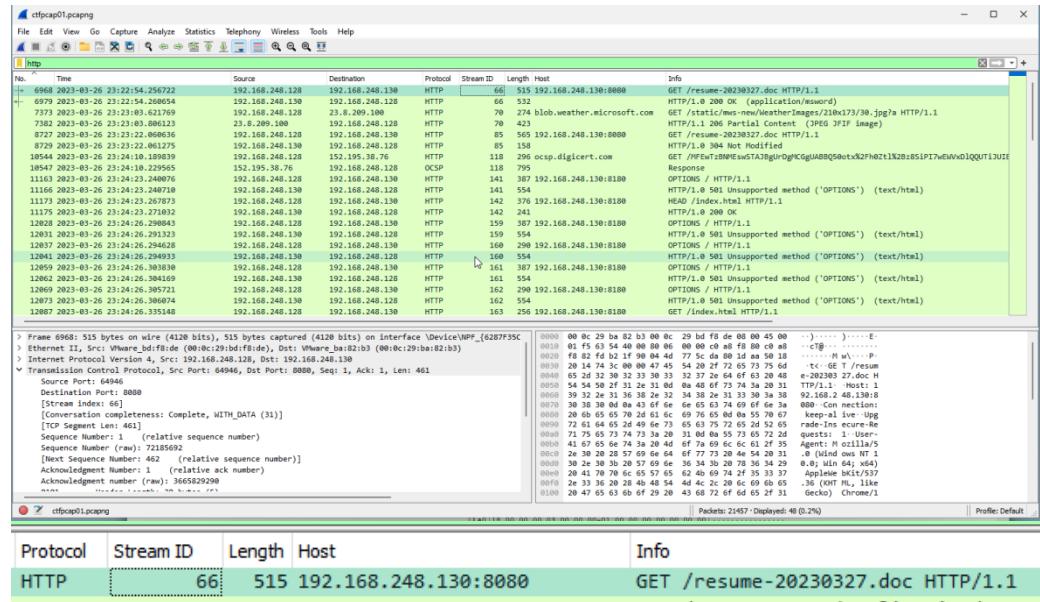
Question: What was the URI of the attachment that John downloaded?

Format: <protocol>://<IP address>:<port>/<file name>.<file extension>

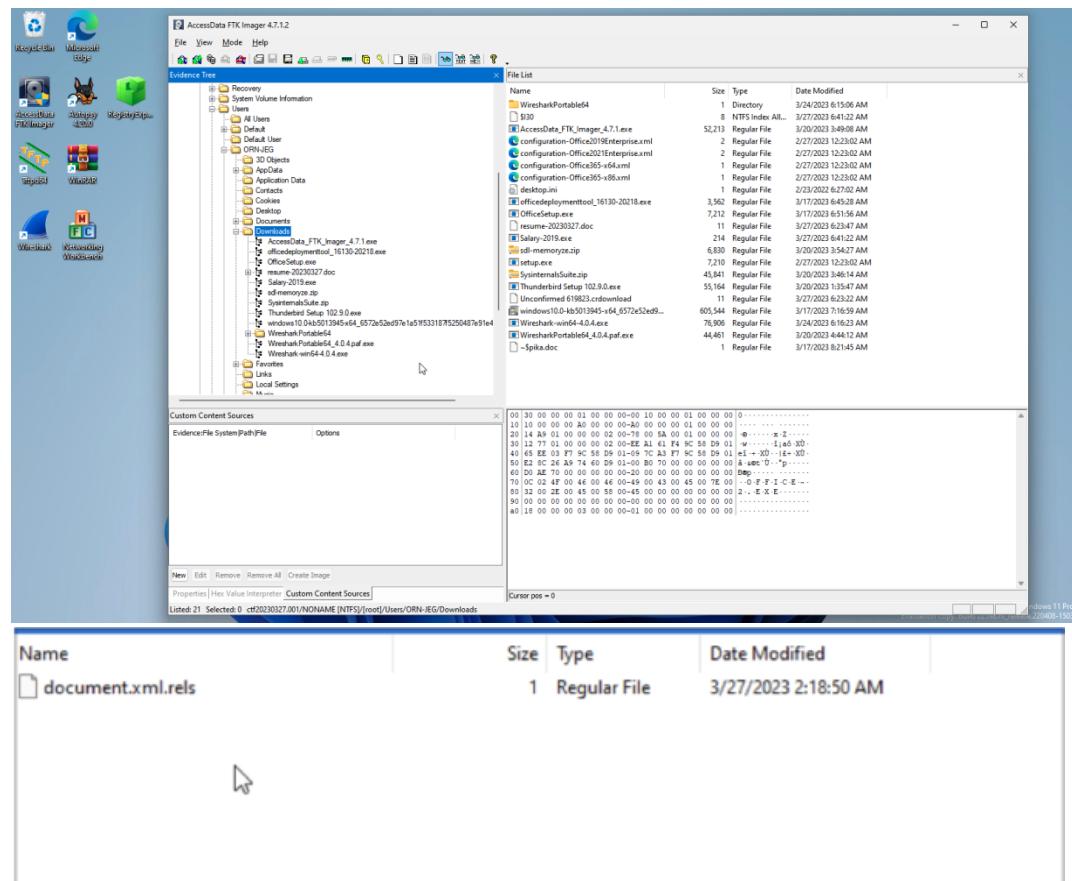
- **Answer:** <http://192.168.248.130:8080/resume-20230327.doc>

■ Thought Process & Analysis

Utilizing Wireshark, I conducted an investigation on the first PCAP file, labeled "ctfpcap01." Considering the context of the question, I focused on analyzing protocols commonly associated with file downloads, with HTTP being a prominent one. To narrow down the analysis, I applied a filter specifically for HTTP traffic. During my examination, I observed a file name that appeared familiar from my previous inspection using Autopsy.



To confirm my suspicions, I revisited the file in Autopsy and indeed, while delving into the details of "resume-20230327.doc," a ransomware error message similar to the one encountered earlier emerged when I pressed document.xml.rels, further corroborating my findings. Consequently, the URI of the attachment that John downloaded is as follows: <http://192.168.248.130:8080/resume-20230327.doc>.



C. Vulnerability Exploited (Question 2)

- **Worth:** 30 points
- **Question:**

The ransomware attack was executed through a vulnerability in the server's system. Your team needs to analyze the system to identify the specific CVE that was exploited.

Question: What was the CVE identifier for the vulnerability that was exploited?

Format: CVE-1234-567890 or MS12-34567 (Only one format used)

- **Answer:** **CVE-2022-30190**

- **Thought Process & Analysis**

During the investigation, I utilized Autopsy to extract the artifact "Operating System Version" in order to identify the operating system version installed on the system. This information is crucial for pinpointing relevant CVEs as vulnerabilities can vary across different OS versions due to variations in system architectures, software components, and security configurations. In this case, the investigation revealed that the system was running the "21H1" version of the operating system.

The screenshot shows the Autopsy 4.2.0 interface with two main tabs open: 'Operating System Version' and 'File Analysis'.

Operating System Version Tab:

- This tab displays system information such as Processor Type (Intel(R) Core(TM) i7-6700HQ CPU @ 2.60GHz), Processor Speed (2.60 GHz), RAM (16.0 GB), and Disk Space (1.00 TB).
- It also lists the operating system version as Windows NT CurrentVersion (Windows 10 Pro) and the setup source as OS.
- A note states: "This determines the operating system type, version, build number and installation dates for current installation and previous updates."
- Associated artifacts include SOFTWARE\Microsoft\Windows NT\CurrentVersion and SYSTEM\Setup\Source OS.

