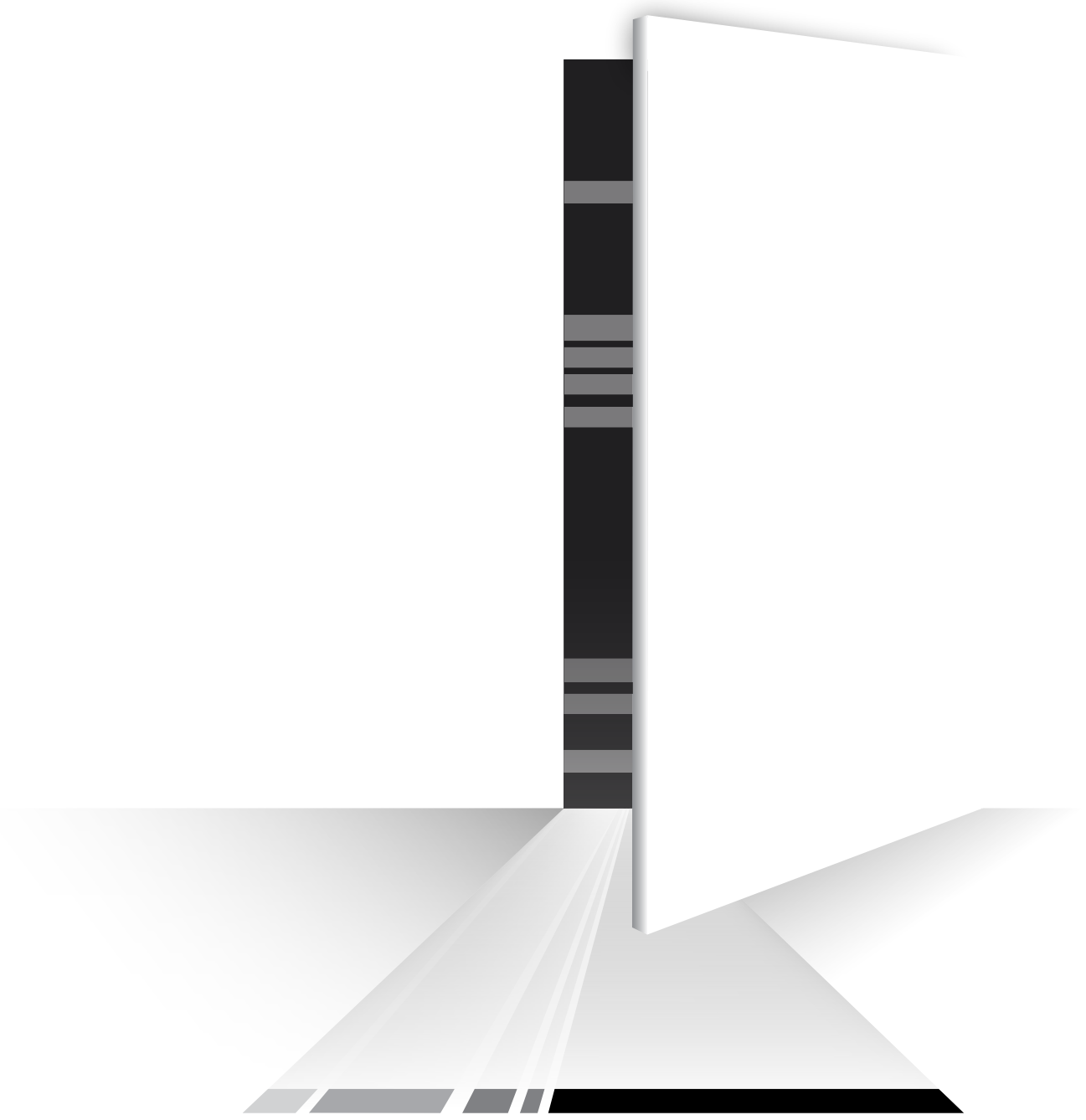
