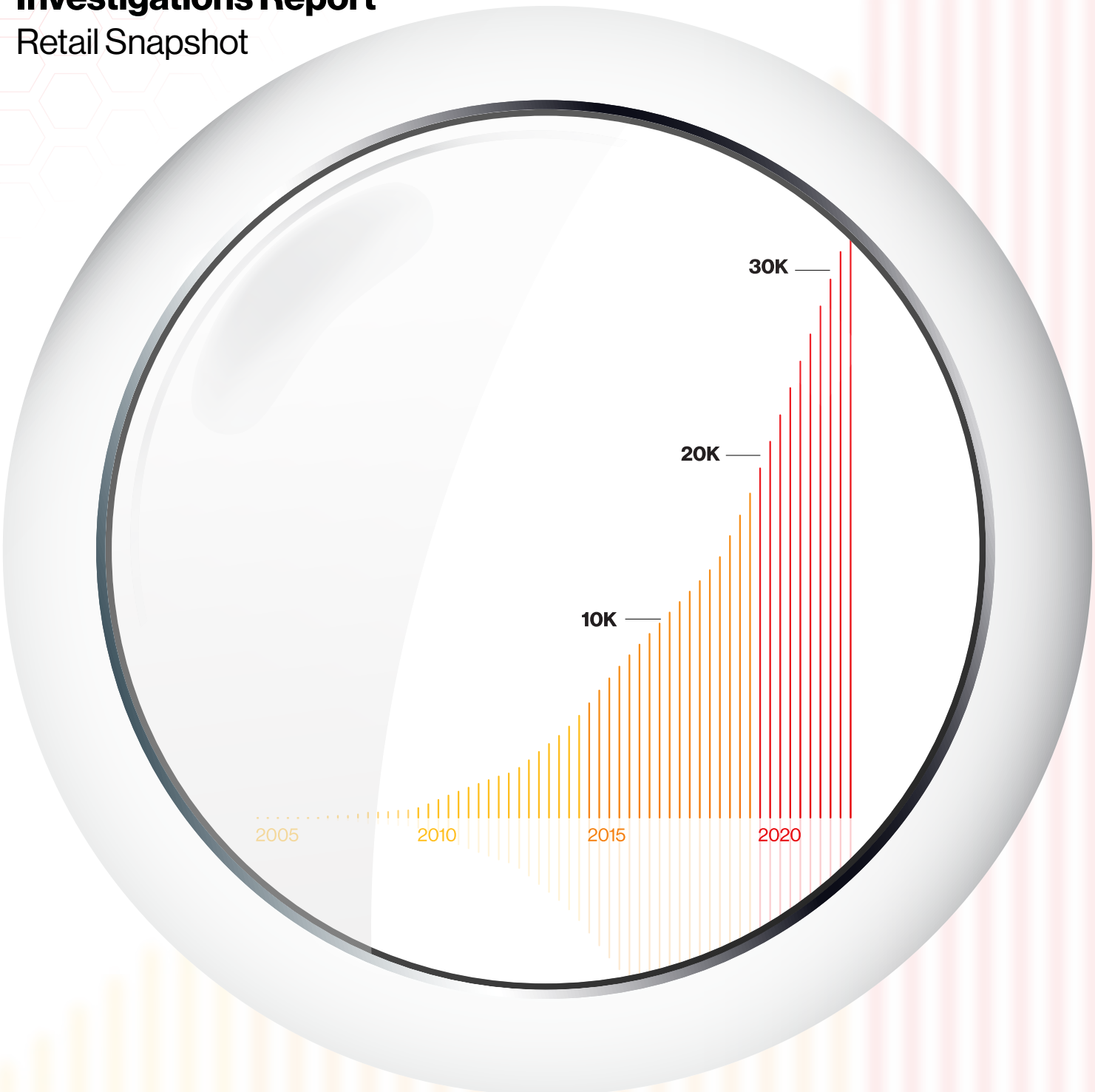
DBIR

2023 Data Breach Investigations Report

Retail Snapshot



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.

