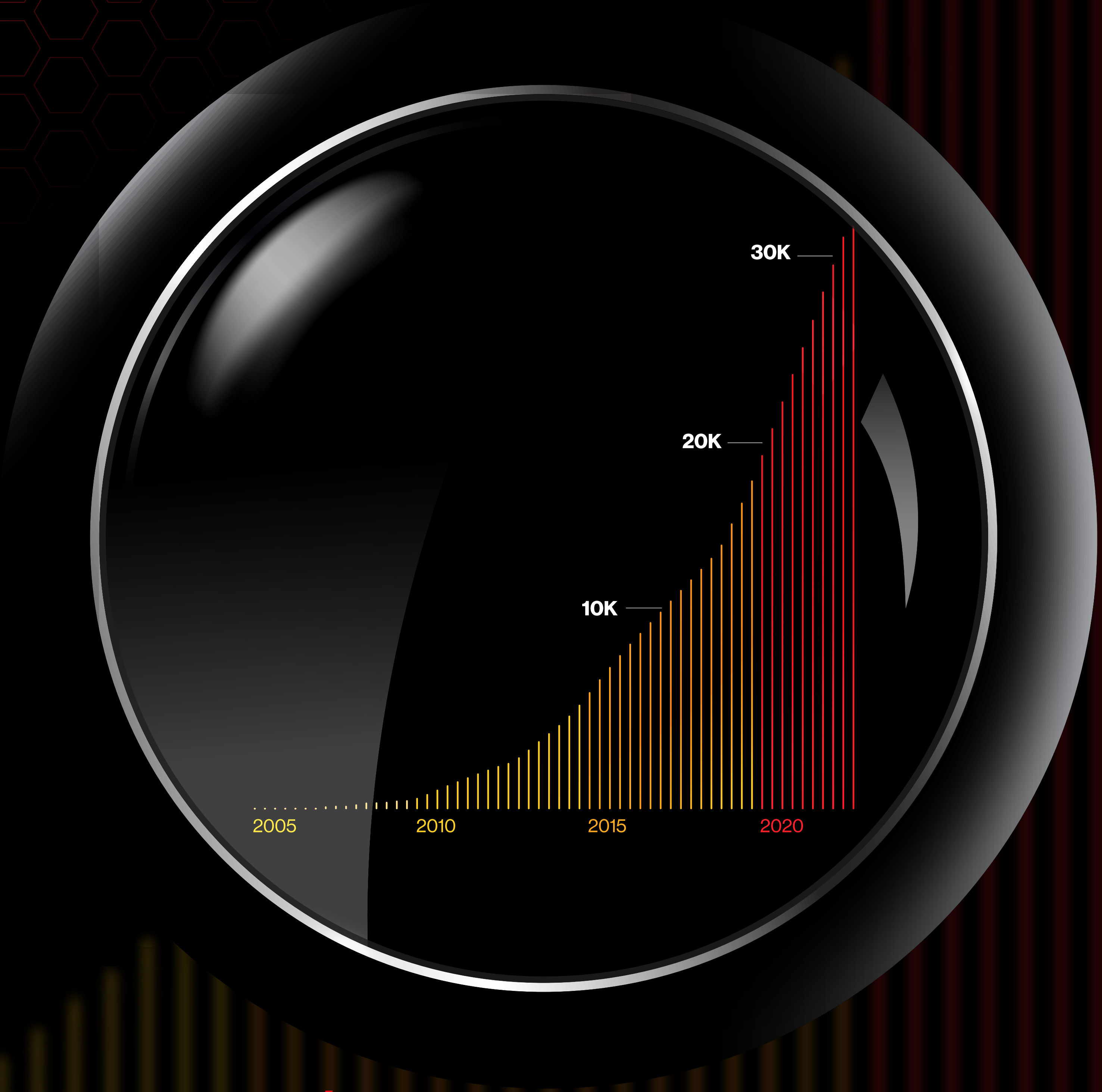
DBIR

2023 Data Breach Investigations Report


30K
20K
10K
2005
2010
2015
2020

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.

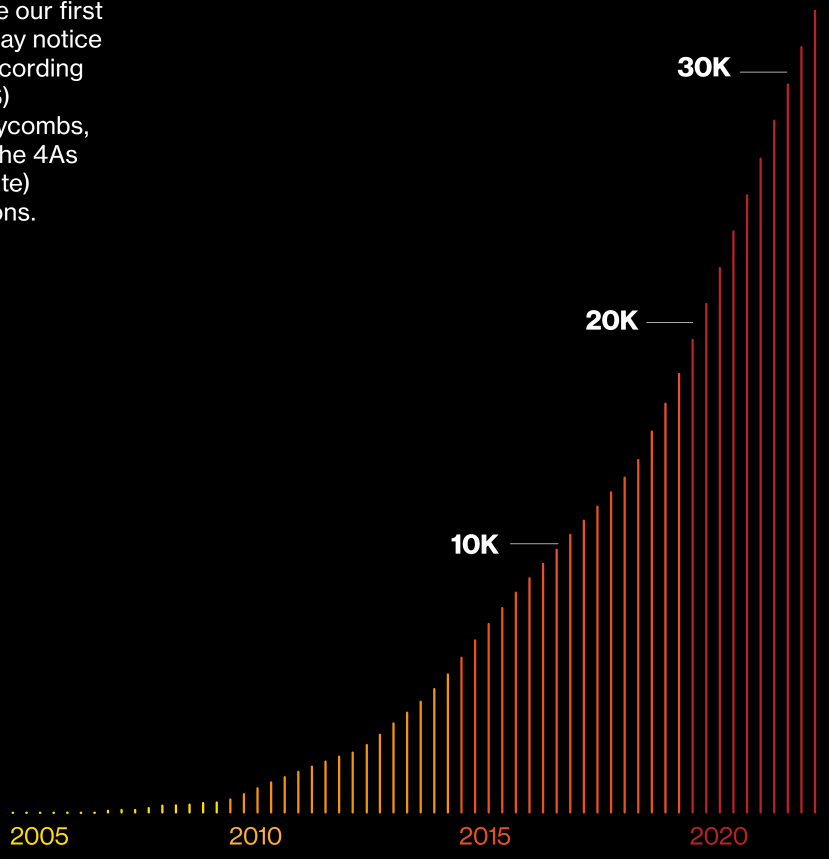


Table of contents

1

Helpful definitions and chart guidance 4
Introduction 7
Summary of findings 8

2

Results and analysis

Introduction 11
Actors 12
Actions 14
Assets 17
Attributes 19

3

Incident Classification Patterns

Introduction 22
System Intrusion 24
Social Engineering 31
Basic Web Application Attacks 35
Miscellaneous Errors 40
Denial of Service 42
Lost and Stolen Assets 44
Privilege Misuse 46

4

Industries

Introduction 49
Accommodation and Food Services 53
Educational Services 54
Financial and Insurance 55
Healthcare 56
Information 57
Manufacturing 58
Mining, Quarrying, and Oil & Gas Extraction + Utilities 59
Professional, Scientific and Technical Services 61
Public Administration 62
Retail 63

Small and medium business 65

5

Regions

Introduction 70

6

Wrap-up

Year in review 74

7

Appendices

Appendix A: Methodology 79
Appendix B: VERIS mappings to MITRE ATT&CK® 83
Appendix C: VTRAC 20-year retrospective 84
Appendix D: Contributing organizations 85

Helpful definitions and chart guidance

Hello, and welcome first-time readers! Before you get started on the 2023 Data Breach Investigations Report (DBIR), it might be a good idea to take a look at this section first. (For those of you who are familiar with the report, please feel free to jump over to the introduction.) We have been doing this report for a while now, and we appreciate that the verbiage we use can be a bit obtuse at times. We use very deliberate naming conventions, terms and definitions and spend a lot of time making sure we are consistent throughout the report. Hopefully this section will help make all of those more familiar.

VERIS Framework resources

The terms "threat actions," "threat actors" and "varieties" will be referenced often. These are part of the Vocabulary for Event Recording and Incident Sharing (VERIS), a framework designed to allow for a consistent, unequivocal collection of security incident details. Here is how they should be interpreted:

Threat actor: Who is behind the event? This could be the external "bad guy" that launches a phishing campaign or an employee who leaves sensitive documents in their seat back pocket.

Threat action: What tactics (actions) were used to affect an asset? VERIS uses seven primary categories of threat actions: Malware, Hacking, Social, Misuse, Physical, Error and Environmental. Examples at a high level include hacking a server, installing malware or influencing human behavior through a social attack.

Variety: More specific enumerations of higher-level categories—e.g., classifying the external "bad guy" as an organized criminal group[1] or recording a hacking action as SQL injection or brute force.

Learn more here:

- **https://github.com/vz-risk/dbir/tree/gh-pages/2023**—includes DBIR facts, figures and figure data
- **https://verisframework.org**—features information on the framework with examples and enumeration listings
- **https://github.com/vz-risk/veris**—features information on the framework with examples and enumeration listings

Incident vs. breach

We talk a lot about incidents and breaches and we use the following definitions:

Incident: A security event that compromises the integrity, confidentiality or availability of an information asset.

Breach: An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party. A Distributed Denial of Service (DDoS) attack, for instance, is most often an incident rather than a breach, since no data is exfiltrated. That doesn't make it any less serious.

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 NAICS code for the Financial and Insurance sector. The overall label of "Financial" is used for brevity within the figures. Detailed information on the codes and the classification system is available here:

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

---

[1] By organized criminal group, we mean a group that does this for a living and has a set process they use repeatedly, not Tony Soprano and his band of merry men.

I'm sorry, this all happened when?

While we have always listed the following facts in our Methodology section (because that is where this type of information belongs), we decided to also mention it here for the benefit of those who don't make it that far into the report. 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 report took place between November 1, 2021, and October 31, 2022.** The 2022 caseload is the primary analytical focus of the 2023 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 this 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. Rome wasn't built in a day, and neither is the DBIR.

Being confident of our data

Starting in 2019 with slanted bar charts, the DBIR has tried to make the point that the only certain thing about information security is that nothing is certain. Even with all the data we have, we'll never know anything with absolute certainty. However, instead of throwing our hands up and complaining that it is impossible to measure anything in a data-poor environment or, worse yet, just plain making stuff up, we get to work. This year, you'll continue to see the team representing uncertainty throughout the report figures.

The examples shown in Figures 1, 2, 3 and 4 all convey the range of realities that could credibly be true. Whether it be the slant of the bar chart, the threads of the spaghetti chart, the dots of the dot plot or the color of the pictogram plot, all convey the uncertainty of our industry in their own special way.

Much like the slanted bar chart, the spaghetti chart represents the same concept: the possible values that exist within the confidence interval; however, it's slightly more involved because we have the added element of time. The individual threads represent a sample of all possible connections between the points that exists within each observation's confidence interval. As you can see, some of the threads are looser than others, indicating a wider confidence internal and a smaller sample size.

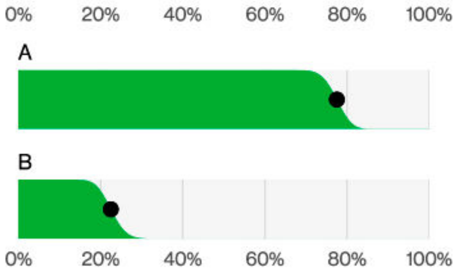


Figure 1. Example slanted bar chart (n=205)

The slanted bar chart will be familiar to returning readers. The slant on the bar chart represents the uncertainty of that data point to a 95% confidence level (which is standard for statistical testing).

In layman's terms, if the slanted areas of two (or more) bars overlap, you can't really say one is bigger than the other without angering the math gods.

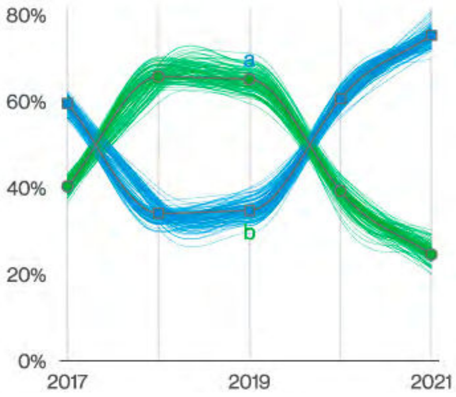


Figure 2. Example spaghetti chart

The dot plot is another returning champion, and the trick to understanding this chart is to remember that the dots represent organizations. If, for instance, there are 200 dots (like in Figure 3), each dot represents 0.5% of organizations. This is a much better way of understanding how something is distributed among organizations and provides considerably more information than an average or a median. We added more colors and callouts to those in an attempt to make them even more informative.

The pictogram plot, our relative newcomer, attempts to capture uncertainty in a similar way to slanted bar charts but is more suited for a single proportion.

We hope they make your journey through this complex dataset even smoother than previous years.

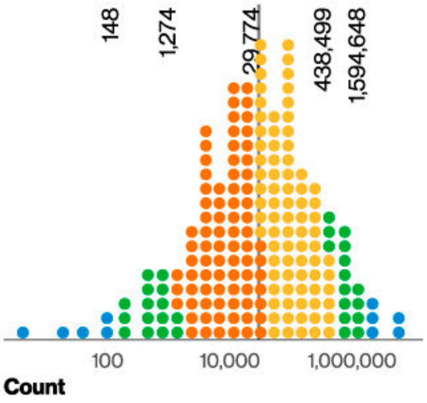


Figure 3. Example dot plot (n=672). Each dot represents 0.5% of organizations. Orange: lower half of 80%. Yellow: upper half of 80%. Green: 80%–95%. Blue: Outliers. 95% of orgs: 148–1,594,648. 80%: 1,274–438,499. Median: 29,774 (log scale).

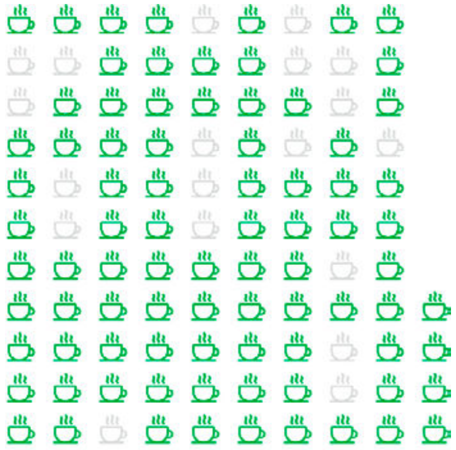


Figure 4. Example pictogram plot (n=4,110). Each glyph represents 40 breaches.

Credit where credit is due

Turns out folks enjoy citing the report, and we often get asked how they should go about doing it.

You are permitted to include statistics, figures and other information from the report, provided that (a) you cite the source as "Verizon 2023 Data Breach Investigations Report" and (b) content is not modified in any way. Exact quotes are permitted, but paraphrasing requires review. If you would like to provide people a copy of the report, we ask that you provide them a link to verizon.com/dbir rather than a copy of the PDF.

Questions? Comments? Organizing a bank run?

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

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**.

Introduction

"Success is stumbling from failure to failure with no loss of enthusiasm."
—attributed to Sir Winston Churchill

Hello and welcome old friends and new readers to the 2023 Verizon Data Breach Investigations Report! We are happy to have you join us once again as we take a look at the sordid underbelly of cybercrime and see what lessons we may collectively learn from doing so. It often seems that with every new defense strategy, appliance or Please-Save-Us-As-A-Service we create, buy or borrow, our adversaries are just as quick to adapt and find a new vantage point from which to attack. While this state of affairs is already unfortunate enough, it becomes worse still when we do not even require them to evolve their tactics because the old ones still work just fine.

Regardless of where we fall on the crazy-secure to not-so-secure spectrum, the quote above is a good road map to cybersecurity (and life in general). This report aims to take a look at the times when things did not work as intended—not to point fingers but to help us all learn and improve. In a time where almost everyone, corporations and individuals alike, is looking at ways to do more with less, we believe a close analysis of when our defenses failed can be very beneficial. While times of great change are always challenging, they often also prompt us to take stock of our situation and, if necessary, refocus both our viewpoint and our energies. Such is the case with the DBIR this year. As a team, we decided to take a step back toward the fundamental things that got us where we are, an intense focus on actual data breaches analyzed using our own VERIS Framework. And speaking of VERIS, one of the new goodies this refocusing brings is an even better mapping between VERIS and MITRE ATT&CK through a collaboration with MITRE Engenuity and the Center for Threat Informed Defense (CTID).[2] It also helps that our parent organization, the Verizon Threat Research Advisory Center (VTRAC),[3] shared the most breaches ever for us to analyze. Did you know it is VTRAC's 20th anniversary this year? Save us a slice of that cake, boss!

As long-time readers will know, over the past few years, we have increasingly utilized non-incident data to add depth and dimension to our breach findings via various forms of research and analysis. While that remains a big part of what we do, as mentioned above, we did take purposeful steps toward a more direct focus on the breach side of the house this year. In short, the result of this was to make the report more concise and succinct and less unwieldy. This year we analyzed 16,312 security incidents, of which 5,199 were confirmed data breaches. As always, we hope you find this information informative, useful, easy to understand and actionable.

Finally, we thank our global data contributors most sincerely, as this report would quite literally not be possible without them. Of course, the same can be said of our readers, so please accept our deep gratitude for your continued support.

Sincerely,

The Verizon DBIR Team
C. David Hylender, Philippe Langlois, Alex Pinto, Suzanne Widup

Very special thanks to:
- Dave Kennedy and Erika Gifford from VTRAC.
- Kate Kutchko, Marziyeh Khanouki and Yoni Fridman from the Verizon Business Product Data Science Team.
- Gabriel Bassett for all the statistical tooling, charts and terrible jokes over the years. Good luck on your next adventure!

---

[2] https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/
[3] https://www.verizon.com/business/resources/reports/verizon-threat-research-advisory-center/

Summary of findings

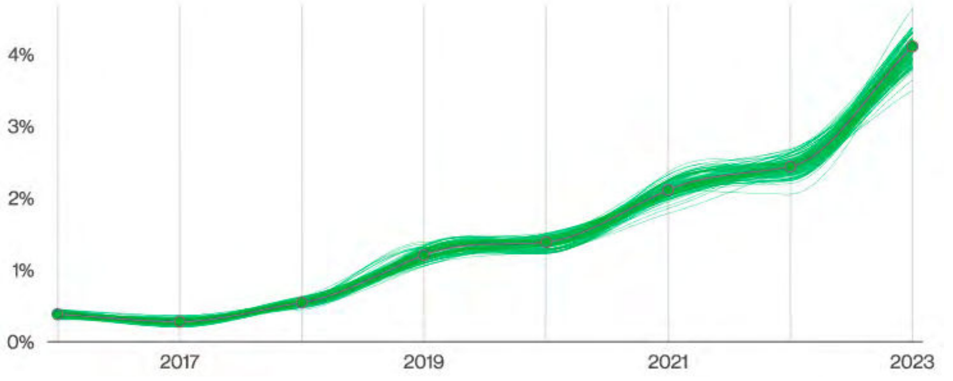


Figure 5. Pretexting incidents over time

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 5, and now represent more than 50% of incidents within the Social Engineering pattern.

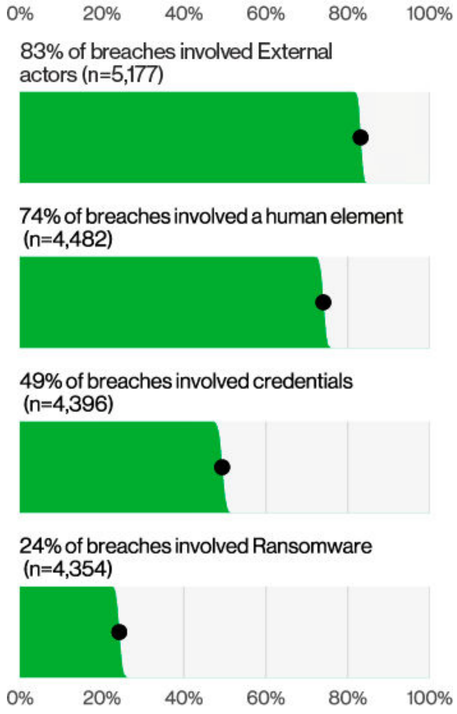


Figure 6. Select key enumerations

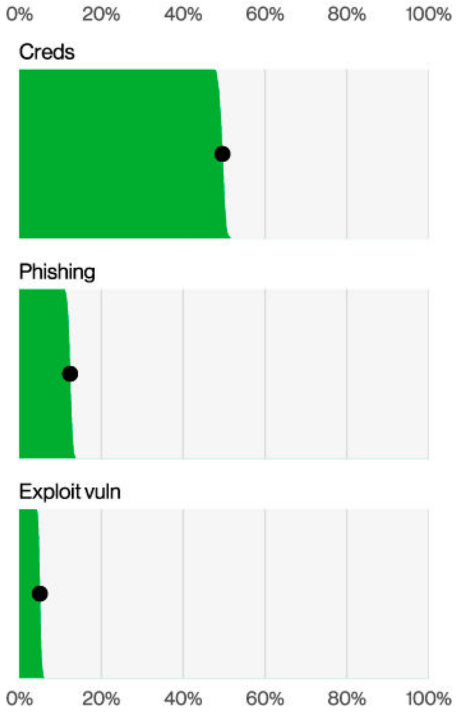


Figure 7. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

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.

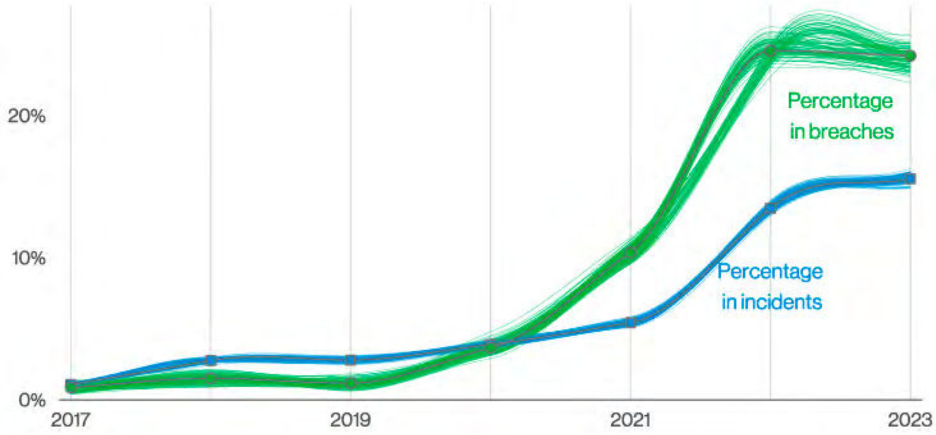


Figure 8. Ransomware action variety over time

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.

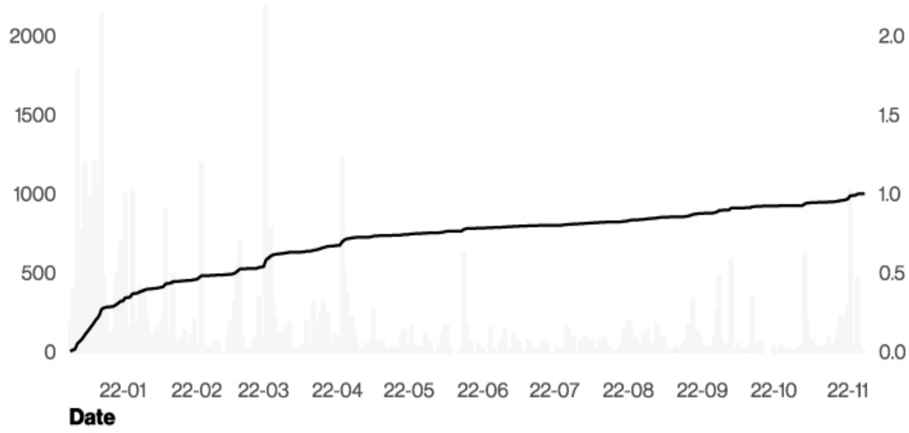


Figure 9. Percentage of Log4j scanning for 2022

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).

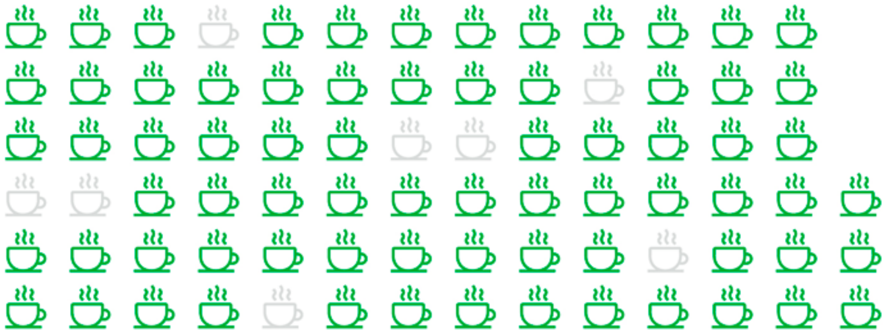
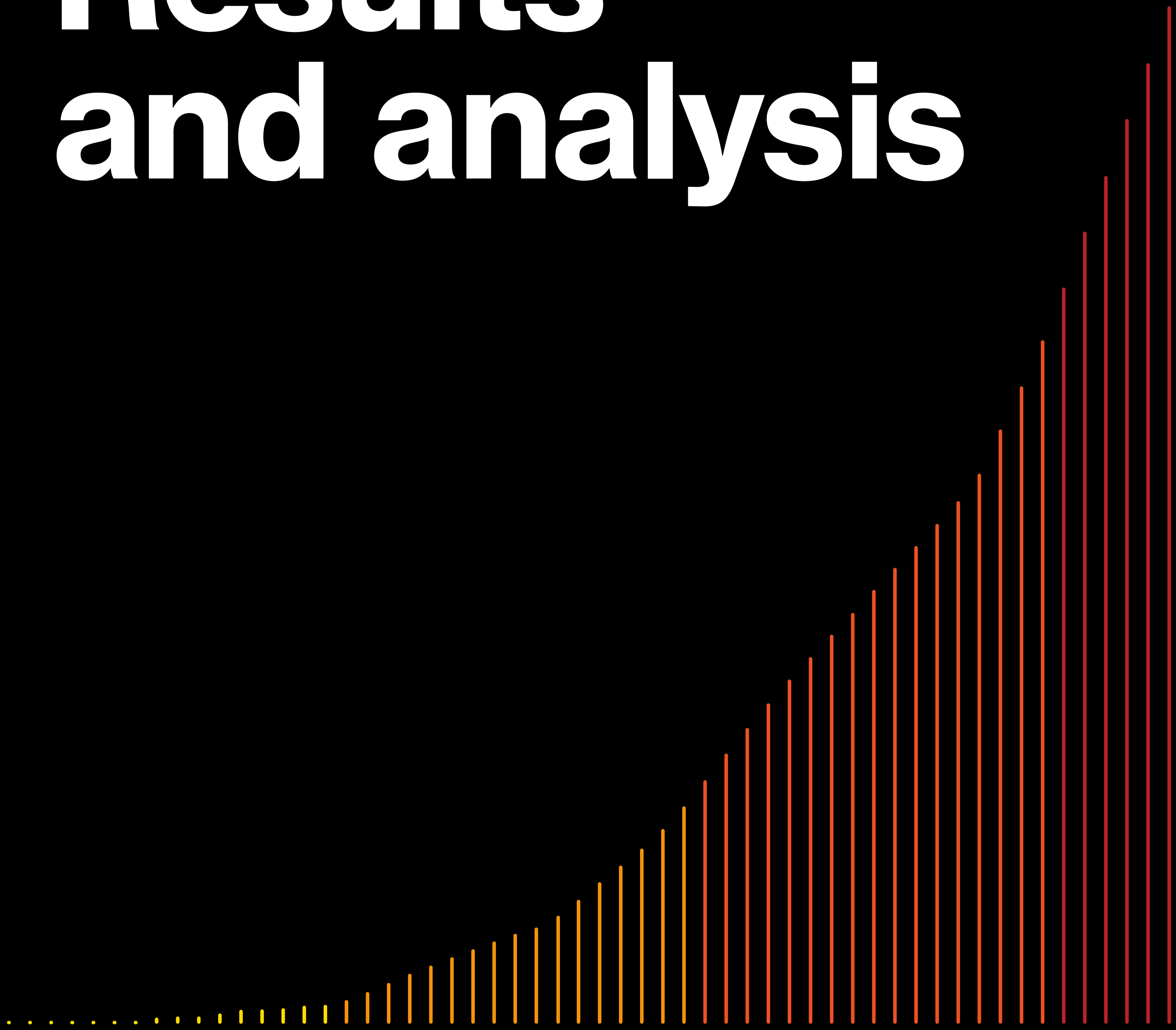


Figure 10. Percentage of identified Exploit vuln that was Log4j (n=81). Each glyph represents an incident.

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.

2

Results and analysis



Results and analysis: Introduction

Hello friends, and welcome to the “Results and analysis” section. This is where we cover the highlights we found in the data this year. This dataset is collected from a variety of sources, including our own VTRAC investigators, reports provided by our data contributors and publicly disclosed security incidents.

Since data contributors come and go, one of our priorities is to make sure we can get broad representation on different types of security incidents and the countries where they occur. This ebb and flow of contributors obviously influences our dataset, and we will do our best to provide context on those potential biases where applicable.

As some of you may have noticed[4] over the years, the incident data collection we do is based on the VERIS Framework. It has been the bedrock upon which our multiyear dataset has been built and is what allows us to be able to speak with confidence when trends in the attack landscape surface. Our dataset currently contains 953,894 incidents, of which 254,968 are confirmed breaches, and we can’t wait to celebrate[5] with you when we reach 1 million[6] incidents!

In VERIS, the core categories we use to describe an incident are called the 4As: Actor (who), Action (how), Asset (where) and Attribute (what). An incident needs all these four to be “complete,” even if at the end of the day some of those are unknown to the parties investigating the incident. Keep an eye out for our instructive callouts in each of those sub-sections giving more context on our VERIS categories.

Let’s go over the results for each one of these.

---

[4] We certainly won’t shut up about it.

[5] Not sure if we should be celebrating security incidents, but everyone loves a round number.

[6] Here’s hoping being a millionaire doesn’t get to our dataset’s head, and they decide to join the “Great Resignation” and retire in some tropical tax haven.

Actors

Life can be scary and unpredictable, which is why we like to start our results discussion with the cozy and familiar Actor analysis. It really is true, as they say, that the only certainties in life are death, taxes and External actors.[7]

As Figure 11 demonstrates, External actors were responsible for 83% of breaches, while Internal ones account for 19%. It is worth reminding our readers that Internal actors are not only responsible for intentional harm in these cases, but they are also just as likely[8] to be responsible for Error actions. Regardless, the clear frequency of External actors as instigators of breaches is a datapoint that has held steady ever since we started this gig.

