Incident Report

Affected User: Jacqueline [redacted]
Role: [redacted]
Victim Email address: jacqueline.[redacted]
Incident type: Business Email Compromise (BEC) attack

Incident description:
There was a suspicious email thread about invoice which had four different parties involved:

- Jagjeet [redacted] ([redacted]) - received the email from Jacqueline on September 26, 2024 3:27 PM under the subject of "1099 contractors".
- Anthony [redacted] Coordinator)
- Paul [redacted])
- Don [redacted])
- Heather [redacted] Supervisor) – received an email on October 3, 2024 12:29 PM under the subject of "AR Report".

These users above had communicated back and forth with the attacker in the email threads.

Initial Investigation & Containment:

Following this discovery, the user's password was reset, and all sessions were revoked. Unrecognized, Authenticator device registered to the account was immediately removed and user was able to re-register her device (iPhone XR) successfully.

After containing the threat completely, we conducted a full root cause analysis investigation. Here are the findings:

Initial Access:

- IP address (89.187.164.82/24) was seen successfully sign in Office 365 Exchange Online using "node-fetch/1.0 (+https://github.com/bitinn/node-fetch)". (The screenshot below is just a small proportion of the whole log.)

Date (UTC)	User agent	Resource	IP address	Location	Status	Multifactor authentication result	Authentication requireme
2024-09-26T18:03:36Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Microsoft Graph	89.187.164.135	Dallas, Texas, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-09-26T18:03:36Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Office 365 Exchange Microservices	89.187.164.135	Dallas, Texas, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-09-26T18:09:09Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Microsoft Graph	212.102.33.83	New York, New York, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-09-26T18:09:09Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Office 365 Exchange Microservices	212.102.33.83	New York, New York, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-09-26T19:24:29Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Microsoft Graph	89.187.164.135	Dallas, Texas, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-09-26T19:24:29Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Office 365 Exchange Microservices	89.187.164.135	Dallas, Texas, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-09-26T19:24:45Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Augmentation Loop	89.187.164.135	Dallas, Texas, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-10-03T16:26:42Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Office 365 Exchange Microservices	181.214.107.248	Chicago, Illinois, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-10-03T16:26:42Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Microsoft Graph	181.214.107.248	Chicago, Illinois, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-10-03T18:28:34Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Office 365 Exchange Microservices	181.214.107.154	Chicago, Illinois, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-10-03T18:28:34Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Microsoft Graph	181.214.107.154	Chicago, Illinois, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-10-03T18:30:02Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Microsoft Graph	181.214.107.154	Chicago, Illinois, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-10-03T18:30:02Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Office 365 Exchange Microservices	181.214.107.154	Chicago, Illinois, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-10-04T14:14:49Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Microsoft Graph	181.214.107.154	Chicago, Illinois, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication
2024-10-04T14:14:49Z	node-fetch/1.0 (+https://github.com/bitinn/node-fetch)	Office 365 Exchange Microservices	181.214.107.154	Chicago, Illinois, US	Success	MFA requirement satisfied by claim in the token	Multifactor authentication

#1 Screenshot (Azure Ingress Sign In logs)

- From the screenshot above, user agent string belongs to node-fetch, which is a library used to perform HTTP requests (more often, in the automatic mode as a web crawler or bot).
- Various IP addresses (89.187.164.0/24) were seen authenticated MFA as a user in Azure sign in on 2024-09-26.

These are malicious IP addresses were seen performed interactive sign in from Jac's account.

- 181.214.107.154
- 181.214.107.248
- 181.214.107.7
- 181.214.107.87
- 89.187.164.77
- 212.102.40.23
- 212.102.40.2
- 89.187.164.142
- 89.187.164.82
- 89.187.164.135
- 212.102.33.83

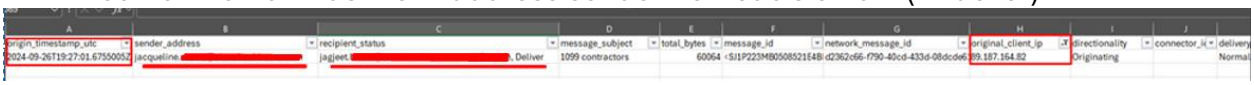
These suspicious IP addresses above were from Texas, Illinois, and New York.

