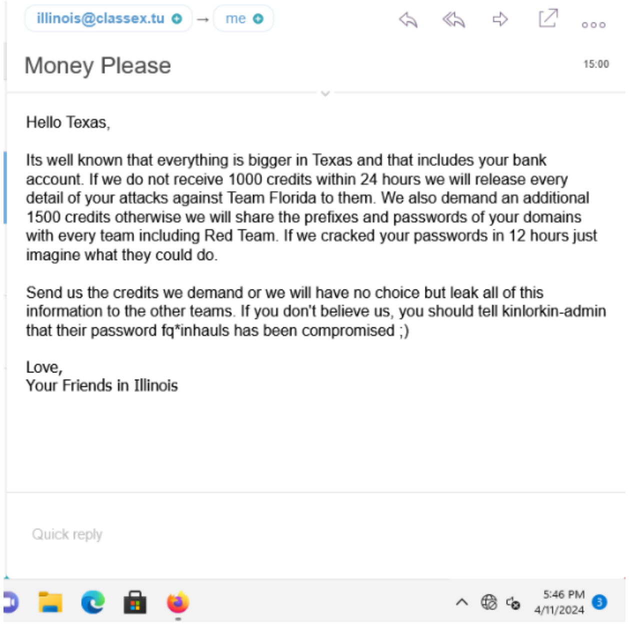
4-15 Incident Response

Team Texas

Illinois Ransom Attack

Overview:

On 4:11, at 3 P.M. Est, our team received a threatening email subjected from team Illinois, demanding us to pay a 2500 credit ransom or they would leak sensitive information about our team, including the usernames and passwords of all our users, and our offense report targeted towards team Florida. The email had matched the correct email address of the corresponding team, and we later got confirmation from an Illinois representative that they were the source of the attack. The following document covers the incident as a whole and how our team responded.



illinois@classex.tu → me

Money Please

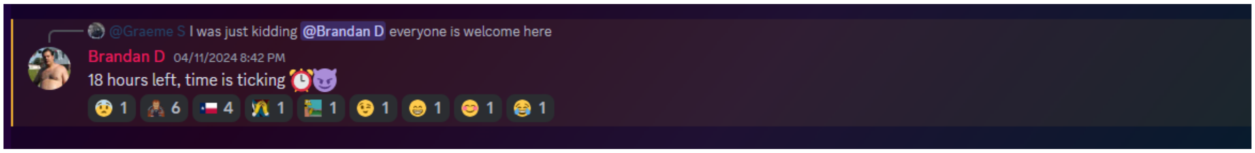
15:00

Hello Texas,

Its well known that everything is bigger in Texas and that includes your bank account. If we do not receive 1000 credits within 24 hours we will release every detail of your attacks against Team Florida to them. We also demand an additional 1500 credits otherwise we will share the prefixes and passwords of your domains with every team including Red Team. If we cracked your passwords in 12 hours just imagine what they could do.

Send us the credits we demand or we will have no choice but leak all of this information to the other teams. If you don't believe us, you should tell kinlorkin-admin that their password fq*inhauls has been compromised ;)

