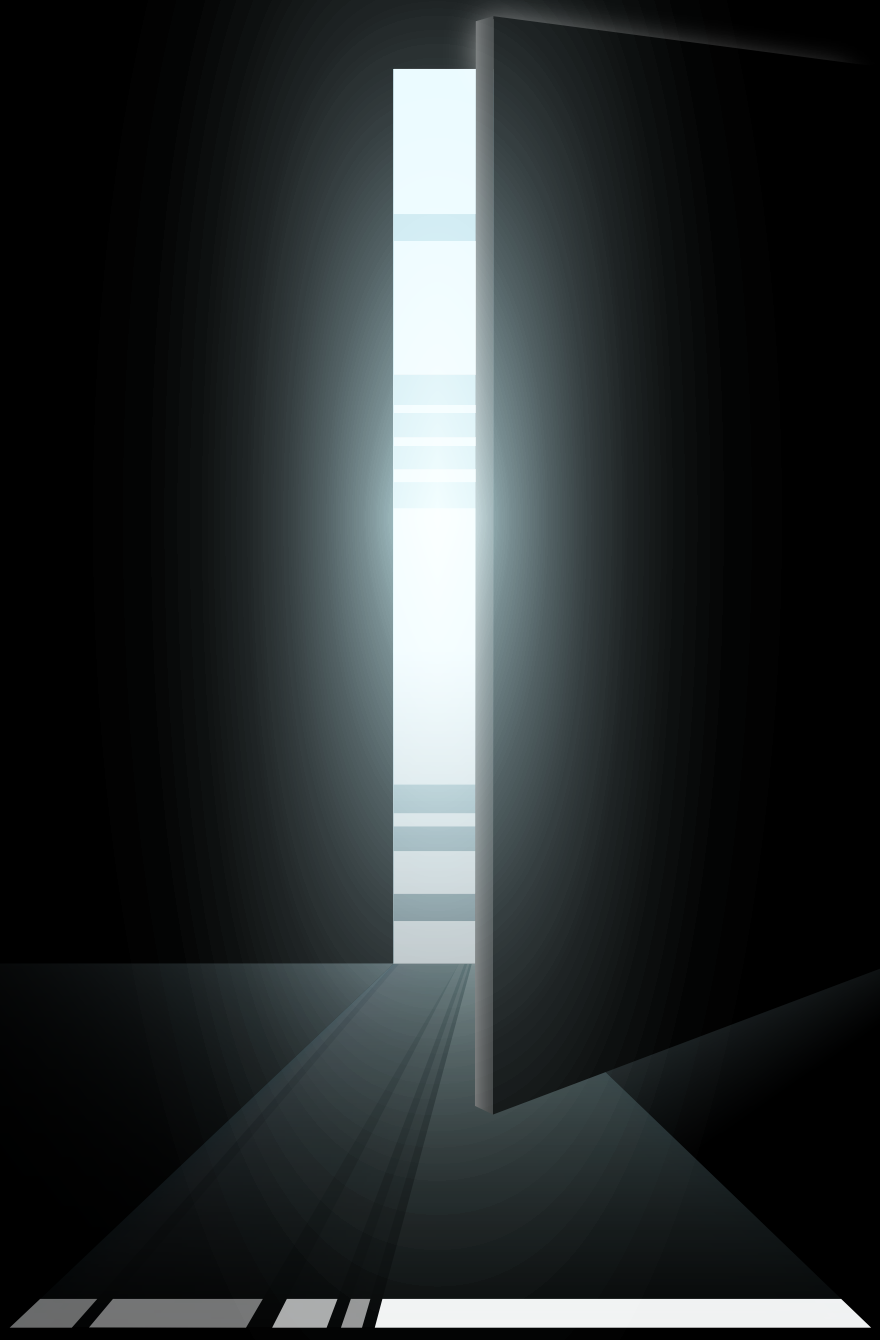
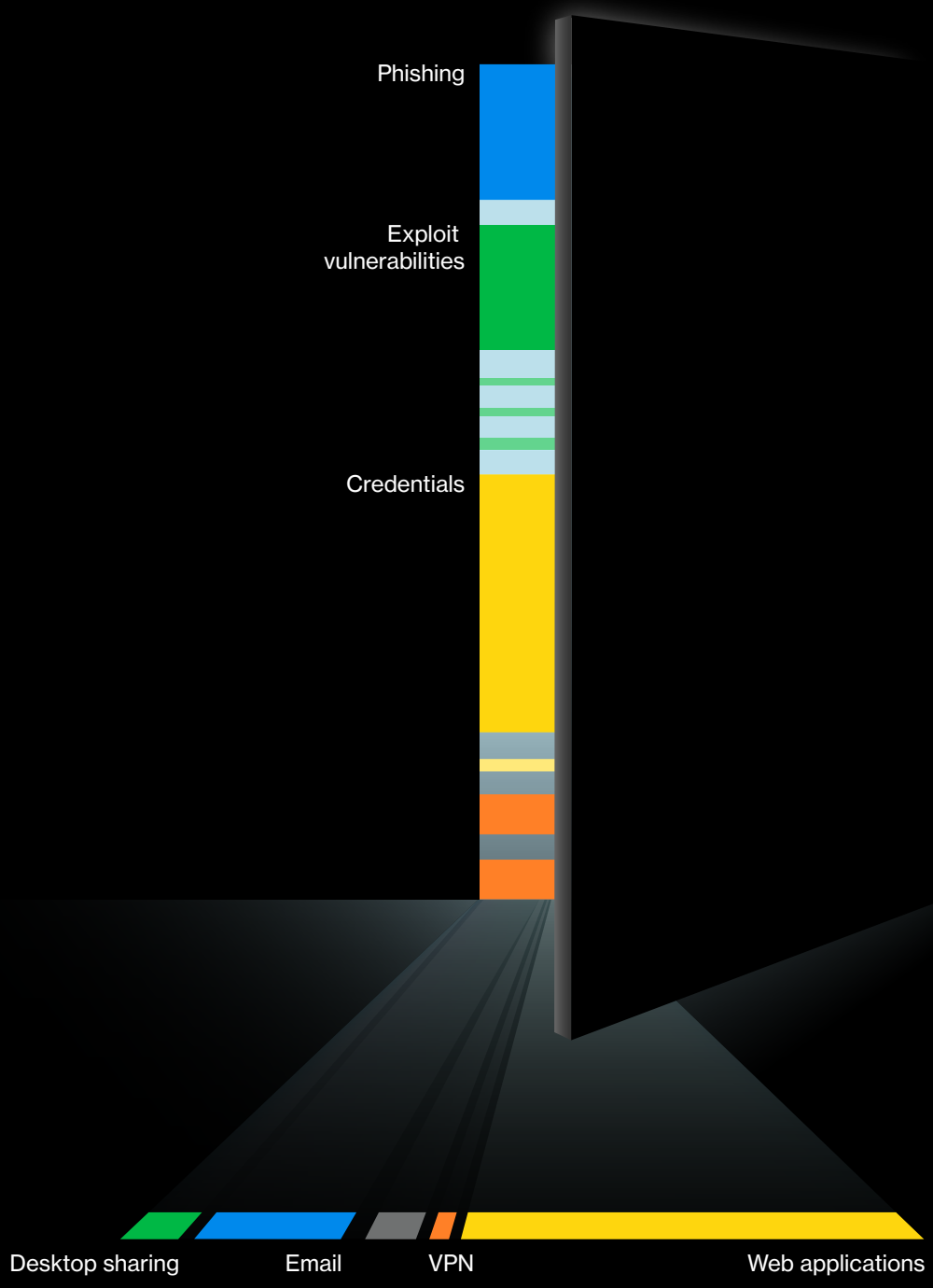
2024 Data Breach Investigations Report



verizon business


Phishing
Exploit vulnerabilities
Credentials
Desktop sharing
Email
VPN
Web applications

About the cover

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

Table of contents

1

Introduction 5
Helpful guidance 6
Summary of findings 7

2

Results and analysis

Results and analysis: Introduction 11
VERIS Actors 15
VERIS Actions 18
VERIS Assets 23
VERIS Attributes 25

3

Incident Classification Patterns

Incident Classification Patterns: Introduction 28
System Intrusion 30
Social Engineering 36
Basic Web Application Attacks 42
Miscellaneous Errors 47
Denial of Service 49
Lost and Stolen Assets 51
Privilege Misuse 53

4

Industries

Industries: Introduction 56
Accommodation and Food Services 60
Educational Services 61
Financial and Insurance 62
Healthcare 64
Information 66
Manufacturing 67
Professional, Scientific and Technical Services 69
Public Administration 70
Retail 72

5

Regions

Regional analysis 75

6

Wrap-up

Year in review 81

7

Appendices

Appendix A: How to read this report 86
Appendix B: Methodology 88
Appendix C: U.S. Secret Service 92
Appendix D: Using the VERIS Community Database (VCDB) to Estimate Risk 94
Appendix E: Contributing organizations 96

Introduction

Greetings! Welcome to Verizon's 2024 Data Breach Investigations Report (DBIR). This year marks the 17th edition of this publication, and we are thrilled to welcome back our old friends and say hello to new readers. As always, the aim of the DBIR is to shine a light on the various Actor types, the tactics they utilize and the targets they choose. Thanks to our talented, generous and civic-minded contributors from around the world who continue to stick with us and share their data and insight, and deep appreciation for our very own Verizon Threat Research Advisory Center (VTRAC) team (rock stars that they are). These two groups enable us to examine and analyze relevant trends in cybercrime that play out on a global stage across organizations of all sizes and types.

From year to year, we see new and innovative attacks as well as variations on tried-and-true attacks that still remain successful. From the exploitation of well-known and far-reaching zero-day vulnerabilities, such as the one that affected MOVEit, to the much more mundane but still incredibly effective Ransomware and Denial of Service (DoS) attacks, criminals continue to do their utmost to prove the old adage "crime does not pay" wrong.

The shifting landscape of cyber threats can be confusing and overwhelming. When, in addition to the attack types mentioned above, one throws in factors such as the human element and/or poorly protected passwords, things become even more confused. One might be forgiven for viewing the current state of cybersecurity as a colorful cyber Mardi Gras parade. Enterprise floats of all shapes and sizes cruising past a large crowd of threat actors who are shouting out gleefully "Throw me some creds!" Of course, human nature being what it is, all too often, the folks on the floats do just that. And, as with all such parades, what is left in the aftermath isn't necessarily pretty. The past year has been a busy one for cybercrime. We analyzed 30,458 real-world security incidents, of which 10,626 were confirmed data breaches (a record high!), with victims spanning 94 countries.

While the general structure of the report remains the same, long-time readers may notice a few changes. For example, the "first-time reader" section is now located in Appendix A rather than at the beginning of the report. But we do encourage those who are new to the DBIR to give it a read-through before diving into the report. It should help you get your bearings.

Last, but certainly not least, we extend a most sincere thanks yet again to our contributors (without whom we could not do this) and to our readers (without whom there would be no point in doing it).

Sincerely,

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

Very special thanks to:
– Christopher Novak for his continued support and insight
– Dave Kennedy and Erika Gifford from VTRAC
– Kate Kutchko, Marziyeh Khanouki and Yoni Fridman from the Verizon Business Product Data Science Team

Helpful guidance

About the 2024 DBIR incident dataset

Each year, the DBIR timeline for in-scope incidents is from November 1 of one calendar year through October 31 of the next calendar year. Thus, the incidents described in this report took place between November 1, 2022, and October 31, 2023. The 2023 caseload is the primary analytical focus of the 2024 report, but the entire range of data is referenced throughout, notably in trending graphs. The time between the latter date and the date of publication for 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. The jokes, sadly, do not write themselves.

Credit where credit is due

Turns out folks enjoy citing the report, and we often get asked how to 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 2024 Data Breach Investigations Report" and (b) the 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 the PDF.

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

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

If your organization aggregates incident or security data and is interested in becoming a contributor to the annual Verizon DBIR (and we hope you are), the process is very easy and straightforward. Please email us at **dbircontributor@verizon.com**.

Summary of findings

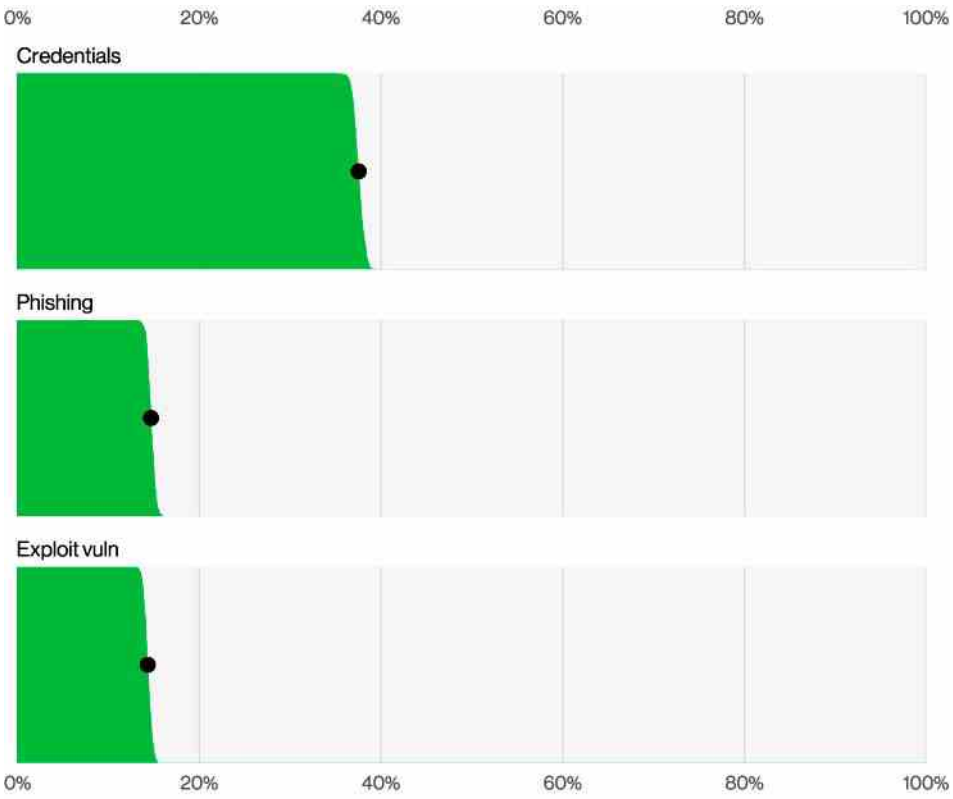


Figure 1. Select ways-in enumerations in non-Error, non-Misuse breaches (n=6,963)

Our ways-in analysis witnessed a substantial growth of attacks involving the exploitation of vulnerabilities as the critical path to initiate a breach when compared to previous years. It almost tripled (180% increase) from last year, which will come as no surprise to anyone who has been following the effect of MOVEit and similar zero-day vulnerabilities. These attacks were primarily leveraged by Ransomware and other Extortion-related threat actors. As one might imagine, the main vector for those initial entry points was Web applications.

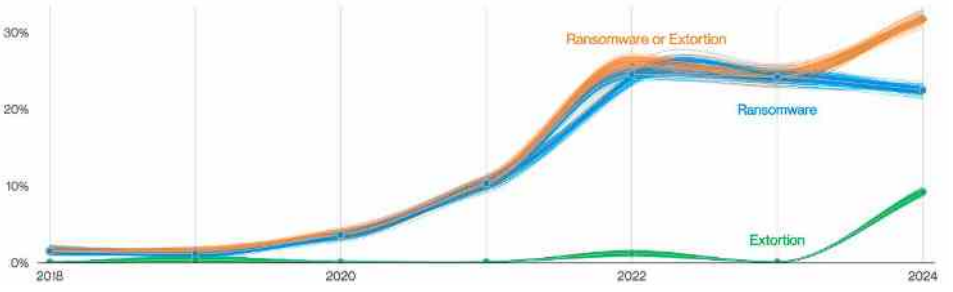


Figure 2. Ransomware and Extortion breaches over time

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

Figure 3. Select key enumerations in breaches

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

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

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

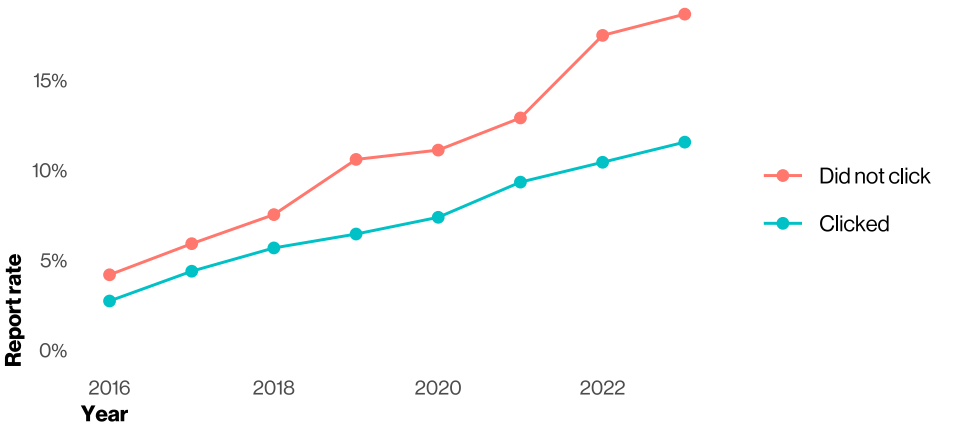


Figure 4. Phishing email report rate by click status

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

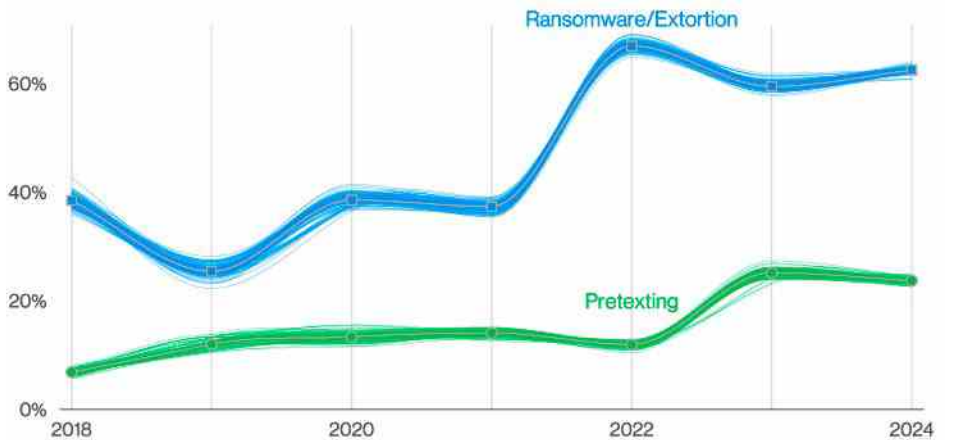


Figure 5. Select action varieties in Financial motive over time

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

Over the past three years, the combination of Ransomware and other Extortion breaches accounted for almost two-thirds (fluctuating between 59% and 66%) of those attacks. According to the FBI's Internet Crime Complaint Center (IC3) ransomware complaint data, the median loss associated with the combination of Ransomware and other Extortion breaches has been $46,000, ranging between $3 (three dollars) and $1,141,467 for 95% of the cases. We also found from ransomware negotiation data contributors that the median ratio of initially requested ransom and company revenue is 1.34%, but it fluctuated between 0.13% and 8.30% for 80% of the cases.

Similarly, over the past two years, we have seen incidents involving Pretexting (the majority of which had Business Email Compromise [BEC] as the outcome) accounting for one-fourth (ranging between 24% and 25%) of financially motivated attacks. In both years, the median transaction amount of a BEC was around $50,000, also according to the FBI IC3 dataset.

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.[1]

Because 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.

This year we onboarded a good number of new contributors and reached an exciting milestone of more than 10,000 breaches analyzed in a single edition.[2] It is an enormous amount of work to organize and analyze, but it is also incredibly gratifying to be able to present these results to you.

In an attempt to be more actionable, we would like to use this section to discuss some high-level findings that transcend the fixed structure of the Vocabulary for Event Recording and Incident Sharing (VERIS) 4As (Actor, Action, Asset and Attribute) and expand on some of the key findings we have been highlighting over the past few years.

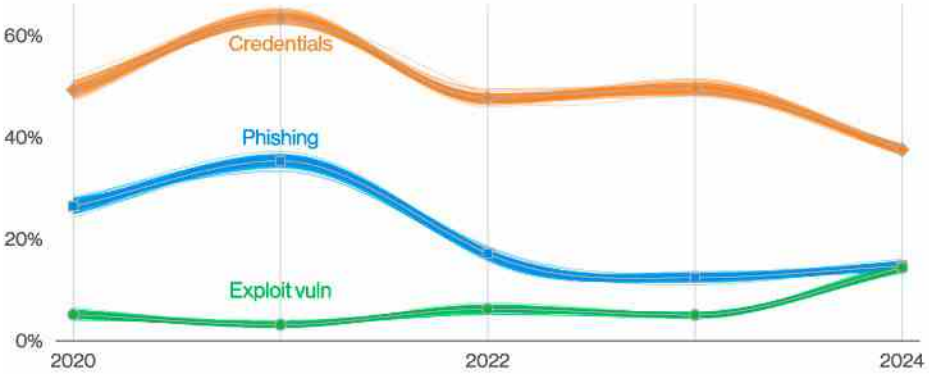


Figure 6. Select ways-in enumerations in non-Error, non-Misuse breaches over time

Ways into your sensitive data's heart

One of the actionable perspectives we have created has been the ways-in analysis, in which we try to make sense of the initial steps into breaches to help predict how to best avoid or prevent them. We still have plenty of unknown Actions and vectors dispersed throughout the dataset as investigation processes and disclosure patterns widely differ across our data contributors,[3] but this view of what we know for sure has remained stable and representative over the years.

Figure 6 paints a clear picture of what has been the biggest pain point for everyone this year. This 180% increase in the exploitation of vulnerabilities as the critical path action to initiate a breach will be of no surprise to anyone who has been following the MOVEit vulnerability and other zero-day exploits that were leveraged by Ransomware and Extortion-related threat actors.

This was the sort of result we were expecting in the 2023 DBIR when we analyzed the impact of the Log4j vulnerabilities. That anticipated worst case scenario discussed in the last report materialized this year with this lesser known—but widely deployed—product. We will be diving into additional details of MOVEit and vulnerability exploitation in the "Action" and "System Intrusion" pattern sections.

1 Have you checked out the VERIS Community Database (VCDB) yet? You should, it's awesome! (https://verisframework.org/vcdb.html)

2 We also passed our cumulative 1 million incident milestone as we forecast in the 2023 DBIR, but we are only mentioning this here in the footnote to not aggravate the report; it was very disappointed that 1 million is not enough to retire on in this economy.

3 We're not throwing shade—different types of contributing organizations focus on what is most relevant for them, as well they should.

To dig further into this concept of the ways in, we are presenting a new slice of the data, where we are overlaying those different types of Actions with their most popular vectors to help focus response and planning efforts. You can take a peek at those results in Figure 7.

Phishing attacks mostly having an Email vector is rather self-explanatory,[4] so we would like to focus on the concentration of the Web application vector prevalence for both credentials and exploit vulnerability. The presence of Credentials in the graphic should not be surprising as it carries a large share of the guilt for our Basic Web Application Attacks pattern (i.e., getting unauthorized access to cloud-based email and collaboration accounts). But recency bias might make folks doubt the prevalence of exploitation of vulnerabilities. Because this report is being written in the beginning of 2024, the focus has been on zero-day (or near-zero-day) vulnerabilities in virtual private network (VPN) software.[5]

Naturally, the share of VPN vector in the exploit vuln variety will likely increase for our 2025 report to reflect those trends, but the bottom line is again self-evident and self-explanatory. Anything that adds to your attack surface on the internet can be targeted and potentially be the first foothold for an external threat actor, and as such, the focus should be to try to keep footholds to a minimum.

No matter how you feel about your VPN software right now, having as many of your web applications as possible behind it might be a better strategy than having to worry about emergency overnight patching of the software—and all the other dependencies that power the web applications themselves. This will not completely mitigate the risk and will not be the right fit for all organizations, but in the worst-case scenario, the Cybersecurity Infrastructure and Security Agency (CISA) might have you rip out only one tool from your network as opposed to several.

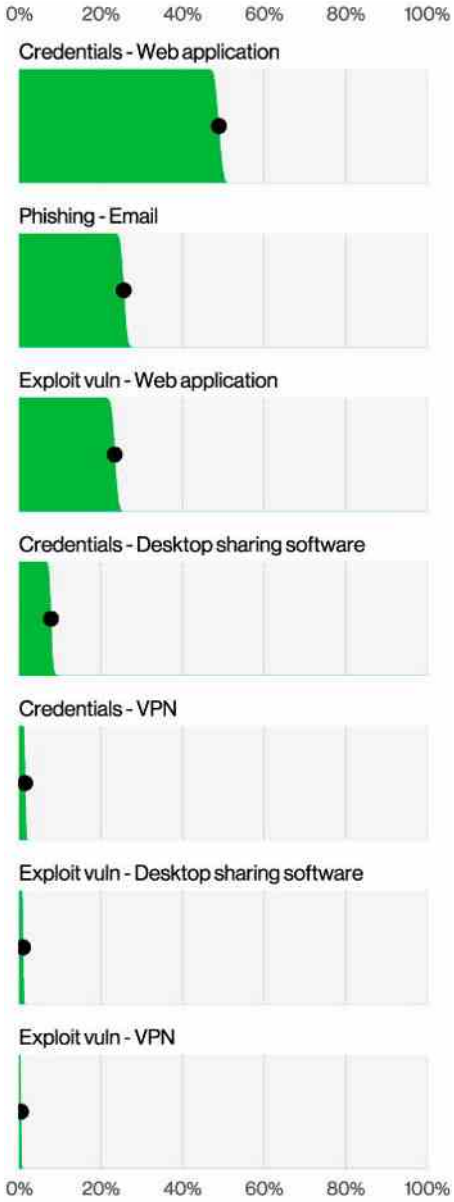


Figure 7. Select ways-in variety and vector enumerations in non-Error, non-Misuse breaches (n=2,770)

Anyway, all this nuance does not affect our opinion of having desktop sharing software directly connected to the internet. Go fix that pronto, please.

We are only human after all.

One other combined metric we have been tracking for a few years is related to the human element in breaches. There is a lot of focus on how fully automated attacks can ruin an organization's day,[6] but it is often surprising how much the people inside the company can have a positive effect on security outcomes.

This year, we have tweaked our human element metric a bit so its impact and action opportunities are clearer. You see, when DBIR authors (and the whole industry in general) would discuss this metric, it would be alongside an opportunity gap for security training and awareness. It is not perfect, but if you had a clear investment path that could potentially improve the outcomes of more than two-thirds of potential breaches, you might at least sit down and listen.

It turns out that our original formula for what was included in the human element metric built in Privilege Misuse pattern breaches, which are the cases involving malicious insiders. Having those mixed with honest mistakes by employees did not make sense if our aim was to suggest that those could be mitigated by security awareness training.[7]

4 And an incredible L for the *ishing portmanteau enthusiasts

5 Unless by now we have successfully ripped them out of our networks entirely and are back to our smoke signals and carrier pigeon ways.

6 We ourselves were just talking about the growth of exploitation of vulnerabilities as a pathway into breaches.

7 We dread to think what "awareness training" for malicious insiders would look like.

Figure 8 showcases the new human element over time (with malicious insiders removed) to provide a better frame of reference for our readers going forward. It is present in more than two-thirds of breaches as foreshadowed two paragraphs ago, more precisely in 68% of breaches. It is statistically similar to our findings last year, which means that in a certain way, the increases we had across the board in the Miscellaneous Errors pattern (human-centric) and as a result of the MOVEit vulnerability (automated) were similar in scope as far as this metric is concerned.

Fans of the "original flavor" human element are not missing much because the inclusion of the Misuse action would have brought the percentage to 76%, statistically only slightly more than the previous report's 74%. Still, we prefer the clearer definition going forward, and we will leave the analysis of those bothersome insiders and their misdeeds to the "Privilege Misuse" pattern section.

The weakest links in the chain of inter-connection

Finally, as we review the big picture of how the threat landscape changed this year,[8] we would like to introduce a new metric that we will be tracking going forward. As the growth of exploitation of vulnerabilities and software supply chain attacks make them more commonplace in security risk register discussions, we would like to suggest a new third-party metric where we embrace the broadest possible interpretation of the term.[9] Have a peek at Figure 9, where we calculated a supply chain interconnection influence in 15% of the breaches we saw, a significant growth from 9% last year. A 68% year-over-year growth is really solid, but what do we mean by this?

For a breach to be a part of the supply chain interconnection metric, it will have taken place because either a business partner was the vector of entry for the breach (like the now fabled heating, ventilating and air-conditioning [HVAC] company entry point in the 2013 Target breach) or if the data compromise happened

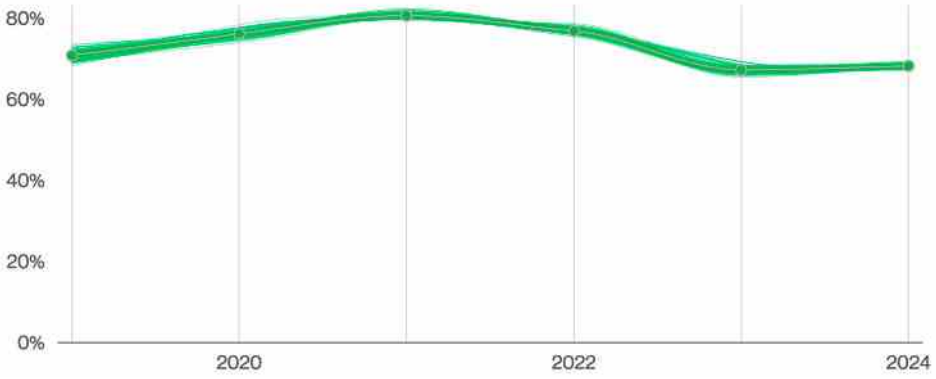


Figure 8. Human element enumeration in breaches over time

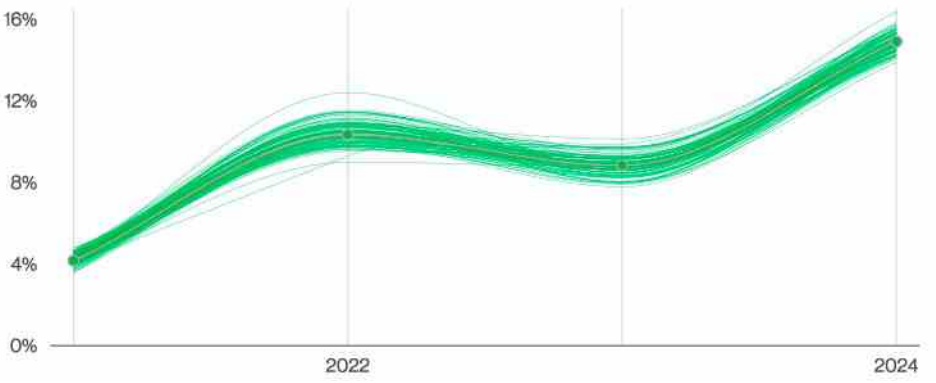


Figure 9. Supply chain interconnection in breaches over time

8 Number of times the word "MOVEit" is mentioned in this report: 25
9 In a surprising role reversal, as we are often very pedantic in our definitions

in a third-party data processor or custodian site (fairly common in the MOVEit cases, for instance). Less frequently found in our dataset, but also included, are physical breaches in a partner company facility or even partner vehicles hijacked to gain entry to an organization's facilities.[10]

So far, this seems like a pretty standard third-party breach recipe, but we are also adding cases, such as SolarWinds and 3CX, in which their software development processes were hijacked and malicious software updates were pushed to their customers to be potentially leveraged in a second step escalation by the threat actors. Those breaches are ultimately caused by the initial incident in the software development partner, and so we are adding those to this tab.

