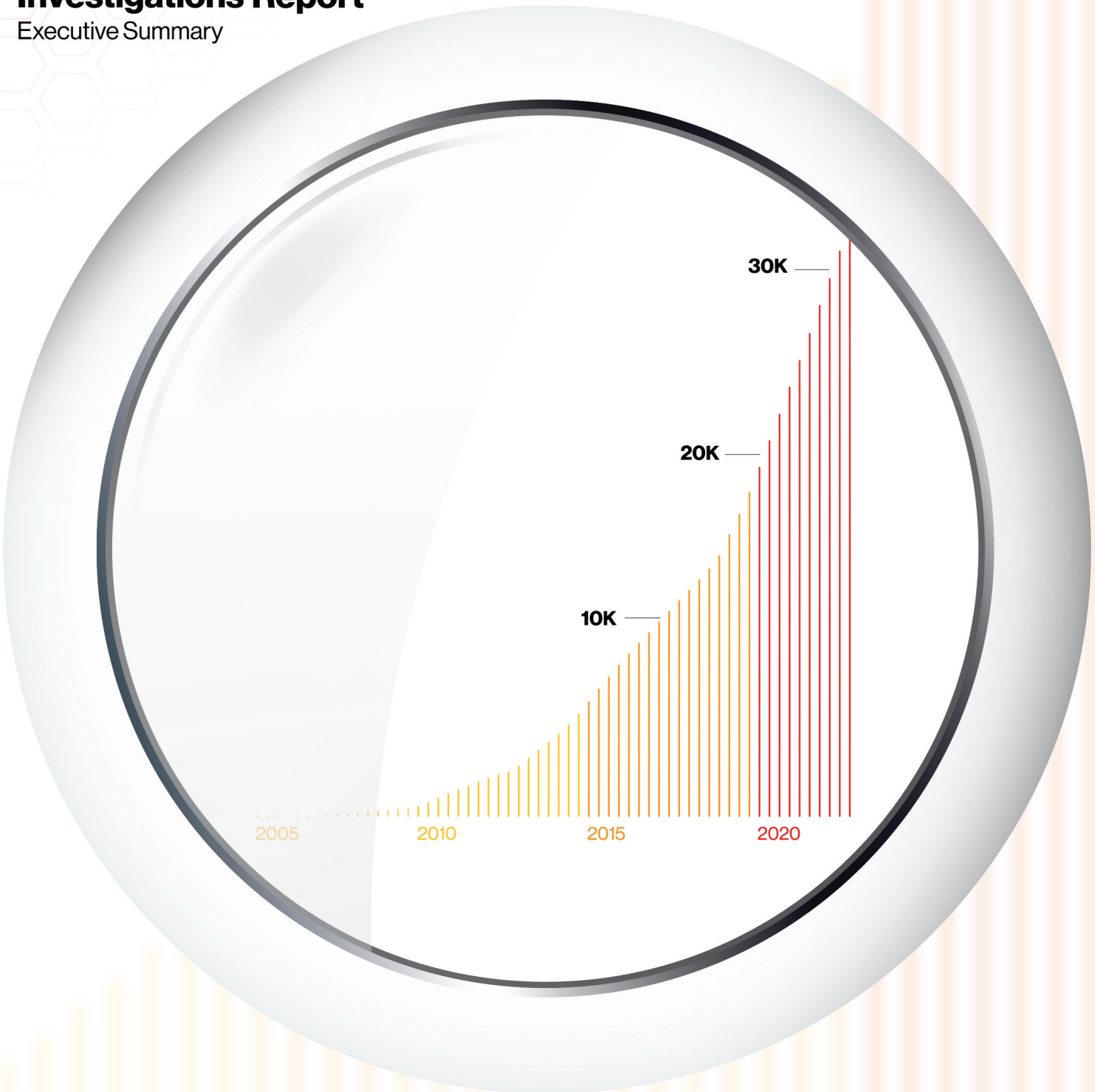
DBIR

2023 Data Breach Investigations Report

Executive Summary



verizon

About the cover

The magnifier on the cover is intended to visually convey the effort the team made to refocus our energy and resources more on our core breach dataset. The graph that is magnified is simply a cumulative count of the number of breaches in our dataset as the years have gone by since our first report. Long-time readers may notice the Vocabulary for Event Recording and Incident Sharing (VERIS) Framework trademark honeycombs, which are meant to convey the 4As (Actor, Action, Asset, Attribute) and their various enumerations.