Love,
Your Friends in Illinois



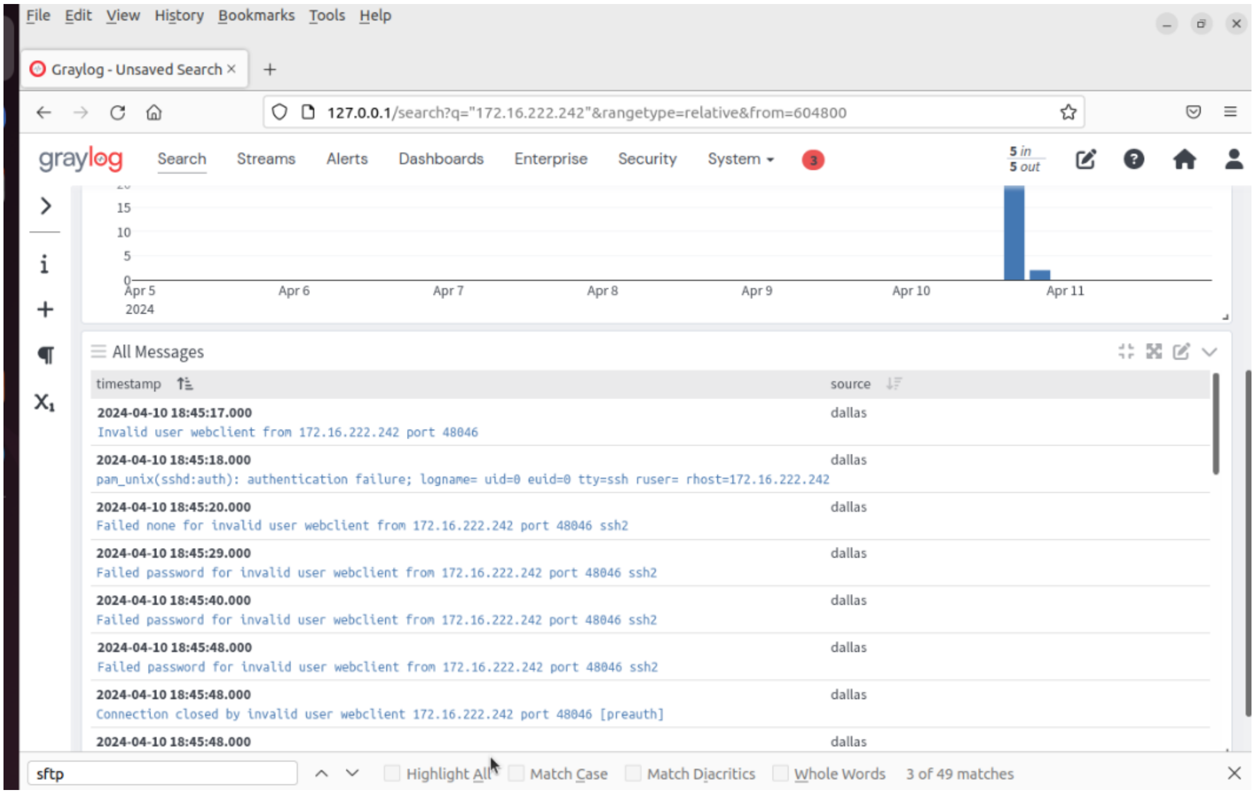
@Graeme S I was just kidding @Brandan D everyone is welcome here

Brandan D 04/11/2024 8:42 PM

18 hours left, time is ticking ⏰😈

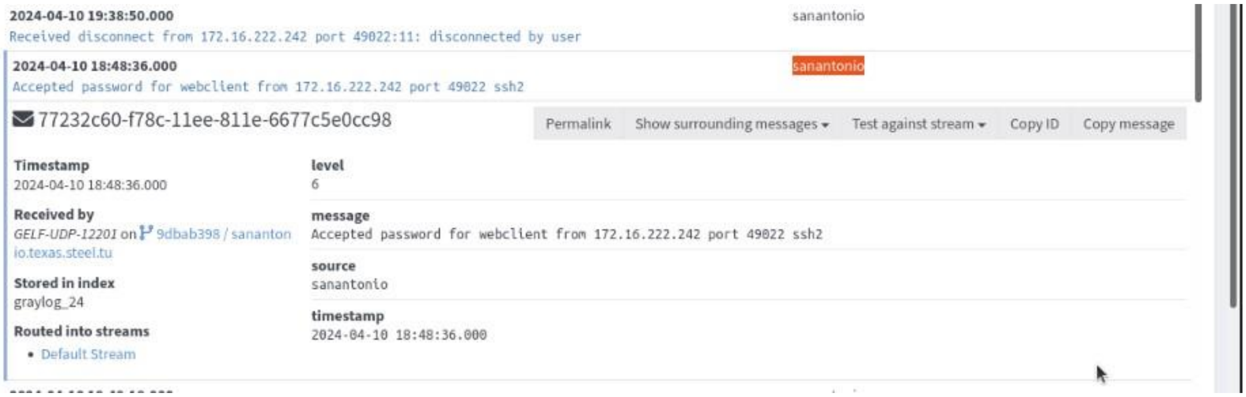
Initial Access:

On 2024-04-10, it was discovered that a suspicious IP had been attempting to log into our Dallas (Samba File Share) machine using an account we previously disabled, discovered to be a persistence method used by Red Team Kaiju (discussed in previous report).



```
timestamp                                                               source
2024-04-10 18:45:17.000                                                 dallas
Invalid user webclient from 172.16.222.242 port 48046
2024-04-10 18:45:18.000                                                 dallas
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.16.222.242
2024-04-10 18:45:20.000                                                 dallas
Failed none for invalid user webclient from 172.16.222.242 port 48046 ssh2
2024-04-10 18:45:29.000                                                 dallas
Failed password for invalid user webclient from 172.16.222.242 port 48046 ssh2
2024-04-10 18:45:40.000                                                 dallas
Failed password for invalid user webclient from 172.16.222.242 port 48046 ssh2
2024-04-10 18:45:48.000                                                 dallas
Failed password for invalid user webclient from 172.16.222.242 port 48046 ssh2
2024-04-10 18:45:48.000                                                 dallas
Connection closed by invalid user webclient 172.16.222.242 port 48046 [preauth]
2024-04-10 18:45:48.000                                                 dallas
```

The infected user was found again on our Graylog System, which allowed this suspicious IP access to our San Antonio (graylog) machine.