Now for the controversial part: Exploitation of vulnerabilities is counted in this metric as well. As much as we can argue that the software developers are also victims when vulnerabilities are disclosed in their software (and sure, they are), the incentives might not be aligned properly for those developers to handle this seemingly interminable task. These quality control failures can disproportionately affect the customers who use this software. We can clearly see what powerful and wide-reaching effects a handful of zero-day or mismanaged patching rollouts had on the general threat landscape. We stopped short of adding exploitation of misconfigurations in installed software because, although those could be a result of insecure defaults, system admins can get quite creative sometimes.

Figure 10 shows the breakdown of VERIS actions in the supply chain metric and, as expected, it is driven by Exploit vuln, which ushers Ransomware and Extortion attacks into organizations.

This metric ultimately represents a failure of community resilience and recognition of how organizations depend on each other. Every time a choice is made on a partner (or software provider) by your organization and it fails you, this metric goes up. We recommend that organizations start looking at ways of making better choices so as to not reward the weakest links in the chain. In a time where disclosure of breaches is becoming mandatory, we might finally have the tools and information to help measure the security effectiveness of our prospective partners.

We will keep a close watch on this one and seek to improve its definition over time. We welcome feedback and suggestions of alternative angles, and we believe the only way through it is to find ways to hold repeat offenders accountable and reward resilient software and services with our business.

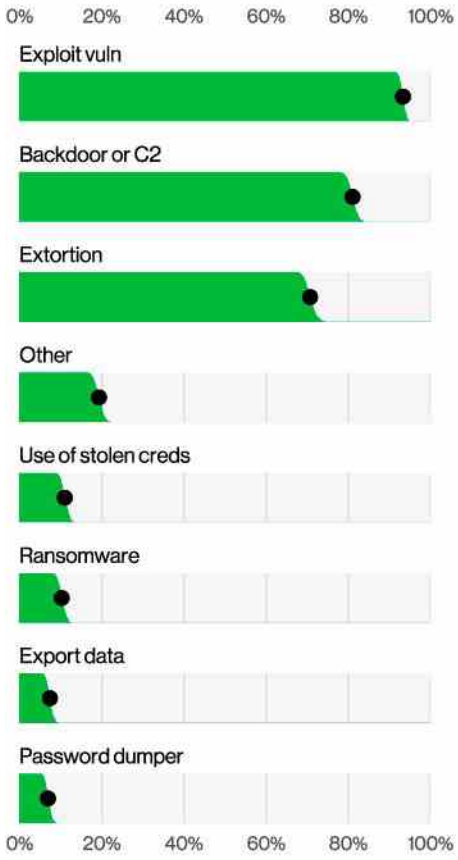


Figure 10. Action varieties in selected supply chain interconnection breaches (n=1,075)

10 We should stop watching those "Mission: Impossible" movies during DBIR writing season.

VERIS Actors

Hey, you, don't skip this section this year! We know we keep repeating, "It's always external criminals wanting your money" alongside dated pop culture references, but we have some interesting data points to discuss this year. Does this mean External actors are not the most prevalent? No, of course they are, silly. But since we got your attention, please read on.

This year, in part because of improved breach collection processes[11] and the onboarding of new data contributors documenting mandatory breach disclosures, it is finally time for Internal actors to shine. After all, why rely on outside help if you have the talent in-house?

We still have the External actors as the top catalyst for breaches at 65%, but we have Internal at a whopping 35%—a significant increase from last year's 20% number. Figure 11 showcases this development over the last few years.

However, before we call an emergency meeting and start pointing fingers at each other trying to figure out who the impostor is, it's important to realize that 73% of those Internal actor breaches were in the Miscellaneous Errors pattern, and we shouldn't really be holding their feet to the fire.[12] We will be discussing more about this Error renaissance[13] in the respective pattern section, but it showcases one long-standing suspicion of the team that mandatory breach disclosure at scale will help us better understand how mundane and preventable some of those incidents can be.

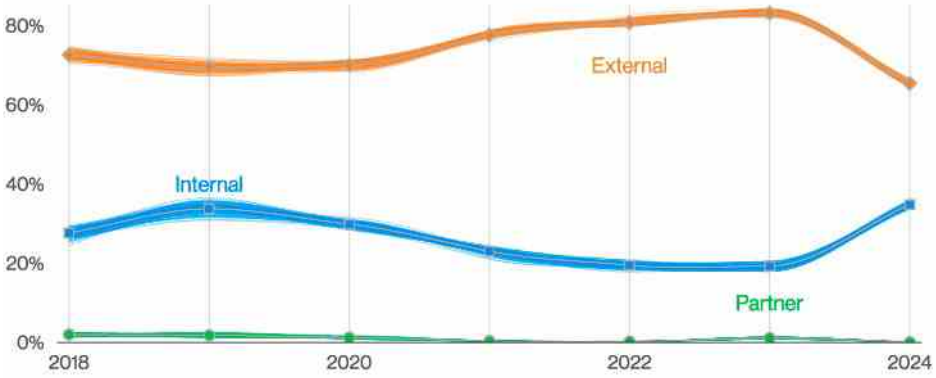


Figure 11. Threat actors in breaches over time

And speaking of disclosure, the numerous Extortion attacks used by ransomware actors have caused an influx of the numbers of external actor incidents we review each year because they tip the hands of their victims and force them to notify their customers of the breach. This helped us keep our dataset balanced. Further mandatory disclosure regulation trends in the world will help us all understand the causal landscape better.[14]

Before anyone gets excited by more groundbreaking changes in the "Actor" section, Figure 12 is pleased to inform you that the Actor motive ranking remains the same. Financial has the clear lead, but it is interesting to note that the Espionage motive has increased slightly over last year, from 5% to 7%. As was the case in the prior report, this motive is mostly concentrated in Public Administration breaches.

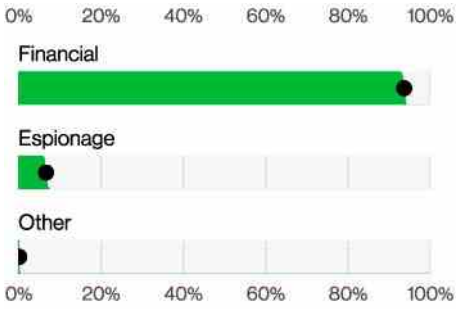


Figure 12. Threat actor motives in breaches (n=5,632)

11 Doubling the number of breaches we analyzed was no easy feat. We feel sorry for the poor DBIR authors who will have to outdo that number for the 2025 edition.
12 Unless carelessness and inattention to detail are wrong.
13 Errorssance? Age of Enerrorment?
14 This will also give threat actors new opportunities to be tattletales and report material breaches to organizations like the U.S. Securities and Exchange Commission (SEC).

We can find the same expected results when we consider the varieties of threat actors with which we are dealing. Figure 13 illustrates the lead that Organized crime-affiliated actors enjoy over their State-sponsored counterparts, as our analysis has shown for many years. Please don't misunderstand: This in no way means that the threat from those Actors should be taken lightly. State-sponsored actors are unusually resourceful and capable of adapting their tactics. Luckily for the average organization, they are less likely to target run-of-the-mill enterprises as often as your everyday, garden-variety criminal.

On a different note, End-user (in VERIS parlance, an average employee or contractor of an organization) has grown a lot, more than doubling from 11% to 26%. Those were mostly involved in Misdelivery errors and were part of the same growth in the Miscellaneous Errors pattern we discussed above. All in all, it's been an upsetting year for all detail-oriented perfectionists[15] out there.

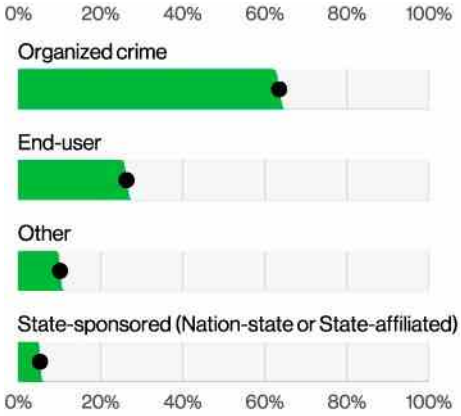


Figure 13. Threat actor varieties in breaches (n=7,921)

Actor categories[16]

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 to be considered the responsible party.

15 Just imagine what it would be like to work for one of those people. *[Editor's note: We resent that!]*
16 https://verisframework.org/actors.html

Artificial general intelligence threat landscape, emphasis on "artificial," not "intelligence"

Despite the pressure from a vocal minority of the cybersecurity community,[17] it seems that the DBIR team will not be adding "Evil AGI"[18] to the VERIS actor enumerations in 2024. However, it is still a very timely topic and one that has been occupying the minds of technology and cybersecurity executives worldwide.[19]

We did keep an eye out for any indications of the use of the emerging field of generative artificial intelligence (GenAI) in attacks and the potential effects of those technologies, but nothing materialized in the incident data we collected globally.[20]

After performing text analysis alongside our criminal forums data contributors, we could obviously see the interest in GenAI (as in any other forum, really), but the number of mentions of GenAI terms alongside traditional attack types and vectors such as "phishing," "malware," "vulnerability" and "ransomware" were shockingly low, barely breaching 100 cumulative mentions over the past two years. Most of the mentions[21] involved the selling of accounts to commercial GenAI offerings or tools for AI generation of non-consensual pornography. Figure 14 illustrates our findings.

If you extrapolate the commonly understood use cases of GenAI technology, it could potentially help with the development of phishing, malware and the discovery of new vulnerabilities in much the same way it helps your 10th grader write that book report for school or your average AI social media influencer pretend to create a website by taking a picture of a drawing on a napkin.

But would this kind of assistance really move the needle on successful attacks? One can argue, given our Social Engineering pattern numbers from the past few years, that Phishing or Pretexting attacks don't need to be more sophisticated to be successful against their targets, as we have seen with the growth of BEC-like attacks. Similarly, malware, especially of the Ransomware flavor, does not seem to be lacking in effectiveness, and threat actors seem to have a healthy supply of zero-day vulnerabilities for initial infiltration into an organization.

From our perspective, the threat actors might well be experimenting and trying to come up with GenAI solutions to their problems. There is evidence being published[22] of leveraging such technologies in "learning how to code" activities by known state-sponsored threat actors. But it really doesn't look like a breakthrough is imminent or that any attack-side optimizations this might bring would even register on the incident response side of things. The only exception here has to do with the clear advancements on deepfake-like technology, which has already created a good deal of reported fraud and misinformation anecdotes.

Incidentally, we did ask one of those GenAI tools what threats this nascent technology could amplify, and it ended up suggesting the same things as above.[23] It made it seem like it already had an outsize influence in those subjects and that "organizations must adapt their defense strategies to keep pace with the evolving sophistication of GenAI-driven threats."[24] This little experiment seems to indicate that even GenAI has a tendency toward beefing up its resume via the use of well-placed exaggeration.

Turns out it's really hard to escape the hype no matter where you sit on the natural vs. artificial divide.

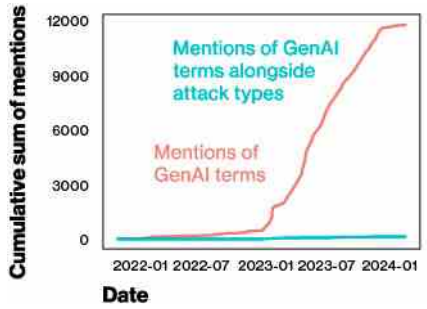


Figure 14. Cumulative sum of GenAI in criminal forums

17 Strange spelling for "unhinged marketing hype"

18 Artificial general intelligence. You know, HAL 9000, Skynet, Cylons, M3GAN ...

19 Just like real impactful technologies such as blockchain and the metaverse

20 But if we had been taken over by an evil AI technology, that is what we would say. Makes you think.

21 It is worth pointing out that while we were writing this section, Kaspersky came up with similar research that is worth a look: https://usa.kaspersky.com/about/press-releases/2024_new-kaspersky-study-examines-cybercrimes-ai-experimentation-on-the-dark-web

22 https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai

23 And when we asked it to do it again but in the voice of the DBIR, it seemed unhealthily fixated in circus and theater jokes and puns. Is that what we sound like?

24 We certainly know where we're getting marketing copy for our next cybersecurity startup.

VERIS Actions

A wise person[25] once said, "We are what we repeatedly do," and wouldn't they be impressed by the stoicism of how some of our top VERIS Actions keep showing up year after year? In all fairness, it does seem more an exercise of "if it ain't broke don't fix it" than any classical philosophical principle. But it highlights that we defenders have a lot of work to do, as usual.

Figure 15 has our top Action varieties in breaches, and it brings a lot to talk about. As we mentioned in the "Introduction" section, a big shift this year was the reduction of the Use of stolen credentials as a percentage of initial actions in breaches. It is still our top action at 24%, although it just barely passes statistical testing when compared to our good old Ransomware in the second spot, with 23%.

Ransomware is less representative than last year, although its common style of financially motivated breach is being complemented by Extortion, which now represents 9% of our action distribution. If you count Ransomware breaches and breaches with Extortion from ransomware actors as just two sides of the same coin,[26] we show a combined activity of 32% from those action varieties.

You can also see Extortion hand in hand with Exploit vuln at 10% of breaches, and the pair of them headline MOVEit's (and other similar vulnerabilities') impact, along with some other malware- and hacking-related varieties, such as Backdoor or C2 (command and control). That is double the exploitation of vulnerabilities of last year, and that obviously has had an impact in our ways-in metric as discussed in the introduction. Readers can find more details about this remarkable event in our "System Intrusion" pattern section.

One other thing worth noting is the clear overtaking of Pretexting as a more likely social action than Phishing. If you have been tracking our chronicle of the rise of BEC attacks, you know this is a viable and scalable way to address threat actor monetization anxieties.[27]

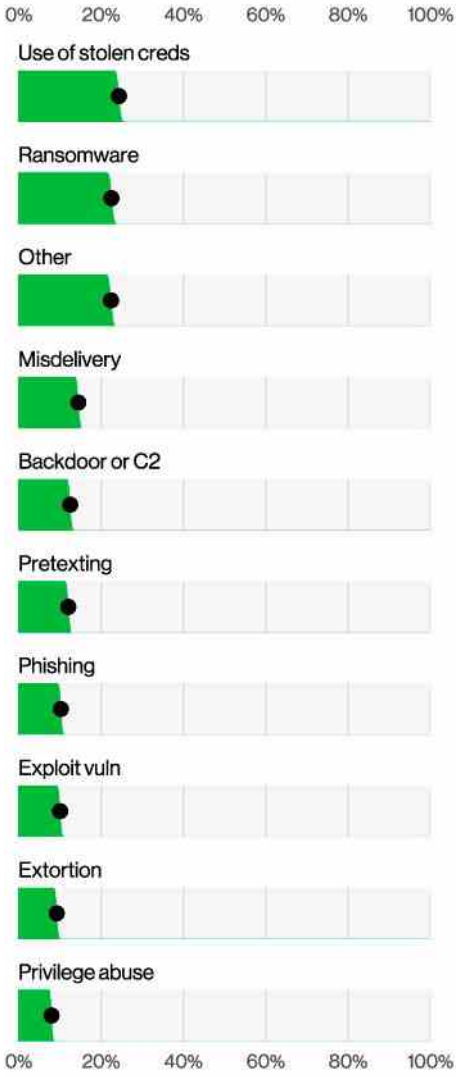


Figure 15. Top Action varieties in breaches (n=9,982)

Action categories[28]

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.

25 Since every quote on the Internet is misattributed, let's just save some time and take the easy way out.

26 Which we kind of do in this issue of the report because it is exhausting to argue with people all the time about things like threat actor methodology details or tactics, techniques and procedures (TTPs) when everyone else seems to be doing it.

27 Unfortunately, everyone has to hit their quotas each quarter.

28 https://verisframework.org/actions.html

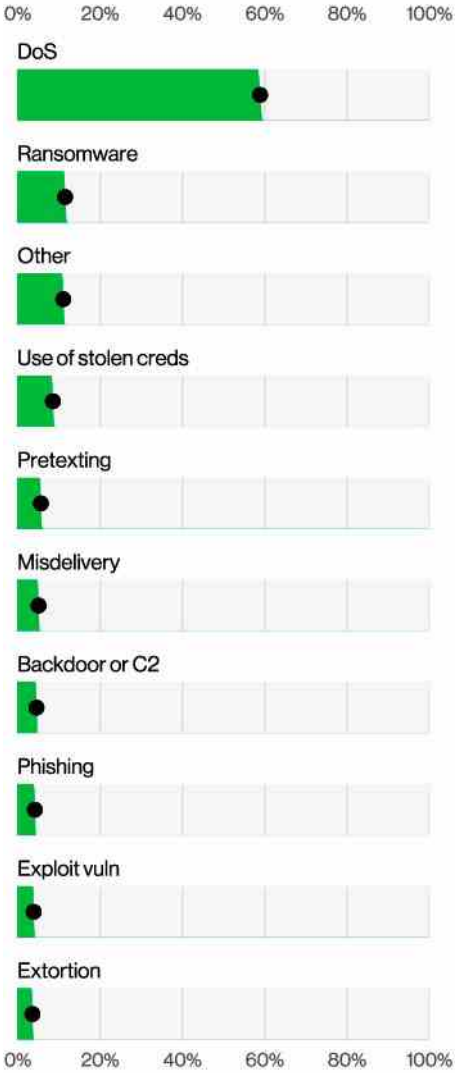


Figure 16. Top Action varieties in incidents (n=28,625)

Moving on to Figure 16, we have a chance to look into top Action varieties for incidents. It should not surprise any returning reader of the prevalence of DoS attacks in the top spot, being present in 59% of our recorded incidents. There is very little we can say about this Action variety that we haven't said before[29] as its lead has been quite stable over the years.

We can also observe the same phenomena in Ransomware that we saw in breaches. It is overall lower than last year, being present in 12% of incidents, but when you combine it with Extortion, we hit a similar ratio to last year's 15% of "Ramstortion."[30]

Figure 17 showcases the Action vectors in breaches, and the results are in line with what we have been discussing in the "Introduction" and "Actors" sections. There was considerable growth of Carelessness due to the increase in error breaches and an uptick in Email as a vector driven by the increase in pretexting. Web applications is hanging in there, though, and as we discussed in the introduction, it goes hand in hand alongside use of stolen credentials and exploitation of vulnerabilities to infiltrate your defenses.

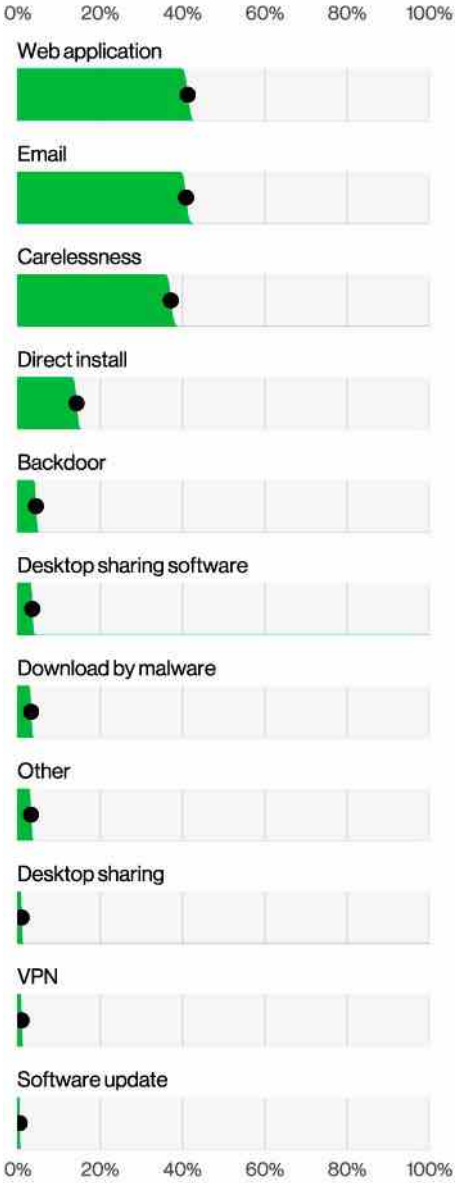


Figure 17. Top Action vectors in breaches (n=7,248)

29 We do try in the "Denial of Service" pattern section regardless.
30 "Extorware"? What would be the best couples name for this pair?

Speaking of ways in, it might also be interesting to explore a handful of goals and outcomes of those attacks.[31] Figure 18 describes the prevalence of ransomware/extortion and pretexting action varieties under the Financial actor motive. As we frequently point out, those are two of the most successful ways of monetizing a breach. The ransom duo has been hovering around the two-thirds mark (62%) for some time, while Pretexting made up nearly a quarter (24%) of goal actions over the past two years.

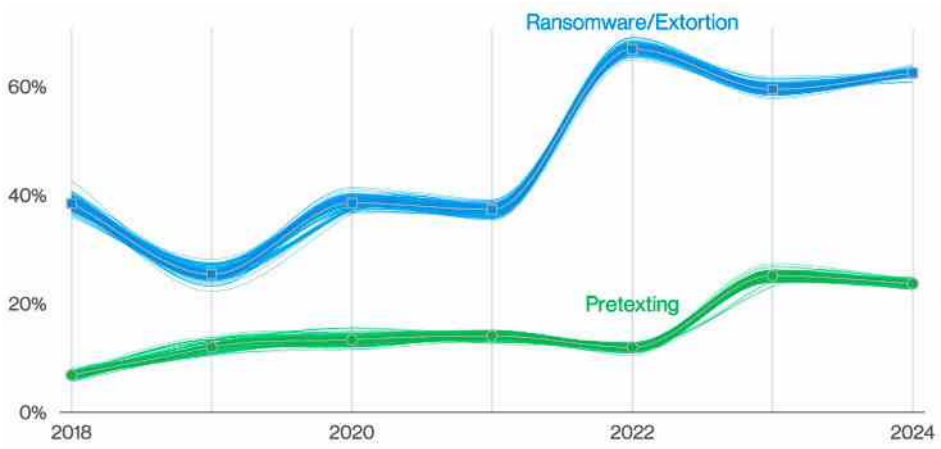


Figure 18. Select action varieties in Financial motive over time

Jen Easterly

Director Cybersecurity and Infrastructure Security Agency (CISA)

Over the past year, CISA has been leading the secure by design software development revolution. We have issued alerts documenting foreign intelligence agencies penetrating hundreds of critical infrastructure entities and establishing a foothold, possibly to be used in a future conflict. We have also published blueprints for what we need to change in order to establish a culture of technology development that puts security first without sacrificing innovation. These two efforts are different and necessary approaches to the same problem.

Today, the software industry is focused on the malicious actors and how they work. As a community, we talk about signature adversary moves, the amount of money made and the vulnerabilities that were exploited.

But it's that last point—vulnerabilities that were exploited—that doesn't get nearly enough focus. Most software vulnerabilities are not unknown, unique or novel. Instead, they fall into well-known classes of vulnerabilities, and unfortunately, we continue to see the same classes of vulnerabilities that have been identified for decades.

Our goal should be to shift away from focusing on individual vulnerabilities and to instead consider the issue from a strategic lens. By focusing on recurring classes of software defects, we can inspire software developers to improve the tools, technologies, and processes and attack software quality problems at the root. I hope that a deeper understanding of how attackers get in will be the catalyst to demand that our technology be secure by design starting today.

31 The obvious "ways-out" pun doesn't make sense here. Maybe if we had cyber getaway cars.

Exploitation moving swiftly in the threat landscape

The DBIR is entering its Vulnerability Era. One of the most critical findings we had this year was the growth of the Exploit vuln action variety. We have emphasized the fact that credential abuse is the big thing to focus on for several years now,[32] and even the most obtuse of us can see a trend when it is smacking us in the face.

We knew that the MOVEit vulnerability was trouble when it first entered the room, and we were able to identify 1,567 breach notifications that related to MOVEit by a combination of (very vague) breach descriptions and the timing of the breach itself. Reports from CISA[33] state that the Cl0p ransomware team had compromised more than 8,000[34] global organizations from a handful of zero-day vulnerabilities being exploited. It is important to mention this high number even if our sampled incident dataset does not account for all of that in either breach notifications or ransomware victim listings scraped from the threat actor's own notification websites.[35]

This love story between zero-day vulnerabilities and ransomware threat actors puts us all in a concerning place. By doing a survival analysis[36] of vulnerability management data and focusing on the vulnerabilities in the CISA Known Exploited Vulnerabilities (KEV) catalog,[37] (arguably an area of priority focus in vulnerability management), we found that it takes around 55 days to remediate 50% of those critical vulnerabilities once their patches are available. As Figure 19 demonstrates, the patching doesn't seem to start picking up until after the 30-day mark, and by the end of a whole year, around 8% of them are still open.

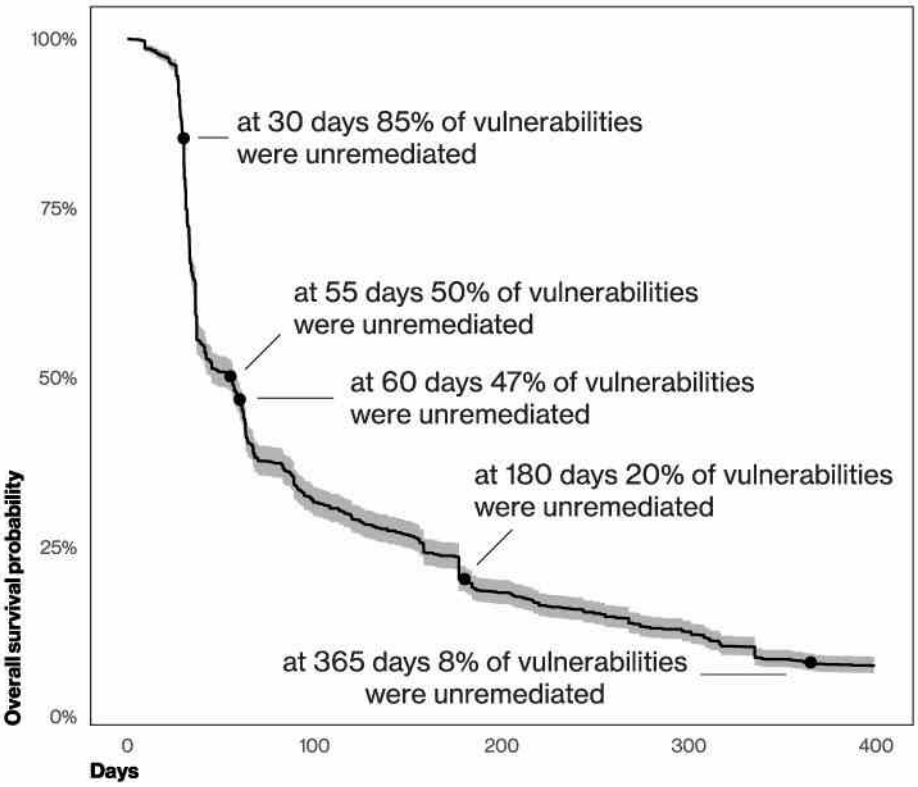


Figure 19. Survival analysis of CISA KEV vulnerabilities

But before organizations start pointing at themselves saying, "It's me, hi, I'm the problem," we must remind ourselves that after following a sensible risk-based analysis,[38] enterprise patch management cycles usually stabilize around 30 to 60 days as the viable target, with maybe a 15-day target for critical vulnerability patching. Sadly, this does not seem to keep pace with the growing speed of threat actor scanning and exploitation of vulnerabilities.

32 DBIR guided visualization: Picture blue team folks in jerseys at the Super Bowl chanting, "MFA! MFA! MFA!"
33 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a
34 Vegeta's power Scouter is still intact.
35 And just like a consultant will say, "It depends," our data scientists will say, "It's the sampling bias."
36 Hat tip to Jay Jacobs of Cyentia on the methodology: https://www.cyentia.com/why-your-mttr-is-probably-bogus
37 https://www.cisa.gov/known-exploited-vulnerabilities-catalog
38 Such as the one in https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-RemediateVulnerabilitiesforInternetAccessibleSystems_S508C.pdf

This is not enough to shake the risk off. As we pointed out in the 2023 DBIR, the infamous Log4j vulnerability had nearly a third (32%) of its scanning activity happening in the first 30 days of its disclosure. The industry was very efficient in mitigating and patching affected systems so the damage was minimized, but we cannot realistically expect an industrywide response of that magnitude for every single vulnerability that comes along, be it zero-day or not.

In fact, if you look at the distribution of when vulnerabilities have their first scan seen in internet honeypots on Figure 20, the median time for that to happen for a Common Vulnerabilities and Exposures (CVE) registered vulnerability in the CISA KEV is five days. On the other hand, the median time for non-CISA KEV vulnerabilities sits at 68 days. There is an obvious "no true Scotsman" fallacy comment to be made here because when exploitation starts running rampant, vulnerabilities get added to the KEV. There are few hindsight metrics as powerful as this one to guide what you should be patching first.[39] In summary, if it goes into the KEV, go fix it ASAP.

Even though this survival analysis chart looks bleak, this is the optimist's view of the situation. We must remind ourselves that these are companies with resources to at least hire a vulnerability management vendor. That tells us that they care about the risk and are taking measures to address it. The overall reality is much worse, and as more ransomware threat actors adopt zero-day and/or recent vulnerabilities, they will definitely fill the blank space in their notification websites with your organization's name.

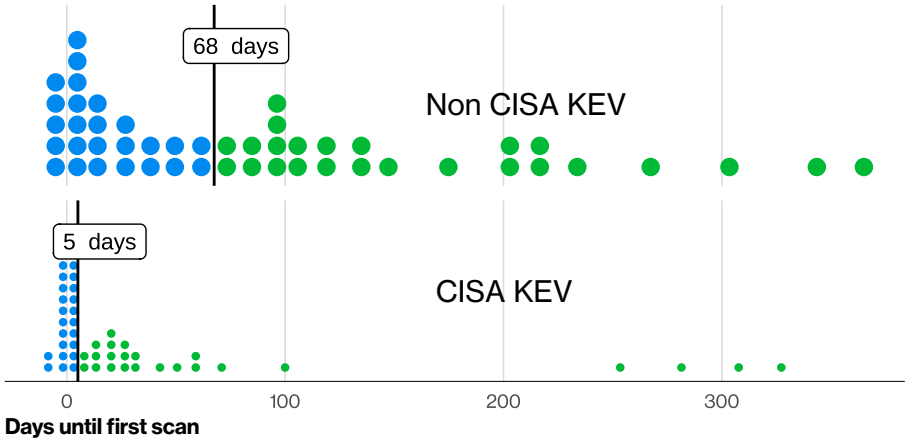


Figure 20. Time from publication of vulnerability to first scan seen (from 2020 onward)

If we can't patch the vulnerabilities faster, it seems like the only logical conclusion is to have fewer of them to patch. We realize this is the stuff of our wildest dreams, but at the very least, organizations should be holding their software vendors accountable for the security outcomes of their product, even if there is no regulatory pressure on those vendors to do better. The DBIR will emphasize this point going forward by expanding our third-party involvement in breaches metric to also account for the exploitation of vulnerabilities.[40] This helps illustrate that when choosing a vendor, software that is secure by design would make a difference.

We recommend that folks who are involved in both software development and software procurement take the time to review the recently updated "Secure by Design"[41] report by CISA and 17 U.S. and international partners. It shows how software can be made to have better security outcomes and what to look for as a buyer. The DBIR does not intend to foster any bad blood with software providers that might be falling short of their goals in keeping their products safe, but if there ever was a clear time to make a statement by prioritizing this elegant solution to a growing threat, this is it. We can see the costs of not acting all too well.

