Workforce Security: The Frontline of Cyber Defense

Hung Ngo
Cyber Security Specialist
(ŠKODA Auto)

Hung Ngo

Cyber Security Specialist (ŠKODA Auto)

Lecturer

Speaker

BSides Prague Co-Organizer

hungoboss hungoboss.com

What is Workforce Security?

“Workforce security is about protecting a company’s sensitive information by ensuring that the people who work there—employees, contractors, or anyone with access.”

Right Access

Only the right people can access the right information, and only when they need it for their job.

Training

Teaching workers how to recognize and avoid security risks, like phishing emails or weak passwords.

Monitoring

Keeping an eye on who is accessing systems and data to make sure there’s nothing suspicious.

Policies

Setting rules for things like passwords, device usage, or what to do if there’s a breach.

What is Digital Identity?

“A digital identity is the unique set of identifiers and attributes associated with an individual, organization, or device in the digital world.”

Emails

Biometric Data

Fingerprints, Facial Recognition, Iris Recognition, Retina Scan etc.

Social Media Profiles

Digital Certificates

Why is Workforce Security matters?

There are multiple factors that are affecting why workforce security matters:

Hybrid and Remote Work

The pandemic accelerated the shift to remote and hybrid work, with 60% of employees now working remotely at least part of the week.

Cybercriminals Target Employees

Social engineering campaigns are designed to exploit human errors, such as clicking malicious links or downloading infostealer malware.

Rise of Infostealer Malware

Infostealer attacks increased by 300% in the past year, becoming one of the most significant threats to employee credentials.

Evolution of Workspace Security

Traditional Era

(1990s-2000s)

- Relied on firewalls, antivirus software, and physical security to protect corporate networks.
- Password policies were minimal, often relying on static or weak passwords.
- Limited remote work, meaning security threats were largely internal or on-premises.

Cloud Era

(2010s)

- The adoption of cloud services (AWS, Azure, Google Cloud) created new security challenges.
- Employees began accessing data from multiple devices, including personal laptops and mobile phones (BYOD policies).
- Organizations started implementing Single Sign-On (SSO) and basic Multi-Factor Authentication (MFA) for cloud applications.

Post-COVID Era

(2020s+)

- The shift to hybrid work has made traditional perimeter-based security obsolete.
- Zero Trust Architecture: Every request is verified—users, devices, and locations must meet security policies.
- Adoption of Adaptive Authentication: Security systems adjust access requirements dynamically based on risk (e.g., requiring additional verification for high-risk logins).

MFA and why it matters?

"Multi-Factor Authentication (MFA) and a strong digital identity are essential in workforce security because they significantly reduce the risk of unauthorized access to sensitive systems and data."

Weak MFA Issues

Vulnerabilities of SMS-based MFA, MFA Fatigue Attacks, Static MFA Factors

Passwordless Auth

Eliminates the reliance on traditional passwords by using alternative methods like biometrics, hardware tokens, or cryptographic keys.

Biometric Auth

Uses unique biological traits such as fingerprints, facial recognition, or voice patterns which are hard to replicate.

Adaptive MFA

Context-aware MFA that dynamically adjusts authentication requirements based on risk factors.

Infostealers: A Growing Threat

“Infostealers are a rapidly growing threat in the cybersecurity landscape, with recent data highlighting their increasing prevalence and impact.”

Broad Data Collection

Infostealers can harvest a wide range of sensitive information, including credentials, cookies, autofill data, and even cryptocurrency wallet keys.

Ease of Use

Many infostealer malware kits, like RedLine or Raccoon, are sold cheaply on underground forums or as Malware-as-a-Service (MaaS).

Rapid Exfiltration

Infostealers operate quickly, often exfiltrating data in seconds without noticeable impact on the infected system.

Post-Exfiltration Threats

Stolen credentials and data are often sold on dark web marketplaces, enabling further exploitation by multiple actors.

