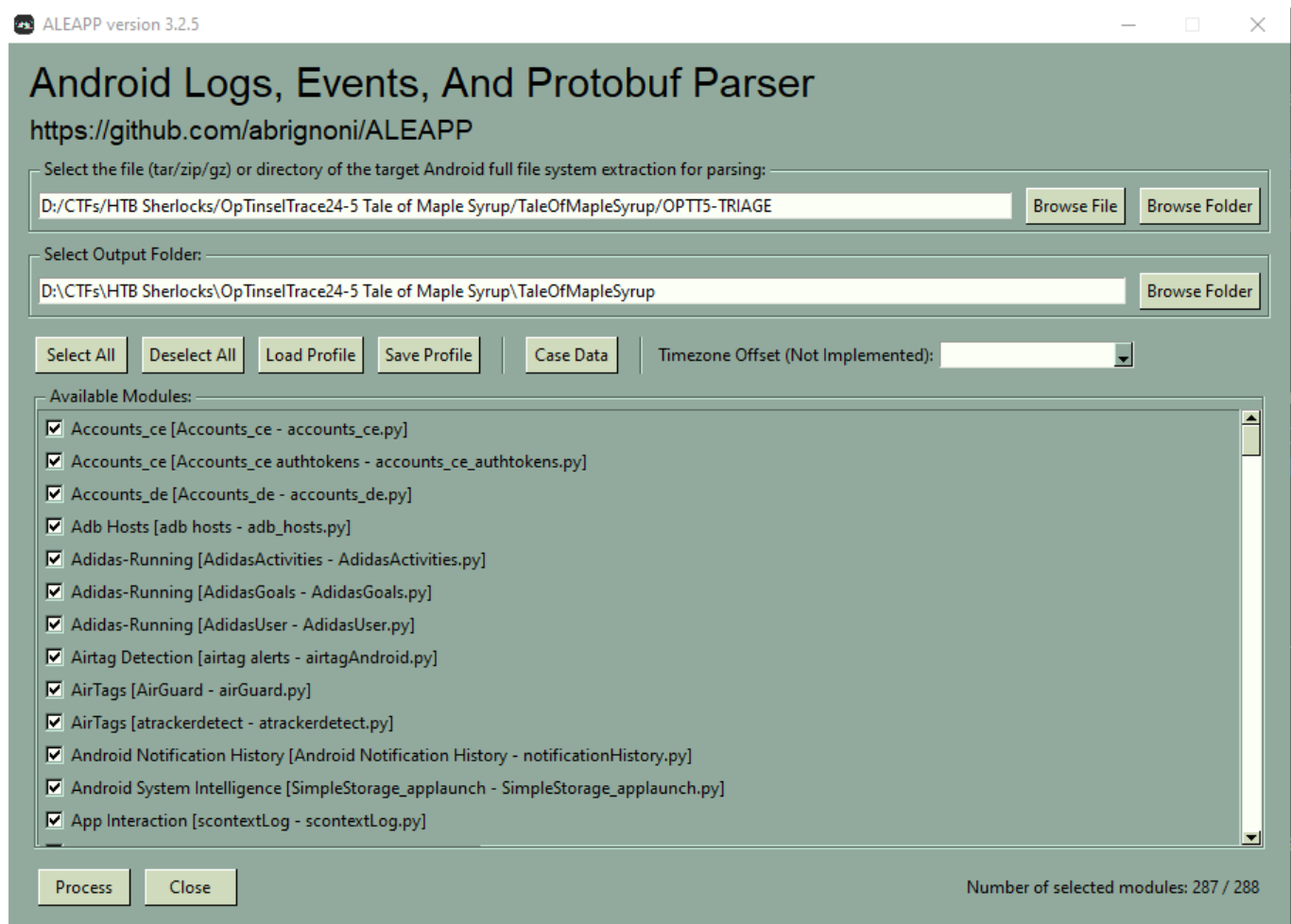


Scenario

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.

Downloaded files are parts of Android devices of the insider Twinkle Snowberry, to analyze this type of artifacts utilize an open source tool ALEAPP (<https://github.com/abrignoni/ALEAPP>). Analyzing through GUI version, pass the artifacts to the tool and select output folder, select all artifacts to be analyzed.



The tool will create HTMLs output of the parsed data, looking through the outputs we can identify application MEGA for private chatting, where we spotted our suspected insider







Twinkle chatting with Krampus.