39 Eat your heart out, CVSS (Common Vulnerability Scoring System).
40 Have a look at the "Introduction" subsection in this "Results and analysis" section.
41 https://www.cisa.gov/resources-tools/resources/secure-by-design

VERIS Assets

Analyzing the VERIS Assets helps us understand where all those attacks we keep harping on are focused, and everyone sure needs help in prioritizing how to defend those assets. Even though those results might not be surprising as they have a good correlation with the VERIS Actions we just discussed, it is worthwhile to understand the year-to-year trends in the threat landscape.

Our asset power ranking[42] has not changed a lot from last year, but there are a handful of changes that are worth pointing out in Figure 21. Even though the order from the 2023 DBIR is the same and the prevalence of Server assets is roughly the same as well, we find substantial growth in both Person[43] and Media assets.

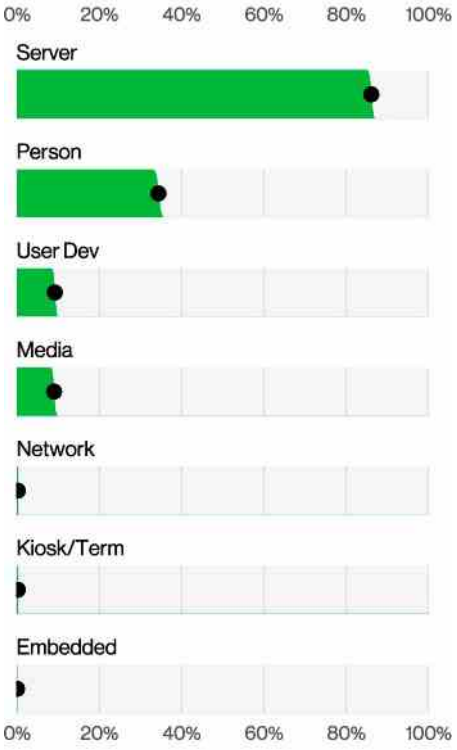


Figure 21. Assets in breaches (n=8,910)

Person as an asset has become more involved this year because of the growth of pure Extortion action-based breaches in our dataset. As a social action, Extortion demands a Person as the direct victim, and the dataset gnomes[44] are happy to oblige. What is interesting here is that the Ransomware action, where pure Extortion got its spin-off from, implied that there was an extortion phase where the money was requested without being connected to a Person asset.[45]

Thus, this growth in Person also makes sense as a more representative truth of the mechanics of such breaches. Your employees need to be aware of how to handle a ransom or extortion demand and follow whatever procedures were established by your organization to handle those. By the way, make sure you have those documented[46] just in case.

42 Who would win in a fight – an email server or a file server with prep time?
43 Perhaps not in maturity, as some people assets will have their security attributes compromised to avoid going to therapy.
44 The DBIR authors' pickleball team name
45 This is likely too much VERIS Standard inside baseball for the average reader, but we are amused very easily by things like this.
46 Just keep it on your file server. It should be fine, right? (Not really)

The Media growth is intrinsically tied with the progression in the Miscellaneous Errors pattern discussed previously. Some of those Misdelivery errors happen via physical documents and fax machines[47] which might limit their scope but does not make them any less breachworthy to regulators.

Digging deeper in Figure 22, we get a better sense of the Server asset breakdown. While the Web application and Mail servers are mostly involved in credential-theft breaches, the File server has been almost dominated by the MOVEit breaches, which explains why more than 95% of breached assets are servers.

All in all, a pretty standard year in the VERIS Assets world. We will be discussing more on how to help keep these assets safe in the "System Intrusion," "Social Engineering" and "Basic Web Application Attacks" pattern sections.

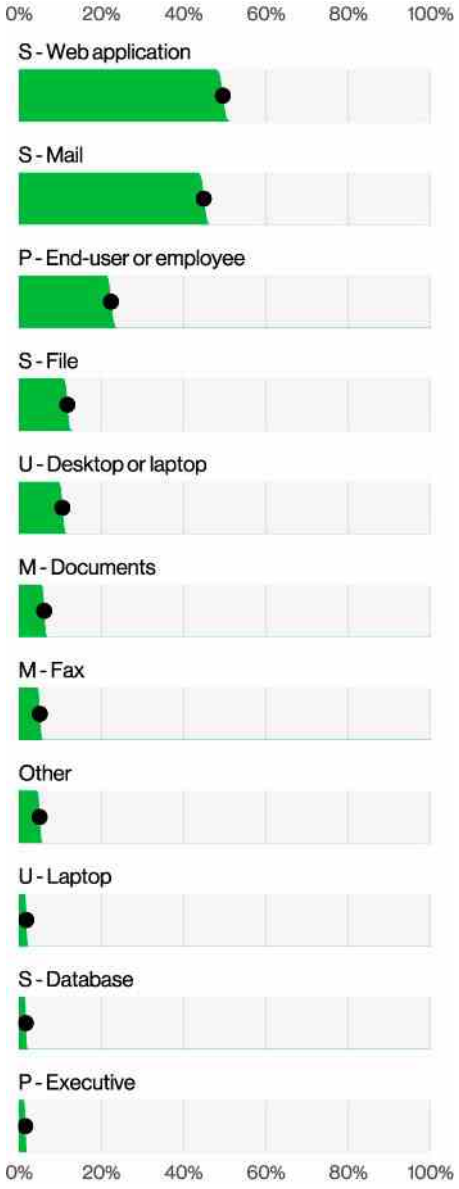


Figure 22. Top Asset varieties in incidents (n=6,606)

Asset categories[48]

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 Persons 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 organization. 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 Assets 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 also a telecommunications company, OK?

Media (med): precious distilled 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 rare.

47 Believe it or not, this is not the 1994 Data Breach Investigations Report.
48 https://verisframework.org/assets.html

VERIS Attributes

As we often need to remind our very young children and grandchildren, actions have consequences.[49] Incidents and data breaches are no different,[50] and said consequences will often materialize as data leaks (confidentiality issue), unauthorized changes on your assets (integrity issue) or a loss of access to your data (availability issue).

More frequently than not, all of them can take a hit over the course of a multistep breach. Figure 23 demonstrates how often those three pillars were compromised over time in one of our charts with the most "DBIR charts do not add up to 100% because events are non-exclusive" energy thus far.

Roughly a third of the incidents we reviewed this year were data breaches where the Confidentiality of data was compromised. Figure 24 has the breakdown of data varieties that were leaked in breaches this year, and Personal data is unsurprisingly at the top of the list.

This continuous prevalence of Personal data in the top spot is in a way a self-fulfilling curse because the breaches that get more frequently disclosed will be the ones involving customer data where regulation requires the affected victims to be notified. Furthermore, customer data is so prevalent and hoarded without need or proper care that it will often be collateral damage in any sort of attack that might not even be specifically targeting it.

Internal company data (such as emails and business documents) and System-specific data also overshadow more exclusive targets such as Payment, Bank, Medical and Secrets. We have often described how the Ransomware (and now pure Extortion) breaches mean that the threat actors don't need to care about the data they are stealing because they will always have the victim organization as the main buyer. We dig into ransomware, ransom amounts and extortion economics in the "System Intrusion" pattern section later in the report.

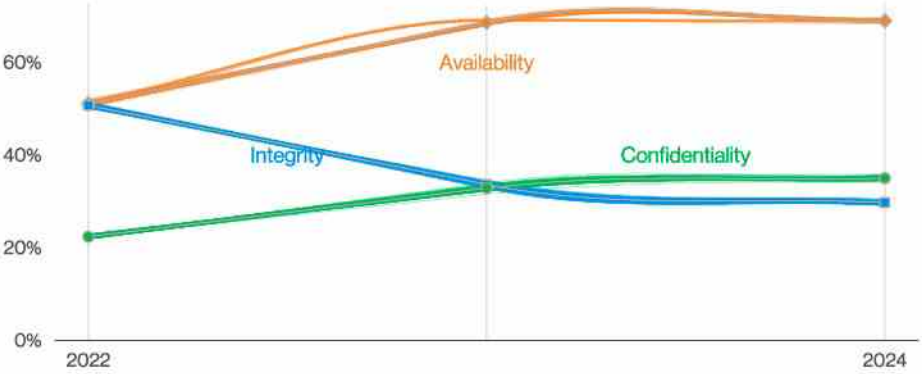


Figure 23. Attributes over time in incidents

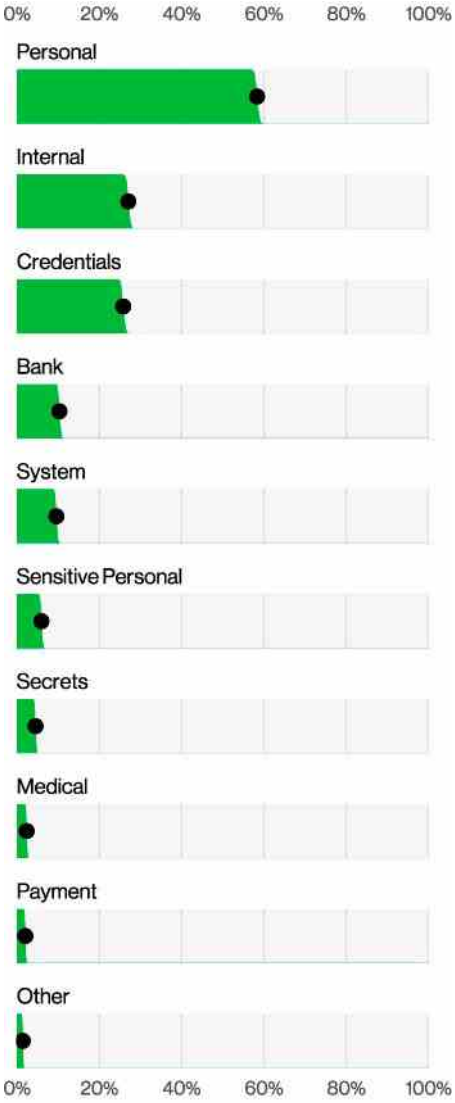


Figure 24. Top Confidentiality data varieties in breaches

49 Especially bad actions. Benevolent ones often go unnoticed.
50 Threat actors should also be sent to bed without TV if they misbehave.

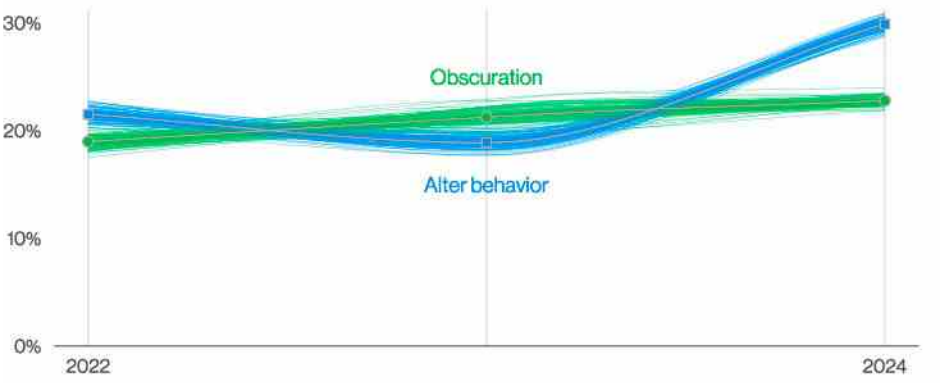


Figure 25. Select Attribute varieties over time in breaches

In addition, we are observing a decline in the Credentials data type from a percentage point of view. This is because the percentage of breaches caused by Error actions is rising (again as a result of our sample) as opposed to external actors who are exploiting weak credentials though credential stuffing or brute force attacks.

As a final curiosity, another side effect of the growth of extortion non-encrypting attacks has resulted in a significant bump in the Alter behavior variety under integrity. This is the integrity violation we get when Persons are influenced by external threat actors, and it is also a common outcome from a Phishing or Pretexting social action.

To see it overcome the Obscuration variety (the usual outcome of the Ransomware action) in such a sharp way in Figure 25 could be a harbinger of things to come. The consequence of which is that System Intrusion pattern attacks become more prevalent in the long run.

Attribute categories[51]

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 or Control[52]). 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.

Stephen Bonner

Deputy Commissioner – Regulatory Supervision, U.K. Information Commissioner's Office (ICO)

People need to be assured their information will be kept safe so they can participate in society, including having the confidence to share their data to access services and use products.

Our security incident trend data, which we have contributed to this report, shows cyber threats not only continue to exist but increase year on year. It is important to remember that there is no single solution to security, but organizations can improve their cybersecurity through our guidance and tools to better protect people's information.

We are also encouraging organizations to be transparent when a cyber incident happens, seeking early support and sharing information so the cyber threat landscape is improved for everyone. The ICO will soon publish a review of past security incidents to help organizations continue to improve their cyber resilience.

51 https://verisframework.org/attributes.html
52 https://en.wikipedia.org/wiki/Parkerian_Hexad

3 Incident Classification Patterns

Incident Classification Patterns: Introduction

Pareidolia is a fancy word for seeing patterns in nature—clouds that look like bunnies, a face in your toast looking back at you from your breakfast plate, etc. As we have said before in this report, the human mind looks for patterns even when they are not actually there.[53] People simply need patterns to make sense of their world, and the realm of cybersecurity is no different. Several years ago, we realized that certain incidents appear to happen over and over again in clusters that share certain similar characteristics. From that realization, we devised our incident patterns that we have featured in our report for the last several years.

These incident patterns serve to cluster similar incidents into categories that make them easier to understand and recall. They are based on the 4As of VERIS (Actor, Action, Asset, Attribute), which you can read more about in the "Results and analysis" section earlier in this report.[54] The incident classification patterns, of which there are eight, are defined in Table 1, and Figure 26 below shows how they have changed over time in incidents.

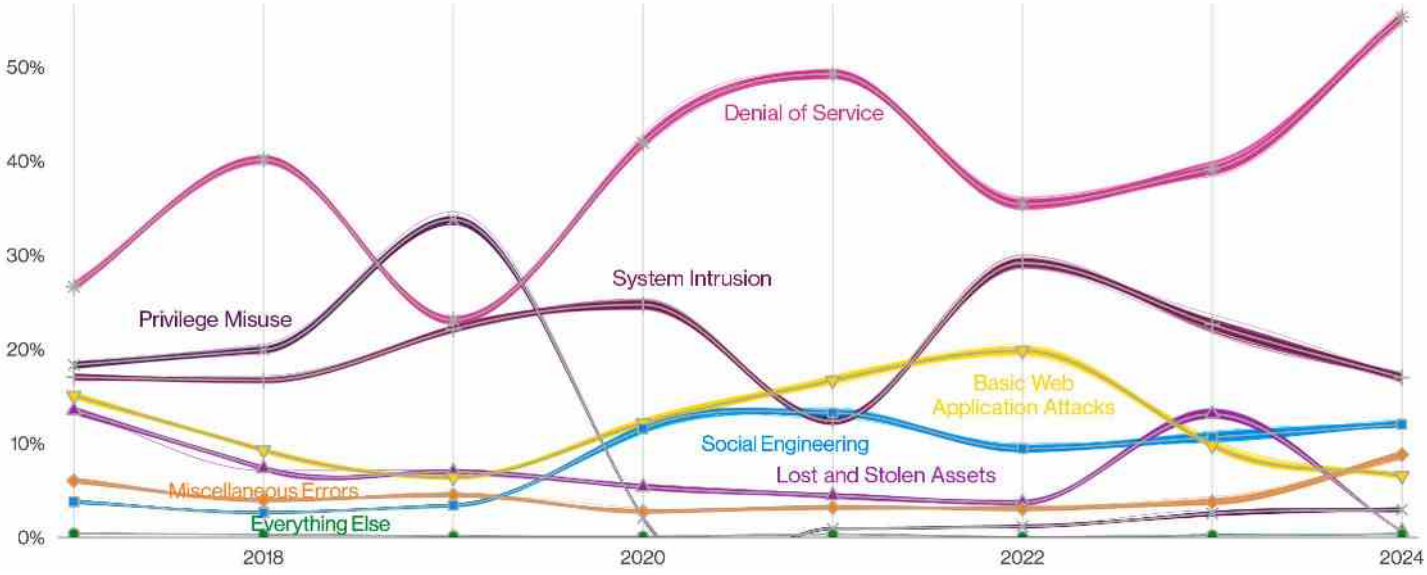


Figure 26. Patterns over time in incidents

53 We are pretty sure the toast face is real, though.
54 You did read it, right? You are not just skimming the report, are you?

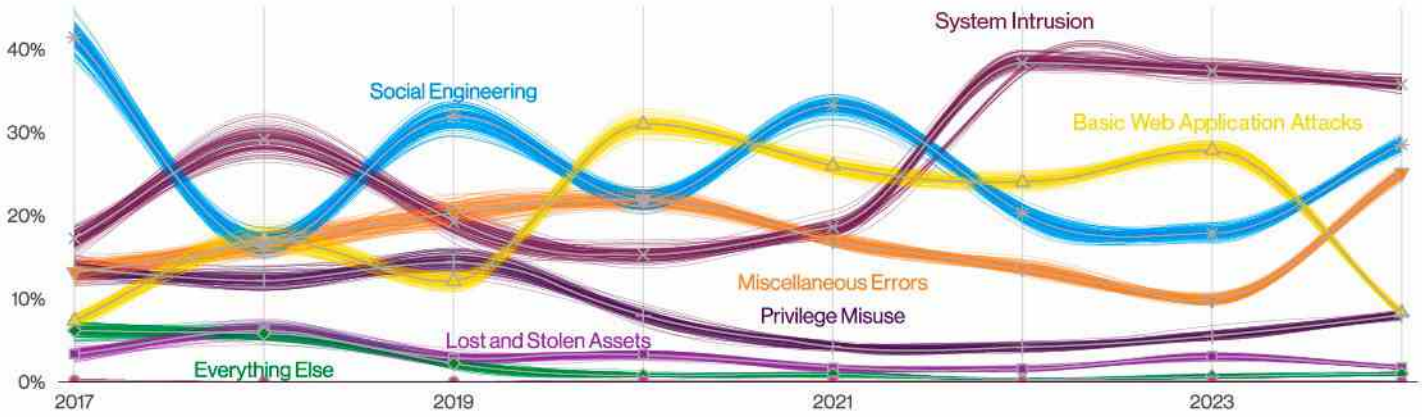


Figure 27. Patterns over time in breaches

We are once again featuring relevant ATT&CK techniques[55] and Center for Internet Security (CIS) Critical Security Controls[56] relevant to certain patterns.

Figure 27 illustrates how the various patterns have ebbed and flowed over the last few years in breaches. As you can see, System Intrusion continues to be the top pattern from a breach perspective (as opposed to incidents, where DoS attacks are still king). Both the Social Engineering and Miscellaneous Errors patterns have risen appreciably, particularly the latter, since last year. Conversely, the Basic Web Application Attacks pattern has fallen dramatically from its place in the 2023 DBIR. We get to delve into the reasons for these fluctuations further along in this section.

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

55 https://attack.mitre.org
56 https://www.cisecurity.org/controls

System Intrusion

Summary

While shifts in tactics leveraged by Actors have modified some of the top Actions, the overall effect of these Actors continues to be felt by the majority of industries and organizations of all sizes.

What is the same?

Ransomware attacks continue to drive the growth of this pattern as they now account for 23% of all breaches.

Frequency	5,175 incidents, 3,803 with confirmed data disclosure
Threat actors	External (100%) (breaches)
Actor motives	Financial (95%), Espionage (5%) (breaches)
Data compromised	Personal (50%), Other (34%), System (26%), Internal (22%) (breaches)

System of an Intrusion

In the world of our attack patterns, it's been a competitive year, and there have been a lot of contenders vying for the first-place prize of MFB: most frequent breach (granted, not as prestigious as the MVP, but you work with what you have). System Intrusion, for the third year in a row, leads the pack with 36% of breaches. Not sure exactly what they're winning (our guess would be a good bit of cash), but we can certainly tell you who is losing, and that's all of us. Let's dive into what is driving the continued success of this pattern.

Relevant ATT&CK techniques

Exploit vuln (VERIS)

- Exploit Public-Facing Application: T1190
- Exploitation for Credential Access: T1212
- Exploitation for Defense Evasion: T1211
- Exploitation for Privilege Escalation: T1068
- 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

The makeup of this pattern hasn't changed much. It is where our more sophisticated attacks[57] are found. They still largely consist of breaches and incidents in which the threat actor leverages a combination of Hacking techniques and Malware to penetrate the victim organization—more or less what one might expect from an unauthorized penetration test. However, rather than providing a helpful written report at the conclusion of the exercise, they typically deploy Ransomware and provide the victim with a much less helpful extortion note. These Ransomware attacks account for 70% of the incidents within System Intrusion, as seen in Figure 28. The other often seen actions in the System Intrusion pattern tend to be those that provide the actor access to the environment, such as Exploit vulnerabilities and Backdoors. We also saw Extortion creeping into this space, primarily due to a large and impactful event that we will discuss later in the report—so stay tuned.[58]

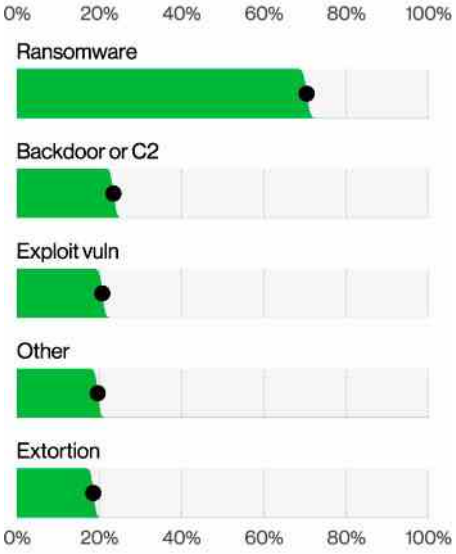


Figure 28. Top Action varieties in System Intrusion incidents

Ransomhow?

With regard to vectors (Figure 29), we saw a great deal of Direct install. This is when threat actors use their existing system access to install malware, such as Ransomware or Backdoors. The vector of Web applications, which is a favored target of exploits, also appeared frequently, as we discussed in the ways-in analysis in the "Results and analysis" section. Of course, we still see threat actors leveraging Email to reach users and Desktop sharing software to gain entry into systems. Because these threat actors use a plethora of tools and techniques, this data is longer tailed, which is why Other shows up relatively often in our top five. Within the category of Other are vectors such as VPNs, Software updates and a whole bunch of Unknowns (our bet is that it is most likely split among the tactics discussed above, just not explicitly reported to us). Therefore, when prioritizing your efforts at protecting yourself, don't neglect addressing malware infections, stolen credentials or unpatched systems as it may lead you to break out in Ransomware.[59]

Ransomwho?

Much like Sisyphus with his never-ending task, it seems that the hardworking people in IT must continue to contend with the evolving threat of Ransomware. Ransomware has again dominated the charts, accounting for 11% of all incidents, making it the second most common incident type. Ransomware (or some type of Extortion) appears in 92% of industries as one of the top threats.

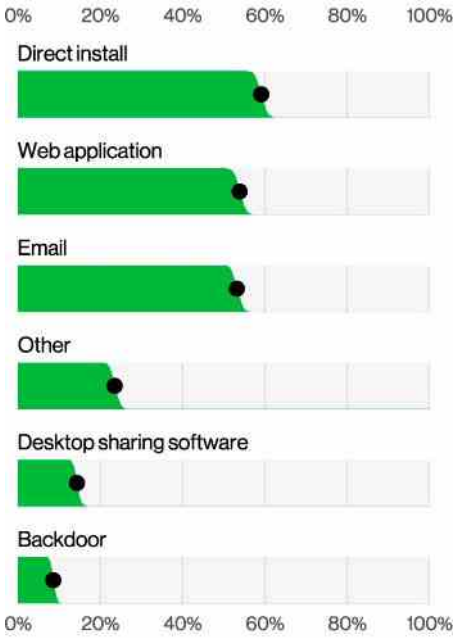


Figure 29. Top Action vectors in System Intrusion incidents (n=1,789)

When we remove the Ransomware groups from this dataset,[60] we're left with a pretty even split of 44% run-of-the-mill types of criminals and 40% State-affiliated actors. It shouldn't be too surprising to find out that the tactics used by criminals are very closely aligned to those used by Actors working on the behalf of their country.

Ransomware (or some type of Extortion) appears in 92% of industries as one of the top threats.

57 If these attacks were people, they would drink fine wine in restaurants, pontificate loudly on the vintage and drive cars made in Scandinavia.
58 And if you could hit the Like and Subscribe buttons, we'd appreciate it. Oh, wait, wrong platform.
59 And a visit to the dermatologist won't help.
60 Ah, wouldn't that be nice? Just the thought of it improved my mood.

Clearly, the major difference is what they do with that access. The subset of criminals in this pattern who aren't doing Ransomware/Extortion are quietly siphoning off Payment data from e-commerce sites and account for 57% of breaches involving stolen Payment cards, while the State-affiliated actors look to pivot and steal other types of data.[61]

Ransomwhat?

Understanding the cost associated with Ransomware is a bit complex as there are several primary and secondary costs to consider, not to mention the possible soft costs associated with reputational impacts. While we try our best to capture these costs, it's worth noting that the result isn't a full picture but simply our best approximation using the data we have.

One of the easier costs to capture is the amount associated with paying the actual ransom. Analyzing the FBI IC3[62] dataset this year, we found that the median adjusted loss (after law enforcement worked to try to recover funds) for those who did pay was around $46,000 as shown in Figure 30. This is a significant increase from the previous year's median of $26,000, but you should also take into consideration that only 4% of the complaints had any actual loss this time, as opposed to 7% last year.

Another way we can slice the data is by looking at ransom demands as a percentage of the total revenue.[63] The median amount of the initial ransom demand was 1.34% of the victim organization's total revenue—with 50% of the demands being between 0.13% and 8.30% (Figure 31). We know this is quite a spread for the initial ransom demand percentage. There were a few within the top 10% of cases reaching up to 24% of total revenue. Hopefully these ranges assist organizations in running risk scenarios with an eye toward potential direct costs associated with a ransomware attack. Of course, there are many other factors that should also be considered, but this is a good starting point.

Figure 30. 95% and 80% confidence intervals of adjusted incident cost for Ransomware

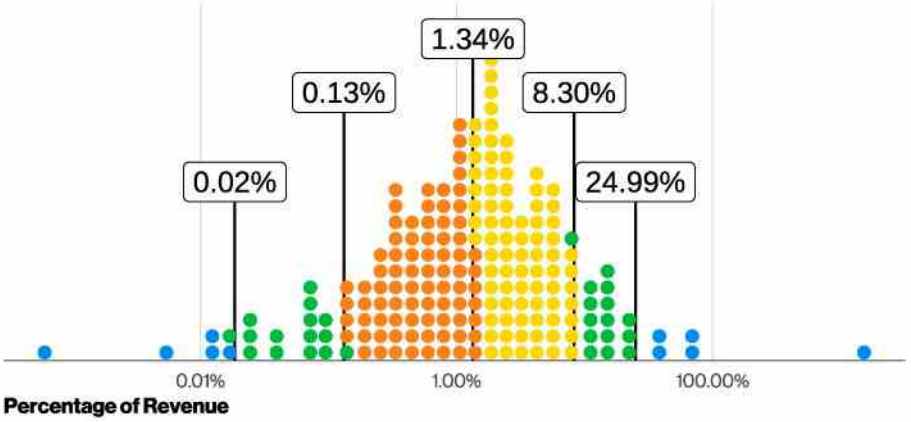


Figure 31. 95% and 80% confidence intervals of ransoms as a percentage of victim revenue

61 Can't tell you what, though. It is strictly confidential information.
62 https://www.ic3.gov
63 Note that the source of this data is from ransomware negotiators, which might be a self-selecting sample. Those who can afford to employ a negotiator in this kind of incident may also be targeted with higher ransom demands since they are likely to be higher revenue organizations.

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. Below is a small subset of all the things an organization could do. They should serve as a starting point for building out your own risk assessments to help 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 Protections [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 Process [6.1, 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]

MOVEit or don't.

Over the summer, we were teased with the idea of a great crossover, one involving the father of the atomic bomb and a plastic doll. For this year's report, we have a similar type of crossover but perhaps a bit less entertaining. In the hope of continuing to increase their shareholders' affiliates' profits, ransomware groups have demonstrated a remarkable ability to evolve their tactics.

One such recent evolution was snapshotted in the MOVEit incident, where threat actors[64] used a zero-day attack (a previously unknown and unpatched vulnerability) in file management software and went on a spree appropriating whoever's data they could get their hands on and holding it hostage. While the attack affected organizations from a variety of sectors, Education was by far the largest impacted (Figure 32), accounting for more than 50% of the breached organizations, according to our breach notification dataset.

While this seems like pretty standard e-criminal stuff, it was a shift in tactics worth discussing. For starters, the group didn't actually deploy Ransomware in all of these cases, even though it was previously partial to that tactic. There could have been myriad reasons as to why the group didn't choose this option, and anything we'd suggest would be speculation. What it did accomplish, however, was to slightly confound the differences that exist between the System Intrusion and Social Engineering patterns by introducing a big chunk of data that neatly fits in both categories. After it stole the data, Cl0p used Extortion as a means of separating the victims from their hard-earned money.

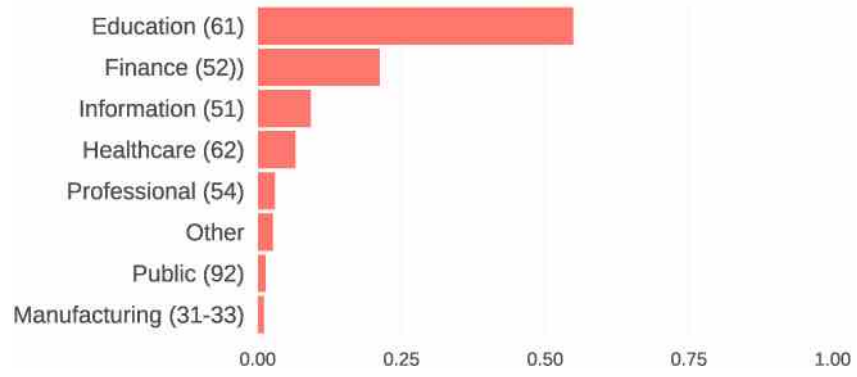


Figure 32. Top industries found in the MOVEit breach notification dataset (n=1,567)

64 Widely attributed to be the Cl0p ransomware group (https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a)

When we look at Ransomware breaches over time (Figure 33), we notice a dip in the cases; however, when we combine it with Extortion, we see that it follows pretty much the same trend line. This indicates to us that it may be the same actors, and they are simply shifting tactics to best leverage the type of access they have. This combination did show a significant growth as a part of breaches, as we touched on in the second entry of our "Summary of findings" section.

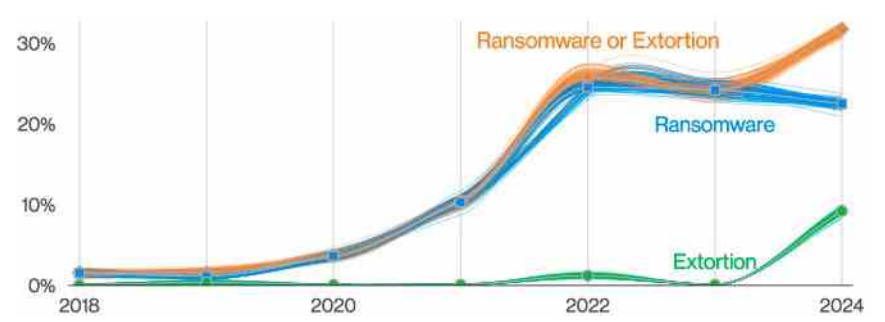


Figure 33. Ransomware and Extortion breaches over time

The DBIR team looks at numbers,[65] not code, so this report isn't the best place to explain all the technical elements. Nevertheless, what the vulnerability essentially did was to allow the attackers to upload a backdoor through a crafty SQL injection attack. This backdoor allowed the attackers to perform several different tasks such as downloading data and manipulating the application's legitimate users.