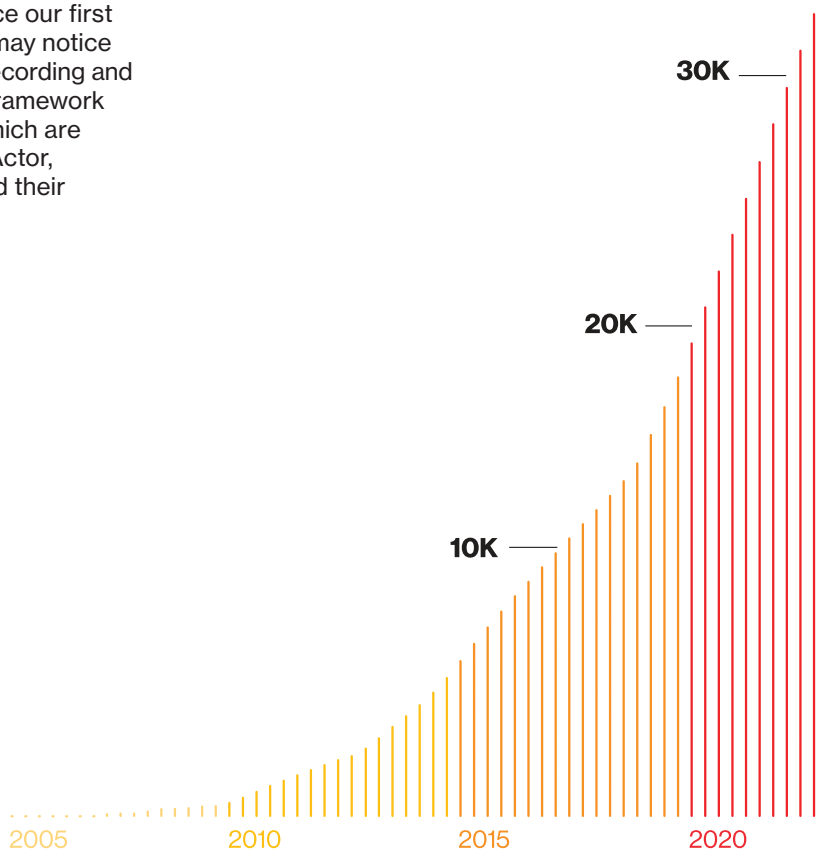


Table of contents

Welcome

Hello, and welcome to the 16th annual installment of the Verizon Data Breach Investigations Report (DBIR).

The DBIR aims to provide security professionals with an in-depth analysis of data-driven, real-world instances of cybercrime and how cyberattacks play out across organizations of different sizes as well as from different verticals and disparate geographic locations. We hope that by doing so, we can provide you with insight into what particular threats your organization is most likely to face and thereby help prepare you to handle them in the best possible manner.

As in past years, we will examine what our data has to tell us about threat actors and the tools they employ against enterprises. This year, we looked at 16,312 security incidents, of which 5,199 were confirmed breaches. This data represents actual, real-world breaches and incidents investigated by the Verizon Threat Research Advisory Center (VTRAC), now celebrating its 20th year, or provided to us by one of our global contributors without whose generous help this document could not be produced. We hope you can use this report and the information it contains to increase your awareness of the most common tactics used against organizations at large and against your specific industry and what you can do to help protect your company and its assets. Read on for report highlights, pass this summary to colleagues and download the full report for a more detailed view of the threats you may face today.

