Abdelrhman

CTF Player, Digital Forensics, SOC

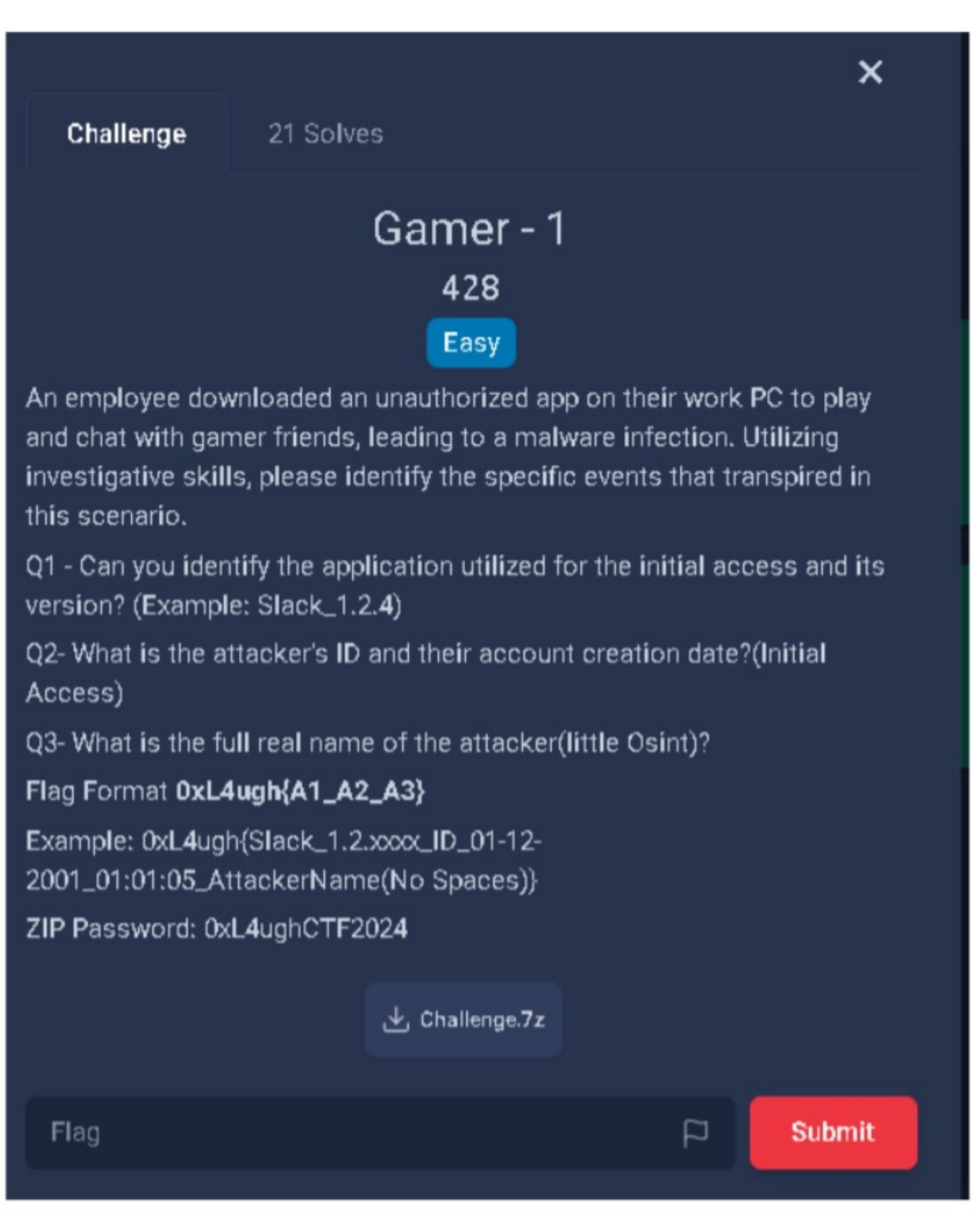
0xl4ugh2024

Posted **Feb 10, 2024** • Updated **Feb 10, 2024**

By **Abdelrhman Mohamed**   1 min read

I participated in the 0xl4ugh2024 I solved all forensics challenge,and this is my write-up for most forensics challenges

Gamer - 1



Challenge   21 Solves

Gamer - 1
428
Easy

An employee downloaded an unauthorized app on their work PC to play and chat with gamer friends, leading to a malware infection. Utilizing investigative skills, please identify the specific events that transpired in this scenario.

Q1 - Can you identify the application utilized for the initial access and its version? (Example: Slack_1.2.4)

Q2- What is the attacker's ID and their account creation date?(Initial Access)

Q3- What is the full real name of the attacker(little Osint)?

