Threat Intelligence Report

# Hot Topic Data Breach

1st November 2024 | Adarsh Rai, MSISPM

## OVERVIEW

On 21st October, 2024, researchers at cybersecurity firm *Hudson Rock* discovered **350 Million** records of sensitive data posted on breach forums for sale on the dark web. *Hot Topic* and its subsidiaries - *Torrid, Boxlunch* were victims of an Infostealer malware affecting a third party vendor (Robling), targeting data from their loyalty programs. This incident is the largest retail data breach yet recorded, and serves as a precedent in third party management, lack of MFA measures & employee training.

## RISK ANATOMY

*Threat actor* “Satanic” is a reputed hacker known for selling data on breach forums on the dark web, *motivated* by financial gain. Due to the nature of retail companies having large volumes of data and lax security measures, the hacker exploited this *opportunity* by the *means and tactics* of an InfoStealer Malware. The infection stemmed from a third party vendor’s employee, from the company Robling, responsible for data analytics and aggregation for Hot Topic and its subsidiaries.

The hacker used credential harvesting and data exfiltration *techniques* to stealthily transfer login details of privileged cloud accounts (Snowflake), resulting in access to a database with records of 350 Million customers, registered in loyalty programs. Certain *vulnerabilities* allowed a violation of *confidentiality* - lack of malware detection tools, improper vulnerability testing and management, lack of MFA authentication for privileged accounts, and failure to recognize indicators of compromise played a key role in this attack.

## ORGANIZATIONAL CONSEQUENCES

Hot Topic and its subsidiaries will face heavy *financial* consequences, due to the high number of PII and financial information being exposed. Victims have started filing class action lawsuits, and the California Attorney General will begin processing CCPA violations and fines in 30 days from the breach. Hot Topic will also face *operational* consequences such as loss of trust from customers, and potentially lose business from associated brands who want to avoid negative media coverage. The *health and safety* impact is considered to be substantial, as customer PII could be used for potential phishing attacks.

## SECURITY RECOMMENDATIONS

A series of security overhauls are required to prevent similar attacks from occurring. Firstly, third party vendors must be thoroughly vetted and checked for meeting compliance standards. Encryption and segmentation of sensitive data should be a standard practice, while also implementing EDR and IPS systems on all surfaces that data is transferred and processed from. MFA should be required for access to critical data, with privileged role access reviewed on a continuous basis.

Organizational recommendations include implementing a Zero Trust Architecture model, defining and implementing an Incident Response Plan, and regularly assessing cloud provider security. Employee training is of the highest priority, teaching all individuals involved with the organization about indicators of compromise, phishing, and malware detection. Phishing simulations and practice drills will keep the employees aware. Security events reporting should be incentivized for improving monitoring and response efficiency metrics (MTTD, MTTR, MTTA)

These recommendations serve as a foundation for reducing the risk for similar attacks that might happen to organizations using cloud services and third party vendors with access to sensitive customer information.

## Bibliography and Sources

1. Gal, Alon. "Largest Retail Breach in History: 350 Million "Hot Topic" Customers' Personal & Payment Data Exposed *InfoStealers*, 23 Oct. 2024, www.infostealers.com/article/largest-retail-breach-in-history-350-million-hot-topic-customers-personal-and-payment-data-exposed-as-a-result-of-infostealer-infection/
2. Kan, Michael. "Hacker May Have Breached Hot Topic, Stolen Data on Millions." PCMAG, PCMag, 23 Oct. 2024, www.pcmag.com/news/hacker-may-have-breached-hot-topic-stolen-data-on-millions
3. Sead Fadilpašić. "Millions of Hot Topic Shoppers Have Data Stolen by "Satanic" Hacker." TechRadar, TechRadar pro, 24 Oct. 2024, www.techradar.com/pro/security/millions-of-hot-topic-shoppers-have-data-stolen-by-satanic-hacker
4. Siemons, Jorja. "Hot Topic Sued after "Satanic" Hacker Stole Customer Data (1)." @BLaw, 28 Oct. 2024.news.bloomberglaw.com/us-law-week/hot-topic-sued-after-breach-allegedly-exposed-thousands-data