OpTinselTrace24-5: Tale of Maple Syrup

Story:
Twinkle Snowberry who works as chief decorator in Santa's workshop for years is suspected of assisting Krampus and his notorious Cyber group. Word is he has been having arguments with Santa for months. The most unfortunate thing finally happened, Santa's Workstation was ransomed. Twinkle's Company owned phone is seized and a forensics acquisition is taking place to identify the suspicious activity.

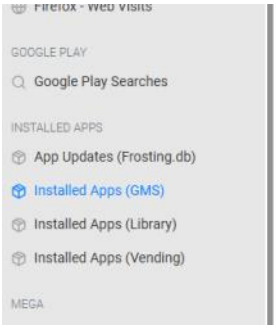
Task1: Identifying IOCs, accounts, or infrastructure is crucial for detecting breaches by attackers. Determine the email address used by the threat actor so it can be added to Santa's threat intel feed.

- At first, I used ALeAPP to parse all the Andorid logs, in HTML, we found the user downloaded MEGA application and chatted with **'krampusevilson@yahoo.com'** which is probably the TA.

2024-11-05 15:09:26		Chat Message	Yeah I know him. He is visiting Northpole to setup his access. I saw him downloaded apps just now. If he will be mostly working remotely from southpole as his wife is sick.
2024-11-05 15:12:39	krampusevilson@yahoo.com	Chat Message	HO HO HO !!!
2024-11-05 15:13:04	krampusevilson@yahoo.com	Chat Message	Thats good. My operators are just about to send him a phishing email.
2024-11-05 16:03:12	krampusevilson@yahoo.com	Chat Message	HAHHA
2024-11-05 16:04:02	krampusevilson@yahoo.com	Chat Message	Your Dev is so dumb!! His password was cracked in 1minute. I did not expect that. My cyber team is currently on his system and trying to move laterally to more interesting machines
2024-11-05 16:39:16	krampusevilson@yahoo.com	Chat Message	We have successfully infiltrated the northpole workshop. We will be sitting low for atleast 1 day as we already have possibly made enough noise
2024-11-14 03:29:57		Chat Message	Hello. These past few days have been hectic with all the chaos going on due to you hacking into Santa's workshop
2024-11-14 03:30:23		Chat Message	So far no one suspects me and i stopped using the phone to stay low
2024-11-14 03:30:34		Chat Message	When will you send my remaining money?

Task2: Which application was used by the insider threat to communicate with the threat actor? Please provide the application's Android package name.

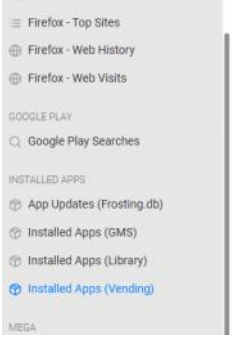
- I found the answer in the 'Install APPs' section, the answer is **'mega.privacy.android.app'**



Bundle ID	Version Code	SHA-256 Hash
com.google.android.contacts	3198795	3306f4b43ac7bb60762a0d4c8a735c753949f6897287d8ca07feb28de7d53745
com.google.android.contacts	3200547	5dd40f4554c48989c705a520b51c91a52a686b781456dc61e3a2d163342929fe
com.google.android.keep	220585163	e010b5c84b4e8d2bbf16ce216f3b8ddc8ca41b7ec748c39ff531afbaaf16537a
com.google.android.keep	220586162	3899306683a0dd296d71cc3c25b0d1c0a214a00948d8304794716b4c70bdd3ae
com.google.android.partnersetup	1997	c46cb66b828397181a4819da2e8698b5cd3415229883ea0a0d70952c27d167fc
mega.privacy.android.app	242890903	27a499b89a30550cf92f32240421c1be2926897289b437a94c73b94b8072cf82
org.mozilla.firefox	2016051567	4e55737fe9a28bbc2c1b93666339c30689b8402ed0708a73784fabeade1ac6c2
org.mozilla.firefox	2016055415	205b77c905affadd13e10d4354a79cc66acf8121782215c384b16d95d80e11c7

Task3: When was this application installed on the device?

- The application first downloaded at **'2024-11-04 11:24:28'**, we found the answer in Installated Apps (Vending) section via Aleapp.