Patterns over time in incidents and breaches

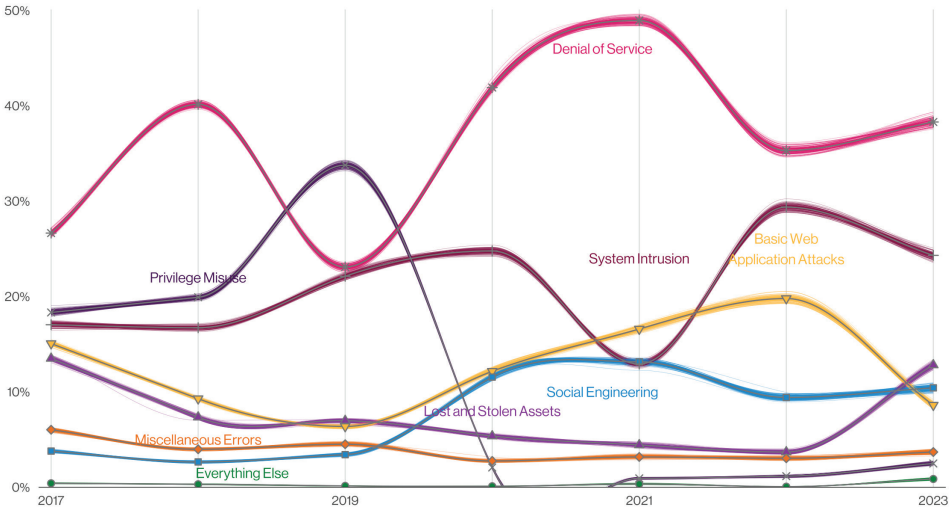


Figure 1. Patterns over time in incidents

It is sometimes helpful to view our incident classification patterns to find out how they have fared year over year. Figure 1 shows the patterns over time for incidents, and it is readily apparent that Denial of Service is top of the heap, as it has been for several years now.

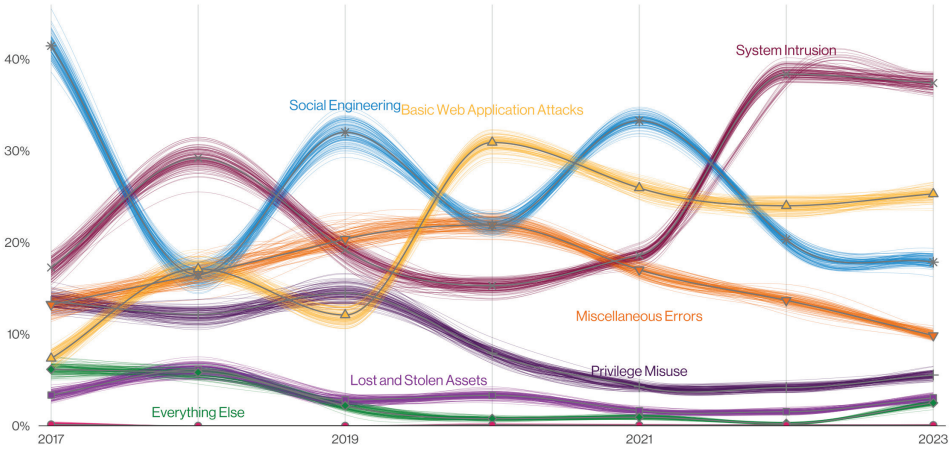


Figure 2. Patterns over time in breaches

By contrast, Figure 2 illustrates how different the environment appears when we are focused on those incidents where there was confirmed data loss.

The System Intrusion pattern—with its more complex attacks—has been on the rise and frequently includes multistep attacks that often include ransomware. But we're getting ahead of ourselves. Let's take a look at a few of the key takeaways from this year's report.

Key takeaways

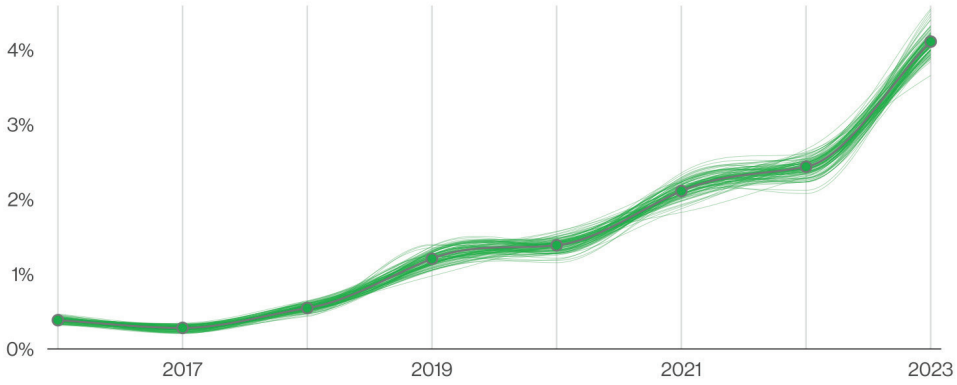


Figure 3. Pretexting incidents over time

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. Perhaps this is why why Business Email Compromise (BEC) attacks (which are in essence pretexting attacks) have almost doubled across our entire incident dataset, as can be seen in Figure 3, and now represent more than 50% of incidents within the Social Engineering pattern.