GRIM_NOID STEALER V3 |UPDATED|CRYPTO GRABER|NATIVE|NO TRACES|

~~$150.00~~ $110.00

Grim_Noid stealer is a Native stealer that no need shit framework for excuation

° Native Stiller

• Excellent build weight (360 kb)

• No downloads from the Internet

• High collection rate

• Collection from all computer accounts

• Collecting data from the client SA: MP (nickname, database of favorite servers)

• Collecting data from Chromium browsers and browsers with non-standard data location (Passwords, Cookies, Autocomplete, Card Data)

• Support for Chrome all versions

• Collect passwords from Edge

• Collect Discord sessions

• Collection of all Telegram sessions

• Collect FileZilla passwords (new / old)

Real World Impacts of Workspace Security Failures

Uber 2022 Incident

“Attacker gained internal access using compromised credentials and MFA fatigue.”

Uber 2022 Incident

Uber 2022 Incident

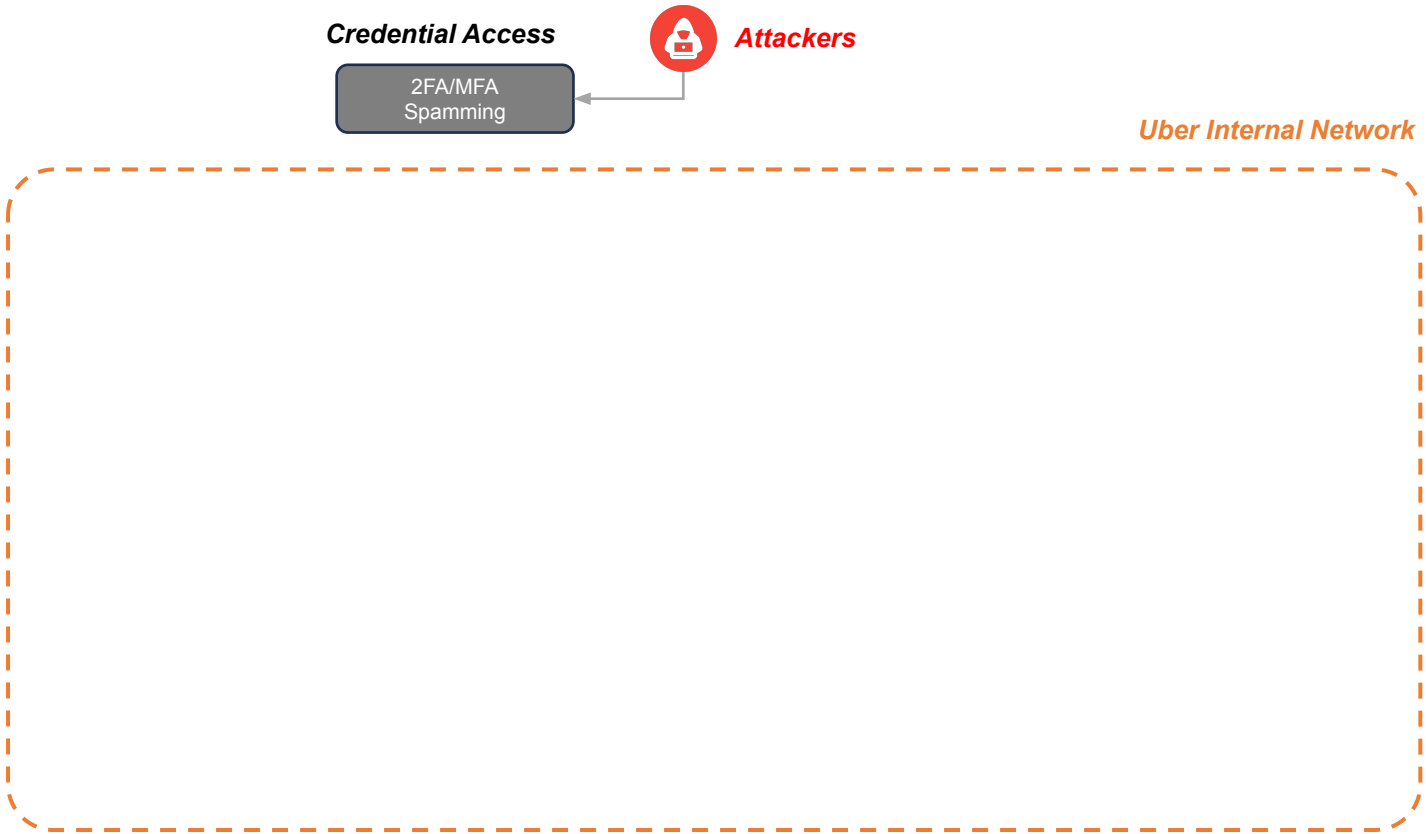
Attackers

Uber 2022 Incident

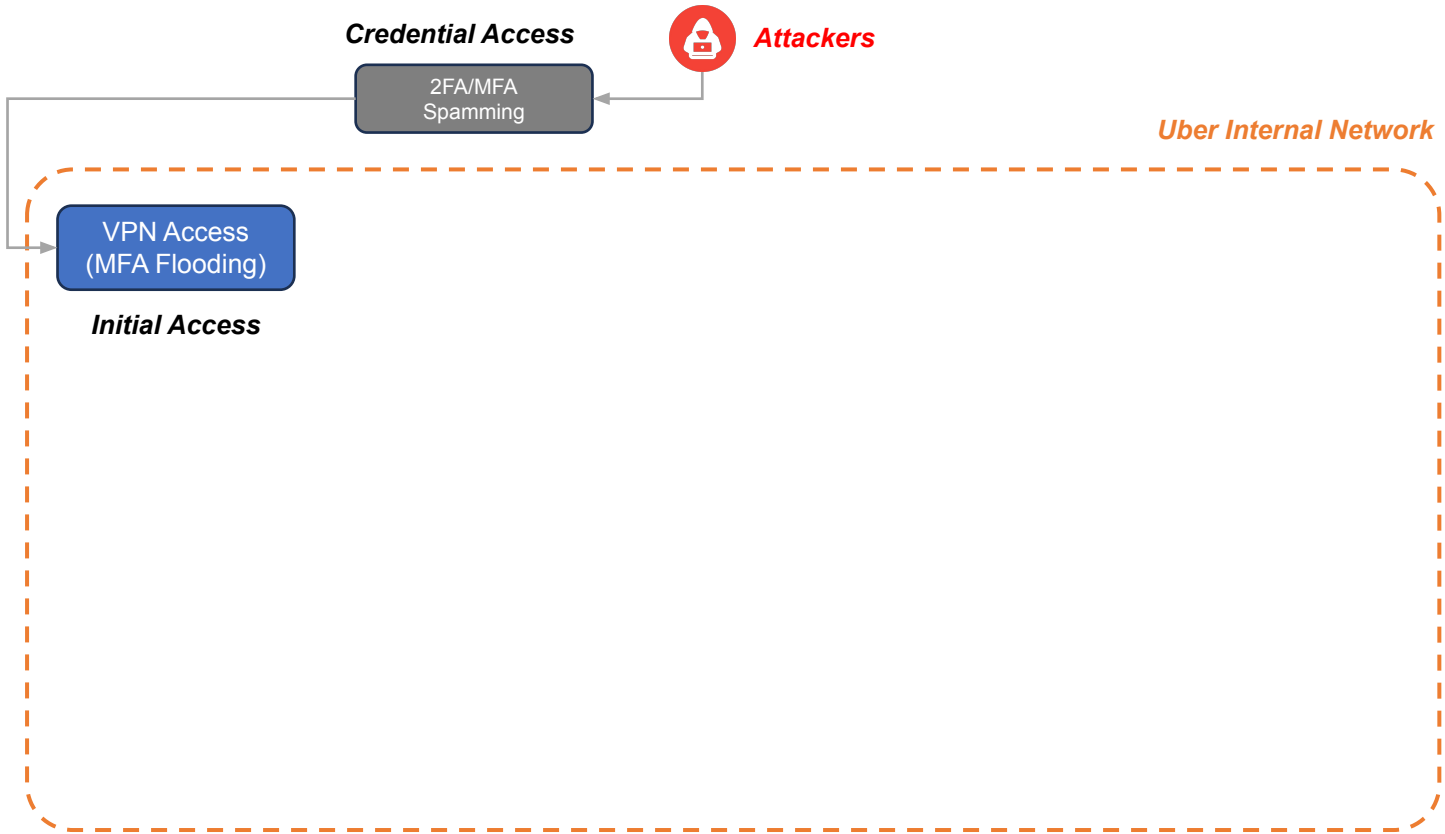
Attackers

