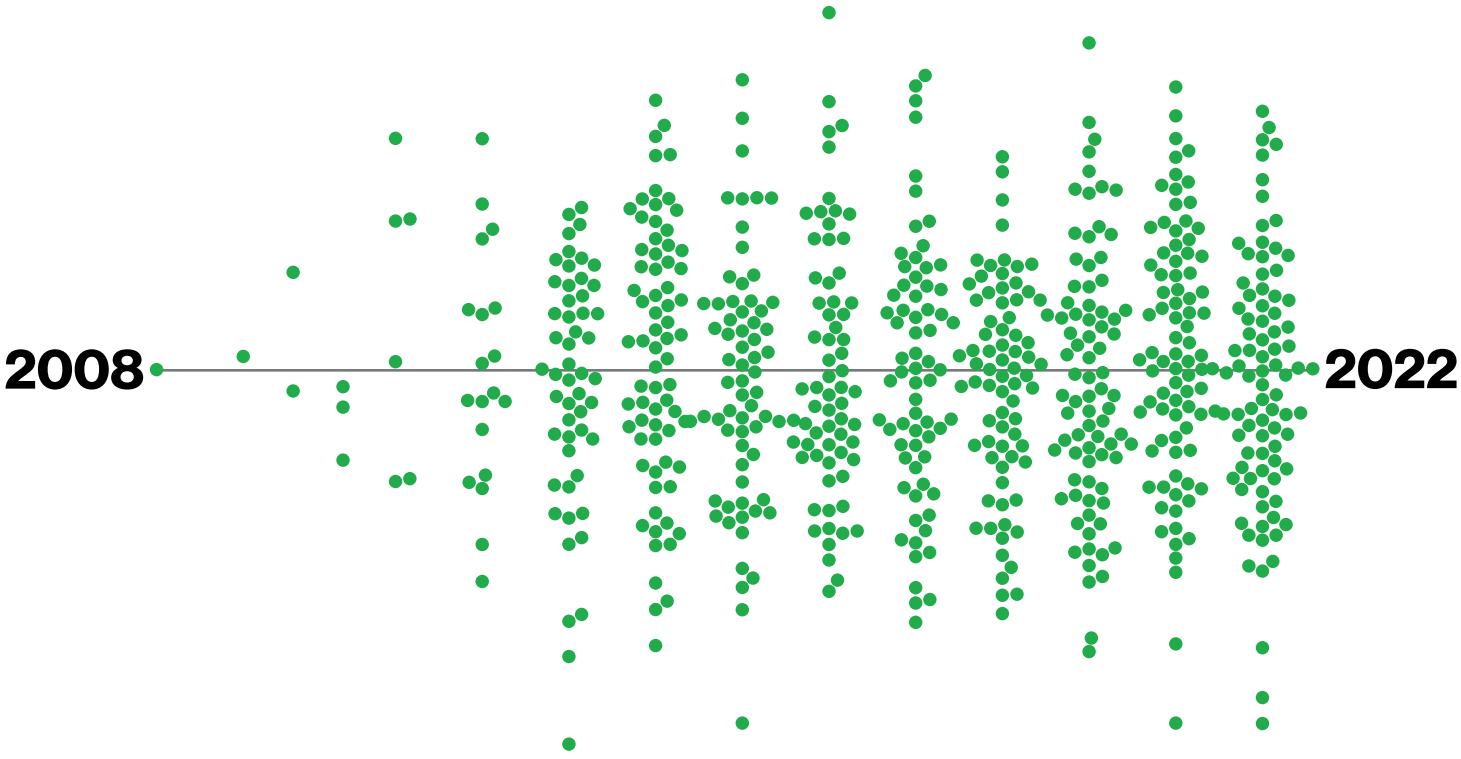
DBIR

2022 Data Breach Investigations Report

Small Business snapshot



About the cover

Our long-time readers may recall that the cover for our inaugural report back in 2008 depicted an empty chair in a server room. It was intended to convey the fact that many organizations are not properly minding their assets and data. The 2022 cover is a throwback to that report, both for purposes of nostalgia and to convey that many organizations continue to struggle with keeping an eye on their people and their systems. The overlay of the timeline with the dot plot illustrates the number of global contributors that have joined us over the 15-year history of the report (broken out by year).

