Reviewing the Verizon DBIR 2023

Amherst Security Group

July 20, 2023

Robert Hurlbut

RobertHurlbut.com • @RobertHurlbut

Who am I?

Twitter:
@RobertHurlbut
LinkedIn:
roberthurlbut

Robert Hurlbut

Principal Application Security Architect / Threat Modeling Lead
@ Aquia, Inc. (https://aquia.us)
(AWS Partner / AWS Public Sector Partner)

- **Microsoft MVP – Dev Sec / Dev Tech**
- **(ISC2) CSSLP**
- **Boston Code Camp – Co-Organizer**
- **Boston .NET Architecture Group – Founder / Leader**
- **Amherst Security Group – Leader**
- **Application Security Podcast – Co-Host**
- **"Threat Modeling Manifesto" – Co-Author**
- **Threat Modeling Connect – Founding Member**
- **Expert Witness (Threat Modeling, Cybersecurity)**
- **Ph.D. Student – Space Cybersecurity**

Revisiting the Verizon DBIR

We last reviewed the Verizon Data Breach Investigations Report 2017 (i.e. more commonly known as the “DBIR”) in May, 2017.

You can find that presentation here:

https://roberthurlbut.com/resources/2017/AmSec/Robert-Hurlbut-AmSec-Reviewing-2017-Verizon-DBIR-05102017.pdf

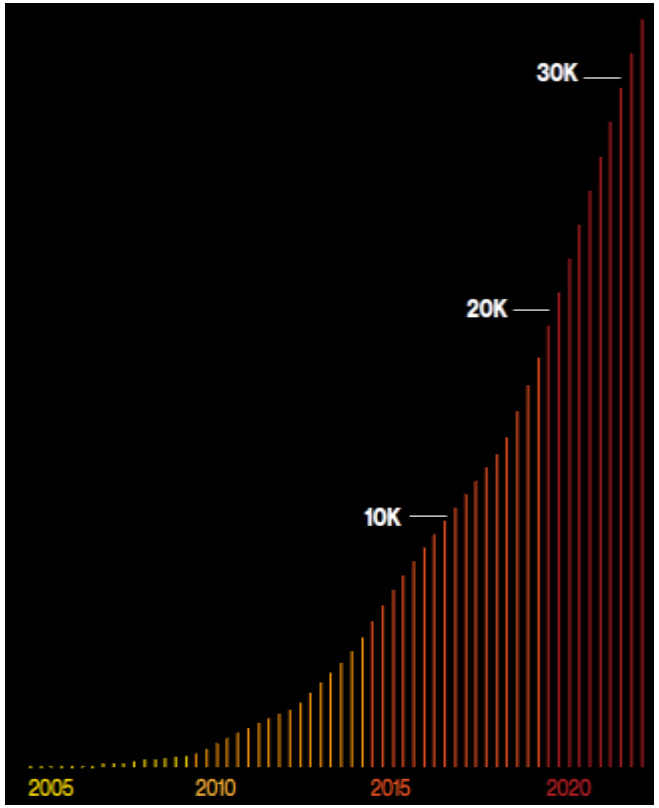
Disclaimer

I am ***not*** an employee of Verizon or their affiliates. All views, opinions, and biases are representative of my own independent research of the 2023 Verizon DBIR, unless noted.

What is the Verizon DBIR?

The Verizon Data Breach Investigations Report (DBIR) was first released in 2008 with data breach data from one organization: Verizon.

Since then, this report continues to be released annually.



What is the Verizon DBIR?

The latest report (released June 6, 2023) represents ***aggregated*** data breach data from **85** contributing organizations.*

See full list on pp. 85-86.

* There were ***65*** contributing organizations in 2017.

Definitions (from the report)

VERIS

Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to provide a common language for describing security incidents in a structured and responsible manner

Definitions (from report)

Incident

A security event that compromises the integrity, confidentiality or availability of a information asset

Breach

An incident that results in the confirmed disclosure (not just potential exposure) of data to an unauthorized party

Definitions (from the report)

Threat actor: Who is behind the event? This could be the external “bad guy” that launches a phishing campaign or an employee who leaves sensitive documents in their seat back pocket.