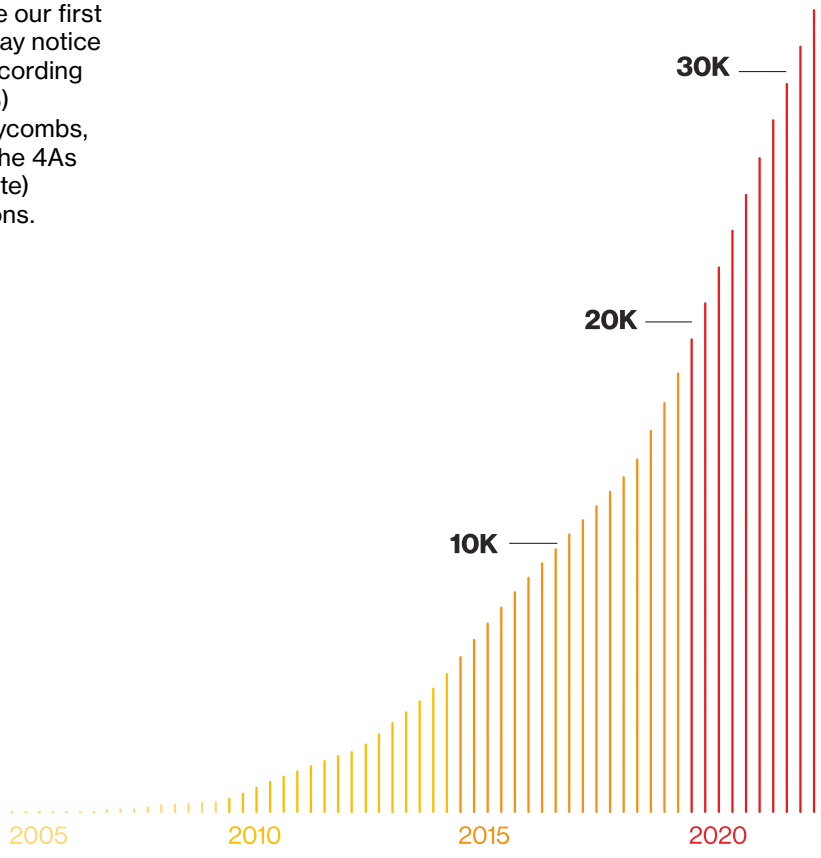


Table of contents

Welcome 4

Summary of findings 5

Incident Classification Patterns 7

Insights for Retail 9

Welcome

Hello, and welcome to the 16th annual installment of 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 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 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.

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

16,312
security incidents investigated

5,199
confirmed breaches

Summary of findings

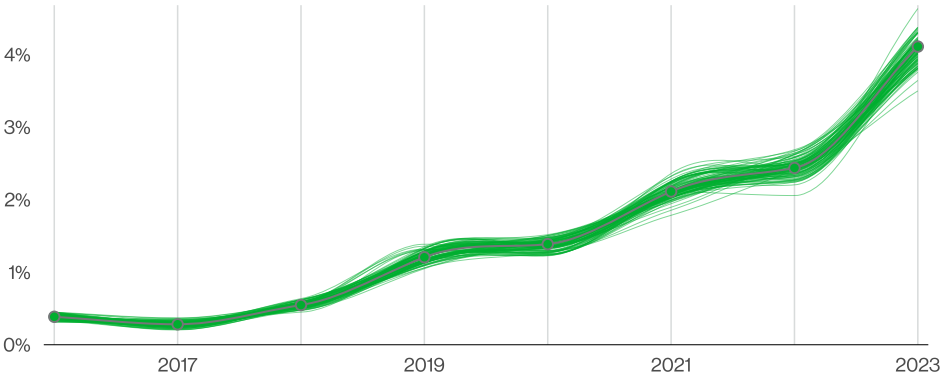


Figure 1. Pretexting incidents over time

Business Email Compromise is a key issue.

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. Perhaps this is 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 1, and now represent more than 50% of incidents within the Social Engineering pattern.