File Analysis Tab:

- This tab shows a file listing for 'Table_Thumb.db' from 'Windows\Windows NT\CurrentVersion\Software\Microsoft\Windows\CurrentVersion\Run'. The file is a SQLite database.
- The table contains columns: Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dr), Flags(Meta), and Known Location.
- Sample data rows include:
 - Name: ELAM\{3b39eac3bae-e1aa-e11-0003bae4612b\}, S: 0, C: 0, O: 2022-02-24 15:57, ...
 - Name: ELAM\{3b39eac3bae-e1aa-e11-0003bae4612b\}, S: 0, C: 0, O: 2022-02-24 15:57, ...
 - Name: Journal, S: 0, C: 0, O: 2019-12-07 14:52, ...
 - Name: RegBack, S: 0, C: 0, O: 2019-12-07 14:52, ...
 - Name: SAN, S: 0, C: 0, O: 2020-02-21 15:51, ...
 - Name: SAN-LOG1, S: 0, C: 0, O: 2020-02-21 15:51, ...
 - Name: SAN-LOG2, S: 0, C: 0, O: 2020-02-21 15:51, ...
 - Name: SECURITY, S: 0, C: 0, O: 2020-02-21 15:51, ...
 - Name: SECURITY\LOG1, S: 0, C: 0, O: 2019-12-07 17:00, ...
 - Name: SECURITY\LOG2, S: 0, C: 0, O: 2019-12-07 17:00, ...
 - Name: SOFTWARE, S: 0, C: 0, O: 2022-02-08 23:22, ...
 - Name: SOFTWARE\GDI1, S: 0, C: 0, O: 2022-02-08 23:22, ...
 - Name: SOFTWARE\GDI2, S: 0, C: 0, O: 2022-02-08 23:22, ...
 - Name: SYSTEM\LOG1, S: 0, C: 0, O: 2019-12-07 17:00, ...
 - Name: SYSTEM\LOG2, S: 0, C: 0, O: 2019-12-07 17:00, ...
 - Name: Tz\Tz, S: 0, C: 0, O: 2020-02-24 15:56, ...
 - Name: [current folder], S: 0, C: 0, O: 2020-02-24 15:56, ...
 - Name: [parent folder], S: 0, C: 0, O: 2020-02-24 15:56, ...
 - Name: systemprofile, S: 0, C: 0, O: 2019-12-07 17:14, ...
- File details for 'Table_Thumb.db' show it is a SQLite database located at 'C:\Windows\Windows NT\CurrentVersion\Software\Microsoft\Windows\CurrentVersion\Run\Table_Thumb.db' with a size of 144 bytes.

With question 4 mentioning '*remote code execution was performed on the compromised system*', I conducted a Google search using the query "remote code execution vulnerability 21H1 Windows" to assist in my investigation. The search yielded two potential CVE results: CVE-2022-34713 and CVE-2022-30190.

4

Question 4: Remote Code Execution (20 points)

It was identified that the exploit was successful and that remote code execution was performed on the compromised system. Your team needs to determine the process used for remote code execution, as well as the time that the execution occurred.

remote code execution vulnerability 21h1 windows    

Videos Images News Books Shopping Maps Flights Finance

About 88,800 results (0.34 seconds)



HKCERT

<https://www.hkcet.org> › security-bulletin › microsoft... :

Microsoft Products Remote Code Execution Vulnerability

May 31, 2022 — A remote code execution vulnerability exists when MSDT (Microsoft ...

Windows Server 2022; Windows 10 Version 21H1 for 32-bit Systems ...

People also ask :

What is Microsoft Windows remote code execution vulnerability? 

Is there a patch for CVE-2023-21716? 

What causes remote code execution vulnerability? 

What is CVE-2023-21716 Microsoft Word remote code execution? 

How safe is Microsoft Remote Desktop? 

[Feedback](#)



Sangfor Technologies

<https://www.sangfor.com> › cybersecurity › cve-2022... :

CVE-2022-34713: Microsoft Windows MSDT Remote Code ...

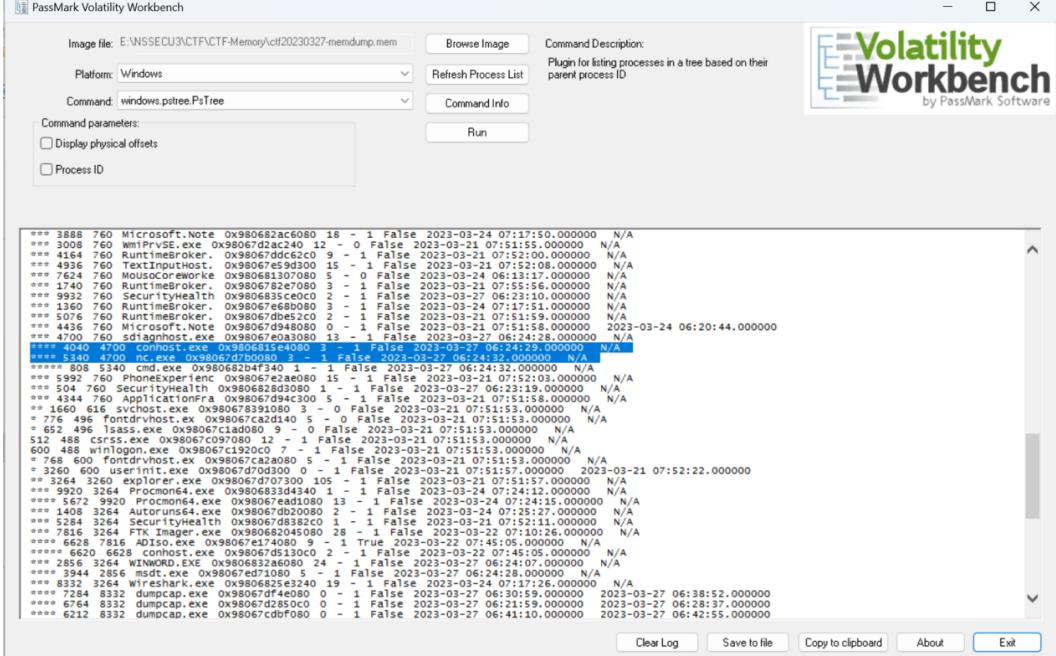
Oct 25, 2022 — Read this vulnerability report about CVE-2022-34713, Microsoft Windows MSDT Remote Code Execution Vulnerability.

Exploit Condition: User Authentication: Not req...

To confirm the suspected CVE, I employed the Volatility Workbench and executed the "pstree" command on the provided memory file, "ctf20230327-memdump.mem," to analyze the system's processes. During the analysis, I noticed the presence of "nc.exe," also known as netcat, which raised suspicion.

Netcat is frequently employed by attackers for malicious purposes, such as establishing backdoors or clandestine file transfers.

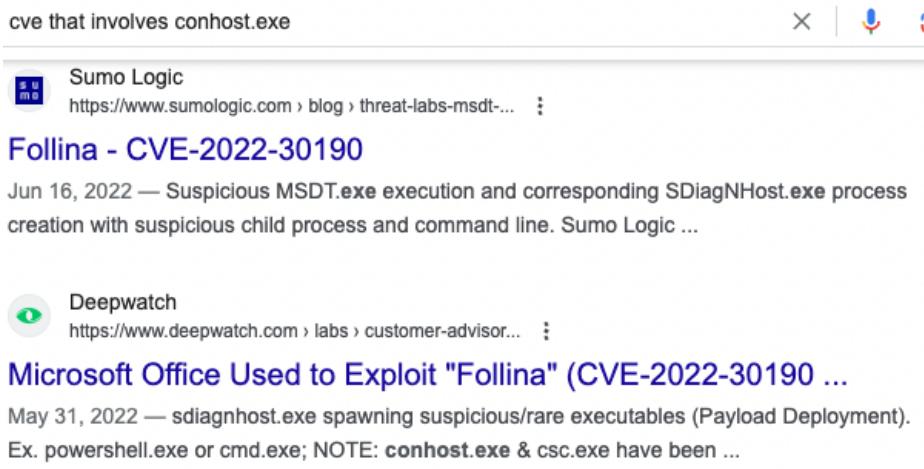
Additionally, I observed "conhost.exe" listed as a child process, which intrigued me since it is a legitimate Windows component responsible for hosting console windows. However, attackers can misuse conhost.exe to execute malicious commands or initiate unauthorized activities.



```
Image file: E:\NSSECU3\CTF\CTF-Memory\ctf20230327-memdump.mem
Platform: Windows
Command: windows.psTree.PsTree
Command parameters:
Display physical offsets
Process ID
```