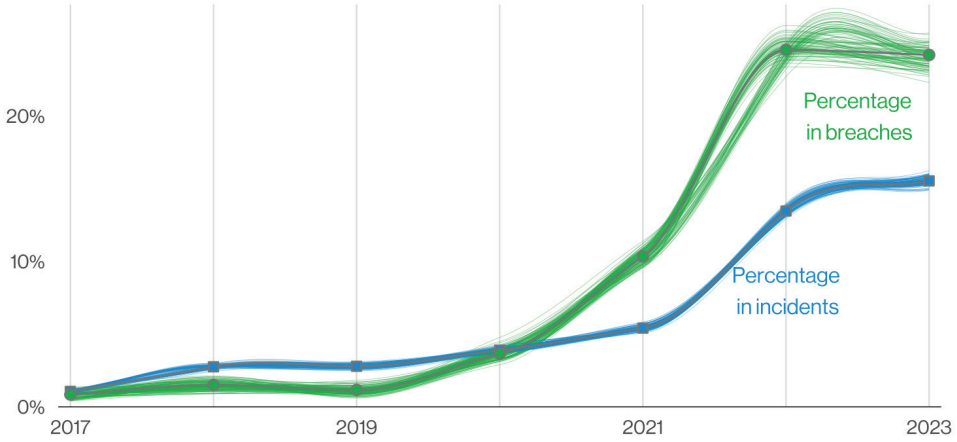


Figure 4. Ransomware action variety over time

Ransomware continues its reign as one of the top Action types present in breaches, and while it did not actually grow, it did hold statistically steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries.

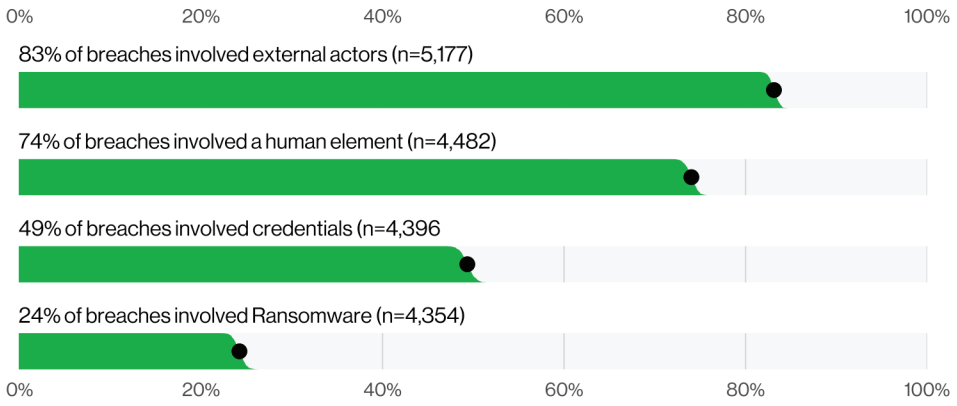
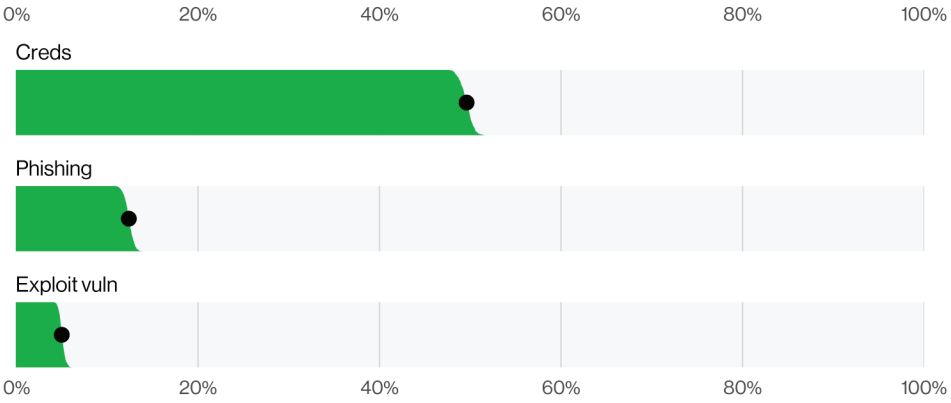