Flag Format **0xL4ugh{A1_A2_A3}**

Example: 0xL4ugh{Slack_1.2.xxxx_ID_01-12-2001_01:01:05_AttackerName(No Spaces)}

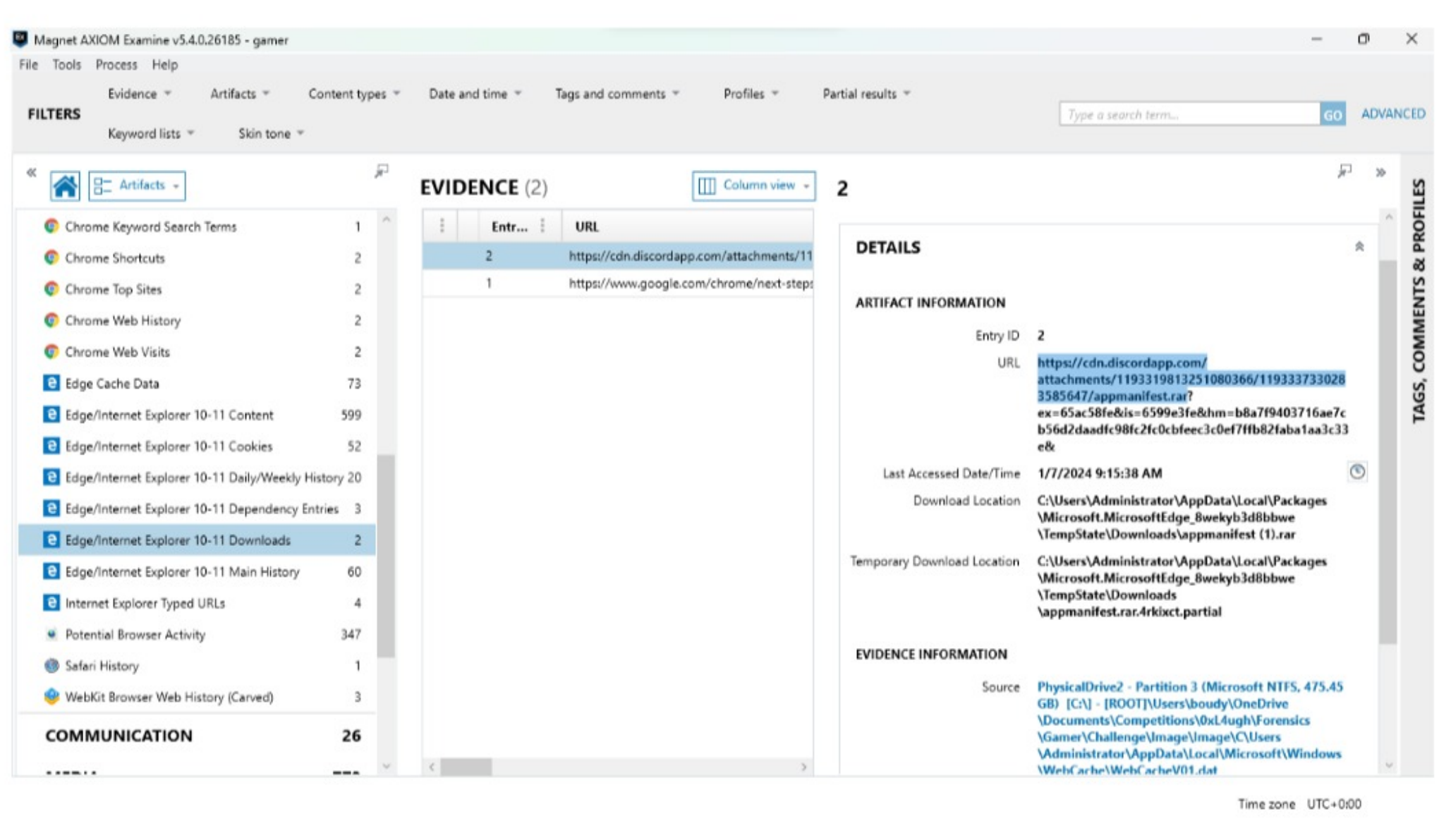
ZIP Password: 0xL4ughCTF2024

Challenge.7z

Flag   Submit

it's disk so i opened it with MagnetAxiom

in the challenge he said that `An employee downloaded an unauthorized app` so we will look for browser history



Magnet AXIOM Examine v5.4.0.26185 - gamer

EVIDENCE (2)

Entr...	URL
2	https://cdn.discordapp.com/attachments/11
1	https://www.google.com/chrome/next-steps

DETAILS

ARTIFACT INFORMATION

Entry ID 2

URL https://cdn.discordapp.com/attachments/1193319813251080366/1193337330283585647/appmanifest.rar?ex=65ac58fe&is=6599e3fe&hm=b8a7f9403716ae7cb56d2daadfc98fc2fc0cbfeec3c0ef7ffb82faba1aa3c33e&

Last Accessed Date/Time 1/7/2024 9:15:38 AM

Download Location C:\Users\Administrator\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\appmanifest (1).rar

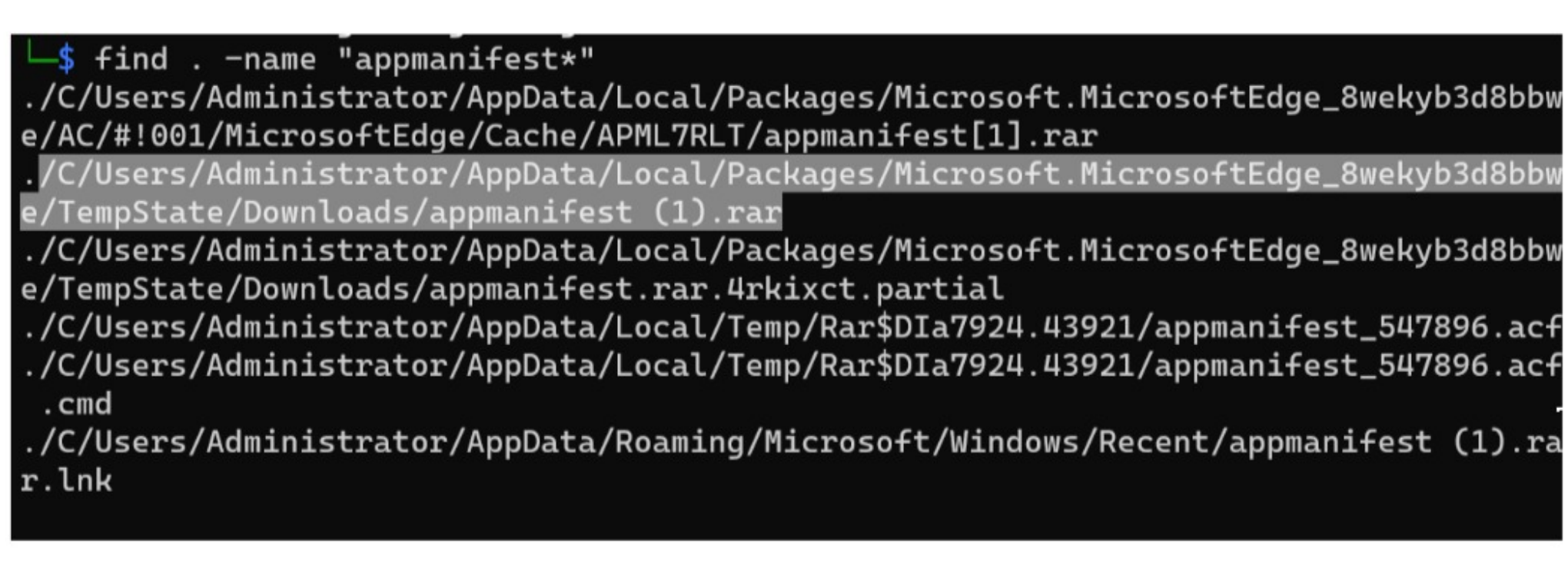
Temporary Download Location C:\Users\Administrator\AppData\Local\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\TempState\Downloads\appmanifest.rar.4rkixct.partial

EVIDENCE INFORMATION

Source PhysicalDrive2 - Partition 3 (Microsoft NTFS, 475.45 GB) [C:\] - [ROOT]\Users\boudy\OneDrive\Documents\Competitions\0xL4ugh\Forensics\Gamer\Challenge\Image\Image\C\Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

