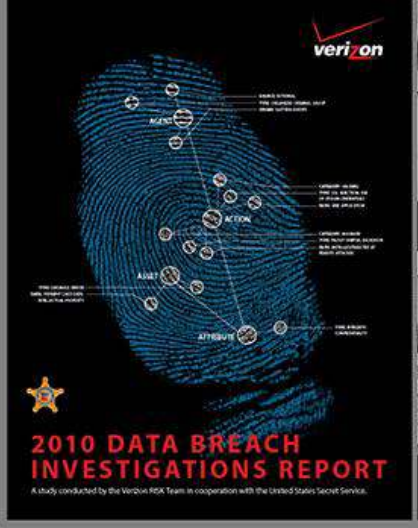
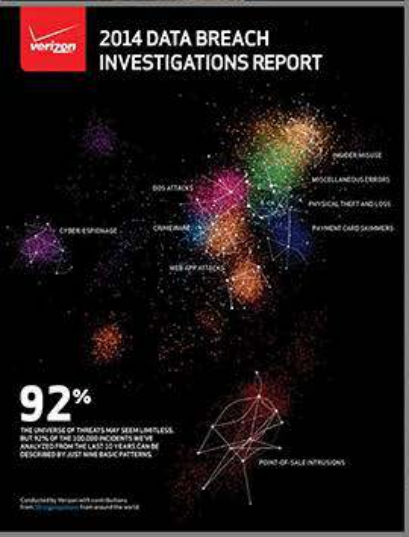
DBIR

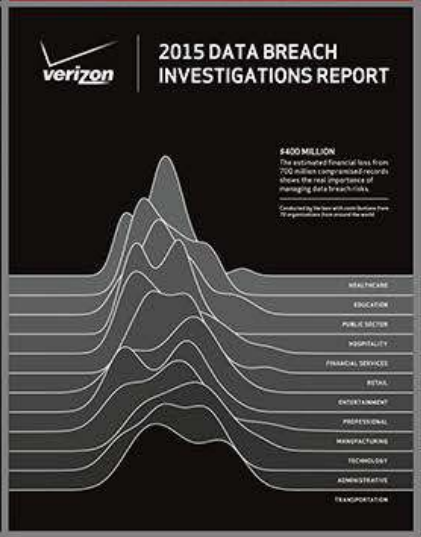
Data Breach Investigations Report

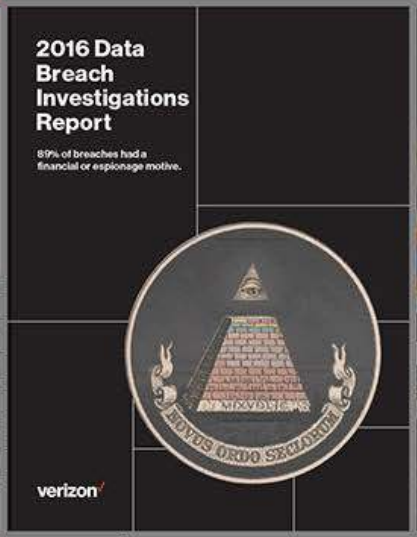


About the 2022 cover

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







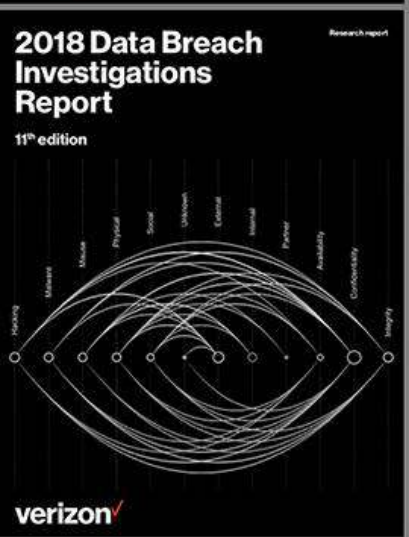


Table of contents 1

DBIR Master's Guide

Hello, and welcome first-time readers! Before you get started on the 2022 Data Breach Investigations Report (DBIR) it might be a good idea to take a look at this section first. (For those of you who are familiar with the report, please feel free to jump over to the introduction). We have been doing this report for a while now, and we appreciate that the verbiage we use can be a bit obtuse at times. We use very deliberate naming conventions, terms and definitions and spend a lot of time making sure we are consistent throughout the report. Hopefully this section will help make all of those more familiar.

VERIS resources

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

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

Threat action: What tactics (actions) were used to affect an asset? VERIS uses seven primary categories of threat actions: Malware, Hacking, Social, Misuse, Physical, Error and Environmental. Examples at a high level 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:

- **github.com/vz-risk/dbir/tree/gh-pages/2022** – DBIR facts, figures and figure data.
- **veriscommunity.net** features information on the framework with examples and enumeration listings.
- **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.

Industry labels

We align with the North American Industry Classification System (NAICS) standard to categorize the victim organizations in our corpus. The standard uses two- to six-digit codes to classify businesses and organizations. Our analysis is typically done at the two-digit level and we will specify NAICS codes along with an industry label. For example, a chart with a label of Financial (52) is not indicative of 52 as a value. "52" is the NAICS code for the Finance and Insurance sector. The overall label of "Financial" is used for brevity within the figures. Detailed information on the codes and the classification system are available here:

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

Being confident of our data

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

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

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).

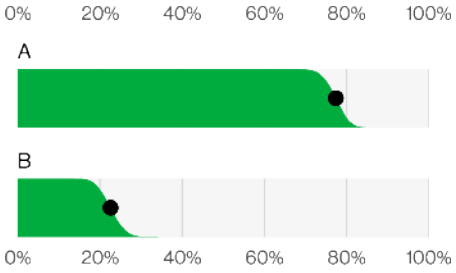


Figure 1. Example slanted bar chart (n=205)

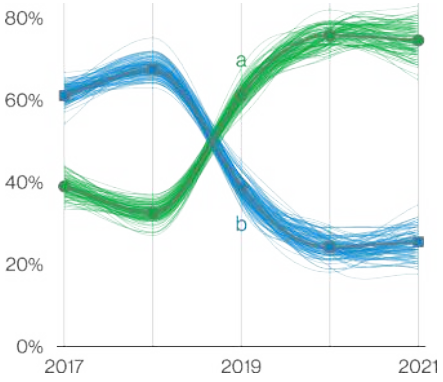


Figure 2. Example spaghetti chart

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.

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

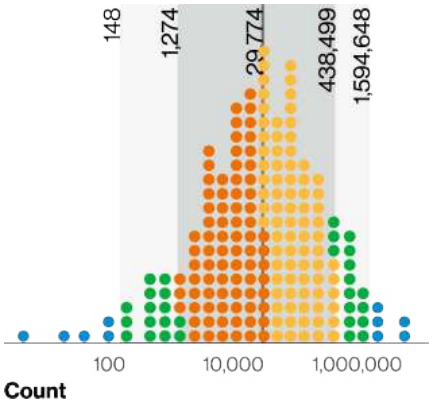


Figure 3. Example dot plot (n=672). Each dot represents 0.5% of organizations. Orange: lower half of 80%. Yellow: upper half of 80%. Green: 80%-95%. Blue: Outliers. 95% of orgs: 148 - 1,594,648. 80%: 1,274 - 438,499. Median: 29,774 (log scale).

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

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

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

PLEASE NOTE: While we have always listed the following facts in our Methodology section (because that is where this type of information belongs) we decided to also mention it here for the benefit of those who don't make it that far into the report. Each year, the DBIR timeline for in-scope incidents is from Nov. 01 of one calendar year until Oct. 31, of the next calendar year. Thus, the incidents described in this report took place between Nov. 01, 2020 to Oct. 31, 2021. The 2021 caseload is the primary analytical focus of the 2022 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 the 80 odd global contributors, anonymizing and aggregating that data, analyzing the dataset and, finally, creating the graphics and writing the report. Rome wasn't built in a day, and neither is the DBIR.

Questions? Comments?

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

Introduction

Welcome to the 15th annual Verizon Data Breach Investigations Report! It is truly hard to believe that it has been 15 years since our inaugural installment of this document. Were we to indulge our imaginations with anthropomorphic comparisons, we might find this report having its braces removed, finally being able to get a driver's permit, overusing sarcasm, perhaps becoming a bit goth and generally being unappreciative. But we won't bother with all that. We will simply say THANK YOU! Thank you to our contributors for your continued willingness to share your data, insight and vast experience in a selfless effort to improve this industry. A huge thank you to our readers for sticking with us through this long and epic journey, for being the reason we work so hard to produce this report, and most of all, for keeping us from having to get real jobs.

The past few years have been overwhelming for all of us. Just when we think we have reached the uttermost limit of our ability to be surprised, the world throws us yet another curve ball. Honestly, at this point, we here on the team would not so much as blink if Sasquatch were elected Governor, if Area 51 opened a bed and breakfast, or if ransomware increased yet again. Spoiler alert – one of those things did, in fact, happen. (Congrats, Squatch! You deserve it.)

The past year has been extraordinary in a number of ways, but it was certainly memorable with regard to the murky world of cybercrime. From very well publicized critical infrastructure attacks to massive supply chain breaches, the financially motivated criminals and nefarious nation-state actors have rarely, if ever, come out swinging the way they did over the last 12 months. As always, we will examine what our data has to tell us about these and the other common action types used against enterprises. Also, in honor of the 15th edition of the DBIR, we will occasionally refer back to comments, charts and figures from previous editions of this report to see how far we, as an industry, have come, and how the threat landscape and the techniques threat actors utilize have changed. This year the DBIR team analyzed 23,896 security incidents, of which, 5,212 were confirmed data breaches.

With that in mind, let's revisit the Introduction to the 2018 DBIR:
"The DBIR was created to provide a place for security practitioners to look for data-driven, real-world views on what commonly befalls companies with regard to cybercrime. That need to know what is happening and what we can do to protect ourselves is why the DBIR remains relevant over a decade later. We hope that as in years past, you will be able to use this report and the information it contains to increase your awareness of what tactics attackers are likely to use against organizations in your industry, as a tool to encourage executives to support much-needed security initiatives, and as a way to illustrate to employees the importance of security and how they can help."

From that perspective, we are proud to say that nothing has changed, and we hope you both enjoy the report and find the information it contains useful. Thanks again, for everything.

The DBIR Team

Gabriel Bassett, C. David Hylender, Philippe Langlois, Alex Pinto, Suzanne Widup

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

Summary of findings

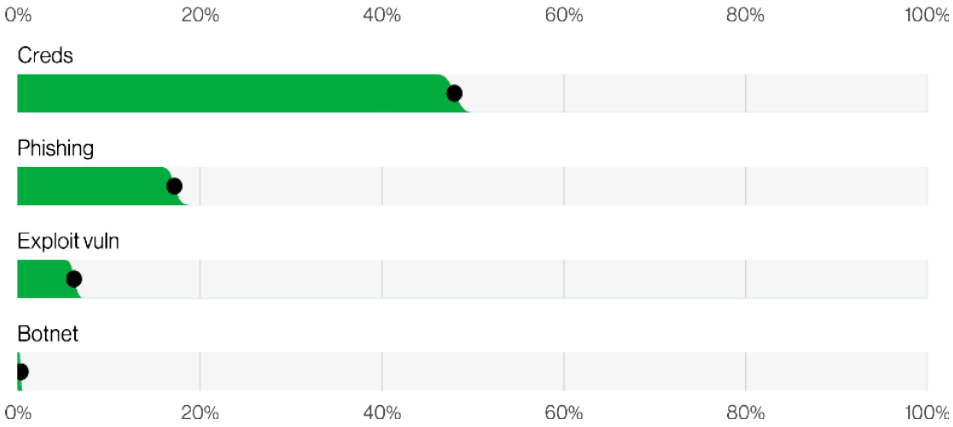


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

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

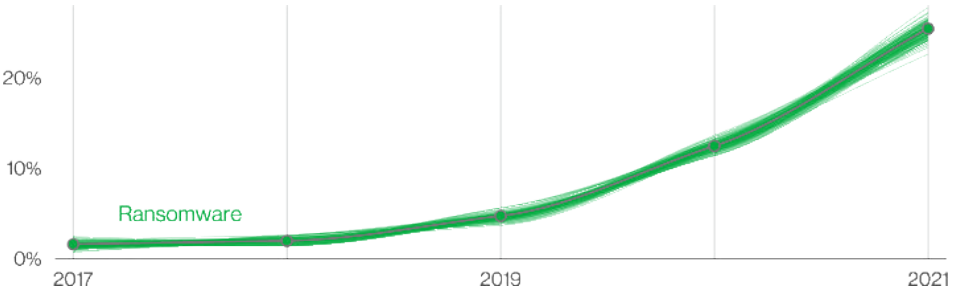


Figure 6. Ransomware over time in breaches

This year Ransomware has continued its upward trend with an almost 13% increase–a rise as big as the last five years combined (for a total of 25% this year). It's important to remember, Ransomware by itself is really just a model of monetizing an organization's access. Blocking the four key paths mentioned above helps to block the most common routes Ransomware uses to invade your network.

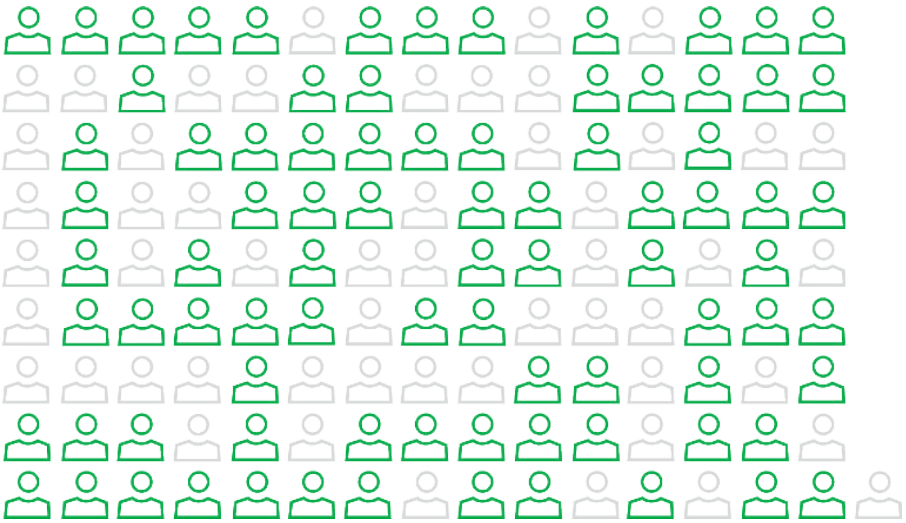


Figure 7. Partner vector in System Intrusion incidents (n=3,403)
Each glyph represents 25 incidents.

2021 illustrated how one key supply chain breach can lead to wide ranging consequences. Supply chain was responsible for 62% of System Intrusion incidents this year. Unlike a Financially motivated actor, Nation-state threat actors may skip the breach and keep the access.

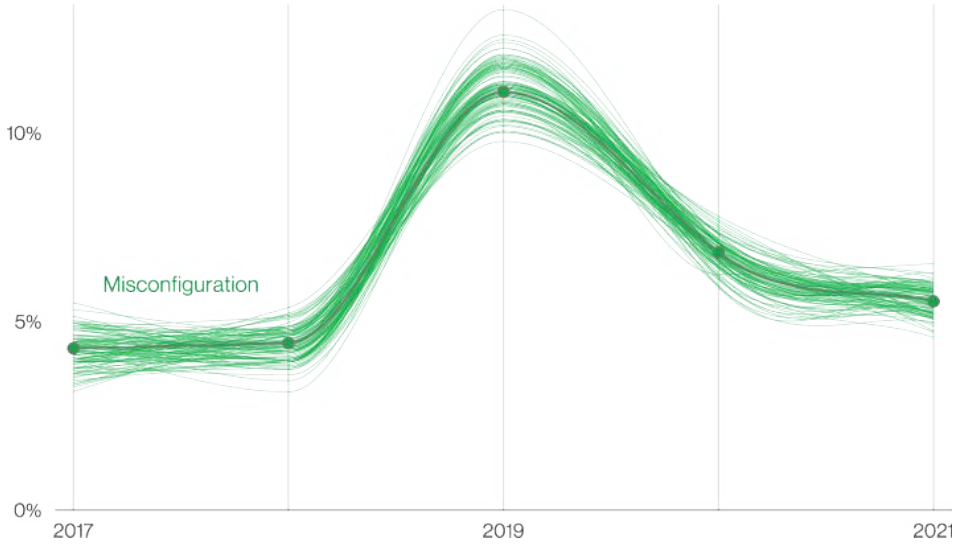


Figure 8. Misconfiguration over time in breaches

Error continues to be a dominant trend and is responsible for 13% of breaches. This finding is heavily influenced by misconfigured cloud storage. While this is the second year in a row that we have seen a slight leveling out for this pattern, the fallibility of employees should not be discounted.