Uber Internal Network

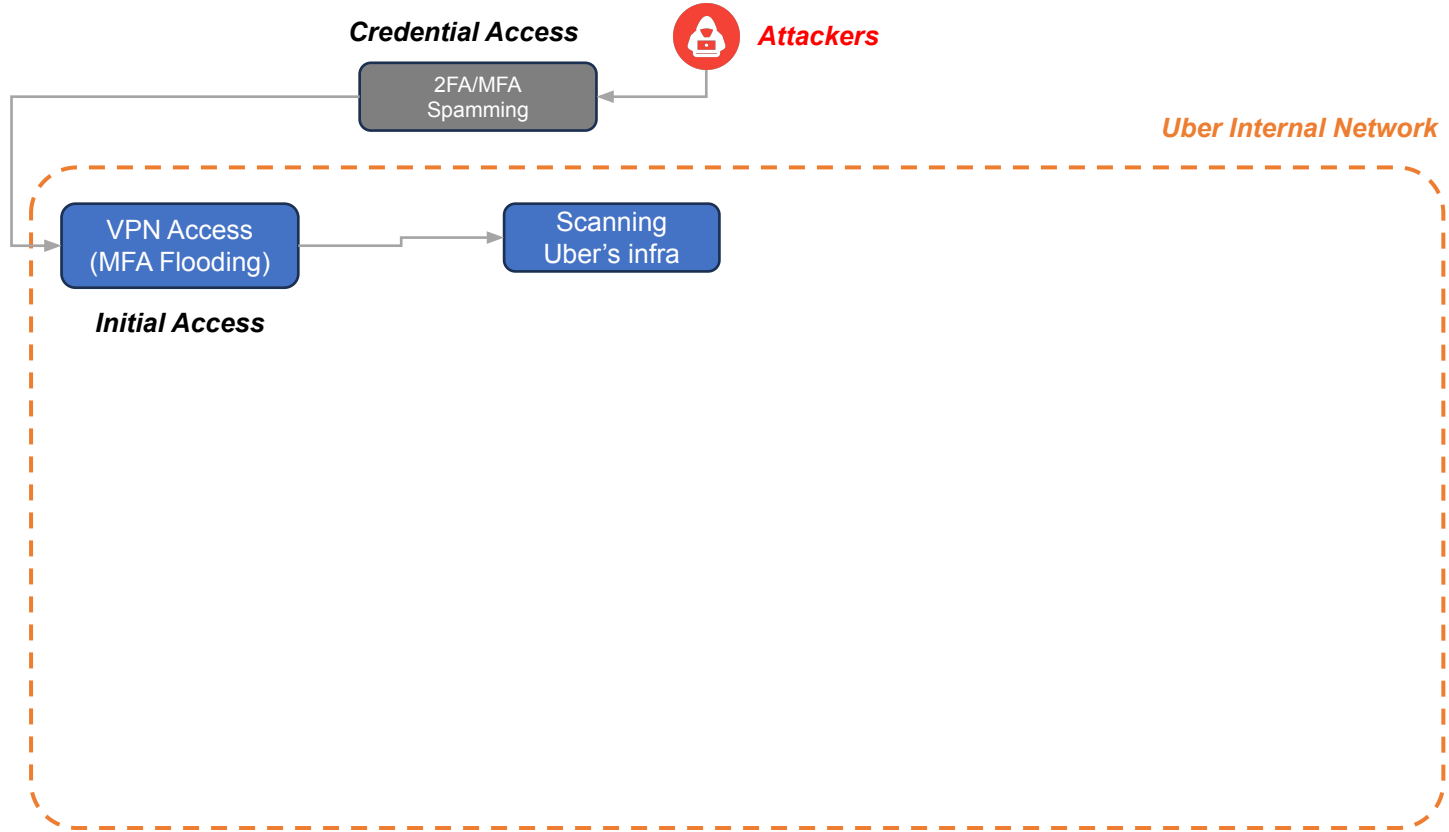
Uber 2022 Incident



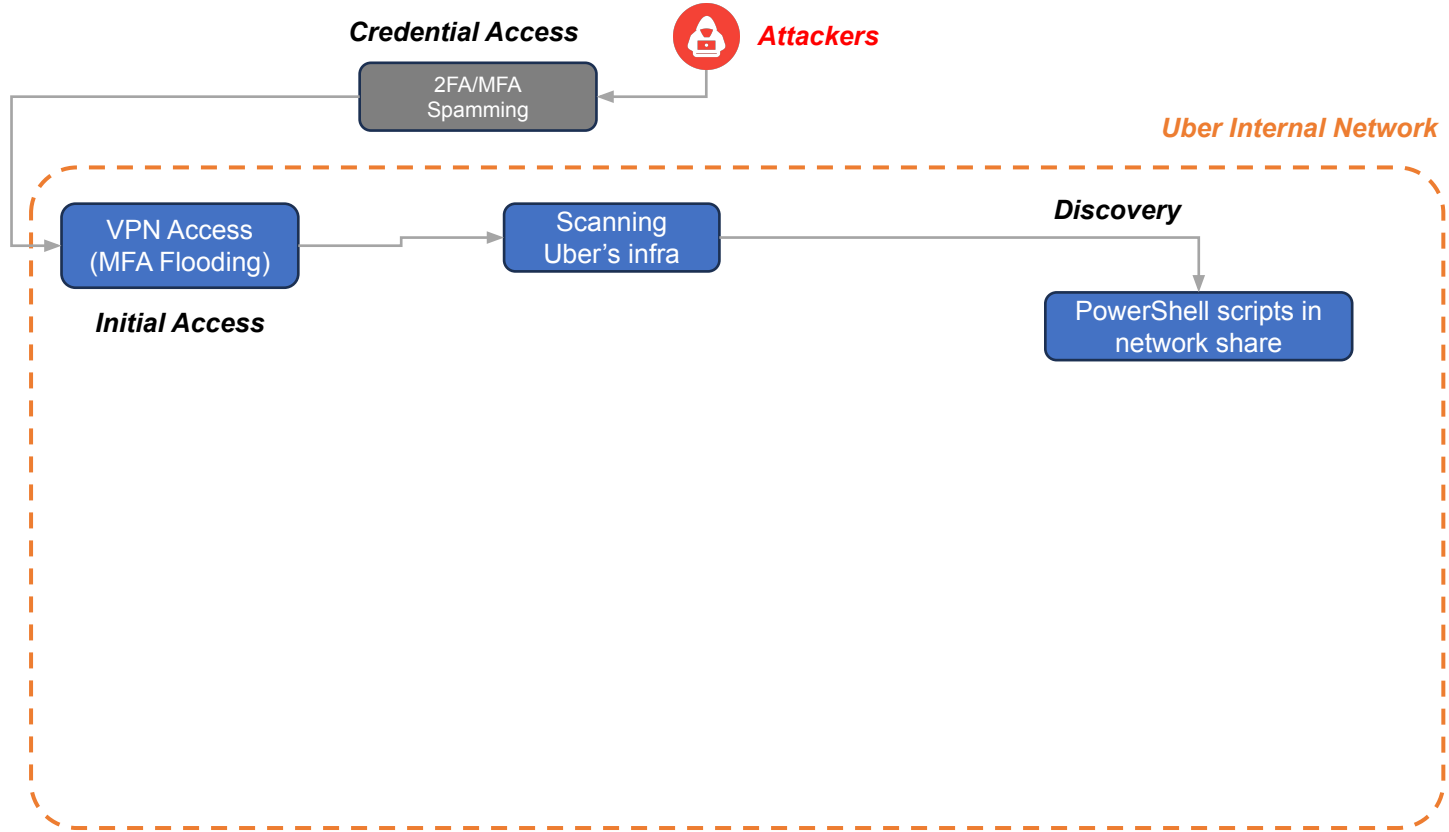
Uber 2022 Incident



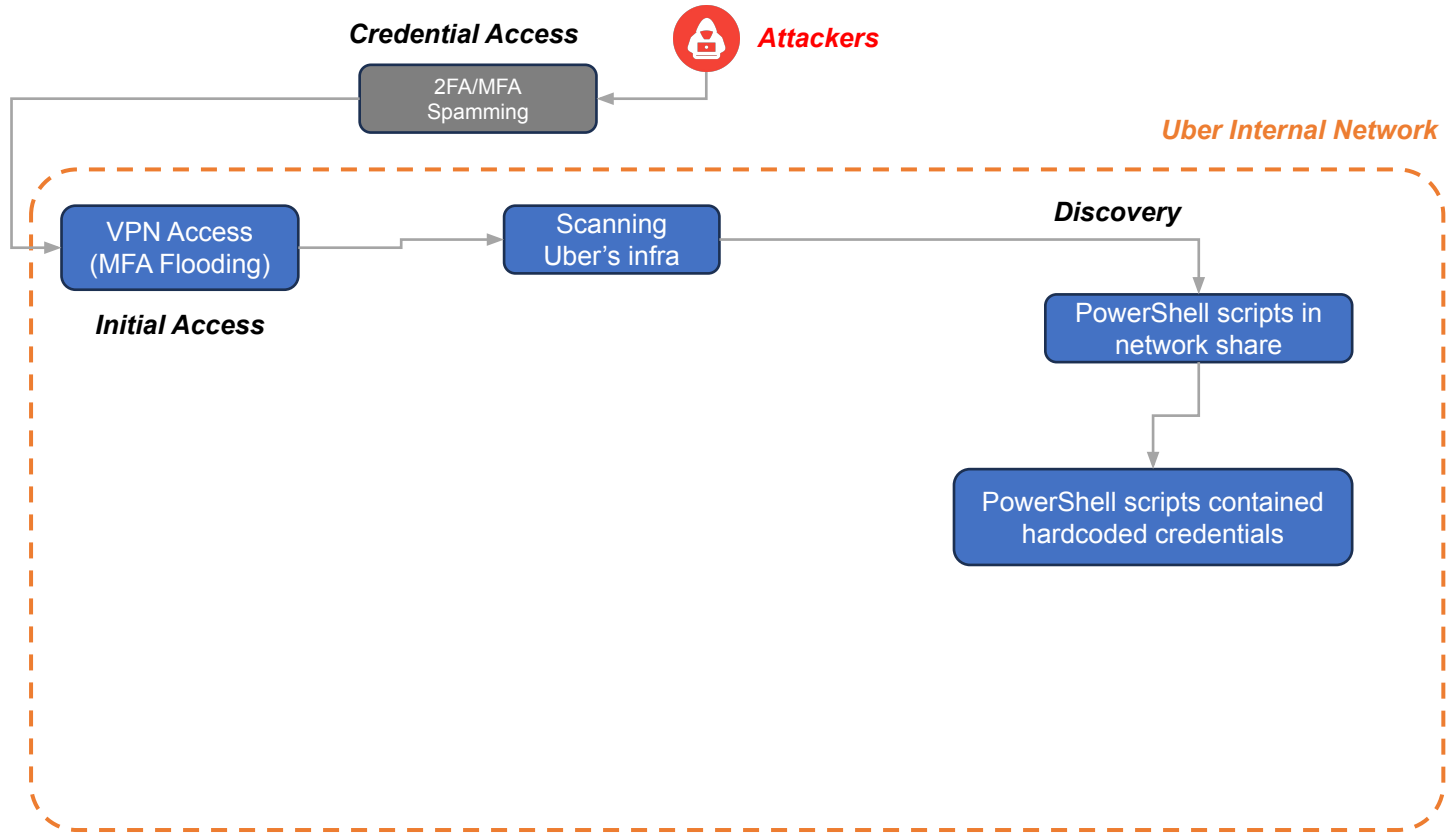