Reconnaissance:

- From the sign in log above, attacker uses the newly created session to roam around the Jackqueline 's mailbox (Microsoft Exchange)
- The attacker must have correspondence any relating transactions history in the victim's mailbox.

Jac's email account got compromised on September 26, 2024 3:27 PM which was the date that attacker used her account on behalf to send an email to jagjeet.[redacted] about fake invoice.

- 89.187.164.82 was the IP address sender from Jac's email. (Attacker)



origin_timestamp_utc	sender_address	recipient_status	message_subject	total_bytes	message_id	network_message_id	original_client_ip	directionality	connector_id	delivery
2024-09-26T19:27:01.6755005Z	jacqueline.[redacted]	jagjeet.[redacted], Deliver	1099 contractors	60064	<SJ1P223MB0508521E4B[redacted]	d2362c66-f790-40cd-433d-08dcde6	89.187.164.82	Originating		Normal

#2 Screenshot (An email was sent to Jagjeet)

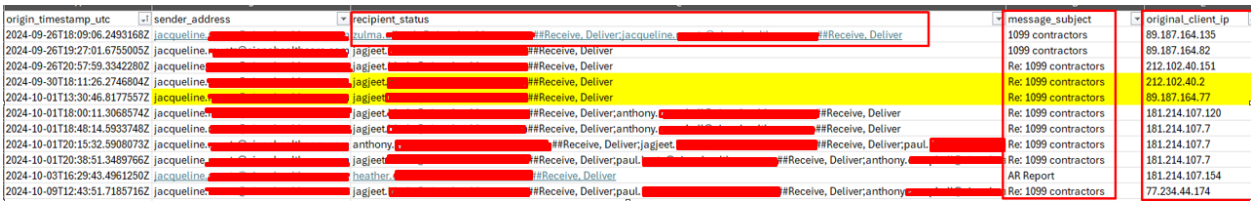
Additionally, the attacker also sent an email to anther user who is zulma.[redacted] under the subject of "1099 contractor". So far, we have not heard anything being reported from Zulma yet.

- 3 IP addresses were the original client IP from the sender address (Jacqueline), as shown in the screenshot below.

origin_timestamp_utc	sender_address	recipient_status	message_subject	original_client_ip
2024-09-26T18:09:06.2493168Z	jacqueline.[redacted]	zulma.[redacted]##Receive, Deliver;jacqueline.[redacted]##Receive, Deliver	1099 contractors	89.187.164.135
2024-09-26T19:27:01.6755005Z	jacqueline.[redacted]	jagjeet.[redacted]##Receive, Deliver	1099 contractors	89.187.164.82
2024-10-01T13:30:46.8177557Z	jacqueline.[redacted]	jagjeet.[redacted]##Receive, Deliver	Re: 1099 contractors	89.187.164.77

#3 Screenshot (Some more emails sent from Jackey to other users)

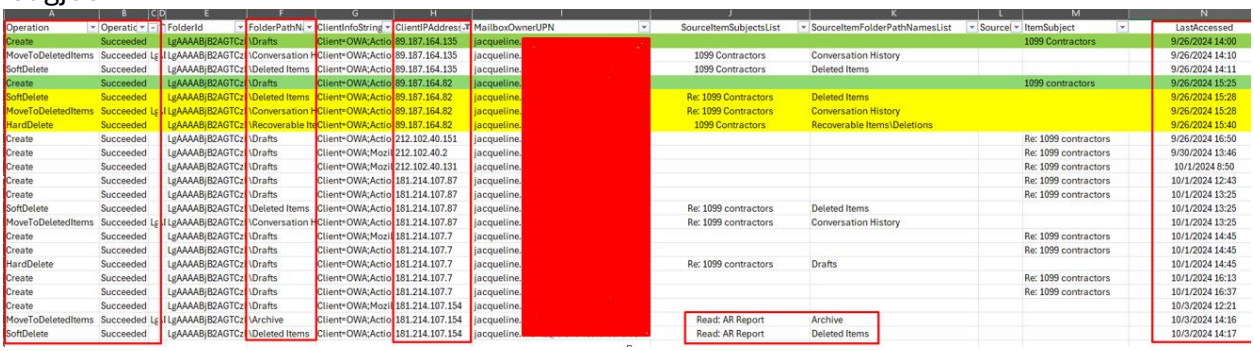
- More IP addresses below were associated from the sender (Jacqueline muntz) as shown below.



