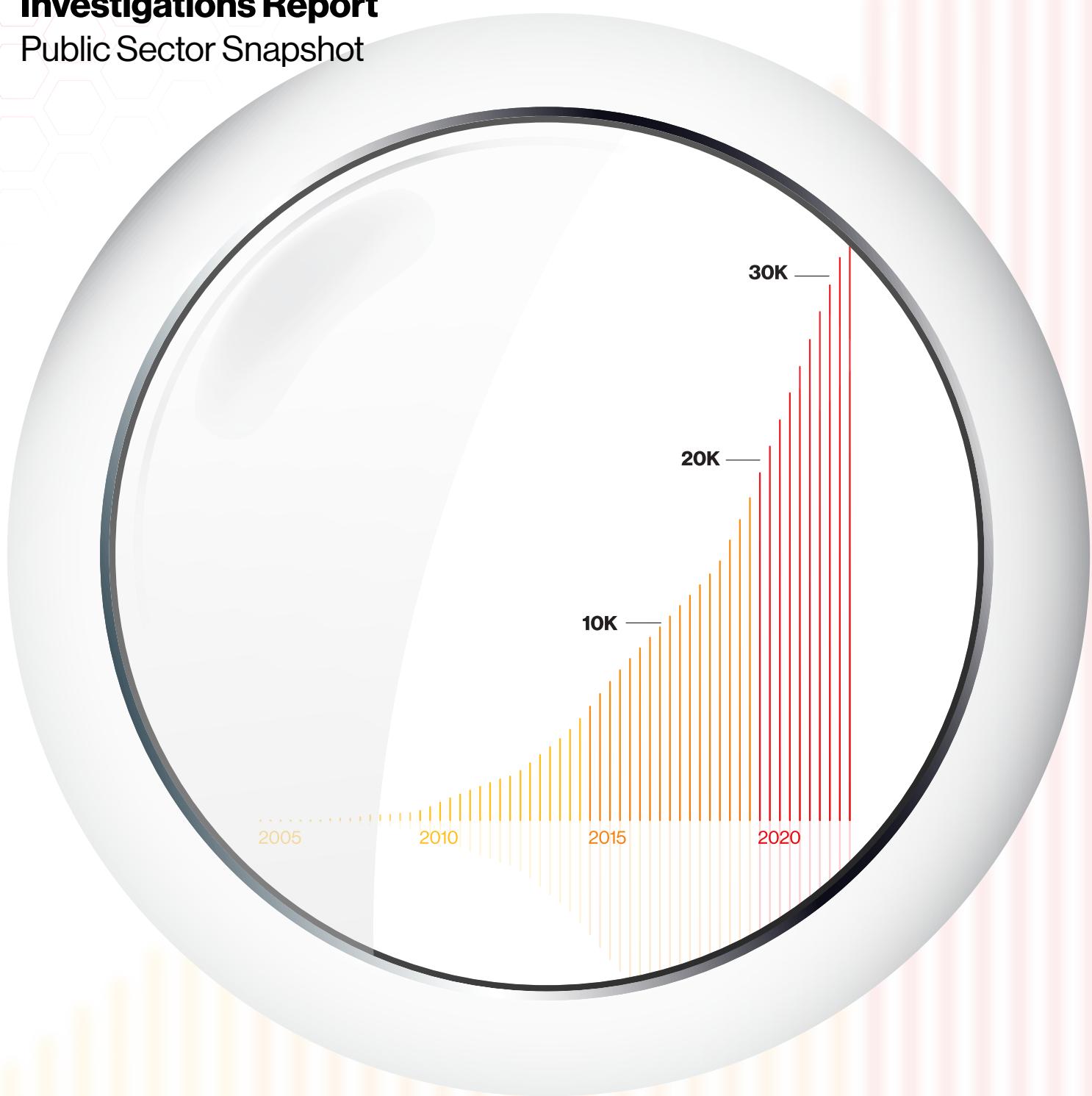


DBIR

2023 Data Breach Investigations Report

Public Sector 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.