Message Timestamp	Sender	Message Type	Chat Message
2024-11-04 11:42:50	krampusevilson@yahoo.com	Chat Message	Hello Twinkles
2024-11-04 11:54:20	krampusevilson@yahoo.com	Chat Message	I Dont Like waiting. REPLY ASAP!!!
2024-11-04 11:54:57		Chat Message	You are not my boss!!!
2024-11-04 11:55:30		Chat Message	I was drinking maple Syrup
2024-11-04 11:56:53	krampusevilson@yahoo.com	Chat Message	Still hating on Santa hahaha?I hate him as well

Looks like Twinkle is looking to betray Santa's and help Kramups in his evil plans, for certain amount of cache, precisely 69000\$.

Krampus demanding to get credentials for remote login and Santa's computer password. After some time Twinkle managed to collect some intel: emails of the employees and KeePass database file that contains Santa's computer password, but in all of the hurry he couldn't remember the password for the zip file so he left Krampus to figure it out alone, which he did it and after that he concluded phishing email at one of the Santa's developer (Bingle Jollybeard), which was successful and where the story of the HtB Sherlock "OpTinselTrace24-1: Sneaky Cookies" begins. The whole conversation between Krampus and Twinkle are locate at the bottom of the writeup.

Going through the installed applications, we determined that Mega applications is installed under ID mega.privacy.android.app and the date of installation is 2024-11-04 11:24.28.

First Download 	Package Name 	Title 	Install Reason 	Last Updated 	Auto Update? 	Account
2024-11-04 11:15:36	com.google.android.gms		unknown	2024-11-04 11:16:42	Yes	
2024-11-04 11:24:28	mega.privacy.android.app		unknown		Yes	twinklesn
2024-11-04 11:24:40	org.mozilla.firefox		unknown	2024-11-21 10:03:39	Yes	twinklesn
2024-11-04 11:24:49	com.google.android.keep		unknown	2024-11-21 10:05:06	Yes	twinklesn
2024-11-04 12:55:49	com.google.android.apps.restore		unknown	2024-11-27 17:55:20	Yes	twinklesn
2024-11-04 12:56:03	com.google.android.partnersetup		unknown	2024-11-04 12:56:07	Yes	
2024-11-04 12:56:09	com.google.android.contacts		unknown	2024-11-21 10:04:33	Yes	twinklesn

Through analyzing database of the Google Keep applications for creating and saving notes (com.google.android.keep) an interesting notes was identified.

User create a note called "Collect Information" at 2024-11-04 12:14:55, the content of the notes:

```
I will need to find any ssh or rdp access that is open to internet. Will need to find their email address as well, maybe krampus will need those as well!!
```

The artifacts was collected from keep.db database located at:

```
./data/com.google.android.keep/databases/keep.db
```

Title of the notes:

Table: text_search_tree_entities_content		
	docid	c0title
	Filter	Filter
1	1	Collect Information

Context of the notes:

Table: text_search_note_content_content		Filter in any column
	docid	c0text
	Filter	Filter
1	1	I will need to find any ssh or rdp access that is open to internet. Will need to find their email address as well, maybe krampus will need those as well!!

Creation time displayed in the the Unix timestamp:

Table: tree_entity			
	time_created	time_last_updated	user_edited_timestamp
	Filter	Filter	Filter
1	1730722495549	1730722597430	1730722597216

Twinkles downloaded files:

Created Timestamp	File Name	URL	MIME Type	File Size (Bytes)
2024-11-05 10:45:11	zipppping.png	https://eu.justbeamit.com:8443/download?token=2u7wh	image/png	0
2024-11-05 10:45:49	zipppping(1).png	https://eu.justbeamit.com:8443/download?token=2u7wh	image/png	24713
2024-11-05 12:03:23	info-send.zip	https://eu.justbeamit.com:8443/download?token=um9w7	application/zip	0
2024-11-05 12:03:44	info-send(1).zip	https://eu.justbeamit.com:8443/download?token=um9w7	application/zip	3249