origin_timestamp_utc	sender_address	recipient_status	message_subject	original_client_ip
2024-09-26T18:09:06.2493168Z	jacqueline.	ulma. ##Receive, Deliver;jacqueline. ##Receive, Deliver	1099 contractors	89.187.164.135
2024-09-26T19:27:01.6755005Z	jacqueline.	jagjeet. ##Receive, Deliver	1099 contractors	89.187.164.82
2024-09-26T20:57:59.3342280Z	jacqueline.	jagjeet. ##Receive, Deliver	Re: 1099 contractors	212.102.40.151
2024-09-30T18:11:26.2746804Z	jacqueline.	jagjeet. ##Receive, Deliver	Re: 1099 contractors	212.102.40.2
2024-10-01T13:30:46.8177557Z	jacqueline.	jagjeet. ##Receive, Deliver	Re: 1099 contractors	89.187.164.77
2024-10-01T18:00:11.3068574Z	jacqueline.	jagjeet. ##Receive, Deliver;anthony. ##Receive, Deliver	Re: 1099 contractors	181.214.107.120
2024-10-01T18:48:14.5933748Z	jacqueline.	jagjeet. ##Receive, Deliver;anthony. ##Receive, Deliver	Re: 1099 contractors	181.214.107.7
2024-10-01T20:15:32.5908073Z	jacqueline.	anthony. ##Receive, Deliver;jagjeet. ##Receive, Deliver;paul.	Re: 1099 contractors	181.214.107.7
2024-10-01T20:38:51.3489766Z	jacqueline.	jagjeet. ##Receive, Deliver;paul. ##Receive, Deliver;anthony.	Re: 1099 contractors	181.214.107.7
2024-10-03T16:29:43.4961250Z	jacqueline.	heather. ##Receive, Deliver	AR Report	181.214.107.154
2024-10-09T12:43:51.7185716Z	jacqueline.	jagjeet. ##Receive, Deliver;paul. ##Receive, Deliver;anthony.	Re: 1099 contractors	77.234.44.174

#4 Screenshot (Some more emails sent from Jackey to other users)

From my observation, the attacker seems to create a draft first before sent an actual email to Jagjeet on 9/26/2024 2:00:04 PM, and then the attacker deleted the email so that the user could not see the email thread in her inbox. Until 9/26/2024 3:40 PM, the attacker recovered the email so that they can respond to the email thread back and forth with "Jagjeet".