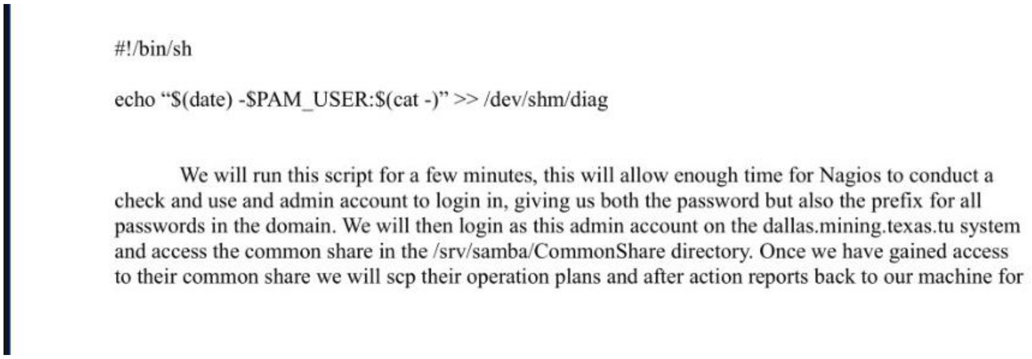
```
2024-04-10 19:38:50.000                                      sanantonio
Received disconnect from 172.16.222.242 port 49022:11: disconnected by user
2024-04-10 18:48:36.000                                      sanantonio
Accepted password for webclient from 172.16.222.242 port 49022 ssh2
77232c60-f78c-11ee-811e-6677c5e0cc98

Timestamp                    level
2024-04-10 18:48:36.000      6
Received by                  message
GELF-UDP-12201 on 9dbab398 / sanantonio.texas.steel.tu
                             Accepted password for webclient from 172.16.222.242 port 49022 ssh2
Stored in index              source
graylog_24                   sanantonio
Routed into streams          timestamp
• Default Stream             2024-04-10 18:48:36.000
```

Privilege Escalation:

As mentioned in the previous incident response and offense report, red team likes to give this account administrative privileges for persistence later, allowing any user who compromises this account immediate administrative privileges, allowing them to bypass this step.

Exfiltration and Lateral Movement:

Using a persistence method we had installed from a previous attack; we were able to find their offense report and discover their plan for moving lateral. A previous attack from the red team discovered on their system abused a vulnerability that allows the passwords gathered from PAM authentication be placed inside a plaintext file. Abusing this allowed them access to our mining prefix passwords, allowing them to SSH into all Mining domain accounts. The following screenshot shows an excerpt from their report:



```
#!/bin/sh

echo “$(date) -$PAM_USER:$(cat -)” >> /dev/shm/diag
```

We will run this script for a few minutes, this will allow enough time for Nagios to conduct a check and use and admin account to login in, giving us both the password but also the prefix for all passwords in the domain. We will then login as this admin account on the dallas.mining.texas.tu system and access the common share in the /srv/samba/CommonShare directory. Once we have gained access to their common share we will scp their operation plans and after action reports back to our machine for

The team then targeted our Dallas Samba Machine, where it was discovered through roots history file that they exfiltrated our CommonShare folder to their own system, giving them access to all our offense reports, incident responses, and episode reports.

Persistence:

No persistence was found throughout the attack. Users were checked for public keys layered in their authorized key files and checks for suspicious cron job files were made with nothing suspicious noted. After the episode, we plan to steal their after-episode report to discover what (if any) persistence was made.

Impact:

During the time of the attack, our team was more worried about the release of our users' passwords than the potential leak of our offense plan. Such a release would compromise all the users on our domains, and not knowing what domain passwords they managed to exfiltrate, potentially allow other teams (including red team) the ability to exfiltrate all data from any user at any time off our system. The leak of our password prefixes also meant that any exfiltration of our shadow file on that machine would allow an easier time for future password hashes to be cracked.

Incident Response:

Immediately after the attack was known, our team put full focus on discovering where the source of the attack came from and the protection of our compromised users. After discovering how team Illinois infiltrated our system, we went through and checked all systems to ensure the point of entry (and any other suspicious user accounts) were deleted off our system. During this time, we also tried to contact our CEO for their input on the situation but received no response during the two attempts at getting in contact. Due to the severity of this attack and understanding that paying the ransom would not guarantee the safety of our passwords (they could still be leaked), the team decided to not pay the ransom and put all work into incident response to ensure the impact will be minimized. By the time team Illinois had leaked our data to a public Pastebin, passwords for all users had been changed.

After the leak, it was discovered that team Illinois had only compromised our auto and mining domain passwords. Moving forward, these systems will be heavily monitored for any suspicious IP's that attempt to login to the system.