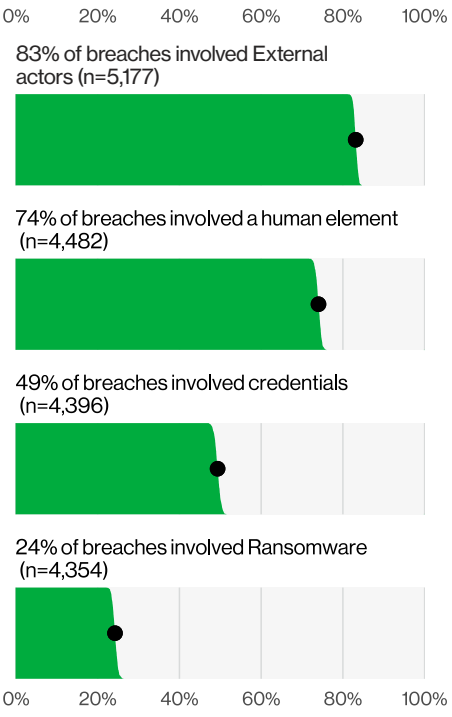


Figure 2. Select key enumerations

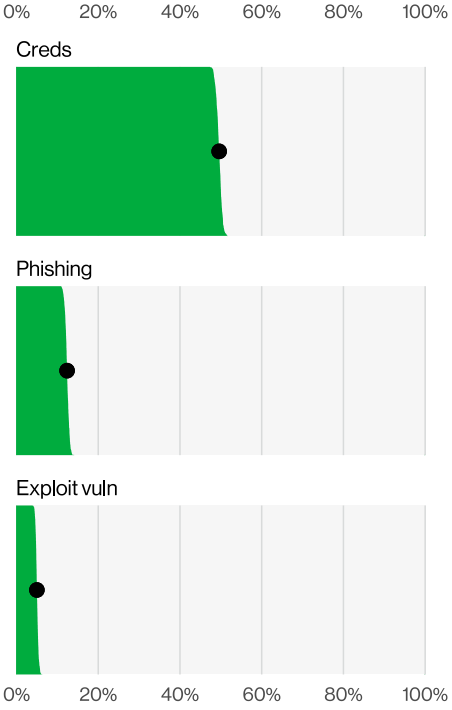


Figure 3. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

The human element risk cannot be understated.

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.

Looking for access on multiple fronts.

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

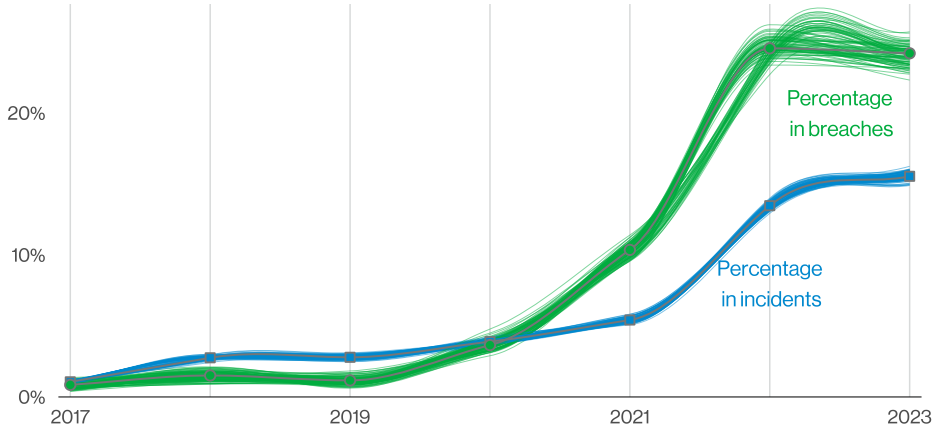


Figure 4. Ransomware action variety over time

Ransomware remains a top action type.

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.

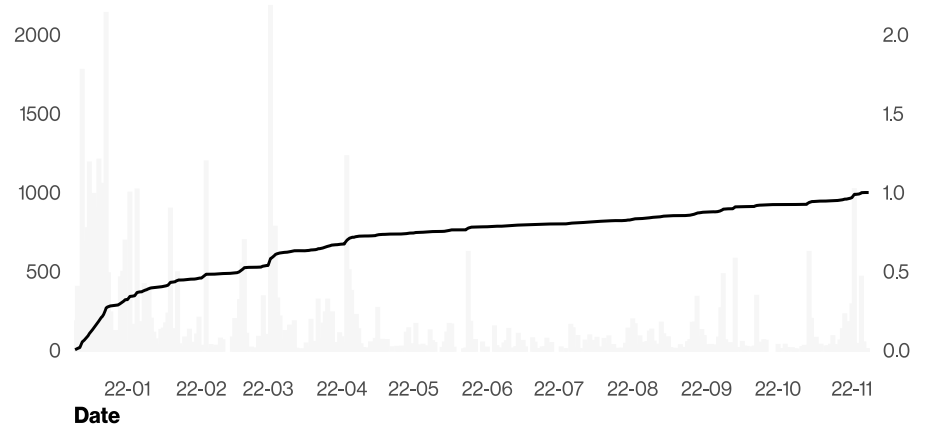


Figure 5. Percentage of Log4j scanning for 2022

The Log4j scanning concentrated near release.

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 6. Percentage of identified Exploit vuln that was Log4j (n=81). Each glyph represents an incident.

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.