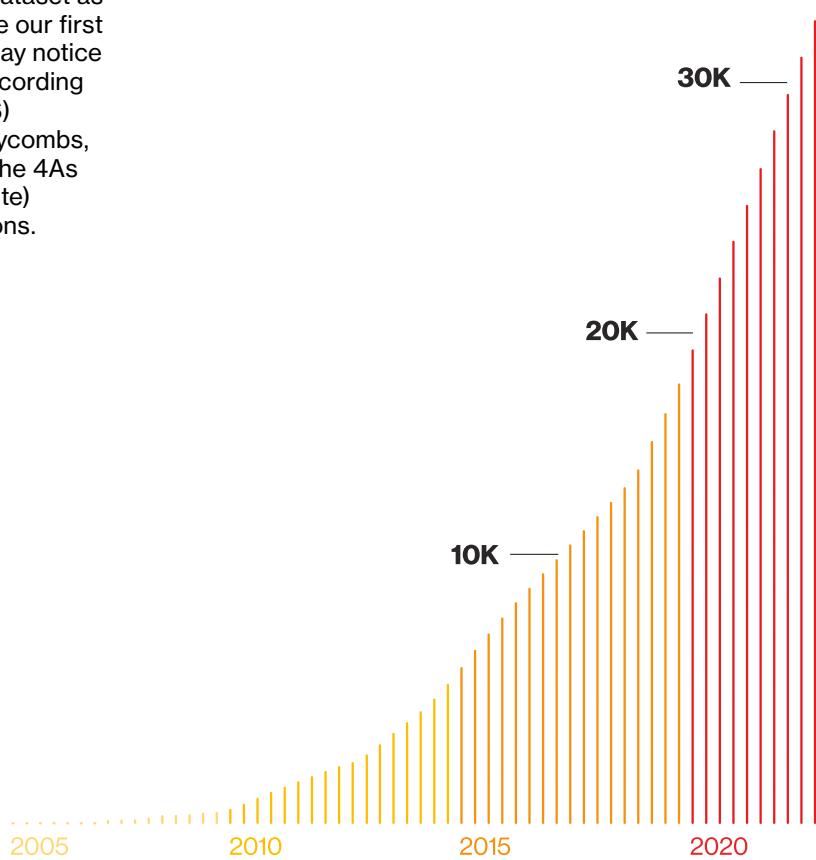


Table of contents

Welcome	4
Summary of findings	5
Incident Classification Patterns	7
Insights for public sector	9

Welcome

Hello, and welcome to the 16th annual installment of the Verizon Data Breach Investigations Report (DBIR) Public Sector 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 Public Administration (NAICS 92) sector, which includes establishments of federal, state and local government agencies as well as public safety agencies.

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 is available here:

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

16,312
security incidents
investigated

5,199
confirmed breaches

Summary of findings

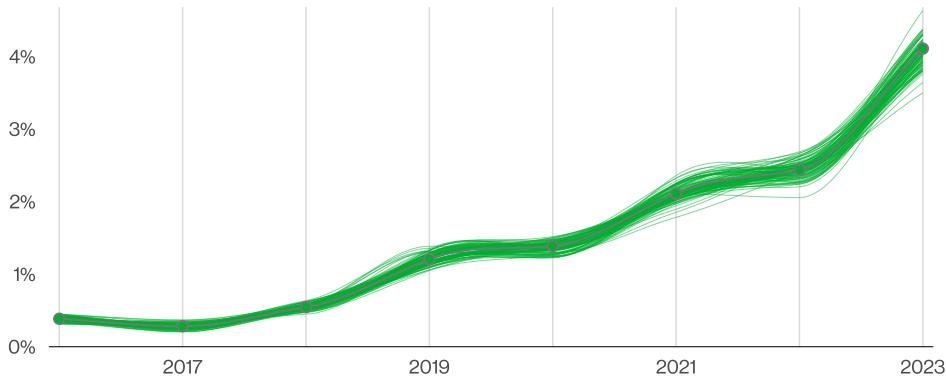


Figure 1. Pretexting incidents over time

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.