Table of contents

Another year, another detailed look at the threat landscape

Welcome to the 15th annual Verizon Data Breach Investigations Report (DBIR). It is truly hard to believe that it has been 15 years since our inaugural installment of this document. Thank you to our contributors for your continued willingness to share your data, insight and vast experience in a selfless effort to improve this industry.

The past year has been extraordinary in a number of ways, but it was certainly memorable with regard to the murky world of cybercrime. From very well-publicized critical infrastructure attacks to massive supply chain breaches, the financially motivated criminals and nefarious Nation-state actors have rarely, if ever, come out swinging the way they did over the past 12 months.

As in past years, we will examine what our data has to tell us about these and other common action types used against enterprises. This year, we looked at 23,896 incidents, 5,212 of which were confirmed breaches. This data represents actual real-world breaches and incidents investigated by the Verizon Threat Research Advisory Center (VTRAC) or provided to us by our 87 global contributors, without whose generous help this document could not be produced. We hope that 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 protect your organization and its assets.

Read on for report highlights related to very small businesses, please pass this summary along to colleagues and download the full report at **verizon.com/dbir** for a more detailed view of the threat landscape in 2022.

23,896

The DBIR team analyzed 23,896 incidents, of which 5,212 were confirmed breaches.

Industry labels

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 Financial (52) is not indicative of 52 as a value. "52" is the code for the Finance and Insurance sector. The overall label of "Financial" is used for brevity within the figures. Detailed information on the codes and the classification system are available here:

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

Summary of findings

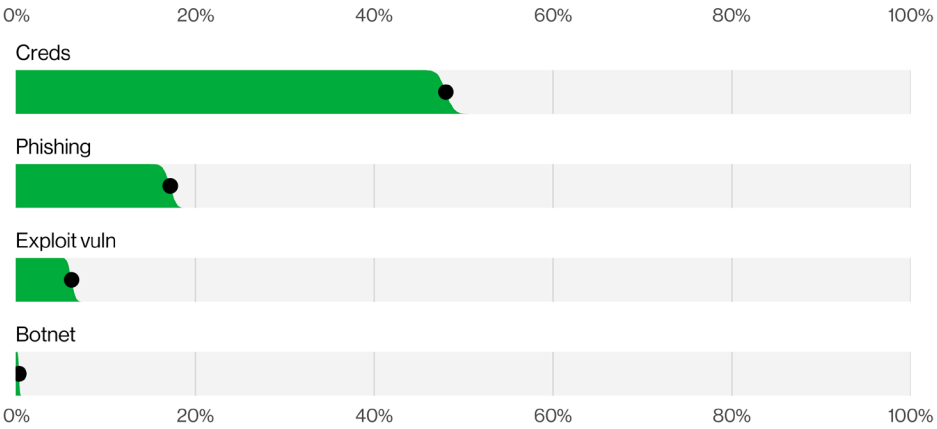


Figure 1. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

There are four key paths leading to your estate: Credentials, Phishing, Exploit vulnerabilities and Botnets. These four pervade all areas of the DBIR, and no organization is safe without a plan to handle them all.