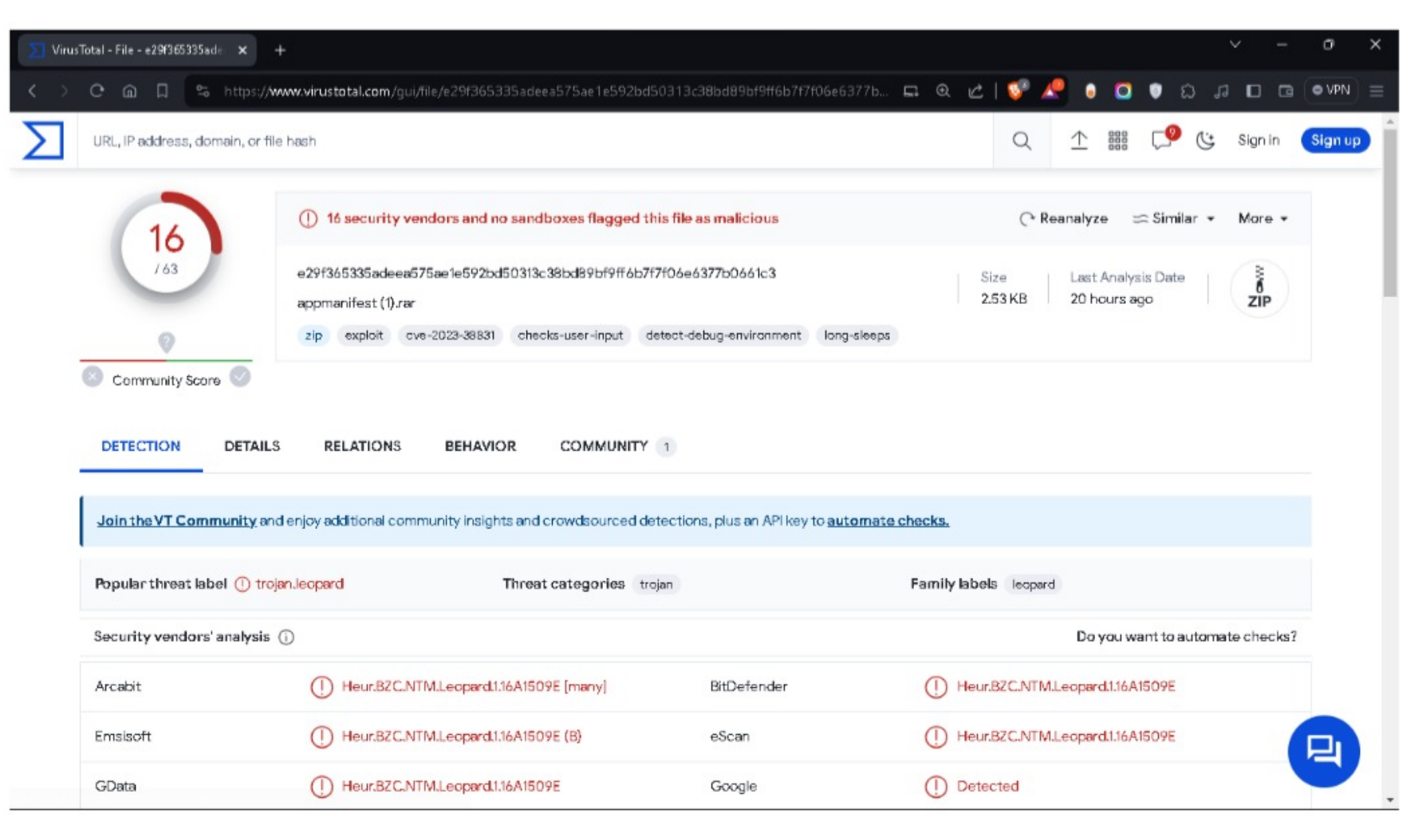
Time zone UTC+0:00

so we look we found that there is suspicous .rar file downloaded from disord we know that it's name is `appmanifest.rar` so let's search about it in disk `find . -name "appmanifest*"`



```
└─$ find . -name "appmanifest*"
./C/Users/Administrator/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbw
e/AC/#!001/MicrosoftEdge/Cache/APML7RLT/appmanifest[1].rar
./C/Users/Administrator/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbw
e/TempState/Downloads/appmanifest (1).rar
./C/Users/Administrator/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbw
e/TempState/Downloads/appmanifest.rar.4rkixct.partial
./C/Users/Administrator/AppData/Local/Temp/Rar$DIa7924.43921/appmanifest_547896.acf
./C/Users/Administrator/AppData/Local/Temp/Rar$DIa7924.43921/appmanifest_547896.acf
 .cmd
./C/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/appmanifest (1).ra
r.lnk
```

so we found it let's calculate it's hash `sha256sum appmanifest (1).rar` we found `e29f365335adeea575ae1e592bd50313c38bd89bf9ff6b7f7f06e6377b0661c3` now upload it to virus total to see it's have malware or not #



VirusTotal - File - e29f365335ade

16 / 63

16 security vendors and no sandboxes flagged this file as malicious

e29f365335adeea575ae1e592bd50313c38bd89bf9ff6b7f7f06e6377b0661c3
appmanifest (1).rar

zip exploit cve-2023-38831 checks-user-input detect-debug-environment long-sleeps

Size 2.53 KB   Last Analysis Date 20 hours ago

DETECTION   DETAILS   RELATIONS   BEHAVIOR   COMMUNITY 1

Popular threat label trojan.leopard   Threat categories trojan   Family labels leopard