ID	Process Name	Parent Process	Start Address	End Address	Flags	Date	Time	Process ID	Thread Count	Memory Usage	State
3888	Microsoft.Note	0x980652ac0080	18	-1	False	2023-03-24	07:17:50	0.000000	N/A	0	Not Started
3008	WmPrvSE.exe	0x9806d3ac240	12	-0	False	2023-03-21	07:51:55	0.000000	N/A	0	Not Started
4164	600 RuntimBroker	0x98067ddc62c0	9	-1	False	2023-03-21	07:52:00	0.000000	N/A	0	Not Started
4936	760 TextInputHost	0x98067e99d00	15	-1	False	2023-03-21	07:52:08	0.000000	N/A	0	Not Started
4938	760 SecurityHealth	0x98067e99d00	15	-0	False	2023-03-21	07:52:24	0.000000	N/A	0	Not Started
1740	760 RuntimBroker	0x9806782e7080	5	-0	False	2023-03-21	07:51:56	0.000000	N/A	0	Not Started
9932	760 SecurityHealth	0x98067835ce0c0	2	-1	False	2023-03-27	06:23:10	0.000000	N/A	0	Not Started
1360	760 RuntimBroker	0x98067e680080	3	-1	False	2023-03-24	07:17:51	0.000000	N/A	0	Not Started
4436	760 SecurityHealth	0x98067e680080	3	-0	False	2023-03-24	07:17:51	0.000000	N/A	0	Not Started
4436	760 Microsoft.Note	0x98067d948080	0	-1	False	2023-03-21	07:51:58	0.000000	2023-03-24 06:20:44.000000	0	Not Started
4700	760 sdIagnhost.exe	0x98067ea3080	13	-1	False	2023-03-27	06:24:28	0.000000	N/A	0	Not Started
1040	4700 conhost.exe	0x9806815d4080	1	-1	False	2023-03-21	06:24:29	0.000000	N/A	0	Not Started
5108	600 powershell.exe	0x9806815d4080	1	-1	False	2023-03-21	07:51:53	0.000000	N/A	0	Not Started
808	5340 cmd.exe	0x980682b4f340	1	-1	False	2023-03-27	06:24:32	0.000000	N/A	0	Not Started
592	760 PhoneExploit	0x98067e2ae080	15	-1	False	2023-03-21	07:52:03	0.000000	N/A	0	Not Started
508	600 SetPriority.exe	0x98067d948080	5	-1	False	2023-03-27	06:24:28	0.000000	N/A	0	Not Started
544	600 ApplicationFr	0x98067d948080	5	-1	False	2023-03-27	07:51:58	0.000000	N/A	0	Not Started
1660	616 svchost.exe	0x980678391080	3	-0	False	2023-03-21	07:51:53	0.000000	N/A	0	Not Started
776	496 Fontdrvhost.exe	0x98067ca2d140	5	-0	False	2023-03-21	07:51:53	0.000000	N/A	0	Not Started
55	600 msdt.exe	0x98067d948080	5	-1	False	2023-03-21	07:51:53	0.000000	N/A	0	Not Started
512	488 csrss.exe	0x98067c097080	12	-1	False	2023-03-21	07:51:53	0.000000	N/A	0	Not Started
600	488 winlogon.exe	0x98067c1920c0	7	-1	False	2023-03-21	07:51:53	0.000000	N/A	0	Not Started
761	600 Fontdrvhost.exe	0x98067ca2a080	5	-1	False	2023-03-21	07:51:53	0.000000	N/A	0	Not Started
3260	600 userinit.exe	0x98067d70300	0	-1	False	2023-03-21	07:51:53	0.000000	2023-03-21 07:52:22.000000	0	Not Started
3264	3260 explorer.exe	0x98067d70300	105	-1	False	2023-03-21	07:51:57	0.000000	N/A	0	Not Started
9920	3260 Procmon64.exe	0x9806833d4340	1	-1	False	2023-03-24	07:24:12	0.000000	N/A	0	Not Started
5108	9920 Procmon64.exe	0x9806833d4340	13	-1	False	2023-03-24	07:24:15	0.000000	N/A	0	Not Started
5208	3264 Autorun64.exe	0x98067d000080	1	-1	False	2023-03-24	07:25:23	0.000000	N/A	0	Not Started
5284	3264 msdt.exe	0x98067d8382c0	1	-1	False	2023-03-21	07:52:11	1.000000	N/A	0	Not Started
7816	3264 FTK Imager.exe	0x980682045080	28	-1	False	2023-03-26	07:10:26	0.000000	N/A	0	Not Started
6620	6628 conhost.exe	0x98067d130c0	2	-1	False	2023-03-22	07:45:05	0.000000	N/A	0	Not Started
2856	3264 WINWORD.EXE	0x9806832a6080	24	-1	False	2023-03-27	06:24:07	0.000000	N/A	0	Not Started
3944	2856 msdt.exe	0x98067ed71080	5	-1	False	2023-03-27	06:21:28	0.000000	N/A	0	Not Started
7284	8332 dumpcap.exe	0x98067df4e080	0	-1	False	2023-03-27	06:30:59	0.000000	2023-03-27 06:38:52.000000	0	Not Started
6764	8332 dumpcap.exe	0x98067d2850c0	0	-1	False	2023-03-27	06:21:59	0.000000	2023-03-27 06:28:37.000000	0	Not Started
6212	8332 dumpcap.exe	0x98067cbf080	0	-1	False	2023-03-27	06:41:10	0.000000	2023-03-27 06:42:55.000000	0	Not Started

To gain further insight into the potential risks associated with conhost.exe, I conducted a specific Google search for CVEs related to conhost.exe. This search enabled me to find relevant information regarding security vulnerabilities associated with conhost.exe.



cve that involves conhost.exe

Sumo Logic

Follina - CVE-2022-30190

Jun 16, 2022 — Suspicious MSDT.exe execution and corresponding SDIgNHost.exe process creation with suspicious child process and command line. Sumo Logic ...

Deepwatch

Microsoft Office Used to Exploit "Follina" (CVE-2022-30190 ...)

May 31, 2022 — sdiagnhost.exe spawning suspicious/rare executables (Payload Deployment). Ex. powershell.exe or cmd.exe; NOTE: conhost.exe & csc.exe have been ...

Based on the findings from the Google search, I identified a matching CVE, which is CVE-2022-30190, aligning with the earlier search result.

Microsoft Products Remote Code Execution Vulnerability

Last Update Date: 15 Jun 2022 | Release Date: 31 May 2022 | 7547 Views

RISK: Extremely High Risk



TYPE: Operating Systems - Windows OS



A vulnerability was identified in Microsoft Products. A remote user can exploit this vulnerability to trigger remote code execution on the targeted system.

Note:

CVE-2022-30190 is being exploited in the wild. A remote code execution vulnerability exists when MSDT (Microsoft Diagnostic Tool) is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, or delete data, or create new accounts in the context allowed by the user's rights.

[Updated on 2022-06-15]

Update available patch released by vendor on "Solution"

D. Remote Code Execution (Question 4)

- **Worth:** 20 points
- **Question:**

It was identified that the exploit was successful and that remote code execution was performed on the compromised system. Your team needs to determine the process used for remote code execution, as well as the time that the execution occurred.

Question: What process was used to perform remote code execution after the exploit was successful?

Format: <File name>.<File Extension>

- **Answer:** msdt.exe

- **Thought Process & Analysis**

Based on the information gathered from the previous question, which identified the specific CVE (CVE-2022-30190) exploited in the ransomware attack, further investigation was conducted to determine the process used for remote code execution after the successful exploit.

To investigate this, the Volatility Workbench was employed to analyze the provided memory file, "ctf20230327-memdump.mem." Using the "pstree" command, the system's processes were examined. Among the processes, a specific process named "msdt.exe" was identified as the one utilized for remote code execution after the successful exploit.

This conclusion was derived by cross-referencing the identified CVE (CVE-2022-30190) with the processes found in the memory analysis. The process "msdt.exe" aligns with the earlier findings, confirming its involvement in the remote code execution.