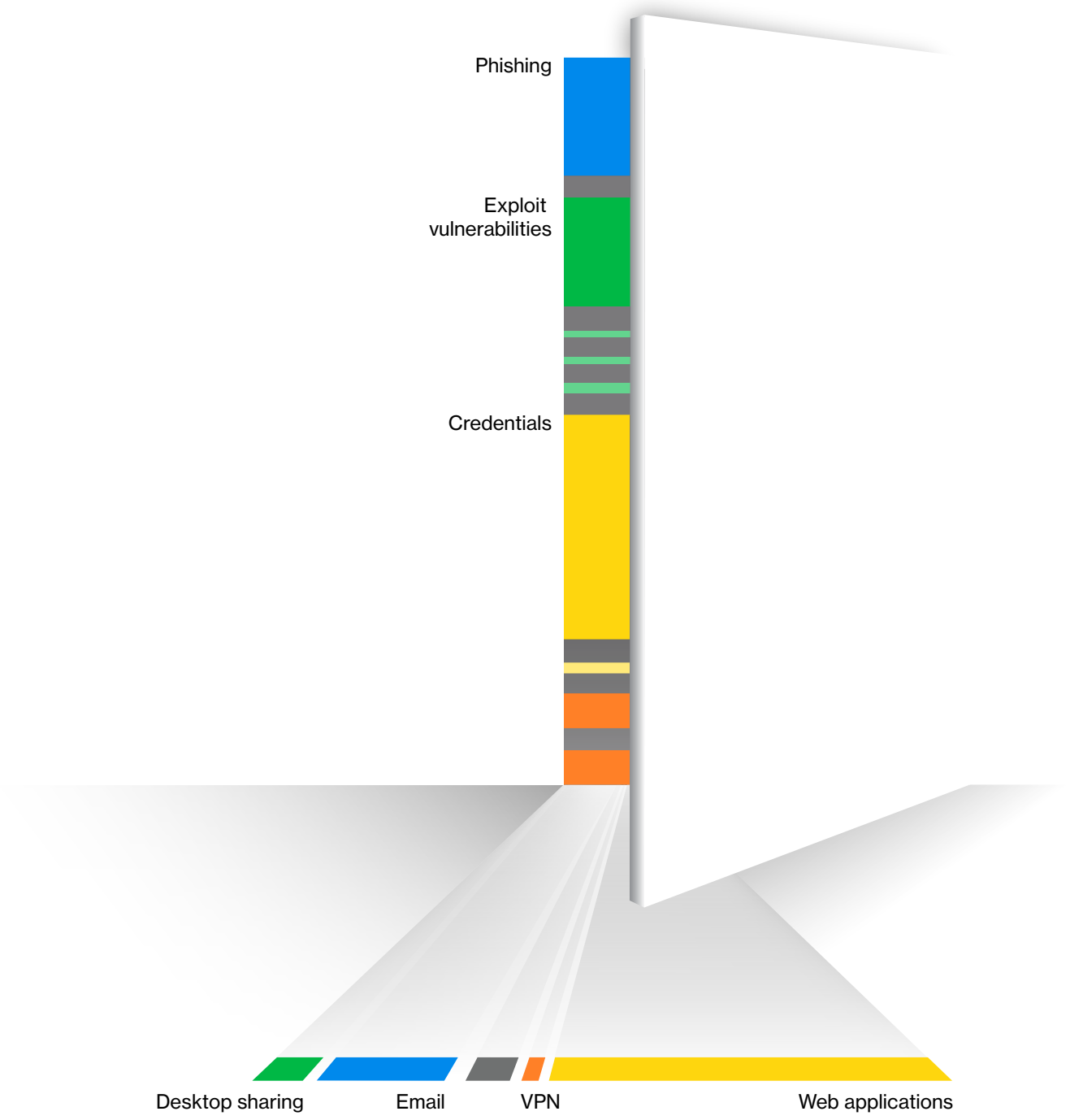
2024 Data Breach Investigations Report