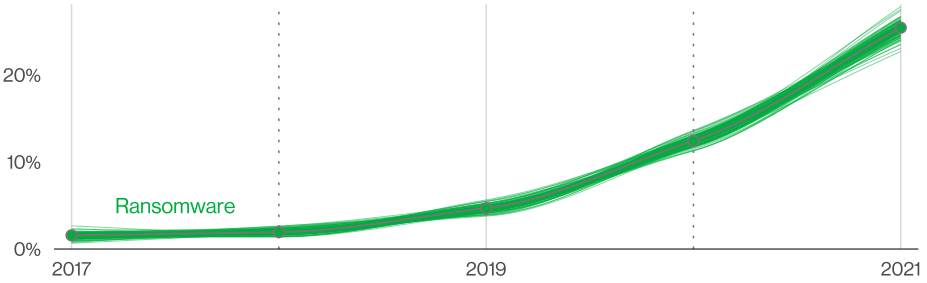


Figure 2. Ransomware over time in breaches

This year, Ransomware has continued its upward trend with an almost 13% increase (for a total of 25% of breaches)—a rise as big as the last five years combined. It's important to remember, ransomware by itself is really just a model of monetizing an organization's access. Blocking the four key paths helps to block Ransomware.

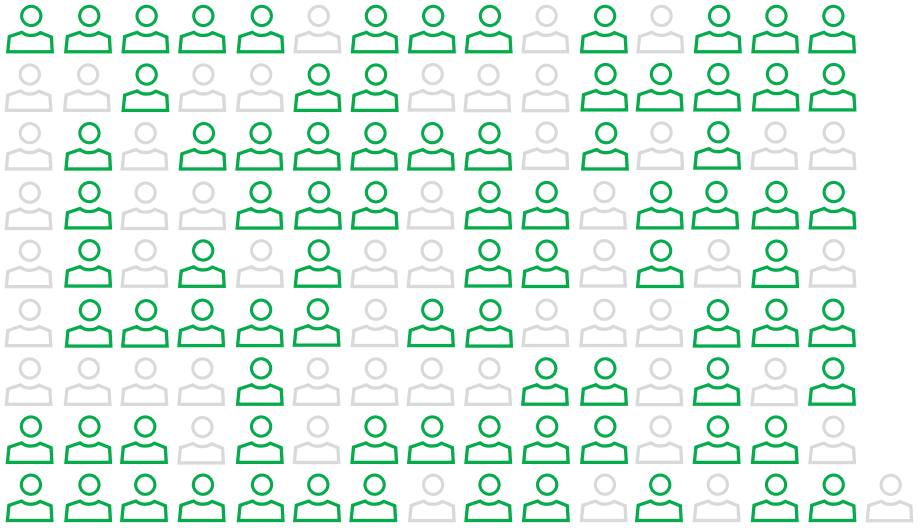


Figure 3. Partner vector in Systems Intrusion incidents (n=3,403)
Each glyph represents 25 incidents.

2021 illustrated how one key supply chain breach can lead to wide-ranging consequences. Compromising the right partner is a force multiplier for threat actors. Unlike a financially motivated actor, Nation-state threat actors may skip the breach and keep the access.

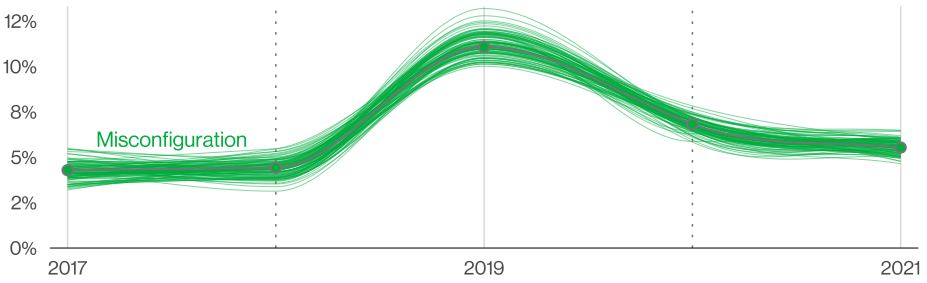


Figure 4. Misconfiguration over time in breaches

Error continues to be a dominant trend, and is heavily influenced by misconfigured cloud storage. While this is the second year in a row that we have seen a slight leveling out for this pattern, the fallibility of employees should not be discounted.