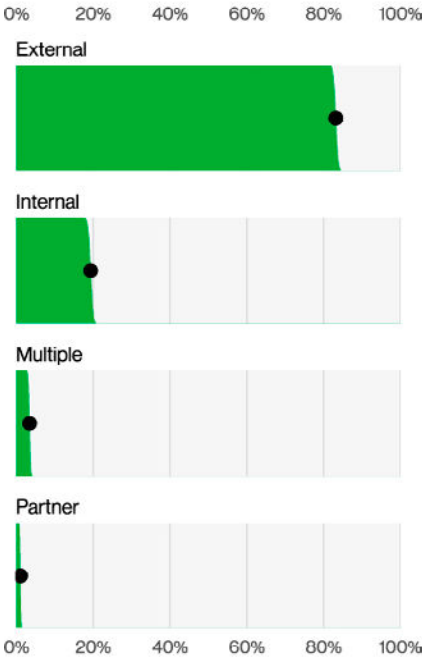


Figure 11. Threat actors in breaches (n=5,177)

Actor categories[9]

External: External threats originate from sources outside of the organization and its network of partners. Examples include criminal groups, lone hackers, former employees and government entities. This category also includes God (as in "acts of"), "Mother Nature" and random chance. Typically, no trust or privilege is implied for external entities.

Internal: Internal threats are those originating from within the organization. This encompasses company full-time employees, independent contractors, interns and other staff. Insiders are trusted and privileged (some more than others).

Partner: Partners include any third party sharing a business relationship with the organization. This includes suppliers, vendors, hosting providers and outsourced IT support. Some level of trust and privilege is usually implied between business partners. Note that an attacker could use a partner as a vector, but that does not make the partner the Actor in this case. The partner has to initiate the incident.

---

[7] That's what they say, right?

[8] OK, actually twice as likely.

[9] https://verisframework.org/actors.html

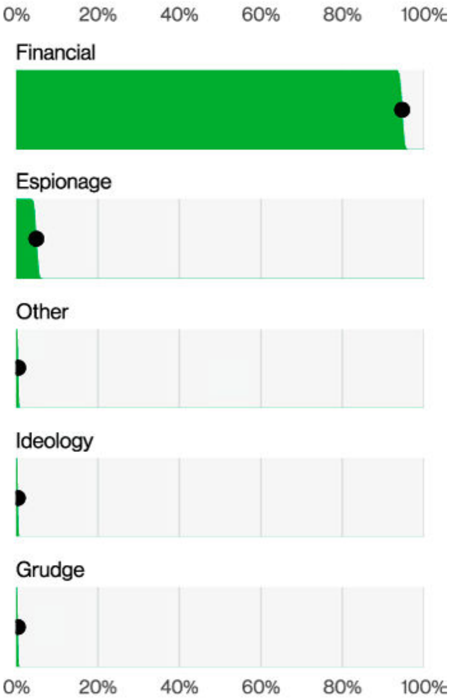


Figure 12. Threat actor Motives in breaches (n=2,328)

Long-time readers of the report will be similarly shocked to learn that Financial motives still drive the vast majority of breaches (Figure 12), showing growth in relation to last year with a whopping 94.6% representation in breaches. If we look inside to see which external actors are the hardest working, the top performer is Organized crime (Figure 13).

What is most interesting in Figure 13, however, is realizing that the internal variety of End-user shows up more often than the external variety State-sponsored attackers.[10] Those organization employees are mostly involved in Misuse (read, internal malicious activity) and Errors (accidents), which suggests where we should be paying more attention on our day-to-day security management.

This is relevant because we were expecting some increased activity in State-sponsored attacks, be it Espionage-related or not, due to the ongoing conflict in Ukraine. Even with anecdotal evidence of increased ideology or hacktivism-related attacks stemming from the geopolitical discussion, it really isn't making a dent in larger statistical terms. It is also worth noting that this kind of activity would also be unlikely to disrupt our average reader's organization.[11]

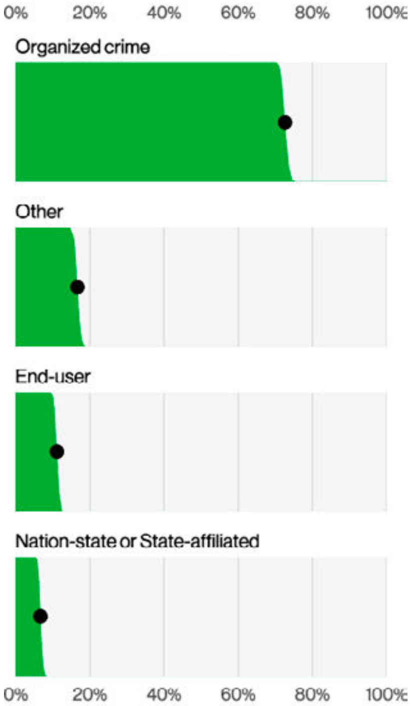


Figure 13. Threat actor Varieties in breaches (n=2,489)

---

[10] Huge win for anarchists and other state-abolishing ideologies, if you ask us.
[11] No, Mr. Bond, MI6 does not represent our average reader.

Actions

Action, as the name would imply, is what brings dynamism to our report. What dastardly deeds have the threat actors been up to? If you replied "ransomware," we'd say you have no imagination, but you would also be right. This pesky Malware variety has been holding our talking points hostage for years now, and we can't scrounge up enough cryptocurrency to pay the ransom!

Figures 14, 15, 16 and 17 describe the top Action varieties (what happened in more detail) and vectors (how those actions came to pass).

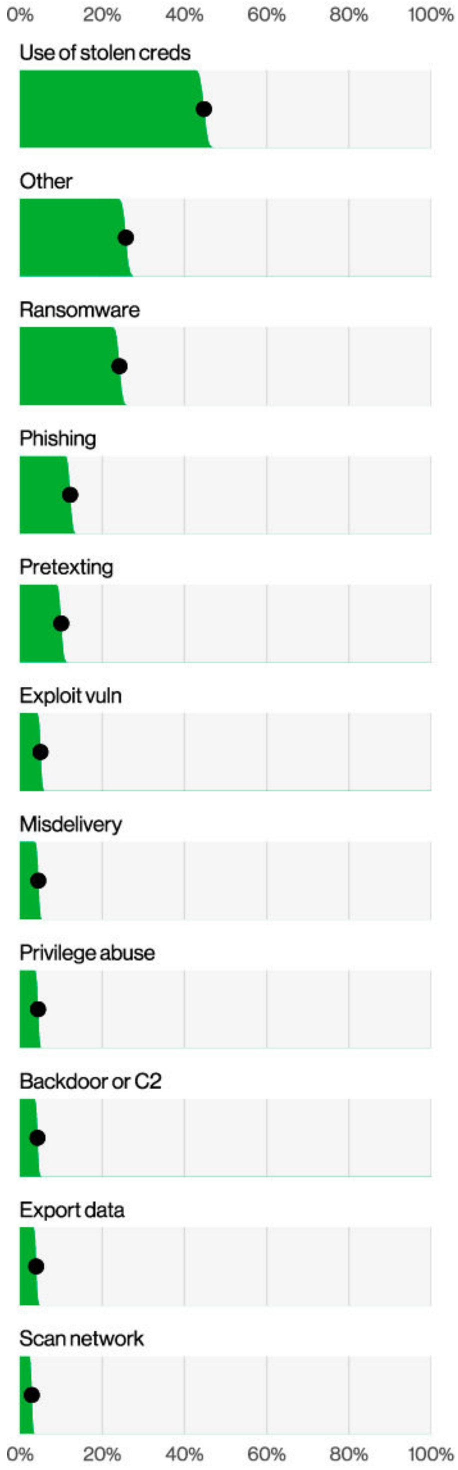


Figure 14. Top Action varieties in breaches (n=4,354)

Action categories[12]

Hacking (hak): attempts to intentionally access or harm information assets without (or exceeding) authorization by circumventing or thwarting logical security mechanisms.

Malware (mal): any malicious software, script or code run on a device that alters its state or function without the owner's informed consent.

Error (err): anything done (or left undone) incorrectly or inadvertently.

Social (soc): employ deception, manipulation, intimidation, etc., to exploit the human element, or users, of information assets.

Misuse (mis): use of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended.

Physical (phy): deliberate threats that involve proximity, possession or force.

Environmental (env): not only includes natural events such as earthquakes and floods but also hazards associated with the immediate environment or infrastructure in which assets are located.

---

[12] https://verisframework.org/actions.html

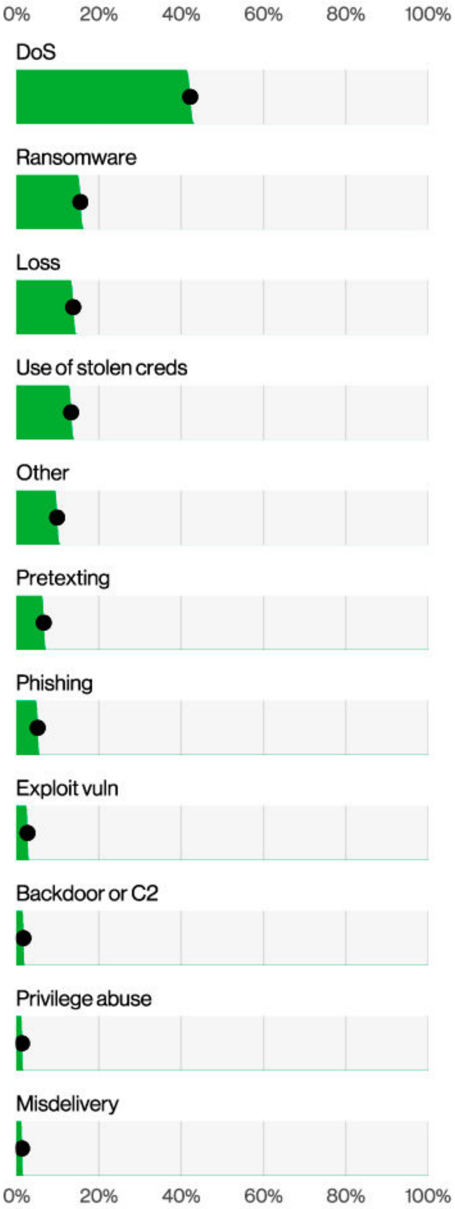


Figure 15. Top Action varieties in incidents (n=14,829)

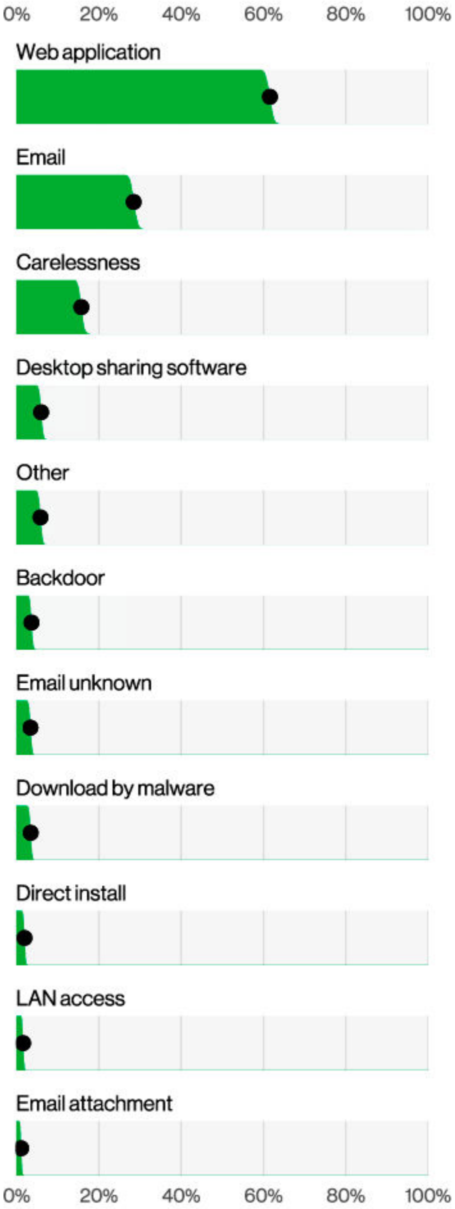


Figure 16. Top Action vectors in breaches (n=3,194)

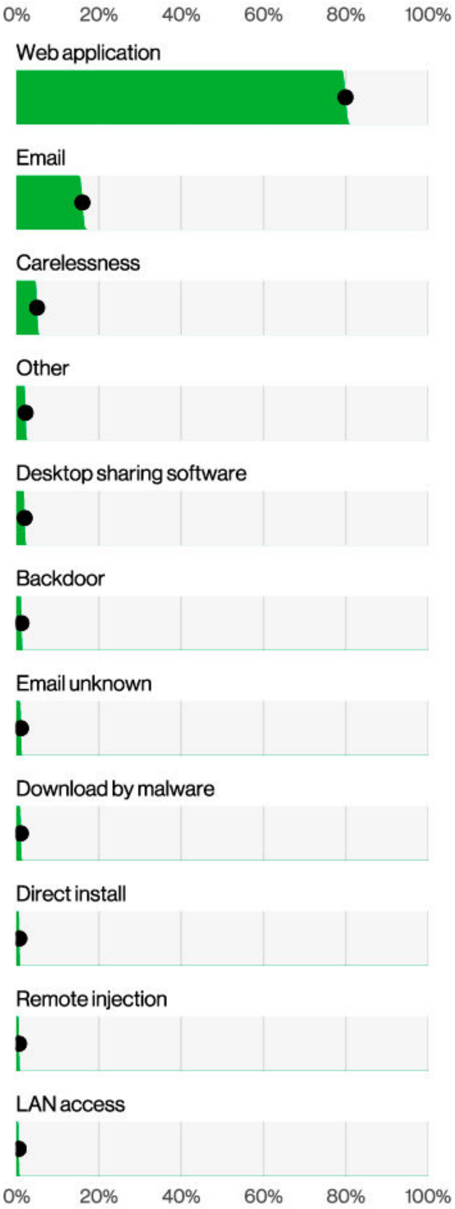


Figure 17. Top Action vectors in incidents (n=10,502)

As expected, the charts are led by either first-stage or single-stage attacks, namely Use of stolen creds for breaches and Denial of Service for incidents. This is consistent with previous years. What is concerning, if unsurprising, is having Ransomware take over the second spot in incidents, now being present in 15.5% of all incidents. Meanwhile, the share of Ransomware did not grow in breaches and held steady (statistically, at least) at 24%. You can see the evolution of both in Figure 18.

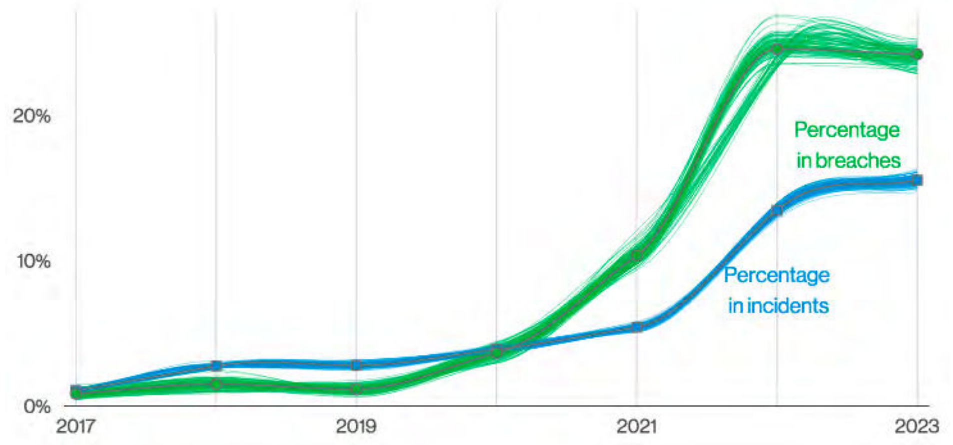


Figure 18. Ransomware action variety over time

That almost a quarter of breaches involve a Ransomware step continues to be a staggering result. However, we had been anticipating that Ransomware would soon be hitting its theoretical ceiling, by which we mean that all the incidents that could have Ransomware, would have. Ransomware is present today in more than 62% of all incidents committed by Organized crime actors and in 59% of all incidents with a Financial motivation, so sadly there is still some room for growth.

Eagle-eyed readers will notice the absence of Partner and Software update as action vectors for incidents this year, in contrast to last year's "software supply chainpocalypse."[13] Instead, our collective Christmas was ruined by another Ghost of Technical Debt Past: the Log4j vulnerability popularly known as CVE-2021-44228.[14]

We will be spending some time digging into the Log4j vulnerability in the "System Intrusion" section, but it is worth noting that the presence of the Exploit vuln action has kept stable in incidents and is actually less prominent in breaches, dropping from 7% to 5%. So, did the collective security industry sacrifice its holidays for nothing?

Not quite. This is one of those cases where the alternatives are just more popular. Use of stolen creds, our current champion, increased its share from 41.6% to 44.7%, which more than accounts for the drop in Exploit vuln.

More importantly, there was swift action from the community to spread awareness and patch all the different systems that had Log4j as a component. That surely helped avert a bigger disaster, so our success makes it look like it wasn't a big deal after all.[15] In fact, 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. Granted, only 20.6% of the incidents had comments at all,[16] so even if it can't fully represent the whole dataset, it certainly speaks to how significant the vulnerability was in late 2021 and early 2022 for the incident response teams.

Finally, before I lose your attention, we should touch base on Loss.[17] This action variety describes losing a physical device or media by accident and is often paired with the Carelessness action vector. It did show up fairly high in incidents. This is often because the data could not be confirmed as having been accessed and was therefore considered at risk rather than a breach. It is worth pointing out though that those were mostly concentrated in the data from some of our public sector contributors, where this sort of event is more tightly reported. Regardless, we know everyone was super excited about leaving the house again as the pandemic waned, but please keep an eye on your stuff when you go work from the coffee shop.

[13] Wouldn't you know, the moment we mention anything has not had relevance in our dataset, something new happens to remind us that change is the only constant. Best of luck for the teams responding to the 3CX supply-chain breach in late March 2023 as we close out this section. Make sure to keep copious notes so we can talk about it in a future edition of the report.

[14] Just rolls off the tongue, doesn't it?

[15] Who here was working on the Y2K bug? Don't forget to schedule your shingles vaccine!

[16] In everyone's defense, most of the data sharing happening here is machine-to-machine. Long gone are the days of artisanal, bespoke, VERIS-coded incidents for most of our contributors.

[17] For the extremely online folks, we apologize for the psychic damage.

Assets

In case you just wandered out of an Accounting 101 class, our Assets are more than the numbers that you list on the left side of your balance sheet.[18] They encompass the entities that can be affected in an incident or breach and end up being manipulated by the threat actors for their nefarious goals. The callout box describes some of the most common top-level Assets in VERIS and some of the most common attack patterns that target them.

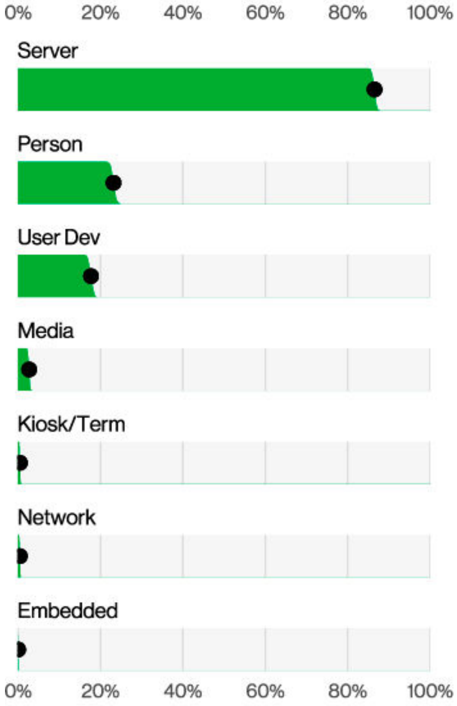


Figure 19. Assets in breaches (n=4,433)

Figure 19 has the breakdown of varieties of Assets affected in breaches, and the results are pretty much what would be expected given the focus of System Intrusion, Basic Web Application Attacks and Social Engineering as the top attack patterns this year.

We can see a small fluctuation on the top three, as slightly less Servers were affected and slightly more User devices, but this order has held true for at least a couple of years, ever since Person overtook the second spot. Don't forget that in VERIS, people are assets too,[19] and they are the "where" that is affected by social threat actions.

Asset categories[20]

Server (srv): a device that performs functions of some sort supporting the organization, commonly without end-user interaction. Where all the web applications, mail services, file servers and all that magical layer of information is generated. If someone has ever told you "the system is down," rest assured that some Servers had their Availability impacted. Servers are common targets in almost all of the attack patterns, but especially in our System Intrusion, Basic Web Application Attacks, Miscellaneous Errors and Denial of Service patterns.

Person (per): the folks (hopefully) doing the work at the organization. No AI chat allowed. Different types of Person will be members of different departments and will have associated permissions and access in the organization stemming from this role. At the very least they will have access to their very own User device and their own hopes and dreams for the future. Person is a common target in the Social Engineering pattern.

User device (usr): the devices used by Persons to perform their work duties in the organizations. Usually manifested in the form of laptops, desktops, mobile phones and tablets. Common target in the System Intrusion pattern but also in the Lost and Stolen Asset pattern. People do like to take their little computers everywhere.

Network (net): not the concept, but the actual network computing devices that make the bits go around the world, such as routers, telephone and broadband equipment, and some of the traditional in-line network security devices, such as firewalls and intrusion detection systems. Hey, Verizon is a Telecommunications company, OK?

Media (med): precious diluted data in its most pure and crystalline form. Just kidding, mostly thumb drives and actual printed documents. You will see the odd full disk drive and actual physical payment cards from time to time, but those are more rare. Common in the Lost and Stolen Assets pattern.

---

[18] However, not caring for them properly could cause liabilities that would go on the right side.
[19] Just ask your organization's HR department.
[20] https://verisframework.org/assets.html

Breaking the Asset varieties down further in Figure 20 showcases Web application and Mail servers on top, as would be expected, but it is interesting to see Person - Finance trending up from last year as we see a related growth in Pretexting social actions. We will be discussing those, and more specifically BECs, in the "Social Engineering" section of this report.

As a parting note, we continue to see very small numbers of incidents involving Operational Technology (OT), where the computers interface with heavy machinery and critical infrastructure, as contrasted with incidents involving Information Technology (IT), where we keep our cat pictures and internet memes. Industries like Manufacturing and Mining, Quarrying and Oil & Gas Extraction + Utilities[21] continue to be relatively well-represented in our dataset, but reports of actual impact on OT devices are still too few for us to meaningfully write about in this report.

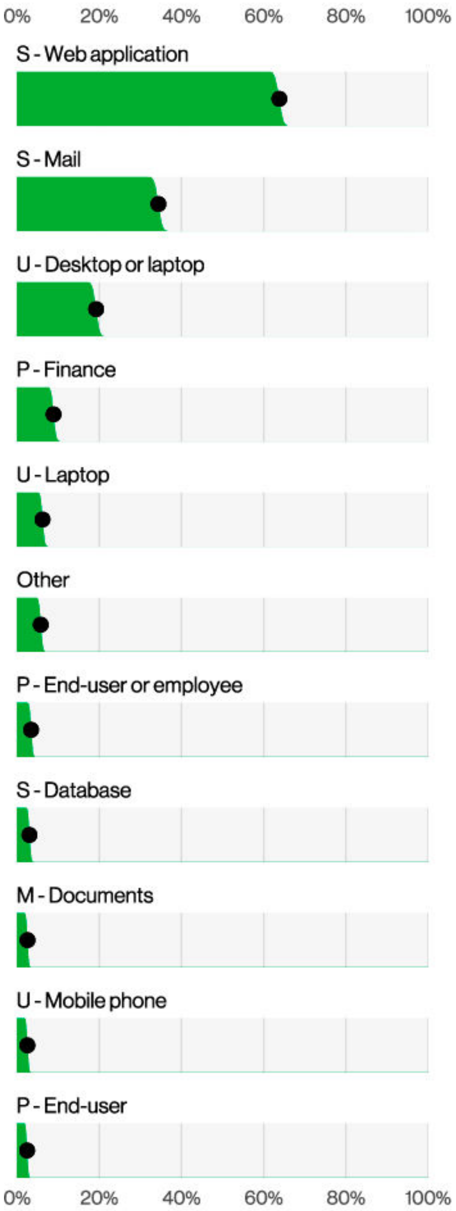


Figure 20. Top Asset varieties in breaches (n=3,207)

For those keeping track, we had a 3.4% showing of OT assets in breaches that declared their impact. In summary—keep your attention level high, given the potential impact when those systems are affected, but either those numbers are very low overall, or they just don't make it to our contributors' dataset due to national[22] security concerns.

---

[21] We know, it's a mouthful.

[22] From any country really.

Attributes

When VERIS describes Attributes, it is directly referencing the CIA triad in information security (InfoSec): Confidentiality, Integrity and Availability. It's a tried-and-true method of understanding the potential impact of an incident by describing what properties of the asset were potentially affected.

Attribute categories[23]

Confidentiality (cp): refers to limited observation and disclosure of an asset (or data). A loss of confidentiality implies that data were actually observed or disclosed to an unauthorized actor rather than endangered, at-risk or potentially exposed (the latter fall under the attribute of Possession and Control). Short definition: limited access, observation and disclosure.

Integrity (ia): refers to an asset (or data) being complete and unchanged from the original or authorized state, content and function. Losses to integrity include unauthorized insertion, modification and manipulation. Short definition: complete and unchanged from original.

Availability (au): refers to an asset (or data) being present, accessible and ready for use when needed. Losses to availability include destruction, deletion, movement, performance impact (delay or acceleration) and interruption. Short definition: accessible and ready for use when needed.

The next time you meet an incident responder in the wild, know that all that goes through their mind is, "Did the asset or a copy of the data get out the door" (Confidentiality), "was it changed from a known and trusted state" (Integrity) and "do we still have access to it ourselves?" (Availability). Please offer them a word of kindness and a beverage, because it is a very tortured existence. If you are feeling cold, they are cold too.

One of the most interesting Attribute varieties we track year over year is the Confidentiality data varieties (Figure 21), or what kinds of data got out in a breach. Personal data represents Personally Identifiable Information (PII) from your customers, partners or employees, and it is the one that usually gets companies the most in trouble with regulators, as more and more privacy-related laws are passed around the world (although Medical data is a whole other ball of earwax).

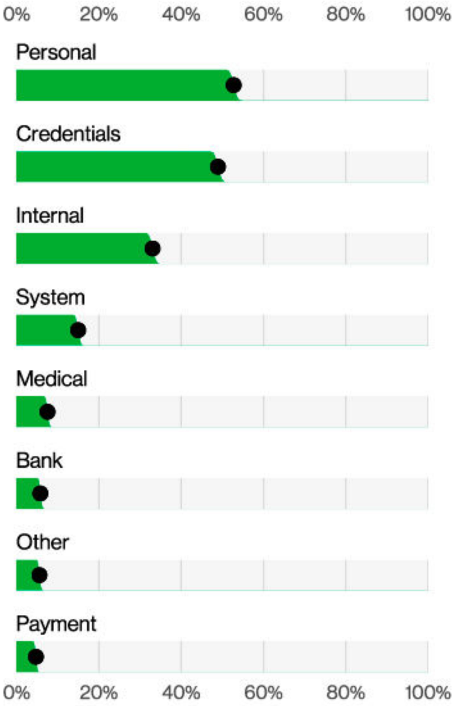


Figure 21. Top Confidentiality data varieties in breaches (n=5,010)

Virtual money, real problems

One data variety really caught the DBIR team's attention this year: Virtual currency. We saw a fourfold increase this year in the number of breaches involving cryptocurrency from last year. That is a far cry from the days of innocence in 2020 and earlier, when we got one or two cases maximum each year. If our cartoon animal NFTs had these kinds of returns, we can assure you we would be living large and writing this report from our Lambos, not from our parents' basements.[24]

Figures 23 and 24 show the top action varieties and vectors in breaches involving virtual currency, and it is a fierce competition between Exploit vulnerabilities, Use of stolen creds and Phishing. These types of breaches

---

[23] https://verisframework.org/attributes.html

[24] Our Lambos might be parked in our parent's garage, though.

Internal data and System data are usually byproducts of an extensive breach with multiple steps, as information from emails and documents are vacuumed up by threat actors. Credentials have really gained ground over the past five years, as the Use of stolen credentials became the most popular entry point for breaches.

Of course, we still get specific data being beset, such as Medical, Bank account information and Payment card data. Those could be specific, targeted events or just be a part of the data that is acquired during a ransomware attack with data exfiltration. And just in case you are not tired of us moaning about ransomware,[25] please enjoy Figure 22, where we can see another impact of the ransomware growth as the Obscuration of data became the most common availability impact variety, handily overcoming plain old Loss of data.

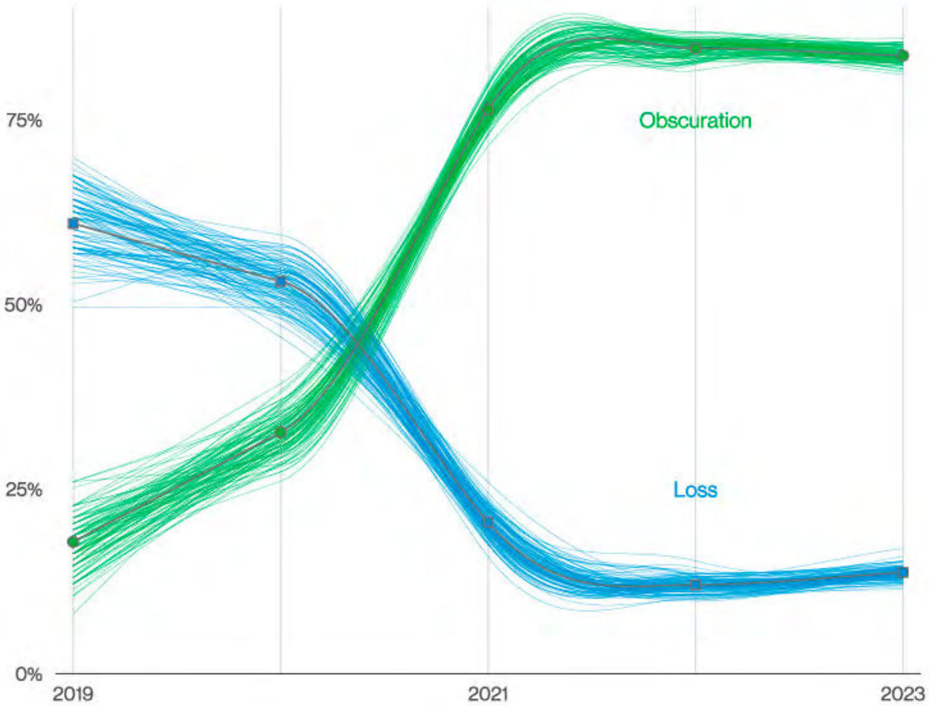


Figure 22. Availability variety over time

fall between the actual coin networks or exchanges being breached via their applications and application programming interfaces (APIs), or phishing and pretexting activity on chat platforms (like Discord) of the coin communities, where after a simple click on a link, suddenly your wallet is not yours anymore.

Having assets in virtual currency is a risky endeavor at best, even when there are no bad actors involved in rug-pulling.[26] The added focus of threat actors on these types of assets doesn't make the landscape any easier. Our parting message is that unless security is taken seriously in those cases, we, in fact, are not going to make it.