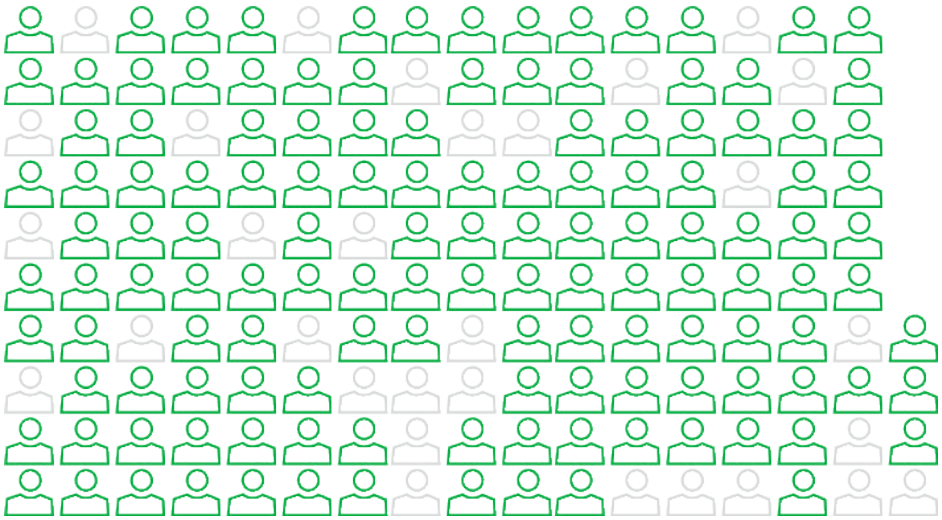
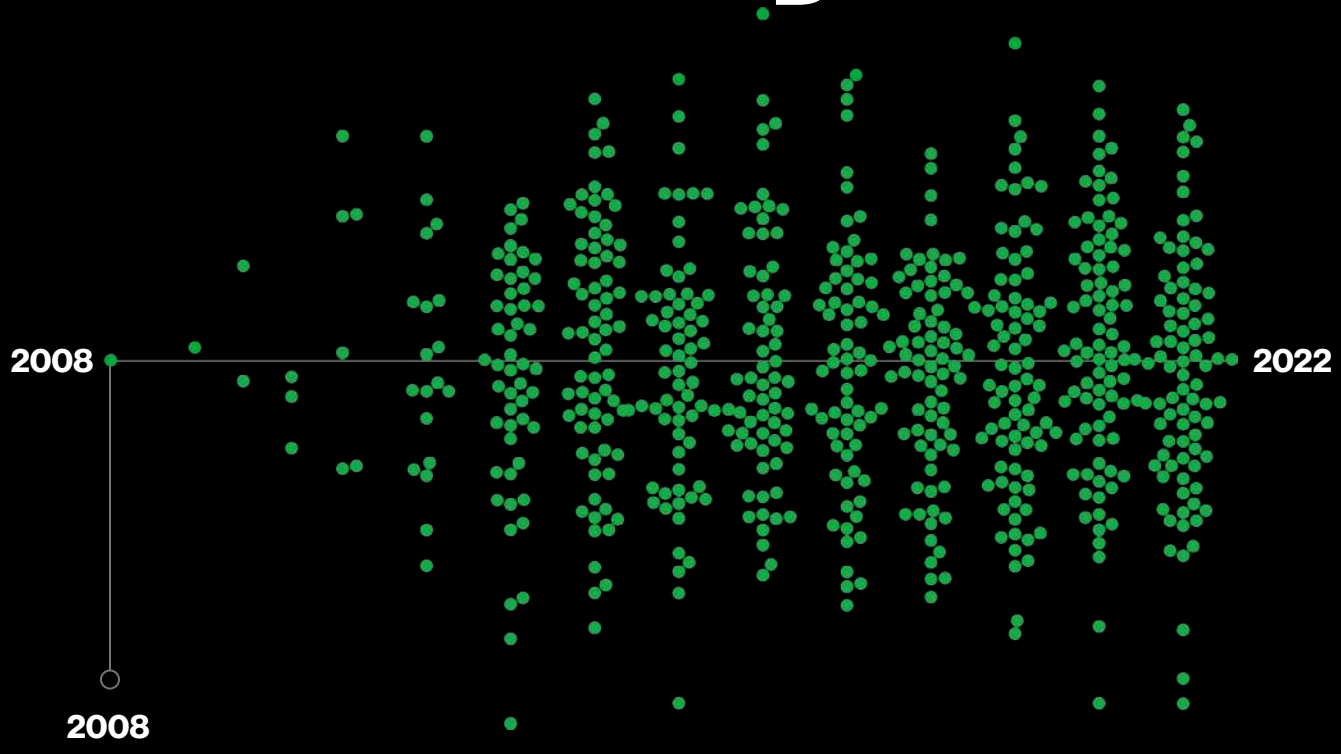


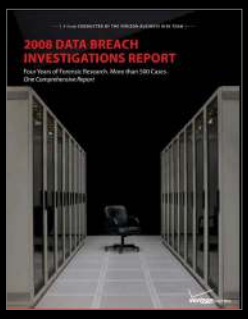
Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches.

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

2

Results and Analysis





Results and Analysis: Introduction

Welcome to the DBIR 15-year reunion! Please grab a name tag, find some familiar faces, and reminisce about the good ole days back in 2008. Now, let's catch everyone up on how we've changed over the years.

A picture may tell a thousand words, but so will a good figure. The charts we use in our report are the result of numerous iterative attempts to convey both the main story of the data, as well as the main constraints, which is a tricky[1] proposition. Our dataset comes to us in a variety of formats and represents many different contributors—each of which come complete with their own particular nuances and biases. We realize that our data is not a 'pure sample' of the world of breaches and incidents (because such a thing does not exist). Nevertheless, we can still extract meaningful analysis.

You may already be familiar with the charts such as Figure 10 we used in the original DBIR, and while these bar charts are an excellent means of allowing for easy comparisons between a small set of things, they can also sometimes hide important information in their percentages. Therefore, in an effort to be more transparent with our readers regarding the level of ambiguity or uncertainty in our data, over time we have transitioned to slanted bar charts such as Figure 11, which captures both the comparison between the "things" and the range of values for those based on the confidence we have in the data. We've also applied the same notion to our line charts, instead of representing trends as singular lines based on the average, we plot a collection of lines within our confidence interval. The good news is that you can still convey the core message of "things change" but also provide an honest illustration of "these are the possible representations of those changes."

After 15 years of this data breach journey, we find ourselves reminiscing about all the deadlines, failed cover ideas, and heated arguments that we encountered along the way. However, maybe the real treasure of our journey wasn't all the fame, mega yachts, book deals and data breach analysis, but the friends we made over the years. Initially this report was based solely on Verizon data, but since then we have been joined by 87 partners and collaborators from across the globe who make this report possible. Due in large part to them, we have collected and analyzed in total over 914,547 incidents, 234,638 breaches and 8.9 TBs of cybersecurity data, to bring our readers the best possible analysis and results. Truly, we stand on the shoulders of giants. Without further ado, let's take a dive into the analysis.

1 It's not just rhymes that are tricky to rock.

Actor – Friends in low places

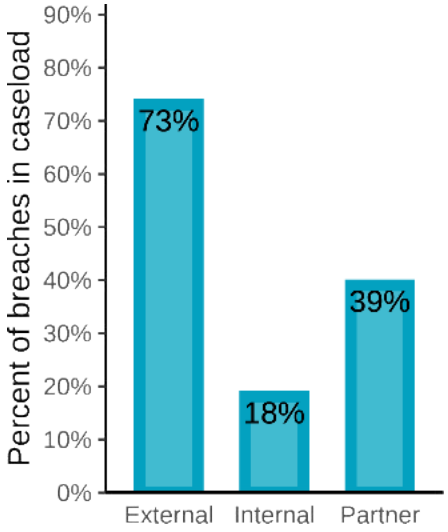


Figure 10. Sources of Data Breaches (2008 DBIR Figure 3)

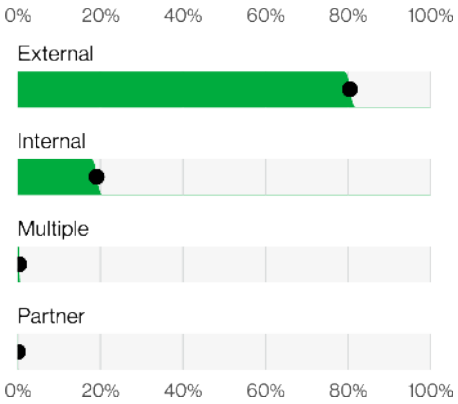


Figure 11. Actors in breaches (n=5,146)

Our findings indicate that data compromises are considerably more likely to result from external attacks than from any other source. Nearly three out of four cases yielded evidence pointing outside the victim organization. In keeping with other studies revealing risks inherent to the extended enterprise, business partners were involved in 39 percent of the data breaches handled by our investigators. Internal sources accounted for the fewest number of incidents (18 percent), trailing those of external origin by a ratio of four to one.

The relative infrequency of data breaches attributed to insiders may be surprising to some. It is widely believed and commonly reported that insider incidents outnumber those caused by other sources. While certainly true for the broad range of security incidents, our caseload showed otherwise for incidents resulting in data compromise. This finding, of course, should be considered in light of the fact that insiders are adept at keeping their activities secret. (2008 DBIR)

Some things haven't changed since we first began publishing this report back in 2008 (For those of you who need context, the original iPhone had been released only one year prior). The 2008 cyber[2] security world, with limited access to handheld wonder machines, held the belief that insider incidents outnumbered external ones, or at least felt it was "certainly true for the broad range of security incidents." As we look back now, with the benefit (?) of 15 years of time-wasting apps, considerably more gray hair and a few chips off the collective Infosec shoulders, we can confidently state that External actors are consistently more common than Internal, with 80% of breaches being caused by those external to the organization, as seen in Figure 11.

2 Can you find all 145 "cyber" references in the DBIR this year? I bet you can't...

The median size (as measured in the number of compromised records) for an insider breach exceeded that of an outsider by more than 10 to one. Likewise, incidents involving partners tend to be substantially larger than those caused by external sources. This supports the principle that privileged parties are able to do more damage to the organization than outsiders. (2008 DBIR)

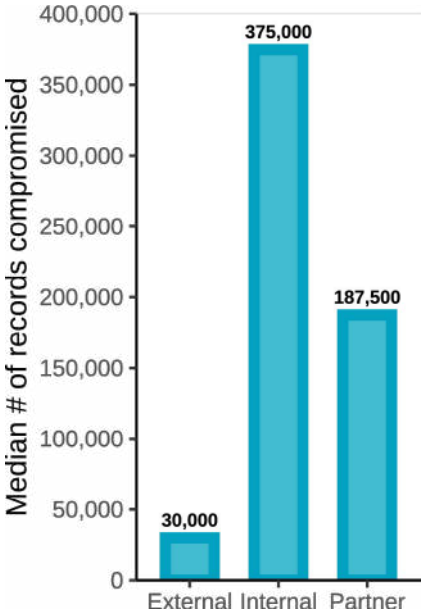


Figure 12. Median Number of Records Compromised (2008 DBIR Figure 5)

In the 2008 report, the number of records breached was the metric of choice. Now that we are a bit further into the 21st century, the currency of impact is the metric du jour. Though records are still of interest, they are typically not viewed with the same level of importance as in past years. However, in 2008 the median internal breach nabbed 375,000 records; as you can see in Figure 13, this year it's only 80,00. While it appears the number of records is decreasing, it is important to keep in mind that a number of changes have taken place both in this report and within the industry at large. Therefore, the change in record count could be reflective of the fact that there are now more ways for attackers to monetize data.

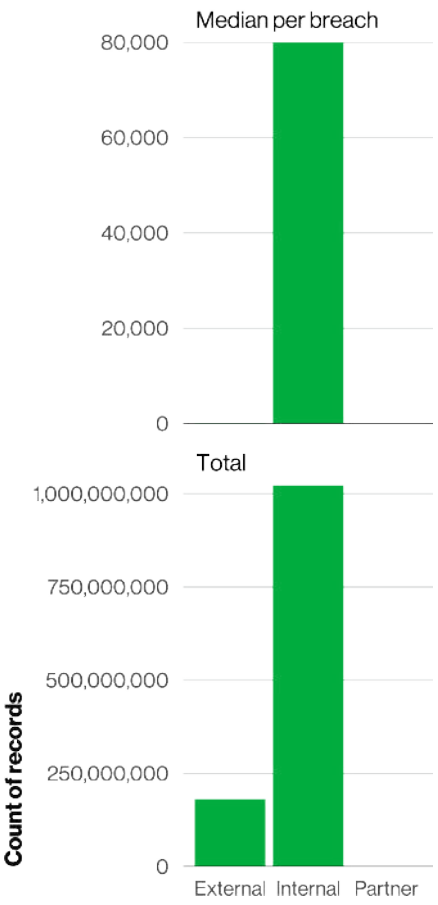


Figure 13. Records by Actor in breaches (n=54)

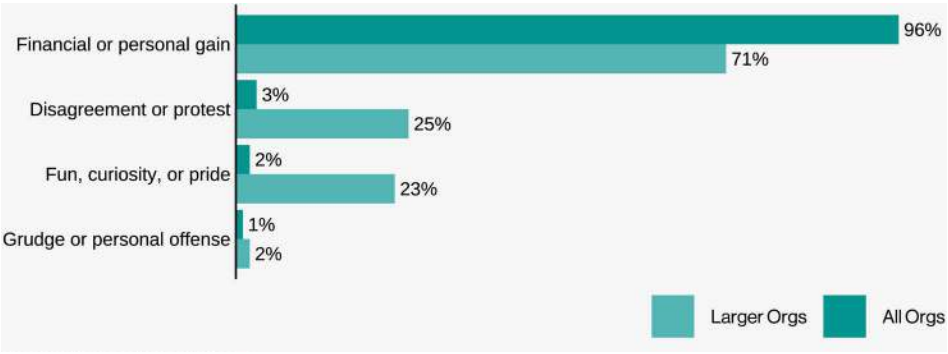


Figure 14. Motive in external agents by percent of breaches within external (2012 DBIR Figure 15)

Bottom line: most data thieves are professional criminals deliberately trying to steal information they can turn into cash. Like we said—same ol' story.

It's not the whole story, however, nor is it the most important one. The most significant change we saw in 2011 was the rise of "hacktivism" against larger organizations worldwide. The frequency and regularity of cases tied to activist groups that came through our doors in 2011 exceeded the number worked in all previous years combined (2015 DBIR).

Motive, for the most part, was not an initial topic of analysis for the DBIR (although in 2008 we did consider it in the context of targeted vs opportunistic breaches). In 2010, we stated "Today's cybercriminals are not hobbyists seeking knowledge or thrills; they are motivated by the illicit profits possible in online crime." While that may seem obvious to today's readers, it is important to remember that at that time the stereotypical "let me hack this site from my mom's basement to impress my bros" type of activity was believed by many to account for a certain proportion of breaches. Regardless, the motive of the threat actor is important to understand in order to attempt to quantify how many of our troubles are caused by the illicit economy, personal vendettas or by accidental blunders.

Financial has been the top motive since we began to track it in 2015. However, that same year the rise of hacktivism (particularly leaks) accounted for many attacks. Espionage-related attacks were not even on the radar, but seven years later the world is a very different place. Espionage has taken the 2nd place spot for years, and hacktivism is, for the most part, simply an afterthought. Before we move on, however, it should be noted that while espionage has almost certainly increased over the last few years, the fact that it did not appear at all in 2015 was quite likely due to our contributors and general case load at the time.

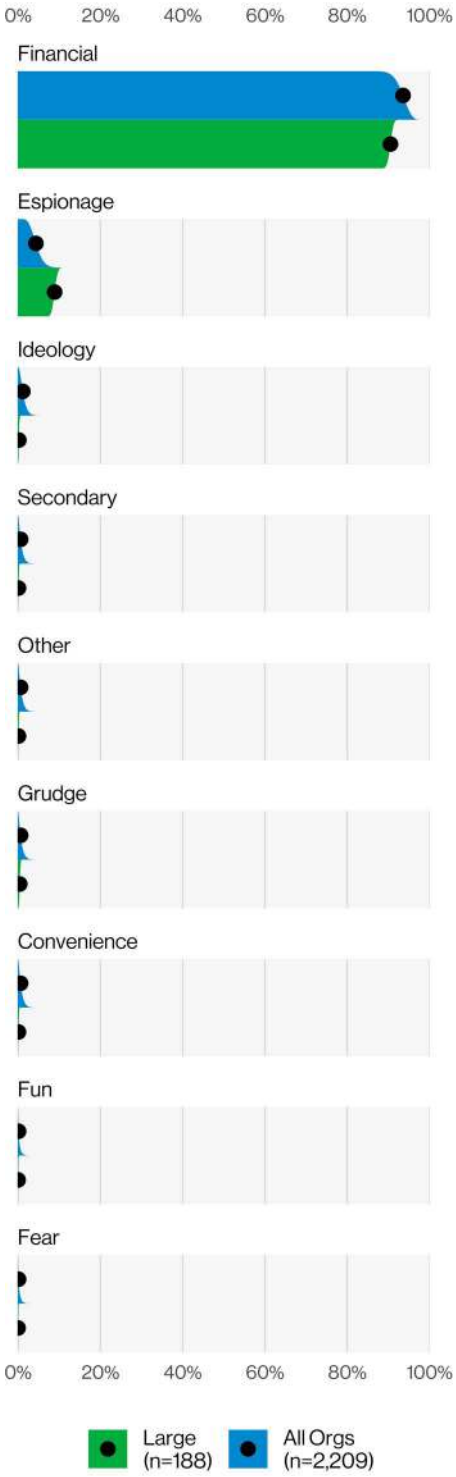


Figure 15. Motives in External actors by org size

Actions

The Actions section tells the story of how the security incident or breach plays out. It's a bit like a Hollywood action movie, only with a modest budget and there are no explosions or car chases. Nevertheless, in spite of the dearth of pyrotechnics, the actions that lead up to these breaches have a definite impact on their victims. Actions are discussed in the DBIR by variety (the type of action) and vector (through what means the action took place). Figure 16 through Figure 19 illustrate the varieties and vectors associated with incidents and breaches.