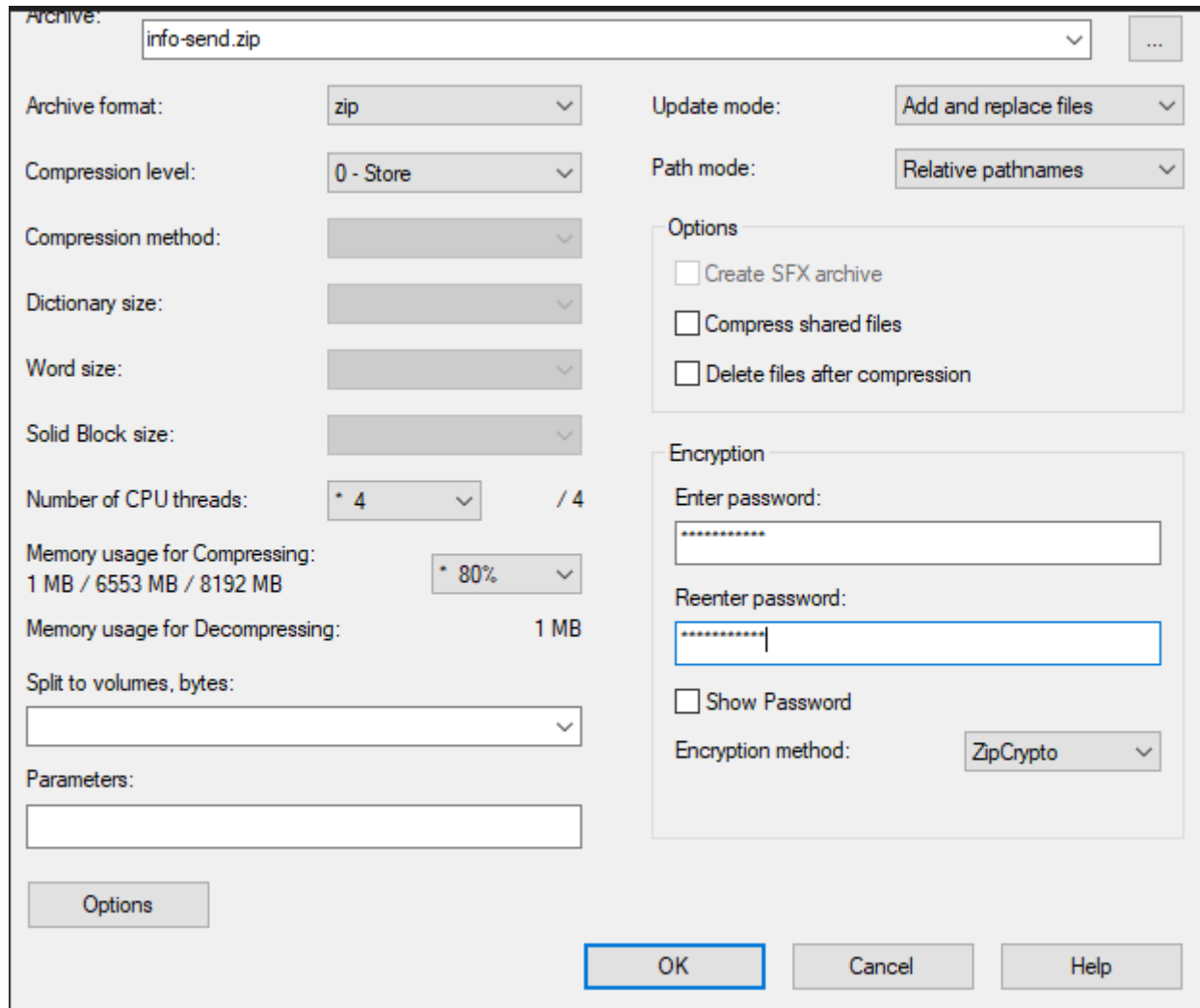
At 2024-11-05 12:04:24 a suspect Twinkles shared these files with Krampus using Mega chat application. Claiming that he don't remember passwords that he used.

2024-11-05 10:47:55		Attachment		zipppping(1).png
------------------------	--	------------	--	------------------

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 12:17:49		Chat Message	Ah\nOh shoot	
2024-11-05 12:18:00		Chat Message	I forgot the password.Damn	

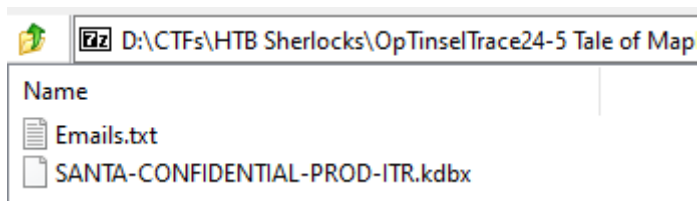
The files "zipping(1).png" and "info-send(1).zip" are collected through the forensic acquisition process.