Figure 5. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

The human element continues to drive breaches. This year, 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing or simply an Error, people continue to play a large part in incidents and breaches alike.

Incident Classification Patterns

The DBIR dataset is very large and, at times, extremely complex. It captures many different types of data points, and it grows larger each year. In order to create an easier way to analyze the ever-growing mountain of data and, even more importantly, to assist us in communicating our findings to our readers, we began using "Patterns" in our 2014 report.

The patterns are essentially clusters of "like" incidents. Starting in 2014, and for several subsequent years, there were nine patterns. Last year, we found that due to changes in attack type and the threat landscape, the data was leading us toward revamping, combining and generally overhauling those patterns. Therefore, starting with the 2021 report, we moved from the original nine patterns down to the eight you see in this report. The eight patterns, and how they are defined, can be found below. Please be sure to peruse the way we define the different patterns, as we will refer to them throughout the report.

Social Engineering	Psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality	• Fifty-nine percent of Social Engineering breaches compromised creds, and 31% used stolen credentials. Credential compromise was three times more likely in Social Engineering breaches than in the rest of the patterns • Phishing is more than two times as likely as Pretexting in the Social Engineering pattern • A Financial motive is eight times more common than an Espionage motive in Social Engineering breaches
Basic Web Application Attacks (BWAA)	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.	• Four out of every five web app attacks involved stolen creds. This finding underlies the importance of password safeguards • Espionage is four times more likely in BWAA breaches than in the rest of the patterns, indicating that Nation-states don't necessarily have to pursue complex attacks when they're able to leverage established and effective attacks to achieve their objectives • Use of stolen credentials is six times more likely than exploiting a vulnerability in BWAA breaches
System Intrusion	Complex attacks that leverage malware and/or hacking to achieve the objectives, including deploying Ransomware	• System Intrusion consists of more complex breaches and attacks that leverage a combination of several different Actions, such as various Hacking actions along with Malware actions • Ninety-two percent of System Intrusion breaches are financially motivated • Use of stolen credentials is four times more likely than Exploiting vulnerabilities in System Intrusion breaches

Miscellaneous Errors	Incidents where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which are grouped with theft instead.	• Miscellaneous Errors largely consist of servers being misconfigured and accidentally exposed to the internet, or Misdelivery actions in which users send emails to the wrong recipient, and represents 13% of total breaches • External cloud assets have decreased 83% since last year in Miscellaneous Errors breaches, potentially indicating a shift in technologies leveraging a secure-by-default approach • Eighty-five percent of Miscellaneous Error breaches involved servers
Privilege Misuse	Incidents predominantly driven by unapproved or malicious use of legitimate privileges	• Documents are three times more likely in Privilege Misuse than in the rest of the patterns
Lost and Stolen Assets (L&SA)	Any incident where an information asset went missing, whether through misplacement or malice	• Unaffiliated actors are 14 times more likely in L&SA incidents than in the rest of the patterns
Denial of Service	Attacks intended to compromise the availability of networks and systems. This includes both network- and application-layer attacks.	• Denial of Service incidents are two times more common in large organizations than the rest of the patterns

Key takeaways

Attacks on all fronts

There are four key paths leading to your estate: Credentials, Phishing, Exploit vulnerabilities and Botnets. All four pervade all areas of the DBIR, and no organization is safe without a way to handle them all.

Ransomware remains a key issue.

Ransomware has increased 13% in breaches, greater than the last five years combined. Ransomware has provided actors with a potential way to monetize access to a wider range of victims than was possible in the past.

Keep your supply chain close ...

2021 illustrated how one key supply chain breach can lead to wide-ranging consequences. Compromising the right partner is a force multiplier for threat actors.

And your partners even closer.

Unlike a Financially motivated actor, Nation-state threat actors may skip the breach and keep the access to leverage it at a future (and possibly more critical) date. Partners accounted for the vector in 62% of incidents discussed in the System Intrusion pattern—although this was mostly due to a single supply chain breach.