Figure 5. Select key enumerations

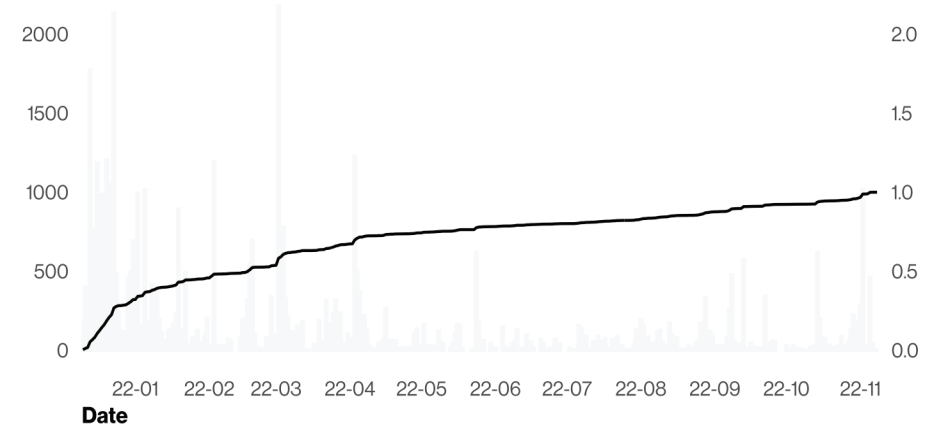
74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

83% of breaches involved External actors, and the primary motivation for attacks continues to be overwhelmingly financially driven, at 95% of breaches.



The three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities.

Figure 6. Select enumerations in non-Error, non-Misuse breaches (n=4,291)



More than 32% of all Log4j scanning activity over the course of the year happened within 30 days of its release (with the biggest spike of activity occurring within 17 days).

Figure 7. Percentage of Log4j scanning for 2022

Log4j was so top-of-mind in our data contributors' incident response that 90% of incidents with Exploit vuln as an action had "Log4j," or "CVE-2021-44228" in the comments section. However, only 20.6% of the incidents had comments.

Figure 8. Percentage of identified Exploit vuln that was Log4j (n=394). Each glyph represents an incident.

Industry highlights

Cybercrime is a serious risk regardless of your industry vertical or organization size, although the type and frequency of the attacks may differ to some degree depending on the size, function and location of your business. To deploy defenses efficiently and effectively, it is necessary not only to view the bigger picture with regard to the threat landscape but also to be very aware of what is most likely to affect you in particular. This year, we again offer 10 industry snapshots.

Industry labels

In the DBIR, we align with the North American Industry Classification System (NAICS) standard to categorize the victim organizations in our corpus.

The standard uses two-to six-digit codes to classify businesses and organizations. Our analysis is typically done at the two-digit level, and we will specify NAICS codes along with an industry label. For example, a chart with a label of Public Administration (NAICS 92) is not indicative of 92 as a value. “92” is the code for the Public Administration sector. Detailed information on the codes and the classification system are available here: https://www.census.gov/naics/?58967?yearbck=2012

Accommodation and Food Services

(NAICS 72)

Frequency	254 incidents, 68 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 90% of breaches
Threat actors	External (93%), Internal (9%), Multiple (1%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Payment (41%), Credentials (38%), Personal (34%), Other (26%) (breaches)
What is the same?	We are seeing the same three attack patterns hitting this sector as we did last year—but the order has changed. External actors continue to target this industry because of the lucrative data the members hold.
Summary	Payment card data continues to be the top target for Data types in this sector, unsurprisingly. The use of RAM scrapers continues to be a favorite tool of the Financially motivated attackers that regularly plague this sector.