The first file "zipping(1).png" is the screenshot of the 7z application when "info-send(1).zip" was prepared to be created. The screenshot provides very useful information, Twinkle uses the old encryption method ZipCrypto and the length of the password is 11 characters.



The second file is the "info-send(1).zip" itself, location of the file is "\storage\emulated\0\Download", the file is password protected like we expected and the archive contains two files:

- Emails.txt
- SANTA-CONFIDENTIAL-PROD-ITR.kdbx



To confirm what exact information Twinkle sent to Krampus, we will try to exploit ZipCrypto vulnerability and extract files from the "info-send(1).zip" archive.

To be able to extract files, we will use open-source tool bkcrack (<https://github.com/kimci86/bkcrack>).

To be able to extract the keys, bkcrack requires at least 12 bytes of known plaintext. At least 8 of them must be contiguous.

Our focus will be at Email.txt and try to guess the first email address that Email.txt contains. To be sure to have a valid email, we will use Twinkle's email that he leaked in the conversation with the Krampus.

2024-11-05 10:37:35		Chat Message	Also in case of emergency for some reason we cannot communicate here, drop me email on my newly created email TwinklesnowberryAlt@gmail.com . DO not even by mistake send it to my TwinkleSnowberry@north.pole email as Santa has lots of magic filter combing all inbound outbound emails	
------------------------	--	-----------------	---	--

Create a file that contains strings "TwinkleSnowberry@north.pole" and store it in .txt file. In our case that will be htb.txt

Executes bkcrack tool to extract keys:

```
D:\Tools\bkcrack-1.7.1-win64>bkcrack.exe -C "info-send(1).zip" -c Emails.txt -p htb.txt
bkcrack 1.7.1 - 2024-12-21
[01:36:51] Z reduction using 20 bytes of known plaintext
100.0 % (20 / 20)
[01:36:51] Attack on 372935 Z values at index 6
Keys: cec26f80 cc8751a0 fdf67470
49.1 % (183067 / 372935)
Found a solution. Stopping.
You may resume the attack with the option: --continue-attack 183067
[01:39:40] Keys
cec26f80 cc8751a0 fdf67470
```

After retrieving the key, utilize again bkcrack to bruteforce password. The "?p" parameter is for the ASCII printable characters and 11 stands for the number of characters, which we

knew from the "zipping(1).png" file.

```
D:\Tools\bkcrack-1.7.1-win64>bkcrack.exe -k cec26f80 cc8751a0 fdf67470 -r 11 ?p
bkcrack 1.7.1 - 2024-12-21
[01:42:43] Recovering password
length 0-6...
length 7...
length 8...
length 9...
length 10...
length 11...
Password: passdrow69#
85.4 % (7708 / 9025)
Found a solution. Stopping.
You may resume the password recovery with the option: --continue-recovery 712d202020
[01:42:44] Password
as bytes: 70 61 73 73 64 72 6f 77 36 39 23
as text: passdrow69#
```

The password is correct, the archive is successful extracted.

File Emails.txt contains:

```
TwinkleSnowberry@north.pole
JingleMcTinsel@north.pole
BuddyFrostbeard@north.pole
TinselSparklefrost@north.pole
MerrySugarplum@north.pole
NippyFlufferson@north.pole
HollyJollybuttons@north.pole
ChipperPeppermint@north.pole
ButtonsFrostwhiskers@north.pole
BlitzenFrostbright@north.pole
SparkleSugarglow@north.pole
BerryMerryweather@north.pole
FlickerSnowflurry@north.pole
CinnamonTwinklebell@north.pole
TobyPinecone@north.pole
IvyGlittertwist@north.pole
NippySnowboots@north.pole
DazzleHollyhop@north.pole
SnickerdoodleFrostnose@north.pole
```

BingleJollybeard@north.pole

ByteSparkles@north.pole

The second file is the KeePass database file and is protected by the master password.

Using the John The Ripper utilities (<https://github.com/openwall/john>) to successfully crack the master password.