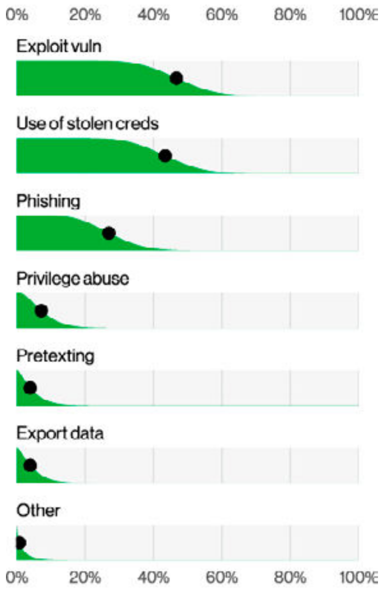


Figure 23. Top Action varieties in breaches where virtual currency was involved (n=30)

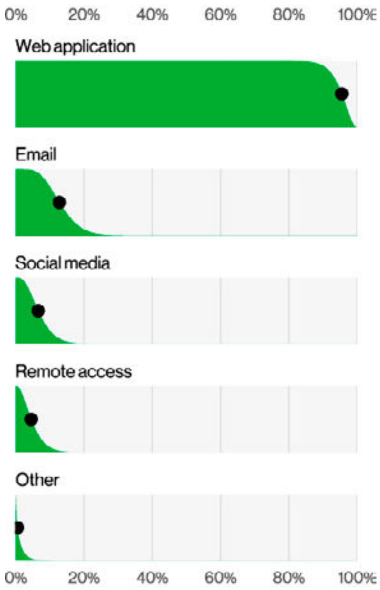


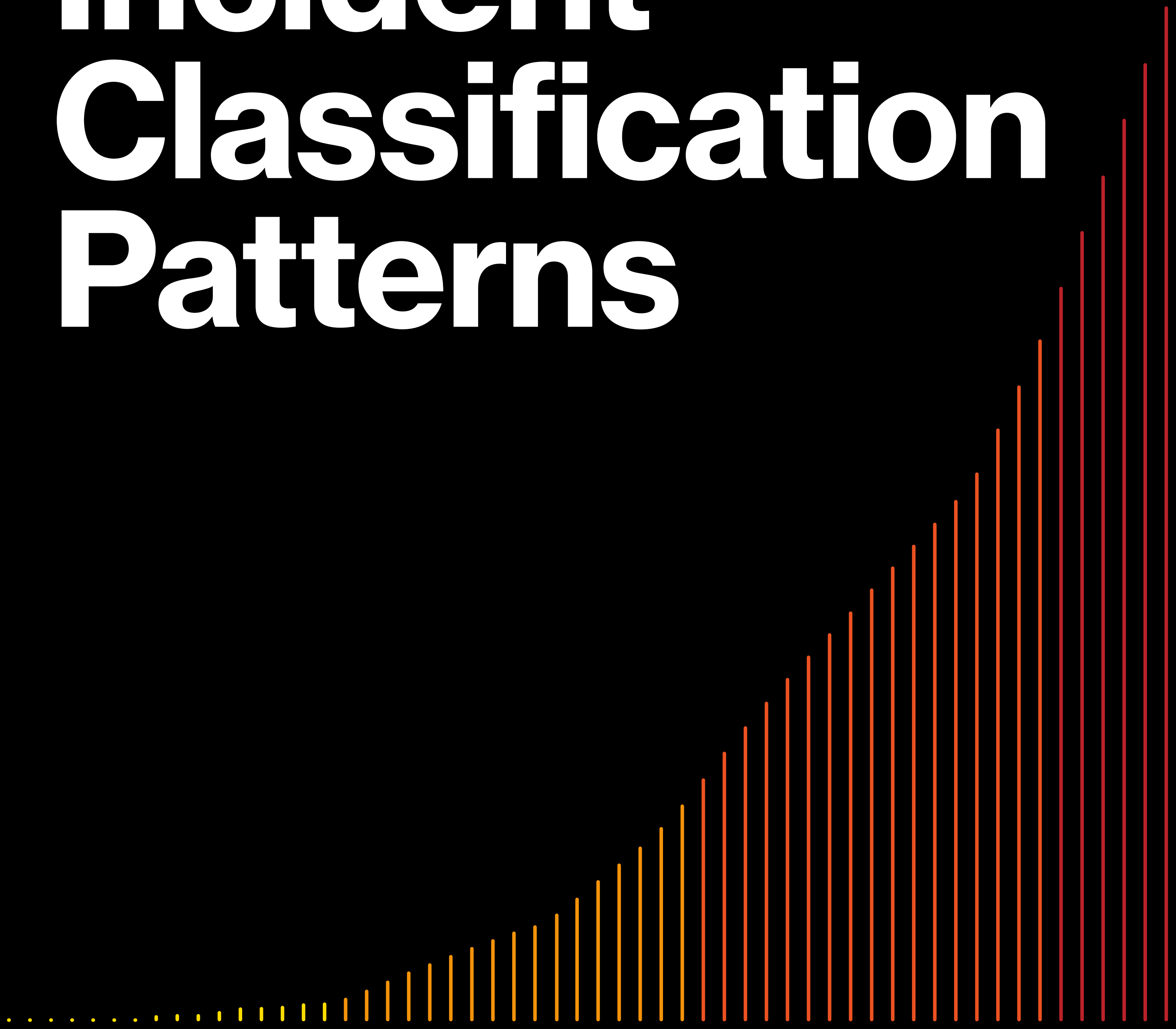
Figure 24. Top Action vectors in breaches where virtual currency was involved (n=48)

[25] We're not bitter; you're bitter.

[26] That rug really tied the room together, man!

3

Incident Classification Patterns



Incident Classification Patterns: Introduction

One of the greatest gifts that evolution has granted the human race is a pattern-seeking brain. Was that just some swaying foliage in the jungle, or is a striped tiger sneaking around to pounce on us? The fact that humans are still around tells us we got that question right more often than we didn't. Thankfully, we can also use our pattern-seeking superpowers to try to organize and make sense of all the different ways in which computers remind us they were a mistake.[27]

Our incident patterns are, in a nutshell, a way to cluster similar incidents into an easy-to-remember shorthand. As we mentioned before, incidents are characterized by the 4As of VERIS, and we can avoid a long descriptive paragraph every time by classifying our incidents in this way.[28] Our eight patterns, and how they are defined, can be found in Table 1.

This year, we are showcasing a detailed breakdown of ATT&CK Techniques[29] and Center for Internet Security (CIS) Critical Security Controls[30] related to certain patterns, as those are the places that make sense so we don't repeat ourselves throughout this report. We are proud of the ATT&CK mappings release, as they represent the culmination of a multiyear collaboration with MITRE CTID in creating and maintaining

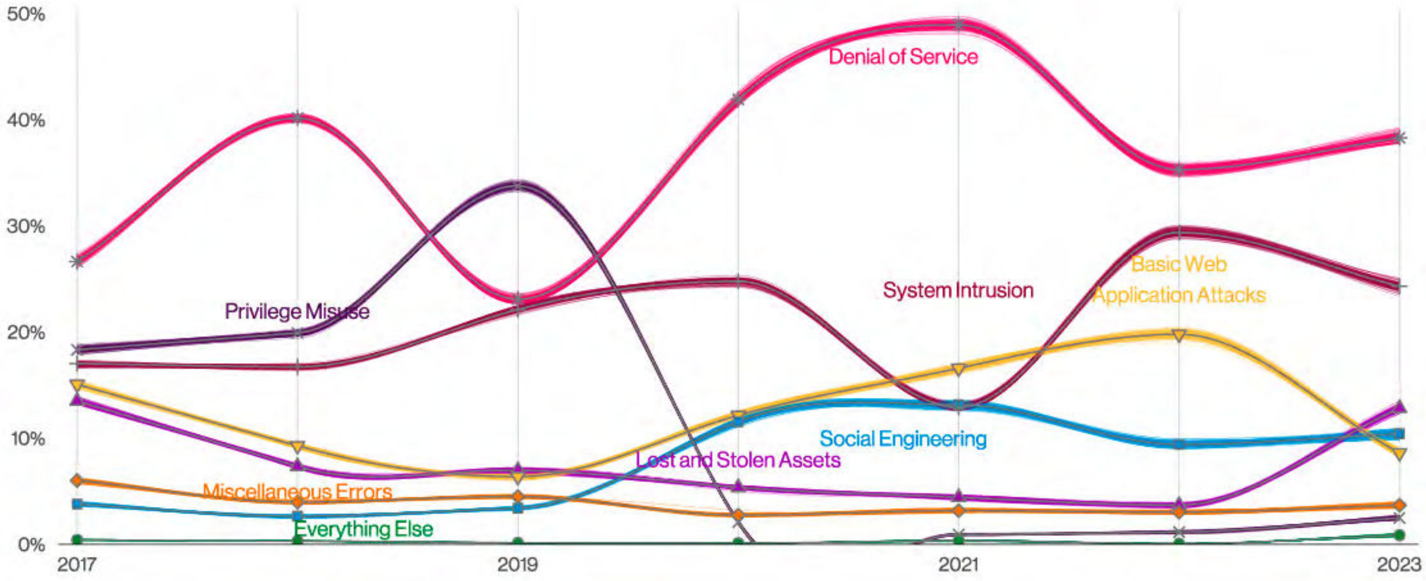


Figure 25. Patterns over time in incidents

a working relationship between its standard and VERIS. You can read more about this in our Appendix B.

---

[27] As opposed to ChatGPT and other AI platforms, which insist that humans may be the mistake.
[28] It's like they say, a pattern is worth about four A's.
[29] https://attack.mitre.org/
[30] https://www.cisecurity.org/controls

So, enjoy the cognitive load we just removed from your (pattern-seeking) grey matter as we deep dive into specific results and detailed analysis for each pattern.

As we have in prior years, here we present our Incident Classification Patterns (patterns) and show how they fared year over year. Figure 25 shows the patterns over time for incidents, and you can see that Denial of Service is top of the heap, as it has been for several years.

When you contrast this graphic with Figure 26, you can see how different the environment looks when we are focused on those incidents where there was confirmed data loss.

The System Intrusion pattern—with its more complex attacks—has been an overachiever and includes multistep attacks that feature ransomware. But we're getting ahead of ourselves. Let's move into the detailed pattern sections for the full story.

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.
Denial of Service	These attacks are intended to compromise the availability of networks and systems. This includes both network and application layer attacks.
Lost and Stolen Assets	Incidents where an information asset went missing, whether through misplacement or malice, are grouped into this 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.
Privilege Misuse	These incidents are predominantly driven by unapproved or malicious use of legitimate privileges.
Social Engineering	This attack involves the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.
System Intrusion	These are complex attacks that leverage malware and/or hacking to achieve their objectives, including deploying Ransomware.
Everything Else	This "pattern" isn't really a pattern at all. Instead, it covers all incidents that don't fit within the orderly confines of the other patterns. Like that container where you keep all the cables for electronics you don't own anymore: Just in case.

Table 1. Incident Classification Patterns

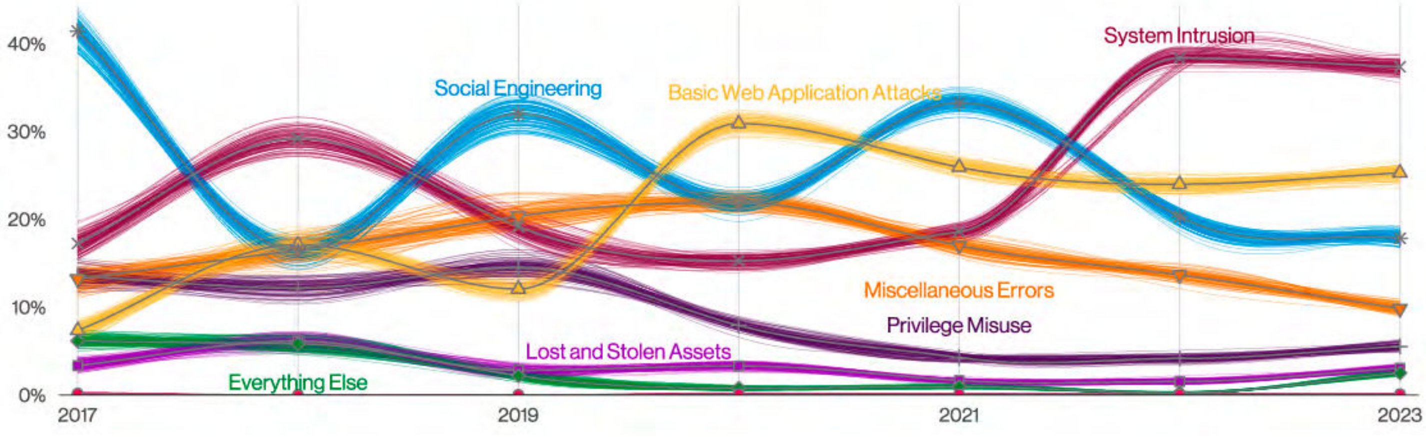


Figure 26. Patterns over time in breaches

System Intrusion

Summary

This pattern largely pertains to attacks perpetrated by more dedicated criminals who utilize their expertise in hacking and ready access to malware to breach and/or impact organizations of different sizes, frequently leveraging Ransomware as their means of getting a payday.

What is the same?

Ransomware continues to dominate this pattern as attackers leverage a bevy of different techniques to compromise an organization.

Frequency	3,966 incidents, 1,944 with confirmed data disclosure
Threat actors	External (96%), Internal (4%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (97%), Espionage (3%) (breaches)
Data compromised	Other (42%), Personal (34%), System (31%), Internal (24%) (breaches)

This is mine, and this is mine …

Imagine strolling into your office one morning only to discover an alarming desktop image from some criminal group with a cringeworthy name requesting Bitcoin (BTC) in exchange for the return of all your data. Hopefully, being the avid DBIR reader you are, you would have recent and well-tested backups to restore from. However, what if these criminals do not stop at only encrypting your data but also threaten to leak portions of your more sensitive information unless paid? Oftentimes it appears that no matter how fast our defenses and practices evolve, attackers adapt theirs just as quickly.

Relevant ATT&CK techniques

Exploit vuln (VERIS)

- Exploitation for Privilege Escalation: T1068
- Exploit Public-Facing Application: T1190
- Exploitation for Defense Evasion: T1211
- Exploitation for Credential Access: T1212
- Exploitation of Remote Services: T1210
- External Remote Services: T1133
- Vulnerability Scanning: T1595.002

Use of stolen creds (VERIS)

- Compromise Accounts: T1586
  - – Social Media Accounts: T1586.001
  - – Email Accounts: T1586.002
- External Remote Services: T1133
- Remote Services: T1021
  - – Remote Desktop Protocol: T1021.001
- Use Alternate Authentication Material: T1550
  - – Web Session Cookie: T1550.004
- Valid Accounts: T1078
  - – Default Accounts: T1078.001
  - – Domain Accounts: T1078.002
  - – Local Accounts: T1078.003
  - – Cloud Accounts: T1078.004

Execution: TA0002

Persistence: TA0003

Privilege Escalation: TA0004

Defense Evasion: TA0005

Credential Access TA0006

This creates a perpetual arms race, and nowhere is it better represented than in the System Intrusion pattern.

We frequently think of the threat actors in this pattern as the "hands on keyboard" type of attackers. While they might leverage automation to gain a foothold, once they are inside the organization, they utilize finely honed skills to bypass controls and achieve their goals. As Figure 28 illustrates, this commonly includes Ransomware. They use a variety of tools to traverse your environment and then pivot, including using phishing and stolen credentials to obtain access and adding backdoors to maintain that access and leverage vulnerabilities to move laterally. We can see these attacks more clearly when we break them into three smaller, more consumable portions. Namely, the initial access phase, the breach escalation and the results. Figure 27 has a breakdown of the Action-Asset combinations that we see during different steps of the attack.

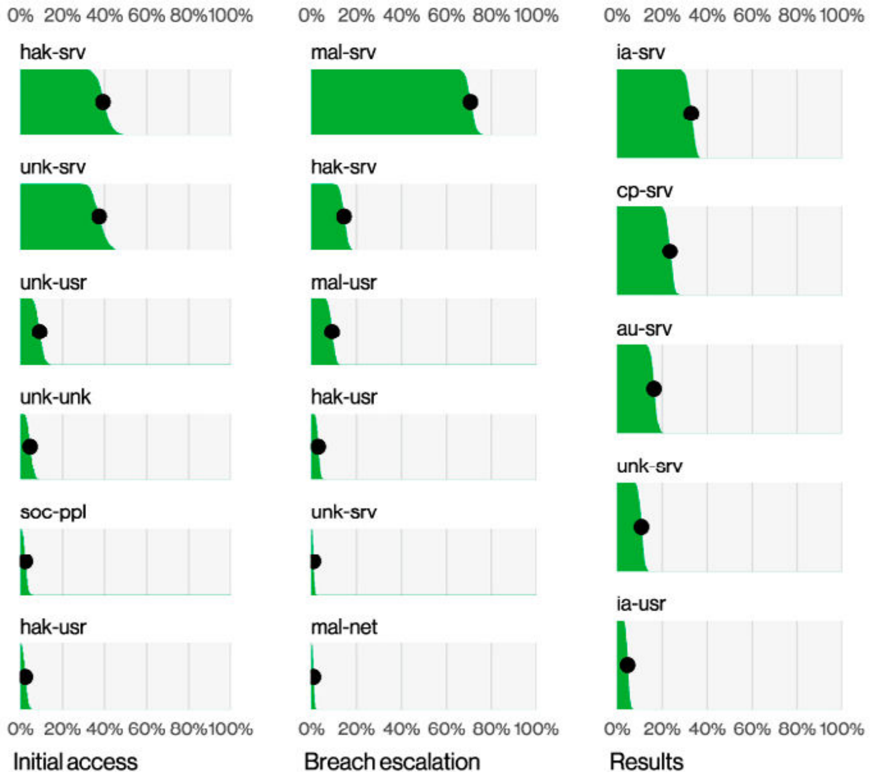


Figure 27. Steps in System Intrusion breaches

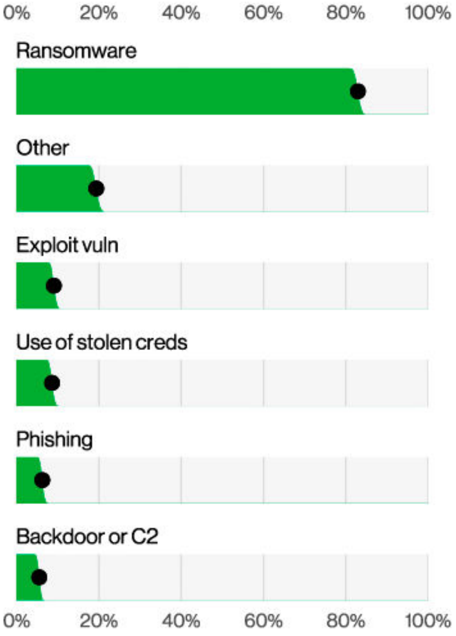


Figure 28. Action varieties in System Intrusion incidents (n=2,700)

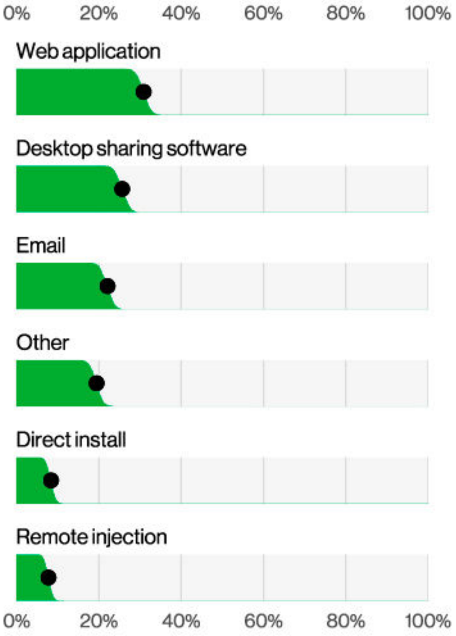


Figure 29. Action vectors in System Intrusion incidents (n=787)

Jiggling locks

When looking at Figure 27, we see the clear leaders for the initial access – a great deal of hacking servers and an almost equal amount of unknown actions. In terms of hacking, 9% of incidents involve Exploiting vulnerabilities and 8% involve the Use of stolen credentials. When we examine only our incidents that contain the exploitation of vulnerabilities, we find those vulnerabilities are largely exploited via Web applications (Figure 29).

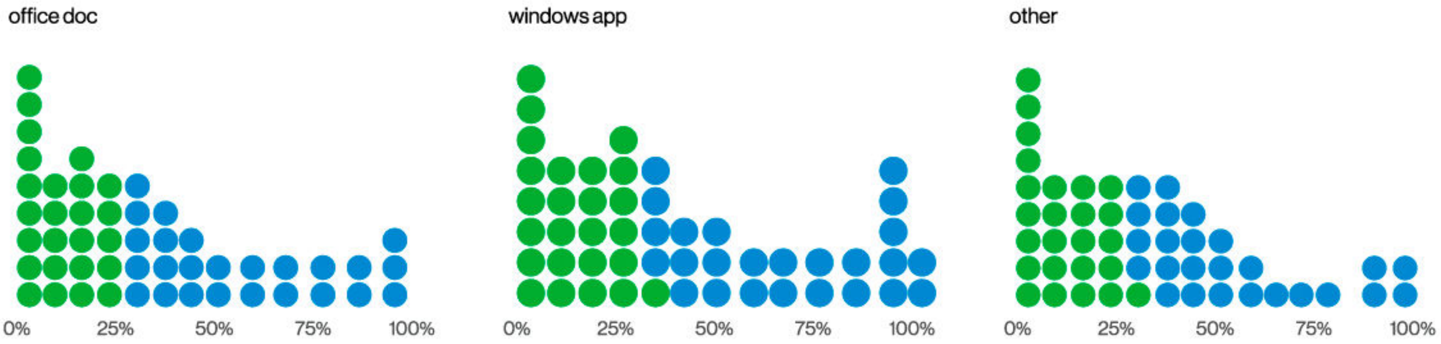
In addition, we see some User devices being directly targeted, and we also observe Phishing in roughly 6% of cases. Phishing provides just another means of ingress, either to get a set of usable credentials or to deploy a payload on a user system. Malware is largely distributed via email and often comes in the form of Microsoft Office documents (see Figure 30). This makes sense when you consider that most of these documents now have the ability to run code on the client system, which is extremely useful if you're an attacker.

Admittedly, there are many cases in which we do not know the exact means of entry the attacker used. However, these pathways of Exploiting vulnerabilities, Using stolen credentials and Phishing are very similar to previous years' findings, and let's face it, they are straight out of InfoSec 101. This again demonstrates the importance of the fundamentals.

Well, that escalated quickly.

Once attackers have access to your environment, they will typically look for ways to escalate privileges, maintain persistence and locate paths to move across the organization to achieve their ultimate goal, whatever that may be. For those ATT&CK aficionados out there, you may be thinking this

Malware file types (n=1,756)



Malware delivery methods (n=1,069)

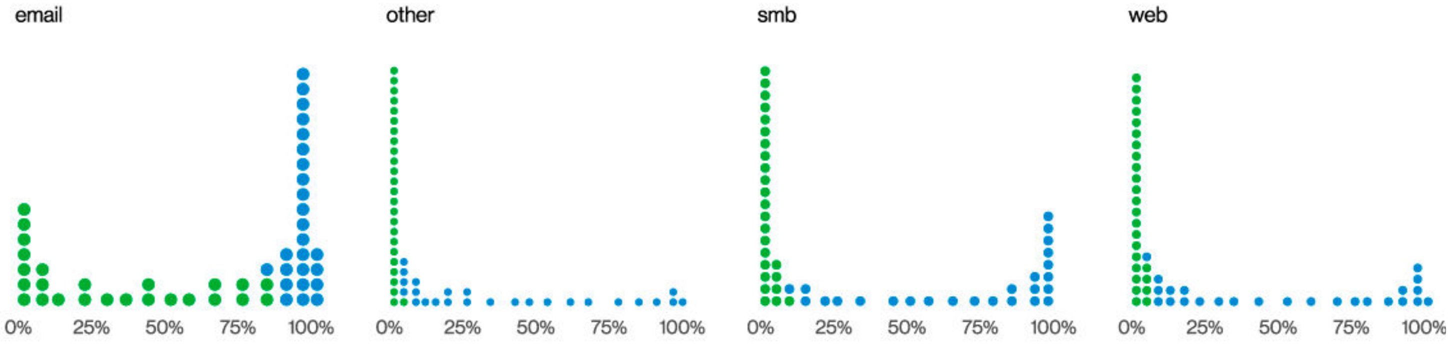


Figure 30. Malware delivery method proportion per organization

sounds like we're talking about a big chunk of that matrix. Well, we are. While we have a higher view of the incidents, we do not always have the telemetry required to find out exactly what techniques were used. However, below we discuss some of the additional hacking techniques and malware capabilities that we can track.

Malware that maintains command and control (C2) access to the system was witnessed in about 5% of incidents. Also present are the more typical types of malware that profile hosts, scan networks and (a local favorite) dump passwords. Lastly, just in case you thought the 2010s were behind us, we even found a handful of crypto miners in this dataset. There were not enough for us to confirm that they are back en vogue, but definitely enough to confirm that certain parties still consider compromised servers as free real-estate from which to mine.

Results

With such a high reliance upon the installation of malware across this pattern (either in the form of Ransomware, backdoors or payment card skimming malware) we shouldn't be too surprised when we find servers that have illicit software installed as the most common combination of Attribute and Asset. The second most common is the exfiltration of data, and rounding out the trio is the loss of availability, aka rendering your data unreadable. These top three describe the final steps associated with many of these attacks quite well—attackers find a way to install their payload across the organization, steal data and then encrypt the systems on their way out.

Ransomware ... seriously, we're still doing this section?

Ransomware continues to be a major threat for organizations of all sizes and industries and is present in 24% of breaches. Of those cases, 94% fall within System Intrusion. While Ransomware has increased only slightly this year, it is so ubiquitous that it may simply be a threat that we will always have to protect against—91% of our industries have Ransomware as one of their top three actions.

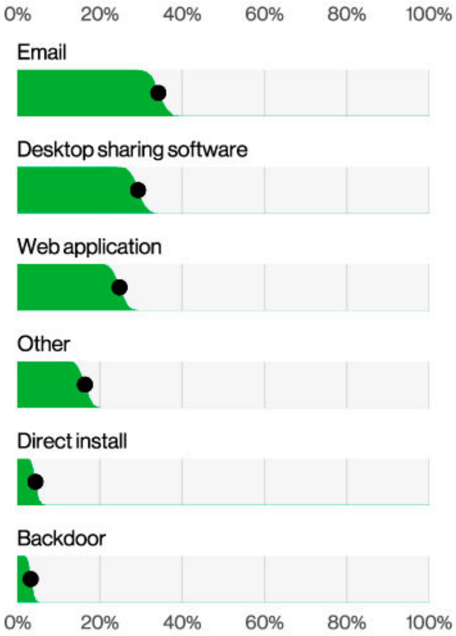


Figure 31. Action vectors for Ransomware (n=690)

To understand how these attacks occur, it is often useful to look at the top Vectors for the actions. In this case, the most common ways in are Email, Desktop sharing software and Web applications (Figure 31). Email as a vector isn't going away any time soon. The convenience of sending your malware and having the user run it for you makes this technique timeless. The next most common vector, Desktop sharing software, makes sense, since these breaches and incidents frequently leverage some means of accessing a system. What better way to do that than by using a built-in tool such as RDP or a third-party version to provide the criminal mastermind a nice GUI?

Splitting the Log4j

As we DBIR authors groggily awoke from our hyperbolic slumber to start collecting and writing about all the major happenings in the cybersecurity world, we saw yet another major cybersecurity event had slowly played out after the cutoff of our data collection. This occurred first in 2020, with SolarWinds,[31] and history has repeated itself in 2021 with Log4j,[32] opening what seems to be a Pandora's box of vulnerabilities. However, there is one advantage to waiting—we get to watch as the dust settles and provide an objective analysis as to what actually occurred. There was a great deal of uncertainty and complexity surrounding the incidents involving the Log4j vulnerability. One of which was the fact that no one really understood the full scope of the breach as it was not simply in one software product but was actually in a library used by numerous applications and programs (both purchased and open sourced.)

A quick recap of the event is perhaps warranted to refresh everyone's memory. The vulnerability was disclosed in late November 2021, and within a few days the first exploitations began to appear. The vulnerability, given the designation of CVE-2021-44228, was given a whopping criticality score of 10.[33] By the end of December, 0.003% of the scanning activity captured by honeypots were actively poking and prodding for this specific vulnerability. While that number might seem small, the velocity was rather striking, with more than 32% of all Log4j scanning activity over the course of the year happening within 30 days of its release (the biggest spike of activity occurred within 17 days, as Figure 32 shows). This velocity is an interesting comparison versus organizations' median time to patch, which is currently 49 days for critical vulnerabilities, a number that has stayed relatively consistent over the years.

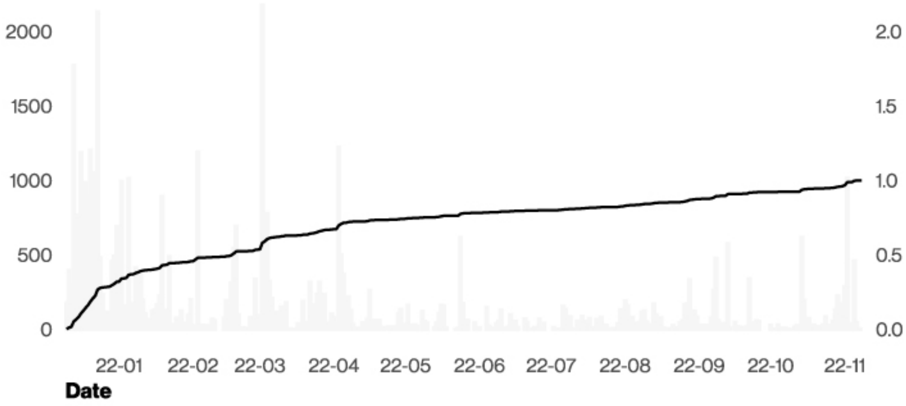


Figure 32. Percentage of Log4j scanning for 2022

However, it may not have been as big of a disaster as many predicted. When examining the DBIR incident dataset, we actually saw a decrease of vulnerability exploitation leading to incidents and breaches, with Log4j being mentioned in 0.4% of our incidents (just under a hundred cases). However, when examining these cases, we found that Log4j was used by a variety of actors to achieve an assortment of different objectives, with 73% of our cases involving Espionage and 26% involving Organized crime. Given the nature of the vulnerability, allowing remote code execution, we predictably saw a lot of malware activity associated with it, such as Backdoors and Downloaders to pull in additional hosts. Finally, in about 26% of the cases, we saw the exploit of Log4j being leveraged as part of Ransomware attacks, which only goes to show that attackers will leverage whatever beachhead they can get.

Based on some of the vulnerability scanning data we analyzed (as in the good folks scanning for vulnerabilities, not the bad ones) we found that vulnerable Log4j showed up in 8% of organizations. And in other somewhat surprising news, we also found that there was a greater percentage of Log4j installations that were end of life (EOL) with 14% of organizations, even if they weren't actually vulnerable to Log4j explicitly. Lastly, 22% of the organizations had multiple (i.e., more than one) instances of the Log4j vulnerability in their systems.

This underlying vulnerability in a dependency has brought back the discussion around having a software bill of materials (SBOM). You may think that SBOM is a term kids are throwing around in between their "no caps" and "bussin," but its goal is to help organizations understand all the ingredients (software packages and libraries) that go into making the software their organization relies upon. Having a mature SBOM process across their ecosystem enables organizations to quickly identify vulnerabilities within the underlying libraries and help with future remediation processes for something like Log4j.