Upon examining the process execution timestamps, the following order and details are observed:

winword.exe: Time and date of execution - 2023-03-27 06:24:07.0000

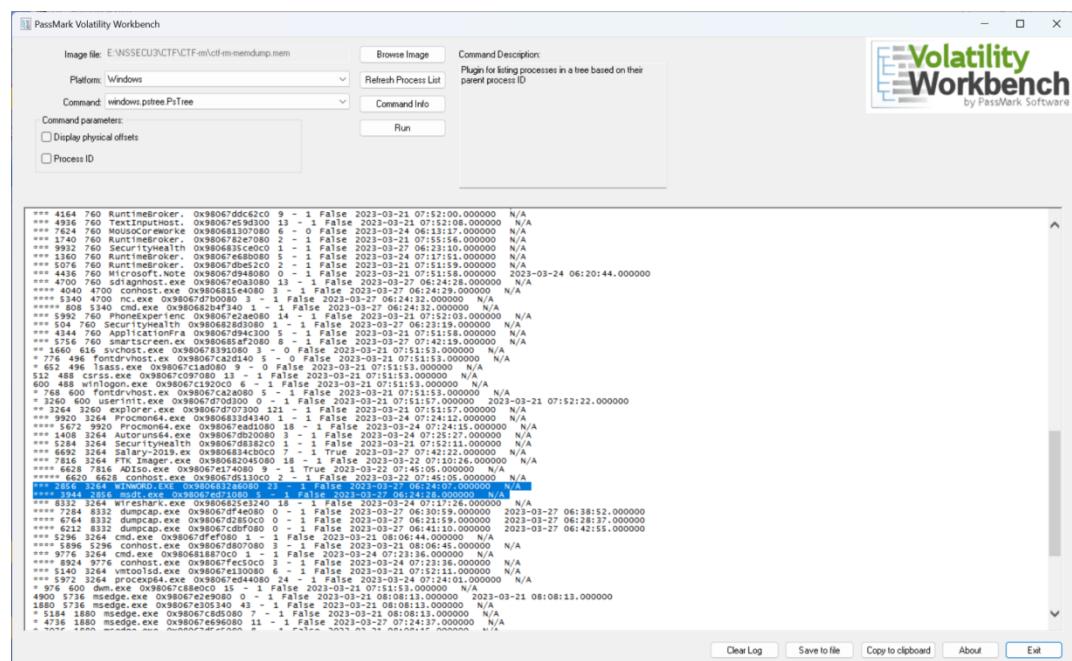
msdt.exe: Time and date of execution - 2023-03-27 06:24:28.0000

conhost.exe: Time and date of execution - 2023-03-27 06:24:29.0000

nc.exe: Time and date of execution - 2023-03-27 06:24:32.0000

It is worth noting that the initial process, Salary-2019.exe, launched winword.exe, which triggered the subsequent chain of process executions.

From these findings, it can be concluded that the process "msdt.exe" was used for remote code execution after the successful exploit. The execution occurred at 06:24:28 on March 27, 2023.



```

PassMark Volatility Workbench
Image file: E:\NSSEU03\CTF\CTF-m\ctf-mmendump.mem
Platform: Windows
Command: windows.pstree.PsTree
Command parameters:
Display physical offsets
Process ID
Run

Command Description:
Plugin for listing processes in a tree based on their parent process ID

Process Tree (Windows):
+-- 4164 760 RuntimeBroker. 0x98067ddc62c0 9 - 1 False 2023-03-21 07:52:00.000000 N/A
+-- 4936 760 TextHost. 0x98067e760000 13 - 1 False 2023-03-21 07:52:10.000000 N/A
+-- 4936 760 RuntimeBroker. 0x98067ddc62c0 14 - 1 False 2023-03-21 07:52:10.000000 N/A
+-- 1740 760 RuntimeBroker. 0x98067e760000 2 - 1 False 2023-03-21 07:55:16.000000 N/A
+-- 1360 760 RuntimeBroker. 0x98067e6bb080 3 - 1 False 2023-03-21 07:55:16.000000 N/A
+-- 1360 760 RuntimeBroker. 0x98067e6bb080 5 - 1 False 2023-03-24 07:17:51.000000 N/A
+-- 5076 760 RuntimeBroker. 0x98067eb52c0 2 - 1 False 2023-03-21 07:51:59.000000 N/A
+-- 5076 760 RuntimeBroker. 0x98067eb52c0 13 - 1 False 2023-03-21 07:51:59.000000 N/A
+-- 4700 760 sdaghnost.exe 0x98067ea03080 13 - 1 False 2023-03-27 06:24:28.000000 N/A
+-- 5140 4700 nc.exe 0x98067d70080 3 - 1 False 2023-03-27 06:24:32.000000 N/A
+-- 5936 808 760 SecurityHealth. 0x98067e2a080 14 - 1 False 2023-03-27 06:24:32.000000 N/A
+-- 5936 808 760 SecurityHealth. 0x98067e2a080 15 - 1 False 2023-03-27 06:24:32.000000 N/A
+-- 504 760 smartscreen.exe 0x9806782d080 1 - 1 False 2023-03-27 06:12:31.9.000000 N/A
+-- 5756 760 smartscreen.exe 0x9806782d080 2 - 1 False 2023-03-27 06:12:31.9.000000 N/A
+-- 5756 760 smartscreen.exe 0x9806782d080 8 - 1 False 2023-03-27 07:42:19.000000 N/A
+-- 5869 616 svchost.exe 0x980678391080 3 - 0 False 2023-03-21 07:51:53.000000 N/A
+-- 7496 496 lsass.exe 0x98067c1ad080 9 - 0 False 2023-03-21 07:51:53.000000 N/A
+-- 652 496 lsass.exe 0x98067c1ad080 10 - 0 False 2023-03-21 07:51:53.000000 N/A
+-- 512 496 lsass.exe 0x98067c1ad080 11 - 1 True 2023-03-21 07:51:53.000000 N/A
+-- 600 488 winlogon.exe 0x98067c1920c0 6 - 1 False 2023-03-21 07:51:53.000000 N/A
+-- 768 600 fontdrvhost.exe 0x98067c2a080 5 - 1 False 2023-03-24 07:11:53.000000 N/A
+-- 7324 3260 explorer.exe 0x98067d707300 121 - 1 False 2023-03-21 07:51:57.000000 N/A
+-- 3264 3260 winhttp.dll 0x98067d707300 18 - 1 False 2023-03-21 07:51:57.000000 N/A
+-- 5672 9292 ProConnode4.exe 0x98067ed1080 18 - 1 False 2023-03-24 07:12:41.15.000000 N/A
+-- 1408 3264 Autoruns64.exe 0x98067db2080 3 - 1 False 2023-03-24 07:25:27.000000 N/A
+-- 6692 3264 msdt.exe 0x98067e6bb080 1 - 1 True 2023-03-27 07:42:22.000000 N/A
+-- 6692 3264 Salary-2019.exe 0x9806834bc0c0 7 - 1 True 2023-03-27 07:42:22.000000 N/A
+-- 5296 3264 cmd.exe 0x98067feff080 15 - 1 False 2023-03-21 07:46:45.000000 N/A
+-- 6428 816 AD1so.exe 0x98067e14080 2 - 1 True 2023-03-22 07:46:45.000000 N/A
+-- 6420 6428 conhost.exe 0x98067d5130c0 2 - 1 False 2023-03-22 07:45:05.000000 N/A
+-- 3344 851 msdt.exe 0x98067ed1080 5 - 1 False 2023-03-27 06:24:28.000000 N/A
+-- 3264 3260 winhttp.dll 0x98067d707300 18 - 1 False 2023-03-27 06:24:28.000000 N/A
+-- 7284 832 msdt.exe 0x98067e760000 0 - 1 False 2023-03-27 06:30:59.000000 2023-03-27 06:38:52.000000
+-- 6764 832 dumpcap.exe 0x98067d2850c0 0 - 1 False 2023-03-27 06:21:15.9.000000 2023-03-27 06:28:37.000000
+-- 5927 3264 cmd.exe 0x98067feff080 1 - 1 False 2023-03-21 07:46:45.000000 2023-03-27 06:42:55.000000
+-- 5296 3264 cmd.exe 0x98067feff080 1 - 1 False 2023-03-21 08:06:44.000000 N/A
+-- 9732 3264 connect.exe 0x98067feff080 3 - 1 False 2023-03-24 07:23:36.000000 N/A
+-- 5296 3264 cmd.exe 0x98067feff080 1 - 1 False 2023-03-24 07:23:36.000000 N/A
+-- 8924 9776 conhost.exe 0x98067fc5c0c0 3 - 1 False 2023-03-24 07:23:36.000000 N/A
+-- 4900 5936 msedge.exe 0x98067e05340 15 - 1 False 2023-03-21 07:51:53.000000 N/A
+-- 4900 5936 msedge.exe 0x98067e05340 43 - 1 False 2023-03-21 08:08:13.000000 N/A
+-- 1880 5736 msedge.exe 0x98067e05340 43 - 1 False 2023-03-21 08:08:13.000000 N/A
+-- 1880 5736 msedge.exe 0x98067e05340 43 - 1 False 2023-03-21 08:08:13.000000 N/A
+-- 4736 1880 msedge.exe 0x98067e05340 11 - 1 False 2023-03-27 07:24:137.000000 N/A
+-- 4736 1880 msedge.exe 0x98067e05340 11 - 1 False 2023-03-27 07:24:137.000000 N/A