Security vendors' analysis

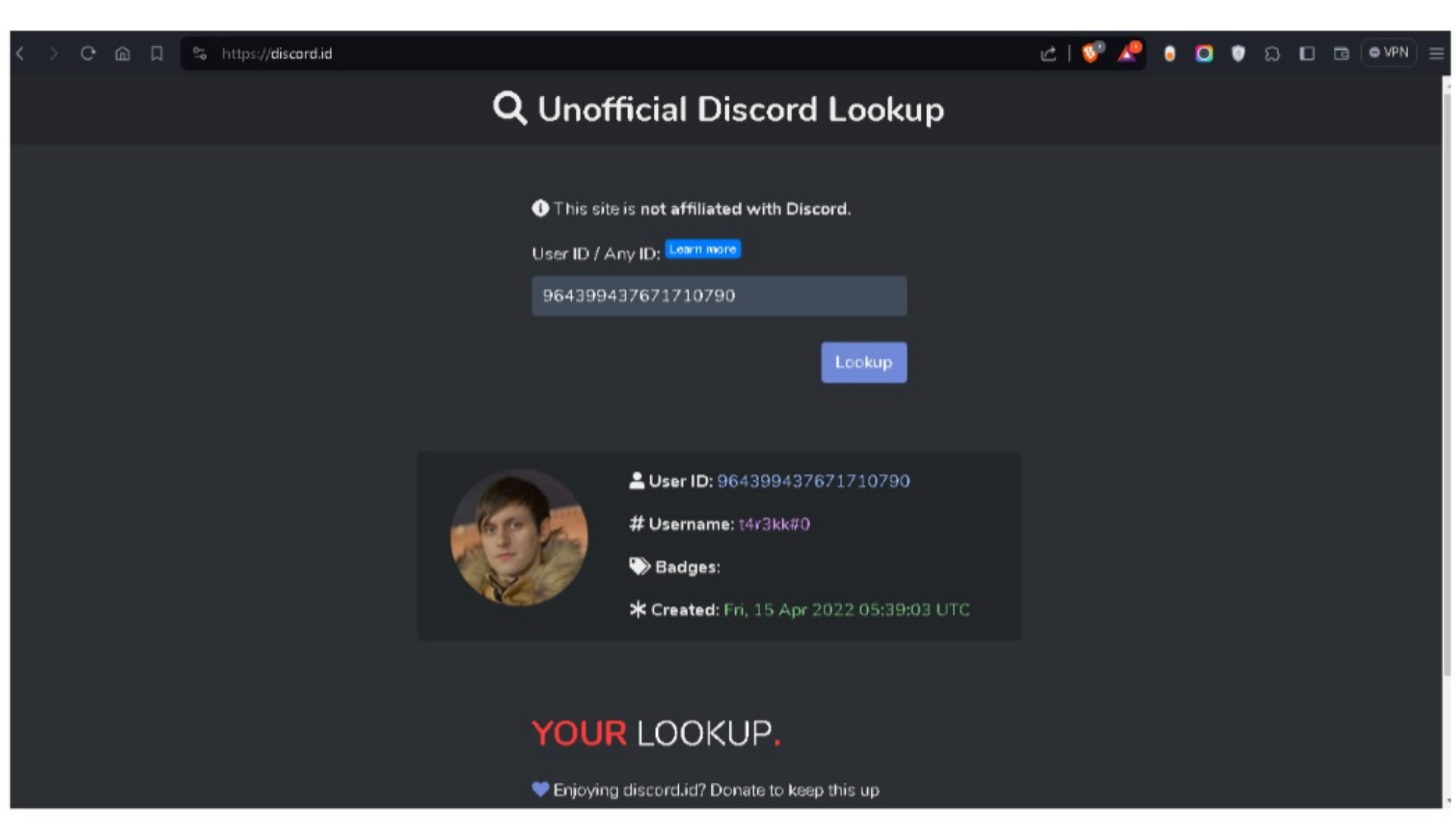
Arcabit	Heur.BZC.NTM.Leopard.1.16A1509E [many]	BitDefender	Heur.BZC.NTM.Leopard.1.16A1509E
Emsisoft	Heur.BZC.NTM.Leopard.1.16A1509E (B)	eScan	Heur.BZC.NTM.Leopard.1.16A1509E
GData	Heur.BZC.NTM.Leopard.1.16A1509E	Google	Detected

so we know know that it's malicious and we got cve of it `cve-2023-38831` now we know that this is attacker sent it in discord and it have malware we will analyze it later

now we need to analyze discord cache file this link helped me so i downloaded this tool and i opened cache file in this program and extract all files by click `ctr a and then press f4` and then i opened `50.json` file

```
al_name":"anani","avatar_decoration_data":null,"banner_color":null},"attachments":[],"embeds":[],"mentions":
[],"mention_roles":[],"pinned":false,"mention_everyone":false,"tts":false,"timestamp":"2024-01-06T23:38:04.
207000+00:00","edited_timestamp":null,"flags":0,"components":[]},{"id":"1193337528015654932","type":0,"cont
ent":"wasn't able to upload the file directly, so i compressed for
u","channel_id":"1193319813251080366","author":{"id":"964399437671710790","username":"t4r3kk","avatar":"e8b
e11c5ad1cac6d3ffc85f6b72a4ace","discriminator":"0","public_flags":0,"premium_type":0,"flags":0,"banner":nul
l,"accent_color":null,"global_name":"dark","avatar_decoration_data":null,"banner_color":null},"attachments":
[],"embeds":[],"mentions":[],"mention_roles":[],"pinned":false,"mention_everyone":false,"tts":false,"timest
amp":"2024-01-06T23:37:17.818000+00:00","edited_timestamp":null,"flags":0,"components":[]},{"id":"119333733
0455560204","type":0,"content":"","channel_id":"1193319813251080366","author":{"id":"964399437671710790","u
sername":"t4r3kk","avatar":"e8be11c5ad1cac6d3ffc85f6b72a4ace","discriminator":"0","public_flags":0,"premium
_type":0,"flags":0,"banner":null,"accent_color":null,"global_name":"dark","avatar_decoration_data":null,"ba
nner_color":null},"attachments":[{"id":"1193337330283585647","filename":"appmanifest.rar","size":2586,"url":
"https://cdn.discordapp.com/attachments/1193319813251080366/1193337330283585647/appmanifest.rar?ex=65ac58fe
&is=6599e3fe&hm=b8a7f9403716ae7cb56d2daadfc98fc2fc0cbfeec3c0ef7ffb82faba1aa3c33e&","proxy_url":"https://med
ia.discordapp.net/attachments/1193319813251080366/1193337330283585647/appmanifest.rar?ex=65ac58fe&is=6599e3
fe&hm=b8a7f9403716ae7cb56d2daadfc98fc2fc0cbfeec3c0ef7ffb82faba1aa3c33e&","content_type":"application/vnd.ra
r","content_scan_version":0}],"embeds":[],"mentions":[],"mention_roles":[],"pinned":false,"mention_everyone
":false,"tts":false,"timestamp":"2024-01-06T23:36:30.716000+00:00","edited_timestamp":null,"flags":0,"compo
nents":[]},{"id":"1193337056592670750","type":0,"content":"lemme show u a sample of it
wait","channel_id":"1193319813251080366","author":{"id":"964399437671710790","username":"t4r3kk","avatar":"
```

now we know that t4r3kk who sent the malicious .rar file to the victim we need to know create time for this user so we use this website and put id `964399437671710790`



https://discord.id

Unofficial Discord Lookup

This site is not affiliated with Discord.