---

[31] https://www.cisa.gov/news-events/news/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network

[32] https://www.cisa.gov/news-events/news/cisa-issues-emergency-directive-requiring-federal-agencies-mitigate-apache-log4j

[33] Though insiders have indicated that it could have gone up to 11.

CIS Controls for consideration

Bearing in mind the breadth of activity found within this pattern and how actors leverage a wide collection of techniques and tactics, there are a lot of safeguards that organizations should consider implementing. A small subset—including the CIS Control Number—is below, which should serve as a starting point for building out your own risk assessments to determine what controls are appropriate to your organization's risk profile.

Protecting devices

Secure Configuration of Enterprise Assets and Software [4]
- Establish and Maintain a Secure Configuration Process [4.1]
- Establish and Maintain a Secure Configuration Process for Network Infrastructure [4.2]
- Implement and Manage a Firewall on Servers [4.4]
- Implement and Manage a Firewall on End-User Devices [4.5]

Email and Web Browser Protection [9]
- Use DNS Filtering Services [9.2]

Malware Defenses [10]
- Deploy and Maintain Anti-Malware Software [10.1]
- Configure Automatic Anti-Malware Signature Updates [10.2]

Continuous Vulnerability Management [7]
- Establish and Maintain a Vulnerability Management Process [7.1]
- Establish and Maintain a Remediation Process [7.2]

Data Recovery [11]
- Establish and Maintain a Data Recovery Process [11.1]
- Perform Automated Backups [11.2]
- Protect Recovery Data [11.3]
- Establish and Maintain an Isolated Instance of Recovery Data [11.4]

Protecting accounts

Account Management [5]
- Establish and Maintain an Inventory of Accounts [5.1]
- Disable Dormant Accounts [5.3]

Access Control Management [6]
- Establish an Access Granting/Revoking Protocol [6.1]
- Require MFA for Externally-Exposed Applications [6.3]
- Require MFA for Remote Network Access [6.4]

Security awareness programs

Security Awareness and Skills Training [14]

Just one more (Ransomware) note

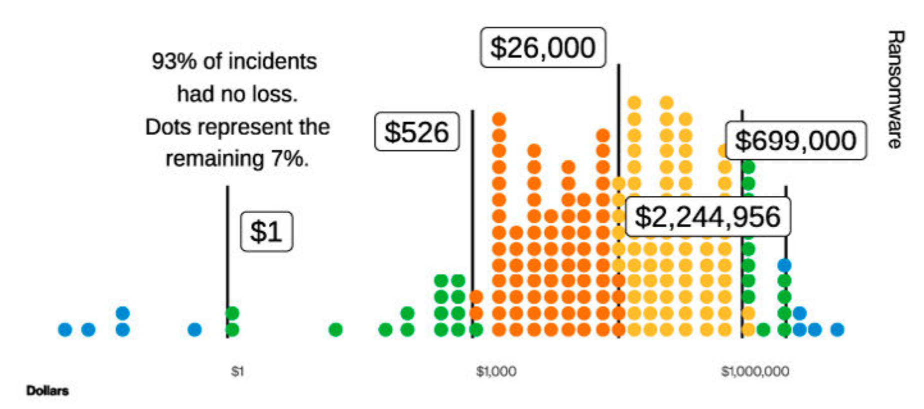


Figure 33. 95% and 80% confidence intervals of Ransomware incident cost per complaint (n=2,575)

Since we are hot on the subject of ransomware, we thought it would be interesting to revisit the breach impact data provided by our partner, the FBI Internet Crime Complaint Center (IC3).[34]

When we last reviewed this data in the 2021 DBIR, we found that 90% of the incidents reported to the IC3 had no financial loss result, but for the remaining 10%, the median amount lost was $11,500, and the range of losses in 95% of the cases were between $70 and $1.2 million.

In reviewing Figure 33, of the incidents with loss, the calculated median more than doubled to $26,000, and the 95% range of losses expanded to sit between $1 and $2.25 million, putting that upper bound in scarier territory if you are a small business. The FBI did find that only 7% of the incidents had losses in this case, so it's not all bad news.

Now, before any one of you makes a snarky quip about inflation and the base rate of the economy, here is the unusual part: When combining the paid-out transactions to the threat actors on the same time period, we get a much smaller median—$10,000 (Figure 34), and this median is actually less than the two previous years when the DBIR team has had access to this dataset.

What this suggests is that the overall costs of recovering from a ransomware incident are increasing[35] even as the ransom amounts are lower. This fact could be suggesting that the overall company size of ransomware victims is trending down. Even though the amounts requested by the threat actors would be smaller for those smaller companies—they want to get any money they can—the added costs of recovering their IT infrastructure under a backdrop of likely technical debt would spike their overall losses.

This is conjecture, as we don't have the company size data and not all complaints have the associated transaction value data in this specific dataset. Even so, this is a result we have been expecting to see due to the increase of automation and efficiency of ransomware operators. Regardless, it's fair to say that an ounce of prevention is worth a pound of cure,[36] so we cannot emphasize enough the need of having a plan and/or incident response resources at the ready ahead of your next unscheduled encryption event.

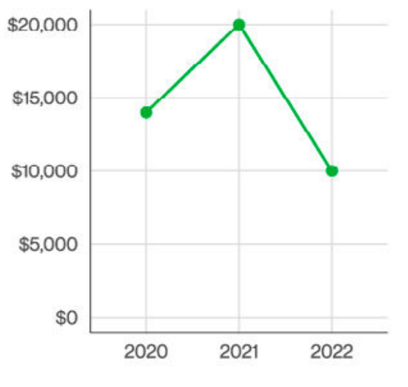


Figure 34. Median transaction size for Ransomware based on FBI IC3 complaints

---

[34] https://www.ic3.gov

[35] Feel free to make that inflation joke now.

[36] This sentence was famously said by a man who flew a kite with a key in a thunderstorm. Makes you think.

Social Engineering

Summary

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. Compounding the frequency of these attacks, the median amount stolen from these attacks has also increased over the last couple of years to $50,000.

What is the same?

Phishing and Pretexting continue to dominate this pattern, thus ensuring that email remains one of the most common means of influencing individuals.

Frequency	1,700 incidents, 928 with confirmed data disclosure
Threat actors	External (100%), Multiple (2%), Internal (1%), Partner (1%) (breaches)
Actor motives	Financial (89%), Espionage (11%) (breaches)
Data compromised	Credentials (76%), Internal (28%), Other (27%), Personal (26%) (breaches)

Relevant ATT&CK techniques

Compromise Accounts: T1586
  – Email Accounts: T1586.002

Establish Accounts: T1585
  – Email Accounts: T1585.002

External Remote Services: T1133

Internal Spearphishing: T1534

Phishing: T1566
  – Spearphishing Attachment: T1566.001
  – Spearphishing Link: T1566.002
  – Spearphishing via Service: T1566.003

Phishing for Information: T1598
  – Spearphishing Service: T1598.001

Use Alternate Authentication Material: T1550
  – Application Access Token: T1550.001

Valid Accounts: T1078
  – Domain Accounts: T1078.002

Professional engineers?

Engineering is a beautiful combination of math and physics applied to a practical and meaningful end—or so we're told. However, much to our parents' disappointment, most of us are not engineers, but only an infinite collection of monkeys tied to typewriters. (Legend has it we will compose "Hamlet" by pure chance any day now. Watch your back, GPT-4.)

However, this section is about another, not-so-useful-to-society, form of engineer—the social engineer. This pattern focuses on tactics used by threat actors that leverage our innate helpful nature to manipulate and victimize us. These attackers use a combination of strategies to accomplish this: by creating a false sense of urgency for us to provide a reply or to perform an action, a fake petition from authority, or even hijacking existing communication threads to convince us to disclose sensitive data or take some other action on their behalf. Social engineering has come a long way from your basic Nigerian Prince scam to tactics that are much more difficult to detect. This increased sophistication explains why Social Engineering continues to rise and currently resides in our top three patterns (accounting for 17% of our Breaches and 10% of Incidents).

Please use this bank account number going forward.

There is a common misconception when it comes to distinguishing phishing from the more complex forms of social engineering. Raise your hand if you haven't received an email with a dubious attachment or a malicious link requesting that you update your password. Nobody? Yeah, that's what we thought. This is phishing, and it makes up 44% of Social Engineering incidents. Now, who has received an email or a direct message on social media from a friend or family member who desperately needs money? Probably fewer of you. This is social engineering (pretexting specifically) and it takes more skill. The most convincing social engineers can get into your head and convince you that someone you love is in danger. They use information they have learned about you and your loved ones to trick you into believing the message is truly from someone you know, and they use this invented scenario to play on your emotions and create a sense of urgency. Figure 35 shows that Pretexting is now more prevalent than Phishing in Social Engineering incidents. However, when we look at confirmed breaches, Phishing is still on top.

One of the more complex social attacks is the BEC. In these pretexting attacks, actors leverage existing email threads and context to request that the recipient conduct a relatively routine task, such as updating a vendor's bank account. However, the devil is in the details, and the new bank account belongs to the attacker, so all payments the victim makes to that account will make zero dents in what they owe that vendor. These types of attacks are often much harder to detect due to the groundwork laid by the threat actors prior to the attack. For example, they might have spun up a look-alike domain that closely resembles that of the requesting party and possibly even updated the signature block to include their number instead of the vendor they're pretending to represent. These are just two of the numerous subtle changes that attackers can make in order to trick their marks—especially those who are constantly bombarded with similar legitimate requests. Perhaps this is one of the reasons BEC attacks have almost doubled across our entire incident dataset, as can be seen in Figure 36, and now represent more than 50% of incidents within this pattern.

Attack type doesn't appear to have much of an effect on click/open rate. The median fail rates for attachment and link campaigns are 4% and 4.7% respectively, and the median click rate for data entry campaigns is 5.8% (though the data entry rate is 1.6%).

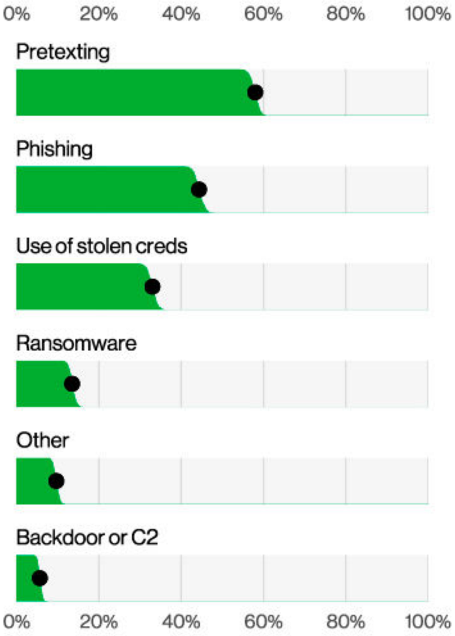


Figure 35. Action varieties in Social Engineering incidents (n=1,696)

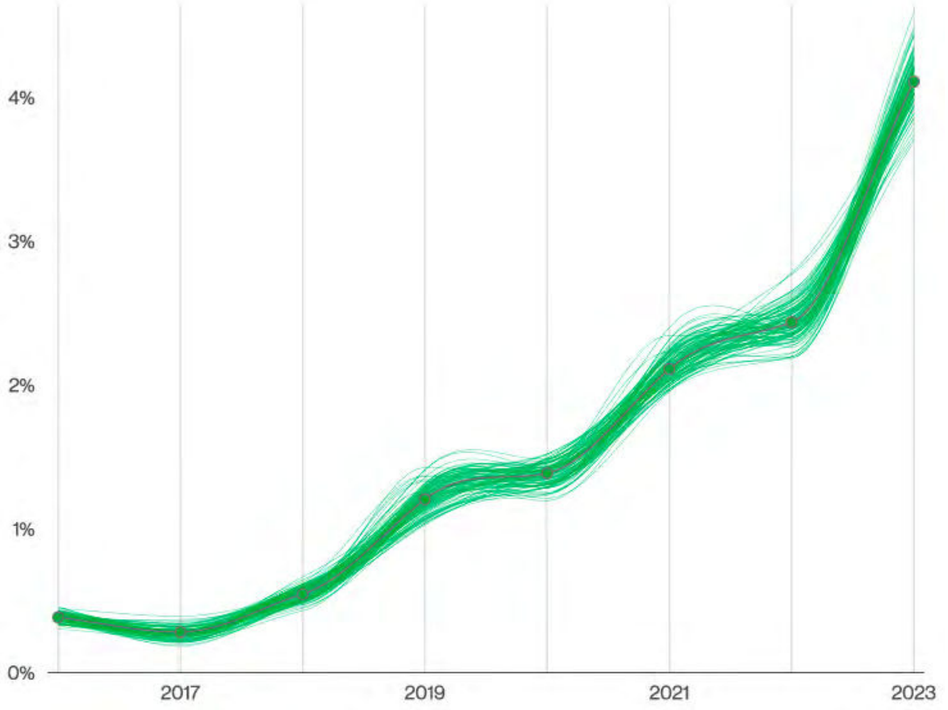


Figure 36. Pretexting incidents over time

Inconspicuous beginnings

Because this pattern is largely based on human-targeted attacks, it makes sense that the very first action in this pattern will be some form of phishing or pretexting email (Figure 37). In fact, email alone makes up 98% of the vector for these incidents, with the occasional sprinkling of other communication methods, such as phone, social media or some internal messaging app that some folks might be Slacking off on (cough, cough).

Two paths diverged, etc., etc.

What happens after that initial email is where things often diverge. There are two major routes that the attacks typically take. Most commonly, if the attackers are soliciting credentials and obtain them, then they will leverage those credentials to access the user's inbox (found in 32% of incidents). The road less traveled is where—by simply using email communication—the attackers are able to spin a credible story (albeit fictitious) to convince someone to do their bidding. Persuading someone to change the bank account for the claimed recipient, for example, is found in 56% of incidents. Of course, a combination of tactics can also be used. The attackers may leverage their acquired access to a user's inbox to look for an email chain they can hijack or search the victim's address book to find people who can be targeted further. It's not uncommon for attackers to add forwarding rules to make sure their activities stay undetected as long as possible, which is why ...

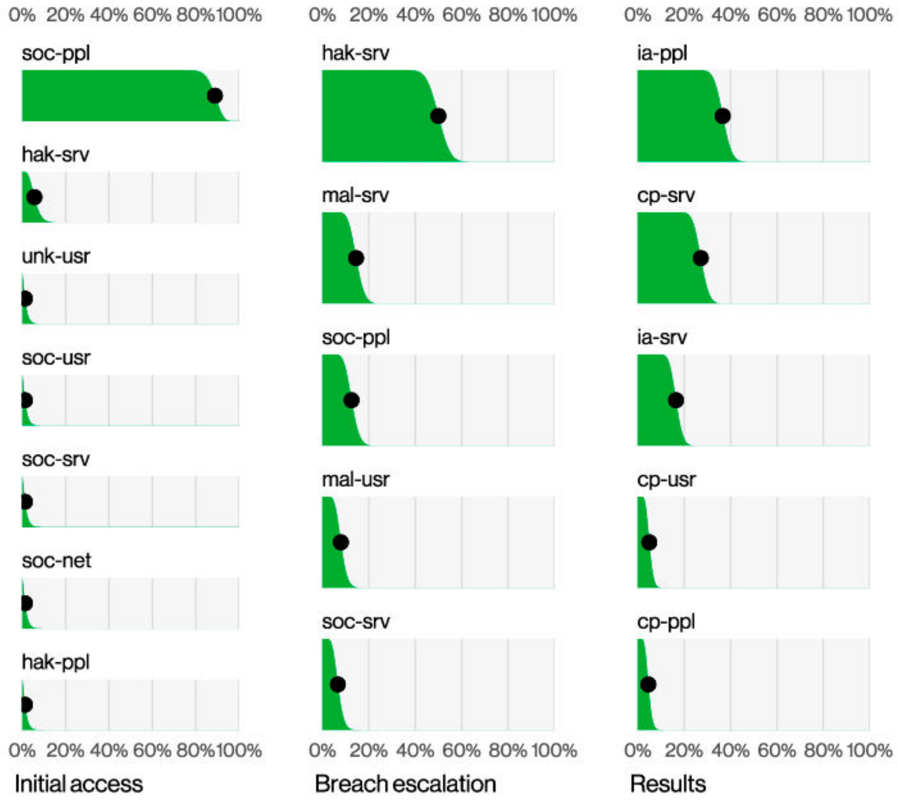


Figure 37. Steps in Social Engineering breaches

Time is of the essence.

When responding to social engineering attacks (and the same could be said of most attacks), rapid detection and response is key. The importance of timely detection is highlighted by the increasing median cost of BECs, as shown in Figure 38, which has risen steadily from 2018 and now hovers around the $50,000 mark. However, unlike the times we live in, this section isn't all doom and gloom. Fortunately for the victims, law enforcement has developed a process by which they collaborate with banks to help recover money stolen from attacks such as BEC. More than 50% of victims were able to recover at least 82% of their stolen money. This illustrates the importance of ensuring that their employees feel comfortable reporting potential incidents to security, since their willingness to do so greatly improves the organization's ability to respond. With this in mind, we encourage companies to step away from the "phishing exercises will continue until click rates improve" stance and adopt a more collaborative approach to security.

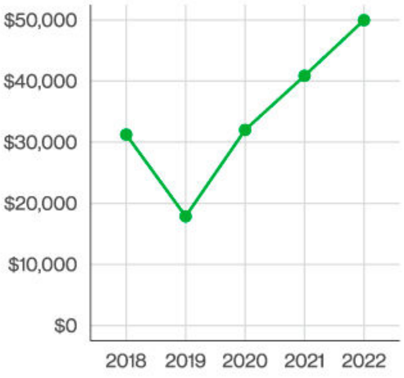


Figure 38. Median transaction size for BECs (n=73,420). Based on FBI IC3 complaints where a transaction occurred.

CIS Controls for consideration

There are a fair number of controls to consider when confronting this complex threat, and all of them have pros and cons. Due to the strong human element associated with this pattern, many of the controls pertain to helping users detect and report attacks as well as protecting their user accounts in the event that they fall victim to a phishing lure. Lastly, due to the importance of the role played by law enforcement in responding to BECs, it is key to have plans and contacts already in place.

Why do BECs work?

Much like Ransomware, which is the monetization of access to an organization's network, BECs are just one of the many means criminals have of monetizing access to a user's inbox and contacts.

- BECs can be targeted internally, meaning that the attacker will leverage a compromised employee's email account to target their own organization by impersonating the user. We commonly see actors trying to redirect payroll deposits into an account they control.
- Alternatively, actors can target partners by using access to an employee's email account, so they can impersonate that user and request updates to payments in order to include their own bank account.

Protect accounts

Account Management [5]
  - Establish and Maintain an Inventory of Accounts [5.1]
  - Disable Dormant Accounts [5.3]

Access Control Management [6]
  - Establish an Access Granting Process [6.1]
  - Establish an Access Revoking Process [6.2]
  - Require MFA for Externally-Exposed Applications [6.3]
  - Require MFA for Remote Network Access [6.4]

Security awareness programs

Security Awareness and Skills Training [14]

Although not part of the CIS Controls, a special focus should be placed on BEC and processes associated with updating bank accounts.

Managing incident response

Incident Response Management [17]
  - Designate Personnel to Manage Incident Handling [17.1]
  - Establish and Maintain Contact Information for Reporting Security Incidents [17.2]
  - Establish and Maintain an Enterprise Process for Reporting Incidents [17.3]

Basic Web Application Attacks

Summary

While representing approximately one-fourth of our dataset, these breaches and incidents tend to be largely driven by attacks against credentials, with the attackers then leveraging those stolen credentials to access a variety of different resources.

What is the same?

Poorly picked and protected passwords continue to be one of the major sources of breaches within this pattern.

Frequency	1,404 incidents, 1,315 with confirmed data disclosure
Threat actors	External (100%), Internal (1%), Multiple (1%) (breaches)
Actor motives	Financial (95%), Espionage (4%), Fun (1%) (breaches)
Data compromised	Credentials (86%), Personal (72%), Internal (41%), Other (19%) (breaches)

Relevant ATT&CK techniques

Brute Force: T1110
- Credential Stuffing: T1110.004
- Password Cracking: T1110.002
- Password Guessing: T1110.001
- Password Spraying: T1110.003

Compromise Accounts: T1586
- Email Accounts: T1586.002

Exploit Public-Facing Application: T1190

External Remote Services: T1133

Valid Accounts: T1078
- Default Accounts: T1078.001
- Domain Accounts: T1078.002

Use Alternate Authentication Material: T1550
- Application Access Token: T1550.001

Active Scanning: T1595
- Vulnerability Scanning: T1595.002

Who dunnit?

While it may liven up our humdrum existence to imagine the threat actors behind breaches as characters from a game of Clue (the cyber version),[37] it is more likely to have been an average Jane Doe using stolen credentials or some well-known vulnerability.

This pattern, which accounts for 25% of our breaches, consists largely of leveraging stolen credentials and vulnerabilities to get access to an organizations' assets. With this beachhead, the attackers can then do a variety of things, such as stealing key information hiding in emails or taking code from repositories. While these attacks aren't complicated, they certainly are effective and have remained a relatively stable part of our dataset, which prompts us to discuss once again (drum roll, please), the importance of multifactor authentication (MFA) and patch management![38]

---

[37] Was the breach caused by the mysterious Spiderlady via a complicated zero day on an internet-facing server? Or was it perpetrated by the Sophisticated Panda using drones inside a Kubernetes cluster?

[38] Yes, it is the "Groundhog Day" of InfoSec topics. I bet you can find it in our past reports!

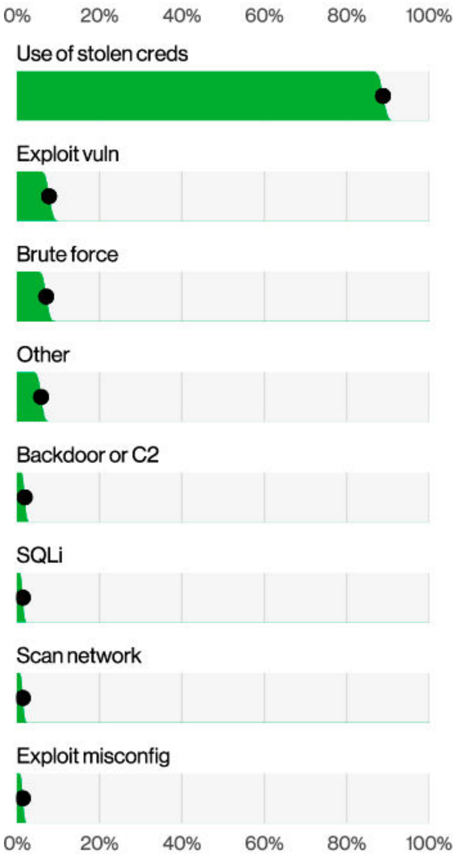


Figure 39. Top Action varieties for Basic Web Application Attacks breaches (n=1,287)

Initial access

86% of the breaches, as you can see in Figure 39, involve the Use of stolen credentials. And where better to use those credentials than against the various web servers that contain our sensitive information? The other major part of the puzzle within this pattern is the use of exploits. This is where attackers have an exploit and the victims just happen to have a vulnerability (handy for the criminal). This typically occurs in only about 10% of the dataset, and while that may sound like an insignificant number of breaches, unpatched vulnerabilities are still the bread and butter for many attackers, with 50% of organizations experiencing over 39 Web application attacks this year.[39]

Breach escalation

Even though we refer to these attacks as "basic," they're not simply "one and done" incidents where credentials are leveraged against a web application and the attacker then goes on their merry way. There is often some sort of middle step (Figure 40). For instance, malware is frequently one of the primary means of maintaining persistence (look at us, using them fancy ATT&CK terms), with Backdoor or C2 in about 2% of the incidents. In other cases, the attackers will leverage their current access to conduct additional attacks.

---

[39] One of the advantages to running these types of attacks is that the server never tires, never sleeps, it just throws exploits at everyone continually, night and day – unlike your humble cybersecurity analyst who needs at least four coffees a day and nine hours of sleep.

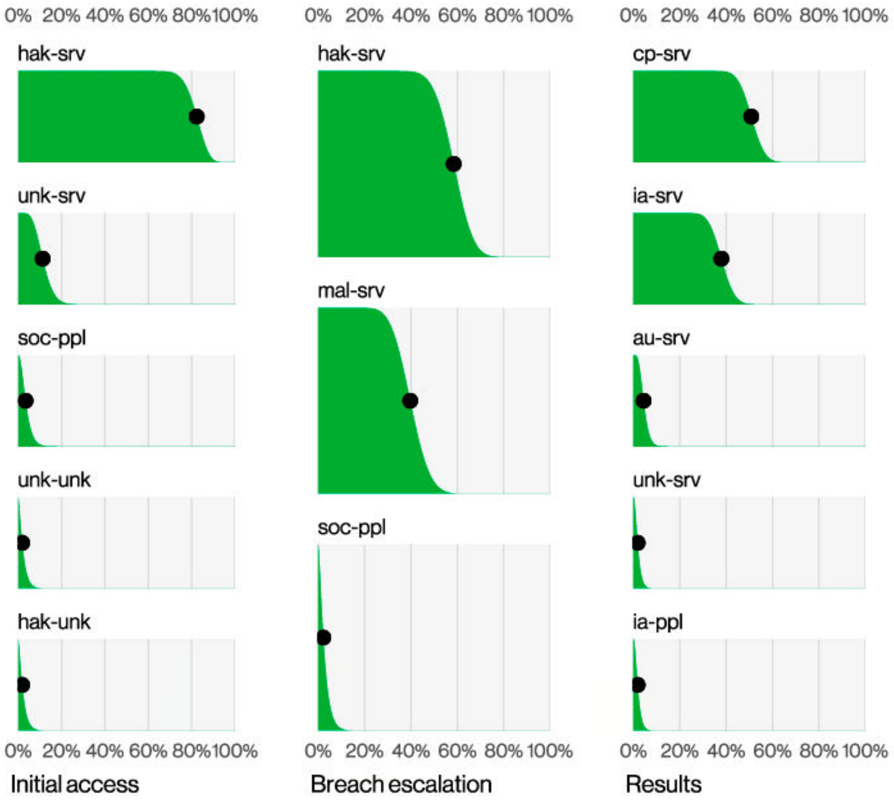


Figure 40. Steps in Basic Web Application Attacks

Impacts

With regard to impact, we commonly see that after Web applications, Mail servers are one of the preferred targets for attackers. This makes sense, because hidden away in our inboxes among the hundreds of unread emails[40] there are often key internal documents (41% of breaches involve mail servers) or, sadly, credentials to some other system. The findings for this pattern show that attackers can access Internal data (41%), Medical data (6%) and even Banking data (6%) using simple inbox mining tactics (again, reminding us of the importance of good email and server hygiene).

---

[40] Sorry, Grandma.

You can't eat just one.

One thing you probably don't hear often is someone saying, "If I only had more usernames and passwords to remember." Credentials are as ubiquitous as sand in the desert and almost as hard to hold onto. Threat actors seem to have a plentiful supply as well. However, what is missing in our data, and we try to be explicit when it comes to biases and limitations, is that we don't necessarily know where all these credentials are coming from. But we here on the DBIR team love a good mystery. Did the butler do it? Are aliens real? What about the Yeti? Ghosts? People with strong work ethics? Alas, we will probably never know. We may also never know where the criminals obtained the credentials in the first place. We might have a good idea in terms of the different ways that one would be capable of getting credentials, such as buying them from password stealers who are nabbing them through social engineering or even spraying them in a brute force attack. What we don't have is the exact breakdown of how many of our breaches and incidents are caused by each. As the old adage goes "What we know is a drop; what we don't know is an ocean."

It's not all bad news, however. Even though there are many ways to steal credentials, we have many ways to protect them as well. One of the best ways (stop me if you have heard this one before) is the use of MFA. Before you recline in your chair and "Well, ACKtually …" us, we do realize there are limitations to some MFA implementations. As you're undoubtably aware, some very high profile breaches this year demonstrated some of those shortcomings. In some cases, criminals used social engineering to convince users to accept the authentication attempts. In other instances, they stole the session cookie and used it to masquerade as the user. Of course, some MFA bypasses weren't really bypassing MFA because some of the services weren't properly configured to ONLY use MFA. As mentioned above, what we can't really tell you at this time is how much there were of each, as we need to both update our standard VERIS and collect the data. While this would be an awesome opportunity for us to finally settle the score and discuss which MFA is better and which bypasses are leveraged the most, we will have to keep this placeholder for another year.

Quote from Jen Easterly

Director
U.S. Cybersecurity and Infrastructure Security Agency

As the Nation's Cyber Defense Agency, the Cybersecurity and Infrastructure Security Agency (CISA) sees how our nation's adversaries operate and what tools they use. While some of these adversaries use advanced tools and techniques, most take advantage of unpatched vulnerabilities, poor cyber hygiene or the failure of organizations to implement critical technologies like MFA. Sadly, too few organizations learn how valuable MFA is until they experience a breach.

Since joining CISA, I've made it a priority to raise MFA awareness across all sectors to better protect our nation's critical infrastructure. Importantly, we need more and better data to understand the scope of, and solutions to, the threats we face in cyber, and we've called on our industry partners to provide radical transparency to allow our defenders to better see, understand and ultimately protect our citizens, customers and companies. In particular, it's critical that "high-value targets" like system administrators and Software as a Service (SaaS) staff use phishing-resistant MFA.

But more and better information is just the beginning.

Working collaboratively, I look forward to seeing what we can do to together to make our nation more resilient, more secure, and to show measurable progress … including in next year's Verizon Data Breach Investigations Report.

CIS Controls for consideration

Mitigating against stolen credentials by protecting accounts

Account Management [5]
- Establish and Maintain an Inventory of Accounts [5.1]
- Disable Dormant Accounts [5.3]

Access Control Management [6]
- Establish an Access Granting Process [6.1]
- Establish an Access Revoking Process [6.2]
- Require MFA for Externally-Exposed Applications [6.3]
- Require MFA for Remote Network Access [6.4]

Mitigating against vulnerability exploitation

Continuous Vulnerability Management [7]
- Establish and Maintain a Vulnerability Management Process [7.1]
- Establish and Maintain a Remediation Process [7.2]
- Perform Automated Operating System Patch Management [7.3]
- Perform Automated Application Patch Management [7.4]

If you happen to be interested in how we updated VERIS to capture attacks that bypass MFA, look no further than the list below:

1. Added a new Action to indicate the take-over of a secondary authentication mechanism (hijack)
2. Added a new data variety—Multifactor credential—to indicate whether the other factors, aside from credentials, were captured
3. Added the social variety of Prompt Bombing[41] for those attacks that target sending annoying levels of authentication requests to users

Hopefully, the combination of our existing enumerations, along with these new ones, will capture the majority of the cases we encounter. If not, we will re-examine our enumerations with the next version of VERIS.

---

[41] This sounds like what you would call someone who photobombs people in a timely manner, doesn't it?

Miscellaneous Errors

Summary

Misdelivery, Misconfiguration and Publishing errors continue to be the headliners, and the errors that lead to breaches are most often committed by System admins and Developers.

What is the same?

Employees continue to make mistakes, and sometimes they result in considerable damage to their organizations.