Threat action: What tactics (actions) were used to affect an asset? VERIS uses seven primary categories of threat actions: Malware, Hacking, Social, Misuse, Physical, Error and Environmental. Examples at a high level include hacking a server, installing malware or influencing human behavior through a social attack.

Variety: More specific enumerations of higher-level categories—e.g., classifying the external “bad guy” as an organized criminal group1 or recording a hacking action as SQL injection or brute force.

Incident/breach eligibility

The incident must have at least seven enumerations (e.g. threat actor variety, threat action category, variety of integrity loss and so on) across 34 fields OR be a DDoS attack. Exceptions are given to confirmed data breaches with less than seven enumerations.

The incident must have at least one known VERIS threat action category (hacking, malware and so on).

What’s included?

Incident / breach must have occurred within this timeframe:

November 1, 2021 to October 31, 2022

(NOTE: While 2022 caseload is the primary analytical focus of the report, the entire range of data is referenced, especially trending graphs.)

What’s not included

Excluded:

- Incidents / breaches affecting individuals that cannot be tied to an organizational attribute loss

  (i.e. If your friend’s laptop was hit with Trickbot, it would not be included in the report.)

Incident Classification Patterns

2023*

1. Basic Web Application Attacks
2. Denial of Service
3. Lost and Stolen Assets
4. Miscellaneous Errors
5. Privilege Misuse
6. Social Engineering
7. System Intrusion
8. Everything Else

***Verizon DBIR 2023, p. 23**

2017

1. Denial of Service
2. Privilege Misuse
3. Lost and Stolen Assets
4. Everything Else
5. Point of Sale
6. Miscellaneous Errors
7. Web App Attacks
8. Crimeware
9. Payment Card Skimmers
10. Cyber-Espionage

Basic Web Application Attacks*

Frequency	1,404 incidents, 1,315 with confirmed data disclosure
Threat actors	External (100%), Internal (1%), Multiple (1%) (breaches)
Actor motives	Financial (95%), Espionage (4%), Fun (1%) (breaches)
Data compromised	Credentials (86%), Personal (72%), Internal (41%), Other (19%) (breaches)

This pattern, which accounts for 25% of our breaches, consists largely of leveraging stolen credentials and vulnerabilities to get access to an organizations' assets. With this beachhead, the attackers can then do a variety of things, such as stealing key information hiding in emails or taking code from repositories. While these attacks aren't complicated, they certainly are effective and have remained a relatively stable part of our dataset, which prompts us to discuss once again (drum roll, please), the importance of multifactor authentication (MFA) and patch management![38]

Relevant ATT&CK techniques

Brute Force: T1110
- Credential Stuffing: T1110.004
- Password Cracking: T1110.002
- Password Guessing: T1110.001
- Password Spraying: T1110.003