Retail Snapshot



verizon business


Phishing
Exploit vulnerabilities
Credentials
Desktop sharing
Email
VPN
Web applications

About the cover

This year, the report is delving deeper into the pathway to breaches in an effort to identify the most likely Action and vector groupings that lead to breaches given the current threat landscape. The cracked doorway on the cover is meant to represent the various ways attackers can make their way inside. The opening in the door shows the pattern of our combined “ways-in” percentages (see Figure 7 of the full report for a more straightforward representation), and it lets out a band of light displaying a pattern of the Action vector quantities. The inner cover highlights and labels the quantities in a less abstract way. Hope you enjoy our art house phase.

Table of contents

Welcome

Hello, and welcome to the Verizon Data Breach Investigations Report (DBIR) Retail Snapshot.

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 analyzed 30,458 real-world security incidents, of which 10,626 were confirmed data breaches (a record high!), with victims spanning 94 countries.

This data represents actual, real-world breaches and incidents investigated by the Verizon Threat Research Advisory Center (VTRAC) 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 your specific industry. It offers strategies to help protect your company and its assets. Read the full report for a more detailed view of the threats you may face today at verizon.com/dbir.

About the 2024 DBIR incident dataset

Each year, the DBIR timeline for in-scope incidents is from November 1 of one calendar year through October 31 of the next calendar year. Thus, the incidents described in this year's report took place between November 1, 2022, and October 31, 2023. The 2023 caseload is the primary analytical focus of the 2024 report, but the entire range of data is referenced throughout, notably in trending graphs. The time between the latter date and the date of publication for the report is spent in acquiring the data from our global contributors, anonymizing and aggregating that data, analyzing the dataset, and finally creating the graphics and writing the report.

Industry labels

This snapshot highlights important takeaways for the Retail Trade (NAICS 44–45) sector, which includes establishments primarily engaged in retailing merchandise generally without transformation and rendering services incidental to the sale of merchandise.

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 Retail (NAICS 44–45) is not indicative of 44–45 as a value. "44–45" is the code for the Retail Trade sector. Detailed information on the codes and the classification system is available here:

https://www.census.gov/naics/?58967?yearbck=2012

30,458
security incidents investigated

10,626
confirmed breaches

Summary of findings

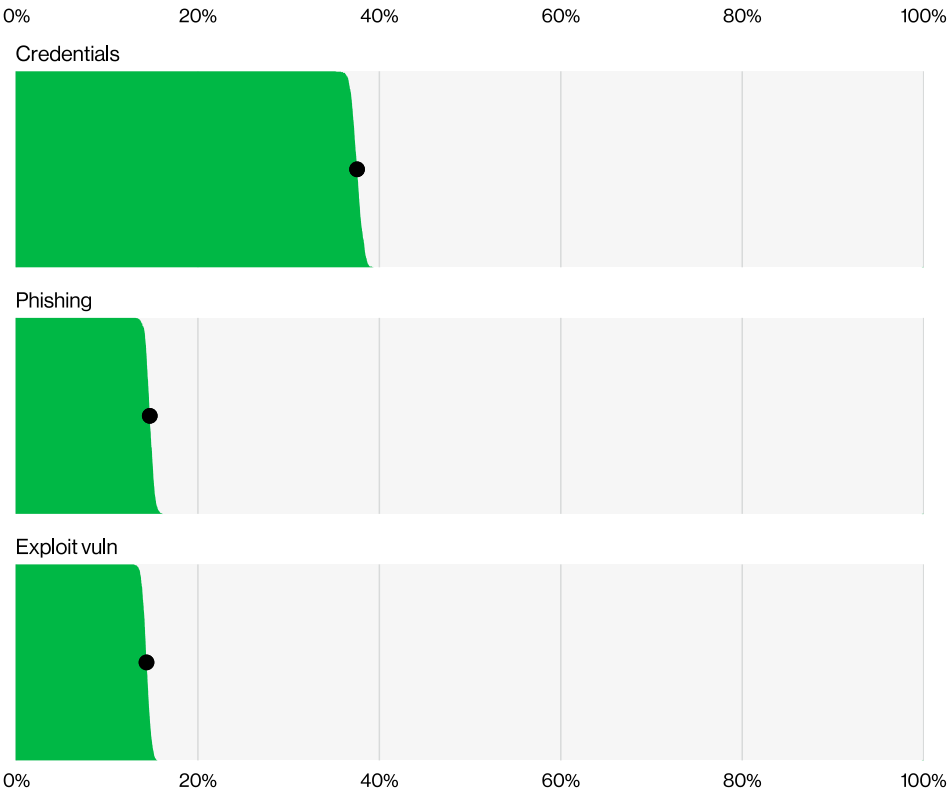


Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

They're exploiting our vulnerabilities.

Our ways-in analysis witnessed a substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach when compared to previous years—almost tripling (180% increase) from last year. This was largely due to the effect of MOVEit and similar zero-day vulnerabilities, primarily leveraged by ransomware and other extortion-related threat actors using Web applications as their initial entry points.

