Executive Briefing & Threat Intelligence Report

95-752 : Introduction to Information Security Management

Hot Topic -

Largest Data Breach in Retail History

Adarsh Rai - MSISPM

Carnegie Mellon University

Why should you care?

- Largest Data Breach in Retail History (350,000,000) ~ 350 M records exposed
- Hot Topic (35) Boxlunch (9), Torrid (23)

  1500+ stores & website archives affected
- Recurring patterns of vulnerabilities, threats, and attack vectors
- Impacting customer trust, operational stability, and financial security

Carnegie Mellon University

Source: Gal, Alon.(1) Kan, Michael (2)

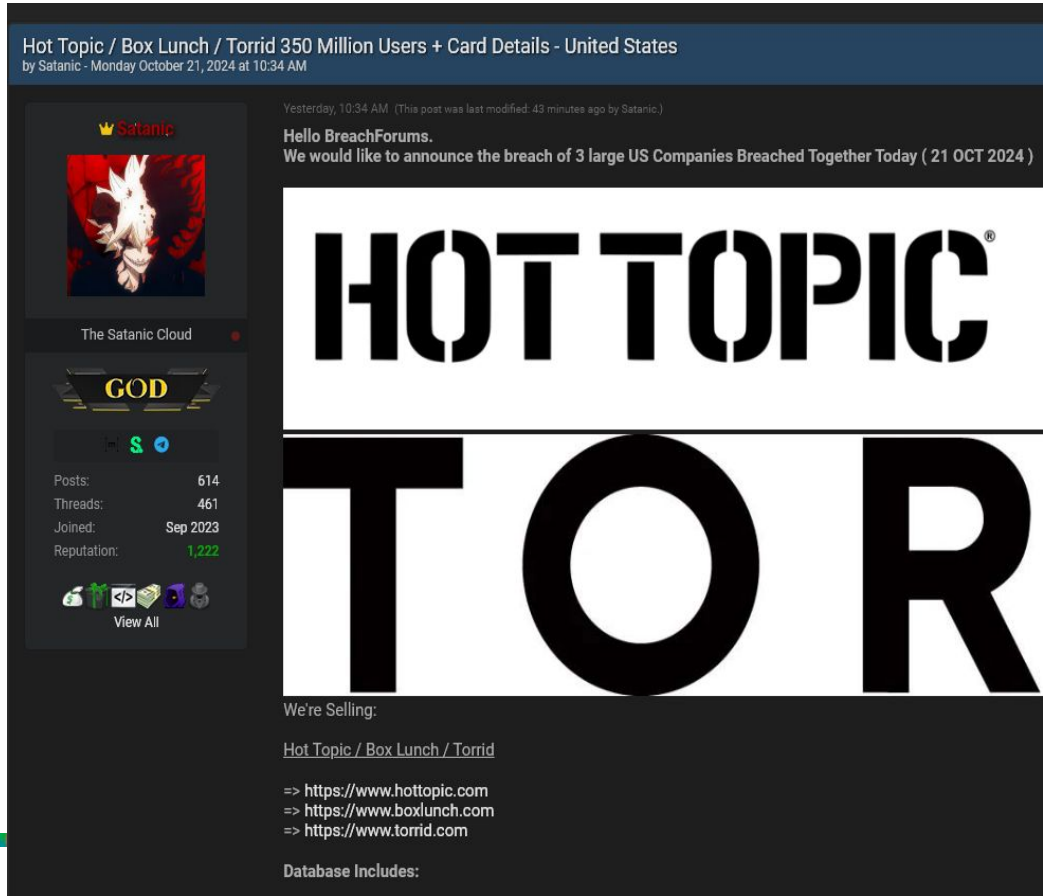
Hot Topic Data Breach | Background

On 21st OCT - Israeli Cybersecurity Vendor Hudson Rock discovered the post

Threat Actor - Satanic, The Satanic Cloud

Selling Price of DB - $20,000

Takedown Price for Hot Topic - $100,000



Source: Gal, Alon.(1) Kan, Michael (2)

Satanic

The Satanic Cloud

GOD

Posts: 614
Threads: 461
Joined: Sep 2023
Reputation: 1,222

View All

Database Includes:

350 Million Customers full informations "email,name,address,phone,birth_date,gender,rewards,loyality,cards,transactions,invoices,tax,orders.."
Billions of lines of Rewards Database.
Billion of lines of Emails Database.
Millions of lines of WorldWide Address's.
Millions of lines of Points Database.
Stores + Location Database.
CC Details : "customer,last4digit,exp"

Much more...