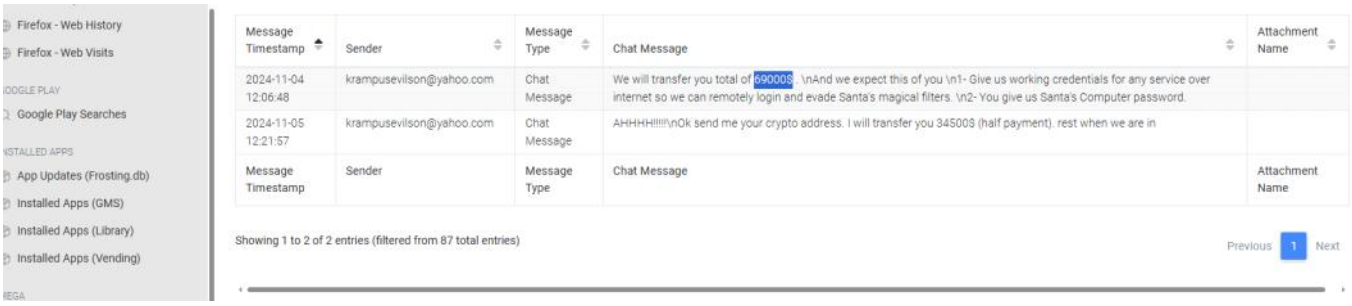


First Download	Package Name	Title	Install Reason	Last Upd
2024-11-04 11:15:36	com.google.android.gms		unknown	2024-11-
2024-11-04 11:24:28	mega.privacy.android.app		unknown	
2024-11-04 11:24:40	org.mozilla.firefox		unknown	2024-11-
2024-11-04 11:24:49	com.google.android.keep		unknown	2024-11-
2024-11-04 12:55:49	com.google.android.apps.restore		unknown	2024-11-
2024-11-04 12:56:03	com.google.android.partnersetup		unknown	2024-11-
2024-11-04 12:56:09	com.google.android.contacts		unknown	2024-11-
First Download	Package Name	Title	Install Reason	Last Upd

Showing 1 to 7 of 7 entries

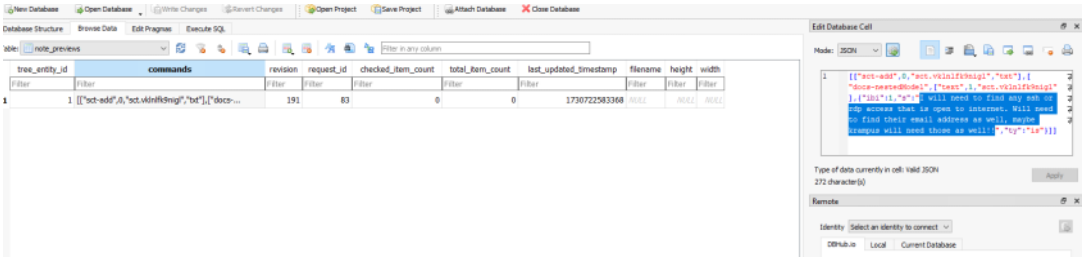
Task4: What is the agreed amount of money to be sent to the insider threat in exchange of him leaking Santa workshop's secrets?

- In the section of the MEGA chat, we found the amount of the money to be sent to the insider. The amount is '**69000$**'



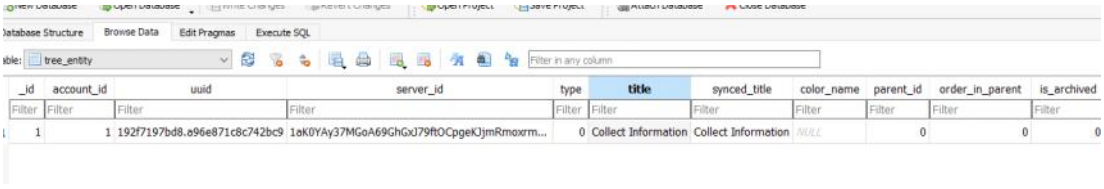
Task5: Twinkle created a note on his phone using a note-keeping app. What were the contents of the note?

- At first, we found that the user searched for "Google Keep" in the Google Play store, which is an application used to write notes. We located the directory for the application at C: \OPTT5-TRIAGE \data\com.google.android.keep\databases. We examined the Keep.db file, which contains the note the user saved.
  The note says: **"I will need to find any SSH or RDP access that is open to the internet. I will need to find their email address as well; maybe Krampus will need those as well!"**



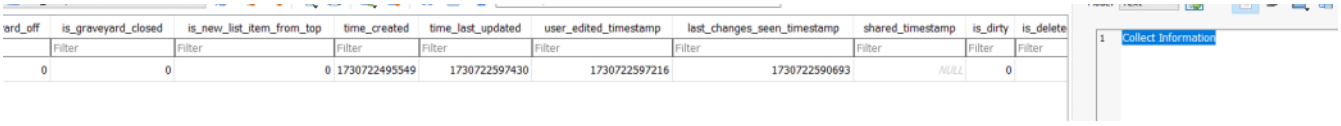
Task6: What is the title of this note?