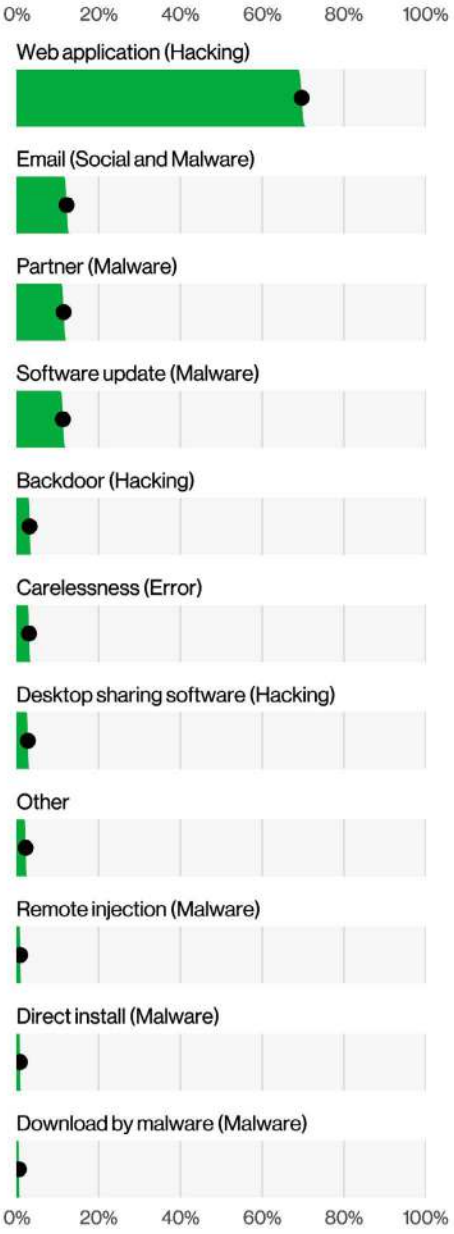


Figure 16. Top Action vectors in incidents (n=18,419)

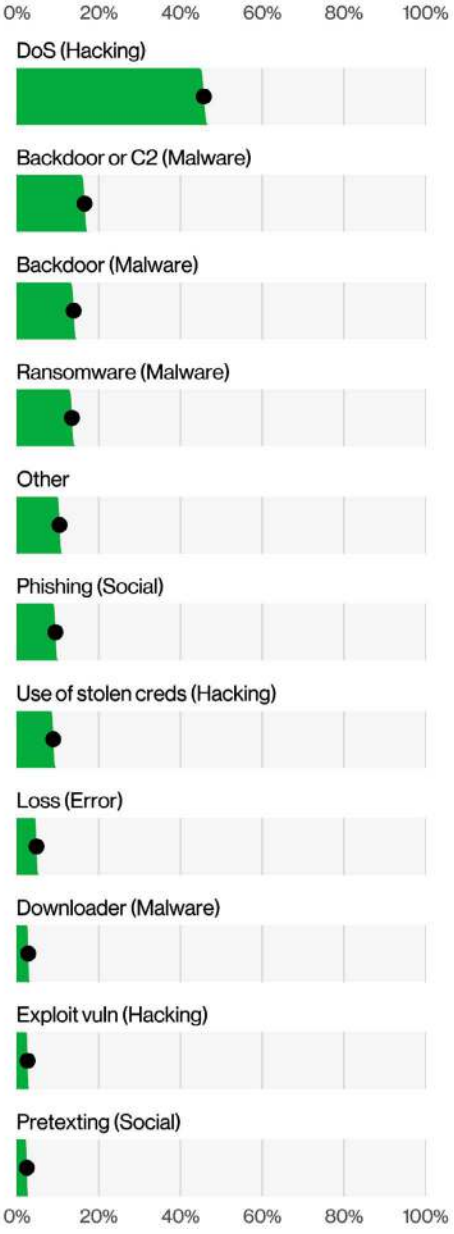


Figure 17. Top Action varieties in incidents (n=18,511)

Action Categories

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

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

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

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

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

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

Environmental: 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.

PLEASE NOTE: That Backdoors provide a direct access point for human operators while C2s are indirect connections used by malware. "Backdoor or C2" contains both Backdoors and C2 provided only by malware, while "Backdoor" covers both backdoors provided by malware and backdoors provided by hacking. Because neither is a subset of the other, we keep them both. As a reader, your takeaway should be that remote access established by the attacker is important and that there are a slew of ways of creating that persistent access.

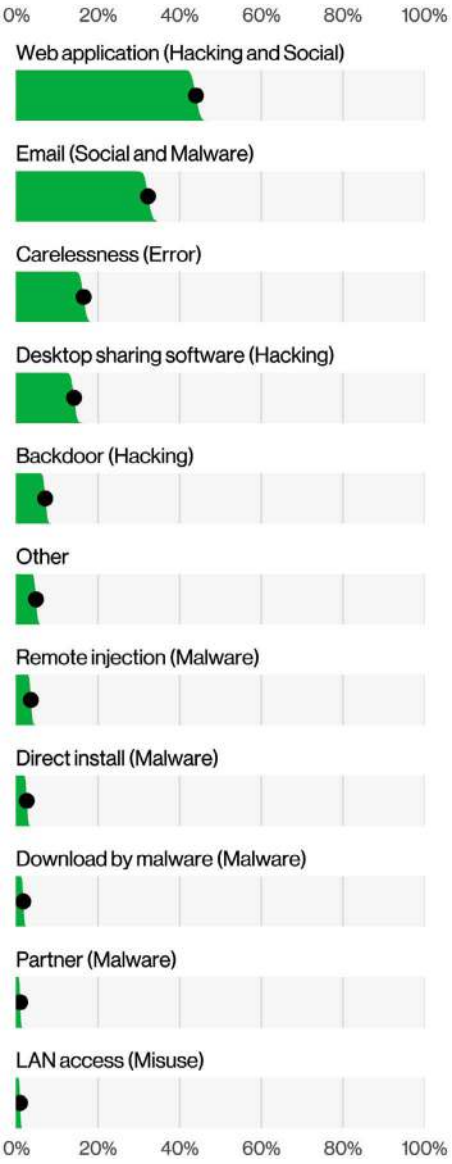


Figure 18. Top Action vectors in breaches (n=3,279)

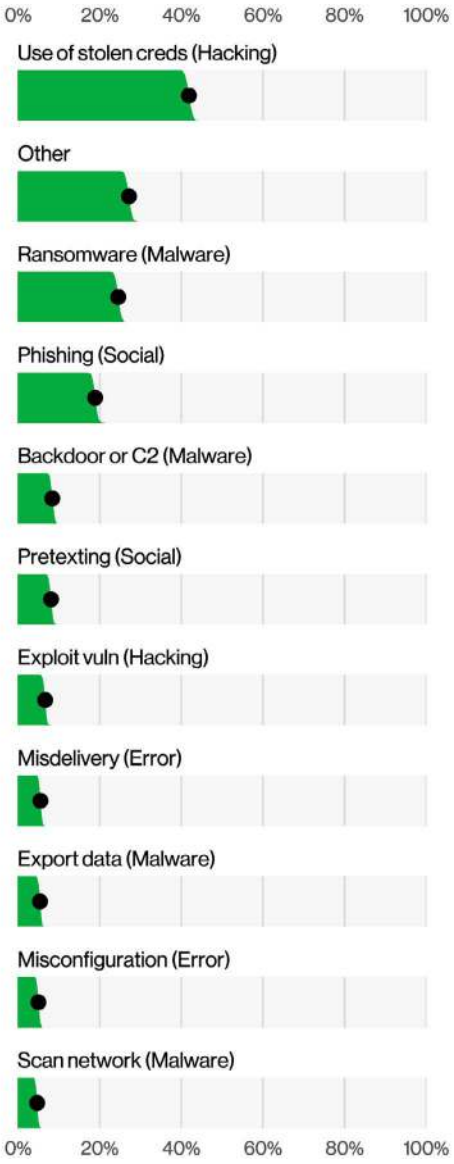


Figure 19. Top Action varieties in breaches (n=3,875)

The Denial of Service (DoS) action is the clear leader, representing 46% of total incidents, followed by the malware types of Backdoor or C2 at 17%. However, a much more interesting finding is the inclusion of Partner and Software update among the top vectors this year. This is a first for Software update, and is something we will discuss in greater detail in a subsequent section. Web application is the number one vector, and, not surprisingly, is connected to the high number of DoS attacks. This pairing, along with the Use of stolen credentials (commonly targeting some form of Web application), is consistent with what we've seen for the past few years.

Turning to breaches, the top varieties are a bit more dynamic, with Use of stolen credentials, Ransomware and Phishing all in the top five. The category of "Other" has stealthily crept into one of the top three spots this year as well. This is largely due to the dataset being long "tailed" and diverse. In other words, there are a lot of different things that aren't in the top 10, but are still noteworthy. We can also flip that on its head and state that 73% of breach varieties are found in the top 10 varieties. Not too shabby considering the fact that we have more than 180 different action varieties. How's that for the Pareto principle?[4]

In terms of vectors, these align well with the notion that the main ways in which your business is exposed to the internet are the main ways that your business is exposed to the bad guys. Web application and Email are the top two vectors for breaches. This is followed by Carelessness, which is associated with Errors such as Misdelivery and Misconfiguration. Next we have Desktop Sharing Software, which captures things like Remote Desktop Protocol (RDP) and third-party software that allows users to remotely access another computer via the Internet. Unfortunately, if you can access the asset directly over the internet simply by entering the credentials, so can the criminals.

4 Not to be confused with the Peter Principle, which is something else entirely.

’08 Throwback

While the DBIR has grown and evolved dramatically since its inception, we find it incredibly interesting how many of the core stats remain the same. In Figure 20 from 2008, you’ll find that the numbers are eerily similar to what we see today. Hacking continues to be the main action, followed by Malcode (Malware). In the 2008 report, Error was recorded in two ways: Errors that directly caused the breach (the dark bar) and Errors that contributed to the breach (light colored bar). We no longer use this breakdown (for a few reasons, one of which is that it can be argued that errors play at least a small part in almost all breaches), but Error accounts for 14% of breaches overall. From there, however, things begin to deviate slightly. This is particularly true with regard to Social and Error, but please keep in mind that our data has grown both in size and diversity of source over the years, expanding from 500 breaches that first year to over 5,000 breaches this year.

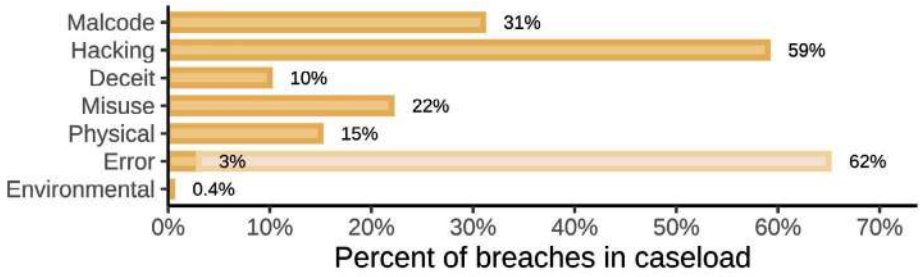


Figure 20. Threat Categories (2008 DBIR Figure 9)
Dark = Caused, Light = Contributed

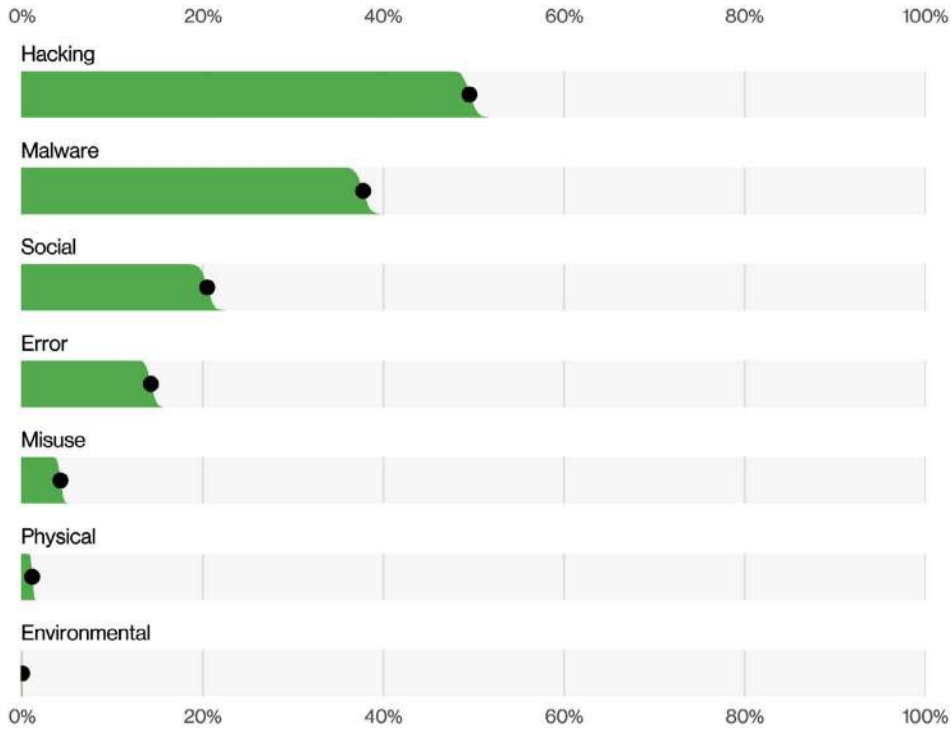


Figure 21. Actions in breaches (n=5,212)

Assets

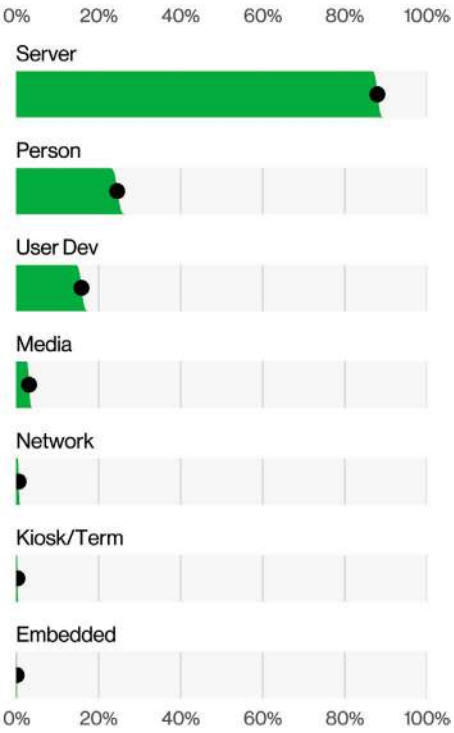


Figure 22. Assets in breaches (n=4,384)

For those not "in the know" about VERIS, (but if you are, that's awesome!) Assets are the THING that the Action happens to. So, this is where you find WHAT was hacked via an exploit (probably a server), WHO was socially engineered by an attacker or WHAT was lost or stolen.[5] For the staunch defenders, this should help you understand what is being targeted and also be a useful tool to start prioritizing what type of coverage your infrastructure needs.

Figure 22 illustrates that the top varieties of Assets impacted in breaches are Servers, People and their devices. When we start to zoom into the specific types of servers (Figure 24) we find Web application (56%) and Mail (28%) servers accounting for the top two varieties, which is rather intuitive when one considers that email servers and web applications are the Assets that are most likely to be internet-facing. As such, they provide a useful venue for attackers

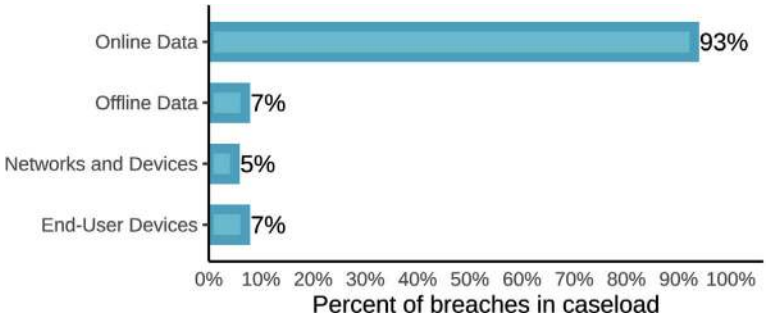


Figure 23. Compromised Assets (2008 DBIR Figure 18)

Looking back

Although how we classified assets in the 2008 DBIR (all those years ago) was different from how we do it today, the findings are relatively similar. Most incidents impact Servers (online data) with a sprinkling of user and networking devices. It seems that servers in data breaches, like JNCO jeans and spiked tipped hair in haute couture, are timeless.

to slip through the organization's "perimeter" by using clever tricks like (spoiler alert) stolen credentials.