```

Clear Log Save to file Copy to clipboard About Exit

PassMark Volatility Workbench

Image file: E:\NSEC3\CTF\CTF-m\ctf-m-memdump.mem

Platform: Windows

Command: windows.psTree.PsTree

Command parameters:

- Display physical offsets
- Process ID

Browse Image Refresh Process List Command Info Run Command Description: Plugin for listing processes in a tree based on their parent process ID

```
*** 4164 760 RuntimeBroker.exe 0x98067ddc62c0 9 - 1 False 2023-03-21 07:52:00.000000 N/A
*** 4592 760 Win32InProcServer.exe 0x98067d193080 13 - 0 False 2023-03-21 07:52:15.000000 N/A
*** 524 760 MouseCoreworker.exe 0x98067d000080 2 - 1 False 2023-03-21 07:55:06.000000 N/A
*** 1740 760 RuntimeBroker.exe 0x9806782e7080 2 - 1 False 2023-03-21 07:55:56.000000 N/A
*** 1740 760 RuntimeBroker.exe 0x9806782e7080 2 - 1 False 2023-03-21 07:55:56.000000 N/A
*** 1360 760 RuntimeBroker.exe 0x98067e6d52c0 5 - 1 False 2023-03-24 07:17:51.000000 N/A
*** 5076 760 RuntimeBroker.exe 0x98067d000080 2 - 1 False 2023-03-24 07:51:59.000000 N/A
*** 4040 760 sdiagnost.exe 0x98067ca03080 13 - 1 False 2023-03-27 06:24:28.000000 N/A
*** 4040 760 conhost.exe 0x98067d193080 3 - 0 False 2023-03-27 06:24:29.000000 N/A
*** 4040 760 csrss.exe 0x98067d193080 3 - 0 False 2023-03-27 06:24:29.000000 N/A
*** 808 5340 cmd.exe 0x980682d4f340 1 - 1 False 2023-03-27 06:24:32.000000 N/A
*** 492 760 SecurityHealth.exe 0x98067d000080 15 - 1 False 2023-03-27 06:24:32.000000 N/A
*** 5076 760 RuntimeBroker.exe 0x98067d000080 14 - 1 False 2023-03-27 06:23:19.000000 N/A
*** 4344 760 ApplicationFrame.exe 0x98067d994300 5 - 1 False 2023-03-27 07:51:58.000000 N/A
*** 4344 760 ApplicationFrame.exe 0x98067d994300 5 - 1 False 2023-03-27 07:51:58.000000 N/A
*** 1660 616 svchost.exe 0x98067d391080 3 - 0 False 2023-03-21 07:51:53.000000 N/A
*** 776 496 fontdrvhost.exe 0x98067ca2d140 5 - 0 False 2023-03-21 07:51:53.000000 N/A
*** 524 3264 cmd.exe 0x98067d000080 1 - 1 False 2023-03-21 07:51:53.000000 N/A
*** 512 488 csrss.exe 0x98067c097080 13 - 1 False 2023-03-21 07:51:53.000000 N/A
*** 600 4040 csrss.exe 0x98067d193080 6 - 1 False 2023-03-21 07:51:53.000000 N/A
*** 768 600 fontdrvhost.exe 0x98067c2a080 5 - 1 False 2023-03-21 07:51:53.000000 N/A
*** 3260 600 userinit.exe 0x98067d703000 0 - 1 False 2023-03-21 07:51:57.000000 2023-03-21 07:52:22.000000
*** 424 760 SecurityHealth.exe 0x98067d000080 12 - 1 False 2023-03-21 07:52:22.000000 N/A
*** 9920 3264 Procmone4.exe 0x9806833d4340 1 - 1 False 2023-03-24 07:24:12.000000 N/A
*** 5672 9920 Procmone4.exe 0x9806833d4340 18 - 1 False 2023-03-24 07:24:15.000000 N/A
*** 5672 9920 Procmone4.exe 0x9806833d4340 18 - 1 False 2023-03-24 07:24:15.000000 N/A
*** 5284 3264 SecurityHealth.exe 0x98067d88382c0 1 - 1 False 2023-03-21 07:52:11.000000 N/A
*** 5284 3264 SecurityHealth.exe 0x98067d88382c0 1 - 1 False 2023-03-21 07:52:11.000000 N/A
*** 7616 3264 Fx_Icon.exe 0x98067d00045080 18 - 1 False 2023-03-27 06:24:10.26.000000 N/A
*** 6628 7816 ADiso.exe 0x98067e1f4080 9 - 1 True 2023-03-22 07:45:00.000000 N/A
*** 4040 760 csrss.exe 0x98067d193080 15 - 1 False 2023-03-22 07:45:00.000000 N/A
*** 2856 3264 WINWORD.EXE 0x9806832a6080 23 - 1 False 2023-03-27 06:24:07.000000 N/A
*** 3344 760 msdt.exe 0x98067d108000 5 - 1 False 2023-03-27 06:24:28.000000 N/A
*** 4344 760 msdt.exe 0x98067d108000 5 - 1 False 2023-03-27 06:24:28.000000 N/A
*** 7284 8322 dumpcap.exe 0x98067df4e4080 0 - 1 False 2023-03-27 06:30:59.000000 2023-03-27 06:38:52.000000
*** 676 8322 dumpcap.exe 0x98067d285c0 0 - 1 False 2023-03-27 06:21:59.000000 2023-03-27 06:28:37.000000
*** 5296 3264 dumpcap.exe 0x98067d285c0 0 - 1 False 2023-03-27 06:21:59.000000 2023-03-27 06:42:55.000000
*** 5296 3264 cmd.exe 0x98067dfef080 1 - 1 False 2023-03-24 08:06:44.000000 N/A
*** 5296 3264 cmd.exe 0x98067dfef080 1 - 1 False 2023-03-24 08:06:44.000000 N/A
*** 976 600 csrss.exe 0x98067d193080 15 - 1 False 2023-03-21 07:51:53.000000 N/A
*** 8924 9776 conhost.exe 0x98067fecc50c0 3 - 1 False 2023-03-24 07:23:36.000000 N/A
*** 8924 9776 conhost.exe 0x98067fecc50c0 3 - 1 False 2023-03-24 07:23:36.000000 N/A
*** 5972 3264 procexp4.exe 0x98067ed44080 24 - 1 False 2023-03-24 07:24:01.000000 N/A
*** 976 600 diagsvc.exe 0x98067d193080 15 - 1 False 2023-03-21 07:51:53.000000 N/A
*** 8924 9776 msedge.exe 0x98067e305340 43 - 1 False 2023-03-21 08:08:13.000000 N/A
*** 1880 5736 msedge.exe 0x98067e305340 43 - 1 False 2023-03-21 08:08:13.000000 N/A
*** 512 1880 msedge.exe 0x98067e305340 43 - 1 False 2023-03-21 08:08:13.000000 N/A
*** 4344 760 msdt.exe 0x98067d193080 11 - 1 False 2023-03-27 06:24:28.000000 N/A
*** 4344 760 msdt.exe 0x98067d193080 11 - 1 False 2023-03-27 06:24:28.000000 N/A
*** 7616 3264 Fx_Icon.exe 0x98067d00045080 18 - 1 False 2023-03-27 06:24:28.000000 N/A
*** 3008 760 WmPvrSE.exe 0x98067d2ac240 12 - 0 False 2023-03-21 07:51:55.000000 N/A
*** 4164 760 RuntimeBroker.exe 0x98067ddc62c0 9 - 1 False 2023-03-21 07:52:00.000000 N/A
*** 524 760 MouseCoreworker.exe 0x98067d000080 15 - 1 False 2023-03-21 07:52:15.000000 N/A
*** 7640 760 RuntimeBroker.exe 0x9806813d07080 3 - 0 False 2023-03-24 08:13:17.000000 N/A
*** 1740 760 RuntimeBroker.exe 0x9806782e7080 3 - 1 False 2023-03-21 07:55:56.000000 N/A
*** 9932 760 SecurityHealth.exe 0x9806833ce0c0 2 - 1 False 2023-03-27 06:23:10.000000 N/A
*** 524 760 SecurityHealth.exe 0x9806833ce0c0 2 - 1 False 2023-03-27 06:23:10.000000 N/A
*** 5076 760 RuntimeBroker.exe 0x98067d000080 2 - 1 False 2023-03-27 06:23:10.000000 N/A
*** 4436 760 Microsoft.Note.exe 0x98067d940800 0 - 1 False 2023-03-21 07:51:58.000000 2023-03-24 06:20:44.000000
*** 4700 760 sdiagnost.exe 0x98067ca03080 13 - 1 False 2023-03-27 06:24:28.000000 N/A
*** 512 4040 csrss.exe 0x98067d193080 15 - 1 False 2023-03-27 06:24:28.000000 N/A
*** 808 5340 cmd.exe 0x980682d4f340 1 - 1 False 2023-03-27 06:24:32.000000 N/A
*** 5992 760 SecurityHealth.exe 0x980682d2a080 15 - 1 False 2023-03-21 07:52:03.000000 N/A
*** 5672 9920 Procmone4.exe 0x9806833d4340 1 - 1 False 2023-03-27 06:23:19.000000 N/A
*** 5672 9920 Procmone4.exe 0x9806833d4340 18 - 1 False 2023-03-27 06:23:19.000000 N/A
*** 1660 616 svchost.exe 0x98067d391080 3 - 0 False 2023-03-21 07:51:53.000000 N/A
*** 776 496 fontdrvhost.exe 0x98067ca2d140 5 - 0 False 2023-03-21 07:51:53.000000 N/A
*** 652 496 lsass.exe 0x98067c1a080 9 - 1 False 2023-03-21 07:51:53.000000 N/A
*** 524 3264 msdt.exe 0x98067d193080 15 - 1 False 2023-03-21 07:51:53.000000 N/A
*** 600 488 winlogon.exe 0x98067c1320c0 7 - 1 False 2023-03-21 07:51:53.000000 N/A
*** 768 600 fontdrvhost.exe 0x98067ca2a080 5 - 1 False 2023-03-21 07:51:53.000000 N/A
*** 3260 600 userinit.exe 0x98067d703000 0 - 1 False 2023-03-21 07:51:57.000000 2023-03-21 07:52:22.000000
*** 424 760 SecurityHealth.exe 0x98067d000080 10 - 1 False 2023-03-21 07:52:22.000000 N/A
*** 9920 3264 Procmone4.exe 0x9806833d4340 1 - 1 False 2023-03-24 07:24:12.000000 N/A
*** 5672 9920 Procmone4.exe 0x9806833d4340 18 - 1 False 2023-03-24 07:24:15.000000 N/A
*** 1408 3264 Autorun64.exe 0x98067d020080 2 - 1 False 2023-03-24 07:25:27.000000 N/A
*** 524 3264 SecurityHealth.exe 0x98067d020080 2 - 1 False 2023-03-24 07:25:27.000000 N/A
*** 7616 3264 Fx_Icon.exe 0x980682d45080 18 - 1 False 2023-03-22 07:10:26.000000 N/A
*** 6628 7616 ADiso.exe 0x98067e1f4080 9 - 1 True 2023-03-22 07:45:05.000000 N/A
*** 2856 3264 WINWORD.EXE 0x9806832a6080 24 - 1 False 2023-03-22 07:45:05.000000 N/A
*** 5672 9920 Procmone4.exe 0x98067d108000 10 - 1 False 2023-03-22 07:45:05.000000 N/A
*** 8324 3264 Wireshark.exe 0x980682d3e240 19 - 1 False 2023-03-24 07:17:26.000000 N/A
*** 7284 8322 dumpcap.exe 0x98067df4e4080 0 - 1 False 2023-03-27 06:30:59.000000 2023-03-27 06:38:52.000000
*** 6764 8322 dumpcap.exe 0x98067d285c0 0 - 1 False 2023-03-27 06:21:59.000000 2023-03-27 06:28:37.000000
*** 6212 8322 dumpcap.exe 0x98067cd8f080 0 - 1 False 2023-03-27 06:41:10.000000 2023-03-27 06:42:55.000000
```