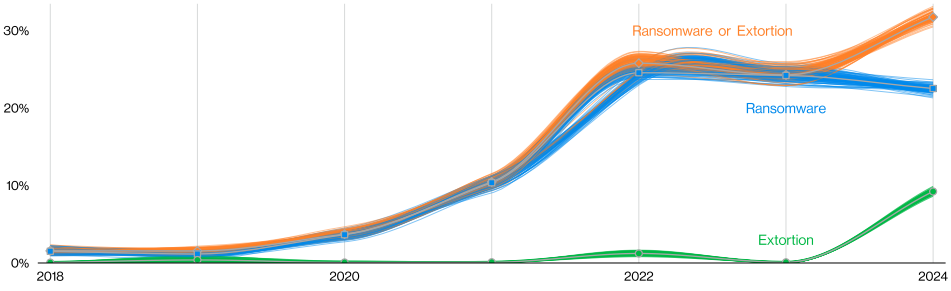


Figure 2. Ransomware and Extortion breaches over time

Ransomware and Extortion are significant threats.

Roughly one-third of all breaches involved Ransomware or some other Extortion technique. Pure Extortion attacks have risen over the past year and are now a component of 9% of all breaches. Ransomware actors have moved toward these newer techniques, resulting in a bit of a decline in Ransomware to 23%. However, when combined, they represent a strong growth to 32% of breaches. Additionally, Ransomware was a top threat across 92% of industries.

Figure 3. Select key enumerations in breaches

We've identified the most common ways in.

We have revised our calculation of the human element in breaches to exclude malicious Privilege Misuse to provide a clearer metric of what security awareness can impact. For this year's dataset, the human element was a component of 68% of breaches, roughly the same as the previous period described in the 2023 DBIR.

In this issue, we are introducing an expanded concept of a breach involving a third party to include partner infrastructure being affected and direct or indirect software supply chain issues—including when an organization is affected by vulnerabilities in third-party software. In short, these are the breaches an organization could potentially mitigate or prevent by trying to select vendors with better security track records. We see this figure at 15% this year, a 68% increase from the previous year, mostly fueled by the use of zero-day exploits for Ransomware and Extortion attacks.

Our dataset saw a growth of breaches involving Errors, now at 28%, as we broadened our contributor base to include several new mandatory breach notification entities. This validates our suspicion that errors are more prevalent than media or traditional incident response–driven bias would have us believe.

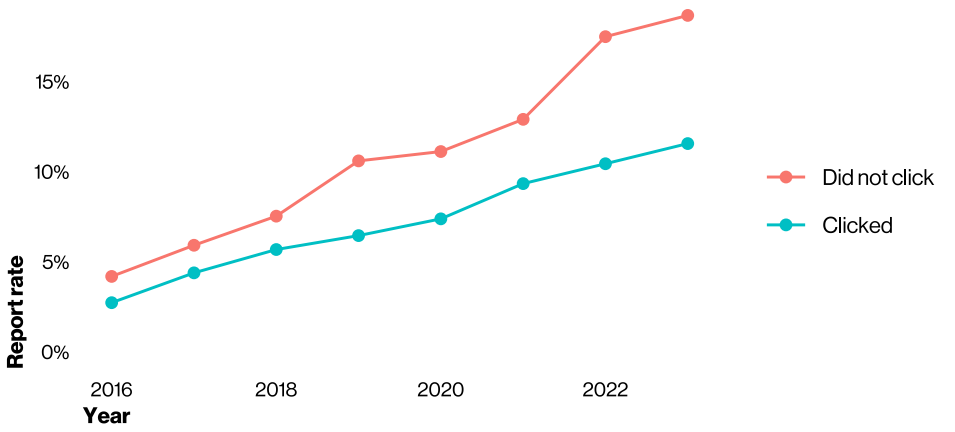


Figure 4. Phishing email report rate by click status

Falling for Phishing happens fast.

The overall reporting rate of Phishing has been growing over the past few years. In security awareness exercise data contributed by our partners during 2023, 20% of users reported phishing in simulation engagements, and 11% of the users who clicked the email also reported. This is welcome news because the median time to click on a malicious link after the email is opened is 21 seconds and then only another 28 seconds for the person caught in the phishing scheme to enter their data. This leads to an alarming finding: The median time for users to fall for phishing emails is less than 60 seconds.