Dropping down the list a bit farther to the folks that are socially engineered. These are commonly the individuals who deal with company money and have the ability to do things with it (like update where it is deposited).

While we are on the topic of assets, it is important to remember that not only are Information Technology (IT) assets important, but so are OT (Operational Technology). The topic of OT is on many people's minds (and in the news) these days due to the current political climate. These are the computer systems that run our national infrastructure, and while we do have a smattering of cases, they only account for approximately 3% of our overall incident data. Technically, this is an increase from last year (about 1%). Please consider this a gentle reminder to protect those systems that are quietly chugging away in the background keeping our infrastructure up and running. It isn't called critical infrastructure for nothing.

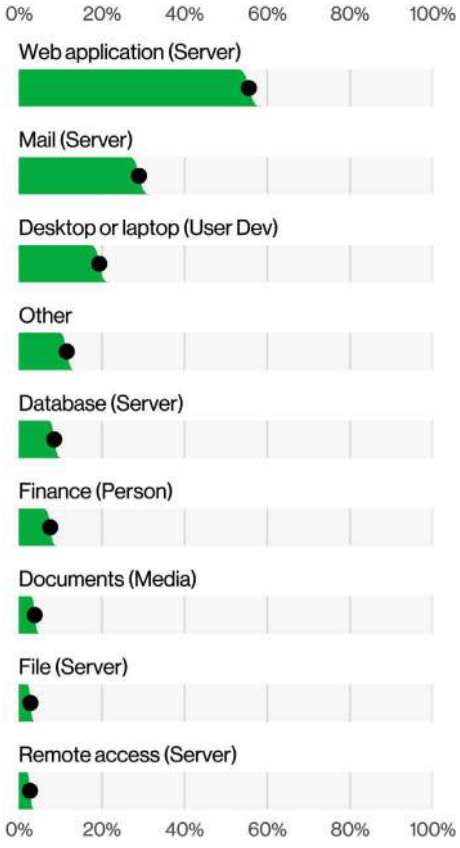


Figure 24. Top Asset varieties in breaches (n=2,796)

5 We feel a Schoolhouse Rock song coming on.

Attribute

If security incidents did not have associated attributes, the life of an InfoSec professional would be a good deal easier. Unfortunately, they do: Confidentiality, Integrity and Availability (commonly referred to as the CIA triad), and they can greatly impact numerous aspects of an incident (who needs to be notified, what actions need to be taken and what explanations need to be given to senior management to name a few). Figure 25 shows the CIA triad over time in our dataset (with regard to security incidents).

The DBIR defines a data breach as a compromise of the Confidentiality attribute, and anytime Confidentiality is compromised, it begs the question what type of data was involved?

Fifteen years ago (Figure 20 from the 2008 DBIR), Payment card data led the pack by a large margin. However, it has slowly declined over the past few years. No doubt this decline is to some degree reflective of the additional security controls that have been added in recent years to protect this type of data. Regardless, Figure 27 shows the top two data types are now Credentials and Personal data. We've long held that Credentials are the favorite data type of criminal actors because they are so useful for masquerading as legitimate users on the system. Much like the proverbial wolf in sheep's clothing, their actions appear innocuous until they attack. With regard to breaches, attackers are frequently exfiltrating Personal data, including email addresses, since it is useful for financial fraud. There is also a large market for their resale, which means they are truly the "gift" that keeps on giving. Unfortunately, what it gives is mostly trouble to the data subjects (whom the data is about).

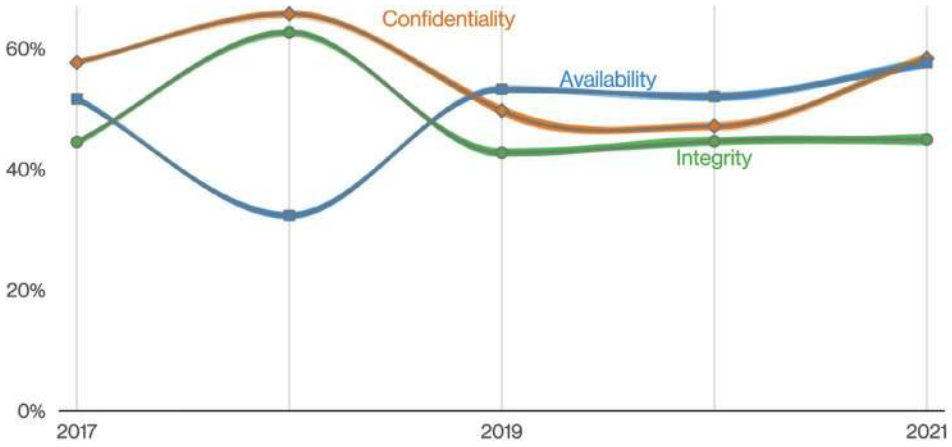


Figure 25. Attributes over time in incidents

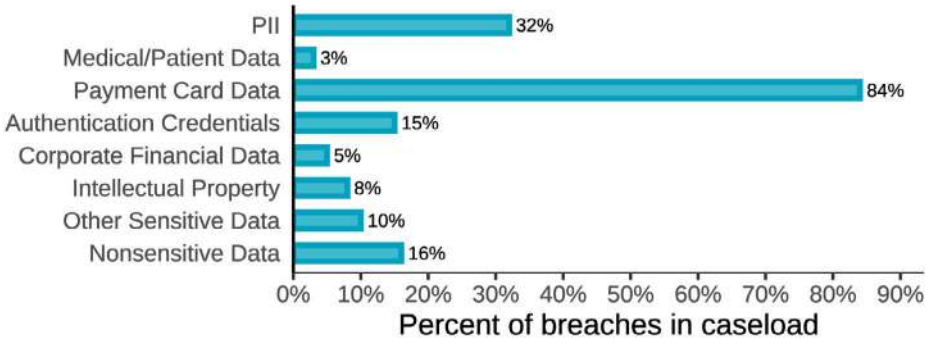


Figure 26. Compromised Data Types (2008 DBIR Figure 20)

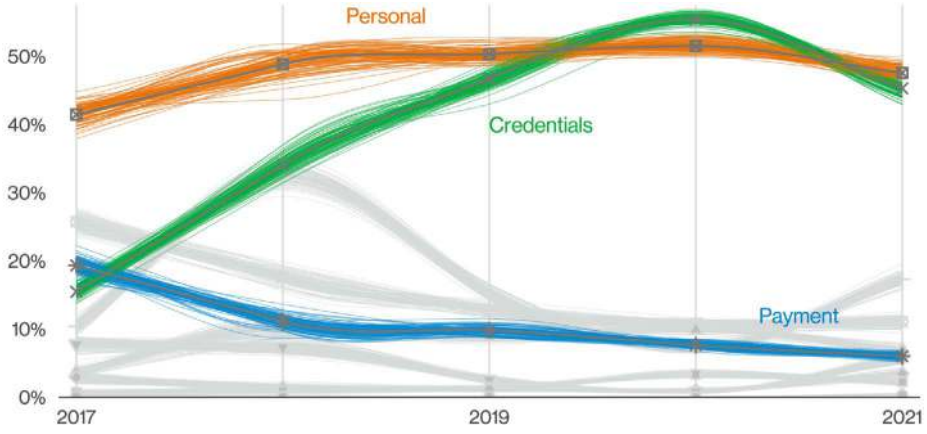


Figure 27. Top Confidentiality data varieties over time in breaches

Once attackers are inside the victim's network they often install malware, which violates the Integrity of a system (as does any other illicit change). The Integrity of a person can also be compromised when they alter their behavior due to the actions of the adversary. Examples include responding to a phishing email or falling victim to a pretexting scenario. These are the two main types of Integrity violations we see in our data, and while they have both been present in all reports, they were not necessarily referred to in the same terminology. In the early days of the DBIR, social actions such as Phishing were not as prevalent as they are now. However, the installation of malware was already quite common back in the day, and our data shows that this year is no exception, with over 30% of breach cases involving some type of malware, and approximately 20% of cases involving a Social action.

Ransomware's heyday continues, and is present in almost 70% of malware breaches this year. Ransomware is an attack that straddles the first two of the CIA Triad (38% of ransomware cases have some Confidentiality compromise), bringing us to the third leg: Availability. When ransomware is triggered, the organization experiences an Availability loss since they can no longer access their data. The particular variety is Obscuration in our dataset, as shown in Figure 28.

Another common form of availability impact is Interruption which often arises from Distributed Denial of Service (DDoS) attacks. These attacks make up a large number of incidents, but are relatively non-existent in our breach caseload. But if DoS is something you are particularly concerned about, we have an entire pattern devoted to it.

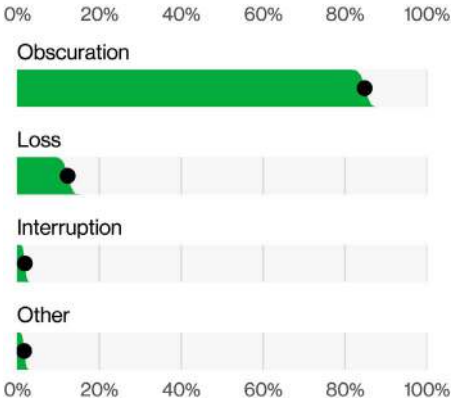


Figure 28. Top Availability varieties in breaches (n=1,109)

Timeline

Discovery time is a good place to begin when viewing timelines. While Figure 29 might seem like good news (that we are more likely to detect breaches within days than months), it gets to be a little less comforting once you start looking at some of the drivers. The top Discovery Method for breaches (more than 50%) is now "Actor Disclosure" (normally either on the asset in the form of a ransomware note or on a criminal forum to sell the data or announce the breach). Neither of which is desirable. "Ignorance is bliss" doesn't readily apply to breaches.

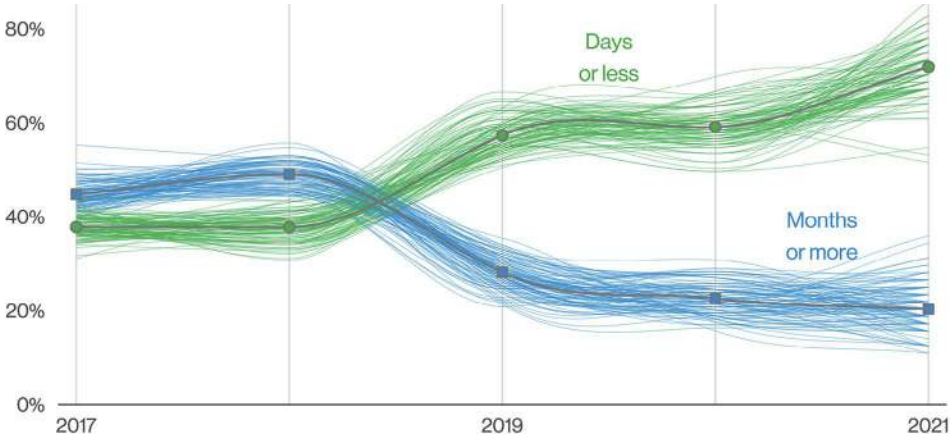


Figure 29. Detection in non-actor-disclosed breaches

Event Chains

Rather than simply analyze how long an attack took in time, we can also analyze how long it took with regard to Actions in Figure 30. We can view this timeline of Actions in our Event Chain data. Event Chains capture the path an attack followed.[6] Figure 30 shows that the vast majority of breaches include only a handful of steps. Three Actions (Phishing, Downloader, and Ransomware) are the most common, while very few breaches utilize five or more Actions. Our job as defenders is to lengthen that attack path. Attackers tend to avoid longer attack chains because every additional step is a chance for the defender to prevent, detect, respond to and recover from the breach.

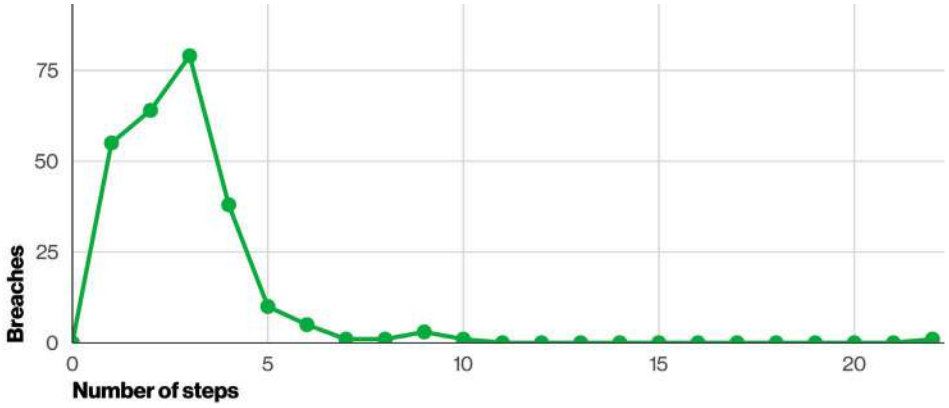


Figure 30. Number of steps per breach in non-Error breaches (n=258)

6 Event Chains are kinda like Attack Flow in Appendix B: VERIS and Standards, but more basic.

Value Chain

Over the past two years the DBIR team has been collecting value chain information, defined as the capabilities and investments an attacker must acquire prior to the actions on the target, either by purchase or investment in its creation. Traditionally, defenders are largely focused on the events that occur within their boundaries, which makes sense since those are the things they control. However, an attacker ecosystem exists both before and after the breach, and it plays into and feeds off of the incident. The value chain asks the question "Where did that email address come from?" Or "Where do those stolen credentials go?" It often seems that breaches beget more breaches, creating a Circle of Breach[7] so to speak. By understanding the transactions associated with this ecosystem, we can understand the key steps involved in attacks and work collaboratively to make those transactions more difficult, expensive or unsustainable for the attackers.

"It takes money to make money"

There are several things attackers must invest in for a breach:

- **Development:** software or content that must be developed to accomplish the actions on the target.
- **Targeting:** work that identifies exploitable opportunities. These overlap heavily with the data varieties that are compromised.
- **Distribution:** services used to distribute actor content including email, compromised servers and websites.
- **Non-Distribution Services:** services provided and used by threat actors other than those used for distribution of actor content.
- **Cash-out:** methods for converting something (likely the attribute compromised) into currency.

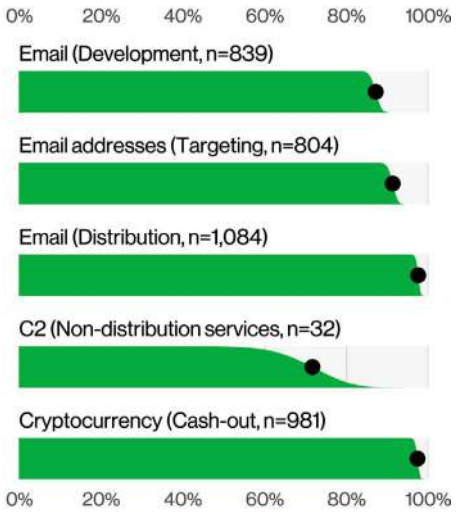


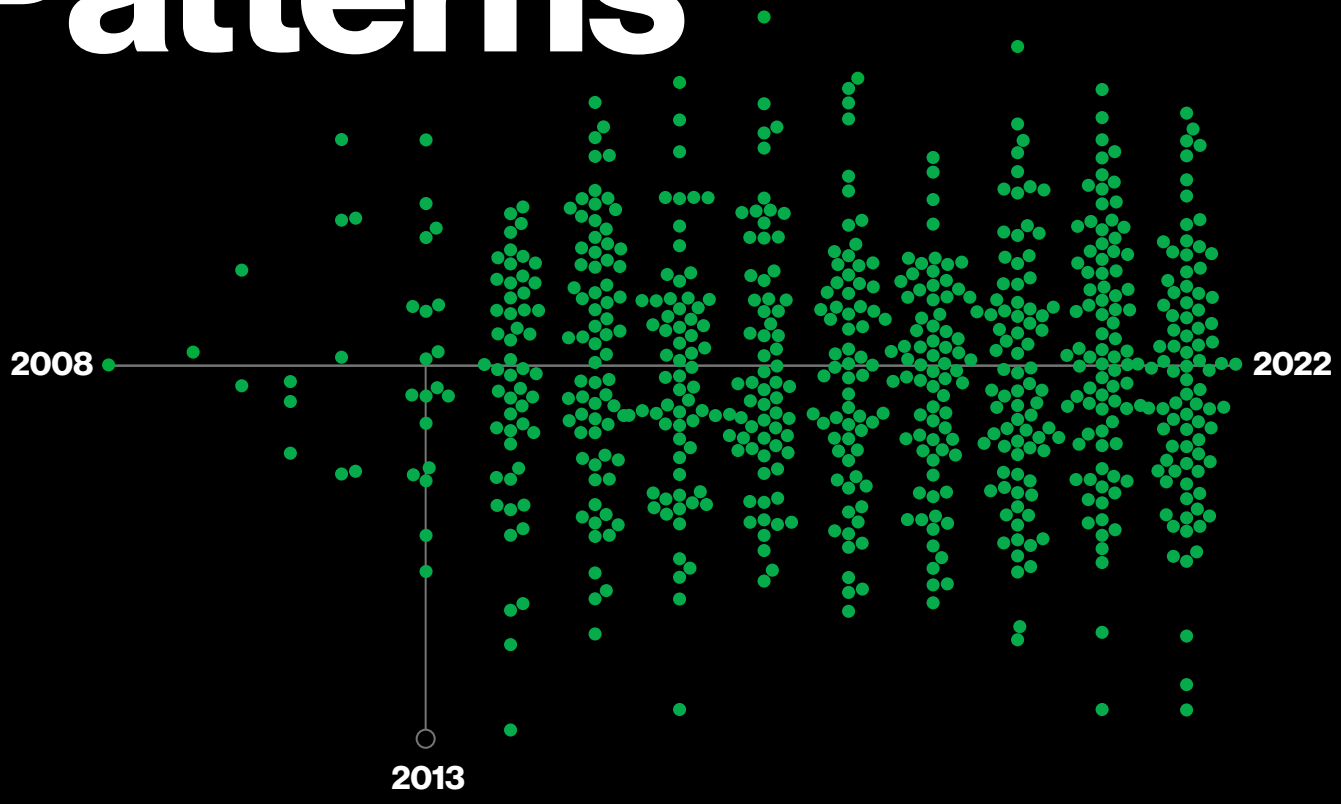
Figure 31. Top value chain variety by value chain category in breaches

Figure 31 provides the top variety for each part of the value chain. Email is the most common method. While we can easily infer email in the value chain, things such as malware in development or credentials in targeting are harder to infer, and so may be underrepresented. Malware can be freely available and credentials may be stolen. The takeaway is not to think of breaches only in terms of starting or ending. Instead, think of them like you might think of a sports team: they are either on the field or preparing to be.