Educational Services
(NAICS 61)

Frequency	497 incidents, 238 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Social Engineering represent 76% of breaches
Threat actors	External (72%), Internal (29%), Multiple (1%), Partner (1%) (breaches)
Actor motives	Financial (92%), Espionage (8%), Convenience (1%), Fun (1%) (breaches)
Data compromised	Personal (56%), Credentials (40%), Other (25%), Internal (20%) (breaches)
What is the same?	System Intrusion and Miscellaneous Errors are yet again two of the top three patterns for this industry. The ratio of External and Internal actors is nearly the same as last year.
Summary	Basic Web Application Attacks dropped out of the top three to be replaced by Social Engineering. Ransomware continues to play a large role in breaches in this vertical.

Financial and Insurance
(NAICS 52)

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.
Summary	With Basic Web Application Attacks as the top pattern, we know that the adversaries are successfully gaining access without too much effort. This, combined with the Misdelivery error, indicates there is room for good controls to help cover a decent percentage of attacks in this sector.

Healthcare

(NAICS 62)

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.
Summary	Ransomware actors continue targeting this sector and are increasingly causing confirmed data breaches in the process. Errors (particularly Misdelivery) are consistently prevalent as well. Finally, don't discount the insider threat in this sector.

Information

(NAICS 51)

Frequency	2,110 incidents, 384 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 77% of breaches
Threat actors	External (81%), Internal (20%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (92%), Espionage (8%) (breaches)
Data compromised	Personal (51%), Credentials (37%), Other (35%), Internal (19%) (breaches)
What is the same?	System Intrusion remains the top pattern in this vertical, and it is still dominated by Financially motivated external actors.
Summary	Error continues the downward trend it has exhibited for the last several years and loses its position in the top three to Social Engineering. Denial of Service attacks account for 70% of incidents in NAICS 51.

Manufacturing

(NAICS 31 – 33)

Frequency	1,817 incidents, 262 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 83% of breaches
Threat actors	External (90%), Internal (11%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (96%), Espionage (4%), Convenience (1%) (breaches)
Data compromised	Personal (60%), Credentials (38%), Other (37%), Internal (18%) (breaches)
What is the same?	The top three attack patterns remain the same, but their order has changed slightly. Financially motivated external actors continue to wreak havoc in this industry.
Summary	Hacking and Malware actions are pacing each other in the race for the top two spots. While Social Engineering attacks are still alive and well, they are a distant third. For incidents, do not discount Denial of Service attacks against this industry's infrastructure to disrupt the ability to meet deadlines.

Mining, Quarrying, and Oil & Gas Extraction + Utilities

(NAICS 21 + 22)

Frequency	143 incidents, 47 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 81% of breaches
Threat actors	External (80%), Internal (20%) (breaches)
Actor motives	Financial (63% – 93%), Espionage (4%–32%), Grudge (1%–21%), Ideology (0%–15%), Convenience/Fear/Fun/Other/Secondary (0%–7% each) (breaches)
Data compromised	Personal (50%), Internal (33%), Other (26%), Credentials (24%) (breaches)
What is the same?	System Intrusion and Basic Web Application Attacks remain significant causes for concern in this industry.
Summary	Ransomware is responsible for approximately one out of three breaches in this vertical. Social Engineering, in spite of its overall rise, has decreased in this industry.

Professional, Scientific and Technical Services

(NAICS 54)

Frequency	1,398 incidents, 423 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 90% of breaches
Threat actors	External (92%), Internal (9%), Multiple (3%), Partner (2%) (breaches)
Actor motives	Financial (96%), Espionage (4%), Convenience (1%) (breaches)
Data compromised	Personal (57%), Credentials (53%), Other (25%), Internal (16%) (breaches)
What is the same?	System Intrusion, Basic Web Application Attacks and Social Engineering continue to be the main threats to organizations in this sector.
Summary	Even though the top patterns haven't changed for this industry, this sector has experienced an increase in ransomware over the year, with incidents following the same core vectors as the previous year.

Public Administration

(NAICS 92)

Frequency	3,273 incidents, 584 with confirmed data disclosure
Top patterns	System Intrusion, Lost and Stolen Assets, and Social Engineering represent 76% of breaches
Threat actors	External (85%), Internal (30%), Multiple (16%) (breaches)
Actor motives	Financial (68%), Espionage (30%), Ideology (2%) (breaches)
Data compromised	Personal (38%), Other (35%), Credentials (33%), Internal (32%) (breaches)
What is the same?	This sector continues to be targeted by Financially motivated external threat actors as well as spying Nation-states that are interested in what their rivals are doing. Personal data remains the most often stolen data type.
Summary	This sector continues to make top scores in Espionage-motivated breaches. It is also rich in multiple actor breaches. External and Partner or Internal actors working together to steal data is not the kind of international cooperation we want to see fostered.