User ID / Any ID: 964399437671710790

Lookup

User ID: 964399437671710790
Username: t4r3kk#0
Badges:
Created: Fri, 15 Apr 2022 05:39:03 UTC

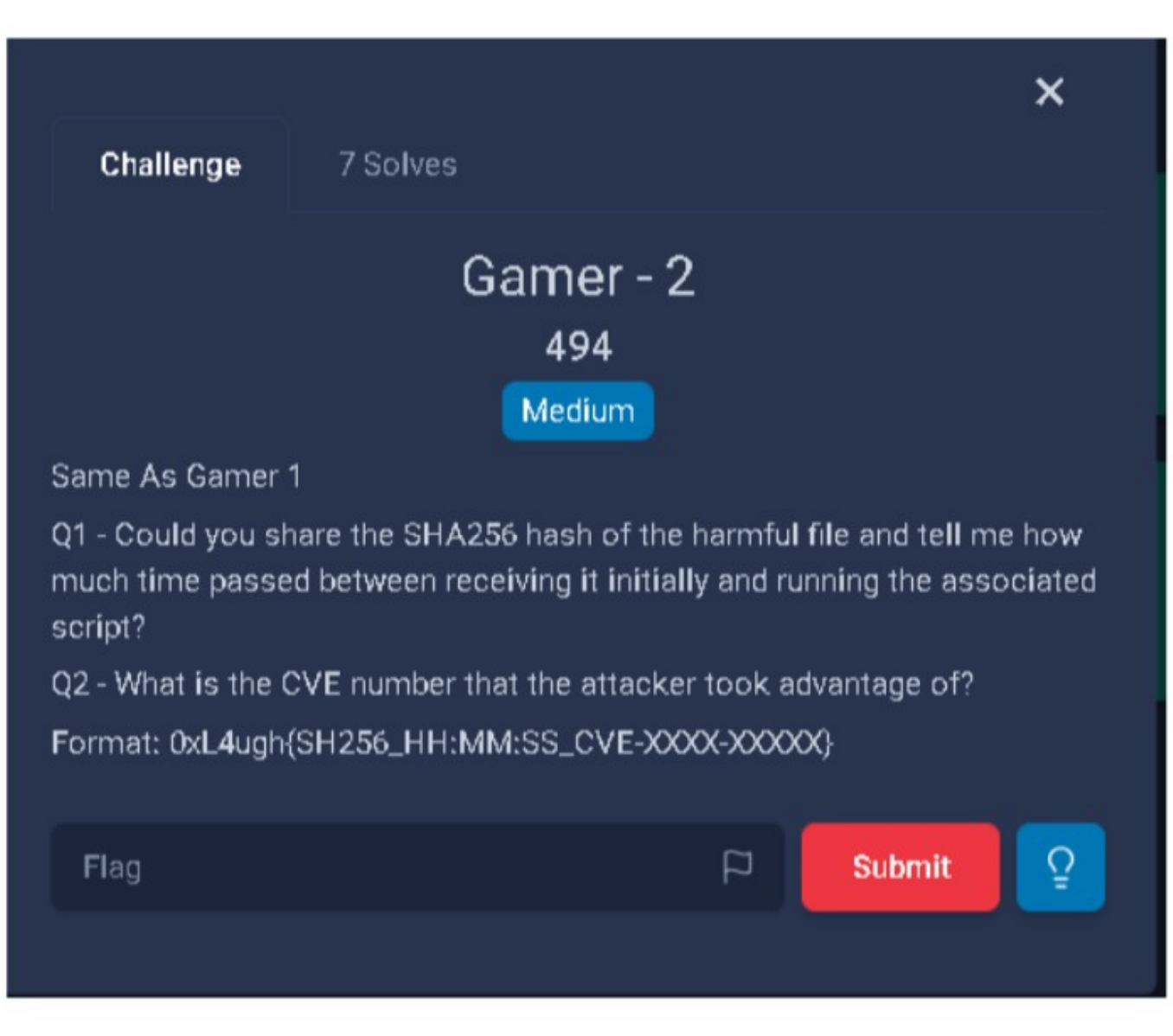
YOUR LOOKUP.

Enjoying discord.id? Donate to keep this up

now we know creation date and id and i did some osint i got the real name of attacker

flag: `0xL4ugh{Discord_1.0.9028_964399437671710790_15-04-2022_05:39:03_IgorDekhtyarchuk}`

Gamer - 2



Challenge   7 Solves

Gamer - 2
494
Medium

Same As Gamer 1

Q1 - Could you share the SHA256 hash of the harmful file and tell me how much time passed between receiving it initially and running the associated script?

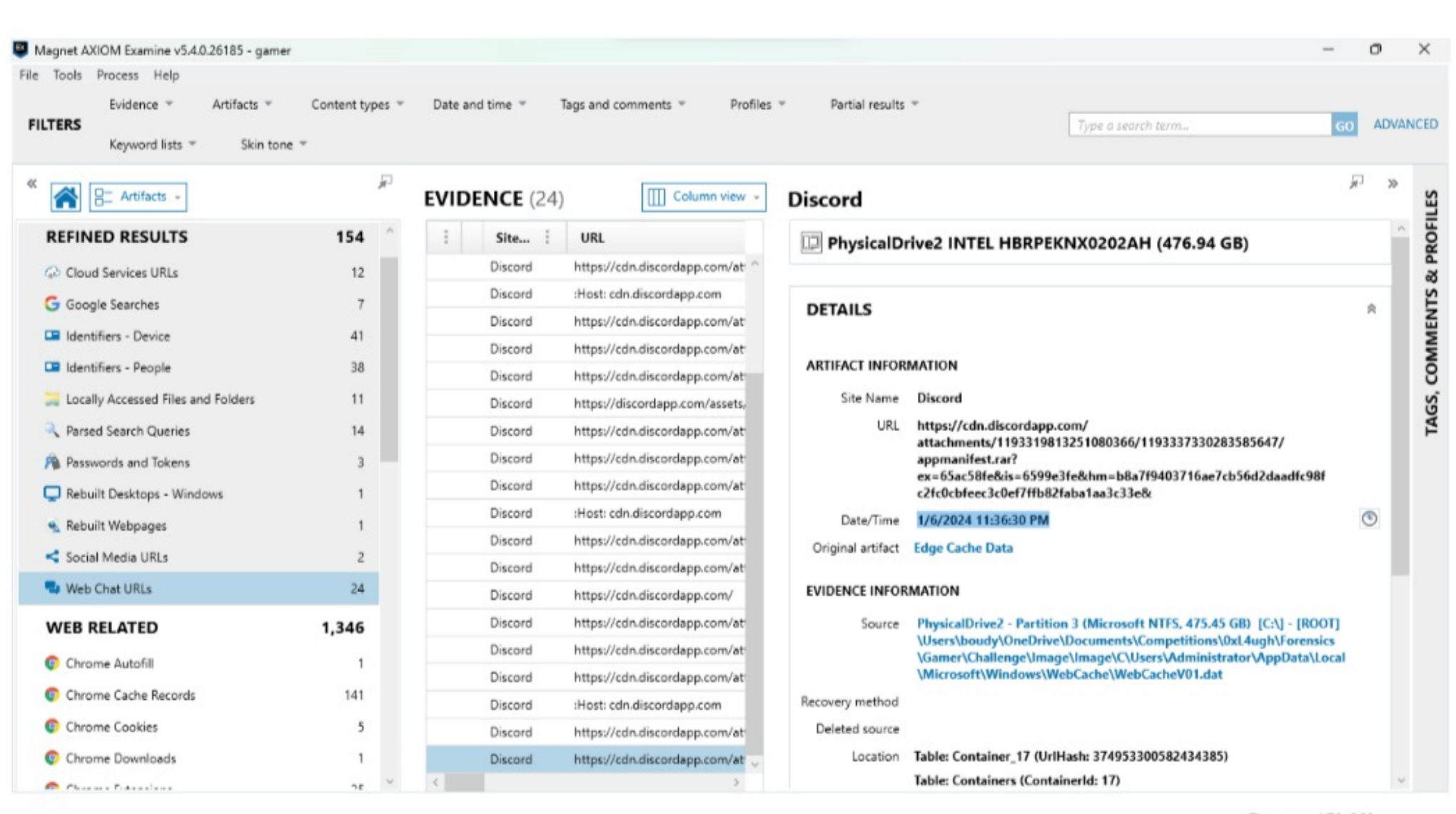
Q2 - What is the CVE number that the attacker took advantage of?