Frequency	602 incidents, 512 with confirmed data disclosure
Threat actors	Internal (99%), Partner (2%), Multiple (1%), External (1%) (breaches)
Data compromised	Personal (89%), Medical (19%), Other (10%), Bank (10%) (breaches)

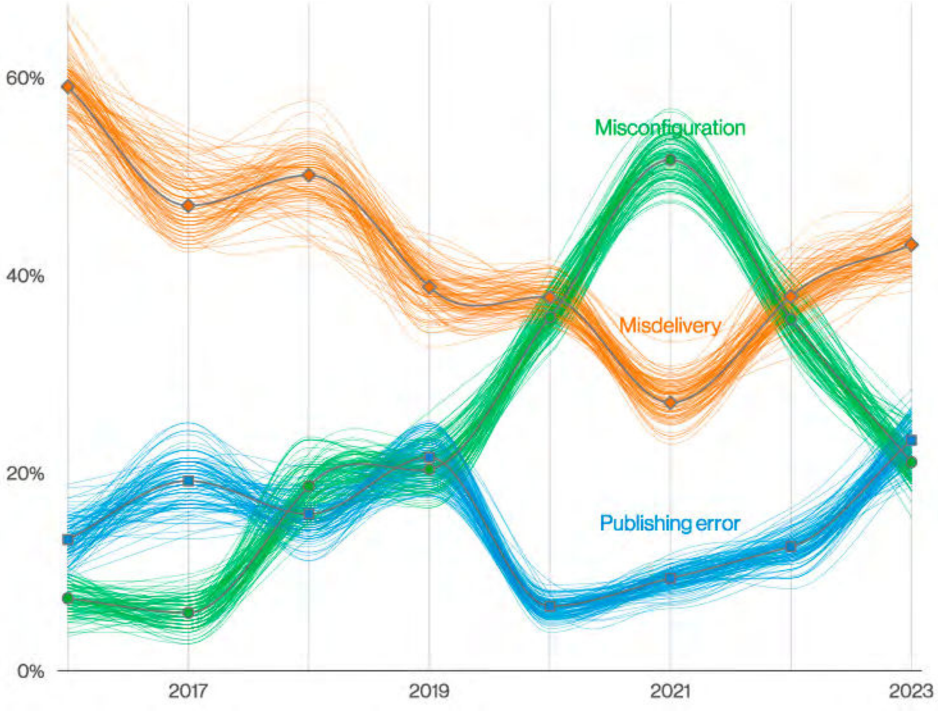


Figure 41. Action varieties over time in Miscellaneous Errors breaches

You can't find good help these days.

The great English poet and essayist, Alexander Pope once quipped, "It is hard to hire people who don't screw things up." Well, it was something more or less along those lines—just take our word for it. Regardless of who said (or did not say) what, the Miscellaneous Errors pattern continues to comprise a decent chunk of our breach data. If you are a "glass half full" kind of reader, you may take comfort in the fact that this year, error-related breaches are down to 9% as opposed to 13% last year. If you are a "glass half empty" reader, you may simply attribute it to reporting since last year we had 715 error incidents and 708 with confirmed data disclosure as opposed to 602 incidents, with 512 confirmed breaches this year.

It's my favorite mistake.

Perhaps "favorite" is too strong a word. Misdelivery (sending something to the wrong recipient) accounts for 43% of breach-related errors in our dataset (Figure 41). Publishing errors (showing something to the wrong audience) is in second place at 23%. Finally, Misconfiguration, the much-loved action type of the lazy person, comes in third and accounts for 21% of error-related breaches. This might tempt us to think that people are unreliable—perish the thought. However, you can rely on them to at least keep things interesting by switching up their mistakes to help keep you on your toes.

In fact, as Figure 41 illustrates, Misconfiguration and Misdelivery have ebbed and flowed over the last few years as if they were part of the choreographed dance of celestial bodies. In last year's report, Misdelivery and Misconfiguration converged, but this year Misdelivery is in the ascendancy,[42] whereas our old faithful dog, the Publishing error, is once again meeting Misconfiguration on its downward slope.

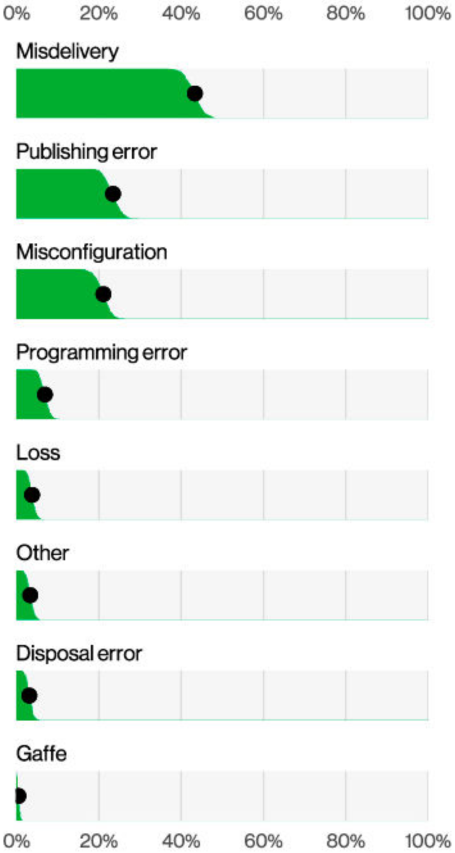


Figure 42. Top action varieties in Miscellaneous Errors breaches (n=450)

If we drill down a little deeper (Figure 42), it's easy to see that these three Error types have won the popularity contest by a wide margin. However, the team is saddened to see that Gaffe is always at or near the bottom (considering how many of those we make ourselves).

As illustrated in Figure 43, the majority of errors that lead to breaches are committed by Developers and System admins, along with a sprinkling of End-users. Given the Error action types that are most often found in breaches, it is hardly surprising that those who have more responsibility for maintaining the data and the upkeep of the environment are also those who are most frequently responsible. Speaking of responsibility, the error vector of Carelessness appeared in 98% of cases. Yikes! Maybe Pope was on to something.

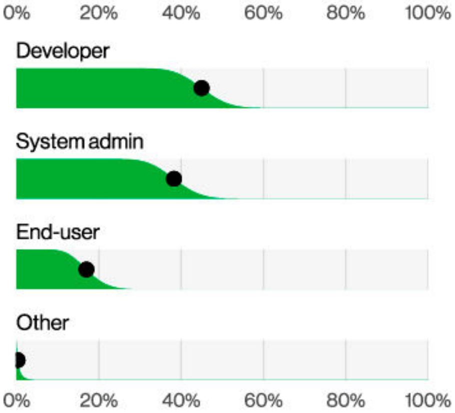


Figure 43. Top actor varieties in Miscellaneous Errors breaches (n=89)

CIS Controls for consideration

Control data

Data Protection [3]
- Establish and Maintain a Data Management Process [3.1]
- Establish and Maintain a Data Inventory [3.2]
- Configure Data Access Control Lists [3.3]
- Enforce Data Retention [3.4]
- Securely Dispose of Data [3.5]
- Segment Data Processing and Storage Based on Sensitivity [3.12]
- Deploy a Data Loss Prevention Solution [3.13]

Secure infrastructure

Continuous Vulnerability Management [7]
- Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets [7.6]

Application Software Security [16]
- Use Standard Hardening Configuration Templates for Application Infrastructure [16.7]
- Apply Secure Design Principles in Application Architectures [16.10]

Train employees

Security Awareness and Skills Training [14]
- Train Workforce on Data Handling Best Practices [14.4]
- Train Workforce Members on Causes of Unintentional Data Exposure [14.5]

Application Software Security [16]
- Train Developers in Application Security Concepts and Secure Coding [16.9]

[42] If you were born under the sign of Misdelivery you should expect good news soon. 3, 9, 13 and 33 are your lucky numbers.

Denial of Service

Summary

As Denial of Service continues to dominate our incidents, so do the capabilities of mitigation services. However, there has been a resurgence of low volume attacks that still cause issues to corporations.

Frequency	6,248 incidents, 4 with confirmed data disclosure
Threat actors	External (100%) (incidents)

What is the same?

Denial of Service attacks continue to be ubiquitous and have remained in the top spot of incidents for several years now.

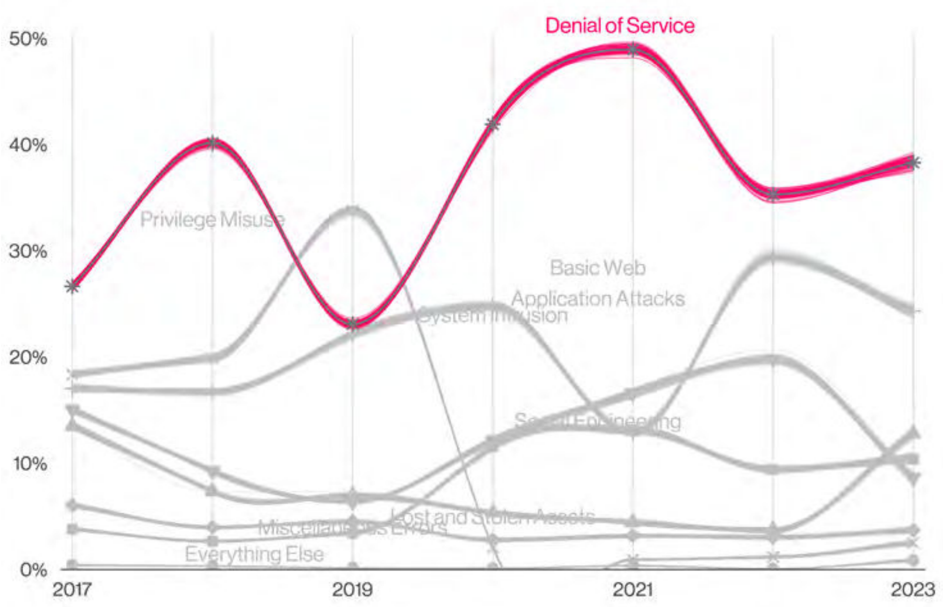


Figure 44. Patterns over time in incidents

We will not be denied.

As the name would imply, the Denial of Service pattern covers all of those attacks that try to keep you from streaming your next episode of "Below Deck," watching your next TikTok movie or loading your timeline on Twitter.[43] Sadly, all of this can obviously add up to the nuisance of having to acknowledge the real world and the people around us. We can all agree that would be terrible indeed.

However, as some of our readers may know, organizations still actually need the internet to be up and running in order to conduct business. Every year, DoS shows up as a huge volume of Incidents in our datasets, stemming from several different mitigation service partners, including Verizon's own. They are all doing an excellent job in preventing those Incidents from having any significant impact on organizations. In that light, even though the Denial of Service pattern has consistently taken the top spot in Incidents for the last several years (Figure 44), there is really not a lot of nuance to be discussed here, apart from our usual suggestion to invest in some sort of mitigation service if you care about the continued availability of your network presence on the internet. This is not due to a lack of nuance in the DDoS dataset overall but more a reflection of a lack of the typical details that we traditionally analyze such as Actors, Assets and Attributes.

---

[43] Not sure if we can blame our usual threat actors for this one.

Even so, it didn't feel right to deny our readers a Denial of Service section, as there are still important trends and information that are necessary to be reviewed. It's important to realize they're still there, even if you can easily solve them. Also, it is a respite to not have to write about Ransomware for a couple of pages.

We are going to need a bigger pipe.

One important point we should touch on is the growth of median and above median percentiles in bits per second of DDoS attacks (see Figure 45).[44] The median grew a whopping 57%[45] from 1.4 gigabytes per second (Gbps) last year to 2.2 Gbps now, and the 97.5 percentile grew 25% from 99 Gbps to 124 Gbps. This is to be expected as costs of bandwidth and CPU processing become more accessible and available and suggests a trend that is hard to break on escalating competition between the attackers and mitigating services. Just make sure your contracted service can clear that bar, and most of the impact will likely be absorbed. Let the machines fight it out Transformers-style and crack open a cold beverage while you worry about all the other attack patterns afflicting your corporation.

Even as the volume of garbage in our networks grows, some attacks have a more subtle touch. A point of attention that some of our partners brought to us was the growth of distributed DNS Water Torture[46] attacks in, you guessed it, shared DNS infrastructure. It is basically a resource exhaustion attack done by querying random name prefixes on the DNS cache server so it always misses and forwards it to the authoritative server. It is quite silly when you think of it, but it can be a heavy burden with some simple coordination by the threat actors'-controlled devices. Make sure to check on your DNS infrastructure resiliency and check for options with your mitigation service as well to make sure you are protected against these attacks too.

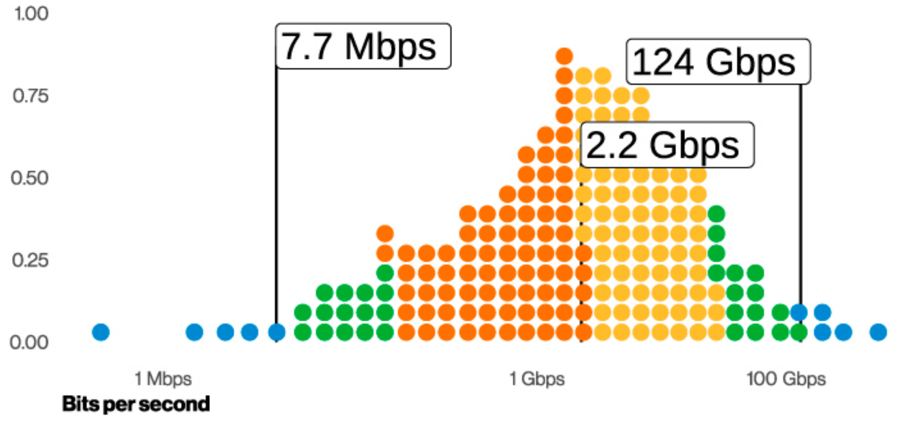


Figure 45. Bits per second in DDoS incidents (n=10,622)

---

[44] Be sure to discuss this at parties. You'll be wildly popular.
[45] I bet you thought our inflation numbers in the U.S. were bad, huh?
[46] This is NOT a subtle name!

Lost and Stolen Assets

Summary

This pattern continues to be a problem for organizations because these small (and not so small) devices are just so portable. We've seen their capacity to store large amounts of data increase over time, while employees' ability to misplace them (or External actors to steal them) remains predictably common.

What is the same?

Devices and media are still more likely to be lost by Internal actors than stolen by External ones.

Frequency	2,091 incidents, 159 with confirmed data disclosure
Threat actors	External (92%), Internal (68%), Multiple (60%), Partner (1%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Personal (87%), Medical (30%), Other (21%), Bank (13%) (breaches)

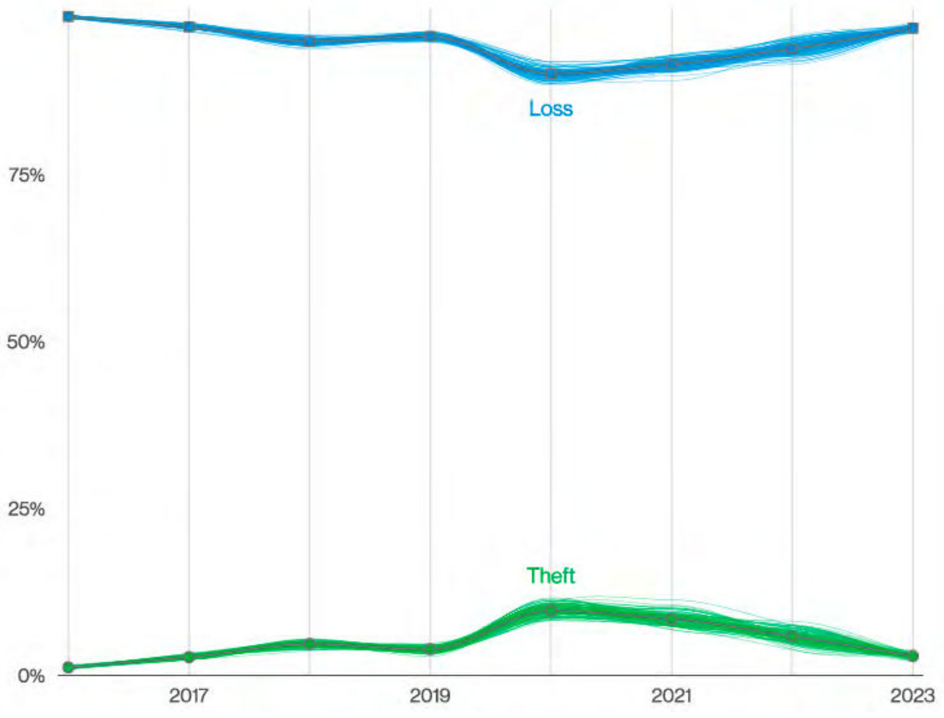


Figure 46. Top Action varieties in Lost and Stolen Assets incidents

Where go my laptop?

The headline in this pattern is "Your stuff is gone," which isn't really a news flash. Whether the missing item(s) had "help" in the form of someone stealing a laptop, or was accidental, as in classified printed documents being mislaid in high-level government officials' residences, the more portable an asset is, the more it needs protection against loss and theft.

This is a pattern where we see a high percentage of incidents not resulting in confirmed data breaches—largely because the status of confidentiality disclosure remains "at-risk" rather than "confirmed" due to the loss of custody of the asset in question. The exception is printed material, since no controls exist to shield documents from view once printed. Similar to last year, we again have less than 10% of the incidents as confirmed data breaches.

While stolen devices certainly represent a risk to organizations, employees are much more likely to cause a breach accidentally through loss. This fact has held true year over year on a consistent basis, as shown in Figure 46.

What is going missing, you may ask? Unsurprisingly, it's the portable user devices, such as laptops, and mobile phones. In fact, phones have become quite the commodity (Figure 47). Considering the fact that no one ever seems to put them down, it's hard to believe so many are lost.

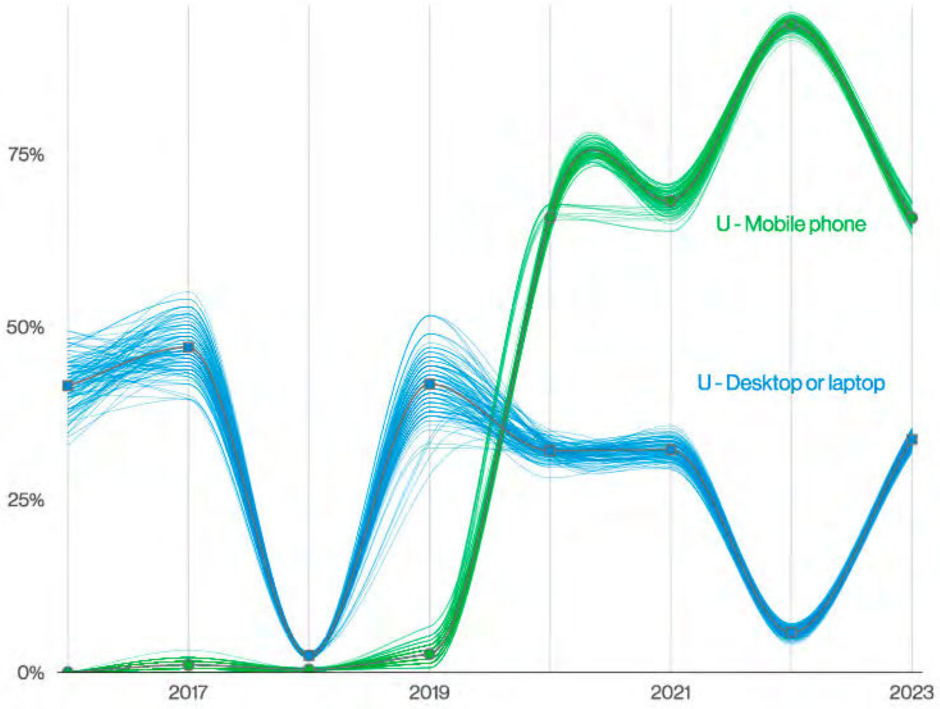


Figure 47. Top Assets in Lost and Stolen Assets incidents

CIS Controls for consideration

Protect data at rest

Data Protection [3]
- Encrypt Data on End-User Devices [3.6]
- Encrypt Data on Removable Media [3.9]

Secure Configuration of Enterprise Assets and Software [4]
- Enforce Automatic Device Lockout on Portable End-User Devices [4.10]
- Enforce Remote Wipe Capability on Portable End-User Devices [4.11]

Privilege Misuse

Summary

Your employees continue to use their access to commit breaches and, in some cases, initiate fraudulent transactions. We saw more collusion between multiple types of actors this year.

What is the same?

This pattern continues to be dominated by the Internal actor, by definition. Most are motivated by financial gain, and Personal data continues to be a favorite target.

Frequency	406 incidents, 288 with confirmed data disclosure
Threat actors	Internal (99%), Multiple (7%), External (6%), Partner (2%) (breaches)
Actor motives	Financial (89%), Grudge (13%), Espionage (5%), Convenience (3%), Fun (3%), Ideology (2%) (breaches)
Data compromised	Personal (73%), Medical (34%), Other (18%), Bank (12%), Payment (12%) (incidents)

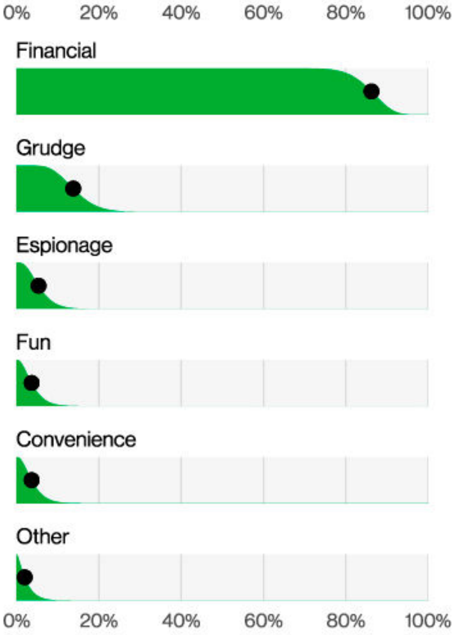


Figure 48. Internal actor motives in Privilege Misuse breaches (n=59)

My employees love me!

People may think they are somehow immune to a data breach. They may put their trust in their security controls, thinking they have amazing, impenetrable defenses. They may put their trust in "flying under the radar" or believe they are too small to have a breach. But this kind of thinking largely assumes breaches come from the outside, from the "bad actors" that are external to the organization. What they fail to take into account is the risk of an insider breach. "Surely, MY people wouldn't do that!" they say. But of course, they would—and don't call me Shirley.

The hard fact to face is that some of our employees also cause data breaches for malicious reasons. The most common nonaccidental Internal actor breach is Privilege abuse. This is just what it sounds like—employees abusing the access they have been given to do their jobs to steal data instead. They are significantly more likely to do this for their own financial gain (Figure 48). We know, it's a shocker.

We'll just help ourselves.

We've talked about your employees committing these acts – but our At-a-Glance table shows that we see other kinds of threat actors in this pattern. Interestingly, we see multiple threat actors (Internal, External, Partner – some combination of these three) in 7% of the breaches. This is collusion – evidence of multiple kinds of Actors working together to bring about a data breach.

Indeed, we have seen instances where organized fraud gangs have sent in people with the objective of being hired by businesses for the purpose of facilitating large-scale scams. We have seen this in multiple industries, and it has continued to plague organizations for years. These people can be difficult to spot – they may present and interview convincingly. This practice by financially motivated criminal groups makes it even more important to have your detective controls in place to catch the inappropriate access that these people are enabling. One of the difficulties in responding to an incident like this is that no company's onboarding process is perfect, and most onboarding involves getting the new hire added to various groups and systems that aren't always directly controlled by IT. Those investigations often reveal process-related weaknesses in the IT infrastructure.

We are increasingly seeing Privilege Misuse breaches paired with Fraudulent transactions, more so this year than in the past several, as shown in Figure 49. Fraudulent transactions are an Integrity violation that is frequently the end game of the BEC and is typically a money transfer to a threat actor-controlled bank account. However, since Internal actors already have access to the systems where bank accounts and routing information are stored in these cases, they're probably just making that banking update themselves. Seeing Internal actors increasingly just redirect funds is especially concerning, considering it may be someone in a position to siphon significant resources away from the organization.

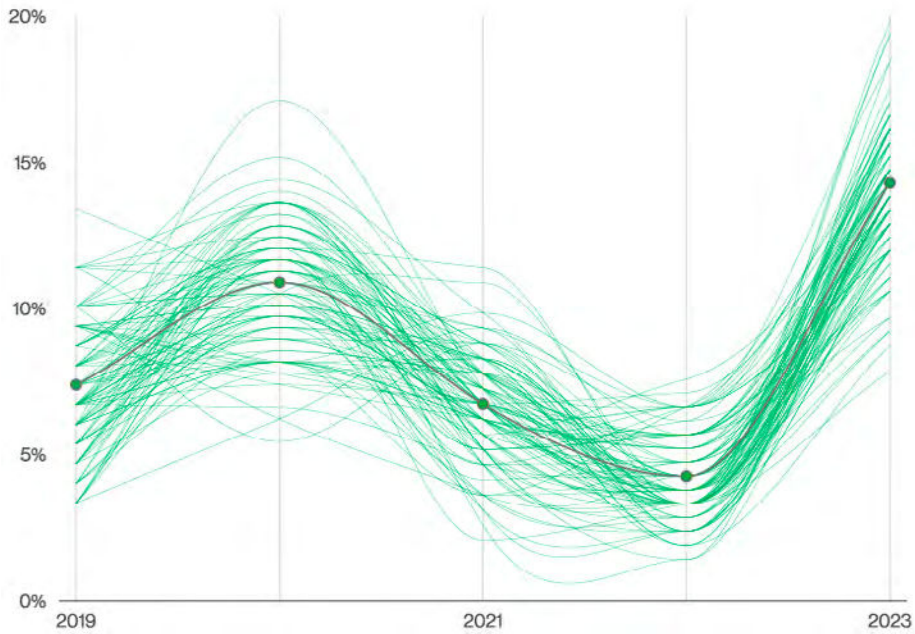
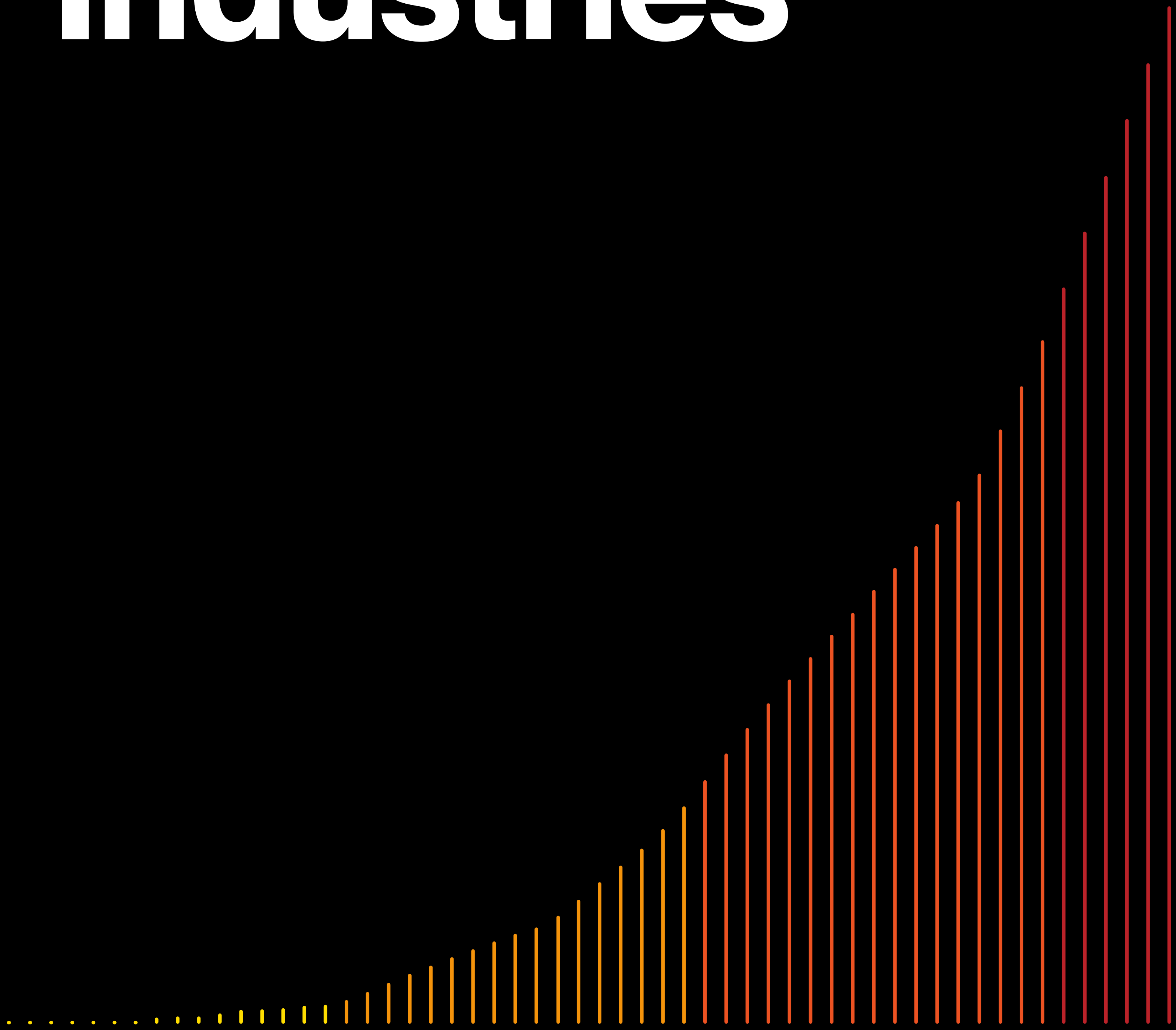


Figure 49. Fraudulent transactions in Privilege Misuse breaches

4

Industries



Industries: Introduction

If you are a new reader, you may find this introduction of some use. If, on the other hand, you are a long-time reader, then just move along; this will all be familiar territory. The 2023 DBIR examined 16,312 incidents, of which 5,199 were confirmed data breaches. We take a look at both from the point of view of their respective industries in the upcoming sections. Attacks that consistently prey on one industry may not affect another industry at all. Attack surfaces, the interest of specific threat actors and the infrastructure a given industry relies upon all play a big role in how they experience security incidents. The types and quantity of data the industry handles, how people (customers, employees, etc.) interact with them, and a host of other factors too numerous to mention will also dictate the kinds of attacks each industry encounters.

A large organization whose business model focuses entirely on mobile devices and the apps it includes will naturally have a different set of risks than a very, very small business with no internet presence but that uses a point-of-sale (PoS) vendor to manage their systems for them. The infrastructure, and conversely the attack surface, largely drives the risk.

Therefore, we caution our readers not to make inferences about the security posture (or lack thereof) of a particular sector[47] based on how many breaches or incidents an industry reports. These numbers are heavily influenced by several factors, including data breach reporting laws and partner visibility. Because of this, some of the industries have very low numbers, and as with any small sample, we must advise readers that our confidence in any statistics derived from a small number must also be less.

If you are reading this only for a glimpse of your industry, our recommendation is to verify what the top patterns are on the summary table accompanying each industry and also spend some time with those pattern sections.