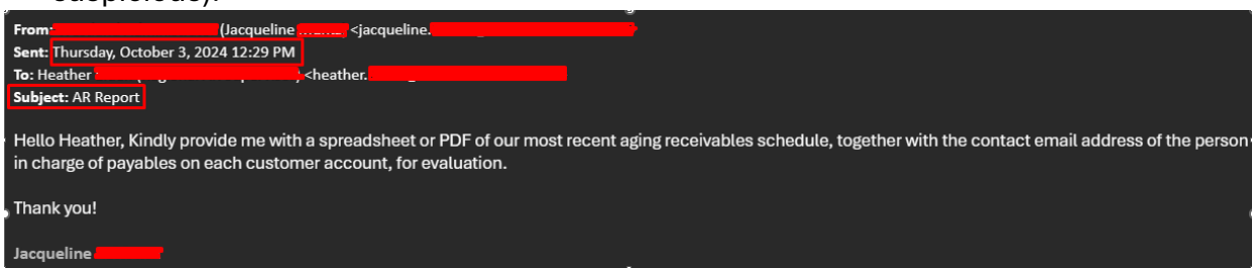


Operation	Operatic	FolderId	FolderPathNa	ClientInfoString	ClientIPAddress	MailboxOwnerUPN	SourceItemSubjectsList	SourceItemFolderPathNamesList	Source	ItemSubject	LastAccessed
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Actio	89.187.164.135	jacqueline.				1099 Contractors	9/26/2024 14:00
MoveToDeletedItems	Succeeded	LgAAAABjB2AGTCz	\Conversation H	Client=OWA;Actio	89.187.164.135	jacqueline.	1099 Contractors	Conversation History			9/26/2024 14:10
SoftDelete	Succeeded	LgAAAABjB2AGTCz	\Deleted Items	Client=OWA;Actio	89.187.164.135	jacqueline.	1099 Contractors	Deleted Items			9/26/2024 14:11
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Actio	89.187.164.82	jacqueline.				1099 contractors	9/26/2024 15:25
SoftDelete	Succeeded	LgAAAABjB2AGTCz	\Deleted Items	Client=OWA;Actio	89.187.164.82	jacqueline.	Re: 1099 Contractors	Deleted Items			9/26/2024 15:28
MoveToDeletedItems	Succeeded	LgAAAABjB2AGTCz	\Conversation H	Client=OWA;Actio	89.187.164.82	jacqueline.	Re: 1099 Contractors	Conversation History			9/26/2024 15:28
HardDelete	Succeeded	LgAAAABjB2AGTCz	\Recoverable Ite	Client=OWA;Actio	89.187.164.82	jacqueline.	1099 Contractors	Recoverable Items\Deletions			9/26/2024 15:40
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Actio	212.102.40.151	jacqueline.				Re: 1099 contractors	9/26/2024 16:50
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Mozi	212.102.40.2	jacqueline.				Re: 1099 contractors	9/30/2024 13:46
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Mozi	212.102.40.131	jacqueline.				Re: 1099 contractors	10/1/2024 8:50
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Actio	181.214.107.87	jacqueline.				Re: 1099 contractors	10/1/2024 12:43
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Actio	181.214.107.87	jacqueline.				Re: 1099 contractors	10/1/2024 13:25
SoftDelete	Succeeded	LgAAAABjB2AGTCz	\Deleted Items	Client=OWA;Actio	181.214.107.87	jacqueline.	Re: 1099 contractors	Deleted Items			10/1/2024 13:25
MoveToDeletedItems	Succeeded	LgAAAABjB2AGTCz	\Conversation H	Client=OWA;Actio	181.214.107.87	jacqueline.	Re: 1099 contractors	Conversation History			10/1/2024 13:25
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Mozi	181.214.107.7	jacqueline.				Re: 1099 contractors	10/1/2024 14:45
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Actio	181.214.107.7	jacqueline.				Re: 1099 contractors	10/1/2024 14:45
HardDelete	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Actio	181.214.107.7	jacqueline.	Re: 1099 contractors	Drafts			10/1/2024 14:45
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Actio	181.214.107.7	jacqueline.				Re: 1099 contractors	10/1/2024 16:13
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Actio	181.214.107.7	jacqueline.				Re: 1099 contractors	10/1/2024 16:37
Create	Succeeded	LgAAAABjB2AGTCz	\Drafts	Client=OWA;Mozi	181.214.107.154	jacqueline.					10/3/2024 12:21
MoveToDeletedItems	Succeeded	LgAAAABjB2AGTCz	\Archive	Client=OWA;Actio	181.214.107.154	jacqueline.	Read: AR Report	Archive			10/3/2024 14:16
SoftDelete	Succeeded	LgAAAABjB2AGTCz	\Deleted Items	Client=OWA;Actio	181.214.107.154	jacqueline.	Read: AR Report	Deleted Items			10/3/2024 14:17

#6 Screenshot (email logs from Jacqueline to other users

Another user received an email from Jacqueline on October 3rd, 2024 12:29PM under the subject of "AR Report" – as you can see from the screenshot #6

- The context inside the email: the attacker was trying to perform more reconnaissance and exfiltrate more information from Heather.
- From the screenshot #5, the attacker created an email on 10/3/2024 12:21PM and then the email was deleted a couple hours later. (This was done to avoid Jacqueline suspicious).