Samples: **https://www.upload.ee/files/1**[redacted]

Full Database Price: 20k$

Telegram: (Dark X) @[redacted]

HT_BL_TD Folder (680 GB)

> Quote:
>
> 4.4GB ./TAX DB.csv
> 5.6GB ./TANSACTION DB.csv
> 0GB ./STORES DB.csv
> 4.4GB ./POINTS DB.csv
> 2.1GB ./PAYMENT METHOD DB.csv
> 24.6GB ./ORDER LINE ARCHIVE.csv
> 39.9GB ./ORDER ITEM ARCHIVE.csv
> 11GB ./ORDER DB.csv
> 7GB ./INVOICE DB.csv
> 2.1GB ./EMAIL DB.csv
> 116.4GB ./CUSTOMER BOTH DB.csv
> 101.6GB ./BIG EMAIL DB.csv
> 48.5GB ./WORLDWIDE ADDRESS DATABASE.csv
> 52.2GB ./SHIPMENTS TRACKING DB.csv
> 1.7GB. ./PLC ACCOUNT DB.csv

Asking Hot Topic 100k to remove the thread.

customer both db sample 1.txt *

1	2	3	4	5	6	7	8	9	10	11
FIRSTNAME	LASTNAME	ADDRESSLINE1	ADDRESSLINE2	CITY	STATE	COUNTRYCODE	ZIPCODE	EMAIL	BESTPHONENUMBER	BIRTHDATE
CHERISH	NOR[redacted]							c[redacted]ail.com	214[redacted]	2004-12-08
TAYLOR	GUS[redacted]	5675 N[redacted]	APT 127	FRESNO	CA	USA	93710[redacted]	s[redacted]9@gmail.com	559[redacted]	1991-05-29
ANGELICA	SAN[redacted]	324 DUR[redacted]		HUTTO	TX	USA	78634	a[redacted]ss@gmail.com	314[redacted]	2000-06-27
KARRA	GU[redacted]	1208 VI[redacted]	RM B05C	VINTON	LA	USA	70668	k[redacted]y@yahoo.com	337[redacted]	1998-12-02
JASMINE	THI[redacted]	1504 GR[redacted]E WAY	APT 912	KNOXVILLE	TN	USA	37909	j[redacted]ou@gmail.com	865[redacted]	1992-08-02
MARILYN	ZEN[redacted]	35140 A[redacted]		MADERA	CA	USA	93636[redacted]	z[redacted]ail.com	559[redacted]	1999-09-24

350,000,000 customers' PII, including names, emails, addresses, phone numbers, and birthdates.

payment method arch db 2 sample.txt *

1	2	3	4	5	6	7	8	9	10
AMOUNT	ACCOUNT_NUMBER	CREATED_BY	PAYMENT_TYPE	CARD_EXPIRY_YEAR	CARD_TYPE	CARD_EXPIRY_MONTH	CREATED_TIMESTAMP	NAME_ON_CARD	ACCOUNT_DISPLAY_NUMBER
202.13	a1IGlFKGxiOUagsZuzIwRRlPh[redacted]	[redacted]ation@hottopic.com	Credit Card	2krSk6+lITkv=	Visa	phvKm7EX13E=	2024-03-16 133BYcx34mldkSGOVR2o9zV4Q==		Visa ending with 9017
97.64	h[redacted]	[redacted]ation@hottopic.com	PayPal				2024-03-27 08		
61.26	IjIl6VfbnjPGIlzojX9XmfbRlPh[redacted]	[redacted]ation@hottopic.com	Credit Card	We/Zo3rlIDYQ=	Visa	KEFyelVs2VU=	2024-03-27 09R6G/C9hYoCpu4qRdhx82tv==		Visa ending with 6259
55.29	h[redacted]	[redacted]ation@hottopic.com	PayPal				2024-03-16 09		
32.56	D0d1UWibcHO/P0jslUZhIBNPh[redacted]	[redacted]ation@hottopic.com	Credit Card	ahtVYvhWPIk=	Visa	COAMlreHrYO=	2024-03-16 13Wc7E/osISFY7YLJXmZz6fw==		Visa ending with 4303
26.25	h[redacted]	[redacted]ation@hottopic.com	PayPal				2024-03-16 10		
158.90	OHEuxhkdldugvsBILZs10%lNPh[redacted]	[redacted]ation@hottopic.com	Private Label Credit Card				2024-03-26 20Wyo/xrKc8CLfh9/hWuJU0A==		ending with 6316
54.83	OHEuxhkdldupcSlvqCKP4LhNPh[redacted]	[redacted]ation@hottopic.com	Private Label Credit Card				2024-03-27 123wZLGJJfz1E/ODv583W15RNPm1w1QKnm		HTCC ending with 5893