Errors are still a concern.

Error continues to be a dominant trend and is heavily driven by misconfigured cloud storage. While this is the second year in a row that we have seen a slight leveling out for this pattern, the fallibility of employees should not be discounted. Breaches due to Misconfiguration errors appear to have peaked in 2019 at 11% of breaches, while they represent 6% of breaches currently.

Social attackers target the human element.

The Human Element was involved in 82% of breaches, and consists of Social attacks, Error and Misuse, but Social attacks such as Phishing and Pretexting were responsible for the majority.

Very Small Businesses

Frequency	832 incidents, 130 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Privilege Misuse represent 98% of breaches.
Threat actors	External (69%), Internal (34%), Multiple (3%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Credentials (93%), Internal (4%), Bank (2%), Personal (2%) (breaches)

When cybercrime makes the news, it is typically because a large organization has fallen victim to an attack. However, contrary to what many may think, very small organizations are just as enticing to criminals as large ones, and, in certain ways, maybe even more so.

Threat actors have the "we'll take anything we can get" philosophy when it comes to cybercrime. These incidents can and have put small companies out of business. Therefore, it is crucial that even very small businesses (10 or fewer employees) should take precautions to avoid becoming a target.

Large organizations have large resources, which means they can afford Information Security professionals and cutting-edge technology to defend themselves. Very small businesses, on the other hand, have very limited resources and cannot rely on a trained staff. That is why we wrote this section.

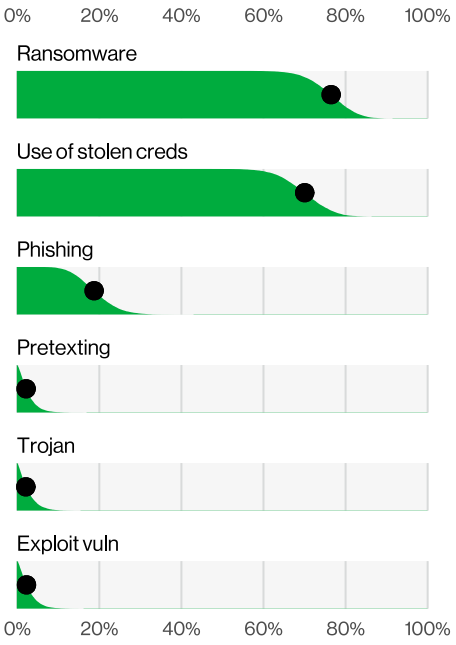


Figure 6. Action varieties in 1-to-10-employee organization breaches (n=61)

Very Small Business Cybercrime Protection Sheet

What are the most common threats facing my business?

The #1 action type in our dataset for very small businesses is ransomware attacks. Ransomware is a type of malicious software that encrypts your data so that you cannot view or utilize it, and once the ransomware is triggered, the threat actor demands a (frequently large) payment to unencrypt it. This is where having those offline[1] backups comes in handy.

The second most common is the Use of stolen credentials. Attackers can get your credentials (username and password) via many different methods: brute-force attacks (where attackers use automation to try numerous combinations of letters, symbols and numbers to guess your credentials), various types of malware (thus the value of having an up-to-date antivirus), reused passwords from another site that has been hacked and, last but not least, social attacks such as Phishing and Pretexting.[2]

You may have heard the term "Business Email Compromise" in news articles. They typically involve Phishing and/or Pretexting, and can be quite convincing, such as an invoice that looks like it comes from a known supplier but has a different payment account, or an email from a business partner saying they're in a pinch and need a quick payment made on their behalf. While most come in through email, criminals have also employed the telephone to convince their target that this is a legitimate request. The criminal element often run their enterprise just like a legitimate business and may even take advantage of criminal call centers (yes, these exist) to help lend credence to their ploy.

