Covering: The North Face Attack

About

The North Face is an American outdoor apparel and footwear company owned by VF Corporation. It recently suffered a cyberattack.

Information about the Attack

- According to VF Corporation's email to customers, the attack was discovered on 29 April 2025, when they observed unusual activity on their website.

- The attack was a credential-stuffing incident. Credential stuffing involves using credentials (email/username/telephone number and password) obtained from previous data breaches of other applications or services. Attackers compile lists of valid credential pairs and attempt to log in on a target website—in this case, thenorthface.com.

- If a user has reused the same credentials on multiple sites, an attacker can log in on the non-compromised site by using that same combination.

Impact of the Attack

- Because attackers were able to log in as legitimate users, they accessed all information available to those users. Affected account details included:

    - Purchase history
    - Shipping address(es)
    - User preferences
    - Email address
    - First and last name
    - Date of birth
    - Telephone number

- VF Corporation claims that they use tokens linked to users' credit cards and that those tokens are only meaningful on their own website; actual credit card information is stored by a third-party payment processor. Therefore, no credit card data was directly disclosed.

- However, if the third-party processor lacked adequate security measures, an attacker—already logged in as a user—could potentially make purchases on The North Face website using the user's stored payment method.

- To mitigate further damage, VF Corporation disabled existing passwords and asked all customers to create new, unique passwords for their web services.

Possible Intent

1. **Customer Data Collection**
    - Retail companies hold large amounts of personally identifiable information (PII). Attackers can leverage stolen PII for various secondary purposes—for example, crafting highly targeted phishing campaigns aimed at individuals known to be outdoor enthusiasts or employees of companies with a high hiking culture (and therefore likely to own The North Face gear).

2. **Advanced Persistent Threat (APT) / Industry-wide Campaign**
    - Other retail brands—such as Victoria's Secret and Adidas—have suffered sophisticated cyberattacks, suggesting a possible coordinated wave targeting the retail sector. This could be influenced by broader political tensions that escalated in early 2025.

Hypothesised Kill Chain (Mapped to MITRE ATT&CK Framework)

1. **Reconnaissance (T1589)**
    - The attacker gathered account identifiers (email addresses, usernames, telephone numbers) for existing The North Face customers. Although credential harvesting can be “blind,” the fact that The North Face was singled out suggests pre-attack planning.

2. **Weaponisation (T1587, T1588, T1608)**
    - After obtaining credential lists, the attacker likely acquired or developed an automated credential-stuffing tool.
    - They probably tested the tool in a controlled environment to validate its effectiveness against The North Face’s defences before launching the live attack.

3. **Delivery & Exploitation (T1110)**
    - The attacker used their credential pairs to brute-force the login portal on thenorthface.com until valid combinations were found.
    - VF Corporation’s notice mentioned observing “suspicious behaviour” on the network—consistent with automated login attempts (e.g., rapid-fire HTTP requests from a script).

4. **Installation & C2 (T1098)**
    - In this particular incident, no malware was installed, and no persistent backdoor was established.
    - However, had the attacker desired long-term control, they could have changed account credentials—locking out the legitimate user—and effectively “owned” those accounts.

5. **Objectives & Data Exfiltration**
    - Once logged in, the attackers extracted all available user data.
    - VF Corporation’s monitoring and anomaly detection likely flagged irregular account activity, leading to the attack’s discovery.

Professional Investigation Report

- According to CyberInsider, VF admitted in April 2025 that a similar credential-stuffing attack had gone undetected for two years. They recommended implementing two-factor authentication (2FA) as an actionable mitigation that might have prevented or reduced the scope of the breach.

Lessons Learned & Takeaways

Scope of Research

Unlike the professional report, this analysis did not investigate The North Face's prior security incidents in depth, nor did it document preventive controls (beyond mentioning 2FA). However now that I think of it there are other things that the company could implement to mitigate this sort of attacks: revisit their captcha implementation and how they limit access attempts for example.

User Impact vs. Corporate Messaging

VF's customer notification emphasises that no payment card data was compromised. However, the exposed PII is nonetheless highly sensitive:

- Threat actors can use it for spear-phishing (T1598.001).

- Extremist or opportunistic groups could leverage PII to orchestrate attacks that extend into the physical world (for example, targeting individuals' home addresses).

It is also worth considering how the attacker might have proceeded if their objective extended beyond harvesting user credentials. For instance, if the goal was to inflict operational damage, tactics like Distributed Denial of Service (DDoS) attacks could come into play. While network-based DDoS attacks (T1498) are common and many companies are equipped to mitigate them, a server-side Denial of Service (T1499)—executed from authenticated user sessions—could be more difficult to detect and mitigate. One hypothetical approach might involve leveraging compromised accounts to submit a large volume of fake orders, overwhelming backend systems. Additionally, they could have explored vulnerabilities within the user-facing components of the web application potentially escalating their access or pivoting into other parts of the infrastructure.

References

CyberInsider (2025a) The North Face Suffers New Credential Stuffing Customer Data Breach [online]. Available at: https://cyberinsider.com/the-north-face-suffers-new-credential-stuffing-customer-data-breach/ (Accessed: 4 June 2025).

CyberInsider (2025b) The North Face and Timberland Inform Customers of Two-Year-Long Breach [online]. Available at: https://cyberinsider.com/the-north-face-and-timberland-inform-customers-of-two-year-long-breach/ (Accessed: 4 June 2025).

Drapers Online (2025) North Face Latest Fashion Business Hit by Cyber Attack [online]. Available at: https://www.drapersonline.com/news/north-face-latest-fashion-business-hit-by-cyber-attack (Accessed: 4 June 2025).

Forbes (2025) Password Attack—The North Face Confirms Data Breach [online]. Available at: https://www.forbes.com/sites/daveywinder/2025/06/03/password-attack---the-north-face-confirms-data-breach/ (Accessed: 4 June 2025).

Maine Government (2025a) Data Breach Notice [online]. Available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/593485db-511e-4f73-a651-dcba80565f3e.html (Accessed: 4 June 2025).

Maine Government (2025b) Data Breach Notice [online]. Available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/792aded4-8b07-4c1d-86ac-5ae24253b722.html (Accessed: 4 June 2025).

MITRE (no date) ATT&CK Framework [online]. Available at: https://attack.mitre.org/ (Accessed: 4 June 2025).

The North Face (no date) Our Story [online]. Available at: https://www.thenorthface.com/en-us/about-us/our-story (Accessed: 4 June 2025).

The North Face (no date) About Us [online]. Available at: https://www.thenorthface.com/en-us/about-us (Accessed: 4 June 2025).

Vermont Attorney General (2025) VF Outdoor Data Breach Notice to Consumers [online]. Available at: https://ago.vermont.gov/document/2025-05-29-vf-outdoor-data-breach-notice-consumers (Accessed: 4 June 2025).

BBC News (2025) North Face Cyber Attack [online]. Available at: https://www.bbc.com/news/articles/c39x3jpv8lyo (Accessed: 4 June 2025).