Uber 2022 Incident



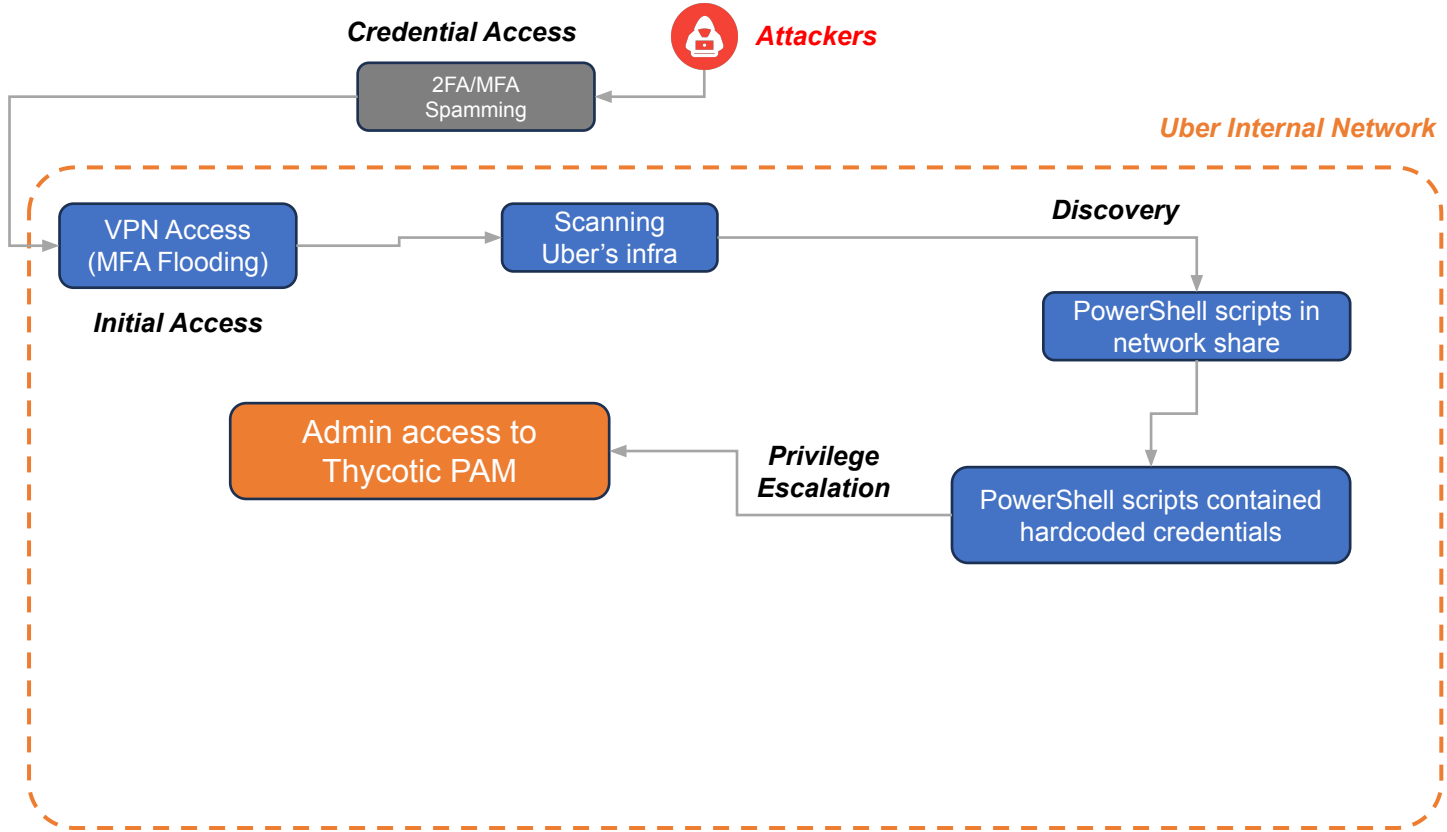
Uber 2022 Incident



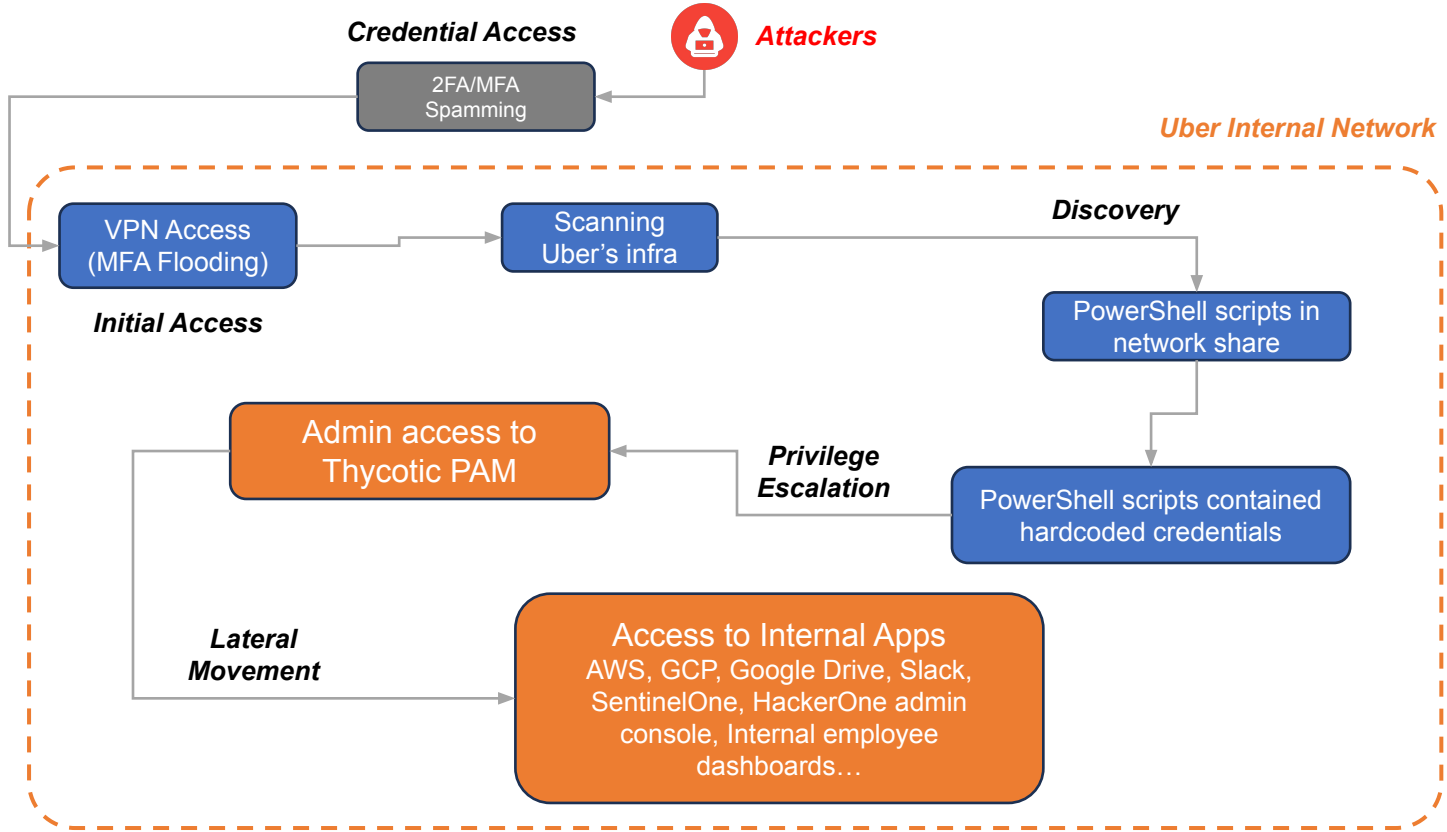
Uber 2022 Incident



Uber 2022 Incident



Uber 2022 Incident



Thank you!

proid.tech