7 Like the Circle of Life, but for threat actors.

3

Incident Classification Patterns



Incident Classification Patterns: Introduction

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

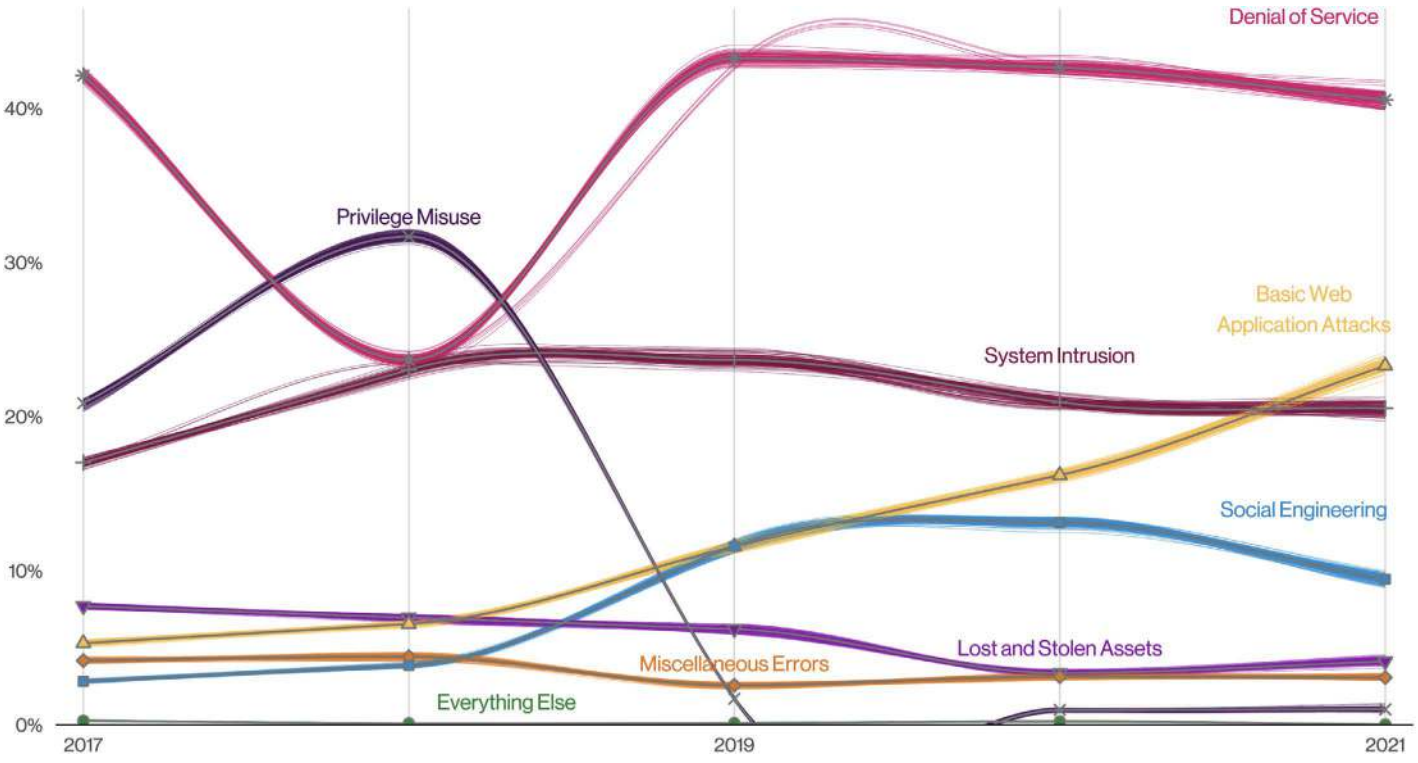


Figure 32. Patterns over time in incidents

The patterns are essentially clusters of "like" incidents. Starting in 2014, and for several subsequent years, there were nine patterns. Last year we found that due to changes in attack type and the threat landscape, the data was leading us toward revamping, combining and generally overhauling those patterns. Therefore, starting with the 2021 report, we moved from the original nine patterns down to the eight you see in this report. The eight patterns, and how they are defined, can be found in Table 1. Please be sure to peruse the way we define the different patterns, as we will refer to them throughout the report.

Basic Web Application Attacks	These attacks are against a Web application, and after 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	Attacks 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.
Miscellaneous Errors	Incidents where unintentional actions directly compromised a security attribute of an information asset. This does not include lost devices, which are grouped with theft instead.
Privilege Misuse	Incidents predominantly driven by unapproved or malicious use of legitimate privileges.
Social Engineering	A psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality.
System Intrusion	Complex attacks that leverage malware and/or hacking to achieve their objectives including deploying Ransomware.
Everything Else	This "pattern" isn't really a pattern at all. Instead, it covers all incidents that don't fit within the orderly confines of the other patterns. Like that container where you keep all the cables for electronics you don't own anymore: Just in case.

Table 1. Incident Classification Patterns

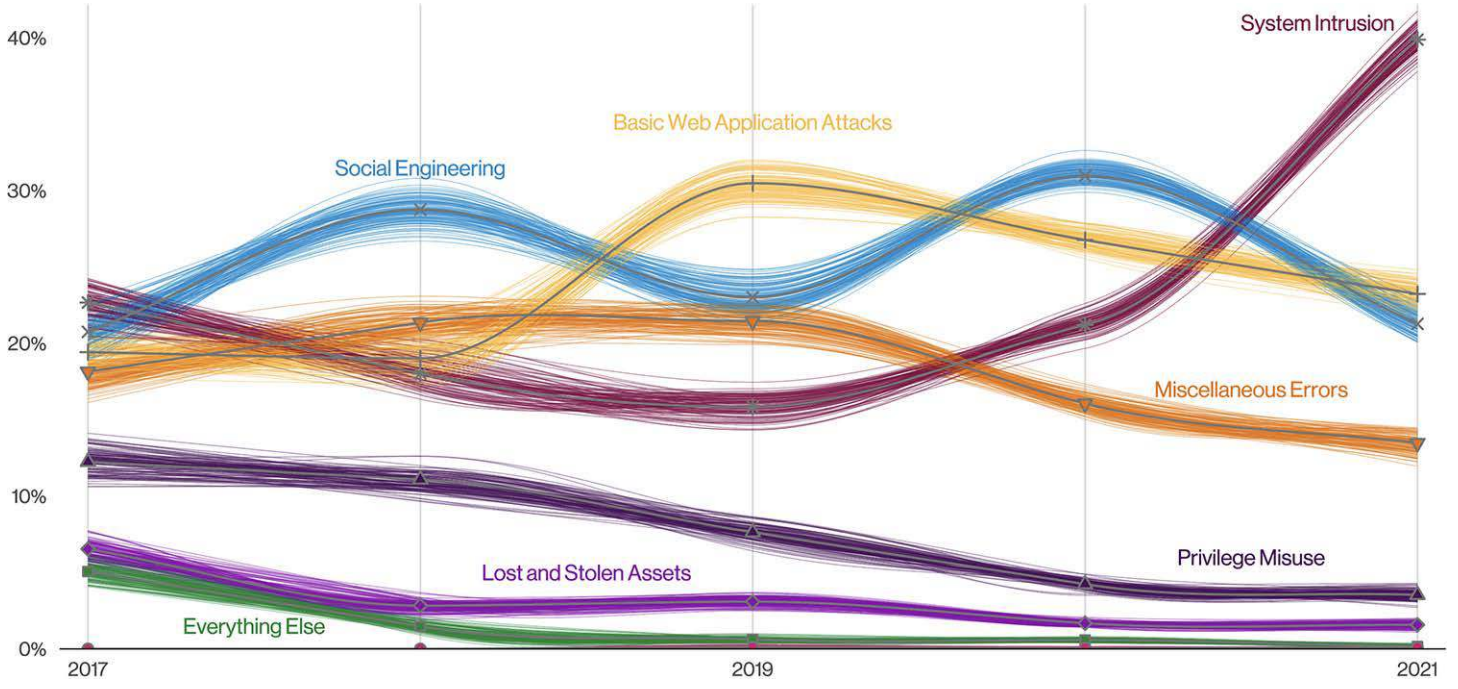


Figure 33. Patterns over time in breaches

System Intrusion

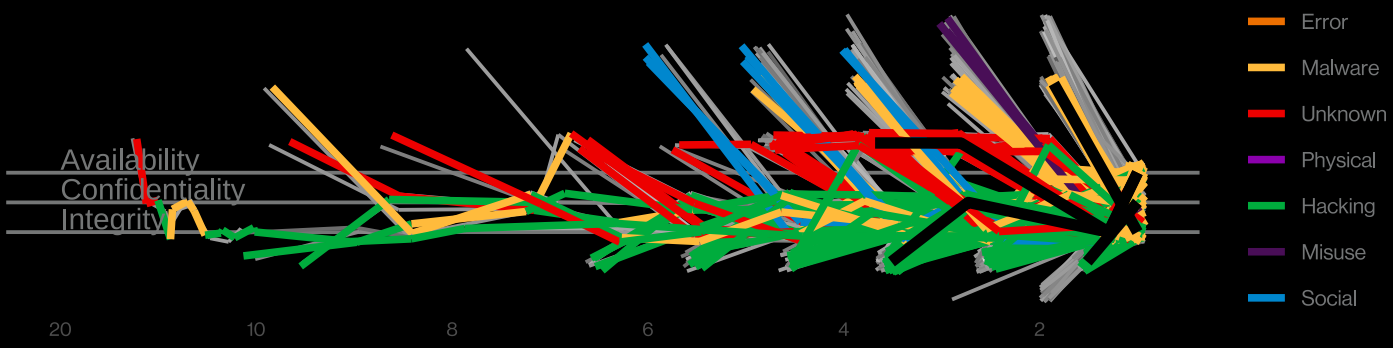


Figure 34. System Intrusion incident paths (n=228)

It's complicated

Although we have defined the System Intrusion pattern earlier in the report, a good example may be called for. When you think of Advanced Persistent Threat (APT) or some other form of capable actor moving across the environment popping shells, dropping malware, dumping creds and doing all the fun stuff you would expect from an unexpected Red Team exercise, that's System Intrusion.

Summary

This pattern consists of more complex breaches and attacks that leverage a combination of several different actions such as Social, Malware and Hacking and is where we find Supply Chain breaches and Ransomware, both of which increased dramatically this year.

What is the same?

This pattern continues to see the Use of stolen credentials and malware, such as Ransomware, as the top concerns.

Frequency	7,013 incidents, 1,999 with confirmed data disclosure
Threat Actors	External (98%), Internal (2%) (breaches)
Actor Motives	Financial (93%), Espionage (6%) (breaches)
Data Compromised	Credentials (42%), Personal (37%), Other (35%), Internal (16%) (breaches)

From a look at our data this year, it would appear that defenders have faced many challenges, particularly with rises in Ransomware and threats originating from partners (including vendors).

To better understand this pattern, let's take a look into the action varieties and vectors that make up the incidents. Figure 35 shows the top Action varieties with Backdoor (provided by the malware) and Ransomware competing for the top spot, followed by Use of stolen credentials. With regard to vectors, in Figure 36, we see Partner and Software update (shocker!) as the leading vectors for incidents. This is primarily attributed to one very large and very public security incident that happened last year. We'll give you a hint, it rhymes with "PolarShins." Please see "Partners, Supply Chains and 3rd parties, oh my" for more information. However, if we look past the Partner and Software update varieties, we find that 14% of incidents involved Desktop sharing software as one of the main vectors, followed by Email at 9%.

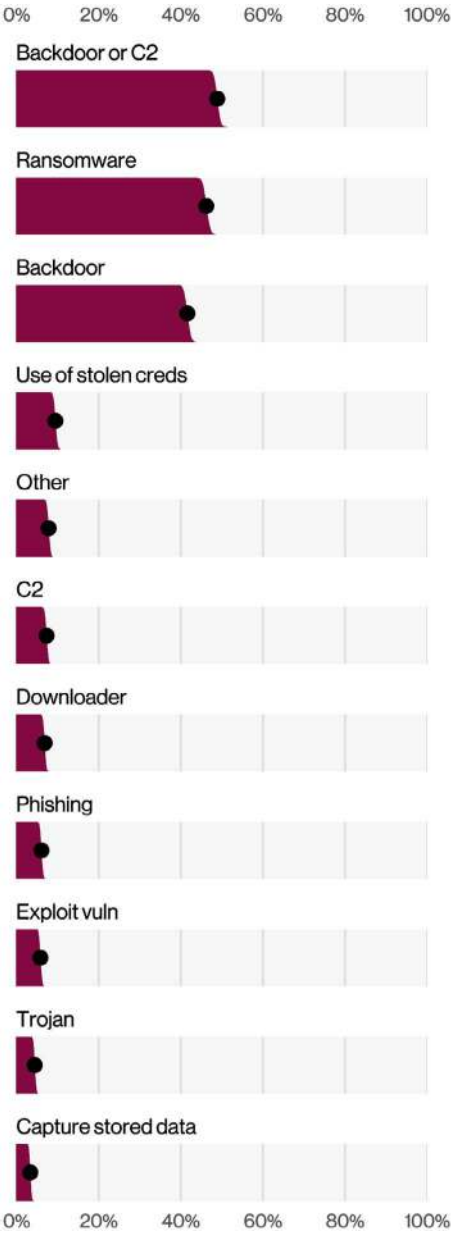


Figure 35. Top Action varieties in System Intrusion incidents (n=5,212)

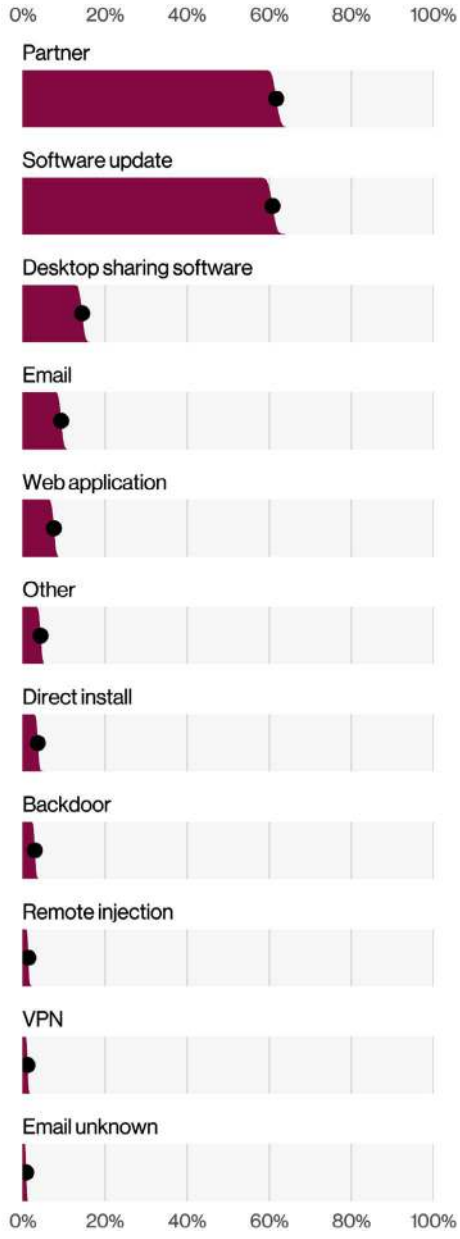


Figure 36. Top Action vectors in System Intrusion incidents (n=3,403)