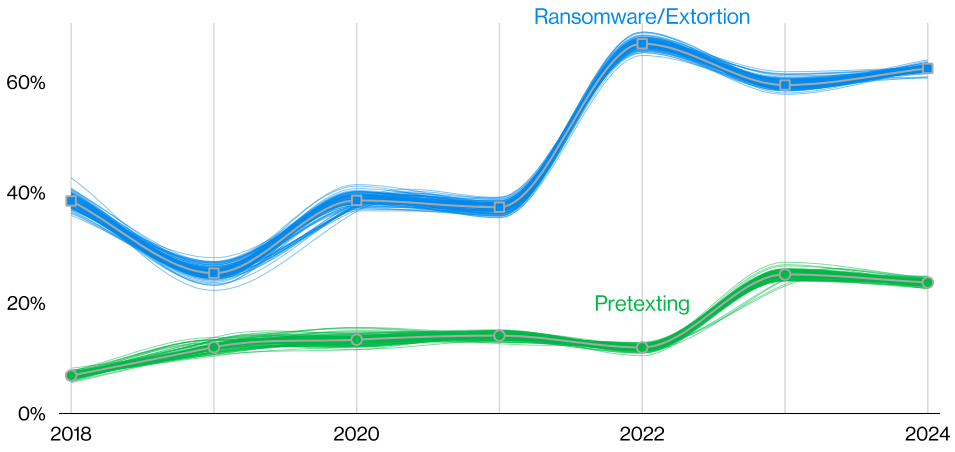


Figure 5. Select action varieties in Financial motive over time

They go where the money is.

Financially motivated threat actors will typically stick to the attack techniques that give them the most return on investment.

Over the past three years, the combination of Ransomware and other Extortion breaches have accounted for almost two-thirds (fluctuating between 59% and 66%) of those attacks. According to the FBI's Internet Crime Complaint Center (IC3) ransomware complaint data, the median loss associated with the combination of Ransomware and other Extortion breaches has been $46,000, ranging between $3 (three dollars) and $1,141,467 for 95% of cases. We also found from ransomware negotiation data contributors that the median ratio of initially requested ransom and company revenue is 1.34%, but it fluctuated between 0.13% and 8.3% for 80% of the cases.

Similarly, over the past two years, we have seen incidents involving Pretexting (the majority of which had Business Email Compromise [BEC] as the outcome) accounting for one-fourth (ranging between 24% and 25%) of financially motivated attacks. In both years, the median transaction amount of a BEC was around $50,000.

Incident Classification Patterns

The DBIR first introduced the Incident Classification Patterns in 2014 as a useful shorthand for scenarios that occurred very frequently. In 2022, due to changes in attack type and the threat landscape, we revamped and enhanced those patterns, moving from nine to eight—the seven you see in this report and the Everything Else "pattern," which is a catch-all for incidents that don't fit within the orderly confines of the other patterns.

These patterns are based on an elegant machine-learning clustering process, equipped to better capture complex interaction rules, and they are much more focused on what happens during the breach. That makes them better suited for control recommendations, too.

Here are our key findings for each pattern:

System Intrusion

These are complex attacks that leverage malware and/or hacking to achieve their objectives, including deploying ransomware.

Ransomware attacks continue to drive the growth of this pattern as they now account for 23% of all breaches and 70% of the incidents within System Intrusion.

- Ransomware (or some type of Extortion) appears in 92% of industries as one of the top threats.
- Analyzing the FBI Internet Crime Complaint Center dataset this year, we found that the median adjusted loss (after law enforcement worked to try to recover funds) for those who did pay was around $46,000.
- Traditional Ransomware's prevalence declined slightly to 23%. However, roughly one-third (32%) of all breaches involved some type of Extortion technique, including Ransomware. The meteoric growth of Extortion attacks made this combined threat stand out in our dataset.

Social Engineering

This attack involves the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.

More than 40% of incidents involved Pretexting, and 31% involved Phishing. Other tried-and-true tactics include attacks coming in via email, text and websites.

