
EAST

Summit & Awards

# Victoria's Secret.com Incident Response

**Jennifer Kutz, PMP** (on behalf of Jeff Sauer)

Cybersecurity Portfolio Manager & CISO Chief of Staff

Victoria's Secret & Co.

Nominee Showcase Presentation

# Company Overview

VS&Co
VICTORIA'S SECRET & CO.

At Victoria's Secret & Co., fostering a happy, healthy and inclusive culture is our top priority

VS&Co
CYBERSECURITY

Deliver world-class security to win trust every day

- Victoria's Secret is the world's largest intimates specialty retailer offering a wide assortment of modern, fashion-inspired collections including signature bras, panties, lingerie, casual sleepwear and athleisure, as well as award-winning prestige fragrances and body care. Victoriassecret.com is top ten in fashion ecommerce, and has prioritized diversity, equity and inclusion and sustainability company wide.
- VS&Co recently launched an Amazon storefront and a new brand called Happy Nation
- **August 2021, Victoria's Secret & Co. separated from Bath & Body Works, Inc to become 2 separate Fortune 500 brands**

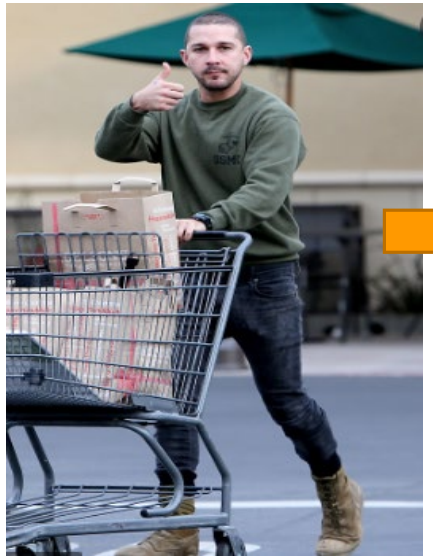
# Presentation Overview -

## Victoria's Secret.com Incident Response

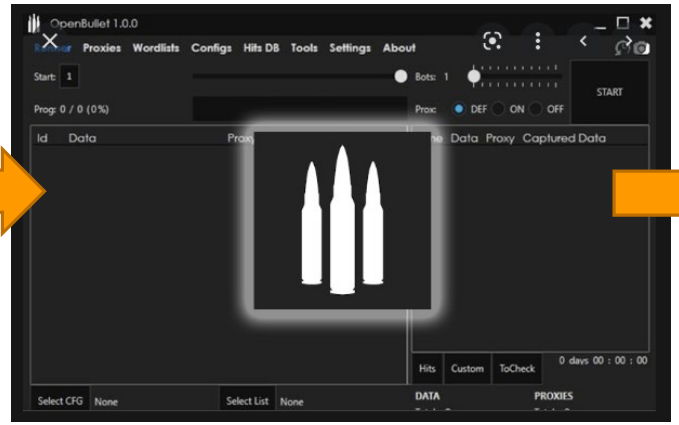
- Given the media attention and business significance of separating two Fortune 500 Brands, the Victoria's Secret CIRC (Cyber Incident Response Center) team, responsible for both VS&Co and Bath&Body Works, was inundated with an attack frequency the company has never seen.
- Our bot mitigation provider reported we were top 5 percentile of their customers targeted.
- The first month of separation, the team mitigated ~50 million bot attacks, up from an average of 6.5 million. The highest month was 82+ million bot attacks.
- The increase in Account Takeover (ATO) and credential stuffing attacks were costing our IR team, legal team, asset protection team, fraud team, and additional security teams hundreds of thousands of dollars in labor hours to respond to these type of attacks.
- Because of the volume and to enhance IR, the team expedited creating a tool that would automate notification to our customers, as well as make them reset their passwords the next time they logged in.

# Ready, Set, ATO!

Wordlist Shopping



Engage "The Bullet"




New Credentials Acquired

Success!?!

## Anatomy of an ATO (Account Take Over) attack

- Bad actors typically purchase wordlists (or combo lists) that are readily available on the dark web
- These lists contain the email and password of accounts that were a victim of a previous known (or unknown) data breach from other digital organizations
- Bad actors will use scripting tools such as OpenBullet to run the same email/password combinations across various websites in an effort to obtain a successful login
- Once a successful login is acquired then the actor can either resell the account or use the account for their own malicious purpose
- The primary abuse that typically occurs with ATOs is credit card and gift card authentication checking

# Key Metrics

**Bot mitigation (main threat focus) key measurable results:**

- Aug '21 – Jan '22 (6 month period): Hundreds of millions attempts to steal customer information were blocked
- Automated tool gained 99% efficiency and 99% cost savings, equals real protection for our customers:
  - Propriety tool cost $15K in labor and no outside vendors were used
  - Before tool was developed, the average time to investigate and notify customers averaged 325 total hours and $100k+
  - After tool was in place, the average time to investigate and notify dropped to 4 hours and <$1k

**Other threat measurable results:**

- Hundreds of billions of events, resulting in only hundreds of cases being escalated to the team from our Managed Services Provider (MSP) – under 200 were confirmed and required response
- Implemented additional endpoint protection rules on tens of thousands of endpoints
- Stopped 55k Log4J2 exploits aimed at our integrated systems
- Blocked hundreds of millions of malicious emails from being delivered to associate's inboxes, up 30% from the monthly average
- Rolled out Bluetooth detection technology to stores hit by an organized criminal ring stealing card data off signature capture devices.

**ULTIMATE RESULT:**

- None of these events mentioned above resulted in any data loss or breach of the VS&Co or Bath&Body Works' corporate systems

# Best Practices/Lessons Learned

## Best practices

- Ensure that all customer traffic is protected by a bot mitigation tool.  VS&Co has always protected their site, but don't assume your third parties have bot mitigation and hold them accountable to enable it.
- Always make certain that your public facing APIs have the most up to date mitigation policies in place
- Apply Defense In Depth (DiD) - the more controls on your website, the more difficult it is for bad actors to accomplish their goal (i.e. CVV; WAF; Fraud tools; obfuscate/masking 13-19 digits for payment card numbers)

## Lessons Learned

- Due to the ever-changing landscape of ecommerce fraud/abuse, being diligent regarding rotation of tactics and tools is important (i.e. IP rotation; protect against scripting tools like OpenBullet)
- Keep in mind that traffic must start behaving like malicious traffic before mitigation can initiate – it is important to keep a close eye on unexpected spikes in traffic and tune mitigation policies when necessary (ie. one IP address using multiple emails and gift/credit cards;  set thresholds used to identify known bad actor behaviors and geo locations)