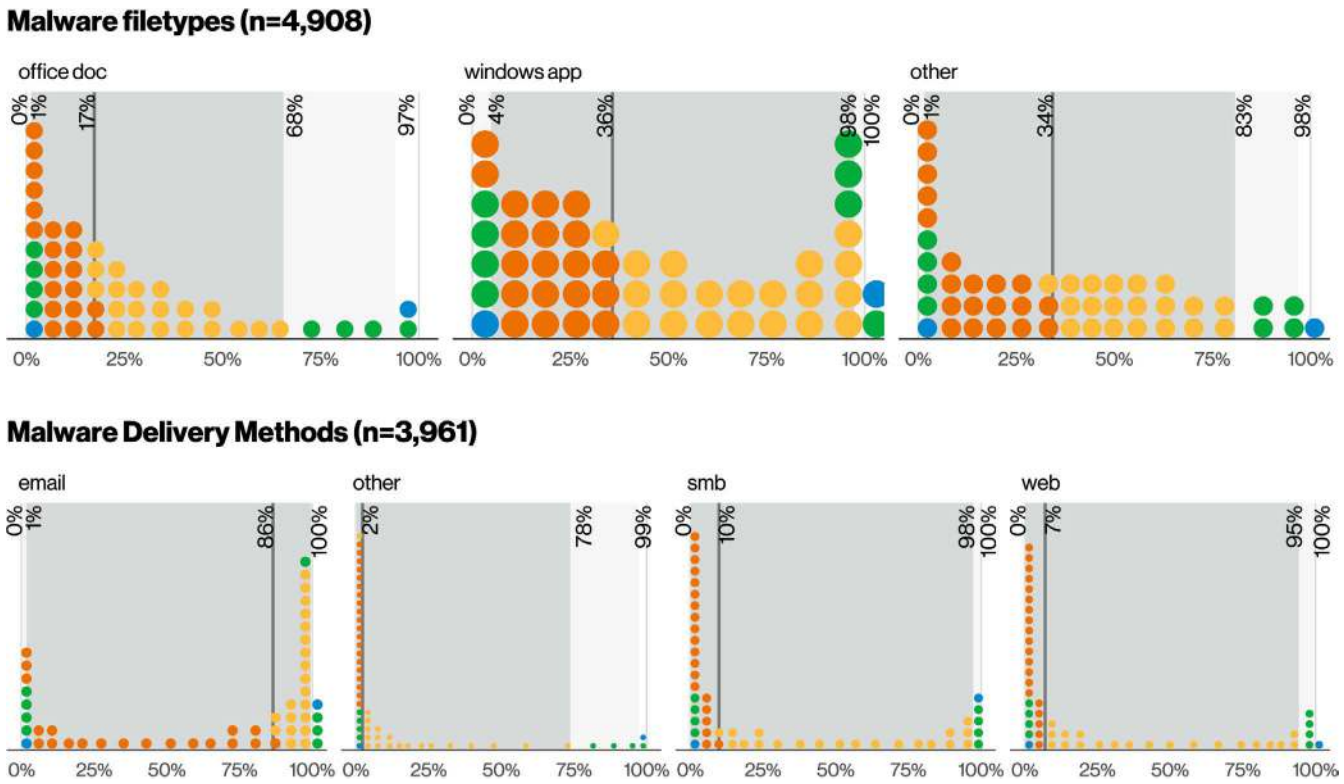


Figure 37. Malware delivery method proportion per organization

Figure 37 captures the distribution of file types along with the distribution of the delivery methods. It seems that the common route of office docs and emails[8] are still the tried-and-true method for delivering those initial payloads, which can then be used for further naughty deeds such as Ransomware deployment.

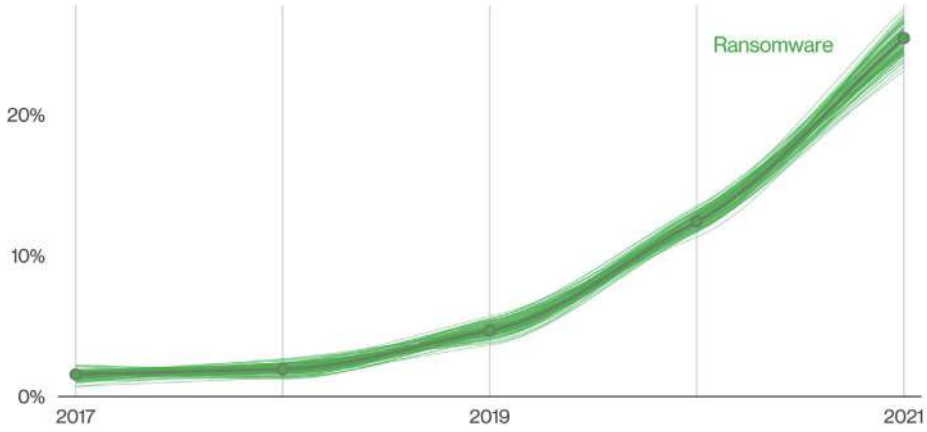


Figure 38. Ransomware over time in breaches

Rampant Rampaging Ransomware

This section is the perfect sequel to last year's finding of Ransomware dramatically increasing (unlike my Unamused Baboons NFT's value). That trend has continued with an almost 13% increase this year (an increase as large as the last five years combined).

Keeping in mind that while insidious, Ransomware alone is simply a model of monetization of a compromised organization's access that has become quite popular. Ransomware operators have no need to look for data of specific value, e.g., credit cards or banking information. They only need to interrupt the organizations' critical functions by encrypting their data.

8 With the median organization receiving over 75% of its malware via email.

Ransomware routes

While Ransomware comes in a variety of different flavors with catchy and not so catchy names, the way that Ransomware makes its way onto a system isn't quite as diverse. In Figure 39 you can see the pairings of the Actions to their respective vectors which are used to deploy Ransomware. There are a couple of key points to consider: 40% of Ransomware incidents involve the use of Desktop sharing software and 35% involved the use of Email. There are a variety of different tools the threat actor can use once they are inside your network, but locking down your external-facing infrastructure, especially RDP and Emails, can go a long way toward protecting your organization against Ransomware.

When we examine the types of malware blocked, we find that Droppers are typically the second most common. This aligns well with Email being such a prevalent entry point. If attackers have credentialed remote access, they can leverage that directly. Otherwise they must make their own remote access by emailing either malicious links or attachments.

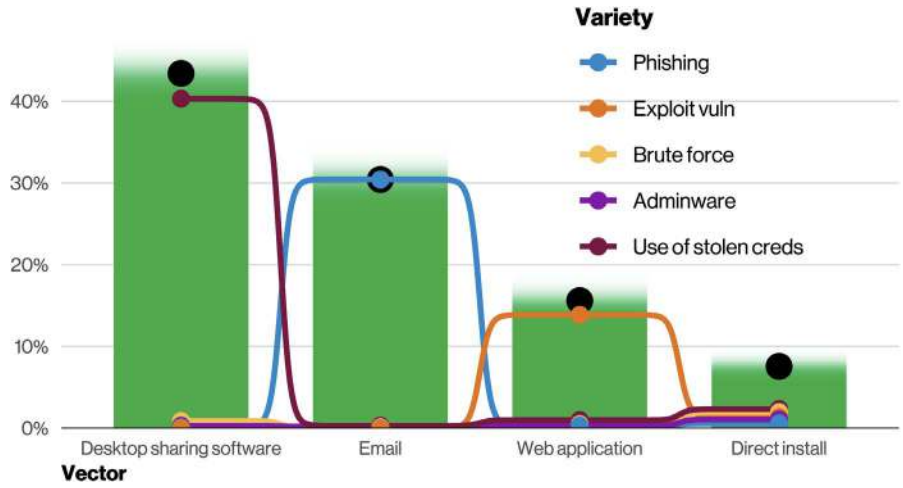


Figure 39. Select action varieties within vectors in System Intrusion Ransomware incidents (n=1,032)

Looking Back: Ransomware

Even though the first Ransomware case occurred when at least one of the current authors was still in diapers (1989), it took quite a while for it to become a mainstay in the DBIR. The first case of Ransomware showed up in our data in 2008 and it wasn't until 2013 that we had sufficient data to write something about it. And we quote:

"When targeting companies, typically SMBs, the criminals access victim networks via Microsoft's Remote Desktop Protocol (RDP) either via unpatched vulnerabilities or weak passwords. Once they've gained initial access they then proceed to alter the company's backup so that they continue to run each night but no longer actually backup any data." (2013 DBIR page 31)

Had we known that what was true nine years ago would still be true today, we could have saved some time by just copying and pasting some text. Oh well, maybe in another nine years things will change for the better.

Partners, Supply Chains and 3rd parties, oh my

For anyone who deals with supply chains, third parties and partners, this has been a year to remember. For those who need a quick recap, 2020 ended[9] (sadly, soon after the data collection window for the 2021 report) with a bit of a bang as a massive espionage campaign was discovered by our intrepid friends in the cybersecurity community. This event kicked off a complex, grueling and herculean effort to identify the potential victims impacted by the supply chain breach. While we typically don't examine individual events, but restrict our attention to the larger trends, this one incident alone had a tremendous effect in the industry and impacted our dataset in some surprising ways. One only need glance at Figure 36 to see just how severe an influence this one incident had on our System Intrusion pattern: skyrocketing Software updates moved Partner from its previous position as somewhat of a novelty (formerly showing up in less than 1% in our data) to an astounding 60% of incidents. However, while this incident might seem like an anomalous one-off, it may actually be representative of larger trends that we've been seeing in the industry, in terms of the interconnected risks that exist between the vendors, partners and third parties we work with on a daily basis.[10]

To understand the big picture of these breaches, we need to define Third-party and Supply chain breaches and that can be a bit complex. First of all, we should caveat that we code our incidents based off of the victim. Therefore, it is typically (though not always, of course) one victim, one incident. However, that fails to capture the interconnected nature of real-world environments when discussing Supply Chain and Third-party breaches. Over time we added fields that would assist to capture breaches with "secondary victims" that were impacted by the initial breach.

We define Third-party breaches as a single breach that compromised a Third-party. In our data, this is when the data owner is different from the breached victim. An example would be a datacenter that suffered a ransomware incident which encrypted their customer's data. While their customer's internal infrastructure was never directly breached, they were certainly impacted.

In our 2022 dataset we found that Third-party breaches represent a small percentage (1%) of our breach data. Nevertheless, we can still find some interesting data points. For example, within these Third-party breaches, we found the Use of stolen credentials along with Ransomware as two of the top five action varieties.

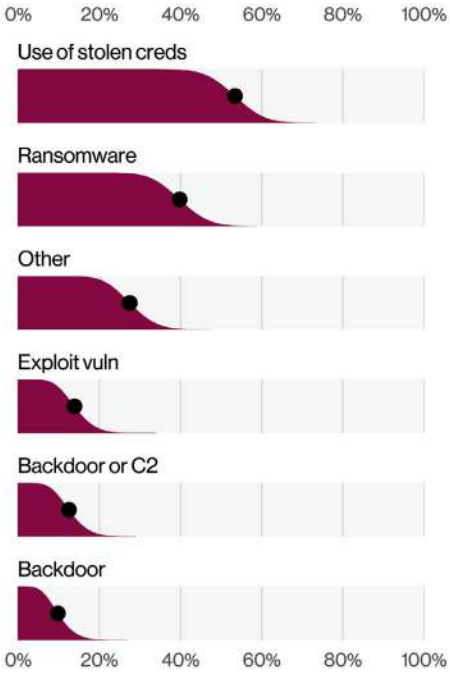


Figure 40. Top Action varieties in third-party incidents (n=73)

9 I mean, we're told it ended. We can neither confirm nor deny, as we are still in our bunkers awaiting the imminent arrival of Ragnarök.
10 The timeline section talks about value chains and event chains, which are both part of the attacker Circle of Breach.

The next type of incident vector is the Supply Chain. We define Supply Chain breaches as a sequence of one or more breaches chained together. In our data this may be a breach where there are secondary victims (when seen from the primary victim's breach) or where a partner was the vector (when seen from the secondary victim's breach). Another common example would be when a compromised software vendor is used to push a malicious update to an organization resulting in a breach, or a generic partner breach where a partner is compromised and either a set of credentials or some trusted connection is used to gain access.

After the major events of last year, these types of incidents account for 9% of our total incident corpus and 0.6% of our breaches this year. Due to the major event in 2021 in which a large network administration tool was compromised and used to push a backdoor to compromised servers, we see an extremely high rate of Backdoor[11] in the action varieties. However, there are still other noteworthy items within those remaining percentages such as Ransomware, Use of stolen credentials and other forms of malware with the capabilities you might expect to see. We have encountered cases of Supply Chain attacks in previous reports, reminding us that even if it's not a frequently used tactic each year, there is an established precedent for these attacks.

Ending remarks

When large-scale events like those we experienced in 2021 happen, they can shake our confidence in our abilities to protect ourselves. However, it is important to keep in mind that the close collaboration between federal security organizations and the cybersecurity community resulted in the detection and remediation of this event within a few months rather than years. While we do not have sufficient information to know whether or not the perpetrators considered it a successful operation, we can say that as an industry and as a community, we were ultimately successful in sharing resources and protecting each other from a complex threat. Thank you to everyone that stepped up and assisted in this effort. You deserve a drink of your choice and the DBIR team would be happy to raise a glass with you.

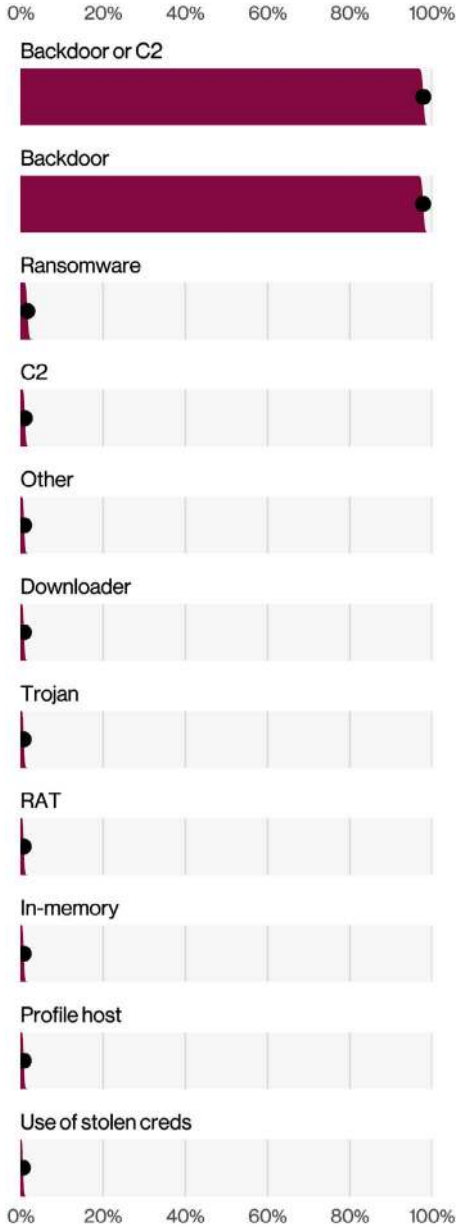


Figure 41. Top varieties in Supply Chain incidents (n=2,103)

11 And because "Backdoor or C2" contains backdoor, we see a large amount of it as well.

Scratching the surface

We discuss many things related to the human element in the DBIR: Phishing, Credentials, Errors, etc. However, this section is about the entry point into your organization that does not directly involve a human asset: Vulnerabilities.

The action variety of Exploit vulnerability is up to 7% of breaches this year, doubling from last year. While it's not on par with the massive numbers we see in Credentials and Phishing, it's worth some thought. The first question one might reasonably ask is "How are attackers finding these vulnerabilities?" As we pointed out last year, attackers have a sort of opportunistic attack sales funnel as seen in Figure 43. They start with scanning for IPs and open ports. Then they move to crawling for specific services. They then move on to testing for specific Common Vulnerabilities and Exposures (CVE). Finally, they try Remote Code Execution (RCE) to gain access to the system.

If attackers have this process for targeting organizations, what do they find? In Figure 42 we found sets of organizations in four different categories with about 100 organizations in each: Secure (or at least actively trying to be secure), Ransomware (organization with a disclosed ransomware incident), Random (organizations chosen purely at random) and Breached (organizations that had suffered a breach). We looked at how many vulnerabilities they had per host on average.[12]

What we found is the median company in all categories had almost no vulnerabilities (with random organizations being just a bit higher). This can happen because so many breaches aren't tied to vulnerabilities.

However, the tails of the distribution tell a different story. While security-concerned organizations run a pretty tight ship, the other three have organizations out in the tail with far more vulnerabilities per internet-facing host. And if you wonder who the threat actors from Figure 43 are looking for, it's the organizations in that tail. Remember that for many attackers it's simply a numbers game—they just want some amount of access—and those tails still provide enough of an incentive for them to continue to try the exploits until they get lucky.