Billions of payment details, including the last 4 digits of customers' credit cards, card types, expiration dates, account holder names.

points db sample.txt *

3	4	5	6	7	8
ACT_POINT_ID	PROFILE_ID	NUM_POINTS	ORDER_REWARD_ID	ACT_TRANSACTION_ID	EXPIRE_AFTER
0B[redacted]099D545	924D65[redacted]0ACECC	-100	49023E53A97E554E8DDA5DAC99E5FDE6		
BF[redacted]2E613A	924C5C[redacted]0A63B1	-100	19808933C8FCDF428B2C8E9B1CCCA77F		
0B[redacted]AA1372A	924C5B[redacted]0A63B1	31		D2ADA1D9531E744398A290FC2A12CD99	9999-12-31 23:59:59.000 -0800
75[redacted]0E144B8	924C5C[redacted]0A63B1	130		4E2BCE5D1DA1E54D8CCBBCC7673F71E3	9999-12-31 23:59:59.000 -0800
3B[redacted]023A95B	924D65[redacted]0ACECC	48		277B674C623D2E49A60DD9CB70DA994D	9999-12-31 23:59:59.000 -0800
88[redacted]3131442	924C5C[redacted]0A63B1	95		67D59CFB0A116446B1315D0D1A151AD2	9999-12-31 23:59:59.000 -0800
3A[redacted]89101D	924D65[redacted]0ACECC	65		AF73127CE6D13546B728996EC5BEE0A0	9999-12-31 23:59:59.000 -0800

Billions of loyalty points tied to Hot Topic & Box Lunch, linked to profile identifiers (PROFILE_ID).
These points could be used by threat actors for account takeovers.

Carnegie Mellon University

Source: Gal, Alon.(1)

Hot Topic Data Breach | Tactics, Tools & Procedures

Hot Topic, Boxlunch, Torrid outsourced their data processing to:

Robling - Third party analytics provider

Hudson Rock researchers found a particular **Robling employee** with privileged access to Snowflake, Looker (GCP) administration logins

Source: Gal, Alon.(1)

https://www.torrid.com/on/demandware.store/Sites-torrid-Site↓
https://www.torrid.com/on/demandware.store/Sites-torrid-Site/default/DDUser-Challenge?redirect=%2Fo
https://hottopic.east-us-2.azure.snowflakecomputing.com/console/login#/?returnUrl=internal%2Fworks
https://hottopic.looker.com/browse↓
https://hottopic.looker.com/projects/HotTopicDev/files/Views/Robling/f_meas_il_b.cust_measures.rob
https://torrid.cloud.looker.com/explore/TorridProd/dv_dm_f_meas_il_b?qid=04jOXDTczFhbL7CQhZIont&or
https://torrid.cloud.looker.com/explore/TorridProd/dv_dm_f_meas_il_b?qid=hUbxgvPSAgwssdngX2ThY8&or
https://torrid.cloud.looker.com/folders/home↓
https://adf.azure.com/en/monitoring/pipelineruns/%2FresourceGroups%2FHotTopic-Prod%2Fproviders%2FMi
https://adf.azure.com/en/monitoring/pipelineruns/%2FresourceGroups%2FHotTopic-Prod%2Fproviders%2FMi
https://adf.azure.com/en/monitoring/pipelineruns/%2FresourceGroups%2FHotTopic-Prod%2Fproviders%2FMi
https://adf.azure.com/en/monitoring/pipelineruns/%2FresourceGroups%2FHotTopic-Prod%2Fproviders%2FMi
https://adf.azure.com/en/monitoring/pipelineruns/%2FresourceGroups%2FHotTopic-Prod%2Fproviders%2FMi
https://adf.azure.com/en/monitoring/pipelineruns/%2FresourceGroups%2FHotTopic-Prod%2Fproviders%2FMi
https://adf.azure.com/en/monitoring/pipelineruns/%2FresourceGroups%2FHotTopic-Prod%2Fproviders%2FMi
https://adf.azure.com/en/monitoring/pipelineruns?factory=%2Fsubscriptions%2Fe772ba78-bf10-443b-aae7
https://adf.azure.com/en/monitoring/pipelineruns?factory=%2Fsubscriptions%2Fe772ba78-bf10-443b-aae7
https://app.snowflake.com/yk57310/hottopic/#/compute/history↓
https://app.snowflake.com/yk57310/hottopic/#/compute/history/copies↓
https://app.snowflake.com/yk57310/hottopic/#/compute/history/copies?preset=PRESET_LAST_7_DAYS&type
https://app.snowflake.com/yk57310/hottopic/#/compute/history/queries/01b359b9-0a05-dfe5-0000-2edd1
https://app.snowflake.com/yk57310/hottopic/#/compute/history/queries/01b359ca-0a05-dfe5-0000-2edd1
https://app.snowflake.com/yk57310/hottopic/#/compute/history/queries/01b359cd-0a05-dfe5-0000-2edd1
https://app.snowflake.com/yk57310/hottopic/#/compute/history/queries?user=[redacted]&start=1
https://app.snowflake.com/yk57310/hottopic/#/compute/history/queries?user=[redacted]&start=1
https://app.snowflake.com/yk57310/hottopic/#/compute/history/queries?user=[redacted]&start=1
https://app.snowflake.com/yk57310/hottopic/#/compute/history/queries?user=[redacted]&start=1
https://app.snowflake.com/yk57310/hottopic/#/data/databases/ROBLING_PRD_DB↓