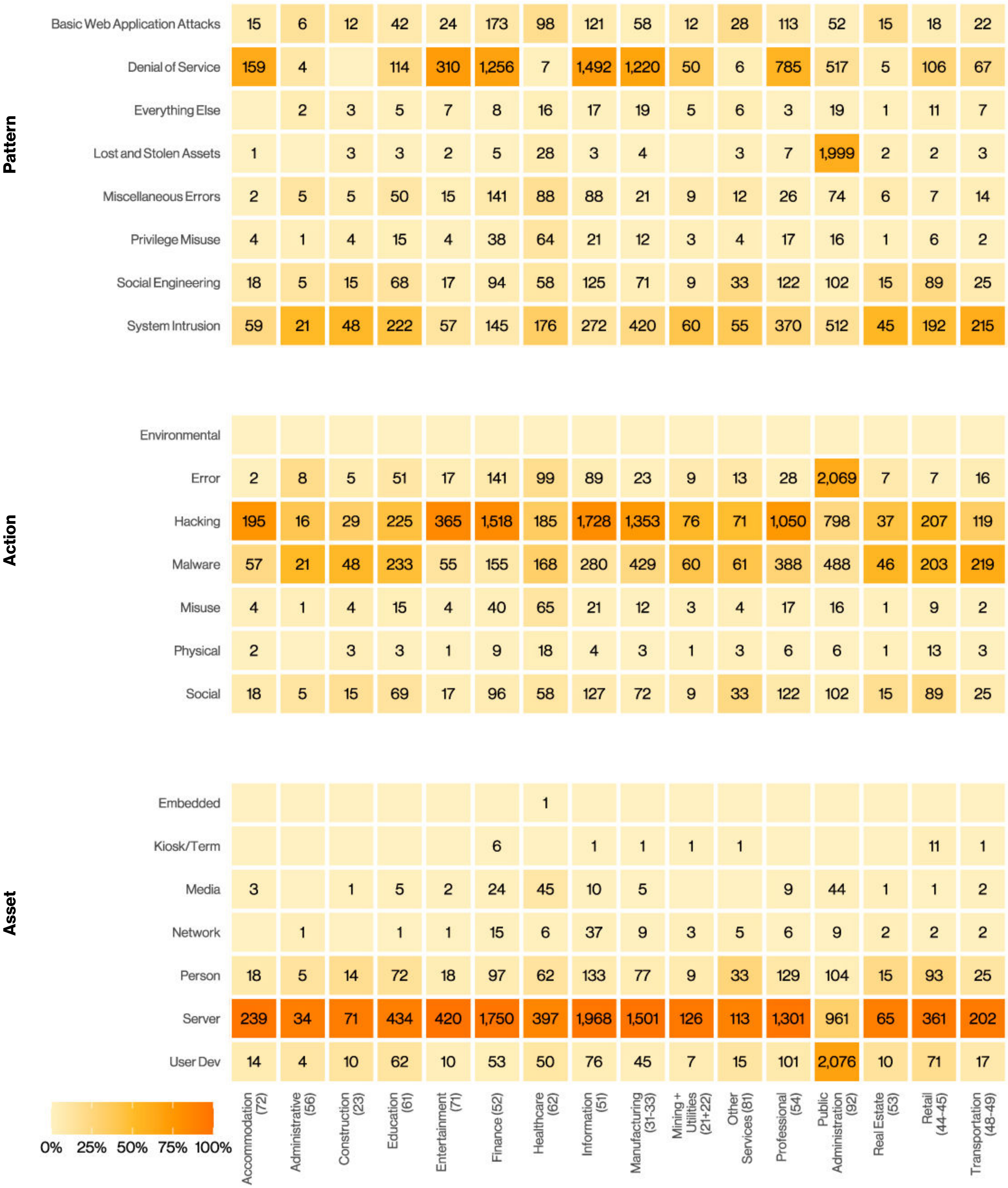
---

[47] Legal made us say that; of course, you should totally ridicule your [fren]emies in other industries.

	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	16,312	694	489	15,129	5,199	376	223	4,600
Accommodation (72)	254	4	2	248	68	4	1	63
Administrative (56)	38	8	14	16	32	8	11	13
Agriculture (11)	66	1	5	60	33	0	3	30
Construction (23)	87	7	1	79	66	4	1	61
Education (61)	496	63	15	418	238	28	8	202
Entertainment (71)	432	13	3	416	93	10	1	82
Finance (52)	1,829	70	30	1,729	477	38	18	421
Healthcare (62)	522	28	15	479	433	23	15	395
Information (51)	2,105	45	110	1,950	380	23	19	338
Management (55)	9	1	0	8	9	1	0	8
Manufacturing (31–33)	1,814	37	24	1,753	259	18	15	226
Mining (21)	25	2	0	23	13	2	0	11
Other Services (81)	143	7	2	134	100	6	1	93
Professional (54)	1,396	176	54	1,166	421	85	32	304
Public Administration (92)	3,270	87	110	3,073	582	48	39	495
Real Estate (53)	83	15	5	63	59	10	2	47
Retail (44–45)	404	62	44	298	191	33	28	130
Transportation (48–49)	349	13	25	311	106	8	13	85
Utilities (22)	117	12	6	99	33	3	3	27
Wholesale Trade (42)	96	42	22	32	53	23	11	19
Unknown	2,777	1	2	2,774	1,553	1	2	1,550
Total	16,312	694	489	15,129	5,199	376	223	4,600

Table 2. Number of security incidents and breaches by victim industry and organization size

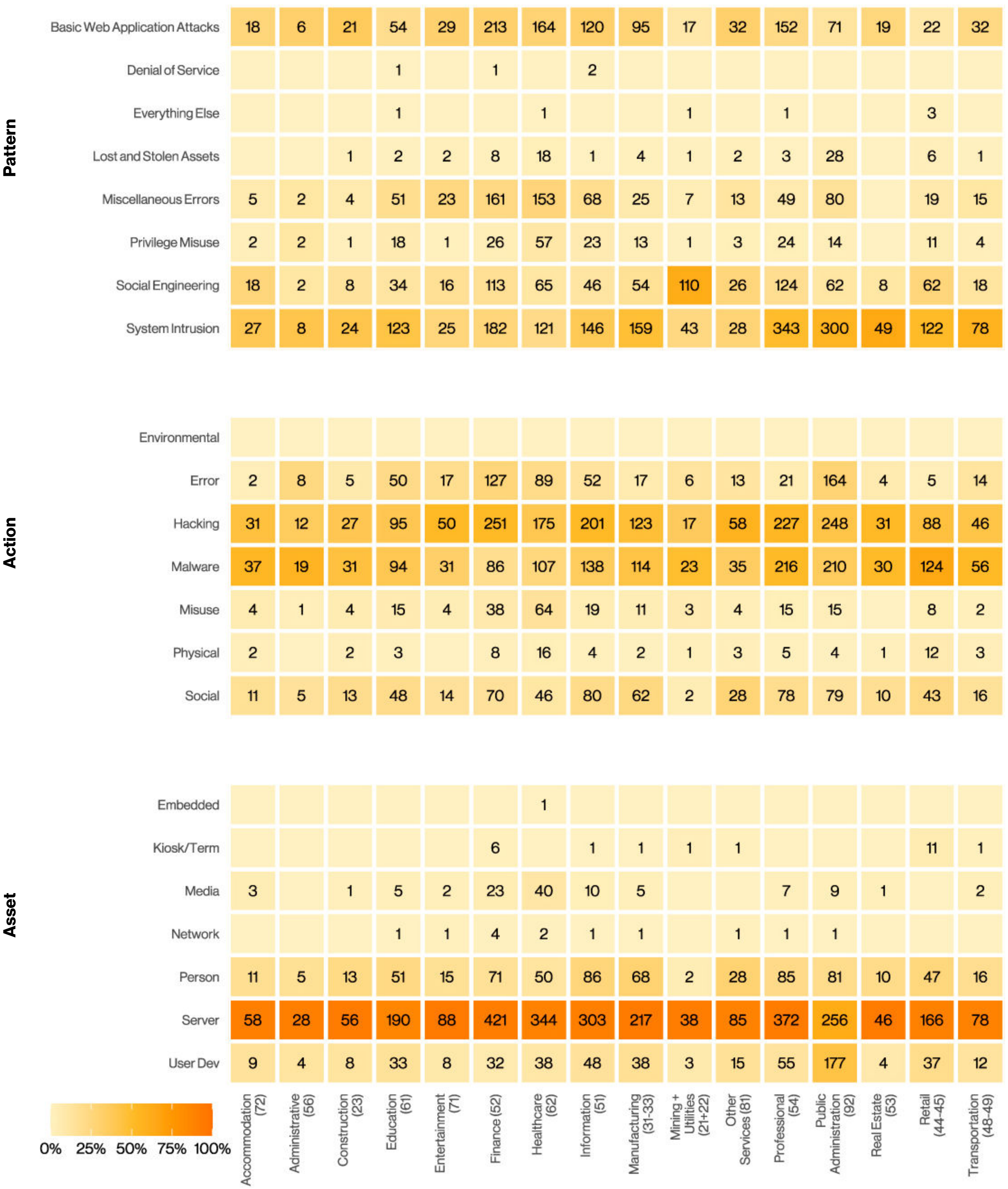
Incidents



		Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Pattern	Basic Web Application Attacks	15	6	12	42	24	173	98	121	58	12	28	113	52	15	18	22
	Denial of Service	159	4		114	310	1,256	7	1,492	1,220	50	6	785	517	5	106	67
	Everything Else		2	3	5	7	8	16	17	19	5	6	3	19	1	11	7
	Lost and Stolen Assets	1		3	3	2	5	28	3	4		3	7	1,999	2	2	3
	Miscellaneous Errors	2	5	5	50	15	141	88	88	21	9	12	26	74	6	7	14
	Privilege Misuse	4	1	4	15	4	38	64	21	12	3	4	17	16	1	6	2
	Social Engineering	18	5	15	68	17	94	58	125	71	9	33	122	102	15	89	25
	System Intrusion	59	21	48	222	57	145	176	272	420	60	55	370	512	45	192	215
Action	Environmental																
	Error	2	8	5	51	17	141	99	89	23	9	13	28	2,069	7	7	16
	Hacking	195	16	29	225	365	1,518	185	1,728	1,353	76	71	1,050	798	37	207	119
	Malware	57	21	48	233	55	155	168	280	429	60	61	388	488	46	203	219
	Misuse	4	1	4	15	4	40	65	21	12	3	4	17	16	1	9	2
	Physical	2		3	3	1	9	18	4	3	1	3	6	6	1	13	3
	Social	18	5	15	69	17	96	58	127	72	9	33	122	102	15	89	25
Asset	Embedded							1									
	Kiosk/Term						6		1	1	1	1				11	1
	Media	3		1	5	2	24	45	10	5			9	44	1	1	2
	Network		1		1	1	15	6	37	9	3	5	6	9	2	2	2
	Person	18	5	14	72	18	97	62	133	77	9	33	129	104	15	93	25
	Server	239	34	71	434	420	1,750	397	1,968	1,501	126	113	1,301	961	65	361	202
	User Dev	14	4	10	62	10	53	50	76	45	7	15	101	2,076	10	71	17

Figure 50. Incidents by industry

Breaches



Pattern	Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Basic Web Application Attacks	18	6	21	54	29	213	164	120	95	17	32	152	71	19	22	32
Denial of Service				1		1		2								
Everything Else				1			1			1		1			3	
Lost and Stolen Assets			1	2	2	8	18	1	4	1	2	3	28		6	1
Miscellaneous Errors	5	2	4	51	23	161	153	68	25	7	13	49	80		19	15
Privilege Misuse	2	2	1	18	1	26	57	23	13	1	3	24	14		11	4
Social Engineering	18	2	8	34	16	113	65	46	54	110	26	124	62	8	62	18
System Intrusion	27	8	24	123	25	182	121	146	159	43	28	343	300	49	122	78

Action	Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Environmental																
Error	2	8	5	50	17	127	89	52	17	6	13	21	164	4	5	14
Hacking	31	12	27	95	50	251	175	201	123	17	58	227	248	31	88	46
Malware	37	19	31	94	31	86	107	138	114	23	35	216	210	30	124	56
Misuse	4	1	4	15	4	38	64	19	11	3	4	15	15		8	2
Physical	2		2	3		8	16	4	2	1	3	5	4	1	12	3
Social	11	5	13	48	14	70	46	80	62	2	28	78	79	10	43	16

Asset	Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Embedded							1									
Kiosk/Term						6		1	1	1	1				11	1
Media	3		1	5	2	23	40	10	5			7	9	1		2
Network				1	1	4	2	1	1		1	1	1			
Person	11	5	13	51	15	71	50	86	68	2	28	85	81	10	47	16
Server	58	28	56	190	88	421	344	303	217	38	85	372	256	46	166	78
User Dev	9	4	8	33	8	32	38	48	38	3	15	55	177	4	37	12

Figure 51. Breaches by industry

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.

I'll just scrape that off.

System Intrusion is the top pattern in this sector for the second year running. Included in this pattern, among other things, is a collection of various types of malware. Approximately one-third of cases involved the use of Ransomware, and much of the remainder consisted of RAM scrapers. In fact, RAM scrapers targeting the PoS is the favorite combo in this sector, which likely comes as no surprise to those trying to maintain their defenses.

Payment card data was targeted 41% of the time, which is the same percentage we saw last year, but since Credentials and Personal data fell as a proportion of the whole, they have taken a back seat to credit cards. Along with the increased focus on the data type of Payment cards comes the motivation of Financial. Last year, we saw the Espionage motive in 9% of the breaches, but this year, it is all Financial all the time.[48]

Give a person a phish and you feed them for a day!

Social continues to have a considerable presence in this sector. While Phishing and Pretexting (the main difference between them is how hard the adversary must work to make it happen) are the main social engineering concerns in Accommodation, they are too close to call for the top spot. Most of these social attacks are coming in via email, so make sure it is easy for your employees to report any questionable attempt quickly. There is nothing like having your employees be your first line of defense—they are certainly already on the front line of targets.

---

[48] Honestly, what isn't though?

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.

Who saw that coming?

In a move that shocked faculty, staff and students alike, last year's much lauded salutatorian, Basic Web Application Attacks, has dropped out (of the top three patterns). Miscellaneous Errors is still present (isn't it always?) and has increased slightly from last year. As you may have guessed, these errors are the usual suspects: Misdelivery, Publishing errors and Misconfiguration.

Social Engineering clawed its way to the number three position, increasing from 14% last year to 21% in 2023 (Figure 52). This rise is primarily represented by Phishing attacks, which showed up in 18% of breaches, and Pretexting scenarios (4%).

Hacking was present in 40% of breaches, with the Use of stolen credentials appearing in 31% of them. Not to be outdone, Malware also showed up in 40% of breaches, with Ransomware present in 30% of those breaches. Let's review that finding for the exam: Ransomware was responsible for almost one-third of all breaches in the Educational Services vertical. In spite of this impressive showing from both Hacking and Malware, the System Intrusion pattern, while maintaining its number one spot, decreased slightly from last year.

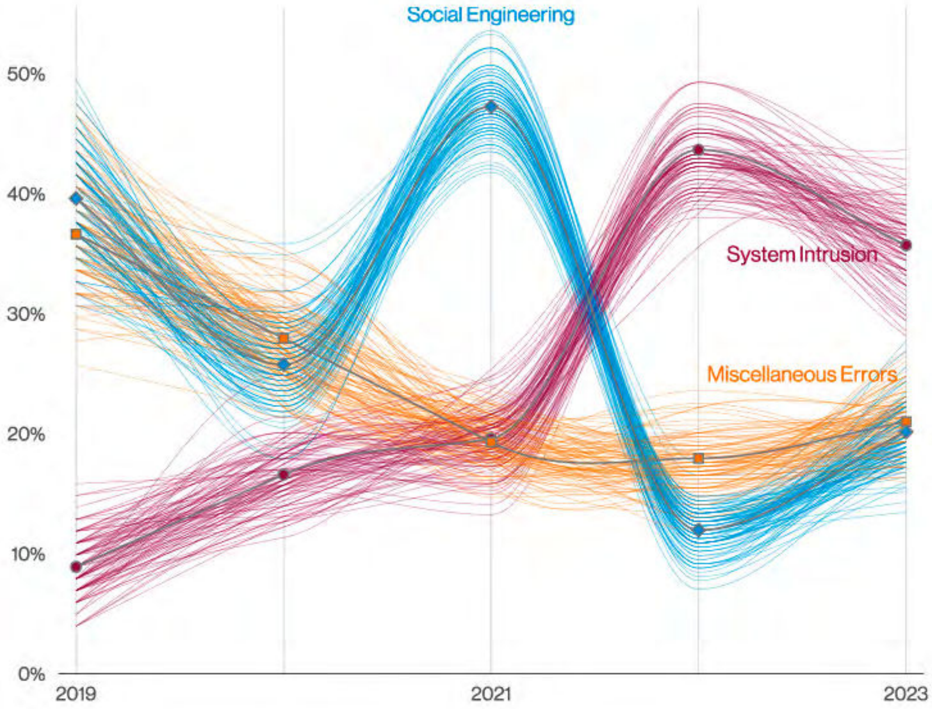


Figure 52. Patterns in Education breaches

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 cover a decent percentage of attacks in this sector.

These attacks are so basic.

“We were compromised by a highly sophisticated cyberattack.” So reads a large percentage of data breach notification letters. But really, just how sophisticated is a brute-forced password? Or better still, credential stuffing where you don’t even have to guess the password—you’ve acquired it from another breach! The Basic Web Application Attacks pattern is the most prevalent in this sector, which means those not-so-complex attacks are succeeding splendidly for the adversaries. Why put forth a great deal of effort when just a little will do?

Wait—did I give you that?

Another prominent attack involves Internal actors making mistakes. Misdelivery—where protected data is sent to the wrong recipient—is the most common. Sometimes it is a matter of paper documents going to the wrong people, and other times it is just the electronic version that goes astray. Either way, extra care needs to be given to catching these kinds of Errors before they cause a data breach.

Make them work for it.

Rounding out the top three is the pattern that requires adversaries to actually put forth a bit of effort, System Intrusion. While it dropped from 27% to 14% this year (allowing Miscellaneous Errors to dominate), it remains a serious issue. This illustrates that at least some of the time, adversaries had to trot out their more sophisticated techniques in order to get the job done. Interestingly, Ransomware is decreasing as a favorite tactic in this pattern for this sector. We discuss it more in depth in the “Incident Classification Patterns” section in case if you skipped that part. We know, some of you just read the DBIR for the pictures.

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 prevalent as well. Finally, don't discount the insider threat in this industry.

A sector under siege

The Healthcare vertical is highly targeted by ransomware gangs, which results in both the loss of use of their systems—potentially with life-threatening consequences—as well as data breaches. While the number of ransomware incidents peaked in this industry in 2021, the last three years have seen a jump in data breaches (where the data is confirmed to have been stolen as well as the encryption triggered) caused by ransomware. This combination of attacks by adversaries is resulting in more data being compromised in addition to the usual chaos of staff being forced to do their jobs without the systems they rely upon.

Mitigating these attacks takes time—if the organization even has reliable, tested backups of the systems compromised—and resources. If both are scarce in your organization, prevention and early detection are your best friends. Don't ignore the threat this type of attack represents when you are planning your controls.

Sorry 'bout that

The Miscellaneous Errors pattern remains prevalent in healthcare. The action variety of Misdelivery is a consistent people problem. This is the mistake that happens when data that is supposed to go to a certain person (or group) actually ends up going to someone entirely different. Sometimes it is in the form of that spreadsheet with sensitive employee health information accidentally being sent to a much wider distribution than planned (those email groups can be so similar—thanks a lot, autocomplete). In other cases, it is a mailing error with paper documents that are placed in such a way that too much information is visible in the envelope's clear window. Who wants their letter carriers to know about their embarrassing condition? Customers (patients) are understandably upset.

Where's my gruntle?

Ah, the disgruntled employee—so often the perpetrator of malicious actions and wreaking the kind of havoc only an insider can achieve. While the Privilege Misuse pattern is no longer in the top three for this industry, it remains a consistent problem. Snooping from curiosity—more the bored employee than the actively hostile—is common in Healthcare as well. But this is also a sector in which we see evidence of collusion, multiple actors working together to make their breach dreams a reality. If only this diligence could be put toward their legitimate work tasks, these employees could be top performers. The industry's only defense for when someone loses their gruntle is fast detection of unusual data access patterns. This remains a challenge for any industry where internal actors are motivated to cause trouble.

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

Miscellaneous Errors 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.

Make no mistake, information is power.

Over the last few years, errors have played a diminishing role in breaches within the Information vertical. That downward trend continues this year, so much so that it has fallen to number four and accounts for only 13% of breaches (Figure 53). Good on ya, Information folks! Securing your assets from the bad guys is hard enough without unwittingly exposing assets yourself.

Social Engineering, on the other hand, has slowly crept up and captured the number three position with 20% of breaches. In some industries, we see a much higher degree of Phishing than we do of its more complicated cousin, Pretexting. In the Information vertical, however, the two social actions are not far apart, with Phishing at 15% and Pretexting at 11%. As mentioned elsewhere in this report, Pretexting is definitely on the rise.

Please listen closely as our options have NOT changed.

As always, external actors (the vast majority of which are Organized crime) are behind most attacks in this vertical. In fact, last year, we showed only External and Internal actors. This year we did see an increase (albeit very small) in the categories of Partner and multiple actors at 1% each. Granted, those are not big numbers, but it is of interest to see them reappearing in this industry for the first time in a couple of years. As one would expect, the vast majority of attacks, regardless of who was committing them, were Financially motivated. The motive of Espionage was still present at 8% of breaches but is significantly lower than last year's 20%. The most likely reason for the change is the move away from web apps and servers and toward spy balloons and remote viewing.

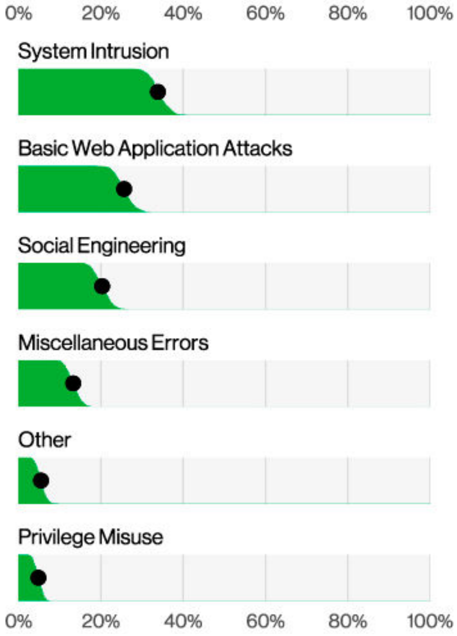


Figure 53. Patterns in Information sector breaches (n=384)

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.

In our postmodern world, we rely on gadgets and gizmos galore to make it through our day – certainly more so than at any other time period in history.[49] The importance of Manufacturing truly cannot be understated as it relates to how we exist and interact with each other on a daily basis. The Manufacturing industry is aware of this and consequently is continually looking for the next big thing that we all think we can't live without. Cybercriminals know it as well and are constantly maneuvering in an effort to cash in.

This year we can see in Figure 54 the same top three patterns that we saw in last year's report, albeit in a slightly different order. Social Engineering (23%) and Basic Web Application Attacks (17%) changed places in the lineup, while System Intrusion remains in first place at 42%.

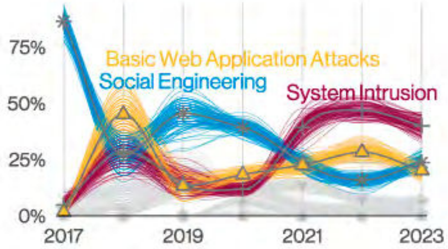


Figure 54. Patterns over time in Manufacturing incidents

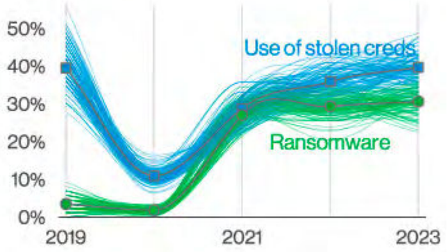


Figure 55. Action varieties over time in Manufacturing breaches

As Figure 56 illustrates, when we drill down into what attack actions most often occur in the Manufacturing vertical, we see that Hacking and Malware attacks are occurring at almost exactly the same rate and that Social attacks continue to make a strong showing. Ransomware, which accounts for a large part of the breaches in the System Intrusion pattern, continues to slowly trend upward in this vertical for the third year in a row (Figure 55).

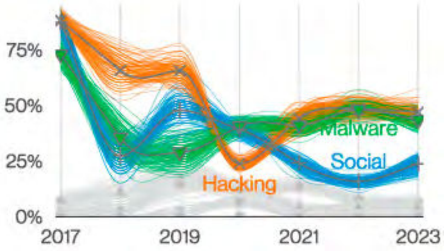


Figure 56. Select Actions over time in Manufacturing breaches

From an incident perspective, it is still mainly about Denial of Service attacks. DoS attacks account for approximately 67% of incidents in this vertical. This has been a rising trend over the past few years, so if your organization resides in this industry, it is definitely something to keep an eye on.

---

[49] And believe me, we have lived through several of them.

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.

Dig around and find out.

Due to the smaller number of incidents and breaches reported to us from NAICS 21 and 22, we have to dig deep (pun intended) at times to have a statistically relevant population. Even so, because of the smaller sample size, we are sometimes still forced to use ranges rather than definite percentages. However, as both these sections are considered critical infrastructure and are not too dissimilar, we do our best to find useful and interesting nuggets where we can. Are you a member of these industries? If so, please consider becoming a DBIR contributor to help us provide more useful analysis.

The number one pattern this year is System Intrusion. If you have been reading the other sections, you will know that this in no way makes those in this vertical the Lone Ranger. As stated in the patterns section, the System Intrusion pattern is made up of more complex, multistep attacks as opposed to the "get in, grab the loot and scram" type of attacks. Specifically, most ransomware attacks fall into System Intrusion, and approximately one out of three breaches (32%) in this industry were ransomware attacks (Figure 57). Given the high rate of success of ransomware (along with the fact that attackers often take data before they encrypt it, and they do love to post it on their leak sites), seeing so much of it in critical infrastructure verticals is a matter for concern.

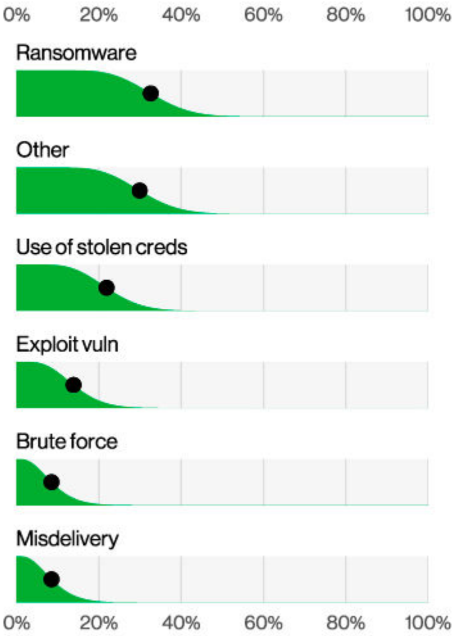


Figure 57. Mining and Utilities top Actions in breaches (n=37)

Last year we commented on the high number of breaches in this vertical that fell into the Social Engineering pattern. This year it has dropped out of the top three completely with Basic Web Application Attacks and Miscellaneous Errors coming in at numbers two and three. In fact, Social Engineering dropped out of the top five. This is mildly surprising due to the uptick we are seeing in phishing and pretexting in other industries. Maybe the criminals don't want to have to actually interact with others to steal money? We can certainly understand that.

When it comes to what the threat actors are taking, personal data accounts for half, and there was a substantial rise in Internal data (33% this year as opposed to 9% last year, as shown in in Figure 58). This may be tied to the name and shame ransomware attacks mentioned on the previous page.

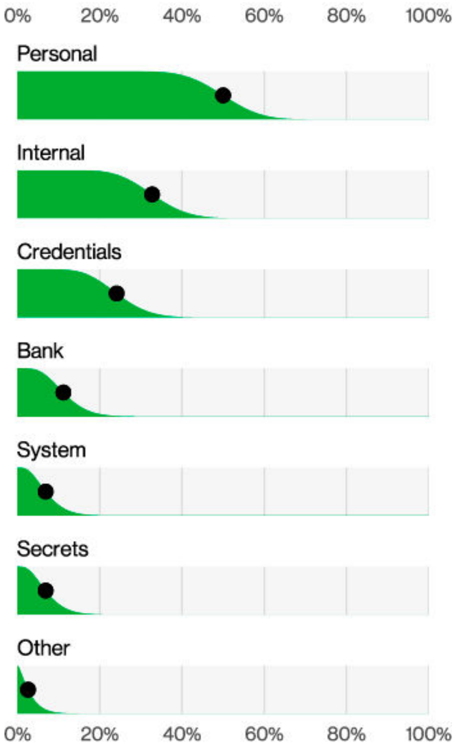


Figure 58. Top Data type stolen in Mining and Utilities (n=46)

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.

This sector could perhaps be considered the lubricant that keeps all industries running smoothly. It consists of many disparate professions, including our lawyer friends [joke redacted by legal], accounting and various other business services. Much like the other sectors they serve, this industry is also affected by the big three patterns of System Intrusion (47%), Basic Web Application Attacks (25%) and Social Engineering (18%).

With regard to action varieties, while we see DoS and Use of stolen creds among the top actions in Figure 59, we also see a good deal of Ransomware. This year, Ransomware accounted for approximately 23% of the incidents in this sector, which is a notable increase from last year's 14%.

If you are wondering how these breaches occur, you need look no further than Web applications (55%), Email (25%) and Desktop sharing software (17%). Considering the frequent usage of stolen credentials and email, it might be a good time to remind folks to implement strong authentication practices and to encourage your team members to keep in mind the importance of staying diligent.

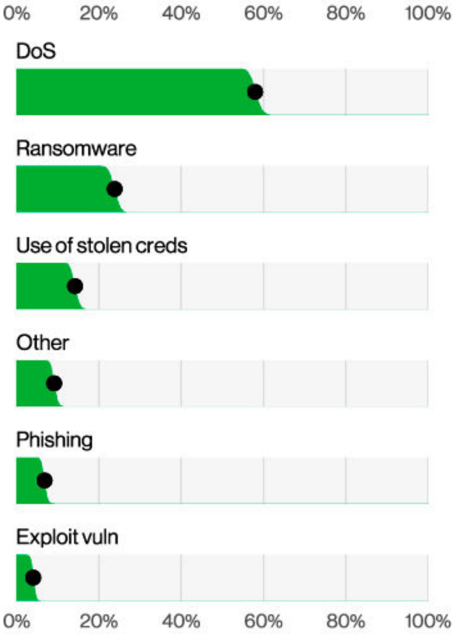


Figure 59. Actions in Professional Services incidents (n=1,351)

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.

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.[50] 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%.

---

[50] There are explosions and car chases in there too, we're sure of it.

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 60), 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"[51]-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 61).