Unfortunately, because of the nature of the platform, file transfer systems need to be on the internet, and the fact that this was an unknown vulnerability at the time of exploit ensured that there was nothing victims could have done to prevent it. There can be no doubt that this was a large-scale and impactful attack; however, it wasn't without precedent. In fact, just a few months before, in January 2023, the same group had targeted another file hosting platform resulting in a rather busy month for Ransomware claims.

As we gaze into our crystal ball, we wouldn't be surprised if we continue to see zero-day vulnerabilities being widely leveraged by ransomware groups. If their preference for file transfer platforms continues,[66] this should serve as a caution for those vendors to check their code very closely for common vulnerabilities. Likewise, if your organization utilizes these kinds of platforms—or anything exposed to the internet, for that matter—keep a very close eye on the security patches those vendors release and prioritize their application.

65 And pop culture references
66 Even though, as 2024 begins, the focus seems to be on VPN and remote Desktop sharing software.

Social Engineering

Summary

Pretexting continues to be the leading cause of cybersecurity incidents, with actors targeting users with existing email chains and context. Extortion also grew dramatically because of the large-scale MOVEit incident.

What is the same?

Phishing and Pretexting via email continue to be the leading cause of incidents in this sector, accounting for 73% of breaches.

Frequency	3,661 incidents, 3,032 with confirmed data disclosure
Threat actors	External (100%) (breaches)
Actor motives	Financial (95%), Espionage (5%) (breaches)
Data compromised	Credentials (50%), Personal (41%), Internal (20%), Other (14%) (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

*ishing in the wind

In the cybersecurity world, or "the cyber biz," as we call it, we certainly love our catchy terminology. Terms such as whaling, smishing, quishing, tishing, vishing, wishing, pharming, snowshoeing[67] and plain old phishing are ever-present in the Social Engineering pattern. This makes sense because there are a lot of vectors on which we need to educate our employees and end users, and we're positive that in another five years, there will be new ones that we will have to add to our list.

However, even with the growth of these new vectors and types of attacks, we tend to see the core social tactics such as Pretexting and Phishing still being used often (Figure 34). More than 40% of incidents involved Pretexting, and 31% involved Phishing. Other tried-and-true tactics such as attacks coming in via email, text and websites (Figure 35) aren't necessarily the most exciting, but any security professionals who have been around for any length of time have probably seen these contenders in some capacity over their careers.

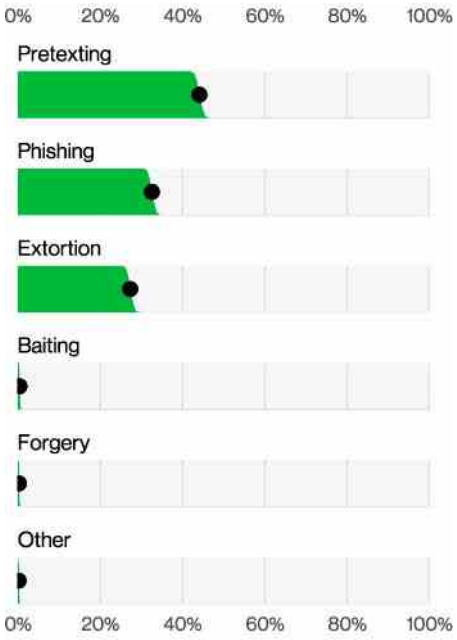


Figure 34. Top Action varieties in Social Engineering incidents (n=3,647)

Regardless of the exact method that attackers use to reach organizations, the core tactic is the same: They seek to exploit our human nature and our willingness to trust and be helpful for their own gain. While these attacks all share that commonality, one rather significant difference is the scale and pervasiveness of these tactics.

First, the good news. We have not seen a dramatic rise in Pretexting like we did last year. However, it is also true that it hasn't decreased but instead has maintained its position as the top type of Social Engineering incident. As a quick reminder, when we talk about Pretexting, largely consider this as a stand-in for BEC, where attackers leverage existing email chains to convince victims to do something, such as update an associated bank account with a deposit.

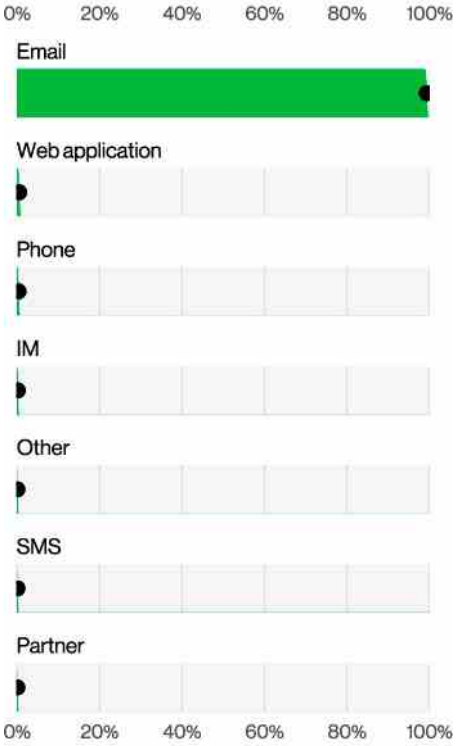


Figure 35. Top Action vectors in Social Engineering breaches (n=2,961)

67 At the time of writing, one of these was fake.

Low tech, high cost

Unfortunately, the bad news comes next, which is that BECs continue to have a substantial financial impact on organizations. Figure 36 captures the growth in terms of costs associated with BEC since early 2018. As we mentioned above, there isn't any growth this year as compared to last year, but neither has it decreased, with the median transaction hovering around $50,000.

One of the best things you can do when you realize you are a victim of BEC fraud is to promptly work with law enforcement. Figure 37 shows the distributions of outcomes from the cases our data contributors at the FBI IC3[68] have worked. In half of the cases, they were able to recoup 79% or more of the losses. On the less fortunate side, 18% of the incidents had nothing frozen and potentially lost everything that was sent to the criminals.

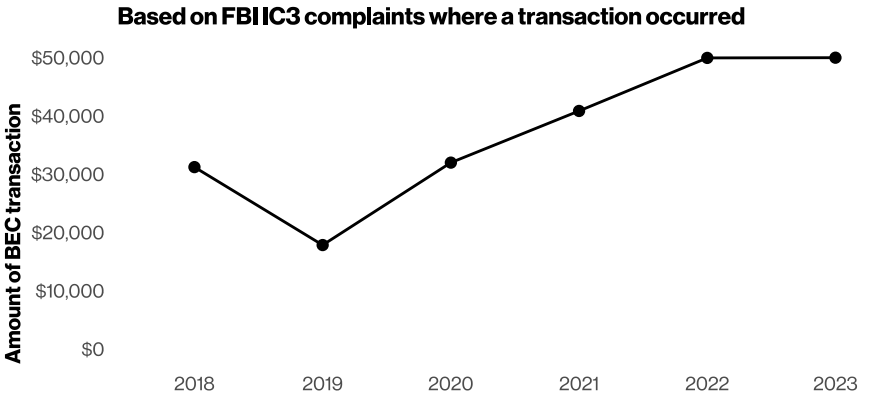


Figure 36. Median transaction size for BECs

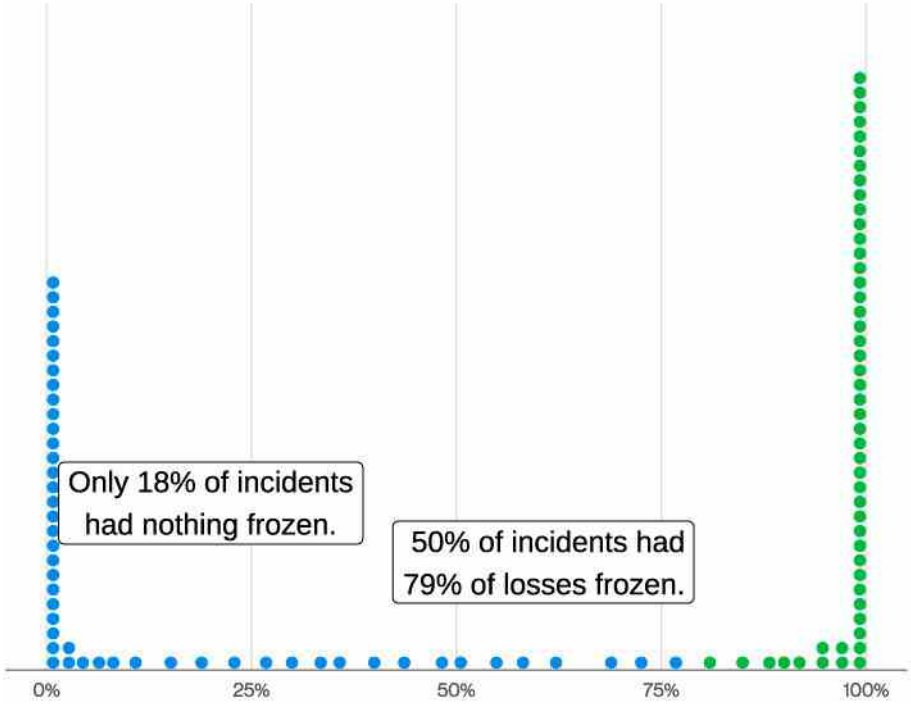


Figure 37. Percent of losses frozen for recovery

68 https://www.ic3.gov

I hope this threat finds you well.

Our introvert selves were already weary of all these social "interactions" even before these extortion-based attacks from ransomware groups busted through the door into the Social Engineering pattern. Social attacks, such as those involving Phishing, have long played their part in ushering in a ransomware deployment, as typified by the leveraging of those techniques in the ALPHV breach of MGM Resorts and other entertainment groups. But given the shift in tactics by some groups, along with the Extortion action being the final result of the breach as opposed to an initial one, this seemingly "System intrusion-y" attack now also shows up in this pattern.

Keep in mind, however, that Extortion isn't anything new in this pattern. We've seen various iterations of it from the empty threats ("We've hacked your phone and caught you doing NSFW stuff.") to somewhat credible threats ("Look us up. We're super-duper hackers that'll DDoS you.") to very credible threats ("We'll leak the data we took. Here are samples for you to validate."). This year, however, Extortion showed up in spades as a result of the MOVEit breach, which affected organizations on a relatively large scale and in an extremely public fashion.

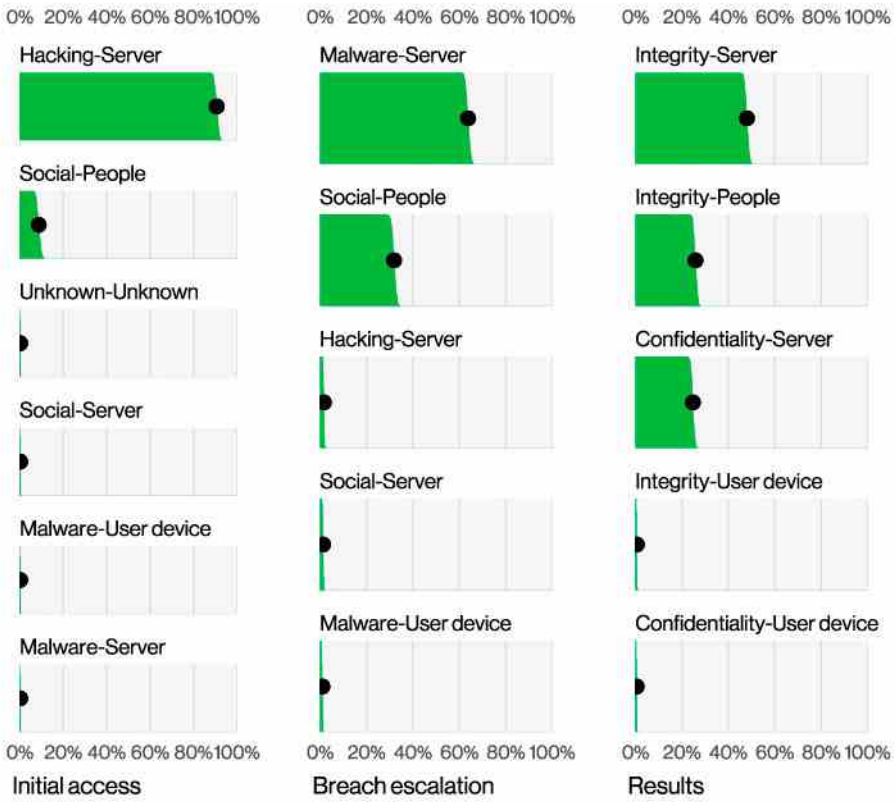


Figure 38. Steps in Social Engineering incidents

This is plainly visible in the steps to breaches chart (Figure 38). As you can see, there has been a dramatic increase in compromising servers via Hacking. Given the prevalence of these types of attacks, we recommend discussions with leadership to determine what the course of action should be if they occur in your organization.

School of phishes

This is probably cliché at this point, but we're believers that the first line of defense for any organization isn't the castrametation[69] of their systems but the education of their key staff, including end users.[70] Fortunately, this isn't simply us standing on our "user-awareness" soapbox. We have both figures and hard numbers to help quantify our stance. The first lesson to learn is that Phishing attacks happen fast. The median time to click on a malicious link after the email is opened is 21 seconds, and then it takes only another 28 seconds to enter the data (Figure 39). That leads to a frightening finding: The median time for users to fall for phishing emails is less than 60 seconds.

Some good news is that, as an industry, we seem to be getting better with regard to phishing test reporting. More than 20% of users identified and reported phishing per engagement, including 11% of the users who did click the email. As Figure 40 illustrates, this is another impressive improvement and one that we desperately need in order to catch up with the previous year's increases in Phishing and Pretexting.

That leads to a frightening finding: The median time for users to fall for phishing emails is less than 60 seconds.

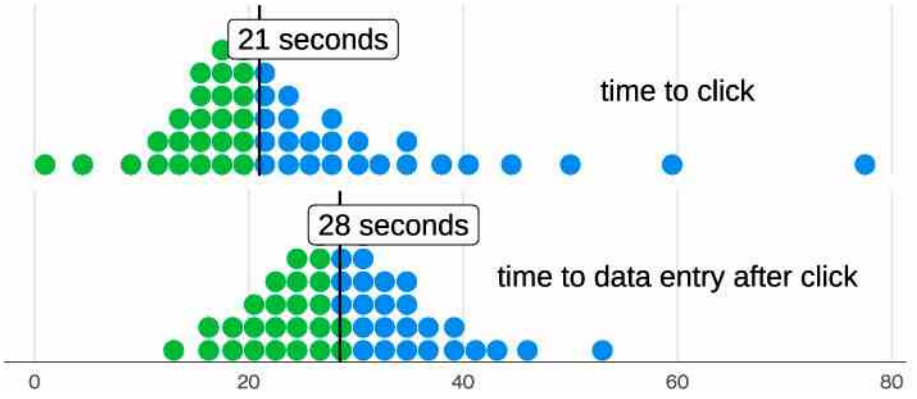


Figure 39. Time between email clicked and data entered

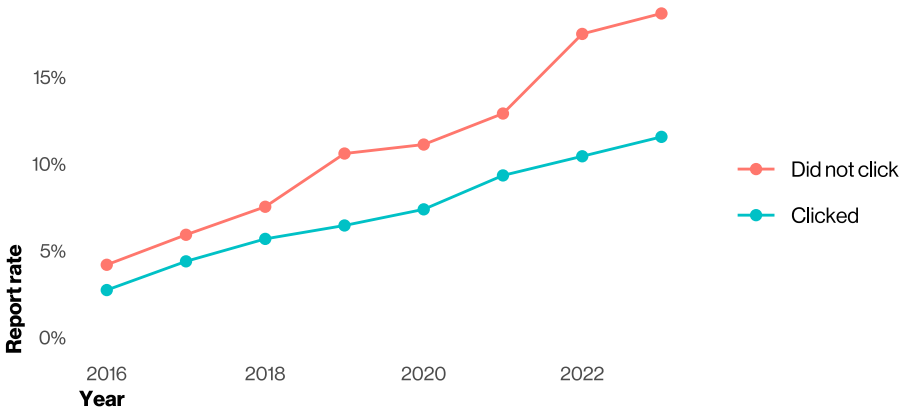


Figure 40. Phishing email report rate by click status

69 There is a very obvious Maginot Line joke to be made here, so we will leave it as an exercise for the readers.

70 Perhaps we should say, "especially end users."

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 attack. 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.

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/ Revoking Process [6.1, 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

Threat actors continue to take advantage of assets with default, simplistic and easily guessable credentials via brute forcing them, buying them or reusing them from previous breaches.

What is the same?

Financially motivated external actors continue to target credentials and personal information.

Frequency	1,997 incidents, 881 with confirmed data disclosure
Threat actors	External (100%), Internal (1%), Multiple (1%) (breaches)
Actor motives	Financial (85%), Espionage (15%) (breaches)
Data compromised	Credentials (71%), Personal (58%), Other (29%), Internal (17%) (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

What if we were to tell you there is perhaps no pattern that is as complex, multifaceted and, quite frankly, riveting to read about as the Basic Web Application Attacks pattern? We'd be pulling your leg, that's what. This pattern is basically just like it sounds: typically uncomplicated attacks against either unprotected or (more often) poorly protected web applications that grant the criminal a foothold into an organization's environment. If the System Intrusion pattern can be thought of as a sophisticated bank[71] heist,[72] this pattern presents us with a good visualization of Occam's razor in action. It has fewer steps and is possibly the simplest and shortest path from point A to point B. Like many things that are not overly complicated, it works extremely well.

Last year, this type of attack accounted for one-quarter of all breaches. This year, however, our dataset shows just over 8% of breaches in the Basic Web Application Attacks pattern. As is always the case in this pattern, the attacker gains access via hacking by the Use of stolen credentials (77%), Brute force (usually easily guessable passwords) (21%) or the Exploit vuln action (13%) (Figure 41).

Beware devs bearing crypto.

Interestingly, approximately 20% of the malware in this pattern consists of cryptocurrency mining Malware. Upon further inspection, we found a small cluster of Nation-state actors that were leveraging known vulnerabilities and cryptocurrency mining malware (and Ransomware) to make a few extra dollars for their country. Not something particularly revolutionary but always interesting to see tactics that are more than a decade old still hold up.

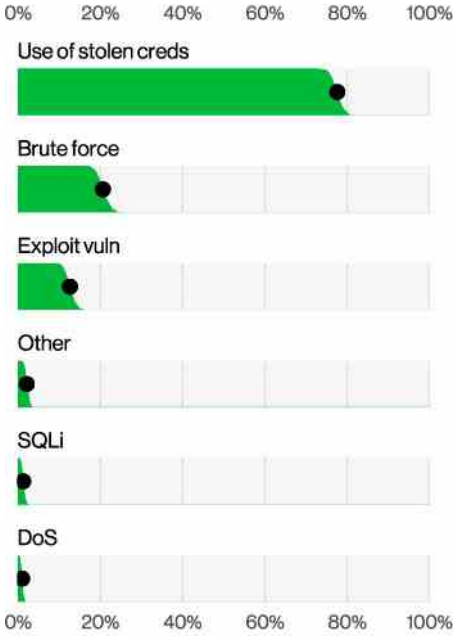


Figure 41. Top Hacking actions in Basic Web Application Attacks breaches (n=713)

Like a one-size-fits-all gas station baseball cap ("Keep on Truckin'"), any organization can fit into the Basic Web Application Attacks pattern, but it won't look too good on you. The Financial and Insurance (18%); Information (14%); and Professional, Scientific and Technical Services (13%) industries make up the top three verticals affected by Basic Web Application Attacks, but we see these attacks in most other industries as well. There is also no substantial difference between large organizations (55%) and small organizations (47%) in the Basic Web Application Attacks pattern.

Attack of the stolen credentials

If you're a regular reader,[73] you may have realized by now that there are a great many incidents in our dataset that leverage stolen credentials. Over the past 10 years, stolen credentials have appeared in almost one-third (31%) of breaches (Figure 42). Ergo, credentials are a core component of compromising organizations. However, while we know this to be a fact, there are a lot of things we don't know about these credentials: Where do they come from, how did they get here and will we ever know the full story?[74]

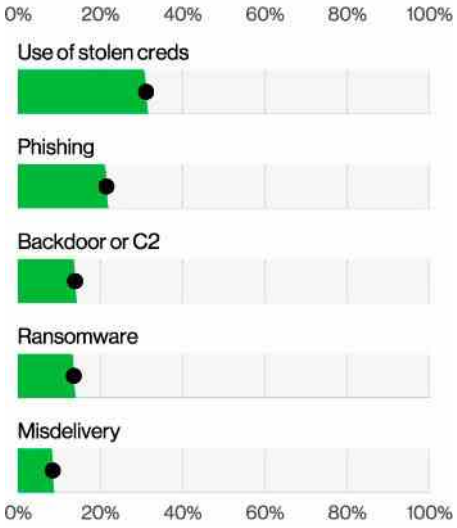


Figure 42. Top Action varieties since 2013 (n=35,970)

71 For more bank heist content, please review the Financial vertical in the "Industries" section.
72 We probably shouldn't mention movies such as "Ocean's Eleven" or "The Great Train Robbery" or we may need to pay royalties.
73 And we hope you are.
74 Or will it just continue to spice up our daily lives with mystery?

If we are to understand where stolen credentials come from, we must consider the different types of credential attacks that exist. Unsurprisingly, Phishing is the most common credential-related attack that we see in our dataset and accounts for 14% of breaches involving Credentials. Social Engineering is extremely common and remarkably effective because it targets individuals versus systems. It's much easier to harden a system than it is to harden an individual,[75] as our Social Engineering section illustrated. Another basic type of credential attack is Brute force (guessing all the passwords), and while it is an effective tool in the attacker's arsenal, it appears in only 2% of breaches this year. This technique is most successful when individuals or applications use weak or, even worse, default credentials. A silver lining here is that Brute force attacks have existed as long as there has been a login option, so a multitude of mitigations are commonly available, such as enforcing password complexity (ick) and length (slightly less ick) as well as limiting how quickly and how often logins can be attempted.

No country for old credentials

Credential stuffing is Brute force's more hip cousin.[76] While these attacks have a lot in common, credential stuffing affords the attacker a greater chance of success. That's because rather than guessing all possible combinations, credential stuffing leverages combinations of usernames/emails and passwords that are already known to exist because they were harvested from previous breaches. Recent high-profile cases have occurred in which attackers leveraged this technique to gain access to highly personal user data.

These types of attacks are more insidious because they spread the attack across various accounts and IP addresses, thus making them more difficult to prevent. If your organization has a high number of customers, especially consumer-facing web applications and application programming interfaces (APIs), you should consider instituting robust protections before attackers use a tool and a free list of proxies to attempt combinations they found in a chat site.

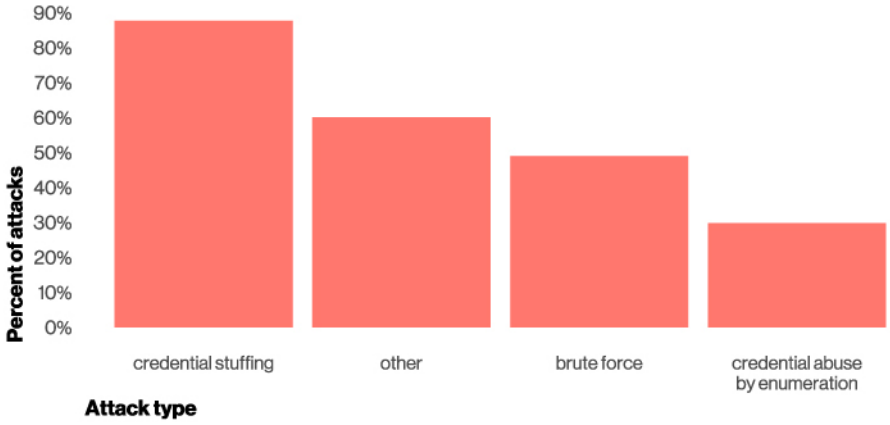


Figure 43. Distribution of web application attack types

Speaking of APIs, we can examine the prevalence of those types of attacks in sampled detection data from our API firewall data partners in Figure 43. As expected, credential stuffing is the most commonly identified attack, but it is often commingled with Brute force. Another interesting result from this dataset was that the prevalence of credential abuse-like attacks amounted to only 15% of attacks, less than half of what we see in Use of stolen credentials in the incident dataset. This makes sense because there is much more to try to exploit on APIs than just credentials.

But what if you don't have consumer facing web applications or APIs? What if you already enforce strict password policies, such as a monthly rotation of 24-character passwords? Surely such a fate could not befall you, right? Unfortunately, password stealers can still snatch your data. While we admittedly do not see password dumpers too often in our dataset (2% of breaches), it is important to keep in mind that we can only report on those things into which we have visibility, and this type of Malware likes to reside in places where there's limited visibility[77] (such as personal computers, not work-related ones).

To get an idea of how pervasive this issue might be, we took a look at the marketplaces dedicated to selling and reselling credentials and cookies collected from these password stealers. Our sample was only two days from one market; nevertheless, we found more than a thousand credentials per day being posted for sale with an average price of $10.

75 The former becomes more secure, while the latter simply becomes jaded.
76 Aviator sunglasses are involved.
77 Not unlike Bigfoot (No DBIR would be complete without at least one Sasquatch reference.)

After examining these postings, we found that 65% of these credentials were posted for sale less than one day from when they were collected.[78] They are often purchased by attackers who leverage them as a beachhead for other attacks, against either individuals or their employers. Oftentimes these product offerings not only list what credentials or cookies are available but also give information regarding the associated region. We wanted to determine whether these credentials are coming from organizationally managed assets or personal computers. On average, more than 30% of postings had no social media credentials listed, which could be an indication that many of the systems aren't for personal use. Figure 44 shows the percentage of postings by stealer family name without social media accounts listed.

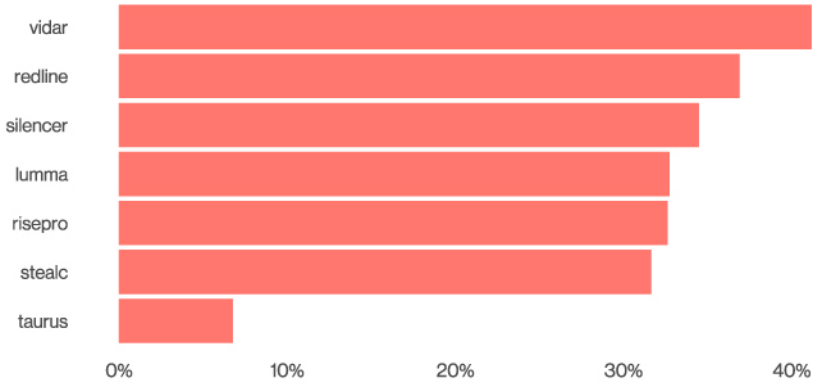


Figure 44. Percentage of stealer postings without major social media accounts listed

Another source of password stealers are libraries posted on public repositories. For the non-developers of the world, writing code is incredibly tedious, and our "if it's not easy, I'm not doing it" society has led to people creating libraries that other developers can import simply by saying "pip install library-of-my-choice" or "install. packages ('library-of-my-choice')"[79] and download the library they find posted. Needless to say, a very real risk with this approach is that you're taking it on faith that the libraries you're downloading are free from malware. Human nature being what it is, that is often not the case, and the libraries act as a means of distributing malware. Fortunately, there are numerous companies that actively scan the uploaded libraries to identify possible malware. When malicious packages are found, they often consist of information stealers (shocker).

Of course, simply uploading a package is not enough, it still requires someone to download it.[80] Figure 45 captures some of the more popular approaches found in an npm repository.[81] The most common type we found in the JavaScript ecosystems were malicious packages that would advertise themselves as free video game currency generators. These target the folks who are clever enough to know how to install and download the code but not sufficiently clever to realize that if it sounds too good to be true, it usually is.[82]

In addition, there were malicious packages that leveraged typosquatting. This is when the developer of the malware posts the package with a similar name as a popular package in the hopes that someone would accidentally mistype the package name when attempting to install the legitimate package. As a group of authors who collectively would be unemployed if it were not for the existence of spell-check, we can see this being a relatively effective tactic.

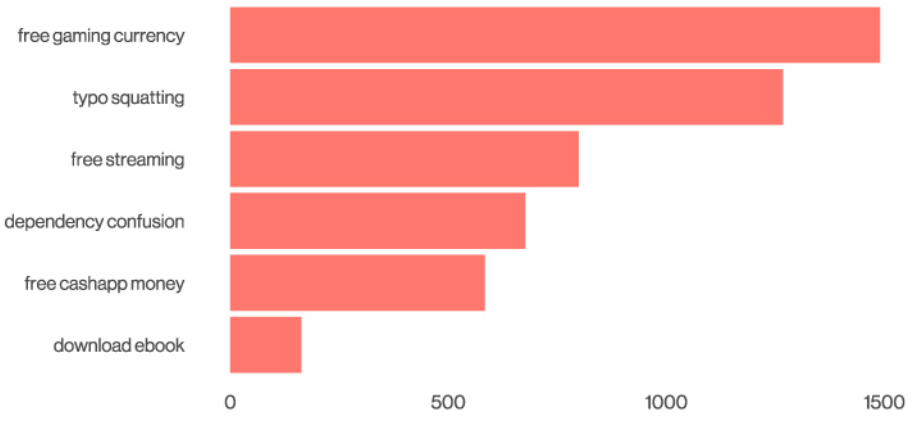


Figure 45. Malicious npm packages by Social Engineering technique

78 If these creds were doughnuts, the "hot and fresh" sign would still be on.
79 Bet you can't guess what coding environments the DBIR team uses :p
80 Same as this report: If you got this PDF or printed issue from a friend, please go to verizon.com/dbir and download a copy for yourself. Download early, download often!
81 https://www.npmjs.com/about
82 We're afraid there are no cheat codes to get money. Microtransactions for live-service games function the other way around.

Lastly, there were also packages that targeted what we (and a few people smarter than we are) believe are dependency confusion attacks. In these types of attacks, the attackers take advantage of how some tooling checks for packages on public repositories before it checks for private ones. If the attackers know that organizations are using the library "super-cool-internal-library," which is stored in their internal repository, the attackers can create a library on a public repository called "super-cool-internal-library" and the tooling may check the public repo first before looking at the internal ones. Fortunately, there are various programming best practices that can help mitigate this, alongside all the great companies that are out there helping protect us from these threats.

Take a breather after reading this section; there seem to be a lot of landmines that you have to avoid to help keep your organization safe from credential attacks. This is not new. We (and many others) have said it before: Multifactor authentication (MFA) goes a long way toward mitigating these types of attacks. For that matter, so does not letting your kids use your corporate computer to find ways of making free V-Bucks.[83] As with anything else security related, the most effective controls are typically the ones that leverage the human element along with technical resources.

CIS Controls for consideration

Mitigating against stolen credentials

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 Process [6.1, 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]

83 Be sure to read all sections of the report to unlock custom cover skins from our DBIR Battle Pass.

Miscellaneous Errors

Summary

Errors have increased substantially this year, possibly indicating a rise in Carelessness, although it may also reflect increased data visibility with new contributors. More than 50% of errors were the result of Misdelivery, continuing last year's trend, while other errors, such as Disposal, are declining. End-users now account for 87% of errors, emphasizing the need for universal error-catching controls across industries.

What is the same?

We can always count on people making mistakes. The categories of mistakes they make are consistent year over year, and while some Error varieties have been decreasing, the ranking of frequency remains the same.