Format: 0xL4ugh{SH256_HH:MM:SS_CVE-XXXX-XXXXX}

Flag   Submit

now here we know sha256 of file and we know the cve we got in first question so now we need to know when this is .rar is installed in the system

this is the first time the file is downloaded to system



Magnet AXIOM Examine v5.4.0.26185 - gamer

EVIDENCE (24)   Discord

PhysicalDrive2 INTEL HBRPEKNX0202AH (476.94 GB)

DETAILS

ARTIFACT INFORMATION

Site Name Discord

URL https://cdn.discordapp.com/attachments/1193319813251080366/1193337330283585647/appmanifest.rar?ex=65ac58fe&is=6599e3fe&hm=b8a7f9403716ae7cb56d2daadfc98fc2fc0cbfeec3c0ef7ffb82faba1aa3c33e&

Date/Time 1/6/2024 11:36:30 PM

Original artifact Edge Cache Data

EVIDENCE INFORMATION

Source PhysicalDrive2 - Partition 3 (Microsoft NTFS, 475.45 GB) [C:\] - [ROOT]\Users\boudy\OneDrive\Documents\Competitions\0xL4ugh\Forensics\Gamer\Challenge\Image\Image\C\Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat

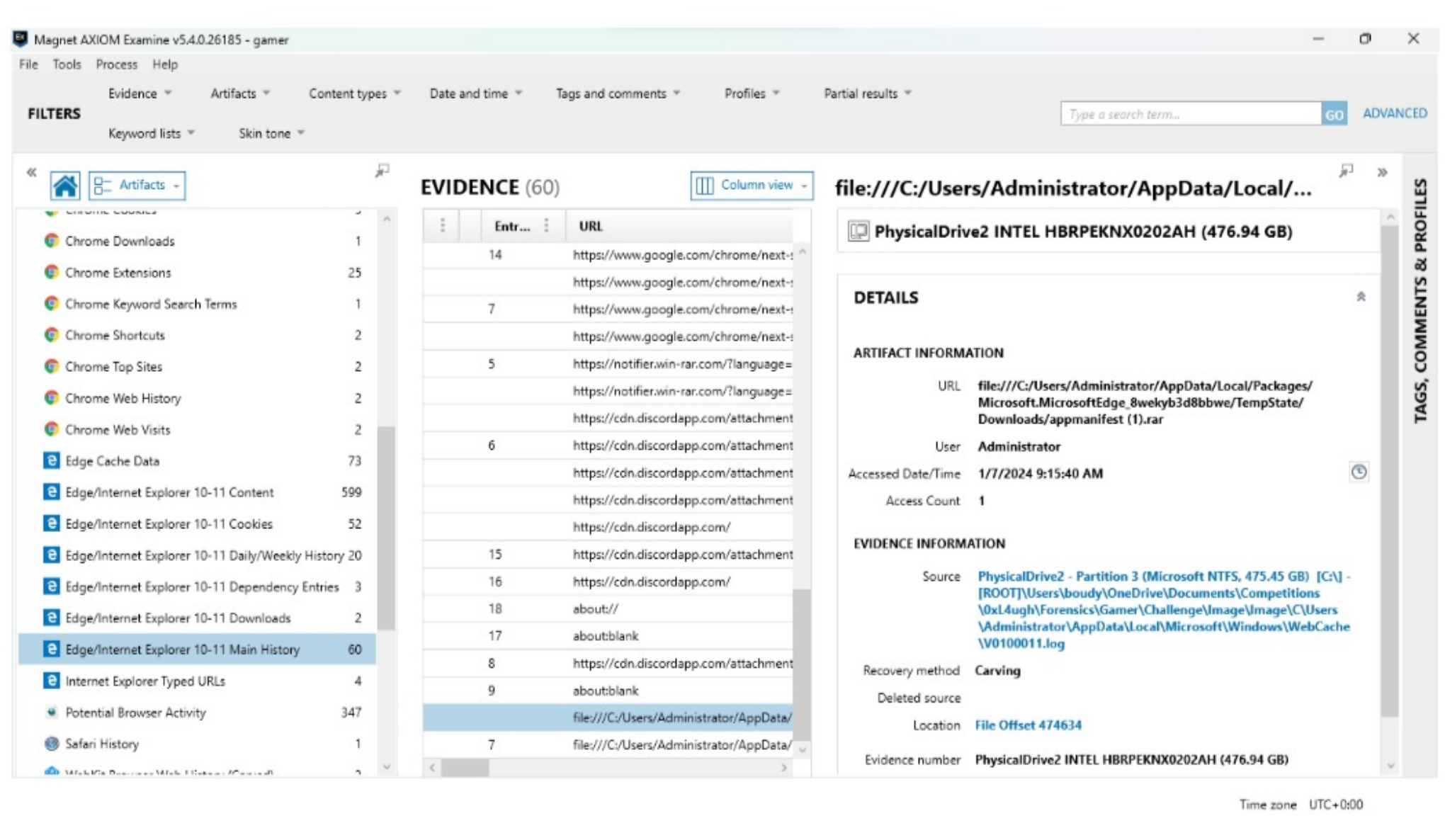
Recovery method

Deleted source

Location Table: Container_17 (UrlHash: 374953300582434385)
Table: Containers (ContainerId: 17)

Time zone UTC+0:00

and the first time it executed



Magnet AXIOM Examine v5.4.0.26185 - gamer

EVIDENCE (60)   file:///C:/Users/Administrator/AppData/Local/...