- On the same database, on the 'tree-entiry' section we found the name of the note.
  The name is **'Collect Information'.**



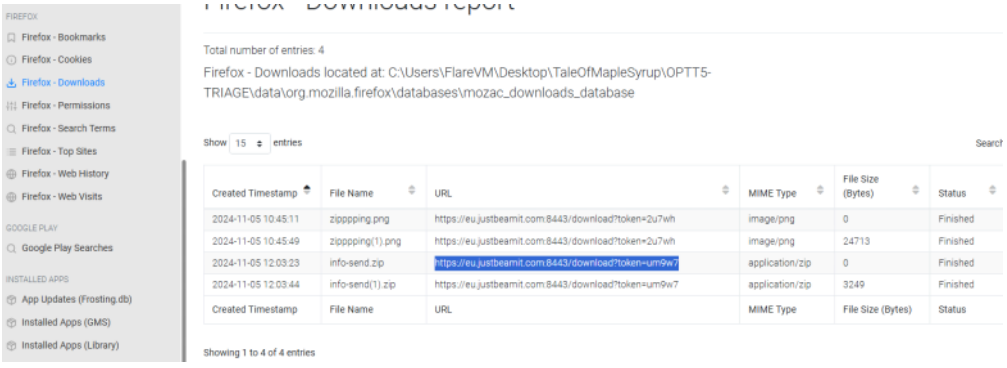
Task7: When was the note created in the note-keeping app?

- The timestamp also appears as Epoch timestamp, we convert it and found the answer,
  '2024-11-04 12:14:55'



Task8: Twinkle Snowberry transferred a few files from his workstation to his mobile phone using an online file transfer service. What is the URL used to download the zip file on the mobile phone?

- Via ALeAPP, we examined the firefox downloads and found the URL that Twinkle downloaded the ZIP file.
  The URL is 'https://eu.justbeamit.com:8443/download?token=um9w7'



Task9: When was this file shared with the threat actor by the insider, Twinkle Snowberry?

- To address this question, I searched the ZIP file in the Mega CHAT section and found that Twinkle sent the ZIP file at **'2024-11-05 12:04:24'**

Show 15 entries Search: zip

Message Timestamp	Sender	Message Type	Chat Message	Attachment Name
2024-11-05 10:47:55		Attachment		zippppping(1).png
2024-11-05 10:48:49	krampusevilson@yahoo.com	Chat Message	Now quit messing around and send me the zip file as well	
2024-11-05 12:04:24		Attachment		info-send(1).zip
2024-11-05 12:17:38	krampusevilson@yahoo.com	Chat Message	Whats the password of this zip?	
2024-11-05 12:40:14	krampusevilson@yahoo.com	Chat Message	I will try to crack the zip and find some way into the network	
2024-11-05 14:18:13	krampusevilson@yahoo.com	Chat Message	My team is currently preparing to social engineer one of your dev. It was clever of you including emails list in the zip. We conducted recon and found a potential Phishing victim. You would know "Bingle Jollybeard". We are targeting him as we speak	
Message Timestamp	Sender	Message Type	Chat Message	Attachment Name

Task10: Twinkle forgot the password of the archive file he sent to Krampus containing secrets. What was the password for the file?

- I discovered a ZIP file located at C:\OPTT5-TRIAGE\storage\self\primary\Download. Inside the Downloads folder, there was an image showing the ZIP encryption method, identified as 'ZipCrypto'. After researching tools to crack the ZIP password, I came across bkcrack, which can decrypt ZIP files without brute-force attacks.

  The command I used was:
  ./bkcrack -C ../../info-send\(1\).zip -c Emails.txt -p known.txt

  -c: A file already contained within the ZIP.
  -p: A known string present in the file inside the ZIP.

  In this case, I found a MEGA conversation in Emails.txt that mentioned a user named 'TwinkleSnowberry', so I created a file called known.txt and added the string 'TwinkleSnowberry' to it.
  Once I executed the command, the keys were successfully extracted and I decrypted the ZIP.