- Phishing and Pretexting via email continue to be the leading cause of incidents in this sector, accounting for 73% of breaches.
- The median time for users to fall for phishing emails is less than 60 seconds.
- More than 20% of users identified and reported phishing per engagement, including 11% of the users who did click the email.
- Over the past two years, roughly one-fourth (between 24% and 25%) of financially motivated incidents involved Pretexting, the majority of which resulted in a Business Email Compromise (BEC). In both years, the median transaction amount of a BEC was around $50,000.[1]

1. According to the FBI's Internet Crime Complaint Center ransomware complaint data

Basic Web Application Attacks These attacks are against a web application, and after the initial compromise, they do not have a large number of additional Actions. It is the "get in, get the data and get out" pattern.	Financially motivated external actors continue to target credentials and personal information. • Over the past 10 years, stolen credentials have appeared in almost one-third (31%) of breaches. • Our dataset shows just over 8% of breaches in the Basic Web Application Attacks pattern. • After examining postings from marketplaces dedicated to selling and reselling credentials and cookies collected from password stealers, we found that 65% of these credentials were posted for sale on criminal forums less than one day from when they were collected. • There is no substantial difference between large organizations (55%) and small organizations (47%) in the Basic Web Application Attacks pattern.
Miscellaneous Errors Incidents where unintentional actions directly compromised a security attribute of an information asset fall into this pattern. This does not include lost devices, which are grouped with theft instead.	More than 50% of errors were the result of Misdelivery, continuing last year's trend, while other errors, such as Disposal, are declining. • Misconfiguration is the next most common error and was seen in approximately 10% of breaches. • Classification errors, Publishing errors and Gaffes (verbal slips) are all relatively tightly packed in order of mention. Disposal errors continue to decline ever so slightly (as has been the general trend for the last several years) and accounted for just over 1% of the cases in this pattern. • End-users now account for 87% of errors, emphasizing the need for universal error-catching controls across industries.
Denial of Service These attacks are intended to compromise the availability of networks and systems. This includes both network and application layer attacks.	Denial of Service is responsible for more than 50% of incidents analyzed this year. • Our ongoing analysis of content delivery network (CDN)-monitored, web application-focused Denial of Service attacks shows that even though the median attack size has reduced slightly from 2.2 gigabits per second (Gbps) to 1.6 Gbps, the 97.5th percentile of those attacks increased to 170 Gbps from the previous high of 124 Gbps. • Subject matter experts (SMEs) continue to report the growth of low-volume, persistent attacks on high-interaction services such as Domain Name System (DNS).

Lost and Stolen Assets Incidents where an information asset went missing, whether through misplacement or malice, are grouped into this pattern.	Devices are still much more likely to be lost than stolen. Laptops continue to be a risk for loss in particular. • This year we saw a higher percentage of incidents involving Assets in this pattern causing confirmed data breaches, with last year showing about 8% confirmed breaches and this year showing a surprising 91%.
Privilege Misuse These incidents are predominantly driven by unapproved or malicious use of legitimate privileges.	In our prior report, we saw collusion—multiple actors working in concert to achieve the goal of the breach—at 7%, which, while nowhere near the highs we saw back in 2019, was still a surprise. This year, things seem to have gone back to normal, and we are seeing collusion dropping to less than 1% of breaches. • Employees are largely taking Personal data—this is likely about taking customers' information. • Internal actors are again largely working on their own in this pattern. The Financial motivation remains in ascension, while Espionage is a distant second. Personal data is still the main targeted data type. • We saw Internal data show a bit of a spike this year as well, which would include sensitive plans and intellectual property that would attract the Espionage-motivated employee. • Finally, Banking data is remaining mostly steady over time as a targeted data type.

Table 1. Incident Classification Patterns key findings

Retail NAICS 44–45

Frequency	725 incidents, 369 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (96%), Internal (4%) (breaches)
Actor motives	Financial (99%), Espionage (1%) (breaches)
Data compromised	Credentials (38%), Other (31%), Payment (25%), System (20%) (breaches)
What is the same?	The three attack patterns not only remained consistent but are even in the same ranked order as last year. Threat actors with a Financial motivation continue to target this sector.

Summary

While this industry is usually the place where we see Payment card data stolen, the focus of the threat actors has shifted to Credentials. Pretexting is also increasing, while Phishing has dropped. Denial of Service attacks remain a problem for Retail organizations, causing disruption to their ability to serve their customers and make sales.