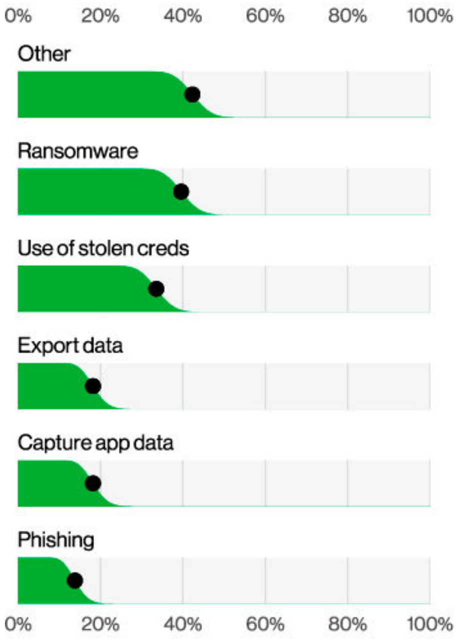


Figure 60. Top Action varieties for Retail breaches (n=182)

---

[51] In layman's terms, it is when wizards race each other in go-carts.

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 62, 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 PoS 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.[52]

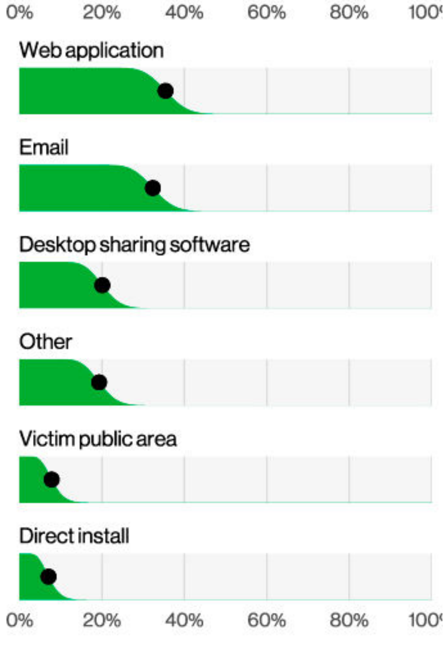


Figure 61. Top Action vectors in Retail breaches (n=130)

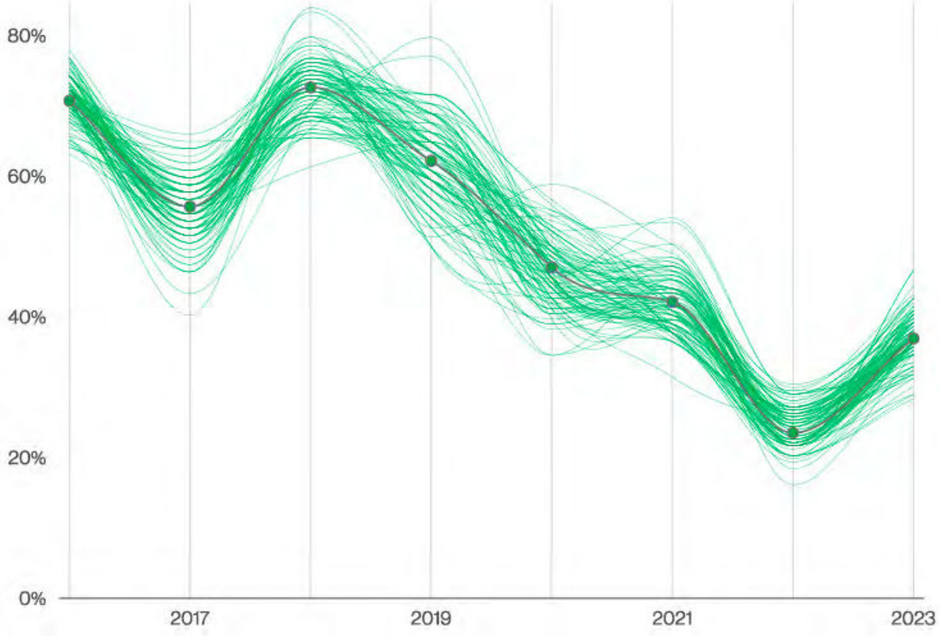


Figure 62. Payment card over time in Retail breaches

---

[52] https://www.pcisecuritystandards.org/resources-overview/

Small and medium business

“Let’s do some word problems!”

–said no one ever (except math teachers)

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.

The tables on the right illustrate the fact that SMBs and large organizations have increasingly become similar to each other. This phenomenon began several years ago, and by now there is so little difference based on organizational size that we were hard-pressed to make any distinctions whatsoever. Therefore, this year we decided to look at these a bit differently[53] by looking at the implementation of security controls for various size SMBs (smaller, midsize and larger) and how they may overlap or differ.

In past reports we have discussed the research we conduct with regard to controls—in particular, the work we have done with MITRE to map VERIS to ATT&CK. This year, we would like to take this research a bit more into the real world and apply it to how you would use these mappings with the appropriate CIS Implementation Group protective controls.

Small businesses (less than 1,000 employees)

Frequency	699 incidents, 381 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches)
Actor motives	Financial (98%), Espionage (1%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Credentials (54%), Internal (37%), Other (22%), System (11%) (breaches)

Table 3. At a glance for SMB

Large businesses (more than 1,000 employees)

Frequency	496 incidents, 227 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 85% of breaches
Threat actors	External (89%), Internal (13%), Multiple (2%), Partner (2%) (breaches)
Actor motives	Financial (97%), Espionage (3%), Ideology (2%), Convenience (1%), Fun (1%) (breaches)
Data compromised	Internal (41%), Credentials (37%), Other (30%), System (22%) (breaches)

Table 4. At a glance for large organizations

---

[53] Again, there is that refocusing thing we keep talking about.

It's not easy being small.

Let's assume you're a startup—a tiny company in its infancy. You have very, very limited resources for implementing security controls of any kind. Your IT person is also your security person is also your Jack- (or Jill-) of-all-trades who wears many hats and never sleeps.

The first step is to see which controls are recommended for your level of security maturity and resources. But where to begin? We like the CIS Critical Security Controls Navigator as a good starting point.[54] It breaks down each of the CIS Controls into small, easy-to-consume chunks and then maps them to various security standards that an organization may want to comply with as their adopted standard. You will see that they are broken into three Implementation Groups, and each one is geared to the organization's maturity level. Since we're at the beginning here, we will start with Implementation Group 1 (IG1). While these are all good controls and should be on the road map, let's take a more threat-centric approach in our scenario.

You can see in Tables 3 and 4 that regardless of an organization's size, they are most commonly going to face the System Intrusion pattern. In last year's report, we mapped the Controls to the pattern and showed which were most commonly going to help you in an attack.[55] The result in IG1 shows Controls 14 (89%), 11 (80%) and then 5 (67%).

When you drill further into the Sub-Controls, more granularity should guide you in your quest for maturing your organization's security posture. Each organization will need to customize and prioritize according to its own risk profile and tolerance, but it is at least a place to begin. Once the most likely suspects are accounted for, move onto the next mostly likely attack pattern you may be facing and determine how to handle that. Using data-driven information on your most probable risk areas is a defensible strategy toward prioritizing controls with few resources. Hopefully after some progress is made, your Jack-/Jill-of-all-trades can go back to sleeping at night.

Control	Description
14	**Security Awareness and Skills Training** Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.
11	**Data Recovery** Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a preincident and trusted state.
5	**Access Control Management** Use processes and tools to create, assign, manage and revoke access credentials and privileges for user, administrator and service accounts for enterprise assets and software.

Table 5. CIS Implementation Group 1 Controls for Incident Classification Patterns most commonly encountered by SMBs

---

[54] https://www.cisecurity.org/controls/cis-controls-navigator/

[55] 2022 DBIR, Appendix B: VERIS and Standards, p. 96

Midsize is the right size.

You've been at this a while. You're not tiny, but you're not quite at the enterprise level just yet. You have been working diligently at maturing your processes in both IT operations and in information security. You have put in place the Controls in IG1 and are now eyeing IG2 to take your company to the next level of protection.

With that in mind, let's take a look at the IG2 controls that cover the Social Engineering pattern, which is the second largest threat for SMBs. The first two controls are the same main categories as they were for System Intrusion, Control 5 (100%) and Control 14 (100%). However, the third control is different for this pattern:

- **Control 17 – Incident Response Management**
  Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training and communications) to prepare, detect and quickly respond to an attack.

An Incident Response Management plan is key to all areas of security but perhaps especially so when it comes to Social Engineering attacks for a few reasons. Many of these attacks, such as pretexting, tend to escalate quickly and can have a high impact. Perhaps just as importantly, employees need to feel secure in the knowledge that they have a place they can report these incidents to when they occur because the sooner they report them, the more quickly you can address them.

> **"You get a resource! You get a resource! Everybody gets a resource!"**

Now let's pivot to look at the larger organizations in the SMB area. To clarify, we are still writing with regard to SMBs, we simply mean the larger companies that still fall into that category (<1,000 employees). When your company reaches this point, there are more resources available to throw at problems, whether in the form of more people, more technology options or just plain more cash,[56] and bringing those resources to bear can yield substantial benefits. At this, level you may have tackled IG1 and IG2 and are ready for IG3 Controls.

These Controls mature along with your organization. Therefore, let us examine the IG3 Controls with regard to the third most common pattern for SMB: Basic Web Application Attacks. The first, Control 17 (100%), we talked about in the previous section, but Controls 16 (100%) and 18 (100%) we have not yet discussed.

- **Control 16 – Application Software Security**
  Manage the security life cycle of in-house developed, hosted or acquired software to prevent, detect and remediate security weaknesses before they can impact the enterprise.
- **Control 18 – Penetration Testing**
  Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes and technology), and simulating the objectives and actions of an attacker.

Control 16 is certainly timely, considering the SolarWinds case from last year's report and the Log4j impact discussed in this year's report, so we should have no problem seeing the relevance of this Control. Sub-Controls 16.2: Establish and Maintain a Process to Accept and Address Software Vulnerabilities, 16.4: Establish and Manage an Inventory of Third-Party Software Components, and 16.5: Use Up-to-Date and Trusted Third-Party Software Components would have gone a long way to defending against both of those cases.

---

[56] And this never really hurts, does it?

Once an entity has reached the larger end of the SMB scale, Control 18 also comes into play. Establishing penetration testing capabilities and incorporating their findings into the security processes can only improve the information security posture of a larger SMB. This is basically real-world testing of your controls to make sure they are performing how you expect them to. Like backups, only controls that have been tested and verified should be trusted.

Now that you've already looked at the Controls and prioritized them, you know what you're most likely to be hit with and you're working your way through to the end—your ducks are almost all in a row. You have balanced preventive and detective capabilities and are on your way to being able to not only detect when something bad has happened but also respond quickly and appropriately. You have moved from the basics of putting your plan together to implementing a road map.

A few final things to consider at this point: Are you looking at aligning with a particular compliance framework? Do you track metrics around security in your environment? Do your efforts result in ongoing improvements to your security posture, or do they just provide a point-in-time snapshot that says, "I was good at this moment, but then things changed"? There is quite a bit you can do when you use good information about what is happening in your organization to steer your security strategy.

From the Center for Internet Security:

Report after report, and study after study, shows that many attacks are successful because network owners did not know their enterprise assets, the software they had running and where their critical data was. Knowing your environment is foundational to any cybersecurity program, so they encompass the first three controls of the CIS Critical Security Controls (Controls). After all, you can't protect what you don't know you have.

After understanding your environment, you can prioritize where to apply and which controls to implement across your enterprise. At CIS we know that this will take time and resources, which is why we have prioritized the Controls and supporting Safeguards to help you plan your security improvement program. We do this through Implementation Groups (IGs). There are three IGs and are based on the risk profile and resources an enterprise has available to them to implement controls. Each IG builds upon the previous one. So IG2 builds upon IG1 and IG3 comprises all the Controls and Safeguards.

We describe a typical IG1 enterprise as small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel. The principal concern of this enterprise is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information.

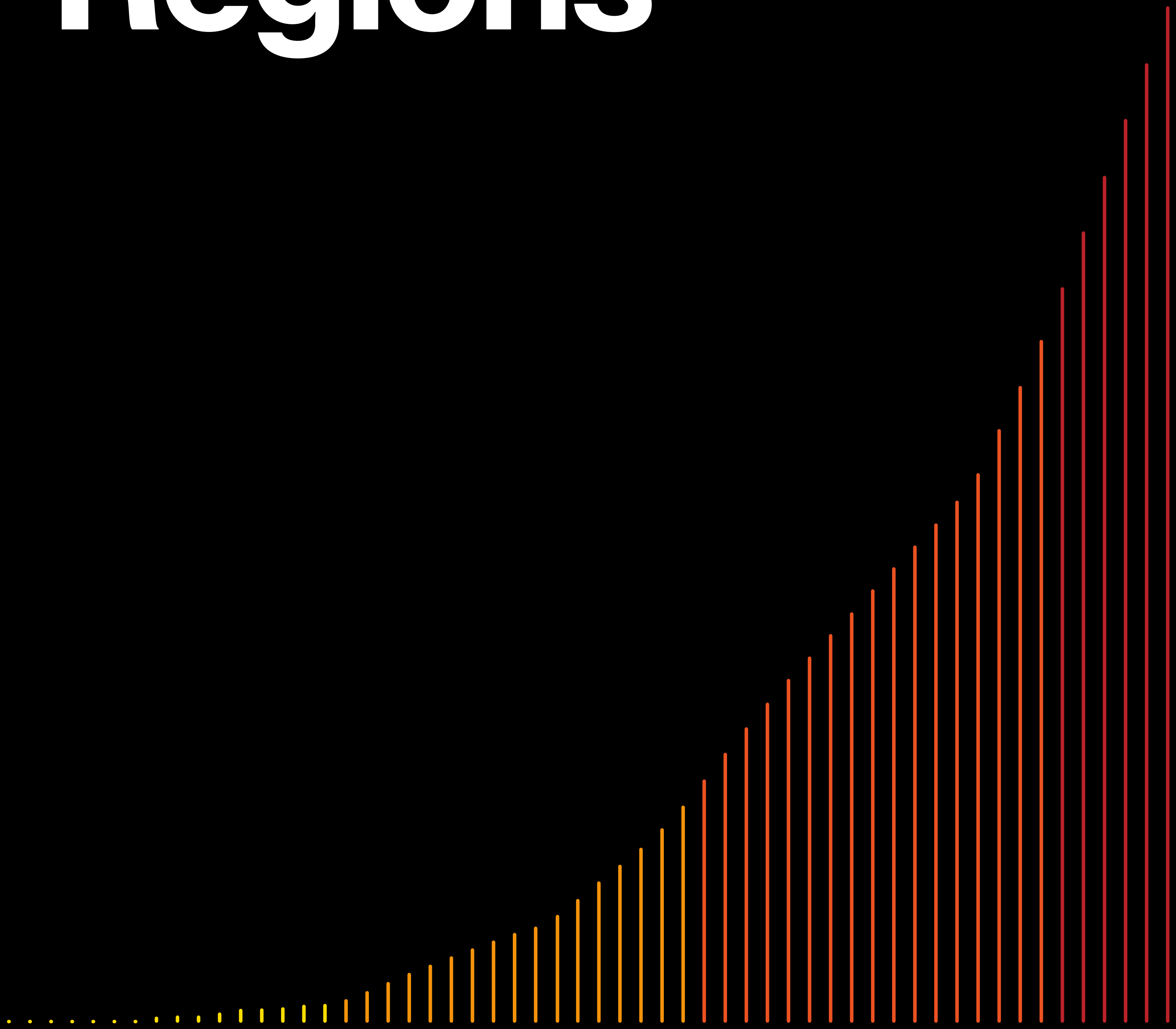
Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

But no matter the size or complexity of your business, we recommend that all organizations begin with IG1. We also refer to IG1 as Essential Cyber Hygiene because it provides the actions necessary for an organization to defend itself against the major attack types being used by cybercriminals. IG1 is not just another list of good things to do; it's an essential set of steps that helps all enterprises defend against real-world threats. And it provides a strong foundation for your cyber maturity growth, or as your security needs change. This is a strong claim, but we back it up with our use of the best-available summaries of attacks (like the Verizon DBIR), and an open, shared methodology (the CIS Community Defense Model v2.0[57]).

---

[57] https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

5
Regions



Regions: Introduction

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.

We define the regions of the world in accordance with the United Nations M49[58] standards, which combines the super-region and sub-region of a country together. By so doing, the regions we will examine are as follows:

APAC: Asia Pacific, including Southern Asia (034), South-eastern Asia (035), Central Asia (143), Eastern Asia (030) and Oceania (009)

EMEA: Europe, Middle East and Africa, including Northern Africa (015), Europe (150) and Eastern Europe (151), and Western Asia (145)

LAC: Latin America and the Caribbean, including South America (005), Central America (013) and Caribbean (029)

NA: Northern America (021), including the United States and Canada

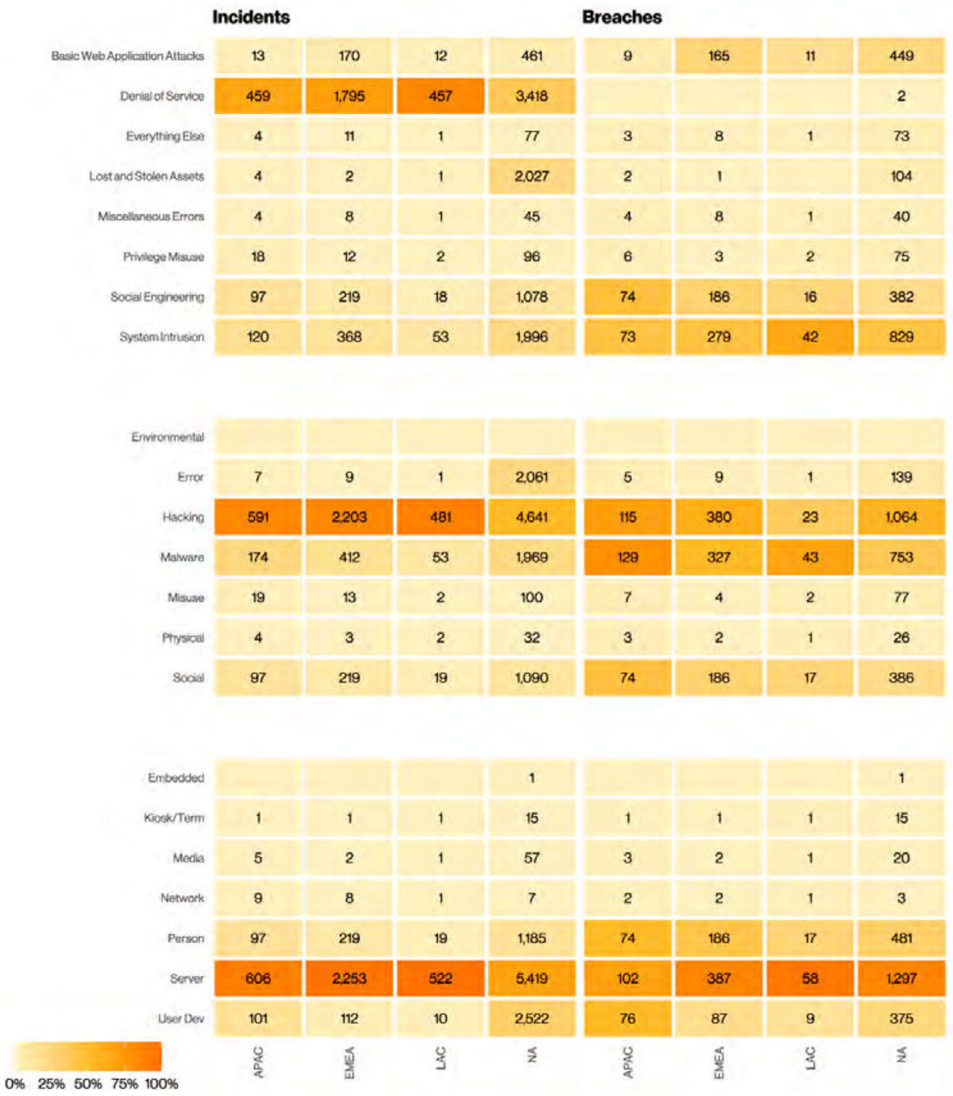
As in previous years, we have sliced and diced our data in many ways, and this time we are presenting the data for the various regions a little differently. Long-time readers will recognize the At-a-Glance tables that we put in each major section, only in this case, we've combined them to give you an easy way to see just how similar (and different) each of the regions are with regard to the frequency, top patterns, etc.

Region	Frequency	Top patterns	Threat actors	Actor motives	Data compromised
APAC	699 incidents, 164 with confirmed data disclosure	Social Engineering, System Intrusion and Basic Web Application Attacks represent 93% of breaches	External (92%), Internal (9%), Partner (2%), Multiple (2%) (breaches)	Financial (61%), Espionage (39%), Convenience (2%), Grudge (2%), Secondary (1%) (breaches)	Internal (56%), Secrets (42%), Other (33%), Credentials (29%) (breaches)
EMEA	2,557 incidents, 637 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 97% of breaches	External (98%), Internal (2%), Multiple (1%) (breaches)	Financial (91%), Espionage (8%), Ideology (1%), Fun (1%) (breaches)	Credentials (53%), Internal (37%), System (35%), Other (15%) (breaches)
LAC	535 incidents, 65 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 94% of breaches	External (95%), Internal (5%), Partner (2%), Multiple (2%) (breaches)	Financial (93%), Espionage (11%), Ideology (2%) (breaches)	System (55%), Internal (32%), Classified (23%), Credentials (23%), Other (19%) (breaches)
NA	9,036 incidents, 1,924 with confirmed data disclosure	System Intrusion, Basic Web Application Attacks and Social Engineering represent 85% of breaches	External (94%), Internal (12%), Multiple (9%), Partner (2%) (breaches)	Financial (99%), Espionage (1%), Grudge (1%) (breaches)	Credentials (67%), Internal (50%), Personal (38%), Other (24%) (breaches)

Table 6. At a glance for regions

---

[58] https://unstats.un.org/unsd/methodology/m49/



	Incidents				Breaches			
	APAC	EMEA	LAC	NA	APAC	EMEA	LAC	NA
Basic Web Application Attacks	13	170	12	461	9	165	11	449
Denial of Service	459	1,795	457	3,418				2
Everything Else	4	11	1	77	3	8	1	73
Lost and Stolen Assets	4	2	1	2,027	2	1		104
Miscellaneous Errors	4	8	1	45	4	8	1	40
Privilege Misuse	18	12	2	96	6	3	2	75
Social Engineering	97	219	18	1,078	74	186	16	382
System Intrusion	120	368	53	1,996	73	279	42	829
Environmental								
Error	7	9	1	2,061	5	9	1	139
Hacking	591	2,203	481	4,641	115	380	23	1,064
Malware	174	412	53	1,969	129	327	43	753
Misuse	19	13	2	100	7	4	2	77
Physical	4	3	2	32	3	2	1	26
Social	97	219	19	1,090	74	186	17	386
Embedded				1				1
Kiosk/Term	1	1	1	15	1	1	1	15
Media	5	2	1	57	3	2	1	20
Network	9	8	1	7	2	2	1	3
Person	97	219	19	1,185	74	186	17	481
Server	606	2,253	522	5,419	102	387	58	1,297
User Dev	101	112	10	2,522	76	87	9	375

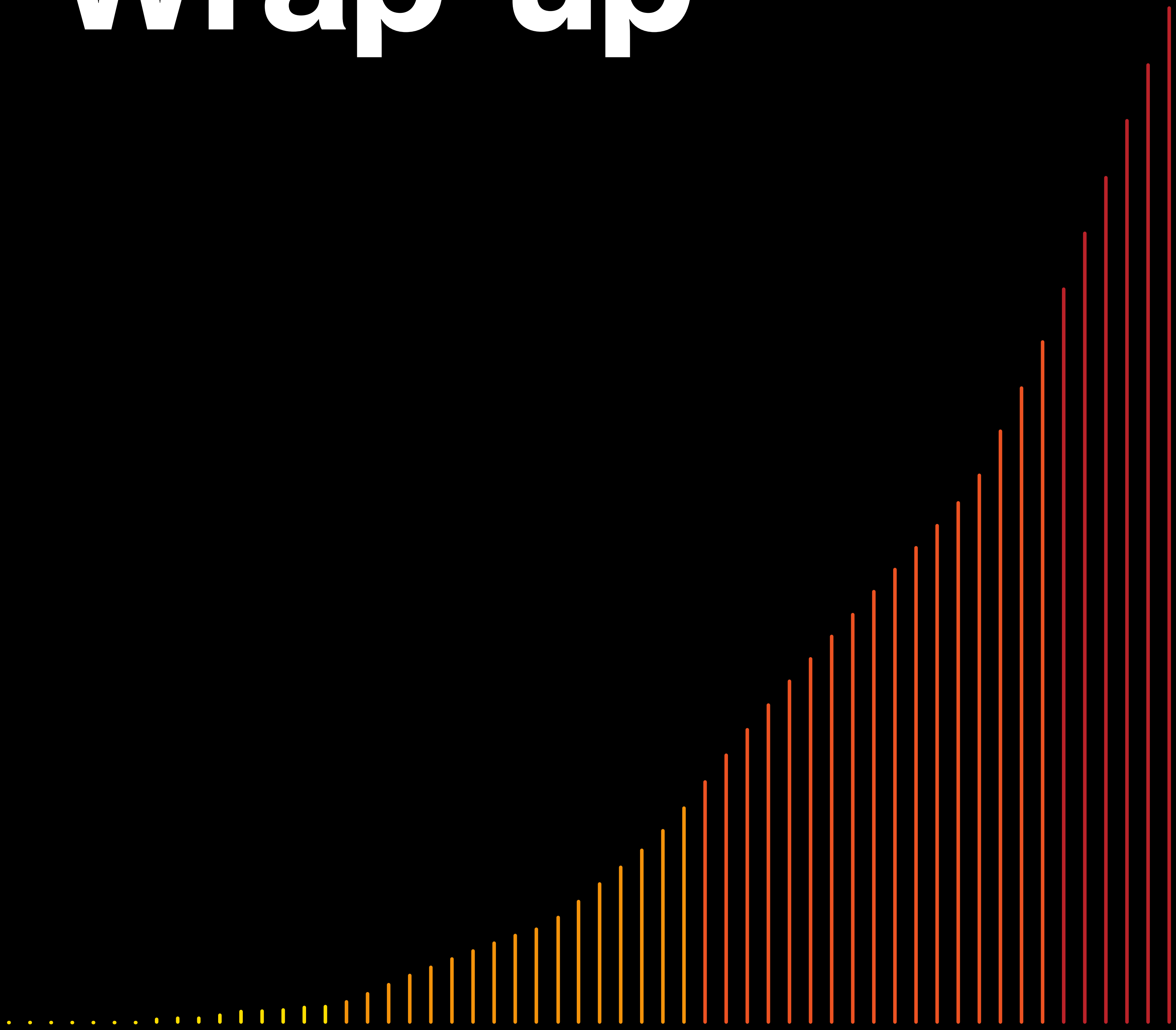
Figure 63. Incidents and breaches by region

It is readily apparent that the System Intrusion pattern is top of the heap for all regions except APAC, where it is still a large problem, just not as pressing as Social Engineering. It is also quite clear that the who and why behind cybercrime is the Financially motivated external actor. We see more variation in the data types favored by these actors in the different regions, and while our data frequently shows us the "what," it rarely tells us the "why." It may be that certain data types are better protected by regulatory requirements in certain regions versus others. It may be some other factor we haven't thought of; it's hard to say. But clearly, Credentials are still figuring prominently and need to be made less valuable when breached (hint: we're looking at you, MFA).

Just feast your eyes on these lovely heatmaps in Figure 63. This is our favorite way to illustrate how different (or similar) these attacks are based on geography. When broken out by pattern and region, you can clearly see that although there are definitely differences (many of which are no doubt based on industry and their resulting common infrastructure partners), there are some concentrations for each region as well as across regions.

Hopefully this is illustrative of what your region—and, when combined with other data in this report, industries and organization size—is most prone to in terms of attacks so that you can better direct your defensive strategy. If you're still unsure where to start and you skipped over the SMB section, it is a good reference for how to apply the information in this report.

6
Wrap-up



This wraps up another year of delving deep into data breaches to mine for useful nuggets of information and analysis.

It is, as always, our hope that you found it instructive, actionable and maybe even fun to read.[59] All of us here on the team feel extremely fortunate to be where we are and doing what we do. We would also like to extend our most sincere gratitude once again to our faithful readers. The feedback and stories you have provided to us throughout the years drives us to work diligently to continually evolve and improve this report.

As always, be well, be prosperous and be prepared for anything.[60]

---

[59] OK, that might be a stretch. How about "not the all-around cure for insomnia"?

[60] Unofficial DBIR team motto, by the way

Year in review

January

The VTRAC Intelligence Analysts experienced déjà vu as we began 2022 tracking attacks exploiting Log4j in much the same way SolarWinds campaigns kicked off 2021. During the first week of December 2021, the Log4j vulnerability became the biggest blip on the InfoSec risk radar. About a week later, VMware observed Log4Shell attacks, and “the majority of the attacks target Linux systems.” Log4j, and especially attacks on VMware, remained a persistent risk issue through 2022. Before the end of the month, Prophet Spider, a notorious initial access broker, was selling VMware Horizons systems breached using Log4j. The Russian Ember Bear threat actor (TA) launched attacks on Ukraine using WhisperGate wiper malware. Microsoft patched a zero-day vulnerability in the Win32k.sys driver. Apple patched a zero-day vulnerability impacting iPhones and iPads.

February

Collection and analysis of intelligence covering cyberattacks supporting Russia’s February 2022 invasion of Ukraine was the most significant activity for VTRAC in February. On and before February 24, the Russian Main Intelligence Directorate (GRU)[61] launched AcidRain wiper malware attacks on the Viasat satellite communications terminals in Ukraine, but significant collateral damage was also done to terminals scattered across Europe. Ukraine was targeted with at least six new wiper malwares by Russian TAs. On February 25, the notorious cybercrime-as-a-service TA, “Conti” announced support for Russia. Two days later, Twitter user “@ContiLeaks” released 400 internal Conti files including 60,000 chat messages. “Ordinary” cyber intelligence in February included zero-day vulnerabilities in Zimbra, Chrome, Apple OS and Adobe Commerce/Magento. Cybercriminals controlling Emotet leveraged the Russia-Ukraine conflict in bait themes in their malspam.

March

Zero-day exploitation of vulnerabilities in Chrome, Firefox, Trend Micro Apex Central and Mitel business telephony components kept enterprise security and patch management teams busy in March. Increased vigilance looking for evidence of Russian-Ukraine cyber-attacks yielded intelligence on APT actors from China, Iran and North Korea. Chinese APT actor Mustang Panda used the Russia-Ukraine conflict in attacks on diplomatic missions, think tanks and ISPs in Mongolia, Vietnam, Myanmar and Russia. New intelligence detailing the exploitation of a vulnerable web application led to lateral exploitation of networks in several US state governments by APT41 (Winnti), another Chinese APT actor. Iranian APT MuddyWater targeted the Arabian Peninsula, Turkey and Pakistan. The largest cryptocurrency theft to date occurred when North Korea’s Lazarus Group stole more than US$620 million from the Ronin Network. North Korean APT Kimsuky targeted a nuclear-related think tank with their signature “BabyShark” malware. The Lapsus$ TA shifted tactics, techniques and procedures (TTP) from ransomware to data theft extortion, claiming compromises at Microsoft, Okta, Nvidia and Samsung.