  In the question, we need to brute force to find the ZIP password after we found the keys.
  The password is

```
┌──(kali㉿kali)-[~/Desktop/bkcrack/build/src]
└─$ ./bkcrack -C '/home/kali/Desktop/info-send(1).zip' -c Emails.txt -p twinkle.txt
bkcrack 1.7.1 - 2024-12-21
[16:58:58] Z reduction using 9 bytes of known plaintext
100.0 % (9 / 9)
[16:58:58] Attack on 744070 Z values at index 6
Keys: cec26f80 cc8751a0 fdf67470
44.8 % (333074 / 744070)
Found a solution. Stopping.
You may resume the attack with the option: --continue-attack 333074
[17:06:26] Keys
cec26f80 cc8751a0 fdf67470
```

```
┌──(kali㉿kali)-[~/Desktop/bkcrack/install]
└─$ ./bkcrack -C ../../info-send\(1\).zip -k cec26f80 cc8751a0 fdf67470 -U newzip.zip easy
bkcrack 1.7.1 - 2024-12-21
[17:19:34] Writing unlocked archive newzip.zip with password "easy"
100.0 % (2 / 2)
Wrote unlocked archive.
```

```
┌──(kali㉿kali)-[~/Desktop/bkcrack/install]
└─$ ./bkcrack -k cec26f80 cc8751a0 fdf67470 --bruteforce ?p --length 11
bkcrack 1.7.1 - 2024-12-21
[17:22:06] Recovering password
length 11 ...
Password: passdrow69#
85.0 % (7668 / 9025)
Found a solution. Stopping.
You may resume the password recovery with the option: --continue-recovery 7064202020
[17:22:08] Password
as bytes: 70 61 73 73 64 72 6f 77 36 39 23
as text: passdrow69#
```

Task11: What is the master password of the KeePass database that was leaked by the insider threat and handed over to the evil Krampus?

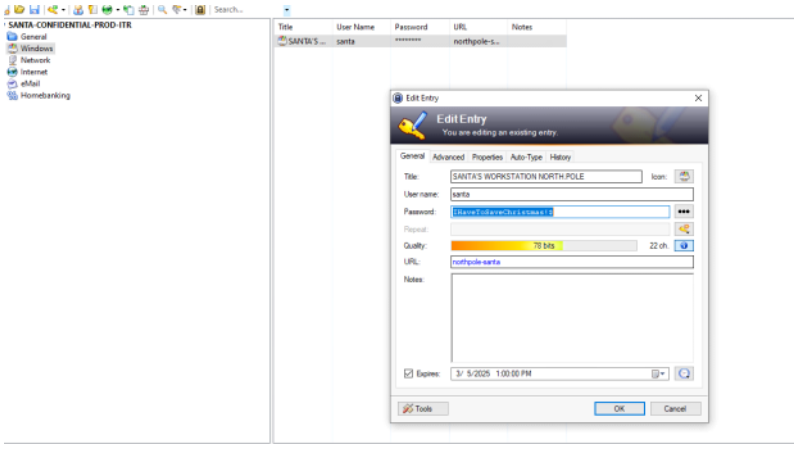
- After we found the ZIP file, we need now to crack the password of the Keepass of Santa.
  I used 'keepass2john' to extract the hash of the DB and bruteforce the password via John and the word list 'Rockyou'.
  The password is: **weed420**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 60000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
weed420          (SANTA-CONFIDENTIAL-PROD-ITR)
1g 0:00:00:14 DONE (2024-12-22 17:58) 0.06715g/s 143.9p/s 143.9c/s 143.9C/s falcon..weed420
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Task12:What is the password for Santa's account on his North Pole workstation?

- The password of Santa's found in the Keepass DB, the password is **'IHaveToSaveChristmas!$'**



Task13: Twinkle got his money in cryptocurrency so it can't be traced. Which cryptocurrency did he receive money in, and what was its address?

- I examined the MEGA chat and found the cryptocurrency and the crypto wallet of Twinkle.
  The answer is **'Elfereum:LVg2kJoFNg45Nbpy53h7Fe1wKyeNJHeXV2'**

12:20:48		Message	
2024-11-05 12:21:57	krampusevilson@yahoo.com	Chat Message	AHHHH!!!!!\nOk send me your crypto address. I will transfer you 34500$ (half payment). rest when we are in
2024-11-05 12:28:37		Chat Message	Elfereum:LVg2kJoFNg45Nbpy53h7Fe1wKyeNJHeXV2
2024-11-05 12:34:26	krampusevilson@yahoo.com	Chat Message	sent