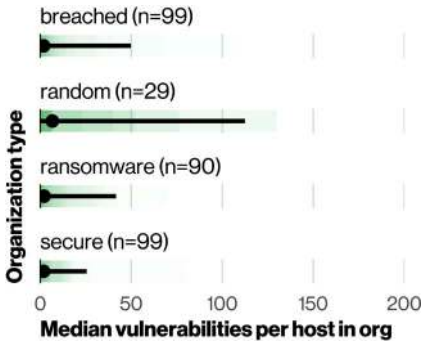


Figure 42. Vulnerabilities per host by organization type (only organizations with internet presence represented)

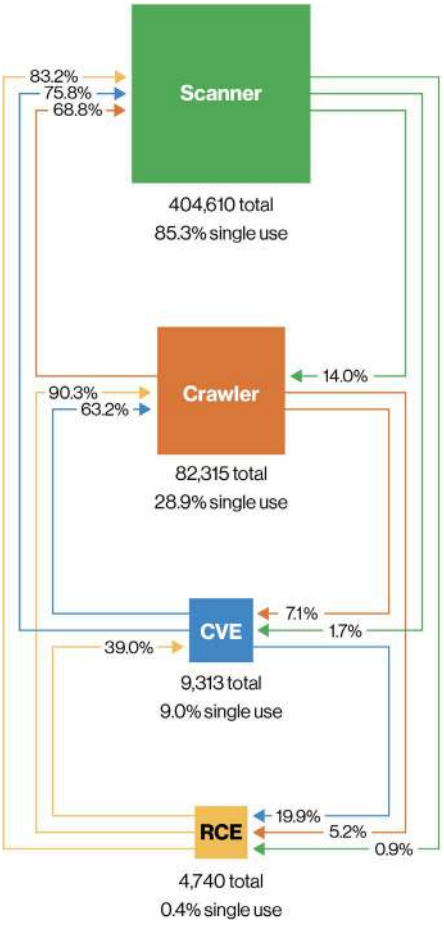


Figure 43. Threat actor opportunistic sales funnel

12 And by average, we mean median because statistics isn't hard enough already. Mode.

The good news is we are getting better. Figure 44 shows vulnerability remediation speed and completeness over the past six years. Higher is better in this figure and, in general, things are looking up. We're patching more and we're patching faster.

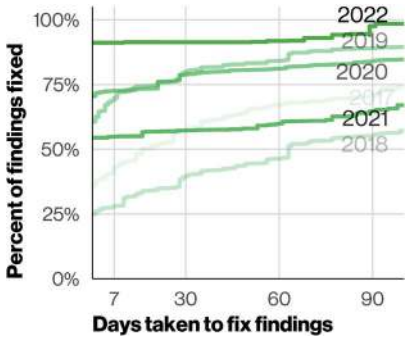


Figure 44. Time to remediate findings

Another bright spot is that last year we talked about Gini coefficients, (basically a measure of if a few things happened a lot and a lot of things happened only a few times). We apply that in Figure 46 to the different levels of the Pyramid of Pain. For the non-threat intelligence expert, the Pyramid of Pain[13] is a model used by threat intelligence analysts to categorize the value of different indicators to the defender. The base of the pyramid is trivial for the attacker to modify (like the hash of a file) and therefore less useful to the defender. The tip of the pyramid is extremely difficult to modify by the attacker (like the attacker's established process also known as Tactics, Techniques and Procedures [TTPs]).

What we found was that other than hashes, most indicators in the Pyramid of Pain have pretty high Gini coefficients. That means that if you block the first few percent of that indicator, you stop most of the malice. Frankly we expected that the Gini coefficient would go up as we went up the pyramid, but from IP addresses on up, they are all about the same. We see something similar with IPs back in Figure 43. Only 0.4% of the IPs that attempted RCEs weren't seen in one of the prior phases showing what SecOps probably already know: Block bad IPs!

You may notice we didn't get the TTPs at the top of the pyramid. The reality is the DBIR team just doesn't have this data. But check out Appendix B: VERIS & Standards for Attack Flow: a solution to this data collection problem!

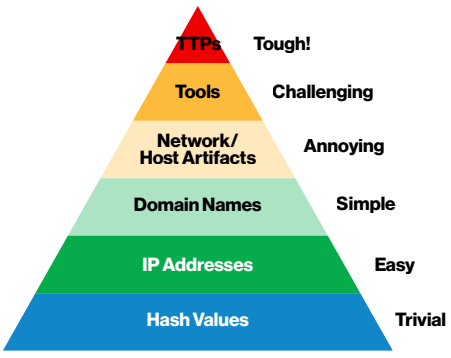


Figure 45. Pyramid of Pain

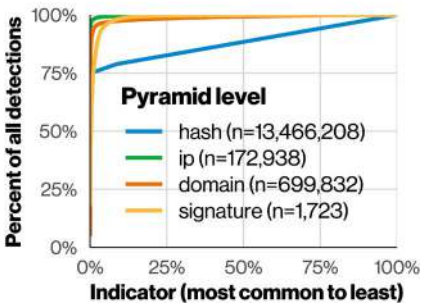


Figure 46. Cumulative sum of indicators

13 "The Pyramid of Pain," Bianco, David J., https://bit.ly/PyramidOfPain, January 2014.

Social Engineering

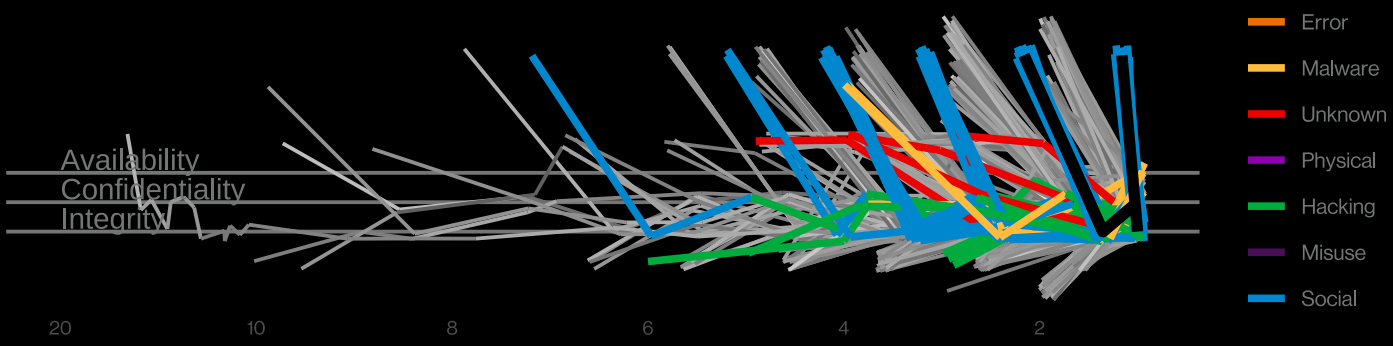


Figure 47. Social Engineering incident paths (n=75)

How is this my fault?

This year, 82% of breaches in the DBIR[14] involved the human element. This puts the person square in the center of the security estate with the Social Engineering pattern capturing many of those human-centric events.

Summary

The human element continues to be a key driver of 82% of breaches and this pattern captures a large percentage of those breaches. Additionally, malware and stolen credentials provide a great second step after a social attack gets the actor in the door, which emphasizes the importance of having a strong security awareness program.

What is the same?

These attacks continue to be split between Phishing attacks and the more convincing Pretexting attacks, which are commonly associated with Business Email Compromises.

Frequency	2,249 incidents, 1,063 with confirmed data disclosure
Threat Actors	External (100%), (breaches)
Actor Motives	Financial (89%), Espionage (11%), (breaches)
Data Compromised	Credentials (63%), Internal (32%), Personal (24%), Other (21%) (breaches)

14 Not just the Social Engineering pattern.

As you can see in Figure 49, the Social Engineering pattern is dominated by Phishing. And we know what you're going to say: "I'm so surprised! Fetch my fainting couch!"

But in a way the chart highlights the numerous paths a social engineering breach can take. We see where the phish steals credentials to then be used in "Use of stolen creds." We see Business Email Compromises (BECs) (with the E for email being directly tied to the phish) in "Pretexting." We see malware being dropped in "Downloader" and "Ransomware" (which, by the way, goes up to 17% of Social Engineering when we are discussing incidents rather than breaches), hacking in "Scan network" and "Profile host," and persistence in "Backdoor or C2." All in all, it highlights the fact that phishing is one of the four main entry points into an organization.[15]

Phishing

Sutton's law tells us "When diagnosing, first consider the obvious." Thus, if you wonder why criminals phish, it is because email is where their targets are reachable. And while only 2.9% of employees may actually click on phishing emails, a finding that has been relatively steady over time, that is still more than enough for criminals to continue to use it. For example, in our breach data alone, there were 1,154,259,736 personal[16] records breached. If we assume those are mostly email accounts, 2.9% would be 33,473,532 accounts phished, (akin to successfully phishing every person in Peru).

The good news is we are getting better at reporting phishing. Figure 48 shows a steady climb with an increase of roughly 10% in phishing test emails reported in the last half decade. The question is "Can your organization both act on the 12.5% that reported and find the 2.9% that clicked?"

BEC

In Figure 49, we see that Pretexting is 27% of Social Engineering breaches, almost all of which are BECs. While we call these attacks BECs, they tend to be a bit more complex than just some bad actor impersonating someone through a compromised email account. Only 41% of BECs involved Phishing. Of the remaining 59%, 43%[17] involved Use of stolen credentials against the victim organization. The percentage remaining were most likely BECs using an email from a partner, or utilizing a free email account of some type requiring no "C"[18] at all. BECs come in many forms: your organization may be targeted due to a breach in a partner, your partners may be targeted due to a breach of your emails, you may be breached and then targeted using your own breach, or as pointed out earlier, there may be no breach at all, just an attacker with a convincing story about why they need your money.

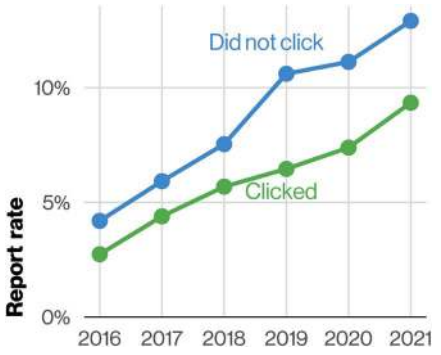


Figure 48. Phishing email report rate by click status (n=295,825,679)

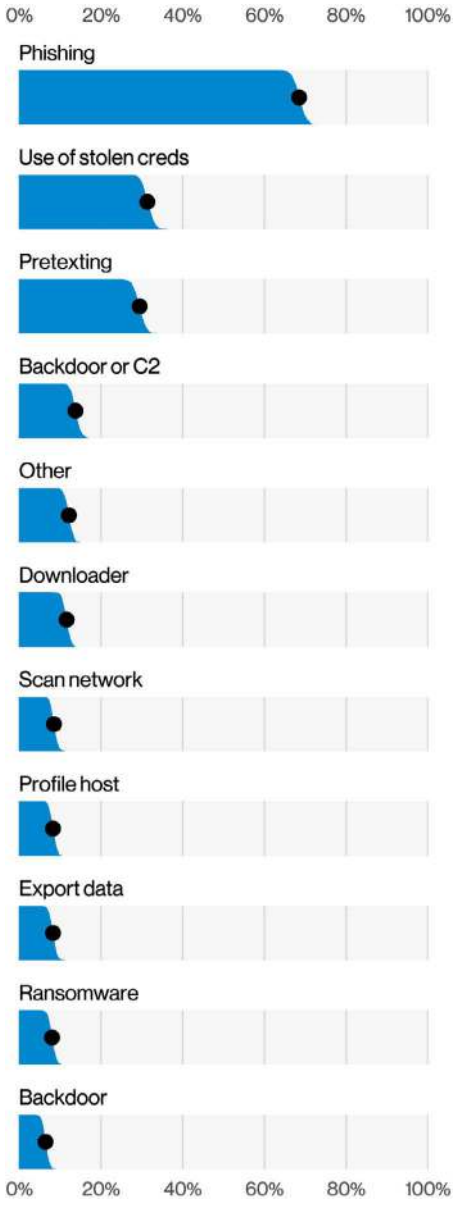


Figure 49. Action varieties in Social Engineering breaches (n=1,063)

15 Along with Credentials, Vulnerabilities and pre-existing Bots.

16 "Personal" doesn't have to be email. It could be addresses and names and such, but it normally includes email. And this doesn't even count credentials where the username is often an email.

17 Ok, so 59% times 43%, carry the 1, convert to roman numerals … that's like 25% of all BECs!

18 Compromise.

Figure 50 gives an idea of how much of that money the criminals feel they need. It appears they saw inflation on the horizon and granted themselves a raise this year. Regardless, you, being the erudite reader of the DBIR that you are, can do something about it. File a complaint at ic3.gov and get in touch with the FBI IC3 Recovery Asset Team (RAT). In cases where the RAT acts on BECs, and works with the destination bank, half of all U.S.-based BECs had 93% of the money either recovered or frozen, whereas only 14% had nothing at all recovered.

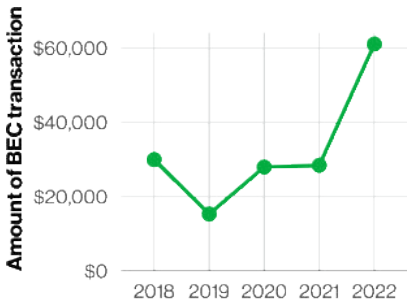


Figure 50. Median transaction size for BECs (n=50,342). Based on FBI IC3 complaints where a transaction occurred.

Malware

"Malware? I already read about it in the Action section. Why do I have to hear about malware again?!" Because there's lots of it! Although, we admit there is a degree of bleed-over in the sections. This year we saw more things that fell into two patterns than we did last year. With System Intrusion and Social Engineering being chief among them.

As Figure 37 in the System Intrusion section points out, email is the most common malware delivery method, at least initially. Figure 52 shows that, in breaches, providing a Backdoor or Command and Control (C2), followed by delivering a Downloader are the top two things actors are looking to do once their successful phish lands their malware. If the phish busts through the door, Figure 52 shows that the Backdoor, C2 and Downloader hold it open for all the rest of the actions to make their way in. It is noteworthy that while Ransomware shows up about halfway down the list in breaches, the same analysis for incidents has Downloader and Ransomware moving into the top two spots with 74% and 64% of malware incidents respectively. This definitively proves that we can't write a single section of the DBIR this year without mentioning Ransomware at least once.

Training

Clearly the Human Element leaves a lot to be desired when it comes to information security. Even when a breach is not directly caused by a person, the information systems were still built by people.[19] Frankly, we'd rather have people solving the problems since asking the AI to do it sounds much trickier.

Unfortunately, nothing is perfect. Not people, not processes, not tools, not systems.[20] But, we can get better, both at what we do and what we build. To that end, training is a big part of improving. Figure 51 gives an idea of the amount of phishing training folks are taking per year. Most training takes twice as long to complete than was expected, with 10% taking three times as long. Training can potentially help improve security behaviors, in both day-to-day (such as Don't Click ... Stuff, and using a password keeper) as well as in design (such as secure coding, lifecycle management, etc.). Unfortunately, while getting training is easy, proving it's working is a bit harder. If you want some pointers on how to do it, have a look at Appendix C: Changing Behavior.

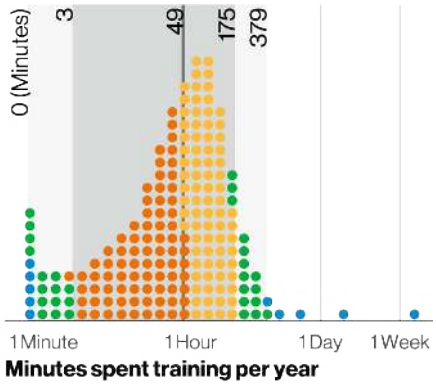


Figure 51. Minutes per year spent on training per person (n=45,372, log scale)

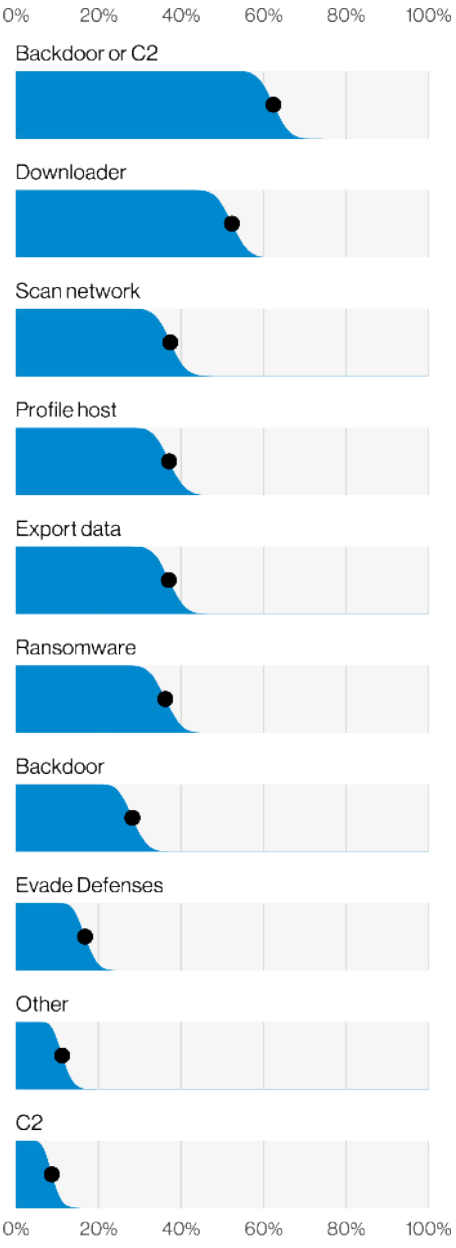


Figure 52. Top Malware varieties in Social Engineering breaches (n=235)

19 Unless that whole bigfoot thing is true. We sent Dave to a conference to find out but haven't heard back.
20 Not DBIR authors (this is debatable. We asked the Oracle, rolled some bones, and signs pointed to "probably perfect").