PhysicalDrive2 INTEL HBRPEKNX0202AH (476.94 GB)

DETAILS

ARTIFACT INFORMATION

URL file:///C:/Users/Administrator/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/appmanifest (1).rar

User Administrator

Accessed Date/Time 1/7/2024 9:15:40 AM

Access Count 1

EVIDENCE INFORMATION

Source PhysicalDrive2 - Partition 3 (Microsoft NTFS, 475.45 GB) [C:\] - [ROOT]\Users\boudy\OneDrive\Documents\Competitions\0xL4ugh\Forensics\Gamer\Challenge\Image\Image\C\Users\Administrator\AppData\Local\Microsoft\Windows\WebCache\V0100011.log

Recovery method Carving

Deleted source

Location File Offset 474634

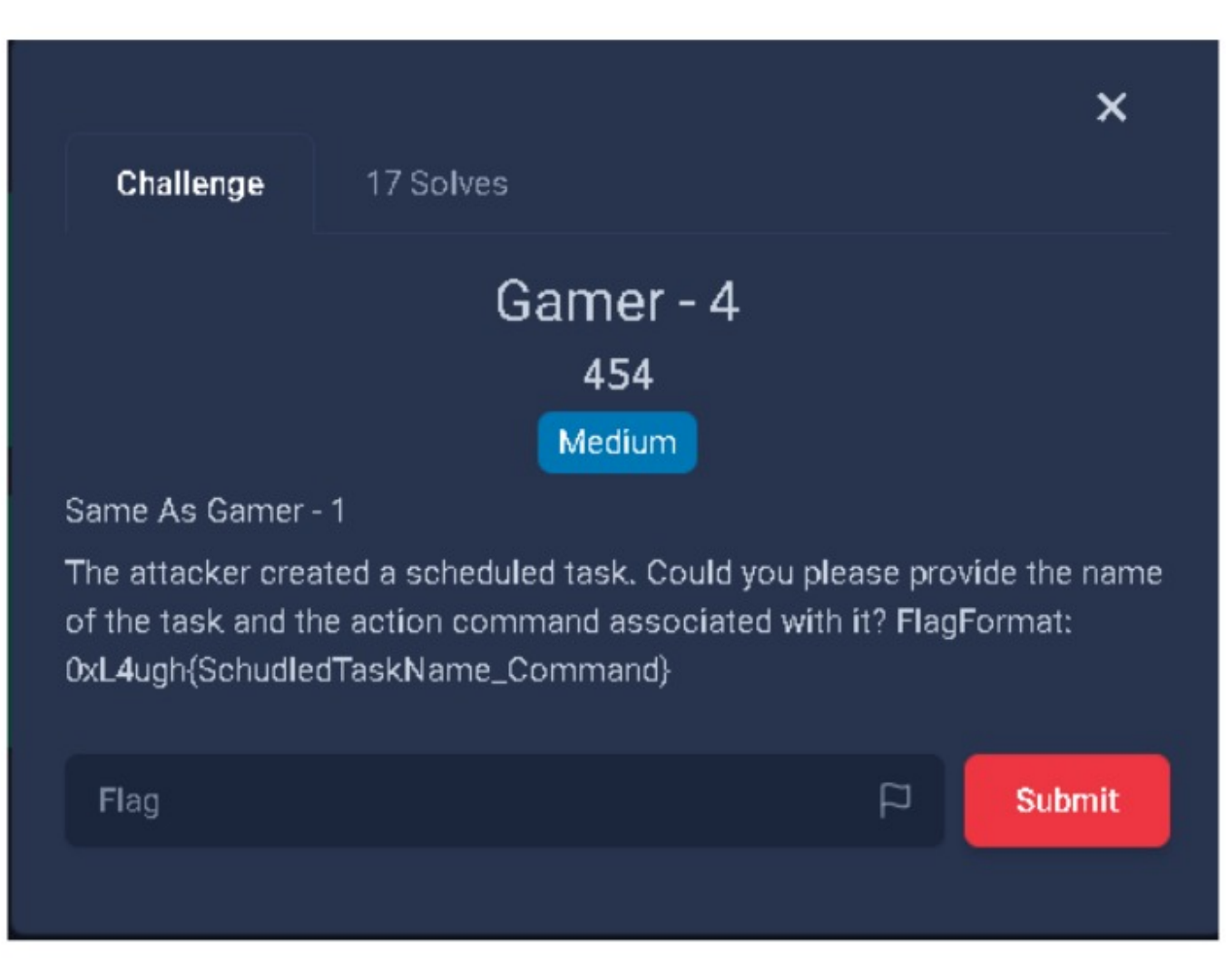
Evidence number PhysicalDrive2 INTEL HBRPEKNX0202AH (476.94 GB)

Time zone UTC+0:00

now date_of_execution - date_of_downloading

flag: `0xL4ugh{e29f365335adeea575ae1e592bd50313c38bd89bf9ff6b7f7f06e6377b0661c3_09:39:44_CVE-2023-38831}`

Gamer - 4



Challenge   17 Solves

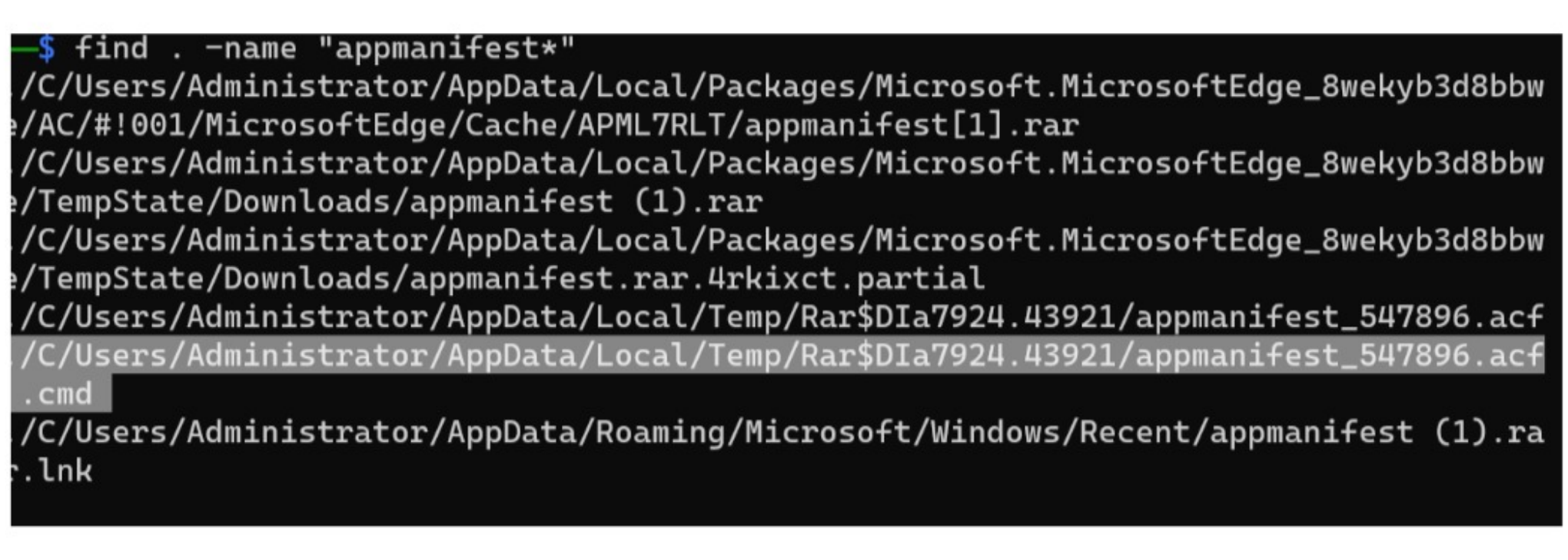
Gamer - 4
454
Medium

Same As Gamer - 1

The attacker created a scheduled task. Could you please provide the name of the task and the action command associated with it? FlagFormat: 0xL4ugh{SchudledTaskName_Command}