Retail

(NAICS 44 – 45)

Frequency	406 incidents, 193 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 88% of breaches
Threat actors	External (94%), Internal (7%), Multiple (2%), Partner (2%) (breaches)
Actor motives	Financial (100%), Espionage (1%) (breaches)
Data compromised	Payment (37%), Credentials (35%), Other (32%), Personal (23%) (breaches)
What is the same?	Retail organizations continue to be lucrative targets for cybercriminals looking to collect Payment card data.
Summary	While the same three patterns dominate this industry as many others, Retail has the added bonus of being targeted for its Payment card data in addition to common threats like Ransomware and Basic Web Application Attacks.

Small and medium business

In certain prior reports, we have compared and contrasted small and medium businesses (SMBs) against large organizations to determine whether the attack surface differed significantly between them. Increasingly both SMBs and large companies are using similar services and infrastructure, and that means that their attack surfaces share more in common than ever before. This has led to a convergence of attack profiles regardless of the size of the organization. However, what is very different is the ability of organizations to respond to threats due to the number of resources they can deploy in the event that they are attacked.

Therefore, this year we decided to leverage the work we have done with MITRE to map VERIS to ATT&CK a bit more into the real world and apply it to how you would use these mappings with the appropriate Center for Internet Security (CIS) Implementation Group protective controls for the various sizes of SMBs.

Attack of the Frameworks
The DBIR team continues to expand the Vocabulary for Event Recording and Incident Sharing (VERIS) Framework to classify and analyze incidents and breaches. We have collaboratively developed mappings with MITRE ATT&CK and the CIS Critical Security Controls to assist organizations with developing and maintaining a data-driven cybersecurity program.

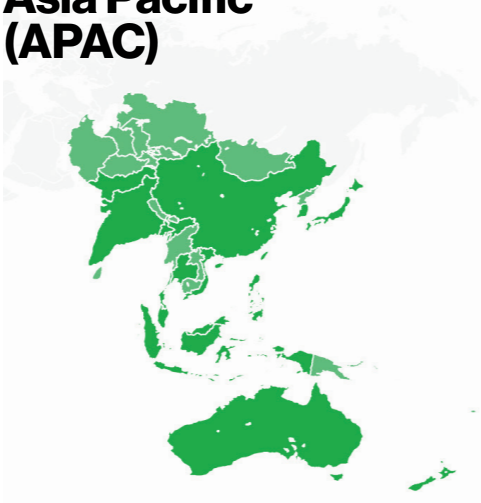
The second version of the VERIS/ATT&CK mapping has just been released as of April 6, 2023, and you can read more about it at https://center-for-threat-informed-defense.github.io/attack_to_veris/. This renewed combination of forces is timely due to the increased regulatory pressure of mandatory data breach reporting, even as there is no commonly accepted format in how this reporting should be done.

	Small businesses (less than 1,000 employees)	**Large businesses (more than 1,000 employees)**
Frequency	699 incidents, 381 with confirmed data disclosure	496 incidents, 227 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches	System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches
Threat actors	External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches)	External (89%), Internal (13%), Multiple (2%), Partner (2%) (breaches)
Actor motives	Financial (98%), Espionage (1%), Convenience (1%), Grudge (1%) (breaches)	Financial (97%), Espionage (3%), Ideology (2%), Convenience (1%), Fun (1%) (breaches)
Data compromised	Credentials (54%), Internal (37%), Other (22%), System (11%) (breaches)	Internal (41%), Credentials (37%), Other (30%), System (22%) (breaches)

