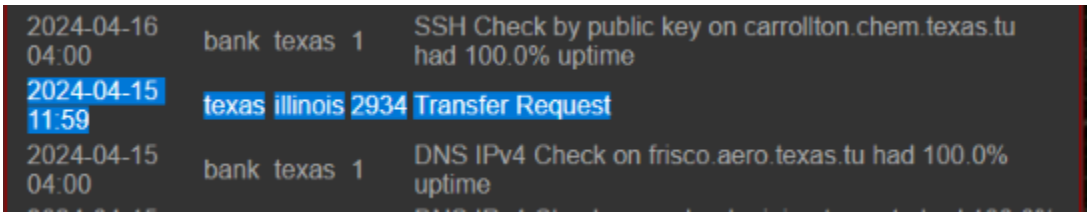
TEAM TEXAS
INCIDENT RESPONSE:
BANK COMPROMISE

Summary:

On 04/15/2024, around 1100 EST, it was discovered that all credits found within the bank of our organization had been transferred to Team Illinois. Upon speaking with representatives from all organizations (New York, California, Florida, and Illinois), it was discovered that an unknown threat actor had transferred the funds of all teams into team Illinois bank account, before transferring the funds to Red Team. We believe the culprits to be part of the malicious hacking group Team Kaiju. Upon looking into the issue, it was discovered that the threat actor had been using a fake bank website along with fake certificates for authenticating the site, where unsuspecting users would type in their user credentials believing the site to be legitimate, where they will be forwarded to the threat actor before forwarding your request to the legitimate bank site. While the IT team were unsuccessful in recovering the stolen credits, Exercise credentials for accessing the bank were immediately changed, along with the adoption of a new group policy for accessing the Exercise domain using two new systems (Orange and Paris) within the organizations network.

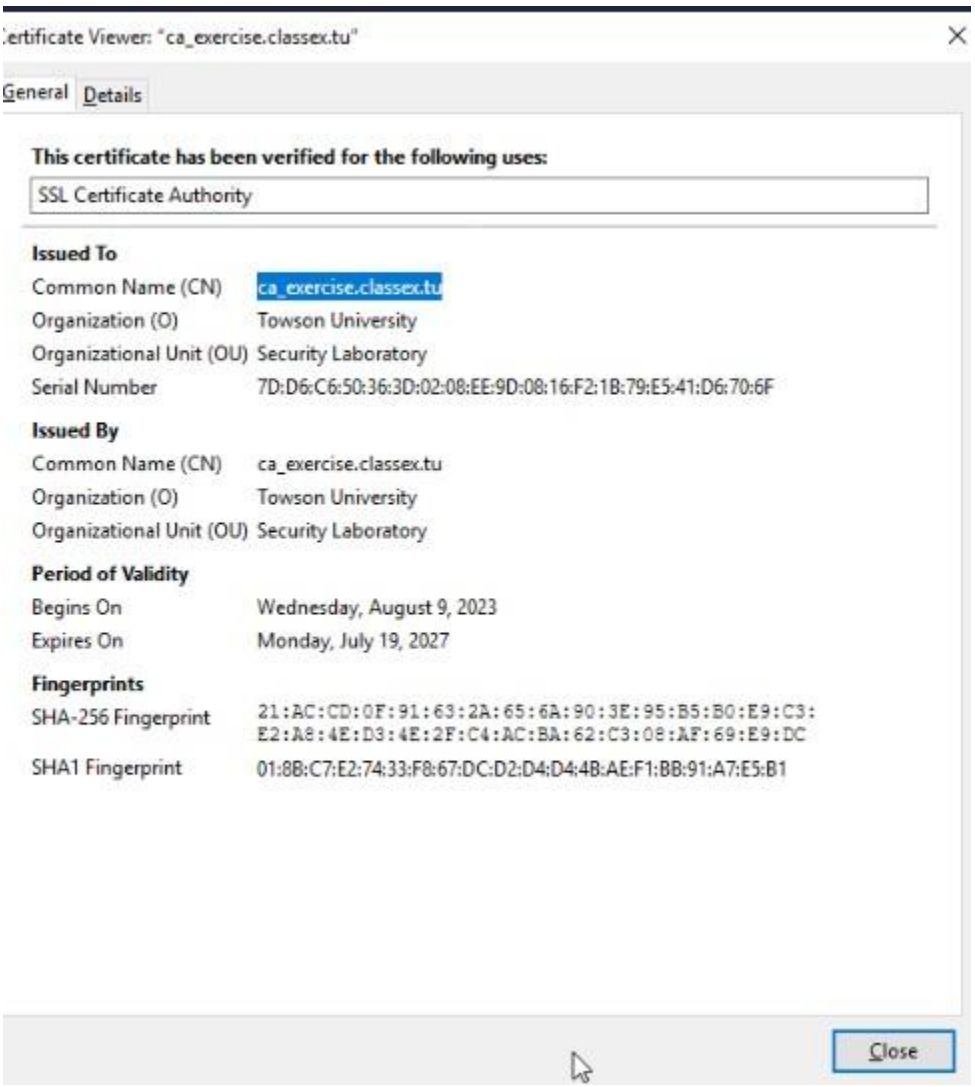
Initial Reconnaissance:

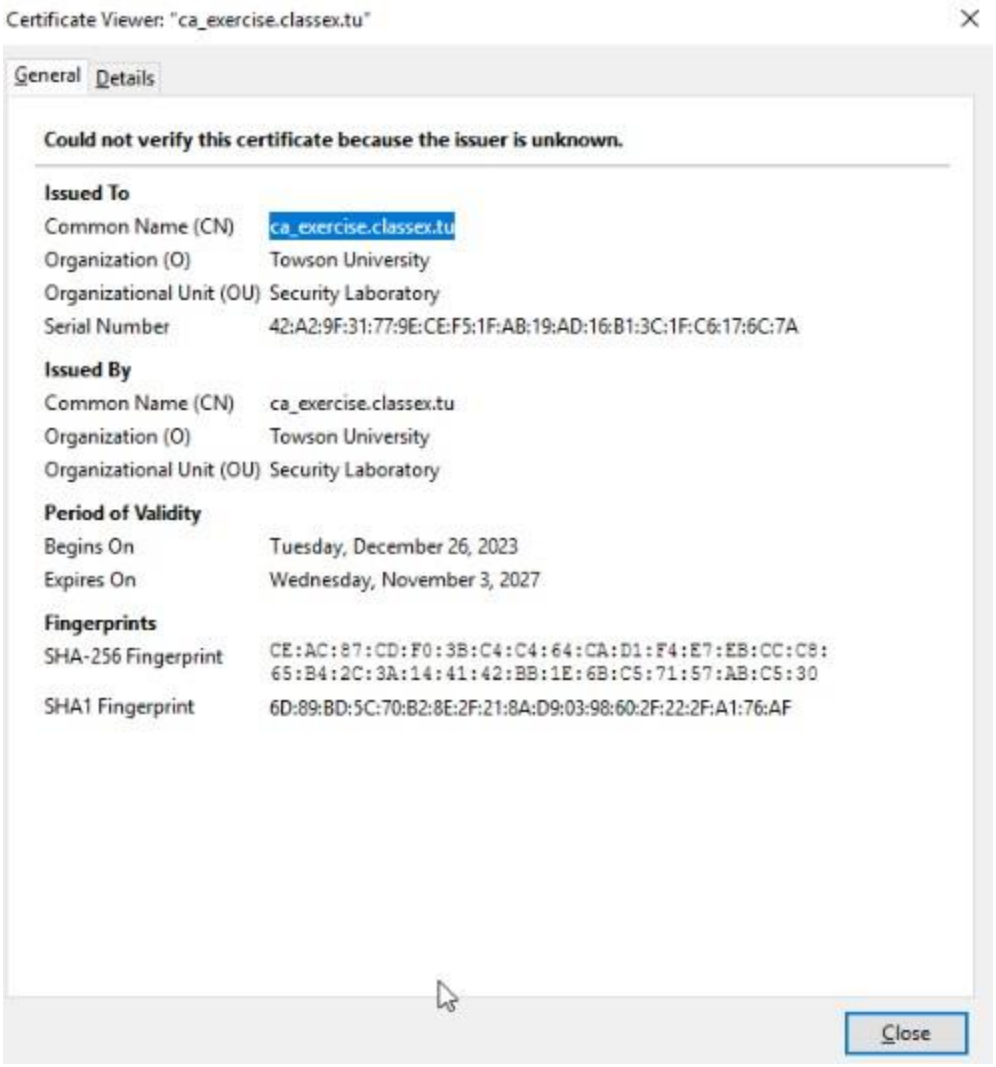
The IT team became aware of the attack on 04/15/2024 at 17:30 EST during a briefing with the CEO. Immediately checking bank logs, it was discovered that 2934 credits were transferred from Texas to Illinois at 11:59 earlier the same day.