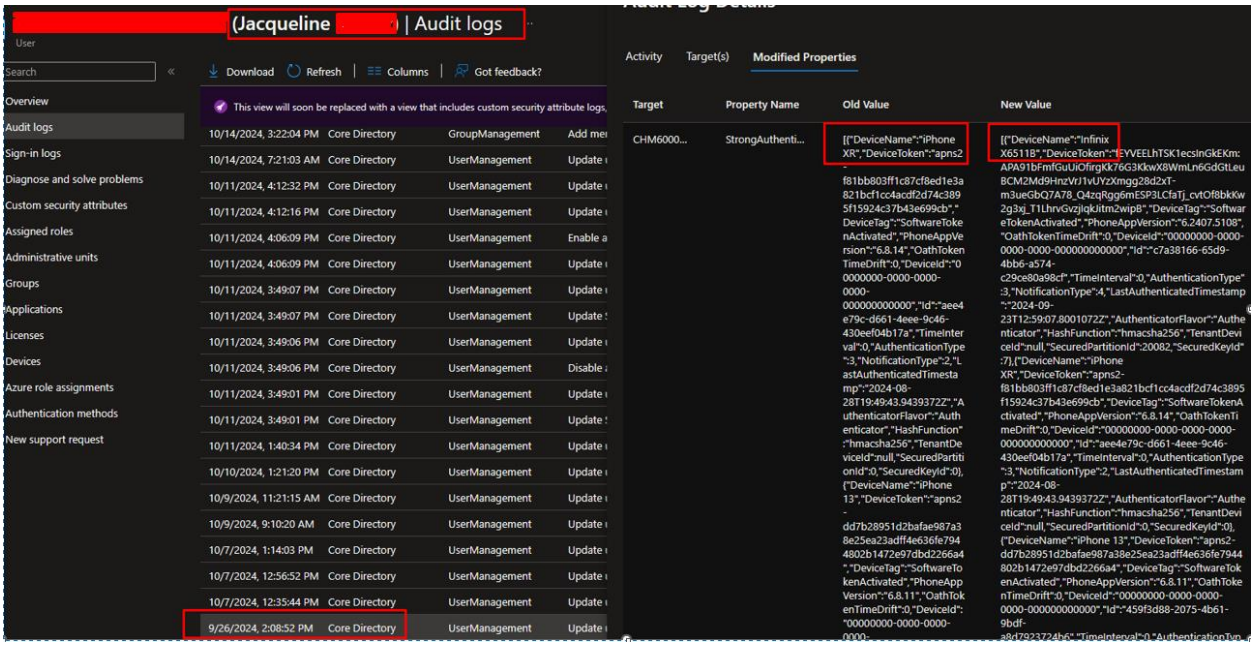


#7 Screenshot (email was sent to Heather)

Persistency:

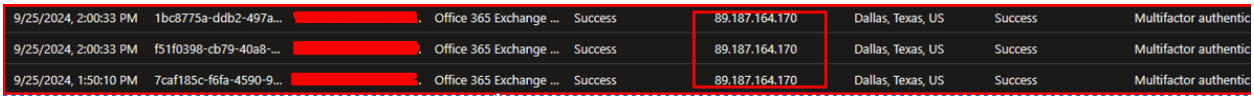
- Further investigation of the compromised account detected that a second Authenticator app had been set up for the user without their knowledge. This gave the attackers full persistence of the breached account and effectively nullified the value of MFA.

Below is an audit log from Jacqueline. The attacker removed Jackey device and replace it with their new device. From "iPhone XR" to "Infinix X6511B".