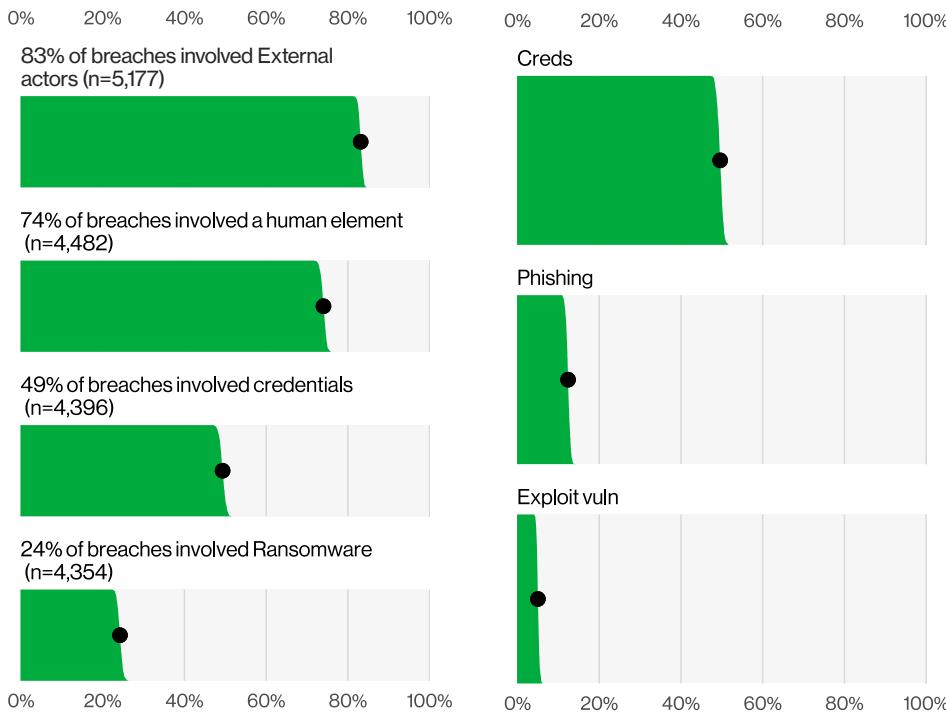


Figure 2. Select key enumerations

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.

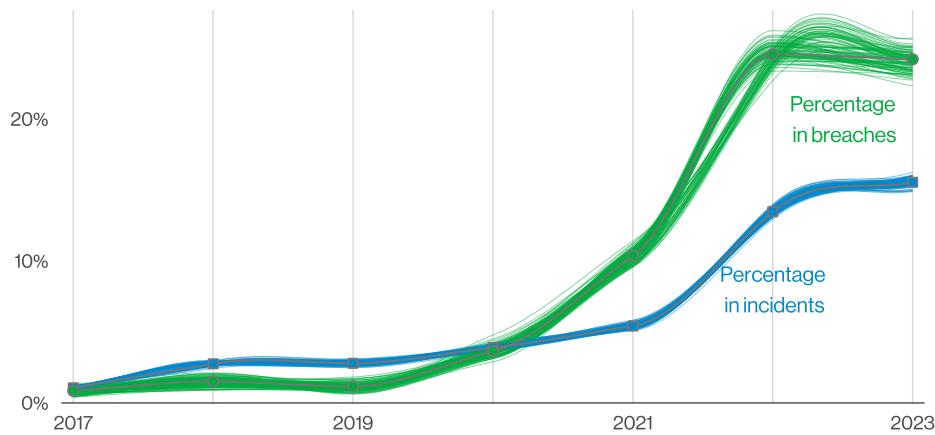


Figure 4. Ransomware action variety over time

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.

