First Quarter 2022 Data Breach Analysis: Data Compromises Off to Fast Start; Victim Rates Continue to Drop

Summary

- Publicly reported data compromises totaled 404 through March 31, 2022, a 14 percent increase compared to Q1 2021.
- This is the third consecutive year when the number of total data compromises increased compared to Q1 of the previous year. It also represents the highest number of Q1 data compromises since 2020.
- The number of individual victims, though, dropped in Q1 2022. The 20.7M victims in this reporting period is a ~50 percent decrease compared to Q1 2021 and a 41 percent drop from Q4 2021.
- Approximately 92 percent of the data breaches in the first three months of 2022 were the result of cyberattacks.
- Phishing and Ransomware remain the #1 and #2 root causes of data compromises; however, a majority of data breach notices in Q1 2022 did not list a root cause of the breach.
- System & Human Errors represent ~8 percent of the Q1 2022 data compromises.
- Data breaches resulting from physical attacks such as document or device theft and skimming devices dropped to single digits (3) in Q1 2022.

Discussion

- After a record-breaking year for data compromises in 2021 (1,862), Q1 of 2022 begins with the highest number of data compromises in the past three years. Traditionally, Q1 is the lowest number of data breaches reported each year.
- Cyberattacks that lead to data compromises continue to increase, representing ~92 percent of all data compromises. Phishing and related attack vectors, ransomware, and malware remain the top three root causes of cyberattack-related data breaches.
- However, continuing a trend that emerged in 2021, 154 out of 367 data breach notices did not include the cause of the breach. That makes "unknown" the single largest attack vector in Q1. That also represents a 40 percent increase of the total number of unknown breach causes for full-year 2021.
- While subsequent breach notice updates may include more attack information, the increasing lack of transparency in breach notices represents a risk to organizations as well as individual consumers.
- The only non-cyberattack-related attack vector in double digits during Q1 was related to email or letter correspondence with 12 instances.
- Healthcare, Financial Services, Manufacturing & Utilities, and Professional Services sectors had the most compromises in Q1 2022.

© 2022 | Identity Theft Resource Center • idtheftcenter.org
888.400.5530 • 2514 Jamacha Rd., Ste. 502-525 El Cajon, CA 92019-4492

Q1 2022 Data Compromise Details

Number of Q1 Compromises

- **Total Data Compromises**: 404 compromises; 20,773,963 victims
- **Data Breaches**: 398 data breaches; 13,676,543 victims
- **Data Exposures**: 4 data exposures; 7,094,528 victims
- **Data Leaks**: N/A
- **Unknown**: 2 unknown; 2,892 victims impacted

Attack Vectors Q1 2022:

- **Cyberattacks**: 367 breaches; 13,525,762 victims
  - 110 Phishing/smishing/BEC
  - 67 Ransomware
  - 22 Malware
  - 9 Other
  - 3 Non-secured Cloud Environment
  - 2 Credential Stuffing
  - 154 NA – not specified
- **System & Human Errors:** 32 breaches/exposures; 7,223,708 victims
  - 12 Correspondence (email/letter)
  - 5 Misconfigured firewalls
  - 4 Failure to configure cloud security
  - 3 Other
  - 1 Lost device or document
  - 7 NA – not specified
- **Physical Attacks:** 3 breaches; 21,601 victims
  - 1 Document Theft
  - 1 Device Theft
  - 1 Improper Disposal

Charts

Compromise Year-over-Year Totals		
Month	**Compromises**	**Victims**
2022 YTD	404	20,773,963
2021	1,862	295,429,724
2020	1,108	310,218,744
2019	1,279	883,558,186
2018	1,175	2,227,849,622
2017	1,506	1,825,413,935
2016	1,088	2,541,092,072

Quarter-to-Quarter		
Year & Quarter	**# of compromises**	**# of Victims Impacted**
2022 Q1 (JAN-MAR)	404	20,773,963
2021 Q4 (OCT-DEC)	566	35,311,922
2021 Q3 (JUL-SEP)	445	163,542,095
2021 Q2 (APR-JUN)	497	55,321,228
2021 Q1 (JAN-MAR)	354	41,254,479
2020 Q4 (OCT-DEC)	326	16,683,032
2020 Q3 (JUL-SEP)	248	60,952,924
2020 Q2 (APR-JUN)	295	100,918,230
2020 Q1 (JAN-MAR)	239	131,664,558

Attack Vector 2022 YTD vs. Full Years 2021 & 2020			
Attack Vector	**2022 YTD**	**2021**	**2020**
Cyberattacks	**367**	**1,613**	**878**
Phishing/smishing/BEC	110	537	383
Ransomware	67	351	158
Malware	22	141	104
Non-secured Cloud Environment	3	24	50
Credential Stuffing	2	14	17
Unpatched software flaw	-	4	3
Zero Day Attack	-	4	1
Other	9	428	162
NA – not specified	154	110	-
System & Human Errors	**32**	**179**	**152**
Failure to configure cloud security	4	54	57
Correspondence (email/letter)	12	66	55
Misconfigured firewall	5	13	4
Lost device or document	1	12	5
Other	3	34	31
NA – not specified	7	-	-
Physical Attacks	**3**	**51**	**78**
Document Theft	1	9	15
Device Theft	1	17	30
Improper Disposal	1	5	11
Skimming Device	-	1	5
Other	-	19	17
NA – not specified	-	-	-
Unknown	**2**	**12**	**N/A**
TOTALS:	**404**	**1,855**	**1,108**

Compromises by Sector Q1 YTD vs. Full Years 2021 & 2020						
Sector	Year					
	Q1 YTD 2022		FY 2021		FY 2020	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	21	106,099	125	1,681,483	42	974,054
Financial Services	68	3,384,769	279	19,973,772	138	2,687,084
Government	13	294,027	66	3,244,455	47	1,100,526
Healthcare	73	2,560,465	330	28,216,273	306	9,700,238
Hospitality	6	56,451	33	238,445	17	22,365,384
Manufacturing & Utilities	52	247,852	222	49,777,158	70	2,896,627
Military	-	-	-	-	-	-
Non-Profit/NGO	18	558,362	86	2,339,646	31	37,528
Professional Services	46	1,719,850	184	22,725,185	144	73,012,145
Retail	18	272,950	102	7,212,912	53	10,710,681
Technology	16	10,832,588	79	44,679,488	67	142,134,883
Transportation	8	20,930	44	569,574	21	1,208,292
Other	65	719,620	308	79,538,669	172	43,391,302
Unknown	-	-	4	35,232,664	-	-
TOTALS:	404	20,773,963	1,862	295,429,724	1,108	310,218,744

METHODOLOGY NOTES: For purposes of quarterly and annual reporting, the ITRC aggregates data events based on the date the breach, exposure, or leak was entered into the database rather than the date the event occurred. This avoids the confusion and data conflicts associated with the need to routinely update previous reports and compromise totals. The date of the original compromise, if known, and the date of the event report are noted in the ITRC's *notified* data compromise tracking database.
The number of victims linked to individual compromises are updated as needed and can be accessed in the ITRC's *notified* breach tracking solution.

The ITRC reports Third-Party/Supply Chain Attacks as a single attack against the company that lost control of the information. The total number of individuals impacted by third-party incidents is based on notices sent by the multiple organizations impacted by the single data compromise.

Unless otherwise noted, all data reported on April 13, 2022, as entered through March 31, 2022.