IDENTITY THEFT RESOURCE CENTER

Call Now 888.400.5530

idtheftcenter.org

First Half 2022 Data Breach Analysis: Victim Rates Decline as Compromises Target Businesses

Key Takeaways

- Data compromises are up slightly – two (2) percent in the second quarter (Q2) of 2022 compared to the first quarter (Q1) of 2022. However, the overall pace of data compromises for the first half (H1) of 2022 is down four (4) percent compared to the same period in 2021. The total number of data compromises reported in 2021 – 1,862 - was a record high.
- The number of people reportedly impacted by data compromises continued to drop in H1 2022 as the nature of data compromises shifted to attacks targeting businesses, government agencies, and institutions. However, an average of 39 percent of all data breach notices issued in H1 2022 do not list a victim count.
- Approximately 40 percent of data breach notices issued in H1 2022 do not include the root cause of the compromise, making "unknown" the top cause of data breaches so far this year for the first time since the Identity Theft Resource Center (ITRC) began tracking the causes of data compromises.
- Cyberattacks continued to be the primary attack vector leading to a data compromise in H1 2022. Ransomware attacks linked to breaches dropped 20 percent in Q2 2022 from the previous Quarter – the first Quarter-over-Quarter (QoQ) drop since the ITRC began tracking ransomware in 2018.

Summary

- After a record-high number of publicly reported data breaches in 2021 – 1,862 – there have been fewer data compromises so far in 2022 than at the same point in 2021: 817 vs. 851.
- The number of victims in H1 2022 was down ~45 percent from H1 2021 as at least 53.3M people were reported as being impacted by a data compromise.
- An estimated 87 percent of the data compromises in H1 2022 were due to a cyberattack. However, ransomware attacks declined QoQ for the first time since ransomware surpassed malware as the #2 primary cause of data breaches in 2019.
- Phishing remained the #1 root cause of data compromises in H1 2022.
- Supply chain attacks, a subset of cyberattacks, continue to be a favored attack vector for cyberattackers.
- For the first time in H1 2022, approximately four (4) in ten (10) data breach notices did not list a root cause of the compromise. Forty (40) percent of entities issuing breach notices did not reveal the number of victims impacted.

Discussion

- After a record-breaking 2021, the number of publicly reported data compromises is down in the first half of 2022 compared to the previous point in 2021. So is the number of publicly identified victims.
- Also, down so far in 2022 are the number of data breaches linked to ransomware attacks. Security researchers speculate that the sudden decline in ransomware attacks is due to a combination of factors, including the ongoing conflict in Ukraine and the collapse of cryptocurrencies favored by cybercriminals.
- All of these trends – fewer compromises, fewer victims, few ransomware attacks – can be reversed quickly with just a handful of large breaches or a series of smaller ones.
- The declines could also be an illusion, masked by the 40 percent of data breach notices that do not include basic information, such as attack vector and/or a victim count. This is a new trend that requires further observation and study.

Q2 & H1 2022 Data Compromise Details

Number of Q2 Compromises

- **Total Data Compromises**: 413 compromises; 27,946,766 victims
- **Data Breaches**: 404 data breaches; 27,902,868 victims
- **Data Exposures**: 6 data exposures; 42,420 victims
- **Data Leaks**: N/A
- **Unknown**: 3 unknown; 1,478 victims

Number of H1 Compromises

- **Total Data Compromises:** 817 compromises; 53,350,425 victims
- **Data Breaches:** 802 data breaches; 46,209,107 victims
- **Data Exposures:** 10 data exposures; 7,136,948 victims
- **Data Leaks:** N/A
- **Unknown:** 5 unknown; 4,370 victims

Attack Vectors Q2 2022

- **Cyberattacks**: 367 breaches; 17,735,760 victims
  - 107 Phishing/smishing/BEC
  - 55 Ransomware
  - 22 Malware
  - 8 Other
  - 4 Credential Stuffing
  - 2 Non-secured Cloud Environment
  - 169 N/A – not specified
- **System & Human Errors:** 30 breaches/exposures; 10,094,133 victims
  - 10 Misconfigured firewalls
  - 9 Correspondence (email/letter)
  - 6 Failure to configure cloud security
  - 3 Other
  - 2 N/A – not specified

- **Physical Attacks:** 13 breaches; 115,395 victims
  - 8 Device Theft
  - 2 Improper Disposal
  - 2 Document Theft
  - 1 Skimming Device
- **Supply Chain Attacks** (*included in the attack vectors above*)
  - 293 entities were impacted by 23 third-party/supply chain attacks, including one (1) attack that was reported in 2021; 2,975,387 individuals were impacted in Q2
  - 292 entities affected 2,975,387 individuals impacted by cyberattacks
  - 1 entity affected; unknown # of victims impacted by system & human errors
  - No entities affected; No victims impacted by physical attacks

Attack Vectors H1 2022

- **Cyberattacks:** 734 breaches; 35,891,170 victims
  - 219 Phishing/smishing/BEC
  - 124 Ransomware
  - 46 Malware
  - 17 Other
  - 6 Credential Stuffing
  - 5 Non-secured Cloud Environment
  - 317 N/A – not specified
- **System & Human Errors:** 62 breaches/exposures; 17,317,889 victims
  - 21 Correspondence (email/letter)
  - 15 Misconfigured firewalls
  - 10 Failure to configure cloud security
  - 6 Other
  - 1 Lost device or document
  - 9 N/A – not specified