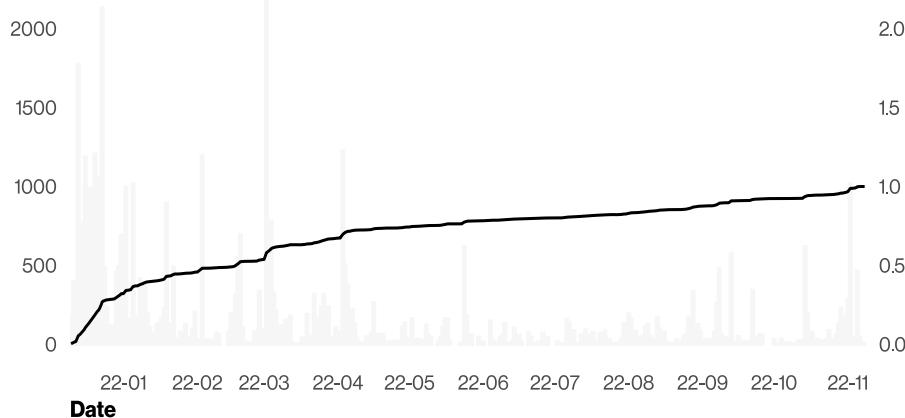


Figure 5. Percentage of Log4j scanning for 2022

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	<p>These are complex attacks that leverage malware and/or hacking to achieve the objectives. Frequently included in this pattern is the deployment of ransomware.</p>	<p>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.</p> <ul style="list-style-type: none">• 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	<p>This attack involves the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.</p>	<p>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.</p> <ul style="list-style-type: none">• 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. <ul style="list-style-type: none"> • 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). <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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 Public Administration

NAICS
G2

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.

That's no moon!

Whether data is stolen by stealthy “weather research” balloons (death stars) floating overhead or by more conventional methods such as phishing, external threat actors are diligently gaining access to data in the public sector. Mind you, when we created VERIS to allow us to categorize breaches, we didn’t expect to see it applied to UFOs being shot out of the sky. But, until it becomes a trend, we will simply tag it as Physical - Other and call it a day for now.

The System Intrusion pattern remains high in this sector. Some intrusions are stuff that movies are made of—complex attacks against a challenging target, where the stakes are high for entire economic systems.¹ We did see an increase in the Espionage-motivated actors in this pattern this year. In fact, this sector is one where the Espionage-motivated actor is consistently among the highest.

Within the System Intrusion pattern, we saw a slight decrease in Ransomware as a tactic. This doesn’t mean you should ignore it, however, as it remains a favored method of disrupting government workings while generating income for the adversaries.

While it is possible to reach their goals by themselves, these actors are not opposed to recruiting help from within the organization. We see evidence of collusion (multiple actors working in concert) in 16% of Public Administration breaches this year. That is significant, given that we didn’t see multiple Actor breaches the past two years in this sector, and in 2020’s report, it was only at 2%.

What's worse than quiet quitting?

This brings us to the point that internal actor Misuse continues to be a consistent problem in this sector. While prevalent, it is not increasing, so that is at least some good news. In fact, Misuse peaked in 2019 (of the past five years) and has decreased somewhat since then. However, the pairing of the unhappy employee with a motivated external adversary shows the continued need for detective controls. If you can catch this kind of Internal actor-facilitated attack in its early stages, you can mitigate the damage significantly.

We see evidence of collusion (multiple actors working in concert) in 16% of Public Administration breaches this year. That is significant, given that we didn’t see multiple Actor breaches the past two years in this sector, and in 2020’s report, it was only at 2%.

¹ There are explosions and car chases in there too, we’re sure of it.

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](https://twitter.com/VZDBIR) to provide feedback for improving the DBIR. Learn more about the VERIS Framework at verisframework.org.