Compromise Accounts: T1586
- Email Accounts: T1586.002

Exploit Public-Facing Application: T1190

External Remote Services: T1133

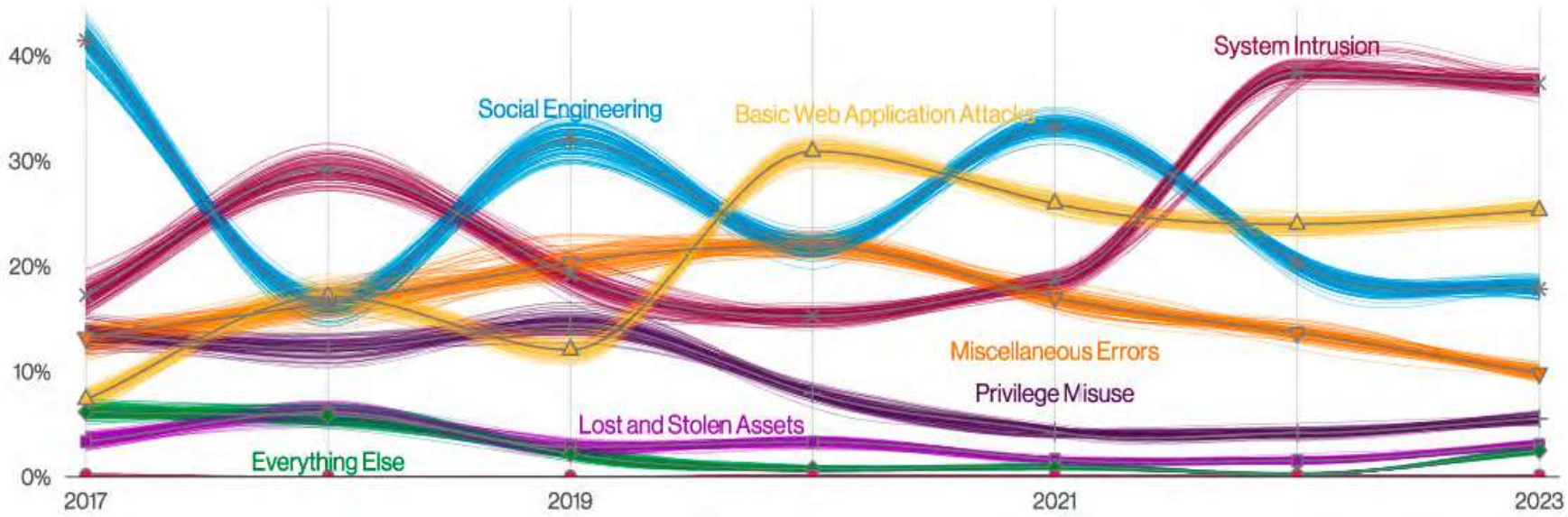
Valid Accounts: T1078
- Default Accounts: T1078.001
- Domain Accounts: T1078.002

Use Alternate Authentication Material: T1550
- Application Access Token: T1550.001

Active Scanning: T1595
- Vulnerability Scanning: T1595.002

***Verizon DBIR 2023, p. 35**

Patterns over time in breaches*



*Verizon DBIR 2023, p. 22

Action categories*

- Hacking
- Malware
- Error
- Social
- Misuse
- Physical
- Environmental

***Verizon DBIR 2023, p. 14**

Asset categories*

- Server
- Person
- User device
- Network
- Media

***Verizon DBIR 2023, p. 17**

Incidents / Breaches – Totals*

of Incidents: 16,312

out of which

# of breaches: 5,199

***Verizon DBIR 2023, p. 49**

Summary of findings*

- The “log4j” vulnerability was used in 75% of digital espionage campaigns
- Social engineering attacks have doubled, and mostly involve Business Email Compromise (BEC) attacks
- 74% of beaches include the human element, including errors and privilege misuse
- 83% of breaches included external actors
- 95% of attacks had a financial motive
- The three primary methods of access were stolen credentials, phishing, and vulnerability exploitation