What we need first is to extract hash of the password from the kdbx file, with the keepass2john.exe and forward extracted hash to the John the ripper tool using "rockyou.txt" as the wordlist.

```
D:\Tools\Password Cracking\run>keepass2john.exe SANTA-CONFIDENTIAL-PROD-ITR.kdbx > KeePass_Master_hash.txt
D:\Tools\Password Cracking\run>john.exe --wordlist=rockyou.txt KeePass_Master_hash.txt
Warning: detected hash type "KeePass", but the string is also recognized as "KeePass-opencl"
Use the "--format=KeePass-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64 OpenSSL])
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 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
weed420 (SANTA-CONFIDENTIAL-PROD-ITR)
1g 0:00:00:08 DONE (2025-01-27 01:51) 0.1141g/s 244.8p/s 244.8c/s 244.8C/s laurita..weed420
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Confirmed access to the KeePass database:

Edit Entry
You are editing an existing entry.

General | Advanced | Properties | Auto-Type | History

Title: SANTA'S WORKSTATION NORTH.POLE Icon:

User name: santa

Password: IHaveToSaveChristmas!\$

Repeat:

Quality: 78 bits 22 ch.

URL: northpole-santa

Notes:

☒ Expires: 05.03.25 22:00:00

Tools OK Cancel

Questions

Q1. 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.

krampusevilson@yahoo.com

Q2. Which application was used by the insider threat to communicate with the threat actor? Provide the application's Android package name.

mega.privacy.android.app

Q3. When was this application installed on the device?

2024-11-04 11:24:28

Q4. What is the agreed amount of money to be sent to the insider threat in exchange of him leaking Santa workshop's secrets?

\$69000

Q5. Twinkle created a note on his phone using a note-keeping app. What were the contents of the note?

I will need to find any ssh or rdp access that is open to internet. Will need to find their email address as well, maybe krampus will need those as well!!

Q6. What is the title of this note?

Collect Information

Q7. When was the note created in the note-keeping app?

2024-11-04 12:14:55

Q8. 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?

<https://eu.justbeamit.com:8443/download?token=um9w7>

Q9. When was this file shared with the threat actor by the insider, Twinkle Snowberry?

2024-11-05 12:04:24

Q10. Twinkle forgot the password of the archive file he sent to Krampus containing secrets. What was the password for the file?

passdrow69#

Q11. What is the master password of the KeePass database that was leaked by the insider threat and handed over to the evil Krampus?

weed420

Q12. What is the password for Santa's account on his North Pole workstation?

IHaveToSaveChristmas!\$

Q13. Twinkle got his money in cryptocurrency so it can't be traced. Which cryptocurrency did he receive money in, and what was its address?

Elfereum:LVg2kJoFNg45Nbpy53h7Fe1wKyeNJHeXV2

Mega Private Chat Logs

2024-11-04 11:42:50	krampusevilson@yahoo.com	Chat Message	Hello Twinkles
2024-11-04 11:54:20	krampusevilson@yahoo.com	Chat Message	I Dont Like waiting. REPLY AS
2024-11-04 11:54:57		Chat Message	You are not my boss!!!
2024-11-04 11:55:30		Chat Message	I was drinking maple Syrup
2024-11-04 11:56:53	krampusevilson@yahoo.com	Chat Message	Still hating on Santa hahaha?I well
2024-11-04 12:00:07		Chat Message	Yeah well i hate you as well. R am only working with you beca Santa because of what he few I also could use the money to k sweetheart wife a nice christma

2024-11-04 12:04:05	krampusevilson@yahoo.com	Chat Message	The more you help us the more we can earn.
2024-11-04 12:05:08	krampusevilson@yahoo.com	Chat Message	We need Working credentials for the server. It could be either RDP or ssh but it has to be open to internet. Once we are in we will give you half of the amount.
2024-11-04 12:06:48	krampusevilson@yahoo.com	Chat Message	We will transfer you total of 69000\$ if you give us we expect this of you \n1- Give us working credentials for any service over the internet so we can remotely login and evaluate the system. \n2- You give us the server Computer password.