Frequency	2,679 incidents, 2,671 with confirmed data disclosure
Threat actors	Internal (100%) (breaches)
Data compromised	Personal (94%), Internal (34%), Bank (14%), Other (12%) (breaches)

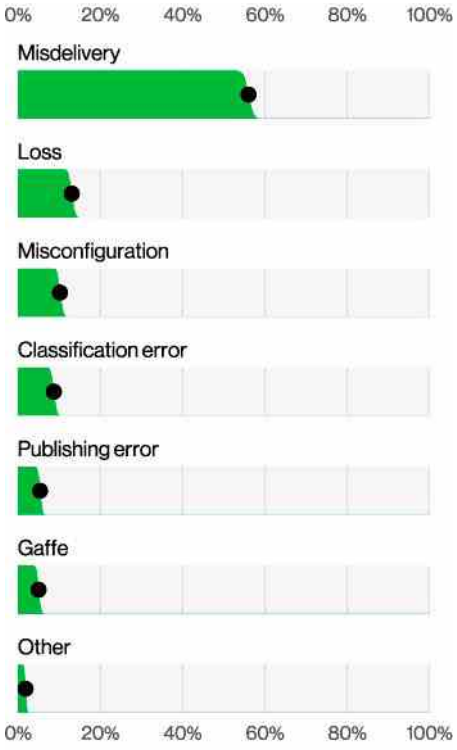


Figure 46. Top Action varieties in Miscellaneous Errors breaches (n=2,586)

I know exactly what I'm doing.

In our fast-paced and hectic world, it is easy to make the occasional mistake. The key is to make sure that those errors remain occasional and do not become habitual. Employees might be inching toward the latter state given the fact that we saw approximately five times as many Error-related breaches this year as we did in last year's report. Does this substantial increase mean that incompetence and inattention to detail are booming?[84] Possibly, but it is also, as stated earlier in this report, indicative of the generosity of our data-sharing partners. The greater the number of breaches that we examine, the higher these percentages become. More than 50% of errors in 2023 resulted from Misdelivery (sending something to the wrong recipient), as shown in Figure 46. This was also the No. 1 category in last year's report.

Misconfiguration is the next most common error and was seen in approximately 10% of breaches. Misconfiguration has been on a downward trend[85] for the last three years. There are a few possible explanations for this. Chief among them is that (thankfully) many systems are becoming more secure by default, making the practice of standing up new tech without reading the manual a less risky proposal. Other factors may include that security researchers are not spending as much time on finding these systems with their screen doors flapping in the wind, and, lastly,

84 Look around at your coworkers, and use your best judgment to answer that question.
85 Not unlike most of civilization

criminals may be using the same tools historically utilized by researchers to discover these errors and exploiting them to steal data, which would result in the attack showing up with a Hacking action rather than Error.

Classification errors, Publishing errors and Gaffes (verbal slips) are all relatively tightly packed in order of mention. Disposal errors continue to decline ever so slightly (as has been the general trend for the last several years) and accounted for just over 1% of the cases in this pattern. It is unclear whether more attention has been paid to this matter or employees have simply gotten better at burning records in a barrel in the parking lot.

Figure 47 shows one rather drastic change in this pattern related to actors: End-user accounted for 87% of errors as opposed to 20% in last year's report, while System administrators dropped to only 11% (from 46% last year). This drop is in large part the result of the corresponding rise in Misdelivery—it takes a System administrator to misconfigure, but any old End-user can misdeliver. Power to the people!

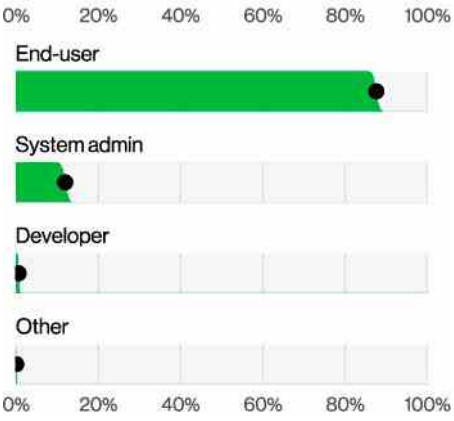


Figure 47. Top Actor varieties in Miscellaneous Errors breaches (n=2,260)

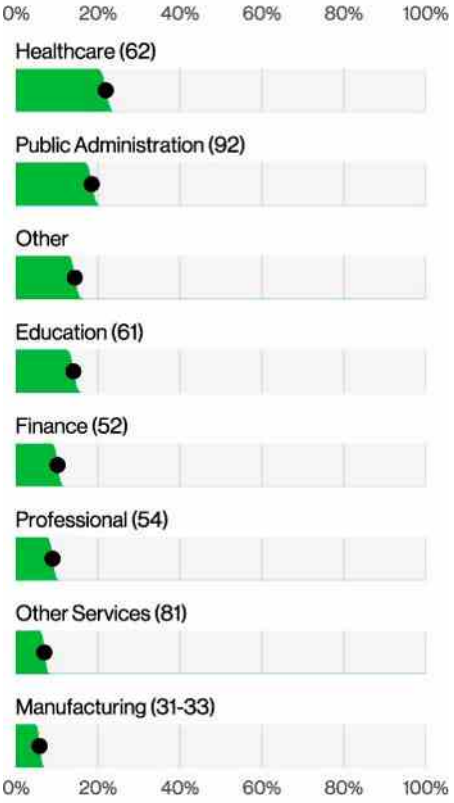


Figure 48. Top industries in Miscellaneous Errors breaches (n=2,671)

Lastly, the Miscellaneous Errors pattern shows a relative diverse array of industry types (Figure 48), with Healthcare and Public Administration at the top (understandably, given reporting requirements) and a good showing from other industries such as Financial and Insurance; Education; and Professional, Scientific and Technical Services. This illustrates the important fact that carelessness is somewhat of a universal trait, so employers in any vertical should ensure that their controls will catch these kinds of errors early.

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]

Denial of Service

Summary

Denial of Service attacks can target different points of infrastructure and will manifest themselves in several forms that organizations need to be prepared to handle.

Frequency	16,843 incidents, 3 with confirmed data disclosure
Threat actors	External (100%) (all incidents)

What is the same?

Denial of Service attacks continue to be ubiquitous and the top pattern for incidents.

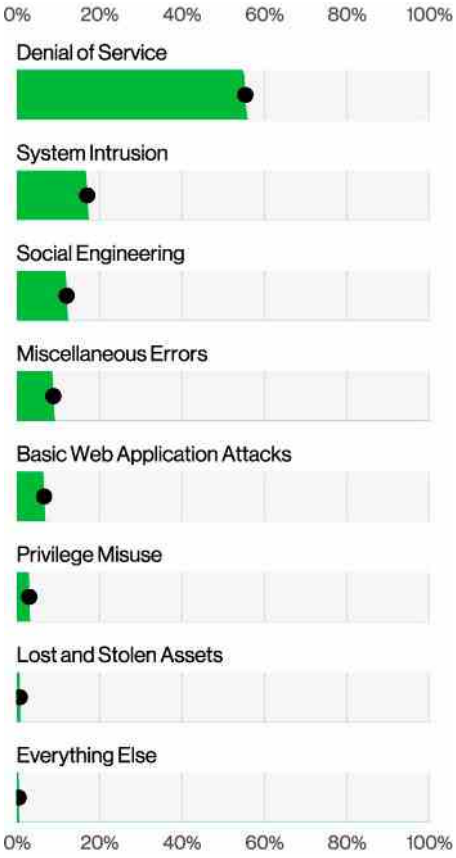


Figure 49. Patterns in incidents (n=30,458)

Another year, another victory lap to our running champion, Denial of Service. Figure 49 shows this pattern being responsible for more than 50% of incidents analyzed this year.[86] This pattern has been the most prevalent one for several years now, and you don't have to think very hard to understand why: Denial of Service attacks are relatively cheap to execute, and it is actually fairly easy for them to be successful,[87] at least until an organization's defenses are activated to mitigate them.

Our ongoing analysis of content delivery network (CDN)-monitored, web application-focused Denial of Service attacks shows that even though the median attack size has reduced slightly from 2.2 gigabits per second (Gbps) to 1.6 Gbps, the 97.5th percentile of those attacks[88] increased to 170 Gbps from the previous high of 124 Gbps. Figure 50 showcases the data and the other percentile break points like the more realistic and grounded 90th percentiles. Those types of attacks are usually short duration, with large volumes—50% of those attacks are less than five minutes long.

However, this year, we would like to try something different: Those precision-targeted attacks are very high volume. It is interesting to see the contrast to the impact of general distributed DoS (DDoS) filtering on the ISP level, where it is necessary to mitigate against a much wider variety of attacks and is prone to collateral damage from the high-volume ones.

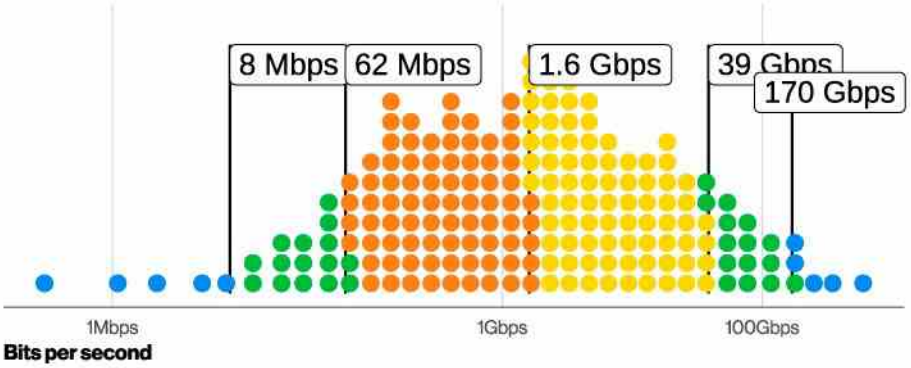


Figure 50. Bits per second in CDN DDoS incidents (n=10,713)

86 No electric toothbrushes were harmed during this observed growth of the Denial of Service pattern.
87 To some degree of negligible success
88 Or as we like to call it, "the statistical worst-case scenario that is not that weird outlier messing up your data analysis."

Figures 51 and 52 represent the distribution of both bits per second and packets per second distribution of ISP-level collateral attacks all over the world.[89] This dataset includes attacks on ISPs themselves; enterprises that paid for DDoS protection from their ISPs; and even individual users with broadband, mobile, wireless or satellite.[90] It's clear that these are much smaller in size because the volume for this diverse group would not need to be as big as for enterprises. Those are also longer duration attacks, with the median attack time being around nine minutes.[91] All in all, this class of Denial of Service attacks might be more representative of the challenges a non-e-commerce or heavily extranet service-oriented organization might face.

Additionally, our subject matter experts (SMEs) continue to report the growth of low-volume, persistent attacks on high-interaction services such as Domain Name System (DNS). When you want to take someone off the internet, there is more than one way to peel a potato.[92]

At the end of the day, our recommendation remains the same as in the previous years. There is relatively minimal setup necessary for a DoS attack to take place, so organizations should consider having some sort of automated or semi-automated protection system to help mitigate those. There is not a lot more to be done than to be prepared for the eventuality of some threat actor wanting to sever you from the internet for a while. To think otherwise is to live in denial.

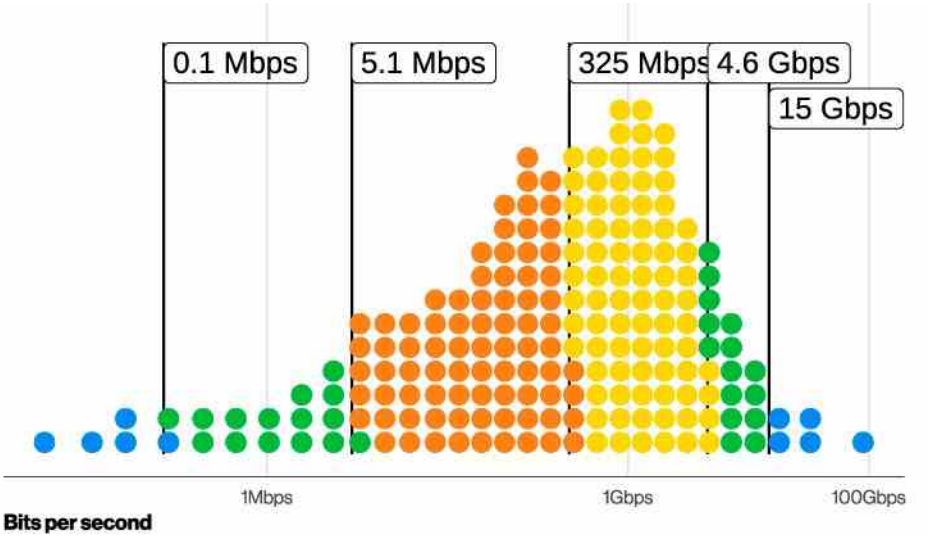


Figure 51. Bits per second in ISP-level DDoS incidents (n=800,155)

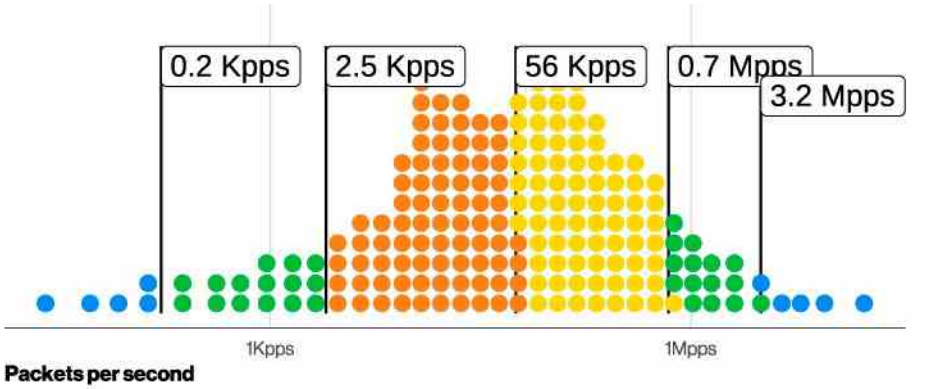


Figure 52. Packets per second in ISP-level DDoS incidents (n=800,155)

89 Look at the size of that number of samples (n)!
90 Psst! Don't tell the Verizon Consumer Group we are encroaching on their turf.
91 More than enough to mess up your online poker match
92 The DBIR is pet-friendly and condemns the "skinning of cats" as a figure of speech.

Lost and Stolen Assets

Summary

This year we saw an increase in the percentage of cases resulting in confirmed data breaches in this pattern.

What is the same?

Devices are still much more likely to be lost than stolen. Laptops continue to be a risk for loss in particular.

Frequency	199 incidents, 181 with confirmed data disclosure
Threat actors	Internal (88%), External (12%) (breaches)
Actor motives	Financial (92%–100%), Convenience/ Espionage/Fear/Fun/ Grudge/Ideology/ Other/Secondary (0%–8% each) (breaches)
Data compromised	Personal (97%), Internal (42%), Bank (25%), Other (17%) (breaches)

Now where did I put that?

If you've ever been through the line at airport security where you had to remove your electronic devices, take off your shoes and throw away that bottle of water you weren't finished with, all while masking the amount of anxiety you were feeling to avoid triggering an "enhanced security screening," you know that it's a stressful experience. It is little wonder items go missing while people are away from their usual environment and potentially distracted. Despite having wonderful data storage capabilities and an ever-smaller size, User Devices are the most likely to go missing—whether by ill will or inattention. Chief among them is the ubiquitous laptop, and we've seen an increase of those events this year after a brief downturn in 2022, as shown in Figure 53.

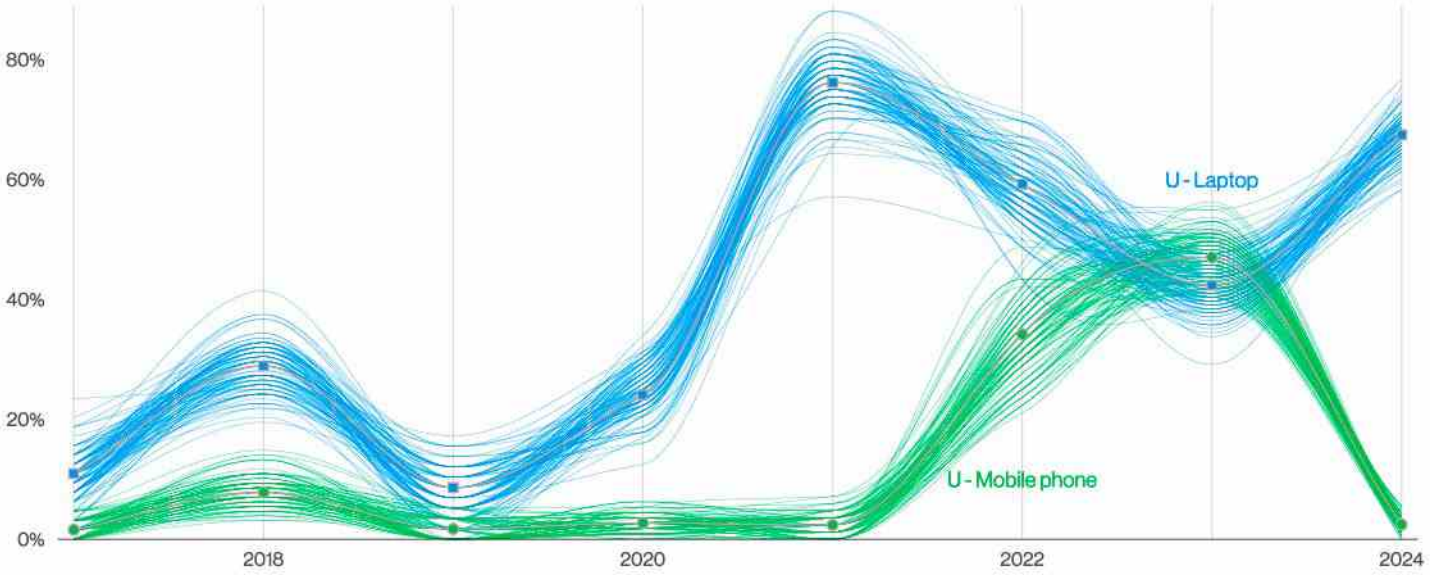


Figure 53. Top Asset varieties over time in Lost and Stolen Assets

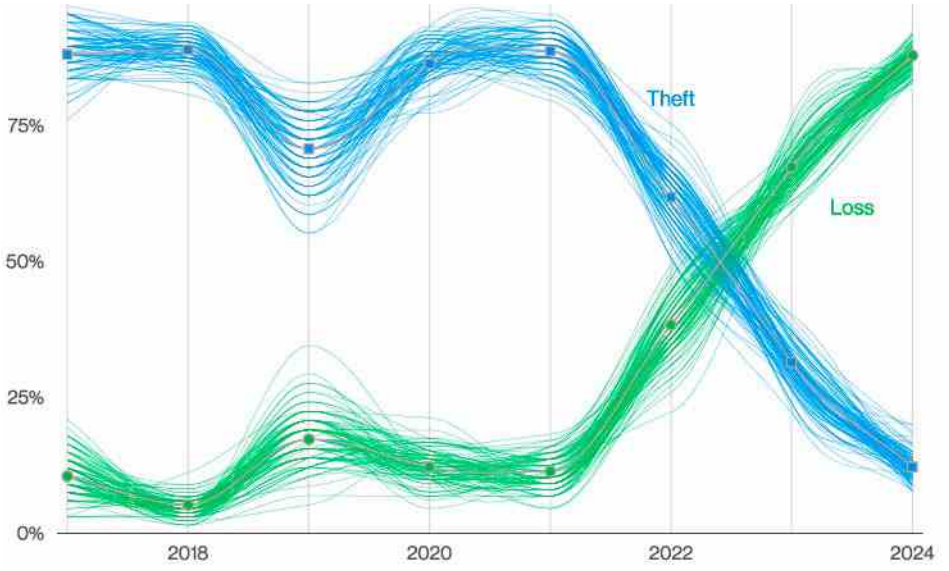


Figure 54. Top Action varieties over time in Lost and Stolen Assets

As we have seen consistently in our dataset, assets are vastly more likely to be lost than stolen. Figure 54 shows that this was not always the case. Until 2021, we saw more items stolen, but perhaps given the pandemic's lessening of people out mingling, the theft opportunities were reduced. That said, we still see this trend despite most companies returning to a more traditional in-person work environment, so there could be something else at play here.

This year we saw a higher percentage of incidents involving Assets in this pattern causing confirmed data breaches as well, with last year showing about 8% confirmed breaches and this year showing a surprising 91%.

The important thing is to have protections on assets, where possible, that can stop a lost or stolen device from becoming a reportable data breach. Given the prevalence of this pattern, it seems that someone lost that memo.

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

Employee betrayal poses a significant threat because employees steal data for personal benefit, sometimes colluding with External actors. Personal data is the prime target, along with Internal information. While we saw a spike in Fraudulent transactions last year, that has once again leveled out and is a lesser concern.

What is the same?

Internal actors are again largely working on their own in this pattern. The Financial motivation remains in ascension, while Espionage is a distant second. Personal data is still the main targeted data type.

Frequency	897 incidents, 854 with confirmed data disclosure
Threat actors	Internal (100%), External (1%), Multiple (1%) (breaches)
Actor motives	Financial (88%), Espionage (46%), Grudge (6%), Ideology (2%), Other (2%) (breaches)
Data compromised	Personal (83%), Internal (46%), Other (22%), Bank (14%) (breaches)

Fool me once.

Companies trust their employees. They trust them to do their jobs, raise issues that need attention and generally have the organization's best interests at heart. And in a perfect world, everyone would go along with this plan. But in this pattern, we see that is not always the case. Sometimes employees are in it for their own benefit at the expense of the company.[93] Sometimes the relationship just isn't working out, and the employee feels entitled to the data that would make their landing at their next employer so much more attractive. As a consequence of actions such as these, we can provide the data breach analysis found in this pattern.[94] Nobody wants to believe their employees will do them dirty, but if it happens, do you know how your organization would detect it? If you don't, you're not alone, and it may have already happened.

Shame on you.

What motivates employees to steal data? In our experience, it is largely Financial. Whether they plan to use the data to commit financial crimes or just help them get a leg up in a new gig, it tends to be for their own direct benefit. We do also see the Espionage motive where employees take their ill-gotten gains to a direct competitor or even use them to start their own competing company. And they don't always work alone.

93 Et tu, Brute?
94 So it's not all bad news, right?

In our prior report, we saw collusion—multiple actors working in concert to achieve the goal of the breach—at 7%, which, while nowhere near the highs we saw back in 2019, was still a surprise. This year, things seem to have gone back to normal, and we are seeing collusion dropping to less than 1% of breaches. This is good news because it's bad enough when employees start making off with company data, but when they team up with outsiders, chaos ensues.

As Figure 55 shows, employees are largely taking Personal data—this is likely about customers, since names, contact info and other such things could be quite useful for both starting a new competing enterprise or for committing financial crimes. We saw Internal data show a bit of a spike this year as well, which would include sensitive plans and intellectual property that would attract the Espionage-motivated employee. Finally, Banking data is remaining mostly steady over time as a targeted data type.

Last year we observed a sharp uptick in the Fraudulent transaction, so we wanted to take a look this year to determine whether it was the start of a trend. This is commonly the end game of the BEC attack—where attackers socially engineer someone into sending them cash electronically. Internal actors already have access to systems containing that capability, and they made good use of it last year. We are happy to report that this trend has not continued. Despite spiking to almost 15% in last year's data, it has returned to a placid 3% this year.

CIS Controls for consideration

Manage access

Secure Configuration of Enterprise Assets and Software [4]
- Establish and Maintain a Secure Configuration Process [4.1]
- Manage Default Accounts on Enterprise Assets and Software [4.7]

Account Management [5]
- Disable Dormant Accounts [5.3]
- Restrict Administrator Privileges to Dedicated Administrator Accounts [5.4]

Access Control Management [6]
- Establish an Access Granting Process [6.1]
- Establish an Access Revoking Process [6.2]

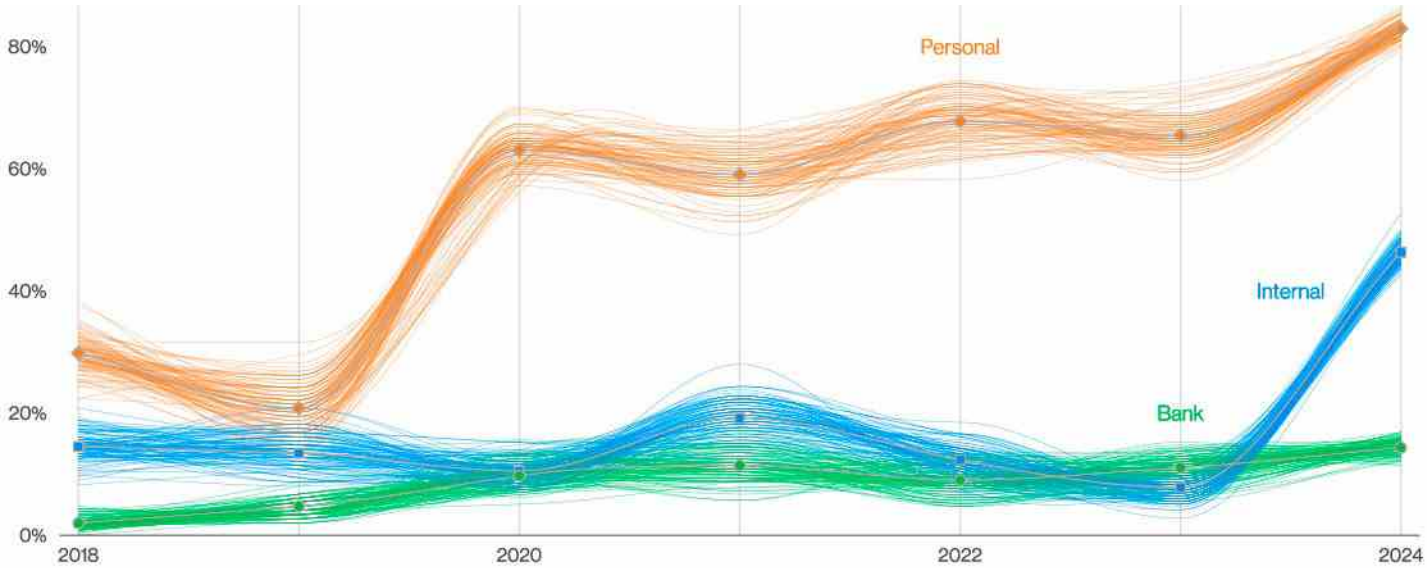


Figure 55. Top Confidentiality data varieties over time in Privilege Misuse breaches

4
Industries

Industries: Introduction

Greetings! If you are just stepping onto the DBIR scene, please consider this your orientation. For our more seasoned veterans, feel free to simply breeze past—this terrain should be familiar ground.

As mentioned previously, in this report we examined 30,458 incidents, of which 10,626 were confirmed data breaches. We will view both of these categories in a more granular fashion, along with how they played out in the various industries and regions, in the following sections of the report. As we have mentioned in previous editions, what keeps one industry tossing and turning at night may not even register as a blip on another's radar. It boils down to attack surfaces—the prime real estate for cyber malfeasance. When you factor in the nuances of specific types of threat actors, the technological infrastructures underpinning each sector, the type of data an organization handles and retains, and how folks access and use that data, you've mixed a potent cocktail of security complexities.

For example, consider a tech behemoth swimming in the digital sea of mobile devices and their respective apps. Its risk profile looks markedly different from that of a boutique establishment relying on a point-of-sale system or a simple e-commerce platform supported by its vendor. Furthermore, these findings are also influenced by reporting requirements, which means that industries may experience varying levels of scrutiny from that perspective. Finally, smaller sample sizes for given industries are also an important factor that comes into play with regard to statistical analysis (smaller sample sizes result in lessened statistical confidence). Therefore, we ask readers to refrain from rushing to conclusions about an industry's security posture based solely on incident reports.

If you are here for insights tailored to your industry, we recommend that you spend time looking at the top patterns for your industry and reading up on the relevant pattern sections of the report. Just to let you know, the DBIR aligns with the North American Industry Classification System (NAICS) to determine which industry an organization belongs to. More detail on this can be found in Appendix A.

