# Recent Cyber Attacks

## Frontier cyber attack

Frontier, a telecommunication giant in the US, was attacked on the 14th of April 2024, [according to the advisory sent to the US Sec and Exchange Commission](https://www.sec.gov/Archives/edgar/data/20520/000119312524100764/d784189d8k.htm). It reported an incident of unauthorised access to its IT systems, which caused a significant portion of its Internal IT network to be shut down to contain and investigate the incident. The company however believe that there was no significant financial damage and that they’re in the process of restoring full business functionality as at the time it was posted on the 18th of April The manner of the breach or the ’How’ was not immediately disclosed and one can only assume until the full report of the incident is revealed. The report mentioned that the Frontier Cyber Security team triggered their existing IR process in trying to contain and remediate the situation.

## Analysis of what possibly happened.

Since there’s no information yet as to the initial access vector, we can guess that it would take one of MITRE ATT&CK frameworks tactics for the initial access, it could have been through any one of the following means:

#### Exploit of public-facing Application

Some threat actors have consistently used this method to compromise public-facing applications or webservers to gain a foothold on the victim's internal network. In the case of Frontier, they believe that a threat group is behind the attack but have no details on the particular threat actors. So on the part of exploiting public-facing applications, it could come in the form of CVEs observed on or more applications in the environment, and could also come in the form of vulnerabilities in the software in use, which allows for remote code execution on the systems in the organization’s network. Hence, my prediction is that the breach could have been through the public-facing hosts, applications, or web servers in the organization if the access vector was a public-facing application.

#### External Remote Services

If the attack’s initial access vector was through the external remote services, then it may have been through some of the remote services such as RDP, VPN, Citrix and some other access methods which grant users access to the org internal network from remote locations. These services require authentication for access to be granted and in most cases, they are exploited, it usually is through a compromised user account and no multiple levels of authentication factors set. Some other times, the compromise could come through the connected public-facing and unauthenticated APIs like Kubernetes API server etc. Groups like Akira ransomware gangs have exploited networks through the use of user's compromised VPN accounts. Other attacks using this attack vector are well documented in the [MITRE](https://attack.mitre.org/techniques/T1133/) site.

#### Phishing

This is one of the most popular methods through which attacks on networks have been delivered. It could come in the form of phishing messages, emails, or all forms of electronically delivered social engineering, which aims to trick users into performing an action that could allow the adversary access into the org network. So, in the case of Frontier, a targeted phishing email (Spear phishing, Whaling and other forms of targeted phishing) could have been used to deliver a malicious URL, payload, attachment or in some cases, non-targeted attack such as a phishing mass campaign. More about this can be found on the [MITRE website](https://attack.mitre.org/techniques/T1566/). There have been several cases of different threat groups using phishing methods to gain access to enterprise networks, groups like Axiom, Royal etc have all used different forms of phishing to attack victims in the past.

#### Supply Chain Compromise

Another way the adversary may have used in gaining access to the company’s internal network could be from the supply chain, the 3rd party suppliers to the organization may be compromised and through them gain access, could be in the form of manipulating development tools, compromised system images and replacement of legitimate software with modified versions. Many open-source projects that are used as dependencies can be exploited to deliver malicious code or a backdoor like the case of the Linux Tar utils. More can be found [here](https://attack.mitre.org/techniques/T1195/)

#### Valid Accounts

The last method to look at as one of the possible initial access vectors in the attack is valid accounts. It can come in the form of a threat actor’s brute forcing public-facing services or resources to obtain a valid account for login, which would enable them to bypass security controls in place. Another means can be from past compromised accounts of a member of the organization, it could be from a leak such as LinkedIn, where user credentials were leaked. Such credentials could be used by threat actors with access to such data to carry out future authentication attacks.

## What could have been done to prevent this attack or possible mitigations?

There are ways an organization can proactively reduce the chance or possibility of an attack, for instance, exploit of facing public applications, valid account, external remote services and to an extent, phishing, boils down to below points.

* Review and enhance the conditional access in place, to block access not meeting set conditions.
* Enable multi-factor Authentication across the organization, even for test tenants or networks.
* Regularly review your UEBA policies and rules with the latest threat intelligence data, this can help detect malicious intent.
* Continually test and review your network segmentation and the practise of least privilege, this limits the access of the compromised account in accessing sensitive resources or data in the organization.
* For public-facing resources and applications, ensure constant and active monitoring of user sessions and IP connections.

This document will be updated as more information emerges from the attack.