VictoriaSecretes_Attack_cleanversion

Date and Time of Report
• **Date of Report:** 2 June 2025

1. Information About the Attack

◇ **Date of Attack:** 26 May 2025

◇ **Victim:** Victoria's Secret (USA website)

◇ **Initial Takeaways:**

▪ The U.S. site was taken offline as a precaution—other regional sites stayed up.

▪ It looks like their payment gateway might've been outdated, so they shut things down to prevent further damage.

▪ Only the U.S. servers were affected, which suggests either regional separation or looser policies in the U.S. compared to other regions.

▪ News reports (e.g., The New York Times) point to a third-party integration as the entry point—probably a sign of weak network segmentation or too much
trust placed in that external service.

2.Impact of the attack

(what was peaced together)

◇ **E-commerce Site Offline:** The entire U.S. online store was down. Customers couldn't return online orders in person, and online customer-care was
unavailable.

◇ **In-Store Effects:** In-store registers worked for regular sales, but any service tied to the website—like order returns—wasn't functioning.

◇ **Email Systems:** Some employees were locked out of their email accounts, hinting that attackers had grabbed credentials and administrators cut access to
contain the breach.

◇ **Other Retailers Hit:** Marks & Spencer, Adidas, and Harrods saw similar issues around the same time, all linked to a shared third-party vulnerability. It feels
like a coordinated attack on big U.S. retailers.

What the Attackers Got

◇ **Disrupted Sales:** Forcing the site down meant lost sales and frustrated customers.

◇ **Possible Data Theft:** With employees locked out, it seems likely they were exfiltrating data—maybe customer payment info or internal documents.

◇ **Show of Force:** Exploiting legacy COBOL backends and weak third-party controls shows attackers know the retail space well. It's a warning to others in the industry.

3. Why They Did It (Hypotheses)

- **Financial Gain:**
  - ◇ Victoria's Secret stores lots of payment data. Stolen cards or customer info can be sold easily.
  - ◇ Disrupting the payment gateway could push customers elsewhere or shake down the company for ransom.
- **Brand Damage:**
  - ◇ A breach like this hurts reputation—maybe rival companies or nation-state actors wanted to make a statement, scare shareholders, or influence politics.
- **Part of a Wider Campaign:**
  - ◇ This might be one piece of a bigger APT (advanced persistent threat) hitting multiple retailers.
  - ◇ If Adidas, M&S, and Harrods were hit too, attackers could be aiming for maximum chaos in the retail sector, possibly tied to international tensions.

4. Hypothetical Kill Chain (What We Think Happened)

- **Reconnaissance**
  - ◇ Attackers gathered information on Victoria's Secret: Reddit posts about outdated COBOL systems, job ads looking for VBA/SQL skills hinted at internal tools.
  - ◇ They probably mapped out the network, noting flat architectures and third-party integrations.
- **Weaponization**
  - ◇ They could've built a malicious VBA or Office-macro document for phishing.
  - ◇ They also may have prepared exploits targeting an old payment-gateway plugin or API endpoint.
- **Delivery**
  - ◇ A spear-phishing email with a macro-laden attachment sent to key staff.
  - ◇ Automated scans targeting known weaknesses in third-party payment or inventory APIs.
- **Exploitation**
  - ◇ Once someone clicked the malicious macro, they harvested credentials.
  - ◇ Or they directly hit an unpatched gateway endpoint to get a foothold.
- **Installation**
  - ◇ Deployed a backdoor on the webserver or the compromised third-party server.
  - ◇ Made sure they had persistent access to the U.S. region's network.
- **Command & Control (C2)**
  - ◇ Established encrypted channels—likely over HTTPS—to blend with normal traffic.
  - ◇ Used stolen credentials to move laterally into email servers and databases.
- **Actions on Objectives**
  - ◇ **Data Exfiltration:** Pulled customer payment records and possibly employee data.
  - ◇ **Service Disruption:** Possibly dropped ransomware or wiper malware on the servers, forcing a

shutdown.

◇ **Cover Tracks:** Disabled logs or corrupted them to make it harder for IR teams to trace activity.

5. Actual TTPs and Observed Kill Chain

Note: There's no fully public, confirmed breakdown. Below are pieced-together details from media reports and industry chatter. (inference)

- **Initial Access:**

◇ **Third-Party Integration:** Multiple news outlets said attackers went after a payment or inventory integration—likely a misconfiguration, not a zero-day.

◇ **Stolen Credentials:** Locking out employee emails points to credential theft, probably via phishing or insider help.

- **Execution & Persistence:**

◇ **Legacy Exploits:** Reddit users mentioned COBOL-based systems that are hard to patch, so attackers may have dropped custom scripts there.

◇ **Macro Malware:** The heavy use of VBA inside the company (per job ads) suggests they used Office macros to get code running on internal machines.

- **Privilege Escalation & Lateral Movement:**

◇ **Credential Theft:** Once attackers had admin or employee creds, they hit email servers and internal databases.

◇ **Flat Network:** Lack of segmentation meant they could roam from web servers into internal systems.

- **Data Exfiltration & Impact:**

◇ **Ransomware Signs:** The fact that they kept things offline indicates databases might've been encrypted, or they paused data flows to stop leaks.

◇ **Business Disruption:** The core web services stayed down longer than expected, suggesting they were cleaning up or negotiating.

- **Detection & Containment:**

◇ **Email Lockouts:** Administrators cut compromised accounts to stop attackers in their tracks.

◇ **Website Shutdown:** Taking the U.S. site offline stopped additional data from leaking and curtailed lateral spread.

6. Lessons and Takeaways

- **Structured Analysis Is Handy**

◇ Even if you can't nail down every TTP, running through each kill-chain phase helps identify gaps.

◇ It guides IR teams on what to look for, from reconnaissance signs to post-breach cleanup.

- **Third-Party Risks Are Real**

◇ Trusting someone else's payment processor or inventory system without strict controls is a recipe for disaster.

◇ Segmentation and least-privilege for all external services can limit how far an attacker can go.

- **Legacy Systems Bite Back**

◇ COBOL backends—still common in retail—suffer from a lack of skilled devs and slower security updates.

◇ VBA macros remain a favorite social-engineering tool; organizations should ban all but signed macros.

- **Access Management Is Critical**

◇ Stolen credentials and insider threats are still major entry points. Zero-trust (e.g., multifactor, microsegmentation) helps block those.

◇ Automated alerts for odd login behavior (geographic anomalies, mass failed logins) can kick off faster containment.

- **Be Ready with an IR Plan**

◇ Shutting down the site quickly limited damage but also hurt the business. Simulations for ransomware or data leaks can help balance containment with
continuity.

◇ Practice communication—both internally and to customers—so you don't lose trust when services go dark.

- **Use OSINT Proactively**

◇ Monitoring Reddit threads, job postings, and other public chatter can reveal weak spots before attackers exploit them.

◇ Blue teams should have alerting on these channels, feeding intel into risk assessments.

- **Industry Collaboration Matters**

◇ Multiple big retailers—Victoria's Secret, Adidas, M&S, Harrods—were hit around the same time. Sharing threat intel on shared third-party vendors or library
vulnerabilities can raise everyone's defenses.

Bottom Line:
We don't have every detail, but combining news reports, job-posting intel, and user speculation gives a solid picture: outdated systems, over-trusted third parties, and lax segmentation let attackers in. Retailers should patch legacy code, lock down third-party access, and build a proactive IR routine to avoid repeating this kind of breach.