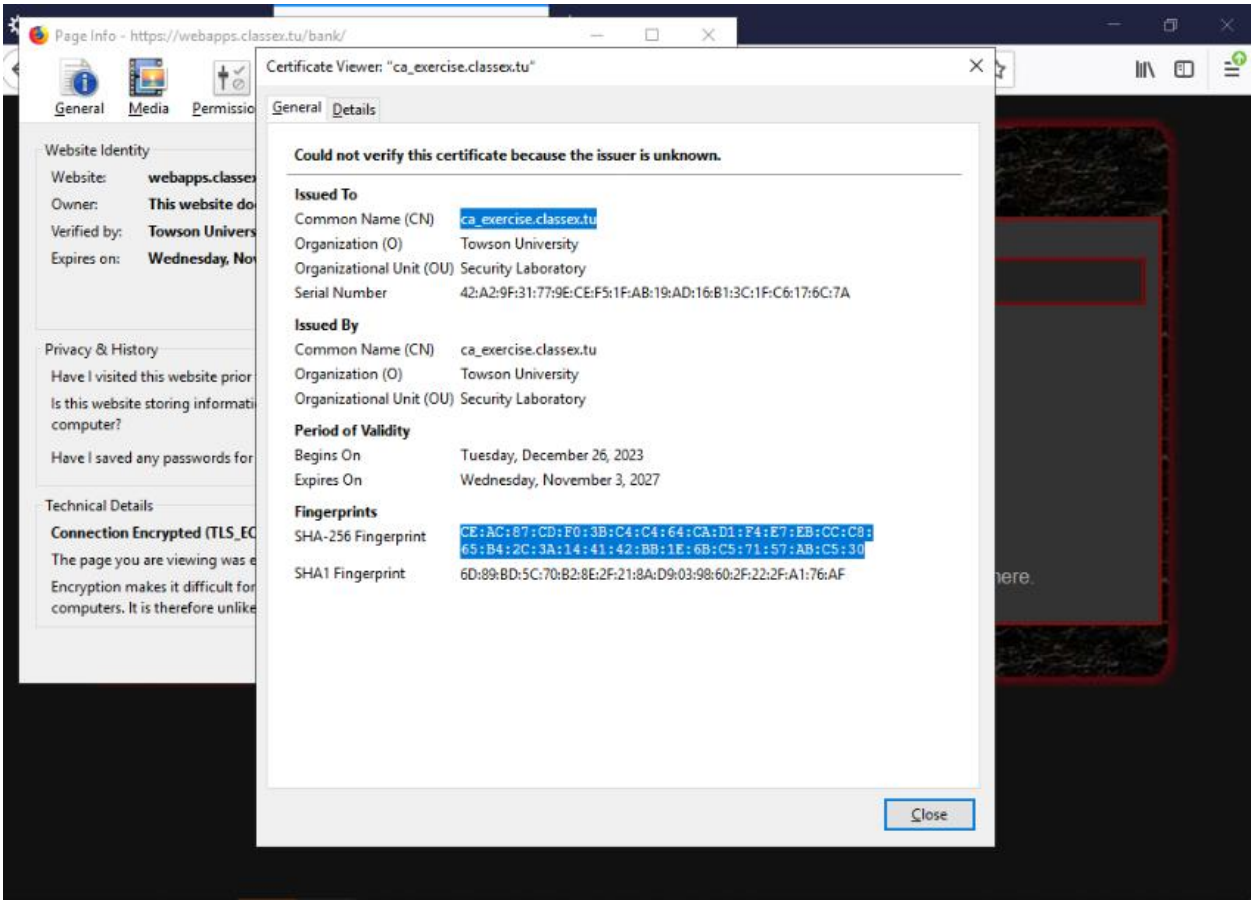
A representative from our team contacted our allies in team New York, discovering a similar compromise had befallen them as well. An emergency meeting was conducted with representatives from all teams, where it was disclosed by team Illinois that a threat actor had used their bank credentials to funnel every organizations' current credits before transferring them to red team.