***Verizon DBIR 2023, pp. 8-9**

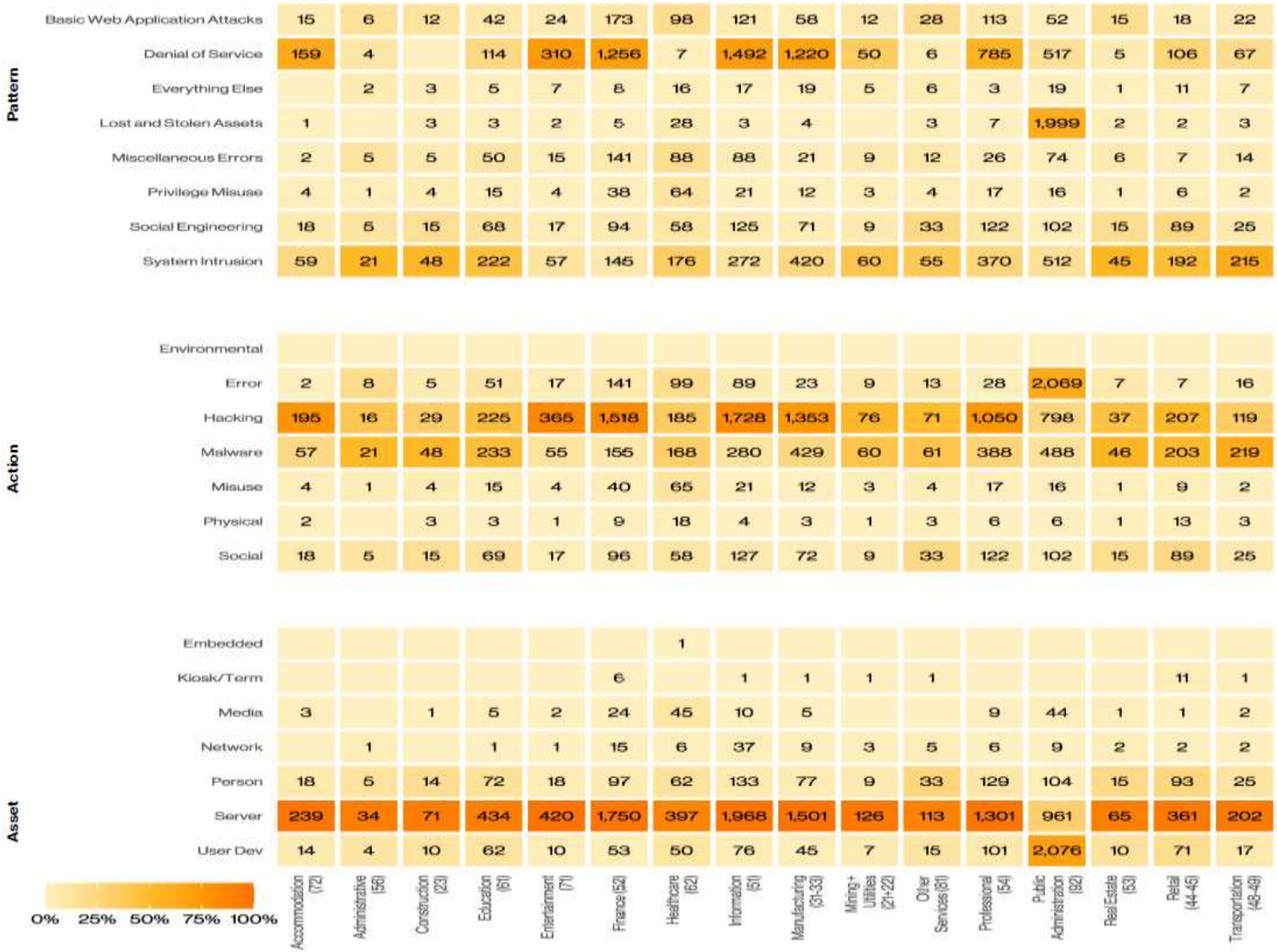
Industries*

	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	16,312	694	489	15,129	5,199	376	223	4,600
Accommodation (72)	254	4	2	248	68	4	1	63
Administrative (56)	38	8	14	16	32	8	11	13
Agriculture (11)	66	1	5	60	33	0	3	30
Construction (23)	87	7	1	79	66	4	1	61
Education (61)	496	63	15	418	238	28	8	202
Entertainment (71)	432	13	3	416	93	10	1	82
Finance (52)	1,829	70	30	1,729	477	38	18	421
Healthcare (62)	522	28	15	479	433	23	15	395
Information (51)	2,105	45	110	1,950	380	23	19	338
Management (55)	9	1	0	8	9	1	0	8
Manufacturing (31–33)	1,814	37	24	1,753	259	18	15	226
Mining (21)	25	2	0	23	13	2	0	11
Other Services (81)	143	7	2	134	100	6	1	93
Professional (54)	1,396	176	54	1,166	421	85	32	304
Public Administration (92)	3,270	87	110	3,073	582	48	39	495
Real Estate (53)	83	15	5	63	59	10	2	47
Retail (44–45)	404	62	44	298	191	33	28	130
Transportation (48–49)	349	13	25	311	106	8	13	85
Utilities (22)	117	12	6	99	33	3	3	27
Wholesale Trade (42)	96	42	22	32	53	23	11	19
Unknown	2,777	1	2	2,774	1,553	1	2	1,550
Total	16,312	694	489	15,129	5,199	376	223	4,600