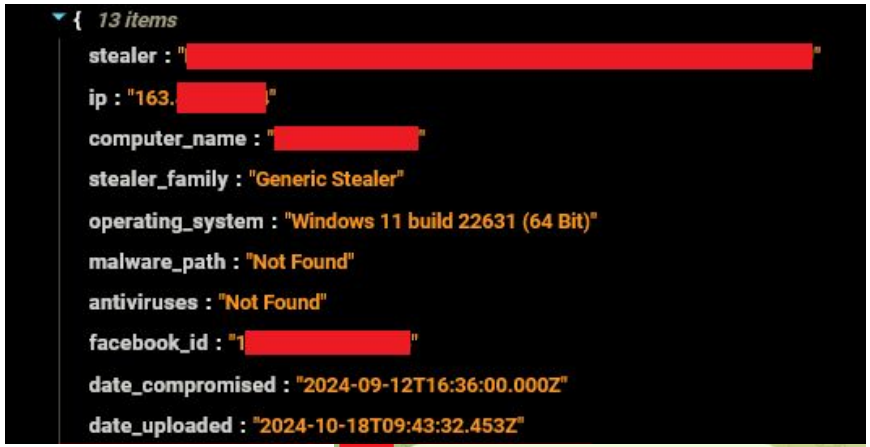
Hot Topic Data Breach | Tactics, Tools & Procedures

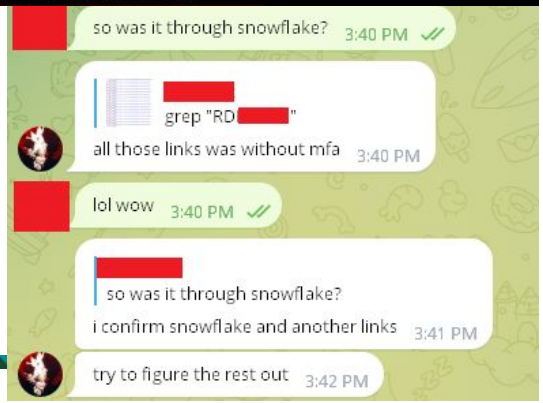
Researchers able to narrow down cause to an infostealer/spyware infection of the employee's device on 9/12/24

Theorized Snowflake, Azure, Looker to be points of exfiltration and transfer.

Snowflake confirmed in later communication with hacker "Satanic", who allegedly stated HoT Topic and Robling **lacked** MFA.