On 04/16/2024, it was discovered that our Elpaso (steel Windows server) and Killeen (aero Windows workstation) machines, which the IT team had been using to access the exercise network, contained two certificates within their browser for the classex domain, both with different fingerprints. The first photo is an authentic certificate, issues from the classex website, while the second is the malicious certificate:

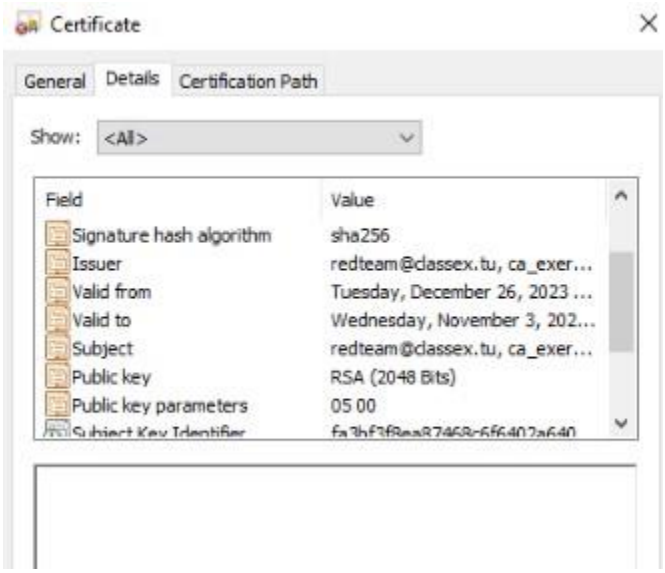




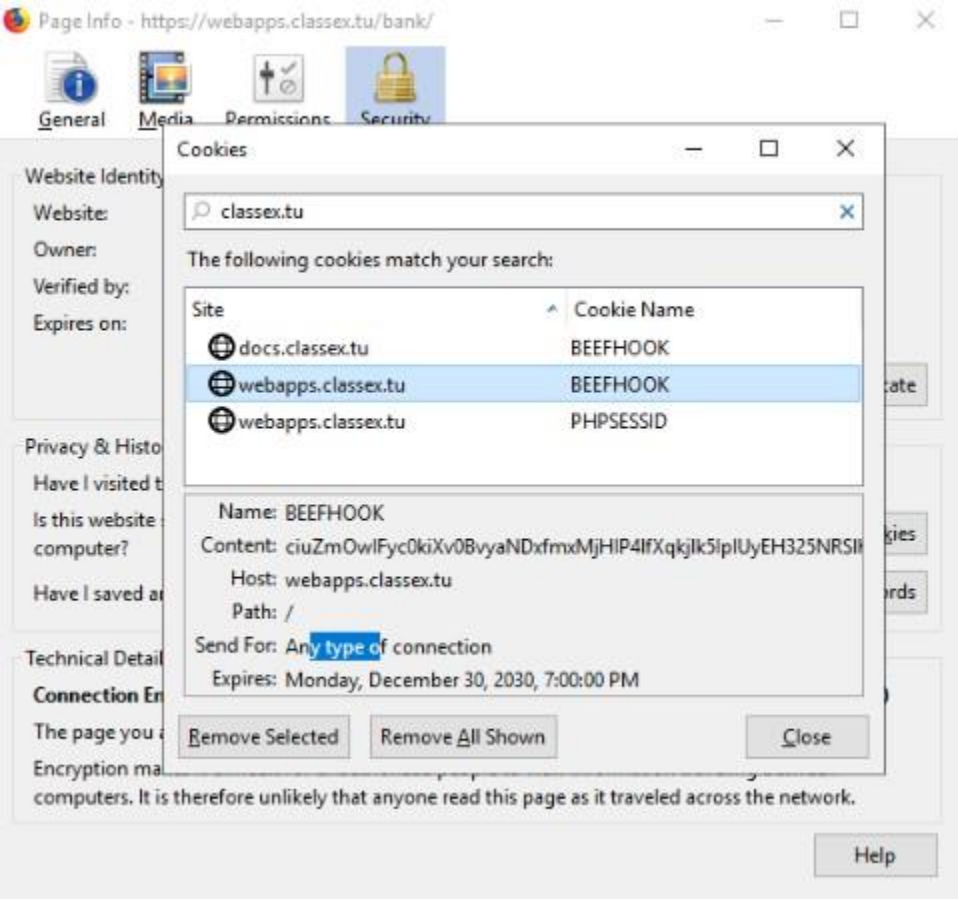
However, when accessing the bank site, we can see that it's the malicious certificate that is being used for verification:



If we were to export the certificate, we would see that the issuer would be redteam@classex.tu



This led the IT team to the conclusion that a fake bank website was being hosted for users to enter their credentials, which were likely being forwarded to the threat actor. By comparing the fake site to the legitimate site, we can see that the fake site is using cookies to store information about the user. Checking the cookies shows cookies named BEEFHOOK. BEEF is a popular penetration tool for websites that can inject JavaScript into the user's PC. This can be used further to log the keystrokes of the user accessing the website.



When the user logs in, the website will forward a valid address and redirect users to the official bank dashboard, requiring the need for both certificates to state both sites were secure to trick the user.

Initial Access:

It is unknown the exact date the malicious certificate was placed into the CA (as our central logging server was configured to only store logs up to 30 days for each system). However, inspecting the properties of the certificate shows it was created 03/03/2024 at 17:00 EST and

owned by dsouth, a member of the IT team. It is believed that the credentials of this user for the steel domain were compromised, and the supposed red team used his account to transfer over the file (as windows typically associates the owner of a file to the user who downloaded it). The threat actor would also ensure that both certificates were in the users trusted certificates folder in Firefox, who simply had to wait until the user logs into the bank.

Execution:

Upon visiting the visiting fake bank site, a BEEF extension will then log any credentials the user types into the site. The website will appear secure to the user since a malicious certificate was planted that authenticates it and allows the threat actor to steal the credentials. The threat actor would then wait and use the stolen credentials to exfiltrate all bank credits within the organizations bank into their own accounts.

Evasion/Persistence:

By keeping the original certificate with the malicious certificate inside the users trusted certificates database in Firefox, the threat actor would be able to create a request and forward the users account to the official bank, making it unsuspecting that a compromise had occurred in the first place. Judging from the time the certificate was created/downloaded on the machine and the time the attack, the threat actor likely had access to the credentials for an extended period of time, but chose to wait before exfiltrating the payload, making it harder to pinpoint the origin of the attack or how the attack was performed, with the only evidence being certificates left undeleted from their attack as clues.

Impact:

This attack caused our organization to lose 2,934 credits, accounting for 49% of the organizations total earning as of 04/15/24 (time of the attack), setting the team back in pace for purchasing future flags (as the IT team was waiting to launch an offensive attack on foreign teams file shares before purchasing more). The discovery of compromised credentials of user dsouth also meant an administrative password for all windows systems on the steel domain had also been compromised, with the threat actor able to move laterally to other critical systems (like our HESK and File Share information systems). As of 5/19/2024, the IT team were unsuccessful in finding a method to re-obtain the stolen credentials.

Response:

Immediately after the attack, a request was sent to change the password for the exercise credentials (used to access information systems hosted on the webapps domain). An emergency policy was immediately introduced that banned all IT team members from using the new credentials until a new policy/system was formed that would prevent future compromises. After the discovery of dsouths credentials being potentially compromised, the account was audited with all passwords changed.On 04/17/2024, the IT team created two new systems, and a new policy for handling exercise credentials.

The two new machines created were Paris, a Windows 11 workstation, and Orange, a Ubuntu 22.04 workstations, with a new policy that strictly limited the use of exercise credentials to these two machines. These machines would be treated with the utmost discretion and would remain powered down when not in use. The following is a breakdown of each system and policy.

Paris – This machine would handle light uses of the exercise network, including checking nagios, checking emails, and checking the organization's bank balance. The machine uses a dynamic IP address, with all forms of remote desktop/ssh capabilities uninstalled and disabled, containing a single account for logging in. The system is installed with Firefox that contains a trusted certificate to the webapps/classex websites.

Orange – This machine shall only be used when flags for the Bank need to be transferred to and from the system and will remain offline at all other times. The systems setup is like Paris but excludes the strict disabled remote connection features.

We hope by limiting the amount of time these system remains online we reduce the time threat actors can access the machine or attempt to intercept our connection with webapps. As of 5/19/2024, there have been no indications of exercise credential compromise within the organization.