2024-11-04 12:07:29		Chat Message	What, are you drunk with maples?
2024-11-04 12:09:21		Chat Message	This year, santa invested so much in server security after last year's incident. Now all services are open to internet with no restrictions needed. The network is tightly secured.
2024-11-04 12:10:18		Chat Message	Also how do you expect me to give you the password. He keeps it secure and hidden.
2024-11-04 12:11:11	krampusevilson@yahoo.com	Chat Message	This is not what my agent convinced me. He told me you were ready to work with us.
2024-11-04 12:12:23		Chat Message	I am!!!!. But this is out of my hands. The server security is tight. And I don't know the password.
2024-11-04 12:12:59	krampusevilson@yahoo.com	Chat Message	I thought you were Santa's right hand man. I think you are useless.
Message Timestamp	Sender	Message Type	Chat Message
2024-11-04 12:13:52		Chat Message	I will do what I can. I will try my best.

2024-11-04 12:20:26	krampusevilson@yahoo.com	Chat Message	You do that!!!! I will make sure ready.
2024-11-05 09:22:50	krampusevilson@yahoo.com	Chat Message	What's the status???
2024-11-05 09:25:19		Chat Message	I have managed to get some in Will send you in a bit
2024-11-05 09:34:39		Chat Message	I am preparing the stuff
2024-11-05 10:05:43	krampusevilson@yahoo.com	Chat Message	Good. Do it fast
2024-11-05 10:06:33	krampusevilson@yahoo.com	Chat Message	My Christmas Hating Cyber \xe2\x98\xa0Operators are itching for action
2024-11-05 10:37:35		Chat Message	Also in case of emergency for : we cannot communicate here, email on my newly created em TwinklesnowberryAlt@gmail.com even by mistake send it to my TwinkleSnowberry@north.pole Santa has lots of magic filter c inbound outbound emails
2024-11-05 10:40:22		Chat Message	I am archiving the data right now
2024-11-05 10:40:34	krampusevilson@yahoo.com	Chat Message	HO HO HO !!!!
2024-11-05 10:44:36	krampusevilson@yahoo.com	Chat Message	Whats taking so long
2024-11-05 10:44:42	krampusevilson@yahoo.com	Chat Message	Show me some progress

2024-11-05 10:46:46		Chat Message	You should chill!!! Drink maple s enjoy the snowfall\nyou are so
2024-11-05 10:47:36		Chat Message	I took a screenshot for you and transferring from my work pc to Cant be caught using MEGA a
2024-11-05 10:47:55		Attachment	
2024-11-05 10:48:11	krampusevilson@yahoo.com	Chat Message	HO HO HO !!!!
2024-11-05 10:48:28	krampusevilson@yahoo.com	Chat Message	I am coming for you santa my c enemy!!
2024-11-05 10:48:49	krampusevilson@yahoo.com	Chat Message	Now quit messing around and zip file as well
2024-11-05 10:49:26		Chat Message	Oh shoot santa has called for a all employees regarding christr should go for now .
2024-11-05 10:49:43	krampusevilson@yahoo.com	Chat Message	Atleast send me the file
2024-11-05 10:49:58	krampusevilson@yahoo.com	Chat Message	Oh shoot you are offline !!
2024-11-05 12:02:44		Chat Message	I am back
2024-11-05 12:02:50		Chat Message	sending you the file
2024-11-05 12:04:24		Attachment	
2024-11-05	krampusevilson@yahoo.com	Chat Message	Whats the password of this zip

12:17:38			
2024-11-05 12:17:49		Chat Message	Ah\nOh shoot
2024-11-05 12:18:00		Chat Message	I forgot the password.Damn
2024-11-05 12:18:13	krampusevilson@yahoo.com	Chat Message	Fudge
2024-11-05 12:18:24	krampusevilson@yahoo.com	Chat Message	Recreate the archive and send
2024-11-05 12:19:46		Chat Message	Cant do, i deleted the original f i think santais a lil bit sus toward couldnt take the chances. You figure this out yourself, you bra that you are so talented!!
2024-11-05 12:19:52	krampusevilson@yahoo.com	Chat Message	How dare you
2024-11-05 12:19:56	krampusevilson@yahoo.com	Chat Message	Ahhhhhh!!!!!!
2024-11-05 12:20:09	krampusevilson@yahoo.com	Chat Message	No Money for you
2024-11-05 12:20:48		Chat Message	I will simply inform santa then a be able to intrude in the worksl
2024-11-05 12:21:57	krampusevilson@yahoo.com	Chat Message	AHHHH!!!!!!\nOk send me your address. I will transfer you 345 payment). rest when we are in