	Incidents				Breaches			
Industry	Total	Small (1–1,000)	Large (1,000+)	Unknown	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	30,458	919	1,298	28,241	10,626	617	986	9,023
Accommodation (72)	220	16	9	195	106	16	9	81
Administrative (56)	28	7	7	14	21	6	4	11
Agriculture (11)	79	5	0	74	56	4	0	52
Construction (23)	249	17	6	226	220	12	5	203
Education (61)	1,780	82	630	1,068	1,537	56	618	863
Entertainment (71)	447	16	2	429	306	10	1	295
Finance (52)	3,348	75	122	3,151	1,115	54	87	974
Healthcare (62)	1,378	54	21	1,303	1,220	41	18	1,161
Information (51)	1,367	79	62	1,226	602	49	19	534
Management (55)	22	4	1	17	19	4	1	14
Manufacturing (31–33)	2,305	102	81	2,122	849	62	49	738
Mining (21)	30	1	2	27	20	1	1	18
Other Services (81)	462	13	5	444	417	8	5	404
Professional (54)	2,599	205	102	2,292	1,314	124	73	1,117
Public Administration (92)	12,217	56	115	12,046	1,085	39	27	1,019
Real Estate (53)	432	35	5	392	399	29	2	368
Retail (44–45)	725	90	47	588	369	55	32	282
Transportation (48–49)	260	21	38	201	138	17	12	109
Utilities (22)	191	17	11	163	130	12	6	112
Wholesale Trade (42)	76	22	21	33	54	17	14	23
Unknown	2,243	2	11	2,230	649	1	3	645
Total	30,458	919	1,298	28,241	10,626	617	986	9,023

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

Incidents

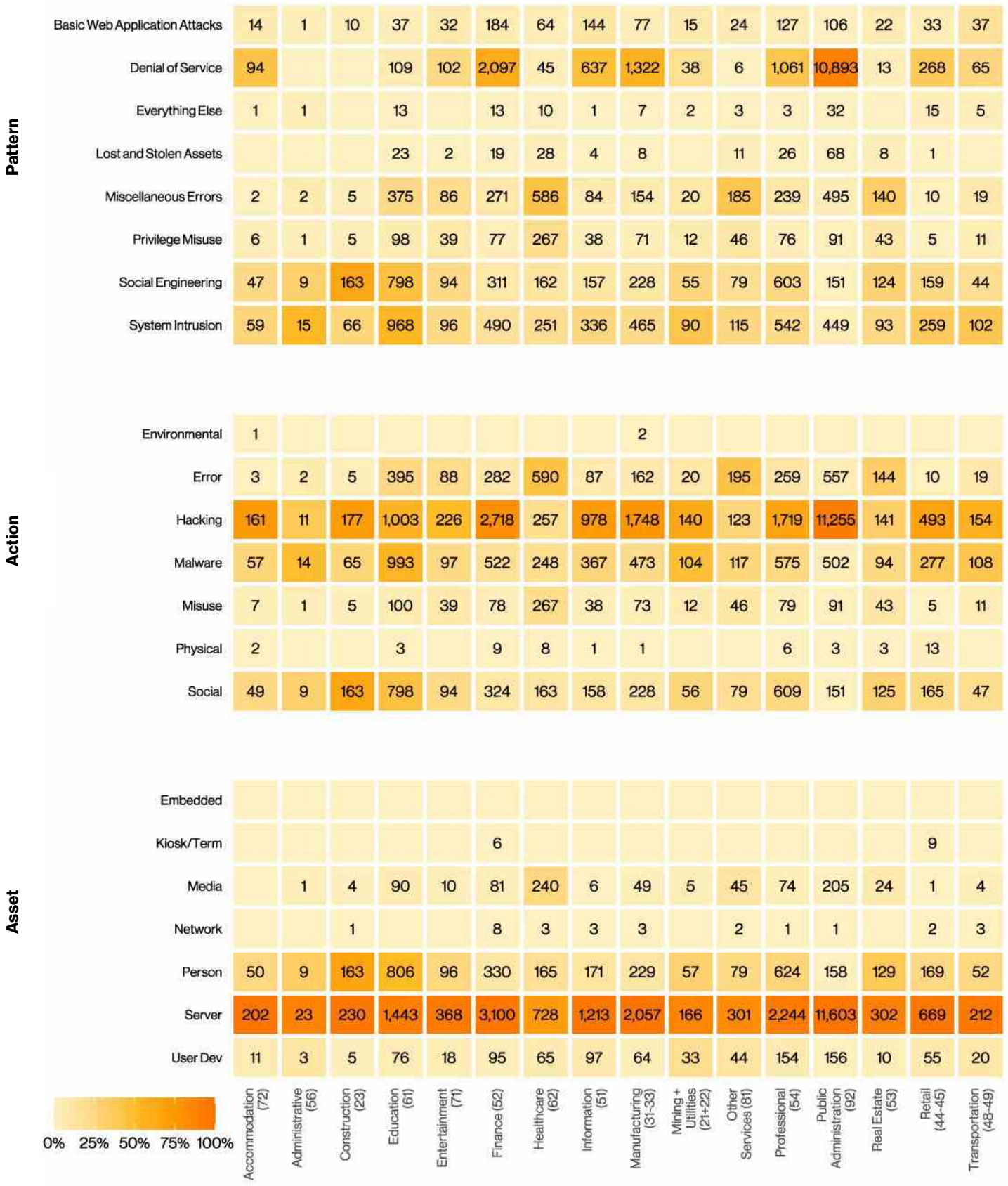


Figure 56. Incidents by industry

Breaches

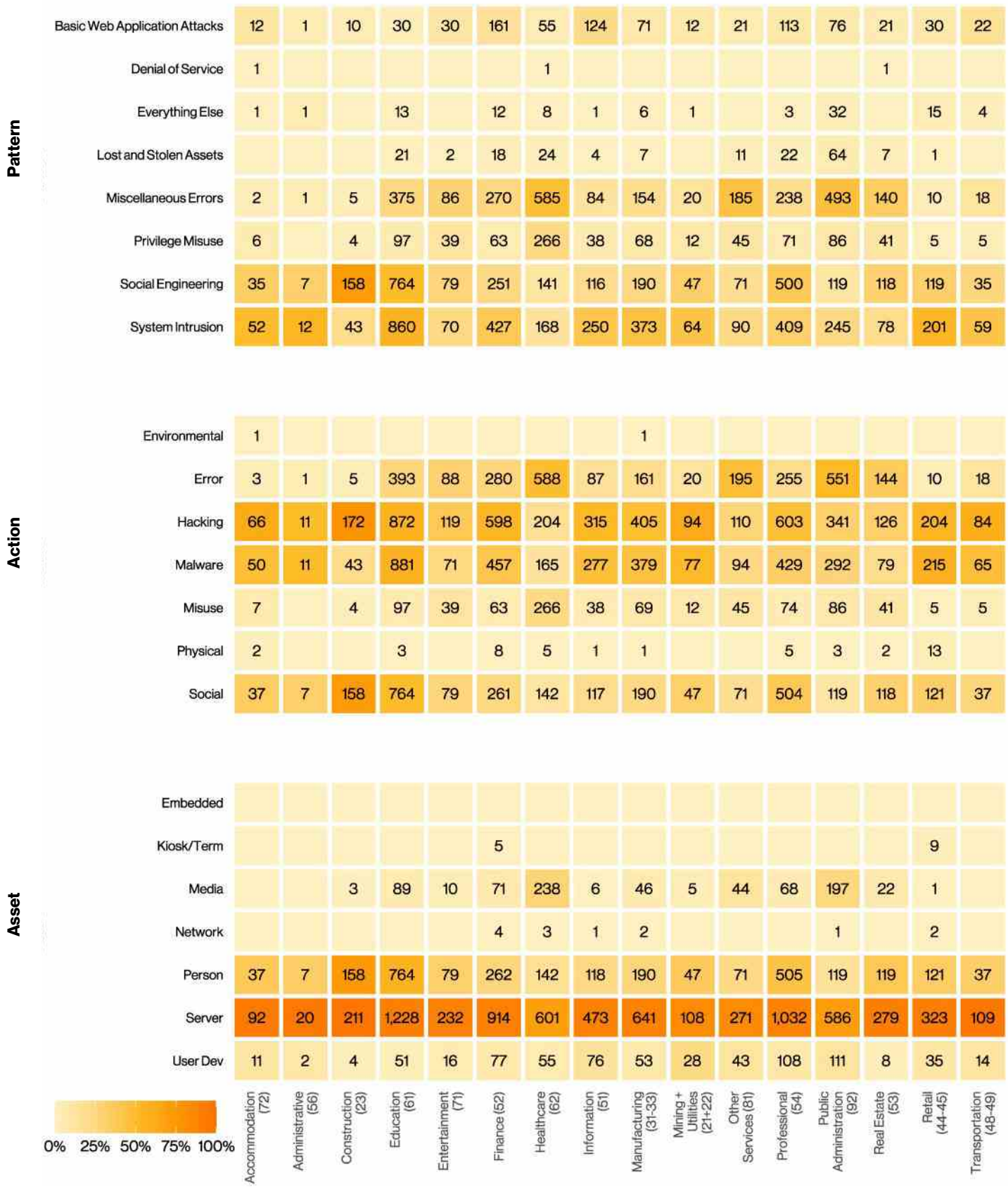


Figure 57. Breaches by industry

Accommodation and Food Services NAICS 72

Frequency	220 incidents, 106 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches
Threat actors	External (92%), Internal (9%), Multiple (1%) (breaches)
Actor motives	Financial (100%) (breaches)
Data compromised	Credentials (50%), Personal (28%), Payment (19%), System (19%), Other (16%) (breaches)
What is the same?	Ransomware and social attacks continue to be a persistent problem within this industry, accounting for 35% of incidents.

Summary

Social Engineering has increased dramatically and now accounts for 25% of incidents in this sector, with Pretexting more than doubling from the previous year and reporting 20% of incidents.

Spilling the bytes

There is always something cozy and comforting about the local coffee shop you call your second home, and attackers couldn't agree more. The Accommodation and Food Services industry continues to face the same core threats as before with System Intrusion, Social Engineering and Basic Web Application Attacks leading the pack. As is visible in Figure 58, there's been a notable increase in social engineering attacks from last year. This is largely a result of the increase in Pretexting, which has more than doubled over the last year and now accounts for 20% of the incidents.

As if accidentally handing over your hard-earned money to criminals wasn't annoying enough, organizations in this sector also have to contend with the rudest guests possible—ransomware actors. Ransomware continues to be one of the top action varieties and has been for the last three years. However, the only good news is that it hasn't increased this year and holds steady at 16% of all incidents.

In other news, Payment card data being compromised has dropped to an all-time low, from 41% of breaches in 2023 to now only 19%. This decrease aligns well with the overall decrease of Payment card data being targeted that we've seen across various industries, which may be indicating that shifts in chip technology might be causing threat actors to focus their efforts on other approaches. A nice bit of good news to enjoy with your cappuccino.

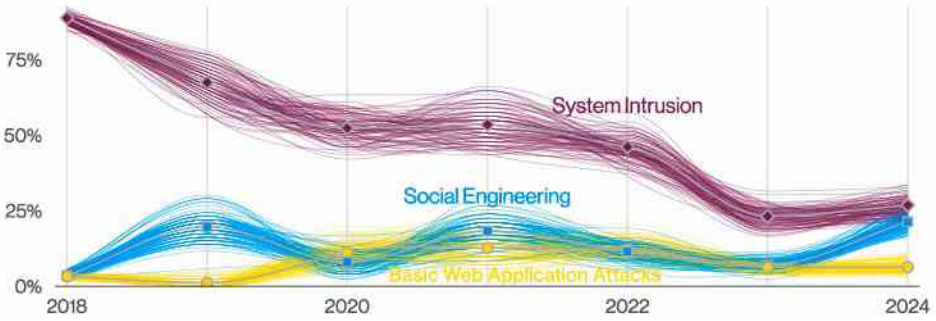


Figure 58. Top patterns in Accommodation and Food Services industry incidents

Educational Services NAICS 61

Frequency	1,780 incidents, 1,537 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Miscellaneous Errors represent 90% of breaches
Threat actors	External (68%), Internal (32%) (breaches)
Actor motives	Financial (98%), Espionage (2%) (breaches)
Data compromised	Personal (83%), Internal (20%), Other (18%), Credentials (9%) (breaches)
What is the same?	The same three patterns dominate this vertical as last year. External actors stealing Personal data accounts for the majority of breaches.

Summary

Errors of various types committed by internal actors and Extortion from external threat actors continue to constitute the curriculum of this industry.

Learn from your mistakes.

The Educational Services industry has a great deal to be proud of. It played a significant role in what was ultimately the creation of the internet, it created the textbook industry that we all know and love, and, of course, arguably its crowning achievement: recess. In spite of all this success, however, it is not without problems. But before we get into the Advanced Placement-level breach findings, let's cover the more remedial Error section. Figure 59 shows that the Miscellaneous Errors pattern has been trending upward for the last two years in the Educational Services vertical. Not unlike the other industries that we examine, Misdelivery is front and center, accounting for 56% of errors. Loss (19%) and Classification error (10%) round off the top three error varieties.

I feel so exploited.

Now that we have Errors out of the way, let's talk about the real area of concern for this vertical. The action types of malware (Backdoor – 57%), hacking (Exploit vuln – 56%) and social (Extortion – 50%) were present in almost the exact same percentages. This, of course, indicates that MOVEit—the well-known file transfer software that, when exploited, caused so much trouble for so many over the last year—was definitely enrolled in the Educational Services industry. As readers may recall, Ransomware was prevalent in this industry in last year's report and the end game of Ransomware is Extortion. The campaign that leveraged the MOVEit exploit was simply another, more refined,[95] method of achieving the same goal. Since the MOVEit exploit was present to such a high degree, Ransomware decreased proportionately as Backdoor increased. However, the end result for Educational Services was the same: It helped criminals pay off their student loans rather rapidly.

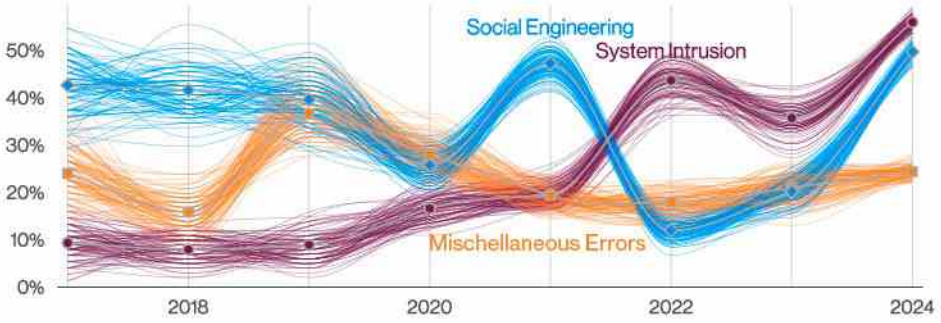


Figure 59. Top patterns in Educational Services industry breaches

95 Certainly less computationally intensive for forgoing the encryption. Who knew threat actors also cared about the environment?

Financial and Insurance NAICS 52

Frequency	3,348 incidents, 1,115 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Social Engineering represent 78% of breaches
Threat actors	External (69%), Internal (31%) (breaches)
Actor motives	Financial (95%), Espionage (5%) (breaches)
Data compromised	Personal (75%), Other (30%), Bank (27%), Credentials (22%) (breaches)
What is the same?	Miscellaneous Errors continue to plague this industry. As it did last year, Misdelivery presents an ongoing challenge for this sector.

Summary

System Intrusion has overtaken Miscellaneous Errors and Basic Web Application Attacks as the primary threat in Financial and Insurance this year, indicating a shift toward more complex attacks, accompanied by a rise in Social Engineering. Increased visibility into the Europe, Middle East and Africa (EMEA) region shows us that Ransomware attacks are alive and well there as well.

High as a Georgia pine

If our dataset is any indicator, interest rates and premiums aren't the only things rising in the Financial and Insurance industry. The System Intrusion pattern, where most of the more complex attacks typically reside, has risen from its third-place position last year to first place this year (Figure 60). The Social Engineering pattern, also typically a sign of increased complexity, is now in the top three patterns as well, while the more simplistic Basic Web Application Attacks (last year's champion) has fallen entirely off the podium. This is in relatively stark contrast to last year's findings in which we pointed out that the adversaries weren't having to expend a great deal of effort to gain access to corporate data in this vertical. These changes seem to indicate that attackers are being forced to work a bit harder in order to compromise organizations in this sector. That is good news for everybody—except the threat actor, of course.

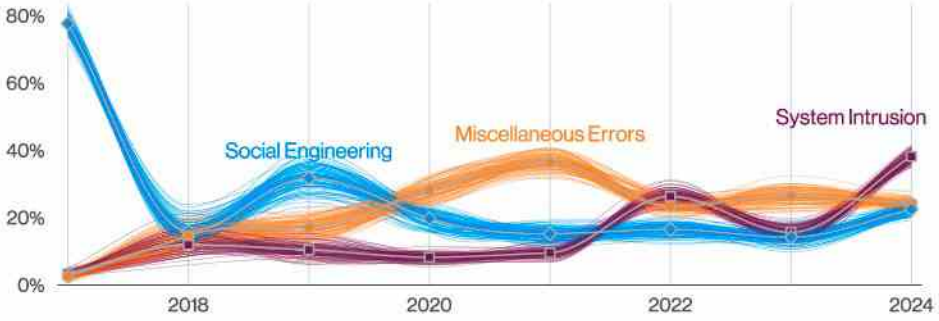


Figure 60. Top patterns in Financial and Insurance industry breaches

Lest they make it simply too difficult for criminals, this vertical remains consistent in committing Errors. As was almost universally the case this year, Misdelivery was quite prominent (Figure 61) and, along with Misconfiguration and Loss, made up most of the errors in this industry.

Has any action been taken?

With regard to Action varieties, they tell the story of the patterns relatively clearly. Ransomware and the Use of stolen credentials, the bread and butter of the System Intrusion pattern, are very common in this industry (and help boost that 95% Financial motive). All of those stolen credentials have to come from somewhere, and that somewhere is frequently from social attacks such as Phishing and Pretexting. Of course credentials can also come from a multitude of other sources such as Brute force attacks (although it was quite low on the list for hacking actions) or simply harvested and reused from another breach.

Lastly, but certainly worthy of mention, is that 8% of the cases in our incident dataset targeting this sector were part of the whirlwind of the MOVEit breach, which shows how far-reaching supply chain breaches can be.

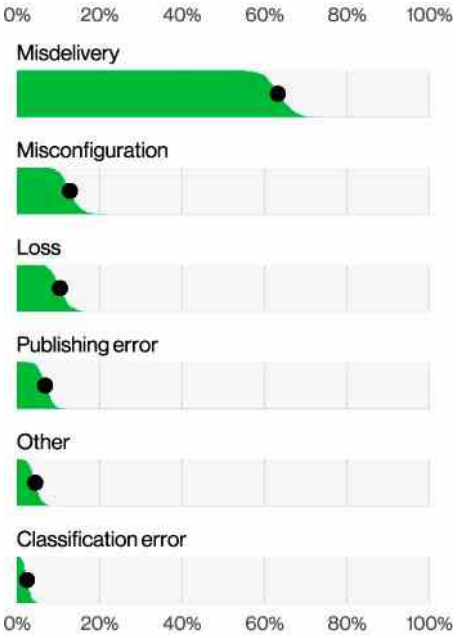


Figure 61. Top Error varieties in Financial and Insurance industry breaches (n=250)

Healthcare NAICS 62

Frequency	1,378 incidents, 1,220 with confirmed data disclosure
Top patterns	Miscellaneous Errors, Privilege Misuse and System Intrusion represent 83% of breaches
Threat actors	Internal (70%), External (30%) (breaches)
Actor motives	Financial (98%), Espionage (1%) (breaches)
Data compromised	Personal (75%), Internal (51%), Other (25%), Credentials (13%) (breaches)
What is the same?	System Intrusion breaches remain in the top three attack patterns.

Summary

This year's Healthcare sector analysis reveals significant shifts compared to previous years. Insiders deliberately causing breaches have surged back into second place after a steady decline since 2018. Interestingly, Personal data has eclipsed Medical data as the preferred target for threat actors.

Their condition is rapidly evolving.

We certainly didn't require X-rays to diagnose the changes in the Healthcare industry this year. There are a wealth of differences from last year to this year, so let's dive in and take a look. There has been a trend of decreasing malicious insider threats in the Healthcare sector since 2018 (Figure 62). However, we saw that trend beginning to reverse itself to some degree last year. It has continued to make up lost ground and now holds the second-place spot this year. This is even more worthy of mention when you consider Privilege Misuse wasn't even in the top three last year.

As a result, the Internal actor has taken back the driver's seat in this industry. Whether wreaking malevolent mischief in terms of Privilege Misuse or simply making a hefty dose of innocent mistakes, resulting in the Miscellaneous Errors pattern taking the top spot in this year's rankings, insiders are making quite the comeback in this sector. Not unlike almost every other industry on which we report, the error that appears to be the most beloved is Misdelivery (sending information to the wrong recipient, whether by electronic or physical means) (Figure 63). Loss is in second place and primarily consists of the misplacement of paper documents, which is bad for the organization and the environment. Lastly, we have Gaffe (a DBIR team favorite), which is when people simply blurt out sensitive data in the hearing of others.

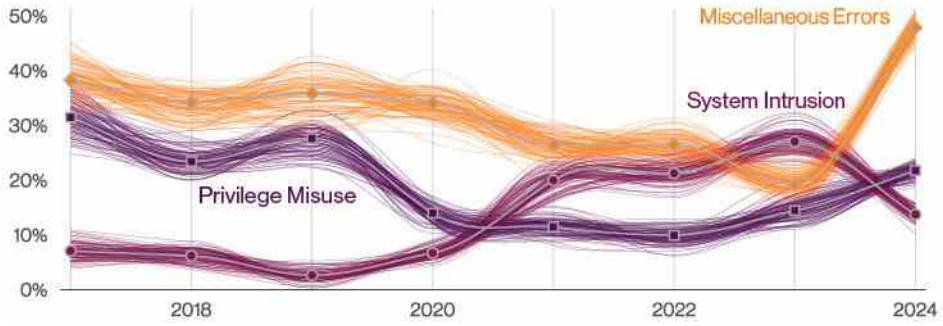


Figure 62. Top patterns in Healthcare industry breaches

Finally, a point of particular interest to the team was that Medical data, usually the most commonly stolen data type in this sector, doesn't even get a passing nod (Figure 64). It seems that Personal data is the flavor of the year for threat actors, and they don't really care about Aunt Bertha's bunions.

Figure 63. Top Error varieties in Healthcare industry breaches (n=568)

Figure 64. Top Attribute varieties in Healthcare industry breaches (n=1,102)

Information NAICS 51

Frequency	1,367 incidents, 602 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 79% of breaches
Threat actors	External (79%), Internal (21%), Multiple (1%) (breaches)
Actor motives	Financial (87%), Espionage (14%) (breaches)
Data compromised	Other (46%), Personal (45%), Credentials (27%), Internal (22%) (breaches)
What is the same?	The top three attack patterns remain constant since last year, and their ranked order has also not changed. The team found this somewhat interesting considering how many more breaches we had in this sector as compared to last year.

Summary

The overall breach sample size increased compared to last year, but this sector experienced substantially fewer incidents. Ransomware and Use of stolen credentials continue to dominate the System Intrusion pattern, while there was a slight decrease in Phishing attacks alongside a rise in Pretexting within the Social Engineering pattern. There was a mild increase in Espionage motives and state-sponsored actors targeting the industry, emphasizing the need for enhanced detective controls.

As we have mentioned elsewhere in this report, our overall breach sample size was greater than last year. However, the Information sector showed 741 fewer incidents this year. It did boast a much higher number of breaches. The top patterns for this vertical remain the same, and so does their order (Figure 65).

Ransomware and the Use of stolen creds (a combination that makes up much of the System Intrusion pattern) remain in the top action varieties as one might expect. With regard to breaches in the Social Engineering pattern, we saw a slight dip in Phishing attacks along with a corresponding rise in Pretexting. This could be one indicator that the threat actors are being forced to deploy more sophisticated techniques against their targets.

This year, EMEA dominates the dataset in this sector in particular, with 243 confirmed Information industry breaches as opposed to just 97 in Northern America. These incidents have been contributed by some of our new law enforcement and regulatory bodies in the region. This is what robust data protection regulation looks like.

Finally, we did see a mild increase in the Espionage motive (14% this year as opposed to 8% in the 2023 report). We also saw a combined increase of the Nation-state/State-affiliated actors from 12% last year to 15% in this sector currently. While this is not a statistically significant finding, it is never good news to find that your industry is increasingly being targeted by more sophisticated threat actors (even if only slightly). Nevertheless, it serves as a reminder to ensure that you have detective controls in place to give you an early warning if you become a target.

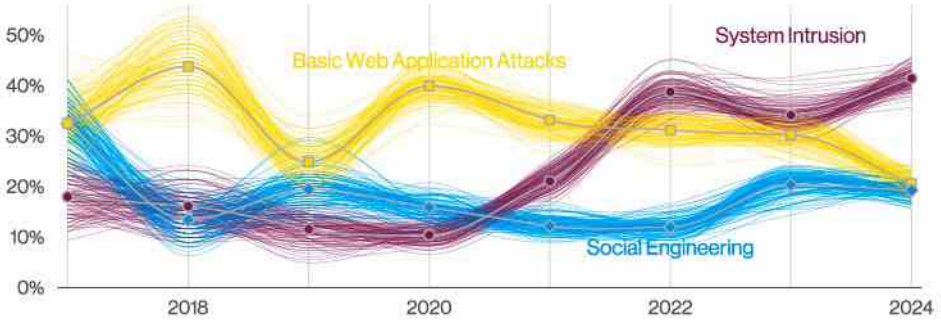


Figure 65. Top patterns in Information industry breaches

Manufacturing NAICS 31–33

Frequency	2,305 incidents, 849 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Miscellaneous Errors represent 83% of breaches
Threat actors	External (73%), Internal (27%) (breaches)
Actor motives	Financial (97%), Espionage (3%) (breaches)
Data compromised	Personal (58%), Other (40%), Credentials (28%), Internal (25%) (breaches)
What is the same?	Two of the top patterns from last year are still in place. Financial motivation continues to be the driver behind most attacks.

Summary

Manufacturing has seen an increase in Error-related breaches. The installation of malware after hacking via the Use of stolen credentials is somewhat commonplace.

This year's model

This year's Manufacturing model comes with a new and improved feature: Errors! As in most other industries, Misdelivery is the error du jour, accounting for almost half (48%) of error-related breaches. As we have mentioned elsewhere, this is in part the result of contributor bias, but nevertheless, sending things to the incorrect recipient does appear to be somewhat widespread regardless of vertical. Loss and Misconfiguration round out the top three error varieties, and they account for approximately 20% and 18% of breaches, respectively.

System Intrusion continues to hold on to the top spot in Manufacturing. This is probably related to the still very effective combination of hacking via Use of stolen credentials (present in 25% of manufacturing breaches) to gain access to the environment and then the liberal application of Ransomware (involved in 35% of breaches in this vertical). It's hard to keep the gadgets rolling off the assembly line when your data is locked up tight and someone else holds the keys.

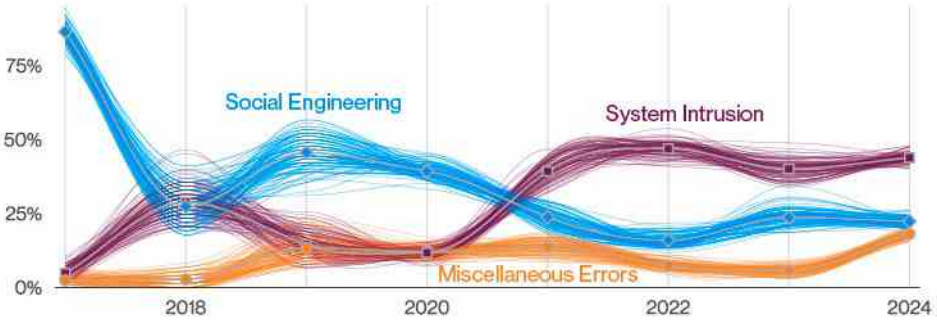


Figure 66. Top patterns over time in Manufacturing industry breaches

It's your asset on the (manu-facturing) line.

Social Engineering remains steady with regard to breaches in this vertical due to action varieties such as Phishing (55%) and Pretexting (42%). Apparently, consumer feedback branded the Basic Web Application Attacks pattern as so 2022, and it now languishes near the bottom of the pattern rankings with the likes of Privilege Misuse. In fact, the asset of Server–Web app has been on a slightly downward trajectory. Figure 67 illustrates this decline and also shows the corresponding rise of Server–Mail. This makes sense when, as mentioned above, one considers that Phishing remains prevalent in the Manufacturing vertical. Of course, the credentials typically obtained via phishing are those that afford the criminal a foothold into the organization via the email account of the victim.

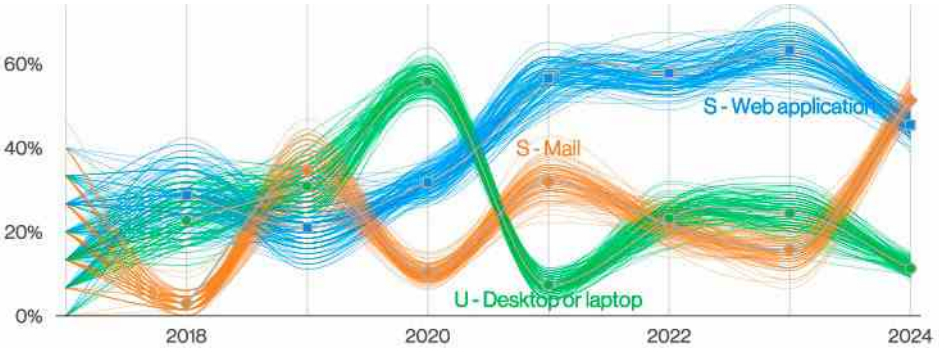


Figure 67. Top Asset varieties over time in Manufacturing industry breaches

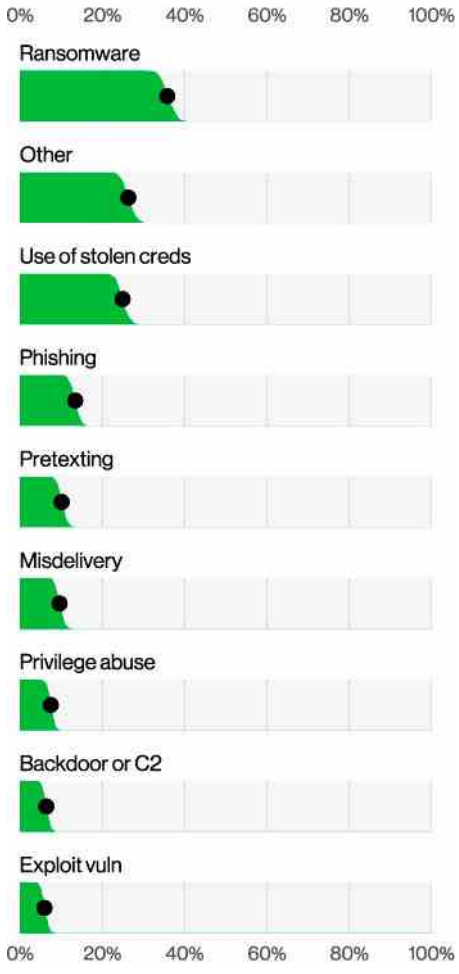


Figure 68. Top Action varieties in Manufacturing industry breaches

Professional, Scientific and Technical Services NAICS 54

Frequency	2,599 incidents, 1,314 with confirmed data disclosure
Top patterns	Social Engineering, System Intrusion and Miscellaneous Errors represent 85% of breaches
Threat actors	External (75%), Internal (25%) (breaches)
Actor motives	Financial (95%), Espionage (6%) (breaches)
Data compromised	Personal (40%), Credentials (38%), Other (33%), Internal (23%) (breaches)
What is the same?	Personal data and Credentials are still the top types of data impacted in this industry.

Summary

Social Engineering is one of the top threats facing this industry, accounting for 40% of breaches, and 20% of breaches are the result of Pretexting. In addition, there has been an increase in errors, specifically Misdelivery.

Casting wide nets

While the use of NAICS codes is helpful, we realize that they are not always the ideal way of creating peer groups. That is particularly the case with this industry, as the wide net it casts includes diverse organizations such as interior designers and nanotech companies. This industry does illustrate the types of breaches that affect most industries, whether they were intentional or accidental. Let's take a look at the breakdown. Like many industries, we see Social Engineering and System Intrusion in the top patterns, although there's also the inclusion of Miscellaneous Errors as seen in Figure 69.

When it comes to intentional breaches, the vast majority of those cases fall into two buckets: Ransomware and the BEC, at 24% and 20% respectively. This isn't the first time that we've seen Ransomware in the top three, but it is one of the first times that we've seen such headway with Pretexting attacks. These have increased significantly from last year and now account for 40% of breaches. Lastly, organizations need to continue to protect the keys to the kingdom, with Credentials showing up in 34% of the breaches.

Although these credentials provide an important beachhead for criminals, we simply can't forget the unintentional (or rarely intentional) insider. Even though 25% of breaches involved someone coming in from within the organization, the majority of them are Misdeliveries (12%), while only a handful involve individuals abusing their position (5%). This helps us remember that there are many more folks who are maladroit than malicious.

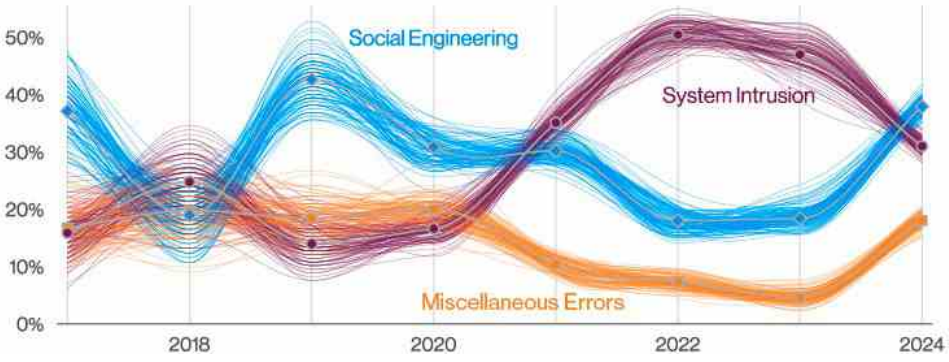


Figure 69. Top patterns over time in Professional, Scientific and Technical Services industry breaches

Public Administration NAICS 92

Frequency	12,217 incidents, 1,085 with confirmed data disclosure
Top patterns	Miscellaneous Errors, System Intrusion and Social Engineering represent 78% of breaches
Threat actors	Internal (59%), External (41%) (breaches)
Actor motives	Financial (71%), Espionage (29%) (breaches)
Data compromised	Personal (72%), Internal (37%), Other (31%), Credentials (17%) (breaches)
What is the same?	System Intrusion and Social Engineering remain top attack patterns in this sector.

Summary

Miscellaneous Errors, particularly Misdelivery, have surged to the top spot in this industry, reflecting the commonality of mistakes leading to breaches. System Intrusion now ranks second, followed by Social Engineering. The predominance of internal actors underscores the potential consequences of employee carelessness, with Errors accounting for the majority of breaches.