Incident Classification Patterns

The DBIR first introduced the Incident Classification Patterns in 2014 as a useful shorthand for scenarios that occurred very frequently. Last year, 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 the objectives. Frequently included in this pattern is the deployment of ransomware.	80% of System Intrusion incidents involved Ransomware as attackers continue to leverage a bevy of different techniques to compromise an organization and monetize their access. • 91% of industries have Ransomware as one of their top varieties of incidents. • 32% of Log4j vulnerability scanning occurred within 30 days of the vulnerability's release. • 97% of breaches were Financially motivated, and 3% were motivated by Espionage. • While only 7% of Ransomware incidents reported losses to the FBI Internet Crime Complaint Center (IC3), the median loss more than doubled from last year to $26,000, with 95% of incidents ranging between $1 and $2.25 million.
Social Engineering	This attack involves the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.	Social Engineering incidents have increased from the previous year largely due to the use of Pretexting, which is commonly used in BEC, almost doubling since last year. • Based on IC3 data, the median amount stolen from these attacks has increased over the last couple of years to $50,000. • Social Engineering accounts for 17% of Breaches and 10% of Incidents.

Basic Web Application Attacks	These attacks are against a web application (as the name implies), and after the initial compromise, they typically do not have a large number of additional Actions. This is the "get in, get the data and get out" pattern.	While representing approximately one-fourth of our dataset, Basic Web Application Attacks breaches and incidents tend to be largely driven by attacks against credentials and then leveraging those stolen credentials to access a variety of resources. • 86% of Basic Web Application Attacks breaches involve the Use of stolen credentials. • 10% of breaches in this pattern involve the Exploitation of a vulnerability.
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 in the Lost and Stolen Assets pattern.	Error-related breaches are down to 9% as opposed to 13% last year. However, this could be due to sample size (715 error incidents and 708 with confirmed data disclosure in last year's data as opposed to 602 incidents, with 513 confirmed breaches this year). • Data compromised included Personal (89%), Medical (19%), Other (10%) and Bank (10%). • Misdelivery (sending something to the wrong recipient) accounts for 43% of breach-related errors. • Publishing errors (showing something to the wrong audience) is in second place at 23%. • Misconfiguration comes in third and accounts for 21% of error-related breaches. • The majority of errors that lead to breaches are committed by Developers and System admins.
Denial of Service	These attacks are intended to compromise the availability of networks and systems, which includes both network and application layer attacks.	The median size of attacks grew 57% from 1.4 gigabits per second (Gbps) last year to 2.2 Gbps this year, and the top size of attacks, the 97.5 percentile, grew 25% from 99 Gbps to 124 Gbps. • A point of attention that some of our partners brought to us was the growth of distributed DNS Water Torture attacks in, you guessed it, shared DNS infrastructure.
Lost and Stolen Assets	Any incident where an information asset went missing, whether through misplacement or malice, is grouped into this pattern.	The loss and theft of mobile phones continues to be an issue across the board. While less data tends to be on these devices, the same cannot be said of laptops, the loss and theft of which increased last year.
Privilege Misuse	Incidents predominantly driven by unapproved or malicious use of legitimate privileges are grouped here.	We are increasingly seeing Privilege Misuse breaches paired with Fraudulent transactions, more so this year than in the past several.

Table 1. Incident Classification Patterns key findings

Insights for 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.

Can you breach me now?

Some people turn to the Retail sector as a form of therapy—and we on the DBIR team probably have more dragons, guitars and cuckoo clocks (don't ask) than we really need. Sadly, criminals have been enjoying their own "retail therapy" by targeting this sector for many years. They continue to do so by capitalizing on this industry's heavy use of payment data.

Top actions/top vectors

When it comes down to how these breaches and incidents occur, it is a roundup of the usual suspects, with both Ransomware and Use of stolen credentials among the top, along with Email and Web applications for vector. However, there is a relatively unique addition to some of these actions—the "Export data" and "Capture app data." This is also one of the few industries where we see "Other" creep up as one of the top actions (Figure 7), and that's largely because there's a variety of secondary actions that actors are using to either deploy their ransomware or find a way to collect payment cards.

If you are in the Retail world and you operate an e-commerce platform, then this section is especially worth paying attention to. Within Retail, we often find the "Magecart"-type actors. These criminals find ways of embedding their malicious code within your site's credit card processing page. This allows them to quietly and subtly abscond with your customers' payment data without actually affecting the functionality of your website. Currently, these attacks represent about 18% of Retail breaches. While we freely admit that we don't always know how these Actors were able to access the web application and upload their bad JavaScript, we have seen them use several different tricks (Figure 8).