#8 Screenshot (New authorized device was added)

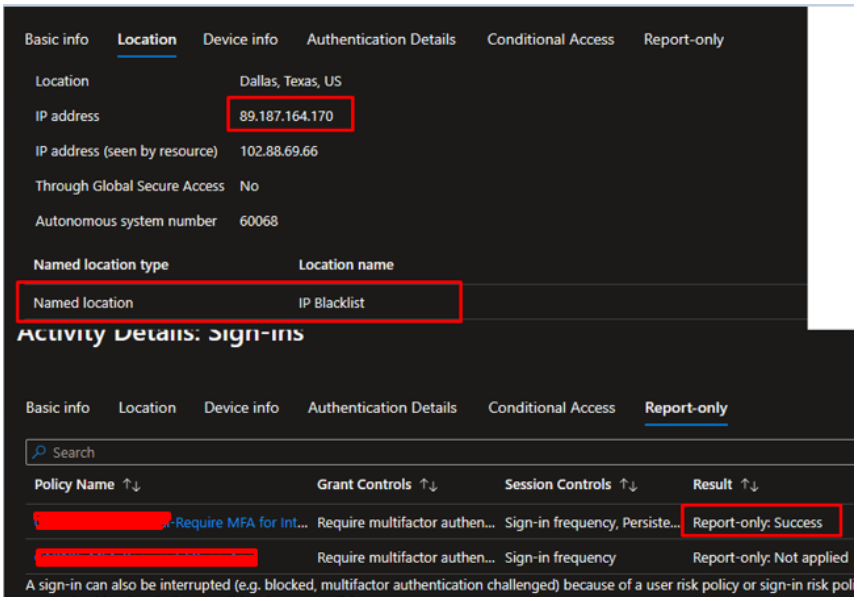
The IP in this ingress was the IP that came from the email that was sent out from Jac email. The incident was reported to IT teams on October 1st. However, the incident started since September 26th based on the email chains.



#9 Screenshot (malicious IP address was seen signing to Jackey's account)

Based on the screenshot below, the attacker was able to sign in successfully using Jackey's email account from IP address "89.187.164.170".
Even though, the IP address was listed under name location "IP Blacklist".

- The sign in attempted was successful due to the session token was compromised from the beginning.
- Sign in frequency was "Persistent", so conditional access did not kick in due to MFA requirement satisfied by claim in the token.



#10 Screenshot (The sign in attempt was successful)

Reason why conditional access did not block the attempt:

- Microsoft reviews the current token in the active session to decide if authentication is necessary. If the session was previously authorized correctly with MFA, Microsoft will not mandate a new MFA challenge. This is reflected in the sign-in logs with the note: "Previously satisfied – MFA requirement satisfied by claim in the token." – Screenshot #1
- Microsoft does not require an MFA re-challenge for accessing or modifying user authentication methods in the Security Info section of the account profile. Users with a Previously Satisfied token can add a new Authenticator app without needing to undergo another MFA challenge. This means that if an account is compromised, even for a brief period, an attacker can use this method to maintain access and reauthenticate with MFA when the session expires or is revoked. It's important to understand that even if an organization enforces a strict MFA expiration policy of one day, this technique can still enable attackers to establish persistent access.

Corrective and Preventative Measure:

- Seeking to implement a new conditional access policy that only requires complaint or authorized device to access company resources.
- Possibly, implement a conditional access policy for token protection (Token Protection Conditional Access policy ensures that tokens are bound to the device they were issued to. If the token is used on a different device, access is blocked.) – need more research and testing on this.
- Create an InsightIDR query that would alert us based on a suspicious "User Agent". As an example from this case, the attacker used "node-fetch/1.0 (+https://github.com/bitinn/node-fetch) while signing in user's account.

- 89.187.164.0/24 and among IP addresses above will be blocked in Name Location in Azure “IP Blacklist”.

Change Log			
REV 1.0	10/30/2024	Soklim Seang	Documentation
REV 1.2	10/30/2024	Soklim Seang	Added more info about Heather