Owning up to your mistakes in public

Due to some of our new data contributors reporting on mandatory breach disclosures, there was an ascendency of the Miscellaneous Errors attack pattern to the top spot in this industry (Figure 70).[96] The most common error in Public Administration was Misdelivery, where information (in whatever form) is delivered to the wrong recipient. While this happens frequently via email, it is also quite common with printed documents and, strangely, faxes. The Lost and Stolen Assets pattern (in second place last year) is no longer among the top three in spite of a rather impressive showing by Loss.

Actions speak louder than campaign promises.

Just as we see in the other verticals, System Intrusion and Social Engineering incidents remain commonplace and account for the next two patterns in this industry, respectively. While hacking only appeared in 31% of Public Sector breaches, it is clear that threat actors are still voting for the Use of stolen creds, which were involved in 83% of hacking-related breaches, mostly against web applications.

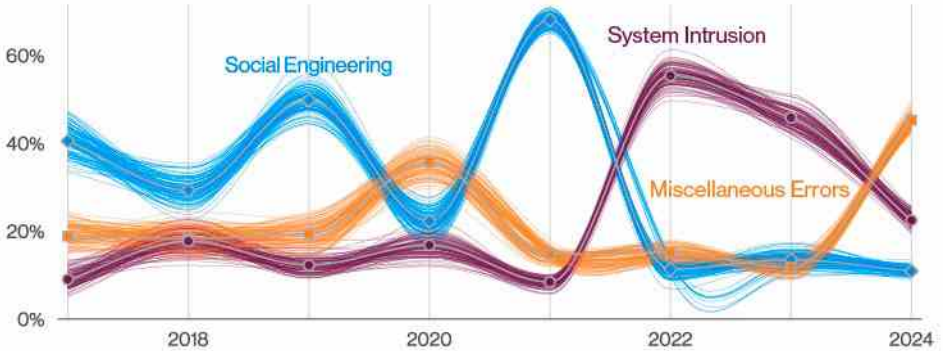


Figure 70. Top patterns over time in Public Administration industry breaches

96 We discuss in the "Results and analysis – Actors" section how mandatory breach reporting helps everyone understand the truer prevalence of breach causes.

Malware figured in 27% of Public Sector breaches this year. Not unlike many other verticals, Ransomware was top of the heap with regard to malware varieties and accounted for 61% of malware-related breaches. Backdoors appeared in 38% of breaches involving malware, after which we saw a tight pack of several varieties jockeying for the third-place spot as illustrated in Figure 71.

The Social Engineering attacks we saw in Public Administration were mostly garden-variety Phishing (66% of breaches) and Pretexting (23%) attacks. No less concerning, but not really noteworthy in relation to the other findings.

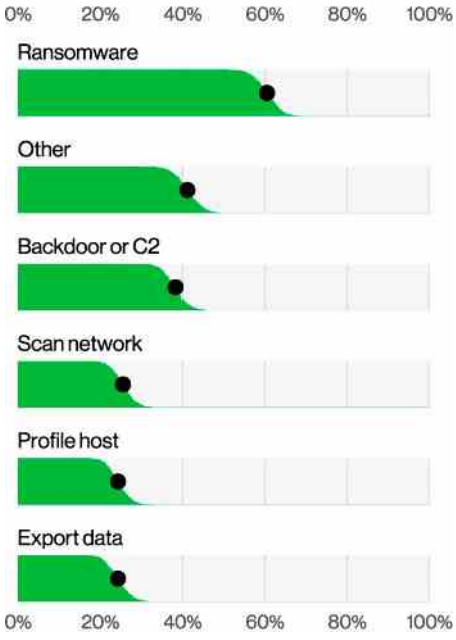


Figure 71. Top Malware varieties in Public Administration industry breaches (n=243)

Actors behaving badly

The fact that Internal actors are the top threat this year underlines the fact that even the most well-meaning employees can trigger a data breach simply by being careless. For all actors, Error actions accounted for 51% of the cases, while malicious internal actors only accounted for 8%. Figure 72 is an illustration of how the road to breaches is paved with good intentions.

If we set aside the error-related breaches and the End-users who cause them, the most common external actors in this vertical were Organized crime (largely Ransomware attacks) at 67% and State-affiliated actors (29%) (Figure 73). And while we saw very little change in Espionage threat actors, we did see a slight uptick in financially motivated attacks.

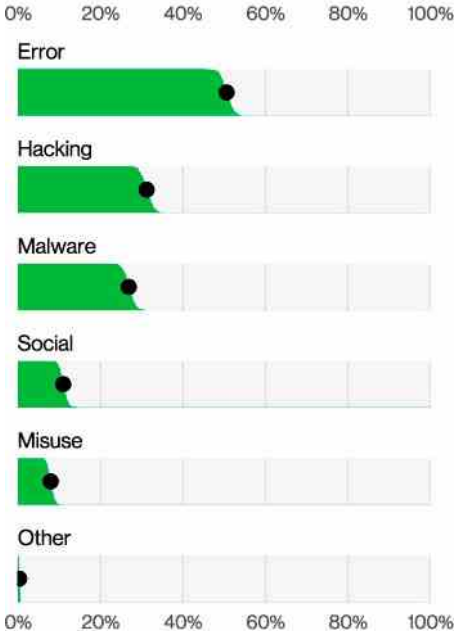


Figure 72. Top Actions in Public Administration industry breaches (n=1,088)

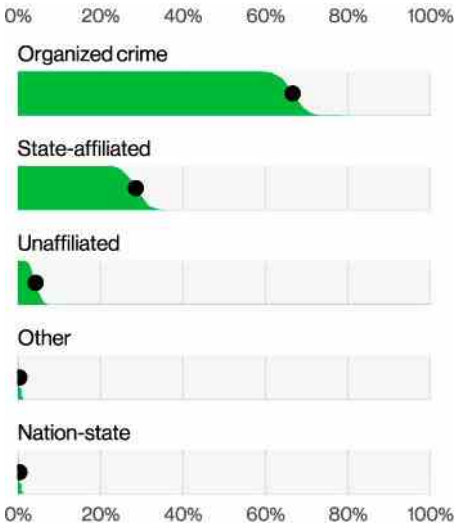


Figure 73. Top External actor varieties in Public Administration industry breaches (n=305)

Retail NAICS 44–45

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

Summary

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

The Retail sector is where we often find "Magecart" threat actors. They are particularly skilled at inserting malicious code into the e-commerce sites of retail entities to siphon off (usually) Payment card information. We saw roughly the same percentage of these kinds of attacks this year as we did last year (Figure 74). However, the type of data being compromised showed a surprising change.

With Credentials standing at 38% (very close to last year's 35%) we didn't expect to see Payment card data drop to 25% (from 37%). Now, we understand how attractive and useful Credentials are to your average threat actor, but we were stunned to see Payment card data, so useful for immediate fraud, drop so precipitously (Figure 75). As we have indicated before, we get the "what" of the changes in the data, but we do not always get the "why." Is this a result of increased controls around the monetization of payment card data, making it harder for the criminals to use the data they have stolen? Or is it just that credentials are so much easier to steal? Either way, we will be interested to see if this is just a blip on the radar or an actual trend starting.

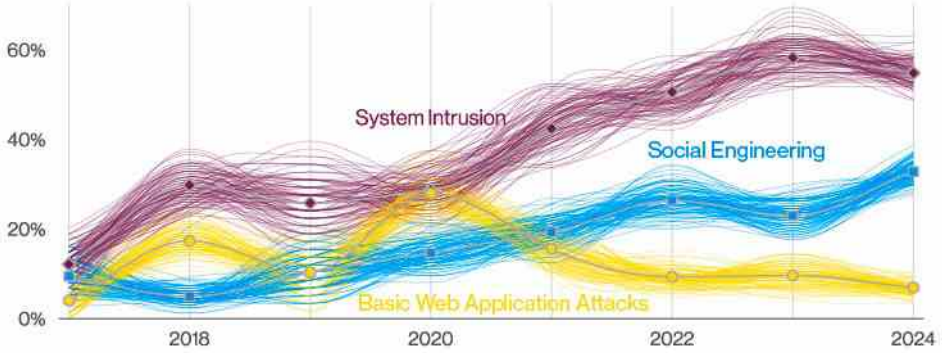


Figure 74. Top patterns over time in Retail industry breaches

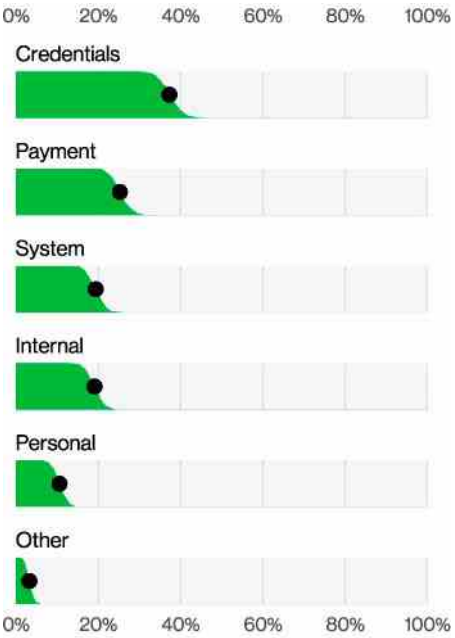


Figure 75. Top Confidentiality data varieties in Retail industry breaches (n=341)

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

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

5
Regions

Regional analysis

In this section, we once again examine cybercrime from a macro-regional point of view. We do this in the hope that it will be a quick and easy way for readers to learn how cybercrime trends differ and how they remain consistent from one geographical region of the world to the next. As always, our visibility into a given area is determined by many variables, including regional disclosure laws, our own dataset and where our data contributors conduct business. If you feel that your own patch of ground is not featured adequately in the following pages, please contact us about becoming a data contributor and motivate other organizations in your area to do the same. Please keep in mind that even if your region is not represented here, it doesn't mean we have no visibility into the region but rather that we don't have a sufficient number of incidents in that area to provide a statistically significant section.

We define the regions of the world in accordance with the United Nations M49[97] standards, which combine the super-region and sub-region of a country together. By so doing, the regions we will examine are as follows:

APAC: Asia and the 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)

NA: Northern America (021), which primarily consists of breaches in the United States and Canada

Many readers may recognize the At-a-glance tables that we place at the top of each major section. We have combined them to provide a quick look at how each of the regions compares to the others with regard to the frequency of incidents, top patterns and so on.

Region	Frequency	Top patterns	Threat actors	Actor motives	Data compromised
APAC	2,130 incidents, 523 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 95% of breaches	External (98%), Internal (2%) (breaches)	Financial (75%), Espionage (25%) (breaches)	Credentials (69%), Internal (37%), Secrets (24%), Other (17%) (breaches)
EMEA	8,302 incidents, 6,005 with confirmed data disclosure	Miscellaneous Errors, System Intrusion and Social Engineering represent 87% of breaches	External (51%), Internal (49%) (breaches)	Financial (94%), Espionage (6%) (breaches)	Personal (64%), Other (36%), Internal (33%), Credentials (20%) (breaches)
NA	16,619 incidents, 1,877 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 91% of breaches	External (93%), Internal (8%) (breaches)	Financial (97%), Espionage (4%) (breaches)	Personal (50%), Credentials (26%), Internal (19%), Other (16%) (breaches)

Table 3. At a glance for regions

97 https://unstats.un.org/unsd/methodology/m49

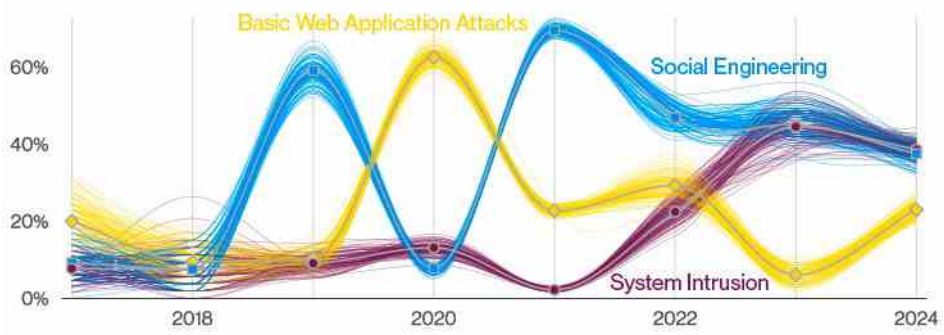


Figure 76. Top patterns over time in APAC breaches

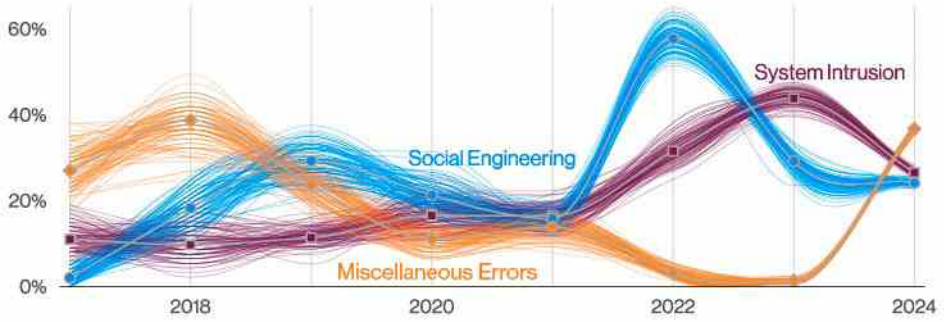


Figure 77. Top patterns over time in EMEA breaches

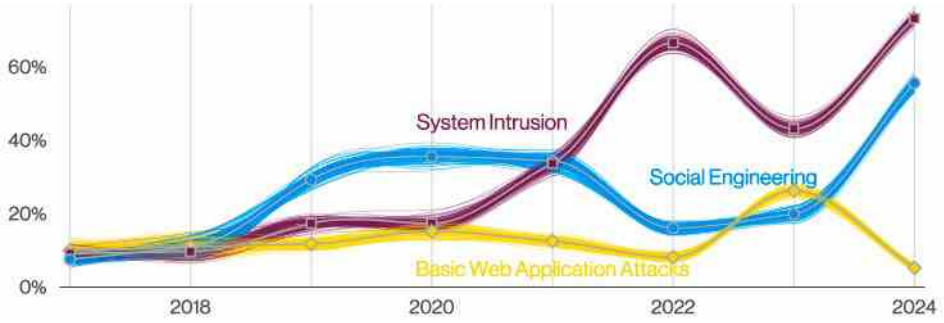


Figure 78. Top patterns over time in NA breaches

Around the world in 4 paragraphs

This year we were fortunate enough to have new contributors from EMEA join us. Due to the nature of contributing agencies along with the reporting requirements in that region, we have seen a substantial rise in the Miscellaneous Errors pattern. So much so that it is now the top pattern for the EMEA region. Any time we have a new contributor dataset that is larger in nature or has a propensity to report on specific types of actions (in this case, errors) we observe the resultant skewing of the data that one might expect. Perhaps next year we will be better positioned to determine if this jump in Miscellaneous Errors will continue or level out to be more consistent with the other patterns.

If we set aside the Error-heavy datasets and take a look at the regions through this lens, we can see that the System Intrusion pattern remains among the top for all regions. As always, the two main action types that we see represented in the System Intrusion pattern are hacking via the Use of stolen credentials and malware (most often) in the form of Ransomware. The "sans error" dataset also illustrates that the System Intrusion pattern has neither risen nor fallen significantly from last year but has instead held a relatively straight trajectory.[98]

Social Engineering, on the other hand, has increased somewhat significantly from 29% to 45% when viewed across the whole dataset (mostly driven by Northern America, where it represents 56% of breaches). Extortion was the greatest driver of this growth in NA as it was present in 46% of its breaches. Our other Social Engineering favorites had a more timid showing in Northern America breaches: 13% for Phishing and 4% for Pretexting.

98 Unlike interest rates

With regard to actors, the majority of cybercrime continues to be carried out by financially motivated external parties. One notable exception is that of APAC, where instead of more than 90% of attacks being financially motivated, we see that the Espionage motive is greater than it is elsewhere and accounts for 25% of breaches (as opposed to between 4% and 6% in the other regions). As a result, the data variety of Internal accounts for 37%, while Secrets is at 24% for APAC. These data types typically do not appear in the top three spots for the other regions. Meanwhile, Credentials make up a whopping 69% of compromised data in APAC. As we mentioned in the 2023 DBIR, while we frequently have visibility into what data types are stolen, we do not always know the details to explain precisely why. We do know that regulatory requirements differ from one region to the next and, consequently, this may make some types of data harder to get than others. However, it is clear that Credentials and Personal data figure prominently in cybercrime regardless of where you are located.

From the Cyber Security Agency of Singapore

Building a trusted and resilient cyberspace requires collective effort and partnership from both governments and the industry. Neither of us can do this by ourselves; we share the responsibility of securing cyberspace for all users. Forging strong public-private partnerships is necessary for strengthening cybersecurity on multiple fronts. This can include threat intelligence sharing to enhance visibility, conducting joint operations to combat sophisticated cyber threats, or jointly investing in the development of much needed capabilities.

This is why the Cyber Security Agency of Singapore (CSA) is committed towards developing deep partnerships with the industry. CSA has various Memoranda of Understanding with important industry partners that helps us to tackle cybersecurity issues of the day together. These memoranda allow us to take on collaborative efforts, including the detection of global malicious cyber or information campaigns, and joint development of mobile security measures to ensure that Singapore's users are protected from common instances of malware. For example, CSA partnered with Google to pilot a new enhanced protection feature within Google Play Protect to further safeguard Android mobile users against malware-enabled scams. This enhanced protection feature will analyze and automatically block the installation of apps from Internet sideloaded sources—browsers, messaging apps and file managers—that declare their intent to use sensitive permissions that are frequently used for financial fraud and scams.

These collaborations also extend towards policy areas. This year, CSA updated Singapore's cybersecurity legislation. This update was done in consultation with industry partners and other stakeholders to understand emerging challenges in cyberspace and seek their views on how to ensure Singapore's regulatory approach meets our policy intent, but is practical and commensurate to the cybersecurity risks represented by different essential service sectors and types of digital infrastructure or service.

CSA strongly believes that the industry has a crucial part to play in our collective cybersecurity, and can start by securing their products and services by design and default. This is especially important for the most vulnerable groups in society. This is why CSA has developed a "Safe App Standard" to help app developers and providers enhance the security of their mobile apps. We encourage DBIR readers to access these guidelines and more at CSA's website.[99]

CSA looks forward to deepening our partnership with industry to further improve the security of our cyberspace.

99 https://www.csa.gov.sg

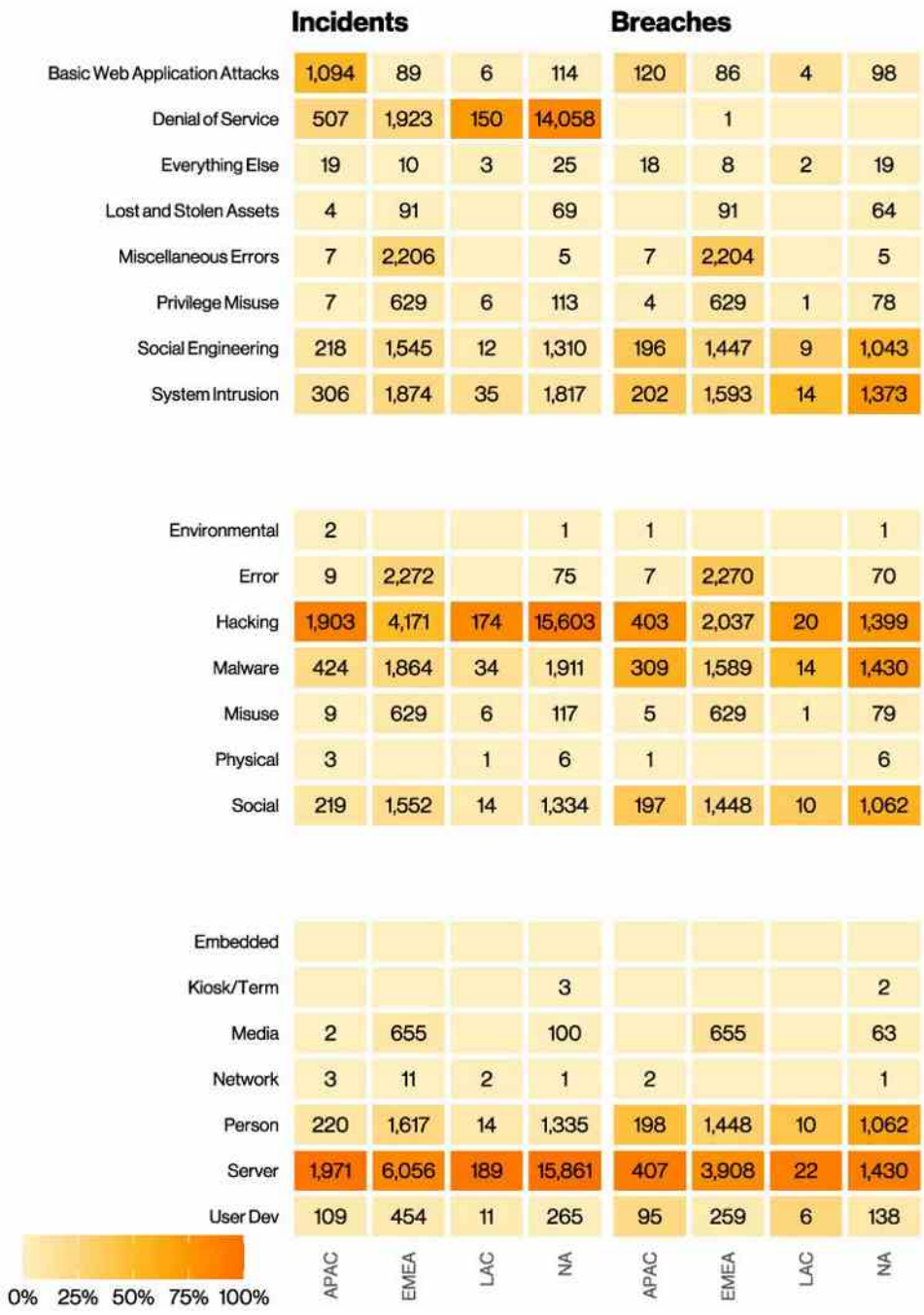
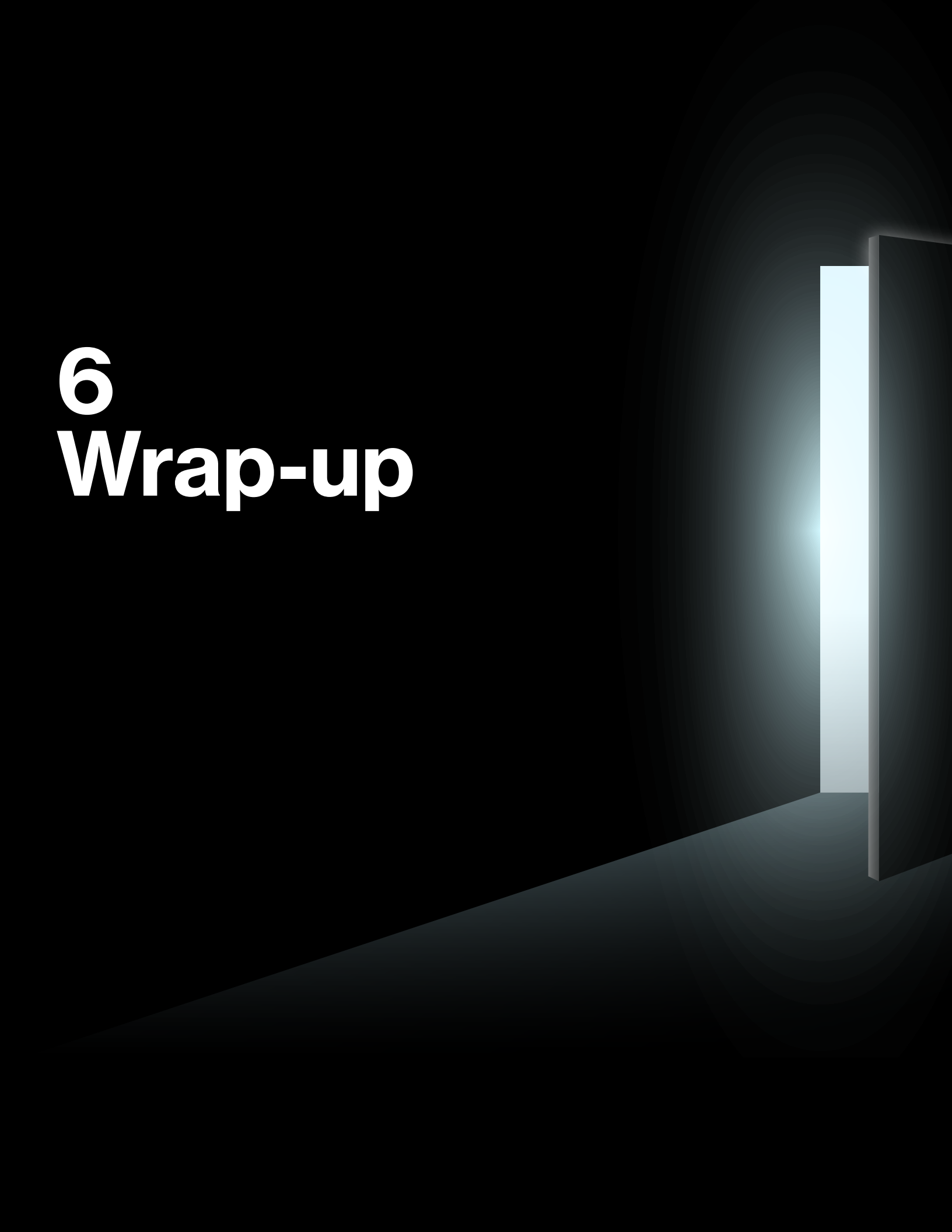


Figure 79. Incidents and breaches by region

We now draw your attention to the heatmap that is Figure 79. While it may not be as captivating to look at as the Mona Lisa, it is more useful, for enterprises at least. This map illustrates how different (or similar) attacks are based on geography (sort of like the At-a-glance section, but with much more detail). The heatmap shows incidents and breaches broken down into the following: top patterns, top action types and top asset varieties. This is a very handy tool to help you locate potential problem areas in your region.

Hopefully you will find this (especially when combined with other data found in this report, such as industry and organization size) informative with regard to what your organization might be more prone to in terms of attacks and can therefore assist you in creating your defense strategy.

6
Wrap-up



This concludes our regularly scheduled programming. We hope you have found the information in this document helpful, actionable and enjoyable.

Once again the DBIR has shown us that while life is, in many ways, unpredictable, being as prepared as possible for all eventualities is the safest course. It is our hope that this document has gone at least some way toward helping you anticipate what threats are most likely to affect your organization and deploy your resources appropriately. We would like to express our sincere appreciation to our data contributors, without whom we could not make this report happen. And of course we thank you, our readers, for continuing to take the time to read this report, making helpful suggestions and greatly assisting us in the improvement of this report each year.

The DBIR team wishes you all a safe and prosperous year, and we look forward to seeing you again in 2025.

Year in review

Monthly snapshot as reported by the VTRAC Monthly Intelligence Briefings. If you'd like to learn more, feel free to reach out to the VTRAC team at Intel.Briefing@verizon.com.

January

The VTRAC's cyber intelligence collections in January reflected most of the recurring information security (InfoSec) risk issues we would observe through the rest of 2023. Ransomware continued to plague every sector. For example, the LockBit threat actors (TAs) attacked the Royal Mail on January 11, disrupting postal operations for more than six weeks. Atlantic General Hospital in Berlin, Maryland, was among the first healthcare organizations struck with ransomware. Vulnerabilities in FortiOS secure sockets layer (SSL) VPN products were exploited by Chinese APT actors attacking government networks and an African managed service provider. Russian advanced persistent threat (APT) actors continued to attack Ukraine. COLDRIVER attempted to breach Brookhaven, Argonne and Lawrence Livermore National Laboratories using spear phishing and fake login pages. Noteworthy zero-day vulnerabilities that were exploited before patch availability were CVE-2023-21674, a Windows advanced local procedure call (ALPC) elevation of privilege vulnerability, and CVE-2023-22952, a remote code execution vulnerability in SugarCRM's email templates. Month's end brought news of a multinational operation to disrupt the Hive ransomware TA that began in July 2022 and had provided decryption keys to more than 1,000 victims.

February

A preauthentication command injection vulnerability in Fortra's GoAnywhere MFT (managed file transfer) solution, labeled CVE-2023-0669, was a zero-day vulnerability that came to light in the first week of the month. Within days, we learned of a GoAnywhere MFT-related breach of more than 1 million patient records from the Community Health System. The Cl0p ransomware gang exploited GoAnywhere to steal data from more than a hundred companies beginning on January 18. The vulnerability was exploited in data breaches for several months only to be supplanted in June by a new zero-day vulnerability in another managed file transfer solution, Progress Software's MOVEit. Microsoft's Patch Tuesday included patches for three zero-day vulnerabilities and Apple also patched a zero-day in WebKit. North Korean APT, the Lazarus Group, conducted the No Pineapple! campaign to exfiltrate more than 100 GB of data from organizations in medical research, healthcare, chemical engineering, energy and defense as well as a leading research university. The city of Oakland, California, declared a state of emergency following a ransomware infection that disrupted most city services. Both the Play and LockBit TA claimed credit.

March

3CX is a Voice over Internet Protocol (VoIP) private branch exchange (PBX) software development company whose 3CX Phone System is used by more than 350,000 customers worldwide and has more than 12 million daily users. A digitally signed and trojanized version of the 3CX VoIP desktop client was used to target the company's customers in an ongoing supply chain attack. Attributed to the Lazarus Group, the ultimate payload was a backdoor Trojan, Gopuram. The attackers used Gopuram with surgical precision. Gopuram was installed on fewer than 10 targets, all of which were cryptocurrency companies. The 3CX campaign demonstrated significantly more sophisticated capabilities from North Korean APT actors. And near the end of the month, a new North Korean APT emerged, APT43. Initial reports indicated that APT43 used cybercrime to fund its cyberespionage campaigns. Winter Vivern, the APT aligned with the national security interests of Russia/Belarus, was using malicious documents to collect credentials and exploit vulnerable Zimbra collaboration servers. Winter Vivern targeted government, military and diplomatic entities in nations supporting Ukraine. March's zero-day vulnerabilities included Outlook, Microsoft Defender SmartScreen and Adobe ColdFusion to keep patch management teams busy.

April

The month began with the exploitation of two zero-day vulnerabilities in Apple products. Google mitigated a zero-day in its Chrome browser's V8 JavaScript engine and then four days later rolled out a new version to mitigate a zero-day vulnerability in the Skia graphics engine. And Microsoft patched the second zero-day this year in its Common Log File System driver. Another zero-day vulnerability, CVE-2022-27926, affected Zimbra collaboration servers. The Winter Vivern APT actor had almost certainly discovered and exploited the vulnerability before the patch was announced. CERT Polska warned that the Russian APT29 was actively pursuing diplomatic targets in many nations, principally North Atlantic Treaty Organization (NATO) members. APT28 attacked vulnerable Cisco routers worldwide. The TTP of exploiting a 4-year-old vulnerability in network infrastructure was at once innovative and sufficiently simple to be adopted and adapted by many TAs. The GRU's Sandworm Team continued to focus on support of the Russian invasion of Ukraine. Multiple top-tier cybercrime actors continued to compromise PaperCut and Fortra GoAnywhere MFT systems to install Cl0p, LockBit and BlackCat/ALPHV ransomware and frequently exfiltrated data from victim networks. Microsoft noted an increase in the pace and the scope of cyberattacks attributed to Iranian threat actors. For example, Mint Sandstorm (Charming Kitten) rapidly weaponized N-day vulnerabilities in common enterprise applications and conducted highly targeted phishing campaigns to quickly and successfully access environments of interest. The Mint Sandstorm APT began exploiting CVE-2022-47966 in Zoho ManageEngine on January 19, 2023, the same day the proof of concept (PoC) became public.