Figure 7. Top Action varieties for Retail breaches (n=182)

Stolen credentials: $5. Domain hosting: $12. Malicious JavaScript: $50. Snagging all the fullz: priceless.

Considering the function of this industry, it is hardly surprising to see Payment card data as one of the most common data types breached, accounting for 37% of breaches this year. If you look at Figure 9, you can readily observe that Payment card data has been trending downward since its high-water mark in 2018. However, we are seeing a relatively large increase in Payment card data stolen as compared to last year. Although stealing card data is a tried-and-true method of monetizing data, sometimes the threat actor simply wants a quicker payday. Ransomware has definitely skewed some of the data in this sector, but it seems as if Payment card data is still extremely valuable and will continue to remain a popular target.

This begs the question: Where is this data being stolen from? Because it's difficult to protect something if you don't know what you are protecting. Luckily, we have some data that may help. In our analysis of just payment card breaches in Retail, we found that 70% of breaches originated from Web applications, 17% from Gas terminals and 8% from Point-of-sale servers. This once again illustrates how e-commerce has made it way too easy to get what you want, including stolen credit cards. If you are looking for some added incentive, it's worth mentioning that by the time our 2024 DBIR is published, you should all already be compliant with Payment Card Industry (PCI) Data Security Standard (DSS) 4.0.[1]

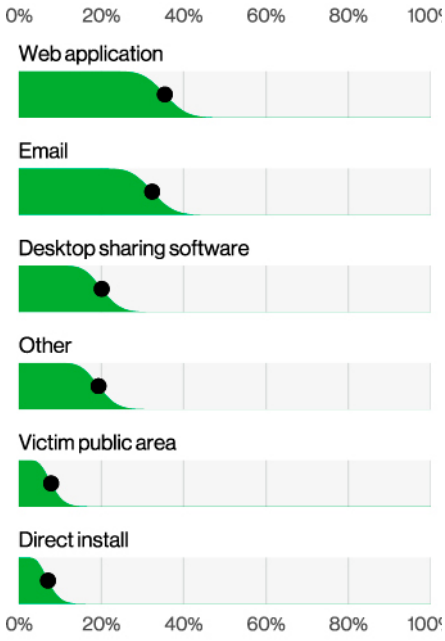


Figure 8. Top Action vectors in Retail breaches (n=130)

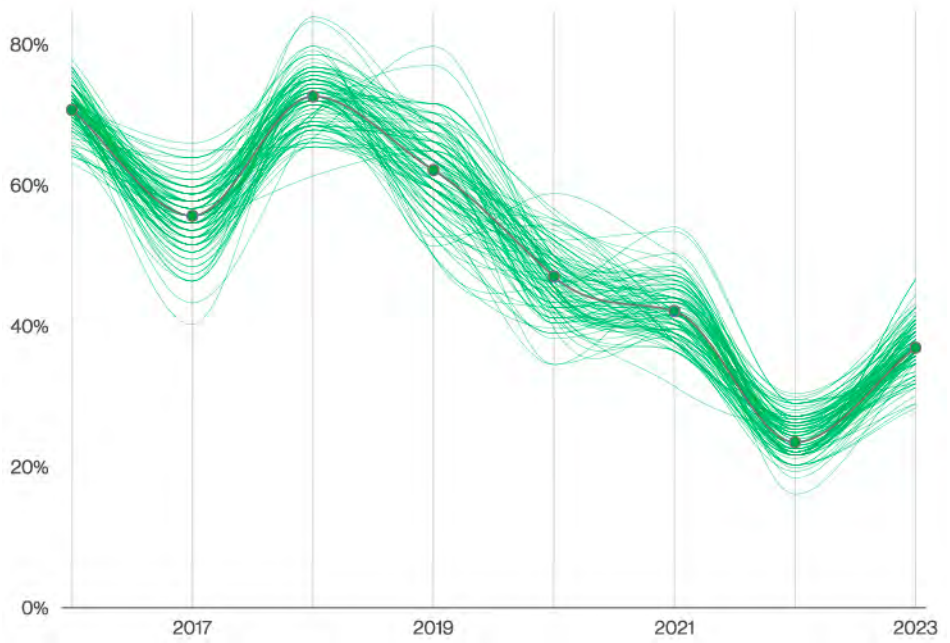


Figure 9. Payment card over time in Retail breaches

1 https://www.pcisecuritystandards.org/resources-overview/

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.

verizon