Table 2. Number of security incidents and breaches by victim industry and organization size

***Verizon DBIR 2023, p. 50**

Incidents by industry*

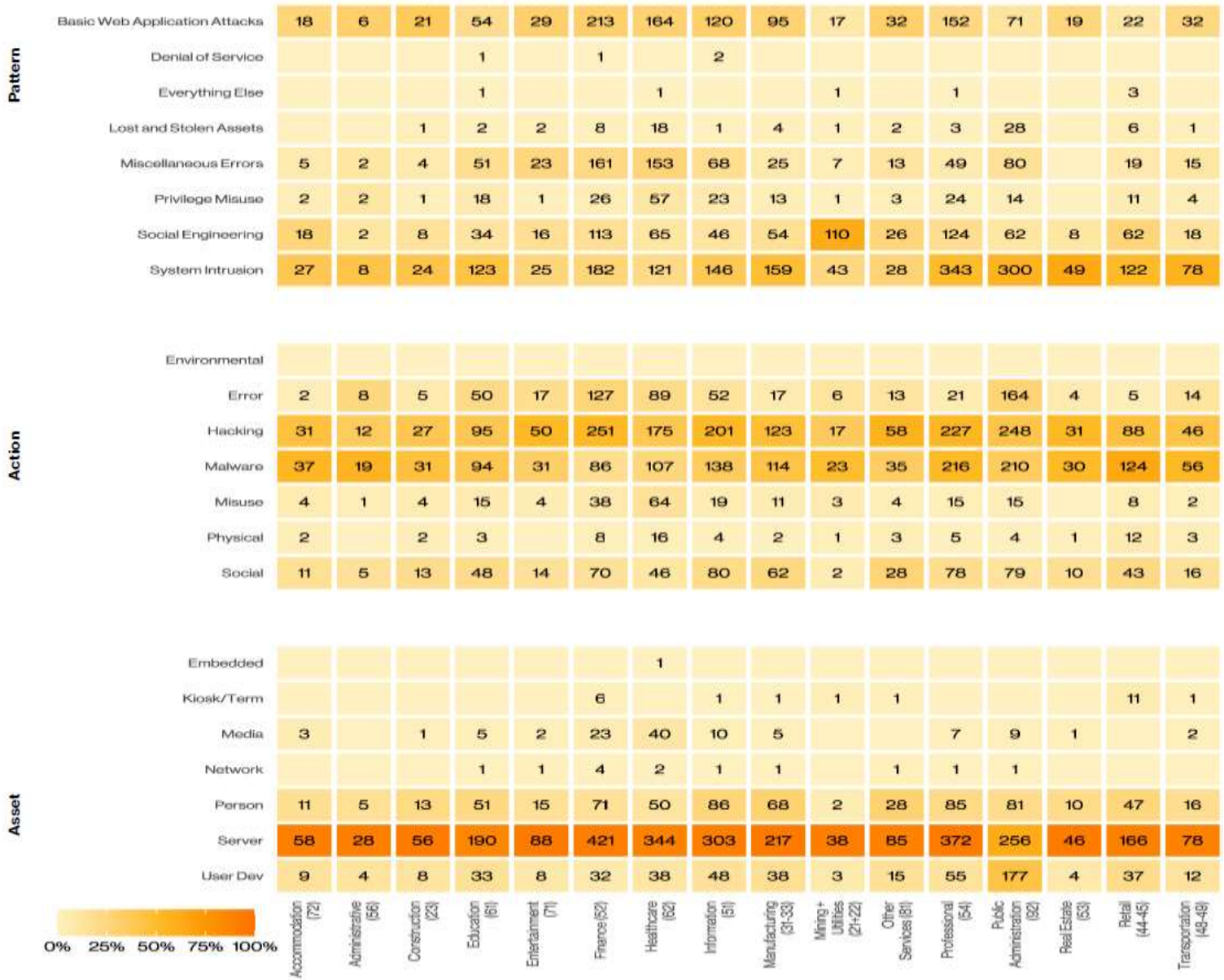


		Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Pattern	Basic Web Application Attacks	15	6	12	42	24	173	98	121	58	12	28	113	52	15	18	22
	Denial of Service	159	4		114	310	1,256	7	1,492	1,220	50	6	785	517	5	106	67
	Everything Else		2	3	5	7	8	16	17	19	5	6	3	19	1	11	7
	Lost and Stolen Assets	1		3	3	2	5	28	3	4		3	7	1,999	2	2	3
	Miscellaneous Errors	2	5	5	50	15	141	88	88	21	9	12	26	74	6	7	14
	Privilege Misuse	4	1	4	15	4	38	64	21	12	3	4	17	16	1	6	2
	Social Engineering	18	5	15	68	17	94	58	125	71	9	33	122	102	15	89	25
	System Intrusion	59	21	48	222	57	145	176	272	420	60	55	370	512	45	192	215
Action	Environmental																
	Error	2	8	5	51	17	141	99	89	23	9	13	28	2,069	7	7	16
	Hacking	195	16	29	225	365	1,518	185	1,728	1,353	76	71	1,050	798	37	207	119
	Malware	57	21	48	233	55	155	168	280	429	60	61	388	488	46	203	219
	Misuse	4	1	4	15	4	40	65	21	12	3	4	17	16	1	9	2
	Physical	2		3	3	1	9	18	4	3	1	3	6	6	1	13	3
	Social	18	5	15	69	17	96	58	127	72	9	33	122	102	15	89	25
Asset	Embedded							1									
	Kiosk/Term						6		1	1	1	1				11	1
	Media	3		1	5	2	24	45	10	5			9	44	1	1	2
	Network		1		1	1	15	6	37	9	3	5	6	9	2	2	2
	Person	18	5	14	72	18	97	62	133	77	9	33	129	104	15	93	25
	Server	239	34	71	434	420	1,750	397	1,968	1,501	126	113	1,301	961	65	361	202
	User Dev	14	4	10	62	10	53	50	76	45	7	15	101	2,076	10	71	17

0% 25% 50% 75% 100%

***Verizon DBIR 2023, p. 51**

Breaches by industry*



		Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Pattern	Basic Web Application Attacks	18	6	21	54	29	213	164	120	95	17	32	152	71	19	22	32