- **Physical Attacks:** 16 breaches; 136,996 victims
  - 9 Device Theft
  - 3 Improper Disposal
  - 3 Document Theft
  - 1 Skimming Device
- **Supply Chain Attacks** (*included in the attack vectors above*)
  - 367 entities were impacted by 44 third-party/supply chain attacks, including ten (10) attacks that were reported in previous years (2021 & 2020); 4,138,125 individuals were impacted in H1 2022
  - 364 entities affected 4,136,825 victims impacted by cyberattacks
  - 3 entities affected; 1,300 victims impacted by system & human errors
  - No entities affected; No victims impacted by physical attacks
  - Noteworthy supply chain attacks include:
    - **Illuminate Education (2022):** As of 7/5/2022, the ITRC has recorded 234 entities w/ 201,586 victims impacted. ***Note: Roughly 600+ school districts are known to have been impacted. The ITRC is continuing to monitor and enter districts as information is being reported. The total number of victims per district has not been reported.*
    - **Ciox Health (2022):** As of 7/5/2022, the ITRC has recorded 34 entities w/ 12,493 victims impacted
    - **Eye Care Leaders (2022):** As of 7/5/2022, the ITRC has recorded 29 entities w/ 2,237,515 victims impacted
    - **MCG Health, LLC (2022):** As of 7/5/2022, the ITRC has recorded six (6) entities w/ 793,283 victims impacted
    - **Horizon Actuarial Services, LLC (2022):** As of 7/5/2022, the ITRC has recorded three (3) entities w/ 2,292,080 victims impacted ***Note: Exposure # updated per total number of victims impacted as reported to the Maine AG by Horizon Actuarial*

Charts

Compromise Year-over-Year Totals		
Month	**Compromises**	**Victims**
2022 YTD	817	53,350,425
2021	1,862	298,078,081
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 Q2 (APR-JUN)	413	27,946,766
2022 Q1 (JAN-MAR)	404	25,403,659
2021 Q4 (OCT-DEC)	566	35,376,838
2021 Q3 (JUL-SEP)	445	166,125,536
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

Compromises with Reported Victims Impacted Quarter-to-Quarter			
Year & Quarter	# of Compromises	# of Compromises with Reported Victims Impacted	Percentage
2022 Q2 (APR-JUN)	413	235	58%
2022 Q1 (JAN-MAR)	404	263	65%
2021 Q4 (OCT-DEC)	566	288	51%
2021 Q3 (JUL-SEP)	445	292	66%
2021 Q2 (APR-JUN)	497	299	60%

Compromises by Sector H1 YTD vs. Full Years 2021 & 2020						
Sector	Year					
	H1 YTD 2022		FY 2021		FY 2020	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	41	405,493	125	1,687,192	42	974,054
Financial Services	127	22,309,482	279	19,973,772	138	2,687,084
Government	33	810,529	66	3,244,455	47	1,100,526
Healthcare	161	11,830,303	330	30,853,767	306	9,700,238
Hospitality	11	76,820	33	238,445	17	22,365,384
Manufacturing & Utilities	115	467,664	222	49,782,583	70	2,896,627
Military	-	-	-	-	-	-
Non-Profit/NGO	34	590,207	86	2,339,646	31	37,528
Professional Services	95	2,053,827	184	22,726,901	144	73,012,145
Retail	30	325,445	102	7,212,912	53	10,710,681
Technology	31	12,394,573	79	44,679,488	67	142,134,883
Transportation	19	328,317	44	569,684	21	1,208,292
Other	120	1,757,785	308	79,536,572	172	43,391,302
Unknown	-	-	4	35,232,664	-	-
TOTALS:	817	53,350,425	1,862	298,078,081	1,108	310,218,744

Attack Vector 2022 YTD vs. Full Years 2021 & 2020

Attack Vector	2022 YTD	2021	2020
Cyberattacks	**734**	**1,613**	**878**
Phishing/smishing/BEC	219	537	383
Ransomware	124	352	158
Malware	46	141	104
Non-secured Cloud Environment	5	24	50
Credential Stuffing	6	14	17
Unpatched software flaw	-	4	3
Zero Day Attack	-	4	1
Other	17	427	162
N/A – not specified	317	110	-
System & Human Errors	**62**	**179**	**152**
Failure to configure cloud security	10	54	57
Correspondence (email/letter)	21	66	55
Misconfigured firewall	15	13	4
Lost device or document	1	12	5
Other	6	34	31
N/A – not specified	9	-	-
Physical Attacks	**16**	**51**	**78**
Document Theft	3	9	15
Device Theft	9	17	30
Improper Disposal	3	5	11
Skimming Device	1	1	5
Other	-	19	17
N/A – not specified	-	-	-
Unknown	**5**	**12**	**N/A**
TOTALS:	**817**	**1,855**	**1,108**

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 July 5, 2022, as entered through June 30, 2022.