2 Claims verified, rest could be true.

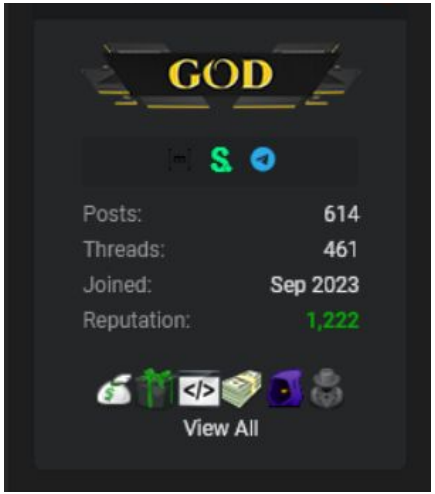




Source: Gal, Alon.(1) , Kan, Michael (2)

Risk Anatomy | Threat Actor “Satanic”

- Reputed on BreachForums and hacking community
- Active since September 2023
- Operates an InfoStealer logs selling service, uses spyware on a daily basis
- Bold, openly displays information, discusses tactics with researchers



Carnegie Mellon University

Source: Gal, Alon.(1) , Kan, Michael (2)

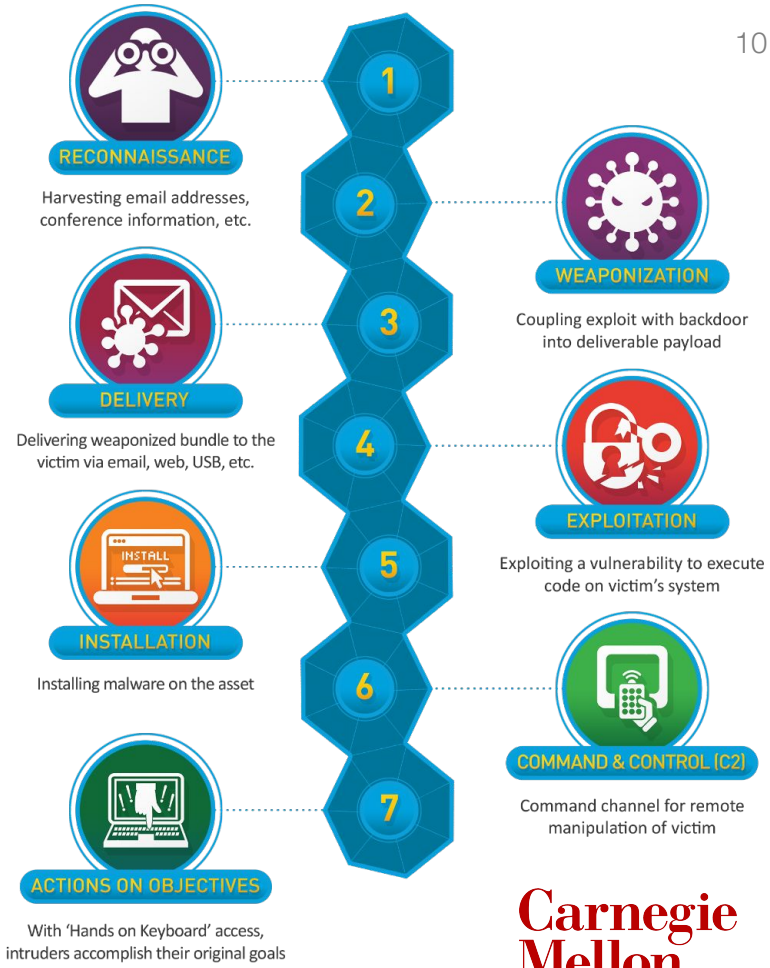
What is an Infostealer?

Type of Malware designed to steal information from infected systems. (Spyware)

Targets passwords, credit card numbers, financial information, PII

Infects through phishing emails, malicious attachments, compromised websites

Keylogging, Clipboard Hijacking, Credential & Email Harvesting/ Dumping



Carnegie Mellon University

Source: Gal, Alon.(1) , Kan, Michael (2)

Risk Anatomy | M.O.M

Motive	Means	Opportunity
Financial Payment Info and PII can be sold on black markets	**Attack Vector** Used Infostealer; malware infected employee's device	**High Data Volume** Took advantage of 3rd party data aggregator and cloud hosted services Bulk data amassed made it an attractive target
Retail High volume of transactions and data stored. Lower scrutiny and security than financial institutions	**Execution** Malware stealthily exported credentials, collected data	**Lack of Security** Retail companies may lack stringent security measures.