Clear Log Save to file Copy to clipboard About Exit

PassMark Volatility Workbench

Image file: E:\NSEC3\CTF\CTF-Memory\ctf20230327-memdump.mem

Platform: Windows

Command: windows.psTree.PsTree

Command parameters:

- Display physical offsets
- Process ID

Browse Image Refresh Process List Command Info Run Command Description: Plugin for listing processes in a tree based on their parent process ID

```
*** 3888 760 Microsoft.Note.exe 0x980682a26c080 18 - 1 False 2023-03-24 07:17:50.000000 N/A
*** 3008 760 WmPvrSE.exe 0x98067d2ac240 12 - 0 False 2023-03-21 07:51:55.000000 N/A
*** 4164 760 RuntimeBroker.exe 0x98067ddc62c0 9 - 1 False 2023-03-21 07:52:00.000000 N/A
*** 524 760 MouseCoreworker.exe 0x98067d000080 15 - 1 False 2023-03-21 07:52:15.000000 N/A
*** 7640 760 RuntimeBroker.exe 0x9806813d07080 3 - 0 False 2023-03-24 08:13:17.000000 N/A
*** 1740 760 RuntimeBroker.exe 0x9806782e7080 3 - 1 False 2023-03-21 07:55:56.000000 N/A
*** 9932 760 SecurityHealth.exe 0x9806833ce0c0 2 - 1 False 2023-03-27 06:23:10.000000 N/A
*** 524 760 SecurityHealth.exe 0x9806833ce0c0 2 - 1 False 2023-03-27 06:23:10.000000 N/A
*** 5076 760 RuntimeBroker.exe 0x98067d000080 2 - 1 False 2023-03-27 06:23:10.000000 N/A
*** 4436 760 Microsoft.Note.exe 0x98067d940800 0 - 1 False 2023-03-21 07:51:58.000000 2023-03-24 06:20:44.000000
*** 4700 760 sdiagnost.exe 0x98067ca03080 13 - 1 False 2023-03-27 06:24:28.000000 N/A
*** 512 4040 csrss.exe 0x98067d193080 15 - 1 False 2023-03-27 06:24:28.000000 N/A
*** 808 5340 cmd.exe 0x980682d4f340 1 - 1 False 2023-03-27 06:24:32.000000 N/A
*** 5992 760 SecurityHealth.exe 0x980682d2a080 15 - 1 False 2023-03-21 07:52:03.000000 N/A
*** 5672 9920 Procmone4.exe 0x9806833d4340 1 - 1 False 2023-03-27 06:23:19.000000 N/A
*** 5672 9920 Procmone4.exe 0x9806833d4340 18 - 1 False 2023-03-27 06:23:19.000000 N/A
*** 1408 3264 Autorun64.exe 0x98067d020080 2 - 1 False 2023-03-24 07:25:27.000000 N/A
*** 524 3264 SecurityHealth.exe 0x98067d020080 2 - 1 False 2023-03-24 07:25:27.000000 N/A
*** 7616 3264 Fx_Icon.exe 0x980682d45080 18 - 1 False 2023-03-22 07:10:26.000000 N/A
*** 6628 6628 conhost.exe 0x98067d130c0 2 - 1 False 2023-03-22 07:45:05.000000 N/A
*** 2856 3264 WINWORD.EXE 0x9806832a6080 24 - 1 False 2023-03-22 07:45:05.000000 N/A
*** 5672 9920 Procmone4.exe 0x98067d108000 10 - 1 False 2023-03-22 07:45:05.000000 N/A
*** 8324 3264 Wireshark.exe 0x980682d3e240 19 - 1 False 2023-03-24 07:17:26.000000 N/A
*** 7284 8322 dumpcap.exe 0x98067df4e4080 0 - 1 False 2023-03-27 06:30:59.000000 2023-03-27 06:38:52.000000
*** 6764 8322 dumpcap.exe 0x98067d285c0 0 - 1 False 2023-03-27 06:21:59.000000 2023-03-27 06:28:37.000000
*** 6212 8322 dumpcap.exe 0x98067cd8f080 0 - 1 False 2023-03-27 06:41:10.000000 2023-03-27 06:42:55.000000
```

Clear Log Save to file Copy to clipboard About Exit

E. Exploitation (Question 3)

■ **Worth:** 20 points

■ **Question:**

It was discovered that the compromised system connected to a specific IP address and port in order to exploit the vulnerability in the system. Your team now needs determine the IP address and port used for the exploit.