Regional findings

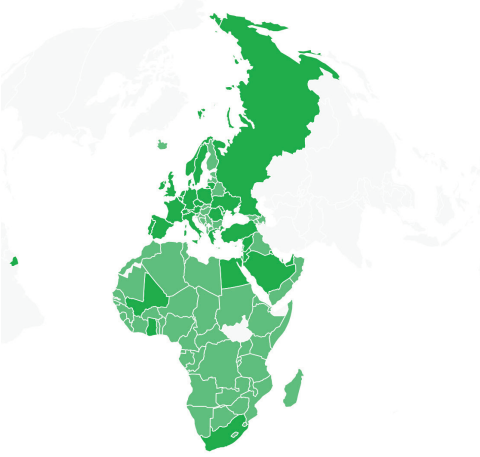
This edition of the DBIR marks the fourth year we have examined cybercrime incidents from a macro-regional point of view. We hope our readers find this broader look at cybercrime useful and instructive. As previously mentioned, our visibility into a certain region is determined by many variables, including contributors, regional disclosure laws and our own data. If your part of the world is not featured in the following pages, please contact us about becoming a data contributor and motivate other organizations in your area to do the same so that we can keep growing and improving our coverage each year. Even if your region is not represented here, this does not mean we have no visibility into the region but rather that we don't have enough incidents in that geography to have a statistically significant section.

Asia Pacific (APAC)



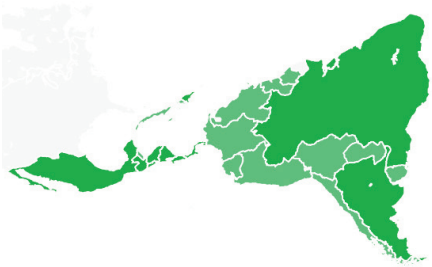
Frequency	699 incidents, 164 with confirmed data disclosure
Top patterns	Social Engineering, System Intrusion and Basic Web Application Attacks represent 93% of breaches
Threat actors	External (92%), Internal (9%), Partner (2%), Multiple (2%) (breaches)
Actor motives	Financial (61%), Espionage (39%), Convenience (2%), Grudge (2%), Secondary (1%) (breaches)
Data compromised	Internal (56%), Secrets (42%), Other (33%), Credentials (29%) (breaches)

Europe, Middle East and Africa (EMEA)



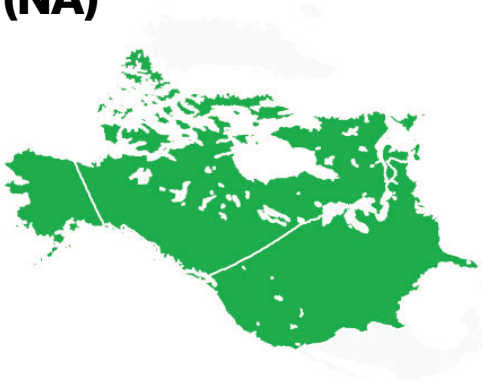
Frequency	2,557 incidents, 637 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 97% of breaches
Threat actors	External (98%), Internal (2%), Multiple (1%) (breaches)
Actor motives	Financial (91%), Espionage (8%), Ideology (1%), Fun (1%) (breaches)
Data compromised	Credentials (53%), Internal (37%), System (35%), Other (15%) (breaches)

Latin America and the Caribbean (LAC)



Frequency	535 incidents, 65 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 94% of breaches
Threat actors	External (95%), Internal (5%), Partner (2%), Multiple (2%) (breaches)
Actor motives	Financial (93%), Espionage (11%), Ideology (2%) (breaches)
Data compromised	System (55%), Internal (32%), Classified (23%), Credentials (23%), Other (19%) (breaches)

Northern America (NA)



Frequency	9,036 incidents, 1,924 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 85% of breaches
Threat actors	External (94%), Internal (12%), Multiple (9%), Partner (2%) (breaches)
Actor motives	Financial (99%), Espionage (1%), Grudge (1%) (breaches)
Data compromised	Credentials (67%), Internal (50%), Personal (38%), Other (24%) (breaches)

Stay informed and threat ready.

Facing today's threats requires intelligence from a source you can trust.

The full DBIR contains details on the actors, actions and patterns that can help you prepare your defenses and educate your organization. Get the intelligence you need to protect your organization:

Read the full 2023 DBIR at verizon.com/dbir.

Want to make the world a better place?

The DBIR relies on contributions from dozens of organizations, and we'd love to have you. If you are interested in becoming a contributor to the annual Verizon DBIR (and we hope you are), the process is very easy and straightforward. Please email us at dbircontributor@verizon.com or tweet us @VZDBIR to provide feedback for improving the DBIR. Learn more about the VERIS Framework at verisframework.org.