Pretexting is the human equivalent of Phishing. Typically, the threat actor attempts to create a dialog with the victim by impersonating a business partner, a bank employee or a superior in your own organization in order to gain access to login information. The end game for Pretexting is usually the automated transfer of funds from your organization to the criminal's bank account.

How do I know I have become a victim?

Watch for anything strange or out of the ordinary. For example, you might see unexpected charges on your bank statement or phone bill. Keep an eye out for transactions on your credit card that you don't recognize. You may receive comments from friends about emailed requests for them to buy a gift card. You may receive phone calls asking for your password or credit card number, or a request to change the account number or how you pay a regular vendor or client. All of these things are warning signs that something malicious might be happening. Think of your computer like a car—if it suddenly won't start, runs slower or makes a weird noise, it's time to have an expert take a look. Finally, with threats such as ransomware, the threat actor will actually alert you that your data has been encrypted.

1 If you're unsure what "offline" means here, see "What to do to avoid becoming a target" below.
2 If you're not familiar with "phishing" or "pretexting," it's okay. Keep reading for the definitions.

Whom do I contact if I learn I have been a victim of cybercrime?

- A large range of resources for many different situations is available through https://fightcybercrime.org/. This website provides information on where to go and what to do in the event of a cyber incident
- Scam Spotter provides simple, easy-to-understand information about how to recognize common scams: https://scamspotter.org/
- If you are in the United States, your state's attorney general's office website may have resources for you as well

Familiarize yourself with these resources and draw up a plan for what steps you will take if you find your organization has become a victim. Plan this ahead of time instead of waiting until your company's "hair is on fire." Even if it is just a document that contains the contact information for all of your vendors and your bank's fraud department, it is a place to start. Print it off and post it somewhere you can access it easily. Don't just keep it on your computer—it might be unavailable as part of the attack.

Some planning on your part, along with a bit of educating the people most likely to encounter these kinds of attacks, can go a long way in helping to make your small company safer.

What to do to avoid becoming a target

1. Use two-factor authentication[3]
2. Do not reuse or share passwords[4]
3. Use a password keeper/generator app
4. Be sure to change the default credentials of the point-of-sale (PoS) controller or other hardware/software
5. Ensure that you install software updates promptly so that vulnerabilities can be patched
6. Work with your vendors to be sure that you are as secure as you can be, and that they are following these same basic guidelines
7. Keep a consistent schedule with regard to backups and be sure to maintain offline backups—meaning that they are not on a device connected to a computer
8. Ensure that the built-in firewall is switched on for user devices such as laptops and desktops ("on" may not be the default)
9. Use antivirus software, for all your devices. Smartphones, tablets and credit card swipers are just as important as laptops and computers. It won't catch everything, but it will help
10. Do not click on anything in an unsolicited email or text message
11. Set up an out-of-band method for verifying unusual requests for data or payments
12. Make sure the computer used for financial transactions is not used for other purposes, such as social media or email
13. Use email services that incorporate phishing and pretexting defenses and use a web browser that warns you when a website may be spoofed

3 This adds an additional layer to just the username and password combination. It may be a code that is texted to your registered cell phone, the use of an authenticator app like Google or Microsoft Authenticator, or the use of a little device that you plug into a USB drive when prompted. If your vendors do not offer two-factor authentication (also called multifactor authentication, or MFA), start lobbying for them to accommodate it.

4 Not between people and not between applications or websites. A password keeper makes this easier.

Stay informed and threat ready.

Successfully navigating through the cyberthreats facing very small businesses today requires intelligence from a source you can trust. The full DBIR contains real-world details on the actors, actions and patterns that can help you to prepare your defenses and educate employees. Get the data-based insights you need to protect your organization.

Read the full 2022 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. Become a contributor to next year's report or provide us feedback for improving the DBIR at dbir@verizon.com, tweet us @VZDBIR and check out the VERIS GitHub page: https://github.com/vz-risk/veris.

verizon