Question: What was the IP address and port used to deliver the exploit
Format: <IP address>:<port>

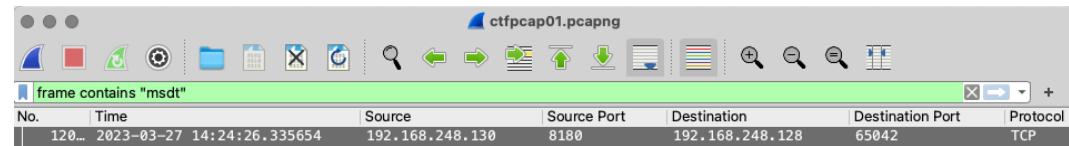
- **Answer:** 192.168.248.130:8180

- **Thought Process & Analysis**

To determine the IP address and port used to deliver the exploit, I utilized Wireshark and analyzed the first PCAP file. To narrow down the search, I applied a filter to capture frames containing "msdt.exe," the process involved in the remote code execution.

By examining the filtered frames in Wireshark, I looked for relevant network traffic that corresponded to the delivery of the exploit. Within the captured frames, I observed a specific IP address and port associated with the exploit.

Based on my analysis, the IP address and port used to deliver the exploit are as follows: 192.168.248.130:8180.



No.	Time	Source	Source Port	Destination	Destination Port	Protocol
120...	2023-03-27 14:24:26.335654	192.168.248.130	8180	192.168.248.128	65042	TCP

F. Data Exfiltration (Question 5)

- **Worth:** 10 points

- **Question:**

After gaining control of the system, the attacker exfiltrated a number of files from the server. Analyze the system to determine the total number of files that were exfiltrated.

Question: How many files were exfiltrated from the system during the ransomware attack?

Format: Numerical

- **Answer:** 6

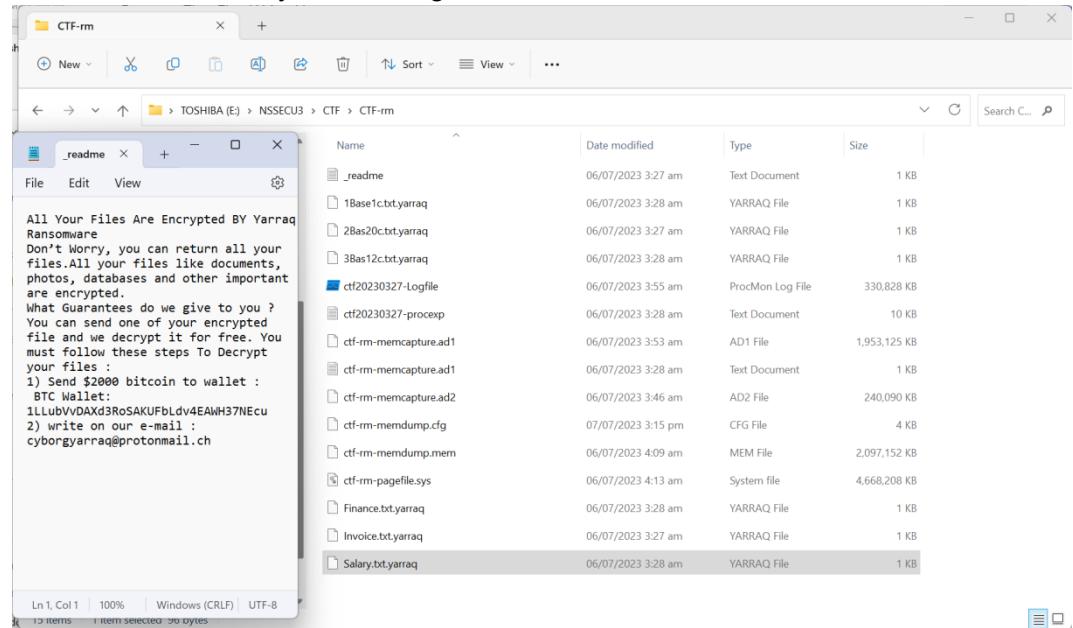
- **Thought Process & Analysis**

While examining the ctf folder, I came across a text file named "_readme". The contents of this file indicated that the attacker had encrypted various files on the server. The message included instructions on how to decrypt the files and a Bitcoin

wallet address for the payment of \$2000. This information suggested that the files had been exfiltrated by the attacker.

Additionally, I noticed that the file extension ".yarraq" was associated with the encrypted files. "yarraq" files are typically associated with the encrypted files created by the Yarraq ransomware. The Yarraq ransomware is a type of malicious software that encrypts various types of files on a victim's system, making them inaccessible without a decryption key. The encrypted files often have the ".yarraq" extension appended to their original file names. These files remain unusable until the victim pays the ransom and receives the decryption key to restore their files to their original state.

By searching for files with this extension in the folder, I identified a total of 6 files with the ".yarraq" extension and it can be determined that these files were exfiltrated from the system during the ransomware attack.



Name	Date modified	Type	Size
_readme	06/07/2023 3:27 am	Text Document	1 KB
1Base1c.txt.yarraq	06/07/2023 3:28 am	YARRAQ File	1 KB
2B8as20c.txt.yarraq	06/07/2023 3:27 am	YARRAQ File	1 KB
3B8as12c.txt.yarraq	06/07/2023 3:28 am	YARRAQ File	1 KB
ctf20230327-LogFile	06/07/2023 3:55 am	ProcMon Log File	330,828 KB
ctf20230327-procexp	06/07/2023 3:28 am	Text Document	10 KB
ctf-rm-memcapture.ad1	06/07/2023 3:53 am	AD1 File	1,953,125 KB
ctf-rm-memcapture.ad1	06/07/2023 3:28 am	Text Document	1 KB
ctf-rm-memcapture.ad2	06/07/2023 3:46 am	AD2 File	240,090 KB
ctf-rm-memdump.cfg	07/07/2023 3:15 pm	CFG File	4 KB
ctf-rm-memdump.mem	06/07/2023 4:09 am	MEM File	2,097,152 KB
ctf-rm-pagefile.sys	06/07/2023 4:13 am	System file	4,668,208 KB
Finance.txt.yarraq	06/07/2023 3:28 am	YARRAQ File	1 KB
Invoice.txt.yarraq	06/07/2023 3:27 am	YARRAQ File	1 KB
Salary.txt.yarraq	06/07/2023 3:28 am	YARRAQ File	1 KB

G. Capture the flag (BONUS Question)

- **Worth:** 50 points
- **Question:**

From the data exfiltrated, there is a hidden message, encrypted but not needed to decrypt, sometimes you are carving for ice cream, sometimes you misread the verb, ultimately, it is easy as 1 2 3

Find the flag and copy and paste and decode it the puzzle. Copy and paste the last and you will get the words when you successfully got the message.