	Denial of Service				1		1		2								
	Everything Else				1			1			1		1			3	
	Lost and Stolen Assets			1	2	2	8	18	1	4	1	2	3	28		6	1
	Miscellaneous Errors	5	2	4	51	23	161	153	68	25	7	13	49	80		19	15
	Privilege Misuse	2	2	1	18	1	26	57	23	13	1	3	24	14		11	4
	Social Engineering	18	2	8	34	16	113	65	46	54	110	26	124	62	8	62	18
	System Intrusion	27	8	24	123	25	182	121	146	159	43	28	343	300	49	122	78
Action	Environmental																
	Error	2	8	5	50	17	127	89	52	17	6	13	21	164	4	5	14
	Hacking	31	12	27	95	50	251	175	201	123	17	58	227	248	31	88	46
	Malware	37	19	31	94	31	86	107	138	114	23	35	216	210	30	124	56
	Misuse	4	1	4	15	4	38	64	19	11	3	4	15	15		8	2
	Physical	2		2	3		8	16	4	2	1	3	5	4	1	12	3
	Social	11	5	13	48	14	70	46	80	62	2	28	78	79	10	43	16
Asset	Embedded							1									
	Kiosk/Term						6		1	1	1	1				11	1
	Media	3		1	5	2	23	40	10	5			7	9	1		2
	Network				1	1	4	2	1	1		1	1	1			
	Person	11	5	13	51	15	71	50	86	68	2	28	85	81	10	47	16
	Server	58	28	56	190	88	421	344	303	217	38	85	372	256	46	166	78
	User Dev	9	4	8	33	8	32	38	48	38	3	15	55	177	4	37	12

0% 25% 50% 75% 100%

***Verizon DBIR 2023, p. 52**

Financial and Insurance*

Frequency	1,832 incidents, 480 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, Miscellaneous Errors and System Intrusion represent 77% of breaches
Threat actors	External (66%), Internal (34%), Multiple (1%) (breaches)
Actor motives	Financial (97%), Espionage (3%), Convenience (1%), Ideology (1%) (breaches)
Data compromised	Personal (74%), Credentials (38%), Other (30%), Bank (21%) (breaches)
What is the same?	The top three patterns remain the same, but their order of ascendancy has rearranged. Personal data, very useful for fraud, continues to be the most desired data type stolen.