The Retail sector is where we often find "Magecart" threat actors. They are particularly skilled at inserting malicious code into the e-commerce sites of retail entities to siphon off (usually) Payment card information. We saw roughly the same percentage of these kinds of attacks this year as we did last year (Figure 6). However, the type of data being compromised showed a surprising change.

With Credentials standing at 38% (very close to last year's 35%) we didn't expect to see Payment card data drop to 25% (from 37%). Now, we understand how attractive and useful Credentials are to your average threat actor, but we were stunned to see Payment card data, so useful for immediate fraud, drop so precipitously (Figure 7). As we have indicated before, we get the "what" of the changes in the data, but we do not always get the "why." Is this a result of increased controls around the monetization of payment card data, making it harder for the criminals to use the data they have stolen? Or is it just that credentials are so much easier to steal? Either way, we will be interested to see if this is just a blip on the radar or an actual trend starting.

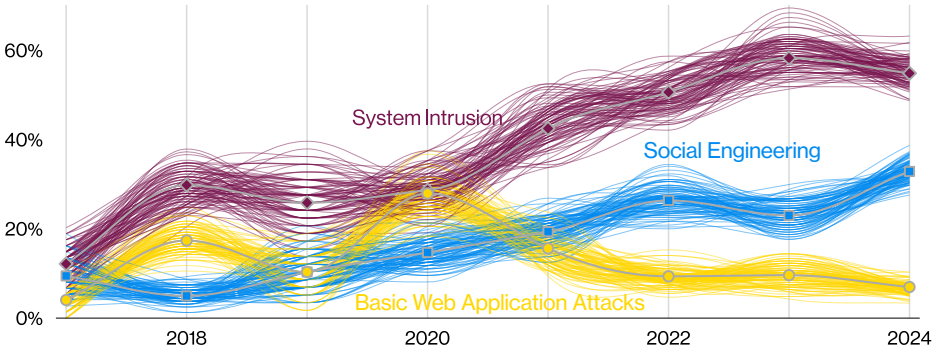


Figure 6. Top patterns over time in Retail industry breaches

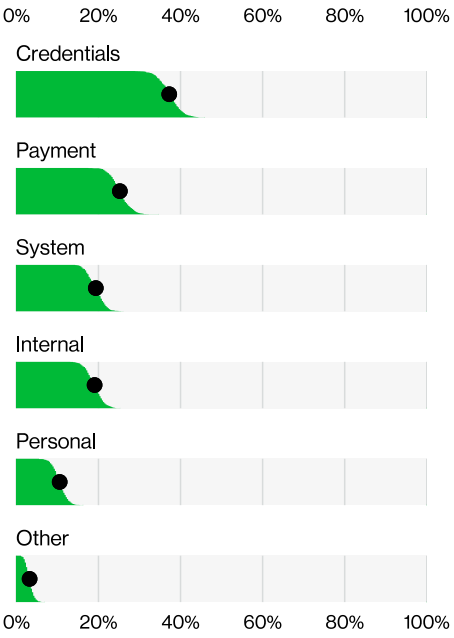


Figure 7. Top Confidentiality data varieties in Retail industry breaches (n=341)

In social-related breaches, Pretexting has emerged triumphant over Phishing as the top social action. It is good to see that the threat actors were required to step up their game to successfully influence their chosen targets. Dare we hope it is because people are becoming better educated and thus able to resist the run-of-the-mill phishing efforts? A suspicious user community is a well-protected user community.

With regard to incidents, Denial of Service continues to represent a serious problem. While these attacks rarely result in confirmed data breaches, they do come with potentially serious disruption of the organization's ability to function. We also saw Ransomware-related incidents continue to decline as they have since 2021.

Stay informed and threat ready.

Facing today's threats requires intelligence from an authoritative source of cybersecurity breach information.

The full DBIR contains details on the actors, actions and patterns that can help you prepare your defenses and educate your organization.

Read the full 2024 DBIR at verizon.com/dbir.

Questions? Comments? Concerns? Love to share cute pet pictures?

Let us know! Send us a note at dbir@verizon.com, find us on LinkedIn, tweet @VerizonBusiness with #dbir. Got a data question? Tweet @VZDBIR!

If your organization aggregates incident or security data and is 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**.

verizon business