2024-11-05 12:28:37		Chat Message	Elfereum LVg2kJoFNg45Nbpy53h7Fe1w
2024-11-05	krampusevilson@yahoo.com	Chat Message	sent

12:34:26			
2024-11-05 12:37:31		Chat Message	Oh one more thing, i got to kno sysadmin that mostly rdp is res only internal network and if need used externaly we use vpn acc
2024-11-05 12:38:07	krampusevilson@yahoo.com	Chat Message	Can you get ahold a vpn file fo
2024-11-05 12:39:18		Chat Message	No can do!!! I am already unde You will have to find your way y the network.
2024-11-05 12:39:35	krampusevilson@yahoo.com	Chat Message	Atleast find the vpn gateway fo
2024-11-05 12:39:50		Chat Message	Ok i will try.
2024-11-05 12:40:14	krampusevilson@yahoo.com	Chat Message	I will try to crack the zip and fin into the network
2024-11-05 12:40:54		Chat Message	Oh and the email magical filter for maintenance for next 2 day
2024-11-05 12:41:00	krampusevilson@yahoo.com	Chat Message	Ooooooh awesome
2024-11-05 13:04:19		Chat Message	The vpn gateway ip is 172.17.7
2024-11-05 14:14:54	krampusevilson@yahoo.com	Chat Message	Ok
2024-11-05 14:18:13	krampusevilson@yahoo.com	Chat Message	My team is currently preparing engineer one of your dev. It wa you including emails list in the . conducted recon and found a p Phishing victim. You would kno Jollybeard". We are targeting h speak

2024-11-05 15:09:26		Chat Message	Yeah i know him. He is visiting setup his access. I saw him do apps just now.\n He will be mo: remotely from southpole as his
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 j 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 pass cracked in 1minute. I did not ex cyber team is currently on his s trying to move laterally to more machines
2024-11-05 16:39:16	krampusevilson@yahoo.com	Chat Message	We have successfully infiltrated northpole workshop. We will be for atleast 1 day as we already possibly made enough noise
2024-11-14 03:29:57		Chat Message	Hello. These past few days hav hectic with all the chaos going hacking into Santa's workshop
2024-11-14 03:30:23		Chat Message	So far no one suspects me and using the phone to stay low
2024-11-14 03:30:34		Chat Message	When will you send my remain
2024-11-14 03:30:40		Chat Message	\xf0\x9f\xab\xa5
2024-11-14 03:34:01	krampusevilson@yahoo.com	Chat Message	HO HO HO !!!
2024-11-14	krampusevilson@yahoo.com	Chat Message	Yes we have been targeting the pods as well. Soon we will targ

03:38:28			environment as well. I just can't finally hack into santa's worksta
2024-11-21 10:00:39	krampusevilson@yahoo.com	Chat Message	HO HO HO !!
2024-11-21 10:01:15	krampusevilson@yahoo.com	Chat Message	Just to provide an update, we've rest of money when our objecti complete.
2024-11-21 10:01:26	krampusevilson@yahoo.com	Chat Message	We are almost there HO HO H
2024-11-21 10:01:53	krampusevilson@yahoo.com	Chat Message	We targeted your cloud infrastr well (Its AWS i think??)
2024-11-21 10:01:59	krampusevilson@yahoo.com	Chat Message	spilled the buckets !!!
2024-11-21 10:02:02	krampusevilson@yahoo.com	Chat Message	HO HO HO !!!
2024-11-21 10:03:29		Chat Message	Ok\ni cant wait to order maples the money
2024-11-21 10:04:54		Chat Message	maplebrewery.com has a great sale going on. 69% Discount u santalovesmaplesyrup2024
2024-11-21 10:05:31		Chat Message	I really hate that everyone love santa's name in everything this year. Who do he thinks he is
2024-11-27 17:58:51	krampusevilson@yahoo.com	Chat Message	HO HO HO!!!
2024-11-27 18:02:04	krampusevilson@yahoo.com	Chat Message	Ok twinkiee listen to me. \n\nY valuable to us as that allowed i your organization. Just recently your so-called AI Chat Bot as v compromised a critical linux se believe we are really close to g Santa's computer.\n\n\nI have i

			send you your remaining money a gesture of Krampus will (cause \n\nNow don't message me here I am disposing of this account. I on your maple syrup !!!
2024-11-27 18:02:38	krampusevilson@yahoo.com	Chat Message	Have a very Merry Krampus !!!