***Verizon DBIR 2023, p. 56**

Healthcare*

Frequency	525 incidents, 436 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 68% of breaches
Threat actors	External (66%), Internal (35%), Multiple (2%) (breaches)
Actor motives	Financial (98%), Espionage (2%), Fun (1%), Ideology (1%) (breaches)
Data compromised	Personal (67%), Medical (54%), Credentials (36%), Other (17%) (breaches)
What is the same?	The top three patterns remain the same, although the order has changed. Internal actors making mistakes continue to trouble this sector.

***Verizon DBIR 2023, p. 57**

Regions*

Region	Frequency	Top patterns	Threat actors	Actor motives	Data compromised
APAC	699 incidents, 164 with confirmed data disclosure	Social Engineering, System Intrusion and Basic Web Application Attacks represent 93% of breaches	External (92%), Internal (9%), Partner (2%), Multiple (2%) (breaches)	Financial (61%), Espionage (39%), Convenience (2%), Grudge (2%), Secondary (1%) (breaches)	Internal (56%), Secrets (42%), Other (33%), Credentials (29%) (breaches)
EMEA	2,557 incidents, 637 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 97% of breaches	External (98%), Internal (2%), Multiple (1%) (breaches)	Financial (91%), Espionage (8%), Ideology (1%), Fun (1%) (breaches)	Credentials (53%), Internal (37%), System (35%), Other (15%) (breaches)
LAC	535 incidents, 65 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 94% of breaches	External (95%), Internal (5%), Partner (2%), Multiple (2%) (breaches)	Financial (93%), Espionage (11%), Ideology (2%) (breaches)	System (55%), Internal (32%), Classified (23%), Credentials (23%), Other (19%) (breaches)
NA	9,036 incidents, 1,924 with confirmed data disclosure	System Intrusion, Basic Web Application Attacks and Social Engineering represent 85% of breaches	External (94%), Internal (12%), Multiple (9%), Partner (2%) (breaches)	Financial (99%), Espionage (1%), Grudge (1%) (breaches)	Credentials (67%), Internal (50%), Personal (38%), Other (24%) (breaches)

Table 6. At a glance for regions

***Verizon DBIR 2023, p. 70**

Year in Review*

- December, 2021/ January, 2022: Log4j
- February, 2022: Invasion of Ukraine
- March, 2022: Zero-days of Chrome, Firefox, etc.
- April, 2022: Patching more Zero-days
- May, 2022: Vulnerabilities in infrastructure components (Folina in MSDT)
- June, 2022: Patches for Atlassian Zero-days
- July, 2022: Cyber intelligence reports before Blackhat/DEFCON
- August, 2022: 2nd Zero-day in MSDT
- September, 2022: More Zero-days in Chrome, Edge
- October, 2022: “ProxyNotShell” (Microsoft Exchange)
- November, 2022: Patches from Microsoft, Google
- December, 2022: Abuse of Microsoft developer accounts

***Verizon DBIR 2023, pp. 74-77**

Resources

Verizon Data Breach Investigations Report (DBIR) 2023

https://verizon.com/dbir/

VERIS Resources

http://verisframework.org

Features information on the framework with examples and enumeration listings

https://github.com/vz-risk/veris

Features the full VERIS schema

https://github.com/vz-risk/vcdb

Provides access to database on ***publicly disclosed breaches***, the VERIS Community Database

Questions?

Contacts

Web Site:
https://roberthurlbut.com

Twitter: @RobertHurlbut

Thank you!