---

[61] Now known as the Main Directorate of the General Staff of the Armed Forces of the Russian Federation – how’s that for a mouthful?

April

Patch management teams were especially harried in April mitigating zero-day vulnerabilities under attack in the Windows CLFS, Apple OS, Trend Micro security products, Chrome browser and VMware. Sophos firewalls came under attack hours after release of a security advisory and patches. SonicWall, Zyxel and FortiGuard also released security advisories and updates for their firewalls. The VTRAC began collecting more than the usual volume of intelligence on APT-grade actors yielding TTP updates usable by both other TAs and Verizon Cyber Security Consulting clients. A campaign by the Chinese APT-grade actor Deep Panda had been exploiting the ill-famed Log4Shell vulnerability in VMware Horizon servers missing December's patches. We also collected intelligence on Russian state actors attacking Ukraine, including details on the attack on Viasat in February, and four operations by North Korea's Lazarus Group. Attacks by cybercrime TAs including LockBit, FIN7, ALPHV, Hive, CL0P and Conti continued unabated.

May

Vulnerabilities in infrastructure components began to emerge as a recurring theme in 2022. In the wild exploitation commenced within one week of the release of security advisories and patches in vulnerabilities in F5 BIG-IP appliances (CVE-2022-1388) and Zyxel firewalls (CVE-2022-30525). Microsoft patched 74 vulnerabilities in May's Patch Tuesday, including a zero-day Windows LSA Spoofing Vulnerability (CVE-2022-26925). CISA initially added it to their Known Exploited Vulnerabilities Catalog but quickly removed it to avoid outages caused by authentication failures resulting from precipitous domain controller patching. Two infamous malware families, Emotet and REvil, thought to have shut down, each made a resurgence in May, but the controversial ransomware group Conti disbanded. As May ended, intelligence emerged that a Chinese APT actor was exploiting another Windows zero-day vulnerability (CVE-2022-30190) to attack targets in Russia and Belarus. The "Folina" vulnerability was a remote code execution vulnerability in the Microsoft Support Diagnostic Tool (MSDT).

June

Days after the discovery of Folina, Atlassian announced patches for a zero-day remote code execution vulnerability (CVE-2022-26134) in Confluence Data Center and Server. Over the Memorial Day weekend in the United States, Volexity's incident responders had detected suspicious activity on two internet-facing Atlassian Confluence Servers with Behinder web shells installed, probably by Chinese threat actors. Volexity also reported that a zero-day vulnerability in Sophos Firewall (CVE-2022-1040) was being exploited by a Chinese APT actor they labeled, "DriftingCloud." Intelligence indicated that widespread attacks, by the infamous Chinese APT actor Deep Panda, were continuing to successfully exploit Log4j in unpatched VMware Horizon servers.

July

The release of cyber intelligence reports usually precedes the Black Hat USA and DEF CON conferences. The quality, quantity and breadth of those reports in 2022 represented the most significant intelligence for the month of July. Tracking successful TTPs has been an intelligence requirement because our adversaries are adept at learning from open source intelligence (OSINT), making agility in tuning security architecture an imperative. Exploitation of zero-day vulnerabilities in Google's Chrome browser and Windows CSRSS kept patch management teams busy, as did three unexploited critical vulnerabilities in multiple Atlassian products. Intelligence emerged that a ransomware and crypto mining TA had been successfully exploiting one, CVE-2022-26138, since June.

August

In addition to "Folina" a second zero-day remote code vulnerability in the Microsoft Windows Support Diagnostic Tool was discovered, exploited and patched in August. Apple, macOS, iOS and iPadOS plus Google Chrome all had their own zero-day vulnerabilities reported and patched. In early August, current and former employees of Twilio received smishing messages purporting to be from Twilio's IT department calling for a password change. That breach led to the compromise of 9,931 accounts in 130+ organizations, most of which used Okta identity and access management solutions. The threat actor compromised 93 users of Twilio's Authy multifactor authentication solutions. Intelligence emerged attributing these and multiple identity attacks at least as far back as March to the "Scatter Swine" or Oktapus TA.

September

September was the zero-day-palooza month for 2022. Two days into the new month, Google Chrome and Microsoft Edge were patching a zero-day vulnerability in their browsers. Trend Micro mitigated their second zero-day vulnerability of the year following successful in-the-wild attacks on their Apex One security products. And Sophos firewall customers had to patch their second zero-day of the year. The most significant zero-days were attributed to a Chinese APT actor that chained a pair of Windows vulnerabilities quickly nicknamed "ProxyNotShell." VMware servers were also targeted by a Chinese cyberespionage actor employing malicious vSphere installation bundles for ESXi, Linux and Windows servers.

October

Microsoft did not patch “ProxyNotShell” in October’s Patch Tuesday release, but they did release a patch for CVE-2022-41033, an elevation of privilege zero-day. Fortinet patched a zero-day authentication bypass vulnerability in multiple products. More than 1,600 servers were breached by exploiting a zero-day in Zimbra Collaboration Suite, CVE-2022-41352, and tardy patching of three earlier Zimbra vulnerabilities. “Text4Shell” entered the InfoSec lexicon after a new Apache Commons Text library vulnerability, even though no attacks were reported. Two notorious malwares repurposed to expand their target sets: URSNIF and Emotet each exhibited significant TTP shifts, the former from banking Trojan to initial access downloader and the latter awoke from a four-month siesta as the tool of a full-service malware-as-a-service operator. Other zero-day attacks, vulnerabilities and patches were reported in Chrome browser and, separately, iOS and iPadOS.

November

Several strains of malware highlighted InfoSec risk intelligence in November. Forty days after the initial reports of ProxyNotShell attacks on Exchange, Microsoft patched those two vulnerabilities. Microsoft also patched four other zero-days in its products on Patch Tuesday. Chrome browser also mitigated a zero-day vulnerability. Updated intelligence on three malware families were prominent in the VTRAC collections. SocGholish is a JavaScript framework and malware-as-a-service used by cybercriminals to implement drive-by-downloads. Bumblebee, a new malicious loader, first appeared in May and in November began delivering Meterpreter and Cobalt Strike payloads. Cybercriminals controlling the Raspberry Robin worm evolved into initial access brokers for deploying other payloads.

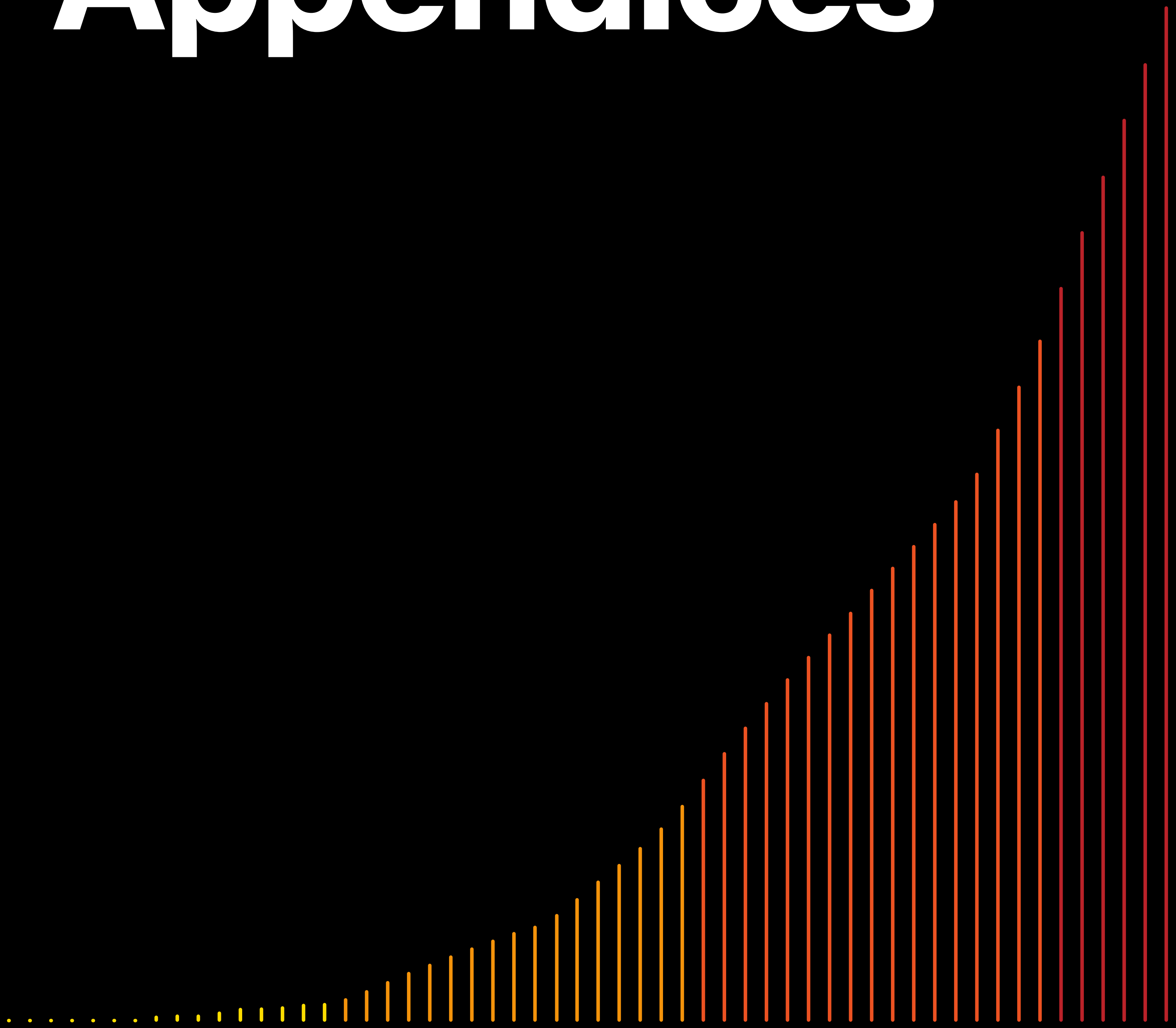
December

Breaking the string of end-of-year InfoSec milestones set in 2020 with SolarWinds Orion and in 2021 by Log4j, December 2022 was comparatively boring. Intelligence indicated several threat actors were abusing Microsoft developer accounts to get malicious drivers signed through their profiles to be used in cyberattacks, including ransomware incidents and SIM swapping operations. The streak of months with attacks exploiting zero-day vulnerabilities was extended with reports of successful attacks on Microsoft, Apple, Fortinet and Citrix products. OWASSRF is a new attack chain exploiting on-premises Exchange Servers using the URL rewrite mitigations provided by Microsoft responding to September’s ProxyNotShell attack chain. The Play ransomware threat actors had exploited OWASSRF to attack at least eight victims. Among the best intelligence collections was a virtual order of battle of TA subordinate to Bureau 121 in the Reconnaissance General Bureau (RGB), North Korea’s military intelligence agency.

Special thanks to Dave Kennedy of the Verizon Threat Research Advisory Center (VTRAC) for his continued support and yearly contribution to this report.

7

Appendices



Appendix A: Methodology

One of the things readers value most about this report is the level of rigor and integrity we employ when collecting, analyzing and presenting data. Knowing our readership cares about such things and consumes this information with a keen eye helps keep us honest. Detailing our methods is an important part of that honesty.

First, we make mistakes. A column transposed here; a number not updated there. We're likely to discover a few things to fix. When we do, we'll list them on our corrections page: verizon.com/business/resources/reports/dbir/2023/corrections/.

Second, we check our work. The same way the data behind the DBIR figures can be found in our GitHub repository,[62] as with last year, we're also publishing our fact check report there as well. It's highly technical, but for those interested, we've attempted to test every fact in the report.

Third, science comes in two flavors: creative exploration and causal hypothesis testing. The DBIR is squarely in the former. While not perfect, we believe we provide the best obtainable version of the truth (to a given level of confidence and under the influence of biases acknowledged below). However, proving causality is best left to randomized control trials. The best we can do is correlation. And while correlation is not causation, they are often related to some extent and often useful.

Non-committal disclaimer

We must reiterate that we make no claim that the findings of this report are representative of all data breaches in all organizations at all times. Even though we believe the combined records from all our contributors more closely reflect reality than any of them in isolation, it is still a sample. And although we believe many of the findings presented in this report to be appropriate for generalization (and our conviction in this grows as we gather more data and compare it to that of others), bias exists.

The DBIR process

Our overall process remains intact and largely unchanged from previous years.[63] All incidents included in this report were reviewed and converted, if necessary, into the VERIS framework to create a common, anonymous aggregate dataset. If you are unfamiliar with the VERIS framework, it is short for Vocabulary for Event Recording and Incident Sharing. It is free to use, and links to VERIS resources are at the beginning of this report.

The collection method and conversion techniques differed between contributors. In general, three basic methods (expounded below) were used to accomplish this:

1. Direct recording of paid external forensic investigations and related intelligence operations conducted by Verizon using the VERIS Webapp
2. Direct recording by partners using VERIS
3. Converting partners' existing schema into VERIS

All contributors received instruction to omit any information that might identify organizations or individuals involved.

Some source spreadsheets are converted to our standard spreadsheet formatted through automated mapping to ensure consistent conversion. Reviewed spreadsheets and VERIS Webapp JavaScript Object Notation (JSON) are ingested by an automated workflow that converts the incidents and breaches within into the VERIS JSON format as necessary, adds missing enumerations and then validates the record against business logic and the VERIS schema. The automated workflow subsets the data and analyzes the results. Based on the results of this exploratory analysis, the validation logs from the workflow and discussions with the partners providing the data, the data is cleaned and reanalyzed. This process runs nightly for roughly two months as data is collected and analyzed.

---

[62] https://github.com/vz-risk/dbir/tree/gh-pages
[63] As does this sentence

Incident data

Our data is non-exclusively multinomial meaning a single feature, such as "Action," can have multiple values (i.e., "Social," "Malware" and "Hacking"). This means that percentages do not necessarily add up to 100%. For example, if there are five botnet breaches, the sample size is five. However, since each botnet used phishing, installed keyloggers and used stolen credentials, there would be five Social actions, five Hacking actions and five Malware actions, adding up to 300%. This is normal, expected and handled correctly in our analysis and tooling.

Another important point is that when looking at the findings, "unknown" is equivalent to "unmeasured." Which is to say that if a record (or collection of records) contains elements that have been marked as "unknown" (whether it is something as basic as the number of records involved in the incident, or as complex as what specific capabilities a piece of malware contained), it means that we cannot make statements about that particular element as it stands in the record—we cannot measure where we have too little information. Because they are "unmeasured," they are not counted in sample sizes. The enumeration "Other," however, is counted as it means the value was known but not part of VERIS (or not one of the other bars if found in a bar chart).

Finally, "Not Applicable," (normally "NA"), may be counted or not counted depending on the claim being analyzed.

This year we have made liberal use of confidence intervals to allow us to analyze smaller sample sizes. We have adopted a few rules to help minimize bias in reading such data. Here we define "small sample" as less than 30 samples.

1. Sample sizes smaller than five are too small to analyze.
2. We won't talk about count or percentage for small samples. This goes for figures, too, and is why some figures lack the dot for the median frequency.
3. For small samples we may talk about the value being in some range or values being greater/less than each other. These all follow the confidence interval approaches listed above.

Incident eligibility

For a potential entry to be eligible for the incident/breach corpus, a couple of requirements must be met. The entry must be a confirmed security incident defined as a loss of confidentiality, integrity or availability. In addition to meeting the baseline definition of "security incident," the entry is assessed for quality. We create a subset of incidents (more on subsets later) that pass our quality filter. The details of what is a "quality" incident are:

- The incident must have at least seven enumerations (e.g., threat actor variety, threat action category, variety of integrity loss, et al.) across 34 fields OR be a DDoS attack. Exceptions are given to confirmed data breaches with less than seven enumerations.
- The incident must have at least one known VERIS threat action category (hacking, malware, etc.).

In addition to having the level of details necessary to pass the quality filter, the incident must be within the timeframe of analysis, (November 1, 2021, to October 31, 2022, for this report). The 2022 caseload is the primary analytical focus of the report, but the entire range of data is referenced throughout, notably in trending graphs. We also exclude incidents and breaches affecting individuals that cannot be tied to an organizational attribute loss. If your friend's laptop was hit with Trickbot, it would not be included in this report.

Lastly, for something to be eligible for inclusion into the DBIR, we have to know about it, which brings us to several potential biases we will discuss below.

Acknowledgement and analysis of bias

Many breaches go unreported (though our sample does contain many of those). Many more are as yet unknown by the victim (and thereby unknown to us). Therefore, until we (or someone) can conduct an exhaustive census of every breach that happens in the entire world each year (our study population), we must use sampling. Unfortunately, this process introduces bias.

Breaches

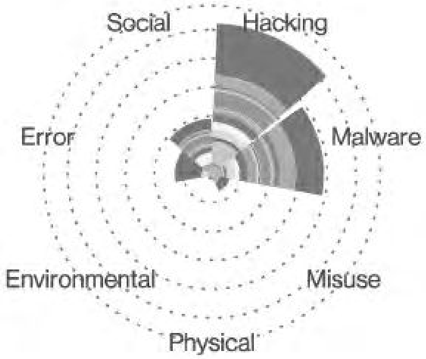


Figure 64. Individual contributors per Action

Breaches

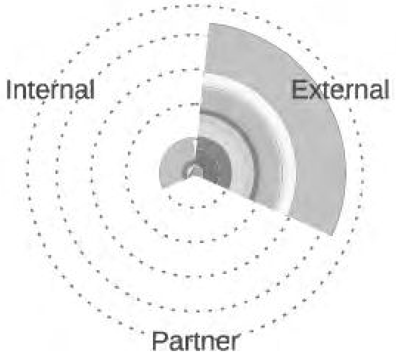


Figure 65. Individual contributors per Actor

Breaches

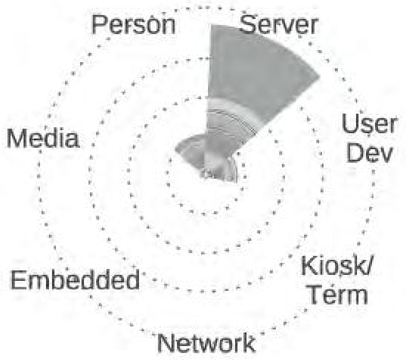


Figure 66. Individual contributors per Asset

Breaches

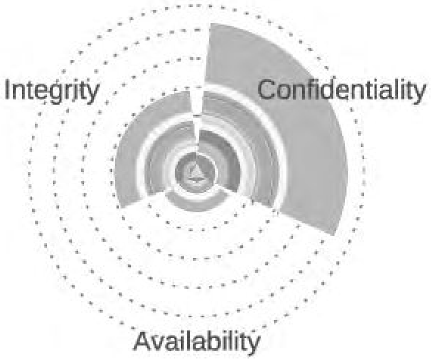


Figure 67. Individual contributors per Attribute

The first type of bias is random bias introduced by sampling. This year, our maximum confidence is +/- 0.7% for incidents and +/- 1.4% for breaches, which is related to our sample size. Any subset with a smaller sample size is going to have a wider confidence margin. We've expressed this confidence in the complementary cumulative density (slanted) bar charts, hypothetical outcome plot (spaghetti) line charts and quantile dot plots.

The second source of bias is sampling bias. We strive for "the best obtainable version of the truth" by collecting breaches from a wide variety of contributors. Still, it is clear that we conduct biased sampling. For instance, some breaches, such as those publicly disclosed, are more likely to enter our corpus, while others, such as classified breaches, are less likely.

The four figures on the left are an attempt to visualize potential sampling bias. Each radial axis is a VERIS enumeration, and we have stacked bar charts representing our data contributors. Ideally, we want the distribution of sources to be roughly equal on the stacked bar charts along all axes. Axes only represented by a single source are more likely to be biased. However, contributions are inherently thick tailed, with a few contributors providing a lot of data and a lot of contributors providing a few records within a certain area. Still, we mostly see that most axes have multiple large contributors with small contributors adding appreciably to the total incidents along those axes.

You'll notice rather large contributions on many of the axes. While we'd generally be concerned about this, they represent contributions aggregating several other sources, not actual single contributions. It also occurs along most axes, limiting the bias introduced by that grouping of indirect contributors.

The third source of bias is confirmation bias. Because we use our entire dataset for exploratory analysis, we cannot test specific hypotheses. Until we develop a collection method for data breaches beyond a sample of convenience, this is probably the best that can be done.

As stated above, we attempt to mitigate these biases by collecting data from diverse contributors. We follow a consistent multiple-review process, and when we hear hooves, we think horses, not zebras.[64] We also try to review findings with subject matter experts in the specific areas ahead of release.

Data subsets

We already mentioned the subset of incidents that passed our quality requirements, but as part of our analysis there are other instances where we define subsets of data. These subsets consist of legitimate incidents that would eclipse smaller trends if left in. These are removed and analyzed separately, though may not be written about if no relevant findings were, well, found. This year we have two subsets of legitimate incidents that are not analyzed as part of the overall corpus:

1. We separately analyzed a subset of web servers that were identified as secondary targets (such as taking over a website to spread malware).
2. We separately analyzed botnet-related incidents.

Both subsets were separated the last six years as well.

Finally, we create some subsets to help further our analysis. In particular, a single subset is used for all analysis within the DBIR unless otherwise stated. It includes only quality incidents as described above and excludes the aforementioned two subsets.

Non-incident data

Since the 2015 issue, the DBIR includes data that requires the analysis that did not fit into our usual categories of "incident" or "breach." Examples of non-incident data include malware, patching, phishing and DDoS. The sample sizes for non-incident data tend to be much larger than the incident data but from fewer sources. We make every effort to normalize the data (for example, weighting records by the number contributed from the organization so all organizations are represented equally). We also attempt to combine multiple partners with similar data to conduct the analysis wherever possible. Once analysis is complete, we try to discuss our findings with the relevant partner or partners so as to validate it against their knowledge of the data.

---

[64] A unique finding is more likely to be something mundane, such as a data collection issue, than an unexpected result.

Appendix B: VERIS mappings to MITRE ATT&CK®

When it comes to sailing the stormy seas of the cybersecurity world, a map comes in handy to help you chart your direction. We consider the DBIR to be one of those maps, helping organizations navigate the complicated and ever-changing conditions of the cybersecurity landscape. To make sure this map is the most accurate possible, we have created the VERIS Framework,[65] which captures most of the important components of data breaches in order to facilitate risk-oriented decision making for our weary cyber mariners.

Over the years, new guiding frameworks have been created that provide different levels of detail, MITRE ATT&CK® being by far the most popular. We have worked with MITRE Engenuity and the Center for Threat Informed Defense[66] to capture the relationships between VERIS to ATT&CK so that organizations can leverage the benefits of both in their navigation.

The results of that work are remarkable: ATT&CK provides excellent tactical and technical details into the specific techniques the threat actors leverage, while VERIS provides a strategic view of the landscape, covering a wider range of possible mishaps. Errors, for instance, are present in 9% percent of breaches this year but are out of scope in ATT&CK. When VERIS and ATT&CK are combined, they provide you with a clearer view of what type of assets were impacted and what type of victims those assets belonged to while still preserving the specifics of the attack techniques that were leveraged.

This combination of forces is timely due to the increased regulatory pressure of reporting data breaches to governments, although there is no commonly accepted format in how this reporting should be done. We, of course, cannot opine on the need for such regulations,[67] but we would like to do our part to make sure that organizations have the right tooling to reduce their burden as new laws come to fruition.

The second version of this mapping has just been released as of April 6, 2023, and we are very excited about it. In addition to VERIS Actions, a lot of thought was put into mapping Attributes. To make it better, Actors were mapped to ATT&CK Groups.[68] There are also new mappings to ATT&CK for Mobile and ATT&CK for ICS.

If this interests you at all, please hop over to https://center-for-threat-informed-defense.github.io/attack_to_veris/ for all the details of the work. Even if it doesn't,[69] you are already reaping the benefits of the work thanks to the ATT&CK Technique mappings we have added to some select Incident Patterns to help you in your epic journey to "full control coverage."

Our team puts a lot of thought and energy into trying to make the VERIS Framework more accessible and helpful for all. If you are curious about the framework or have tried it in the past and want to check what's new, get in touch with the DBIR team at dbir@verizon.com.

---

65 https://verisframework.org/
66 https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/
67 Who are we kidding? We would love to have more data to analyze!
68 https://attack.mitre.org/groups/
69 How dare you?

Appendix C: VTRAC 20-year retrospective

**By Chris Novak,
Managing Director
Cyber Security Consulting
Verizon**

It's hard to believe that the Verizon Threat Research Advisory Center (VTRAC) is 20 years old! I've had the unique pleasure of being part of the team since the very beginning—or should I say the "zero-day"?

Over those 20 years, we've had a few different names but always the same passionate team behind the scenes. Back then, I was part of a small gaggle of geeks in New York City, always having a suitcase packed and ready to hop a flight to anywhere to take on the next big data breach investigation. Our forensic lab at the time was a collection of systems that didn't even fill a single full-height server rack.

It bears reminding that, 20 years ago, "cybersecurity" was not a commonly used or understood word. If you asked the average person what "cyber" was, you would probably get back responses that sounded like something from a science fiction movie. There was no such thing as a cybersecurity college degree—the closest thing that existed at the time was a computer science or engineering degree. Today, there are hundreds of universities around the world that not only offer cybersecurity bachelor's degrees, but also master's degrees and Ph.D.s.

I can still remember some of the first data breaches I ever investigated. Old timers will appreciate the days when we showed up onsite with our "medical bag"—typically a bag that had a binder of bootable floppy disks, a collection of assorted cables, and a variety of hard drives and enclosures. As mentioned above, hardly anyone knew what cybersecurity was back then, and the average person had no idea of the purpose of the equipment in that medical bag. In a world just following 9/11, going through airport security with that bag of odd-looking electronics and cables guaranteed that I was frequently the lucky winner of "random" extra screening. If only that luck carried over into a few of the trips to Vegas ...

Today, we rarely need to travel. We have enterprise tools that can facilitate remote forensic evidence collection from anywhere in the world. Taking advantage of our telecommunications backbone and advances in cellular connectivity, we're even able to provide immediate emergency and out-of-band communications via 5G, allowing us to collect forensic data at speeds in excess of 1 Gbps, even if the victim organization has its own network, systems or infrastructure outages.

The then and now comparisons over the last 20 years are staggering to consider. Today, we have exponentially more people on our team, with incredible diversity of backgrounds and geographic locations. The VTRAC supports organizations across more than 100 countries. We not only have several physical lab locations around the world but also cloud-based and client on-premises lab locations to care for nearly every conceivable data privacy and sovereignty concern.

Of course, I cannot forget to mention the incredible work of the DBIR team that makes this very publication possible. Many have heard me say that the DBIR is my third child. It was born 16 years ago as part of an early incarnation of VTRAC (back then we were called the RISK Team) with a vision of sharing our data breach insights with the world. Metaphorically, I heard it say its first words and watched it take its first steps alongside the other co-creators. Thankfully, I don't have to save for the DBIR's college tuition.[70]

I couldn't be prouder of what the past and present members of the VTRAC have built and accomplished over the past 20 years. It is the passion and dedication of each and every team member that contributes to our long client tenure, never having missed a contractual service level agreement, world-class thought leadership and consistent rating as a leader by industry analysts.

I look forward to the adventures, innovation and excitement to come in our next 20 years!

Happy 20th birthday, VTRAC!

—Chris Novak

---

[70] Editor's note: We hope the DBIR is actually helping you pay for tuition for your human children.

Appendix D: Contributing organizations

A

Akamai Technologies

Ankura

Apura Cyber Intelligence

B

Bit-x-bit

BitSight

BlackBerry

C

Censys, Inc.

Center for Internet Security

Cequence Security

CERT Division of Carnegie Mellon University's Software Engineering Institute

CERT – European Union

CERT Polska

Check Point Software Technologies Ltd.

Chubb

Coalition

Computer Incident Response Center Luxembourg (CIRCL)

Coveware

CrowdStrike

Cybersecurity and Infrastructure Security Agency (CISA)

CyberSecurity Malaysia, an agency under the Ministry of Communications and Multimedia (KKMM)

Cybersixgill

CYBIR

D

Dell

Department of Government Services, Victorian State Government, Australia

DomainTools

E

Energy Analytic Security Exchange (EASE)

Edgescan

Elevate Security

Emergence Insurance

EUROCONTROL

Eviden

F

Federal Bureau of Investigation – Internet Crime Complaint Center (FBI IC3)

Fortinet

G

Global Resilience Federation

GreyNoise

H

HackEDU

I

Irish Reporting and Information Security Service (IRISS-CERT)

Ivanti

J

JPCERT/CC

K

K-12 Security Information Exchange (K-12 SIX)

Kaspersky

KordaMentha

L

Legal Services Information Sharing and Analysis Organization (LS-ISAO)

M

Malicious Streams

Maritime Transportation System ISAC (MTS-ISAC)

mnemonic

N

NetDiligence®

NETSCOUT

O

Okta

OpenText Cybersecurity

P

Palo Alto Networks

Proofpoint

S

S21sec

SecurityTrails, a Recorded Future Company

Shadowserver Foundation

SISAP – Sistemas Aplicativos

Shodan

Swisscom

U

U.S. Secret Service

V

VERIS Community Database

Verizon Cyber Risk Programs

Verizon Cyber Security Consulting

Verizon DDoS Defense

Verizon Network Operations and Engineering

Verizon Threat Research Advisory Center (VTRAC)

Vestige Digital Investigations

W

WatchGuard Technologies, Inc.

Akamai	ankura	apura	bit-x-bit SM	BITSIGHT
BlackBerry	censys	CIS Center for Internet Security	CEQUENCE	Carnegie Mellon University Software Engineering Institute
CERT-EU FOR THE EU INSTITUTIONS, BODIES AND AGENCIES	NASK CERT.PL>_	CHECK POINT	CHUBB	Coalition
CIRCL Computer Incident Response Center Luxembourg	COVEWARE	CROWDSTRIKE	CISA CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY	CyberSecurity MALAYSIA
cybersixgill	CYBIR	DELL Technologies	VICTORIA State Government Australia	DomainTools
EASE Energy Analytic Security Exchange	edgescan	Elevate Security	emergence	EUROCONTROL
EVIDEN	IC3 FEDERAL BUREAU OF INVESTIGATION INTERNET CRIME COMPLAINT CENTER	FORTINET	GLOBAL RESILIENCE FEDERATION	GREYNOISE

Hack_EDU	IRISS Irish Reporting and Information Security Service	ivanti	JPCERT CC®	K12 SIX
kaspersky	KordaMentha	LEGAL SERVICES ISAO	Malicious Streams	Maritime Transportation System Information Sharing and Analysis Center
mnemonic Securing your business.	NetDiligence®	NETSCOUT.	okta	opentext™
paloalto NETWORKS®	proofpoint. Security Awareness Training	S21 SEC Cyber Solutions by Thales	SecurityTrails A Recorded Future® Company	SHADOWSERVER Lighting the way to a more secure Internet
SISAP Sistemas Aplicativos	SHODAN	swisscom	United States Secret Service	V C D B
Verizon Cyber Risk Programs	**Verizon Cyber Security Consulting**	**Verizon DDoS Defense**	**Verizon Network Operations and Engineering**	**Verizon Threat Research Advisory Center (VTRAC)**
VESTIGE Digital Investigations	WatchGuard®			

© 2023 Verizon.