Risk Anatomy | Weaknesses

- Lack of malware detection tools - Robling
- Lack of Patching / Updating / Vulnerability testing & management
- Improper access control implementation - MFA for Hot Topic Resources
- Implicit Trust Model instead of Zero Trust
- Lack of employee training
- No Data Minimization procedures, increased complexity in management

Risk Anatomy | Security Requirements Violated

Confidentiality	Integrity
Personally Identifiable Information - names, addresses, and payment card information was exposed **Causes** Lack of Authentication Insufficient endpoint security	No direct manipulation Account credentials leaked, may result in changes to account and billing history, could be used for blackmail

Risk Anatomy | Response

Note that Hudson Rock attempted to reach out to Hot Topic and Robling, but has received no answer yet.

Recommended response:

Contain and isolate devices, networks, accounts, servers

Investigate impact, vulnerabilities, evidence logs (IPS, IDS, SIEM)

Notify Stakeholders, Businesses, Individuals, & Authorities

Implement changes after security reviews and audits

Carnegie Mellon University

Source: Gal, Alon.(1) , Kan

Unwanted Outcomes & Organizational Consequences

Financial Impact	Operational Impact	Safety Impact
Regulatory Compliance Fines, Legal fees, customer compensation costs to incur Class action lawsuits by victims affected (350 M) California Consumer Privacy Act (CCPA) - $750 per person by the California Attorney General	Loss of trust from customers and compromised potential business. Reputational Damages Negative Media Coverage Customer Support Overflow	Customers data exposed on the dark web, may become victims of identity theft & financial fraud

4.CCPA Fines - Secureprivacy.ai, 8. Siemons, Jorja

Additional Considerations

Hot Topic and affiliated companies owned by Sycamore Partners, a NY based P.E firm.

May be outsourcing data to different third party providers for aggregation and analytics.

Potential of similar attacks occurring due to lack of security controls and measures by third part

Holdings [edit]

Current [edit]

- CommerceHub
- Staples and Staples Canada (Acquired 2017)[4]
- Pure Fishing (Acquired January 2019)[5]
  - Brands include: ABU Garcia, All Star, Berkley, Chub, Fenwick, Greys, Hardy, Hodgman, Johnson, JRC, Mitchell, Penn, Pflueger, Sebile, Shakespeare, SpiderWire, Stren, and Ugly Stik.
- Belk (Acquired 2015)[6]
- Hot Topic (Acquired 2013)[7]
- MGF Sourcing, formerly known as Mast Global Fashions (Acquired 2011)[8][9]
- NBG Home (Acquired 2017)[10]
- Talbots (Acquired 2012)[11]
- The Limited (Acquired 2017)[12]
- Torrid (Acquired 2013)[13]
  - In July, 2021, Sycamore Partners sold off 25.2% of the company to the public. It is currently traded on the New York Stock Exchange (NYSE) under the "CURV" symbol. Sycamore Partners currently owns 74.8% of the company.
- Premium Apparel LLC (affiliate of Sycamore Partners used to acquire Ann Taylor, Lane Bryant and related brands from Ascena Retail Group in December 2020.)[14]
  - Ann Taylor
  - Lane Bryant (Cacique)
  - LOFT
  - Lou & Grey
- Azamara Cruises (Acquired 2021)
- Rona Inc. (Acquired 2023)
- Playa Bowls (Acquired 2024)

5. Sycamore Partners.” Wikipedia,

Security Recommendations - Prevention & Mitigation

Networks

Segment data streams, critical information

Implement EDR, IPS, DLP, SIEM systems

Implement MFA for access controls

Conduct vulnerability assessments and Penetration testing (VAPT)

Organizational

Vetting, Audits, and Compliance monitoring for third party organizations

Operate on a Zero Trust Model

Perform encryption (in transit and at rest)

Ensure cloud providers controls are regularly assessed

Create and implement incident response plan (IRP)

Security Recommendations - Prevention & Mitigation 2

Employees

Ensure security awareness training (Password hygiene, Phishing, IOCs, Malware prevention)

Incentivize security event reporting

Mandatory secure device usage and remote device policies

Perform phishing simulations

Continually review privileged access accounts (RBAC)

Sources & Bibliography

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. “What Is InfoStealer Malware and How Does It Work?” Packetlabs, 2014, www.packetlabs.net/posts/what-is-infostealer-malware-and-how-does-it-work/
4. “CCPA Fines: Consequences of Non-Compliance | CCPA Enforcement.” Https://Secureprivacy.ai/, secureprivacy.ai/blog/ccpa-fines
5. “Sycamore Partners.” Wikipedia, 27 Oct. 2021, en.wikipedia.org/wiki/Sycamore_Partners
6. 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
7. 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

Carnegie Mellon University