May

A Chinese state-sponsored APT group dubbed Camaro Dragon was found infecting TP-Link routers with a malicious firmware implant that allowed attackers to gain full control of infected devices and access compromised networks while evading detection. The group overlaps with activity previously attributed to Mustang Panda. Mustang Panda was also observed conducting phishing campaigns against European entities. Other phishing emails delivered fake "official" Ukrainian government reports that downloaded malware onto compromised machines. Mustang Panda's most used malicious implant was a Trojan program called PlugX, and it continued to remain the group's preferred spying tool. A new Chinese aligned APT actor, Volt Typhoon was identified after it had been found targeting critical infrastructure organizations in Guam and elsewhere in the United States since mid-2021. Barracuda identified a zero-day vulnerability (CVE-2023-2868) in its Email Security Gateway (ESG) appliance on May 19. A security patch to eliminate the vulnerability was applied to all ESG appliances worldwide on May 20. Microsoft Patch Tuesday included two zero-day vulnerabilities. Apple released security advisories and patches mitigating more than 30 vulnerabilities, including three zero-day exploits affecting WebKit. On May 31, Progress Software released patches for a SQL injection vulnerability in MOVEit managed file transfer software. Labeled CVE-2023-34362, we later learned exploitation began on May 27.

June

MOVEit moved into the mainstream. VTRAC began receiving a large number of victim reports—and we were still getting them as this went to press in February 2024. (MOVEit would continue to wreak havoc throughout the year, with multiple cybersecurity experts reporting increasing numbers of organizations and individuals affected.)[100,101,102,103] There were indications the Cl0p ransomware TA had been testing MOVEit exploits in 2021. At least 1,000 organizations became victims, and personally identifiable information (PII) of at least 100 million individuals was compromised. The Russian APT Gamaredon Group attacked Ukraine featuring a PowerShell-based information stealer distributed on malicious USB thumb drives. Google released a new version of its Chrome browser to mitigate a vulnerability in the V8 JavaScript engine that was already being exploited in the wild. A zero-day vulnerability in Fortinet's FortiOS and FortiProxy SSL-VPN preauthentication was being exploited in the wild. After May's alert for CVE-2023-2868, on June 6, Barracuda announced any ESG appliance that had been compromised must be taken out of service and disposed of; patching was insufficient. Kaspersky's security architecture detected suspicious activity originating from several iOS-based phones. It discovered a targeted APT campaign that it labeled Operation Triangulation. The target iOS device received a zero-click message via the iMessage service with an attachment containing an exploit. With no user interaction, the message triggered a vulnerability that led to code execution. After installation of the APT payload, the message was deleted. On June 21, Apple patched the Operation Triangulation zero-day vulnerabilities in the iOS kernel and in WebKit.

100 July: https://techcrunch.com/2023/07/27/us-government-contractor-says-moveit-hackers-accessed-health-data-of-at-least-8-million-individuals

101 August: https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers

102 November: https://www.cpomagazine.com/cyber-security/more-fallout-from-moveit-data-breach-documented-632000-emails-from-us-departments-of-defense-and-justice-accessed-by-russian-hackers

103 December: https://www.techradar.com/pro/security/the-moveit-breach-may-well-have-been-the-biggest-cyberattack-of-the-year

July

The top three ransomware TAs had a very good July. That is, InfoSec practitioners spent July avoiding successful attacks by LockBit, Cl0p and ALPHV. On Monday, July 4, the port of Nagoya, Japan, was struck by LockBit 3.0. Cl0p continued to take advantage of more than 130 organizations they had breached in May and June before MOVEit was patched. ALPHV (BlackCat) used search engine optimization (SEO) poisoning and malvertisements to lure users into downloading a trojanized WinSCP (Windows Secure Copy Protocol), leading to lateral exploitation, data theft and ransomware infection. A Chinese APT labeled Storm-0558 acquired a Microsoft account (MSA) consumer key from a Microsoft engineer's system using an arcane series of loopholes. That key enabled the group to access Outlook and Outlook Web Access (OWA) accounts affecting about 25 organizations, including government agencies. Five zero-day vulnerabilities were mitigated on Microsoft Patch Tuesday. Zimbra Collaboration Suite contained a cross-site scripting zero-day vulnerability affecting the confidentiality and integrity of data. Adobe released an update to ColdFusion on Patch Tuesday. Three days later, Adobe released an out-of-cycle security bulletin for a deserialization zero-day vulnerability in ColdFusion. Two new zero-day vulnerabilities in Ivanti Endpoint Manager Mobile were exploited to breach the IT systems of a dozen ministries in Norway. Citrix released an advisory and patches for three vulnerabilities in NetScaler (formerly Citrix) application delivery controller (ADC) and NetScaler Gateway. CISA advised that one NetScaler vulnerability had been exploited to breach the network of a U.S. critical infrastructure organization in June. On August 2, we learned that 640 NetScaler servers had been backdoored by an unidentified TA and a China Chopper web shell installed.

August

Multiple sources reported a decline in ransomware attacks in the range of 20%–33%. An ongoing espionage campaign targeting dozens of organizations in Taiwan was discovered. Researchers attributed the activity to a new Chinese APT group labeled Flax Typhoon. The threat group minimizes the use of custom malware and instead uses legitimate tools found in victims' operating systems to conduct its espionage operations (living off the land). VTRAC collected intelligence for another new APT, labeled Carderbee. That TA mounted a supply chain attack weaponizing updates from a Chinese security company to install a code-signed version of the PlugX backdoor to attack about 100 computers, mostly in Hong Kong. The North Korean Lazarus Group fielded new remote access trojans (RATs), QuiteRAT and CollectionRAT, and there were indications that the Lazarus Group was also shifting to "living off the land" TTP. The FBI announced a global operation against the Qbot (aka Qakbot). In Operation Duck Hunt, the FBI seized control of the botnet, removed the malware from infected devices and identified a substantial number of affected systems. As with many malware takedowns, the core cybercriminals were not arrested or confined, and Qbot would begin a comeback in December. Microsoft Patch Tuesday included mitigation of two exploited zero-day vulnerabilities: CVE-2023-38180 (patched) and CVE-2023-36884 (not patched).

September

Caesars Entertainment discovered on September 7 that the ALPHV ransomware TA had performed a social engineering attack that targeted an outsourced IT support vendor resulting in a breach of Caesars' network and its loyalty program database, which stores driver's license numbers and Social Security numbers for many customers. Caesars chose to pay roughly half of the $30 million ransom to recover its data. On September 11, MGM Resorts International disclosed the ALPHV ransomware TA had breached MGM's network using social engineering, then stole sensitive data and encrypted more than a hundred ESXi hypervisors. MGM informed the SEC that the cyberattack cost the company $100 million. Akira ransomware threat actors were targeting Cisco VPNs that were not configured for MFA to infiltrate organizations. Cisco released an advisory for vulnerability in the remote access VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) that could allow an unauthenticated, remote attacker to conduct a brute force attack in an attempt to identify valid username and password combinations. In August, Cisco became aware of attempted exploitation of this vulnerability in the wild. The University of Toronto's Citizen Lab reported that iOS zero-day vulnerabilities were exploited to install NSO Group's Pegasus commercial spyware. Microsoft Patch Tuesday included two zero-day vulnerabilities. The WebP Codec is used in countless applications and websites, and it had a zero-day vulnerability with attacks reported by Apple and Google. Adobe released an out-of-cycle advisory and patch to mitigate a zero-day remote code execution vulnerability in Adobe Acrobat and Reader.

October

In an advisory sent to an undisclosed number of customers on October 19, Okta said it had "identified adversarial activity that leveraged access to a stolen credential to access Okta's support case management system." An Okta spokesperson said the company notified about 1% of its customer base (~170 customers), including 1Password and Cloudflare. On October 7, Hamas invaded Israel, triggering significant unrest. Within an hour, the Russian-affiliated group Anonymous Sudan claimed responsibility for potentially disabling an Israeli civilian app designed to alert citizens about missile attacks. Hacktivists aligned with each side of the conflict began conducting DoS attacks as well as hack-and-leak and defacements. For the most part, nation-state aligned APT actors conducted limited or no offensive cyber conflict activities targeting Hamas or Israel. Organizations with Atlassian's Confluence Data Center and Confluence Server reported compromises. Atlassian determined that a zero-day access control vulnerability, CVE-2023-22515, was being exploited. Apple released updates to iOS and iPadOS to address two more zero-day vulnerabilities. Three zero-days were among 104 security updates on Microsoft Patch Tuesday. Cisco and multiple intelligence sources have been tracking attacks exploiting a chain of two zero-day vulnerabilities in Cisco IOS XE software enabling creation of new accounts and implanting remote control malware.

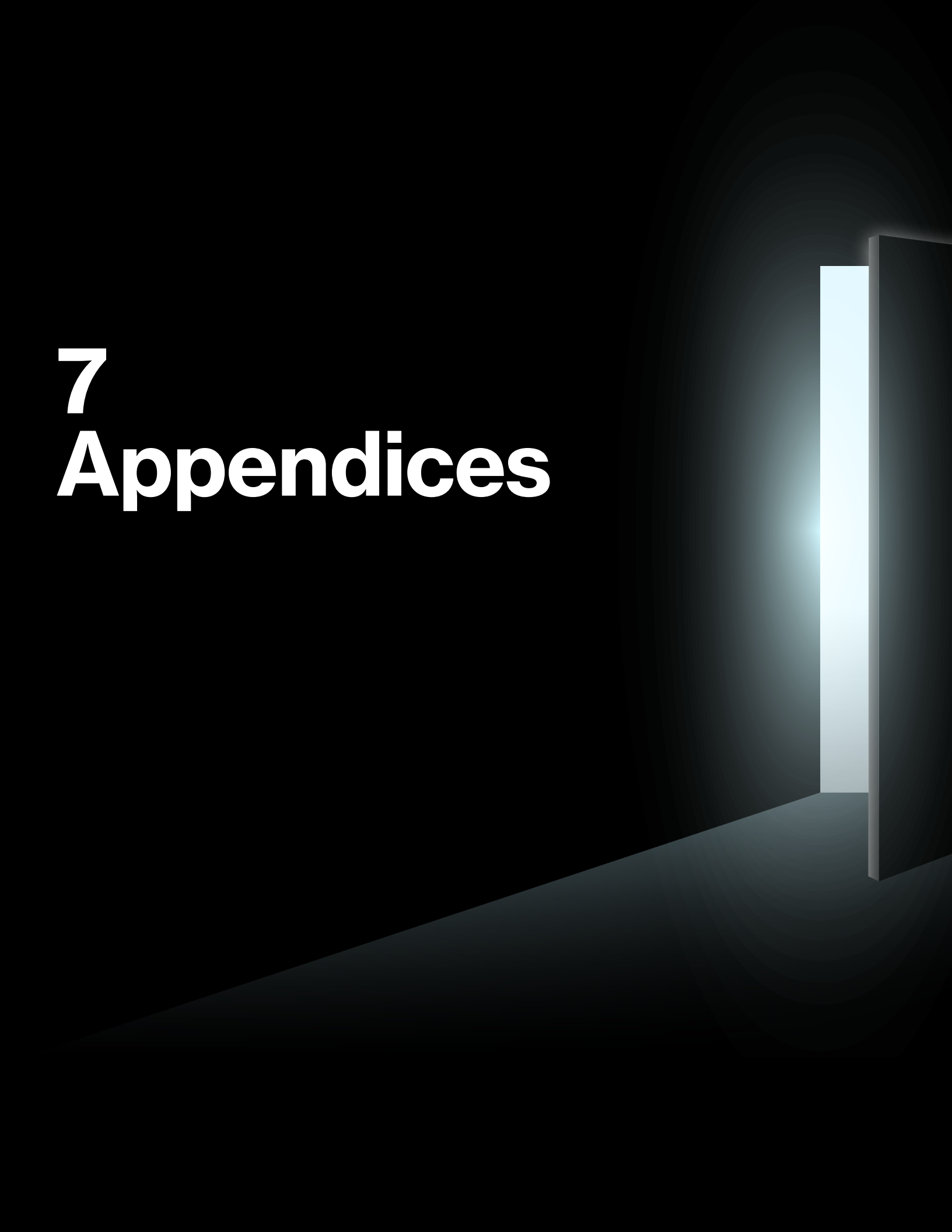
November

After a significant drop in observed ransomware attacks in September and October, November saw numbers rebound more to where we expected them to be. Carbanak, a well-known banking malware, returned from relative obscurity controlled by the FIN7 APT-grade cybercrime actor. Multiple sources linked FIN7 to Carbanak, Cl0p and ALPHV ransomware TAs. HelloKitty ransomware was attacking a zero-day vulnerability in Apache ActiveMQ, the popular open source, multiprotocol message broker. A zero-day vulnerability in SysAid IT service management software was being exploited by the Cl0p ransomware actors. The Russian APT Sandworm group was responsible for attacks against 22 critical infrastructure organizations in Denmark. November's Patch Tuesday addressed 77 Microsoft patches, among them, Microsoft-released patches for three new zero-day vulnerabilities being exploited in the wild. Two F5 Big IP vulnerabilities were being attacked within five days of release of security advisories and patches. Chrome browser and multiple Apple products patched zero-day vulnerabilities. The Chinese APT, Mustang Panda, conducted cyberespionage campaigns targeting organizations in the Philippines and western Pacific Rim region.

December

The Cyber Av3ngers, a hacktivist TA affiliated with the Islamic Revolutionary Guard Corps (IRGC), took responsibility for defacing workstations at Pennsylvania's Municipal Water Authority of Aliquippa. The TA reportedly hit multiple water utility companies in the United States by targeting Unitronics' PLC devices. Ukraine's largest mobile operator, Kyivstar, was hit by a cyberattack that left its system infrastructure extensively damaged and knocked it out of operation for days. The Solntsepek TA—which had been previously linked to the notorious Sandworm Group—claimed the attack a day later, stating that it had destroyed 10,000 computers, more than 4,000 servers, all cloud storage and backup systems. Google's Chrome browser, QNAP's VioStor network video recorder and Future X Communications' wireless LAN routers AE1021PE and AE1021 each patched new vulnerabilities that had already been successfully exploited in the wild. Barracuda ESG appliances had a zero-day vulnerability that was being successfully exploited by a Chinese threat actor. Midmonth, Microsoft warned that Qbot (Qakbot) was being distributed again in a phishing campaign pretending to be an email from an IRS employee.

7
Appendices



Appendix A: How to read this report

Hello, and welcome first-time readers! Before you get started on the 2024 DBIR, it might be a good idea to take a look at this appendix first. 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" who 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 are 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 or recording a hacking action as SQL injection or brute force.

Learn more here:

- **https://github.com/vz-risk/dbir/tree/gh-pages/2024**—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 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 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 are available here:

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

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 80, 81, 82 and 83 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.

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 80. Example slanted bar chart (n=205)

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 exist within each observation's confidence interval. As you can see, some of the threads are looser than others, indicating a wider confidence interval and a smaller sample size.

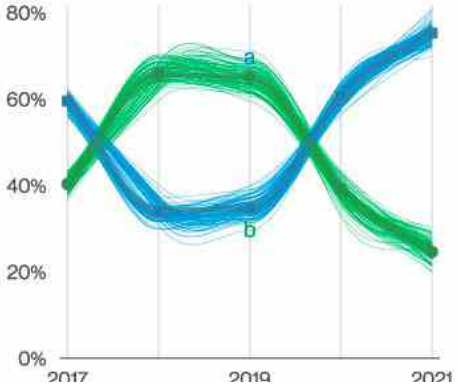


Figure 81. Example spaghetti chart

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 82), 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.

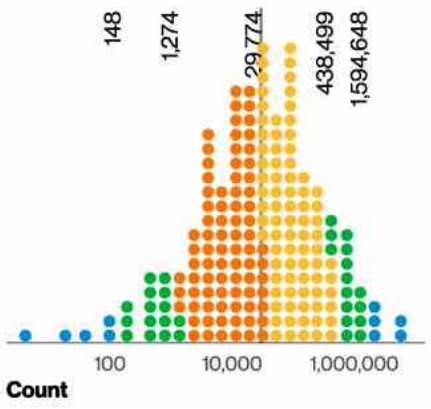


Figure 82. Example dot plot (n=672). Each dot represents 0.5% of organizations. Orange: lower half of 80%. Yellow: upper half of 80%. Green: 80%–95%. Blue: Outliers. 95% of orgs: 148–1,594,648. 80%: 1,274–438,499. Median: 29,774 (log scale).

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.

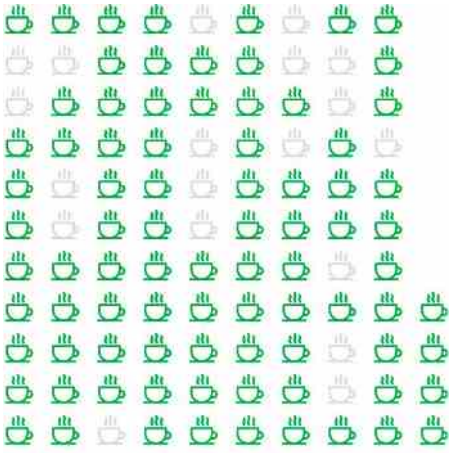


Figure 83. Example pictogram plot (n=4,110). Each glyph represents 40 breaches.

Appendix B: 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: **https://verizon.com/business/resources/reports/dbir/2024/corrections.**

Second, science comes in two flavors: creative exploration and causal hypothesis testing. The DBIR is squarely in the former. While we may not be 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 would like to 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.[104] 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 appear throughout 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.

104 As does this sentence

Incident data

Our data is non-exclusively multinomial, meaning that 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 because it means that 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 "n/a") 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 time frame of analysis (November 1, 2022, to October 31, 2023, for this report). The 2023 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.

Acknowledgment 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

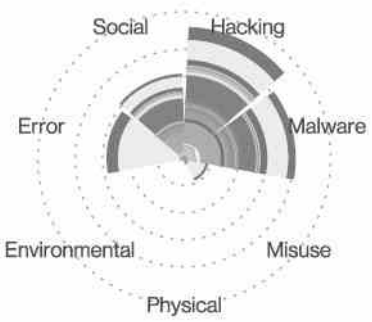


Figure 84. Individual contributors per Action

Breaches

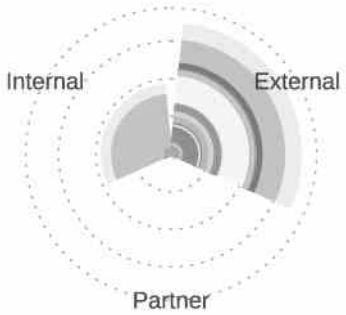


Figure 85. Individual contributors per Actor

Breaches

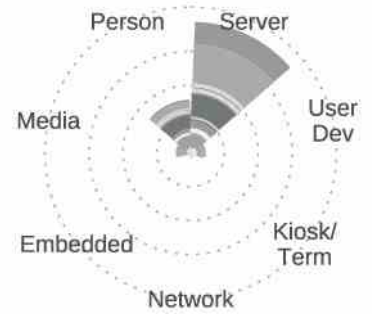


Figure 86. Individual contributors per Asset

Breaches

Figure 87. Individual contributors per Attribute

The first type of bias is random bias introduced by sampling. This year, our maximum confidence is +/- 0.5% for incidents and +/- 0.8% 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 that axis.

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.[105] 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 seven 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 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 weighing 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.

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

Appendix C: U.S. Secret Service

By Assistant Director Brian Lambert and Assistant Special Agent in Charge Krzysztof Bossowski, United States Secret Service

Combating Cybercrime Amid Technological Change

The U.S. Secret Service worked to combat fraud through traditional methods while identifying new threats driven by emerging technology in 2023. Ransomware continued to feature prominently in data breaches impacting U.S. companies. Meanwhile, transnational cybercriminals were increasingly successful in finding innovative ways to enable their fraud schemes. Artificial Intelligence (AI) captured the world's attention and imagination, and cybercriminals were among the early adopters. The Secret Service investigated numerous cybercriminals experimenting with these generative new tools to commit fraud. In response, the agency also partnered with the same technology companies these fraudsters relied upon for their schemes. This proved a valuable strategy to detect scams and hold bad actors accountable.

The Secret Service is built on a foundation of protecting the integrity of our nation's financial system. The agency was created in 1865 to address a surge in counterfeiting following the Civil War. Today, the agency continues to fight counterfeiting while also battling computer fraud and abuse, bank fraud, payment card fraud, identity theft, financial extortion, wire fraud, and more. Additionally, the Secret Service is charged with providing investigative assistance to local law enforcement and the National Center for Missing & Exploited Children. The continued success of the Secret Service's investigative mission depends on partnerships with law enforcement agencies and private sector experts. The Secret Service operates a network of Cyber Fraud Task Forces (CFTF) throughout the country, which fosters these interactions with our partners. Long-term partnerships are the best mechanism to prevent and mitigate cybercrime.

The use of ransomware to exploit businesses again played a significant role in major data breaches. The criminal organizations behind these attacks heavily leveraged the crime-as-a-service business model, including threatening to publish stolen data. The Secret Service, alongside its law enforcement and private sector partners, fought against these criminals. The team approach foiled several ransomware campaigns and protected a number of targeted American companies and organizations. Agents also infiltrated these criminal organizations and developed tangible

information for IT administrators. This enabled IT teams to implement countermeasures to protect their corporate infrastructure, significantly reducing data breaches and financial losses. Industry reports on ransomware show mixed trends in the prevalence and revenue generated through ransomware scams in 2023. Our work continues as we strive to end the profitability of such schemes.

Generative AI remains a hot topic. ChatGPT became a technological hit in January 2023 with 100 million registered active users. Legitimate customers used the AI tool to write papers and answer questions. But within weeks, criminals also leveraged AI tools in fraud and extortion schemes. For example, a Secret Service investigation led to the arrest of a group of individuals who used AI-powered translation tools. These individuals did not speak English or have any advanced computer skills. Yet, these bad actors used the new tools to create transnational romance and extortion plots to defraud victims of millions of dollars. The victims in these cases were not aware the translation was taking place or even that they were interacting with someone in a foreign country.

To stay ahead of the criminal element, the Secret Service is increasingly partnering with technology companies to ensure new technology aids in preventing—rather than enabling—crime. This includes measures that companies can implement to detect misuse of their tools and explore how these technologies can appropriately aid investigations. For example, our research teams and investigators increasingly face difficulty analyzing large digital data sets. However, new data analytic techniques can significantly improve our ability to detect and address illicit activity. These new techniques were used successfully in investigating a large-scale fraud scheme impacting the state of California. Within a few weeks of work on this case, investigators identified patterns in the fraud schemes that resulted in Secret Service agents arresting five criminals withdrawing tens of thousands of dollars from ATMs using information stolen from California-based users of Electronic Benefit Transfer (EBT) cards.[106] This case demonstrated how new data tools aid in analysis and have the potential to quickly detect and address illicit activity in both the public and private sectors.

Whether battling ransomware, credit card fraud, or protecting minors from online child predators, the Secret Service works to stay on the cutting edge of technology. New technology enables criminals and investigators alike, and our private sector and law enforcement partnerships are the key to detecting and preventing illicit activity. Our network of Cyber Fraud Task Forces will continue to foster regular interaction with our partners to promote the prevention and mitigation of cybercrime with the critical goal of protecting America's financial interests. Working together, we can identify and implement ways to use technology effectively to prevent crime.

106 https://www.secretservice.gov/newsroom/releases/2023/06/five-charged-theft-california-benefits-low-income-families

Appendix D: Using the VERIS Community Database (VCDB) to Estimate Risk

By HALOCK Security Labs and the Center for Internet Security (CIS)

The VCDB was a leap forward in incident sharing. For CIS and HALOCK it's been a solid foundation for risk analysis. One of the biggest challenges in conducting risk assessments is estimating the likelihood that an incident will occur. The VCDB contains a lot of structured incident data, so we were sure we could use it to somehow help us solve that challenge.

When we started exploring the VCDB together, it held about 7,500 incident records—each with about 2,500 data points—telling us how each incident occurred. But that's almost 19 million data points! How could we shape that data to help the CIS community estimate risks?

We experimented and discovered many useful aggregations that brought shape and meaning to the mass of recorded incidents. By focusing on the attack varieties in the recordset, we could see how commonly (or uncommonly) certain attacks were used. Shifting our attention to attack vectors or vulnerabilities helped us understand how certain weaknesses have contributed to incidents. Aggregating data based on industries (right down to the NAICS codes) showed how attack methods are correlated to the distribution of assets that are common in types of organizations.

We realized that the data could be shaped to answer more complex questions, like what industries are more or less susceptible to which kinds of attacks, or what attack methods are most or least commonly associated with which asset classes. If you were patient and skilled you could also find out what kinds of attacks trended higher or lower year-over-year, or which assets and methods are most frequently correlated with each other in attacks.

If your heart rate went up while reading that previous paragraph, then you're our kind of people. But as much fun as we were having, we had to focus on our purpose: find the simplest way to model risk probability for the widest population.

We settled on a simple correlation between the VCDB data and the CIS Controls when we noticed how commonly certain asset classes were exploited in attacks. Because the CIS Controls safeguards are associated with asset classes and the VCDB shows the assets involved in each incident, we could tie the VCDB incidents to the CIS safeguards that would help prevent types of attacks. We were then able to bake that into our risk assessment method, CIS RAM,[107] to help enterprises estimate the likelihood portion of their risk analysis. The more commonly an asset appeared in incident records, the more likely it would be the cause of an eventual incident, unless its corresponding safeguards were strong. This insight became our "Expectancy" score to automatically estimate risk likelihood.

These two diagrams illustrate that Expectancy correlation. Figure 88 depicts a correlation between the commonality of an asset in the VCDB and the maturity of a CIS Controls safeguard that would protect that asset. A low asset commonality matched with a high maturity control would make the expectancy score low (in this illustration, '2' out of '5').

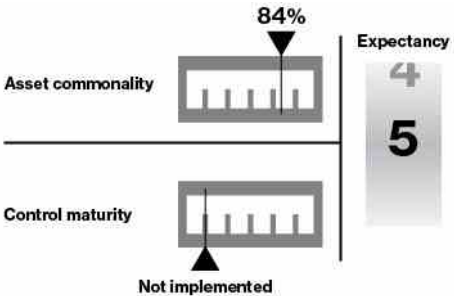


Figure 88. Low asset commonality and high control maturity

Conversely, Figure 89 shows how a high Expectancy score would result from a high asset commonality and a low control maturity.

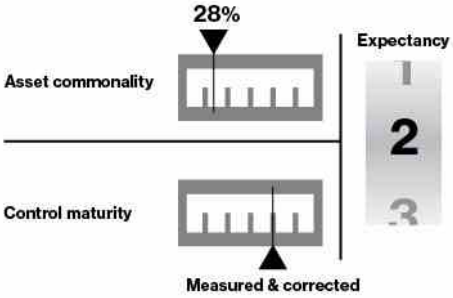


Figure 89. High asset commonality and low control maturity

If we stated this correlation in plain language, we would say that the more commonly an asset is compromised, the more capable our controls for that asset should be.

But no risk analysis is complete without also considering the impact of an incident. CIS RAM uses additional methods to help enterprises estimate impact scores, so when paired with the Expectancy scores, they have evidence-based risk analysis. And in the spirit of the VCDB community, CIS RAM could freely provide that analysis to anyone who needs it.

Risk analysts might wonder about our use of the word "expectancy" rather than "likelihood" or "probability." This was a careful choice driven by what the VCDB can tell us.

The word "probability" is best suited for statistical analysis that results in a calculated percentage range or value within a time period (e.g. "between a 12% and 22% chance," or "12% probability in a year"). "Likelihood" is typically used more colloquially or for less rigorous estimation processes ("very likely," "not likely", etc.) but still implies a time period or frequency.

The Expectancy score, however, does not consider a time frame. It says that we accept that an incident of some kind will occur, and that the higher the Expectancy score, the more we expect that asset and control to be involved. The lower the Expectancy score, the less we expect the asset and control to be involved.

This helps each enterprise prioritize the improvement of safeguards that could reduce risk the most.

Our correlation is not the only way that organizations can use the VCDB to estimate the likelihood of attacks. Even CIS and HALOCK use our own aggregations of the data given our different purposes. Consider how you would manage your cyber security program if you knew what attack methods were most common in your industry, or what attack methods correspond to what assets, or what was trending higher over time.

Take time to explore the VCDB for your risk analysis uses. You'll be impressed with what you find.

The VERIS Community Database
https://verisframework.org/vcdb.html

107 https://learn.cisecurity.org/cis-ram

Appendix E: Contributing organizations

A

Akamai Technologies

Ankura

Apura Cyber Intelligence

B

Balbix

bit-x-bit

Bitsight

BlackBerry

C

Censys, Inc.

Center for Internet Security (CIS)

Cequence Security

CERT Division of Carnegie Mellon University's Software Engineering Institute

CERT – European Union (CERT-EU)

CERT Polska

Check Point Software Technologies Ltd.

Chubb

City of London Police

Coalition

Coveware

Cowbell Cyber Inc.

CrowdStrike

Cyber Security Agency of Singapore

Cybersecurity and Infrastructure Security Agency (CISA)

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

Cybersixgill

CYBIR

Cyentia Institute

D

Defense Counterintelligence and Security Agency (DCSA)

DomainTools

E

Edgescan

Emergence Insurance

EUROCONTROL

EVIDEN

F

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

G

Global Resilience Federation

GreyNoise

H

Halcyon

HALOCK Security Labs

I

Information Commissioner's Office (ICO)

Irish Reporting and Information Security Service (IRISS-CERT)

Ivanti

J

JPCERT/CC

K

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

Kaspersky

KnowBe4

KordaMentha

L

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

M

Maritime Transportation System ISAC (MTS-ISAC)

Mimecast

mnemonic

N

National Crime Agency

National Cyber-Forensics & Training Alliance (NCFTA)

National Fraud Intelligence Bureau

NetDiligence®

NETSCOUT

O

Okta

OpenText Cybersecurity

P

Palo Alto Networks

Q

Qualys

R

Recorded Future, Inc.

Resilience

ReversingLabs

S

S21sec by Thales

Securin, Inc.

SecurityTrails, a Recorded Future Company

Shadowserver Foundation

Shodan

Sistemas Aplicativos

Sophos

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.

Z

Zscaler

Akamai	ankura	apura	Balbix	bit-x-bit
BITSIGHT	BlackBerry	censys	CIS Center for Internet Security	CEQUENCE
Carnegie Mellon University Software Engineering Institute	CERT-EU	NASK CERT.PL	CHECK POINT	CHUBB
CITY OF LONDON POLICE	Coalition	COVEWARE	COWBELL CYBER	CROWDSTRIKE
CSA SINGAPORE	CISA	CyberSecurity MALAYSIA	cybersixgill	CYBIR
Cyentia INSTITUTE	DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY	DomainTools	edgescan	emergence
EUROCONTROL	EVIDEN	FBI	GLOBAL RESILIENCE FEDERATION	GREYNOISE
halcyon	HALOCK	ico.	IRISS Irish Reporting and Information Security Service	ivanti

JPCERT CC®	K12 SIX	kaspersky	KnowBe4 Human error. Conquered.	KordaMentha
LEGAL SERVICES ISAO	Maritime Transportation System Information Sharing and Analysis Center	mimecast	mnemonic	NCA National Crime Agency
NCFTA	National Fraud Intelligence Bureau	NetDiligence®	NETSCOUT	okta
opentext™	paloalto NETWORKS	Qualys. Continuous Security	Recorded Future®	resilience
REVERSINGLABS	S21SEC Cyber Solutions by Thales	Securin	SecurityTrails A Recorded Future® Company	SHADOWSERVER
SHODAN	SISAP Sistemas Aplicativos	SOPHOS	swisscom	
	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	zscaler™	

verizon business

© 2024 Verizon. OGREP3970524