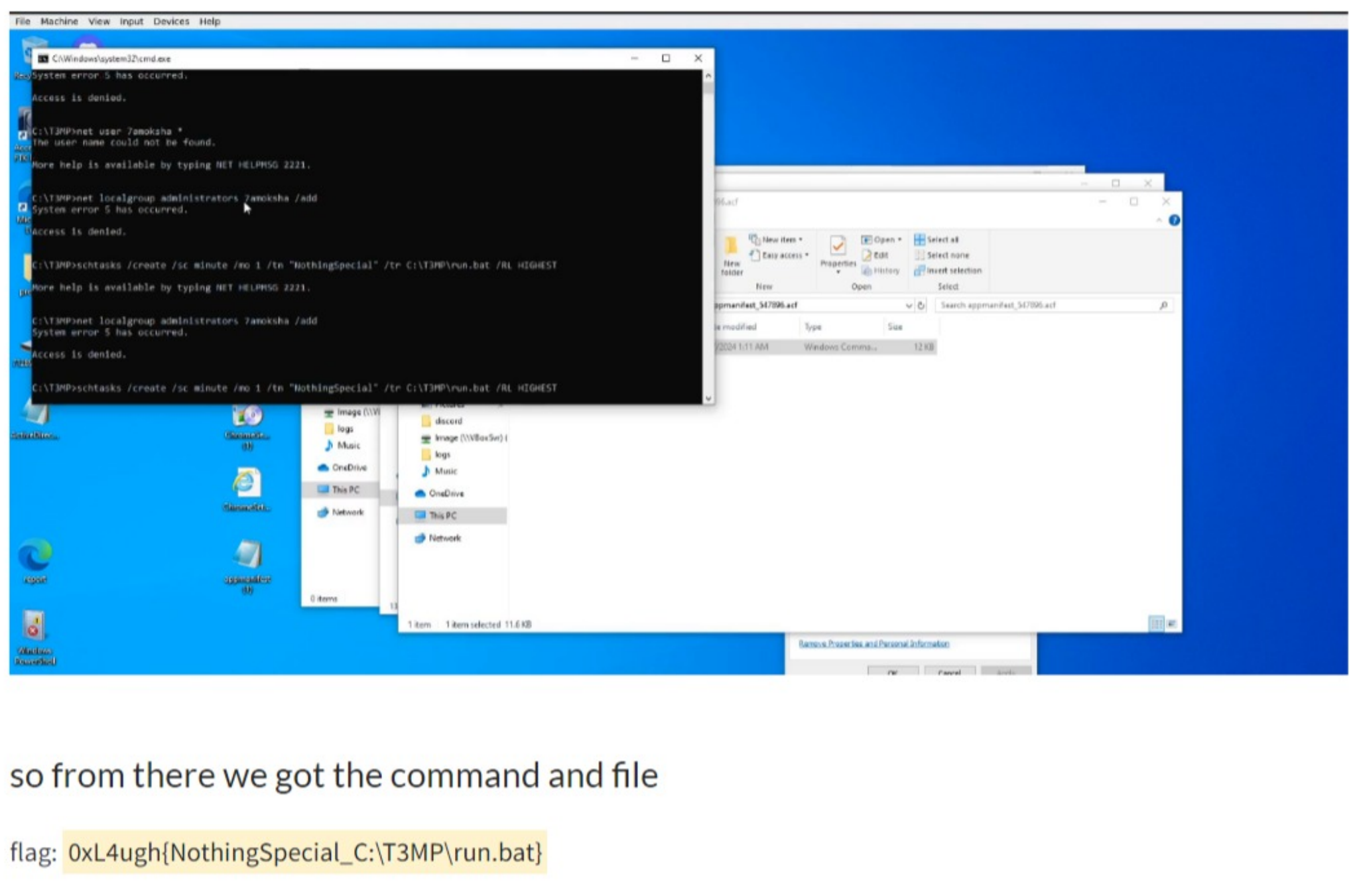
Flag   Submit

ok when we searched about malware with `find . -name "appmanifest*"` we found suspicious file



```
─$ find . -name "appmanifest*"
./C/Users/Administrator/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbw
e/AC/#!001/MicrosoftEdge/Cache/APML7RLT/appmanifest[1].rar
./C/Users/Administrator/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbw
e/TempState/Downloads/appmanifest (1).rar
./C/Users/Administrator/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbw
e/TempState/Downloads/appmanifest.rar.4rkixct.partial
./C/Users/Administrator/AppData/Local/Temp/Rar$DIa7924.43921/appmanifest_547896.acf
./C/Users/Administrator/AppData/Local/Temp/Rar$DIa7924.43921/appmanifest_547896.acf
.cmd
./C/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/appmanifest (1).ra
r.lnk
```

so i run this script in the virtual machine windows



```
System error 5 has occurred.

Access is denied.

C:\T3MP>net user 7amoksha *
The user name could not be found.

More help is available by typing NET HELPMSG 2221.

C:\T3MP>net localgroup administrators 7amoksha /add
System error 5 has occurred.

Access is denied.

C:\T3MP>schtasks /create /sc minute /mo 1 /tn "NothingSpecial" /tr C:\T3MP\run.bat /RL HIGHEST

More help is available by typing NET HELPMSG 2221.

C:\T3MP>net localgroup administrators 7amoksha /add
System error 5 has occurred.

Access is denied.

C:\T3MP>schtasks /create /sc minute /mo 1 /tn "NothingSpecial" /tr C:\T3MP\run.bat /RL HIGHEST
```

so from there we got the command and file

flag: `0xL4ugh{NothingSpecial_C:\T3MP\run.bat}`

Forensics

task schedule   cve   disk   discord

Share:

Further Reading

Jan 15, 2024

UofTCTF

I participated in the UofTCTF 2024 I solved all forensics challenge,and th…

OLDER
UofTCTF

NEWER
-

Using the **Chirpy** theme for **Jekyll**.

Recently Updated

0xl4ugh2024
UofTCTF

Trending Tags

task schedule   backdoor   crypto   cve   discord   disk   firmware   network   pdf   trevorc2

Contents