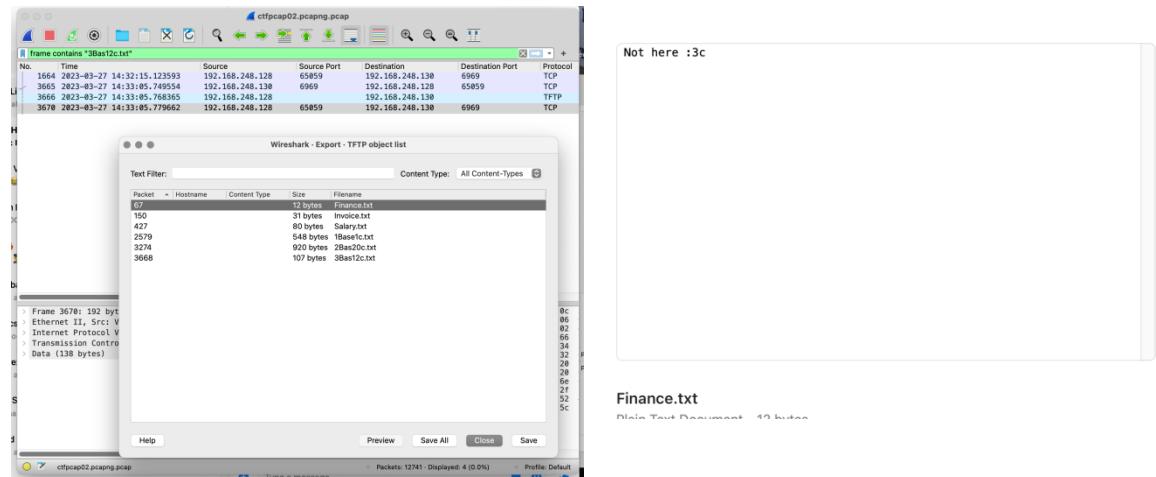
Format: flag{string}

■ Answer: f14g{C0ngr@tum4l4t!Ons!!!}

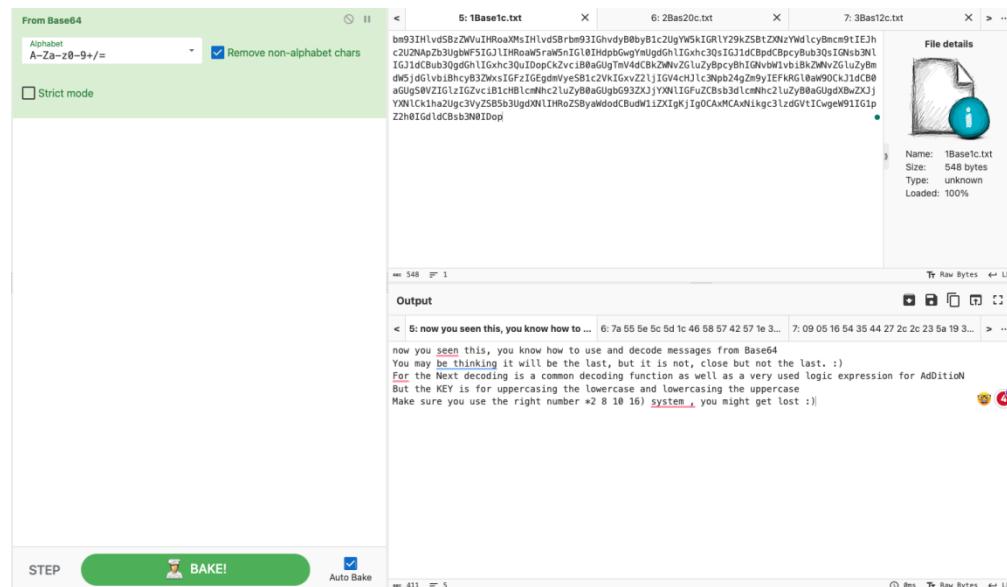
■ Thought Process & Analysis

Using the clues provided in the bonus question, the process of decoding the hidden message began. The mention of "carving" led to the decision to carve the original exfiltrated files from Wireshark to reveal the hidden message.

All six files were inspected, and it was determined that the files labeled with numbers 1, 2, and 3 were seemingly encrypted, while the others explicitly stated that they were not to be decoded.



Starting with the file with "1," decoding was attempted using CyberChef's "From Base64" operation. This successfully revealed a message that provided hints for decoding the next file.



The message from the first file hinted at a common decoding function involving a logical expression using XOR. To facilitate the decoding process, the file was brute-forced using dcode.fr, which eventually provided clues for the third file. These clues directed attention towards finding an anime reference and a specific character's name.

```

    _But m@ke sure yeu kn0w where
    th0 re@d@ble text dn the key the
3230323032 @;lme ls fr0m.
3032303265 --x
3230323032 The catchphras0 of the renowned
30 and famous Chu nibyou.

    You kn:w their alter e2o: _ _ _
    _ _ _
    _That's the lasto password or
    ke,? A Proper nameufor the Lord
    ofuEminence.

    Hello,there.

    The Magic (Password) key ls:
    !(1@m@t0mlc)!

    But m@ke sure y0u kn0w where the
    re@d@ble text ln the key the
    @nlme ls fr0m.
3230323032 ---
3032303230
32303230
    The catchphrase of the renowned
    and famous Chuunibyou.

    You know their alter ego: _ _ _
    _ _ _
    That's the last: password or
    key? A Proper name for the Lord
    of Eminence.

```

To gather the necessary information, consultation with ChatGPT, YouTube, and extensive searches on good ol' Google were conducted.

Hello! Here.

The Magic (Password) key is:
(t@mgr@0m1c!)

But m@ke sure you kn0w where the re@d@ble text in the key the @nrlme ls fr0m.

The catchphrase of the renowned and famous Chuunibyou.

You know their alter ego:

That's the last: password or key? A Proper name for the Lord of Eminence.

The readable text in the provided key "t@mgr@0m1c!" is "t@mgr@0m1c," which is derived from the catchphrase of the renowned and famous Chuunibyou. Chuunibyou is a term used to describe individuals, usually adolescents, who have delusions of grandeur and pretend to possess special powers or abilities. The catchphrase often associated with Chuunibyou is "I am atomic" or "Atomic."

As for the last part of your message, it is not clear what you mean by "A Proper name for the Lord of Eminence." Could you please provide more context or clarification?

maybe its related to the anime

Apologies for the confusion. If you're referring to a proper name for the Lord of Eminence related to an anime, it's possible that you are referring to a specific character or title within an anime series. However, without further context or specific information, I'm unable to provide a precise answer. If you can provide more details or clarify your question, I'll do my best to assist you.

[Regenerate response](#)

[Send a message](#)

Main Chronology Relationships Image Gallery

" The time of the games it's over. "

Shadow to his enemies, Anime

Cid Kagenō (シド・カゲノー, Shido Kagenō), formerly Minoru Kaō Search this wiki Search all wikis f v o Eminence in Shadow series. He is the leader of the secret organization Shadow Garden under the moniker Shadow, which he founded to live out his chūnibyō fantasies, unaware that his Imaginary enemies actually exist.

Contents [hide]

1. Appearance
- 1.1. Cid Kagenō
- 1.2. Shadow
- 1.3. Mundane Mann
- 1.4. John Smith
- 1.5. Minoru Kagenō

Cid Kagenō

Cid Shadow Minoru Mundane Mann Light Novel Manga Anime

Eventually, a matching XOR key for the third file was discovered, enabling its decoding. The decoded content of the third file revealed the flag.

The obtained flag, after successfully decoding the hidden message, is: flag{C0ngr@tum4l4t!0ns!!!}.

The screenshot shows the dCode.fr/xor-cipher website. On the left, there's a search bar and a sidebar with various tools like XOR Cipher, dCode and more. The main area displays the XOR Cipher tool with the following details:

XOR CIPHER
Cryptography - Modern Cryptography - XOR Cipher

Superior web hosting.
Fast, reliable and stable hosting at a great price with GoDaddy.com [Shop Now](#)

XOR DECODER
TEXT TO BE XORED (MULTIPLIED BY XOR)
Hexadecimal ASCII [00-7F] (Automatic Detection)

09 05 16 54 35 44 27 2c 2d 23 58 19 30 03 23 54 0b 20 63 58
03 20 3d 47 1a 3c 23 11 0e 0e 16 00 28 3c 5e 4a

ENCRYPTION/DECRYPTION METHOD

- AUTOMATIC (Bruteforce 1 to 16 bytes) ⓘ
- USE THE BINARY KEY: 10110111
- USE THE HEXADECIMAL KEY: 7F
- USE THE ASCII KEY: Shadow
- KNOWING THE KEY SIZE (N BYTES): 1

RESULTS FORMAT ASCII (PRINTABLE) CHARACTERS

- HEXADECIMAL: 00-7F FF
- DECIMAL: 0-127-255
- OCTAL: 000-177-377
- BINARY: 00000000-11111111
- INTEGER NUMBER
- FILE TO DOWNLOAD

CRYPTANALYSIS
 SEARCH FOR KEY SIZE (N BYTES)

See also: Binary Code – ASCII Code – Boolean Expressions Calculator

XOR CALCULATOR
 BINARY NUMBER / MESSAGE 1

The screenshot shows the CyberChef interface with the following configuration:

Operations

- Search...
- Favourites
- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic
- XOR
- Swap case

Recipe

From Base64

Alphabet: A-Za-z0-9%+/=

Remove non-alphabet chars Strict mode

Input

Zmw0Z3tDMG5nckB0dW0bDR0ITBucyEhIX0=

Output

f14g{C0ngr@tum4l4t!0ns!!!}

STEP **BAKE!** Auto Bake

III. References

Pequalsnp-Team. (n.d.). Writing Good Writeups. Retrieved from <https://pequalsnp-team.github.io/cheatsheet/writing-good-writeup>

Sumo Logic. (n.d.). Threat Labs: MSDT Vulnerability. Retrieved from <https://www.sumologic.com/blog/threat-labs-msdt-vulnerability/>

Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT). (2022, May 31). Security Bulletin: Microsoft Products Remote Code Execution Vulnerability. Retrieved from https://www.hkcet.org/security-bulletin/microsoft-products-remote-code-execution-vulnerability_20220531