Basic Web Application Attacks

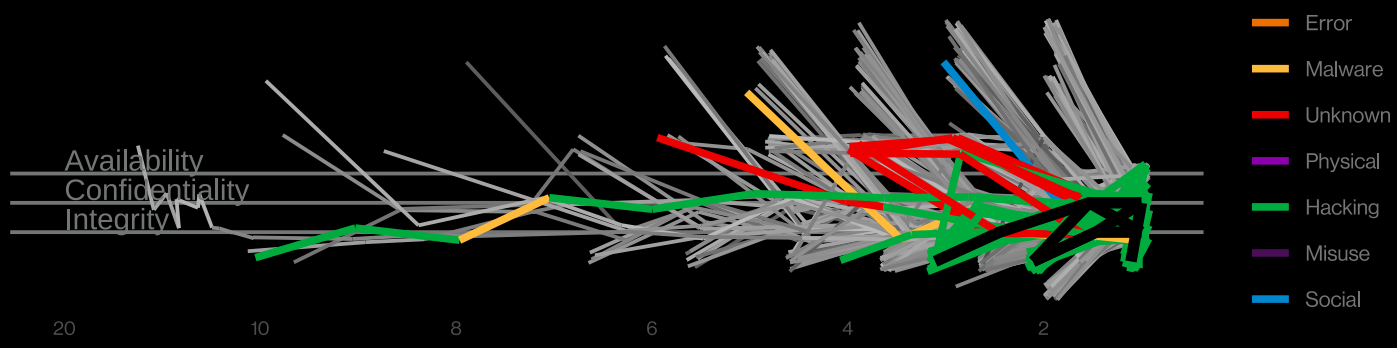


Figure 53. Basic Web Application Attacks incident paths (n=92)

Does this make my infrastructure look big?

In Basic Web Application Attacks (BWAA), we are largely focusing on attacks that directly target an organization's most exposed infrastructure, such as Web servers. These incidents leverage one or the other of two entry points, the Use of stolen credentials or Exploiting a vulnerability.

Summary

Attacks within this pattern are split between two areas. The means of accessing the server, such as using stolen credentials, exploiting vulnerabilities and brute forcing passwords constitutes the first. The second represents the specific payload, such as backdoors, which are used to maintain persistence or monetize access.

What is the same?

This pattern continues to largely be dominated by the Use of stolen credentials to access an organization's internet-facing infrastructure, like web servers and email servers.

Frequency	4,751 incidents, 1,273 with confirmed data disclosure
Threat Actors	External (100%) (breaches)
Actor Motives	Financial (65%), Espionage (31%), Grudge (2%), Ideology (1%) (breaches)
Data Compromised	Personal (69%), Credentials (67%), Other (29%), Medical (15%) (breaches)

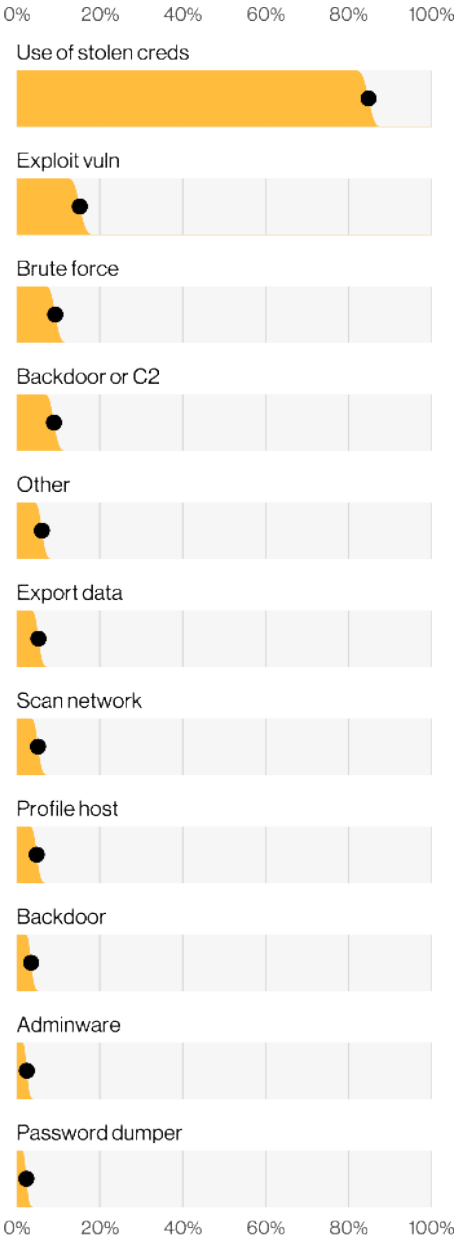


Figure 54. Top Action varieties in Basic Web Application Attacks breaches (n=962)

Hopefully, Figure 54 demonstrates the importance of proper password protection since over 80% of the breaches in this pattern can be attributed to stolen credentials. Figure 55 reveals the larger trends in terms of using stolen credentials vs exploiting vulnerabilities. There's been an almost 30% increase in stolen credentials since 2017, cementing it as one of the most tried-and-true methods to gain access to an organization for the past four years.

Figure 55 clearly displays how the vast majority of incidents involving Web application are using stolen credentials. There is a sprinkling of other vectors in Figure 56, such as Backdoor (useful after you have a foothold), Remote injection (how malware gets on the system after an exploited vulnerability) and, of course, Desktop sharing software.

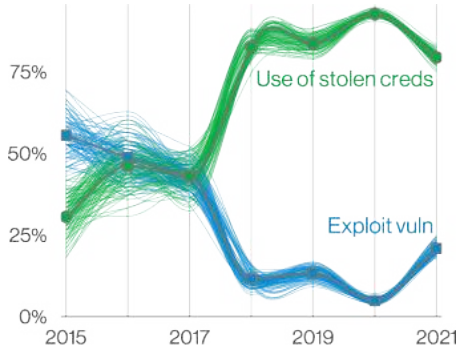


Figure 55. Exploit vuln vs Stolen creds over time in Basic Web Application Attacks breaches

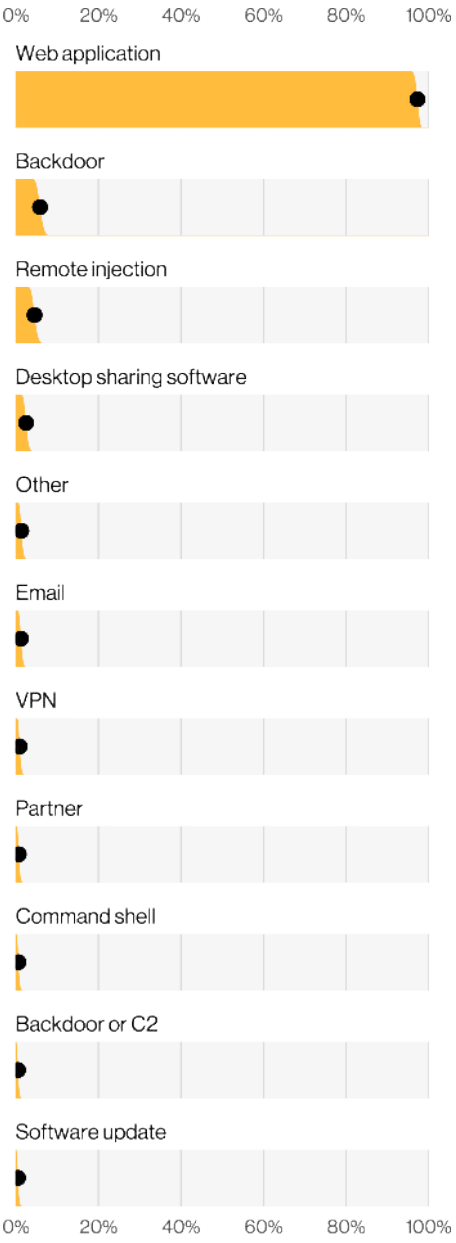


Figure 56. Top Action vectors in Basic Web Application Attacks breaches (n=972)

Mail servers under attack

With regard to what is being targeted, Figure 59 captures the high prevalence of Web application (which seems obvious based on the title of the section) but also of Mail servers, which represented less than 20% of the total breaches in this pattern. Of those Mail servers, 80% were compromised with stolen credentials and 30% were compromised using some form of exploit. While this 30% may not seem like an extremely high number, the targeting of mail servers using exploits has increased dramatically since last year, when it accounted for only 3% of the breaches.

Basic != not useful

One might be forgiven for assuming that these types of attacks would largely be the work of enterprising criminals spraying the internet looking for weak credentials. However, it seems that Nation-state actors have also been leveraging this low-cost, high-pay-off strategy with over 20% of our BWAA breaches being attributed to Espionage. If the front door has a weak lock there is no reason to develop a complicated polymorphic backdoor with a fast flux network of C2 servers.

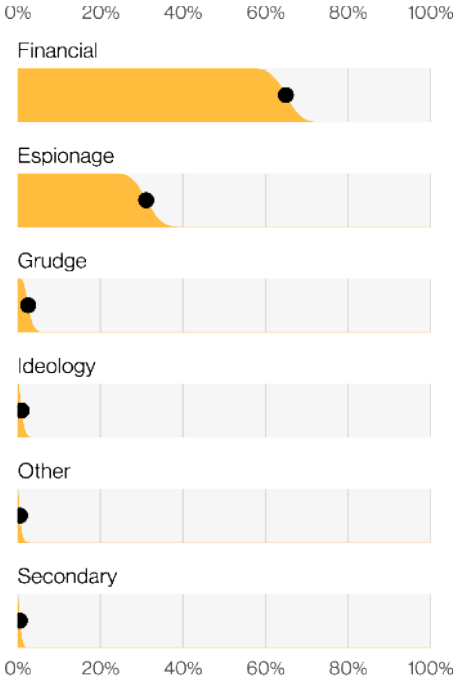


Figure 58. Top Motives in Basic Web Application Attacks breaches (n=251)

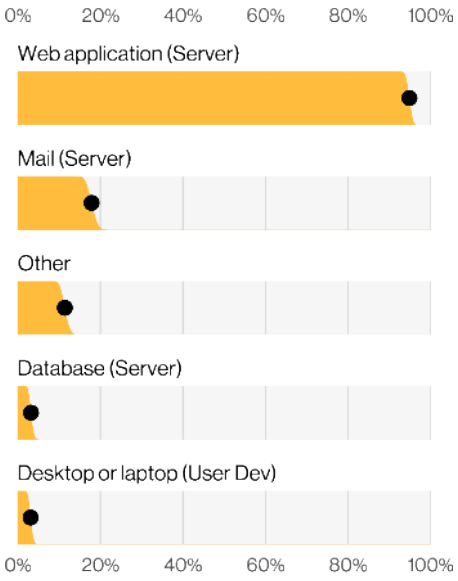


Figure 59. Top Asset varieties in Basic Web Application Attacks breaches (n=1,001)

Looking back:

Santayana tells us that "those who do not learn from history are doomed to repeat it." That seems to be the case, as we have continued to see poor password practices as one of the leading causes of data breaches dating back to 2009.

"From the chart, it is evident that many intrusions exploit the basic (mis)management of identity. Unauthorized access via default, shared, or stolen credentials constituted more than a third of the entire Hacking category and over half of all compromised records. It is particularly disconcerting that so many large breaches stem from the use of default and/or shared credentials, given the relative ease with which these attacks could be prevented."
(2009 DBIR page 17)

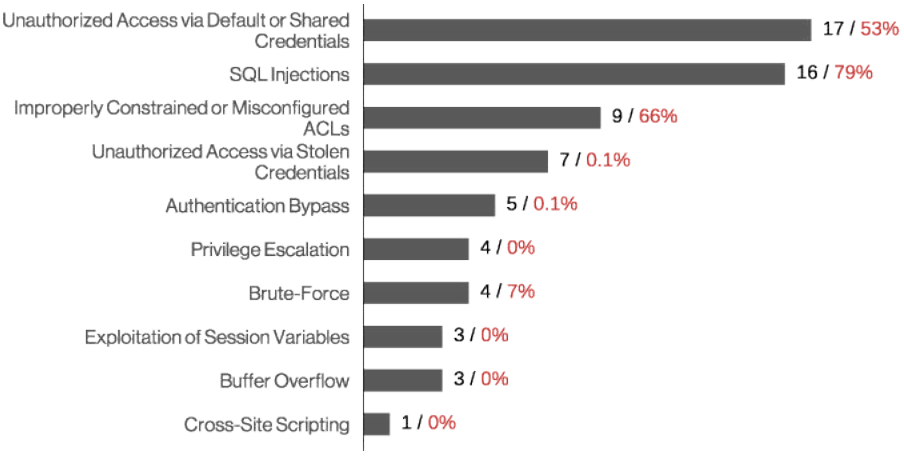


Figure 57. Types of Hacking by number of breaches (black) and percent of records (red) (2009 DBIR Figure 15)

Miscellaneous Errors

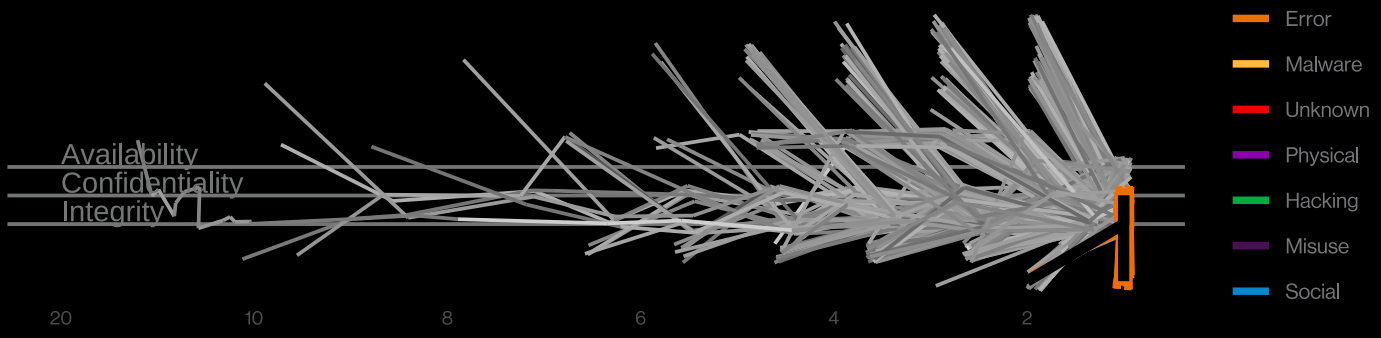


Figure 60. Miscellaneous Errors incident paths (n=32)

Misconfiguring the situation

While most patterns have changed over the years, one constant has been people making mistakes. In 2015, most mistakes were the Misdelivery of Media assets (Documents) while Misconfiguration accounted for less than 10% of breaches. This year, however, Misconfiguration and Misdelivery have converged.

Summary

While this pattern is by definition made up of either Internal or Partner actors, this year's data shows it is all about your employees. Misdelivery and Misconfiguration are the top two varieties. Misconfiguration is frequently paired with the Discovery Method of "Security Researcher."

What is the same?

People are still fallible, and that fallibility can cause data breaches.

Frequency	715 incidents, 708 with confirmed data disclosure
Threat Actors	Internal (100%) (breaches)
Data Compromised	Personal (81%), Other (23%), Medical (18%), Bank (8%) (breaches)

The rise of the Misconfiguration error began in 2018 and was largely driven by cloud data store implementations that were stood up without appropriate access controls. Many security researchers made a name for themselves by finding these exposed databases on the internet. Despite the efforts of the major cloud providers to make the default configurations more secure (which we applaud), these errors persist.

These days Misdelivery data breaches are frequently electronic in nature and consist of email going to the wrong recipients, although physical Documents do remain a problem to some degree.

The data types involved in these breaches are still overwhelmingly of the Personal variety. Medical and Banking information are occasionally involved, but they are not the norm. The data tends to be from customers, and it is also the customers who are notifying the breached organizations in a high number of cases. However, Security researchers are still the stars of this Discovery show (although their percentage is down from last year).

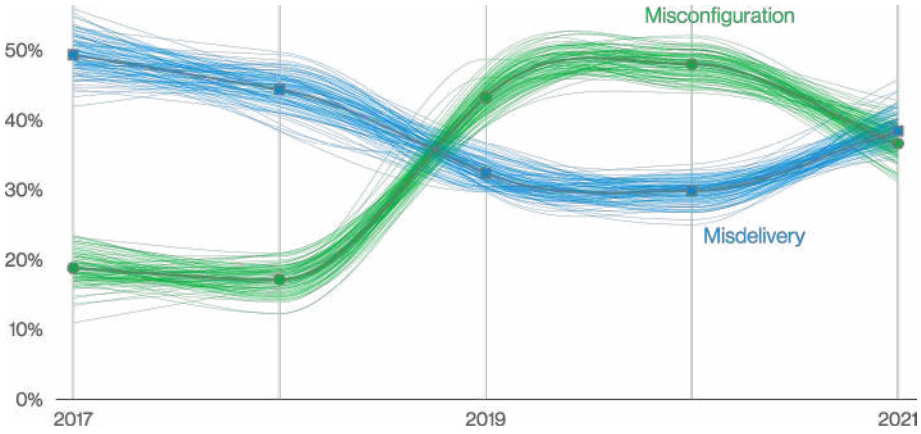


Figure 61. Top Action varieties over time in Miscellaneous Errors breaches

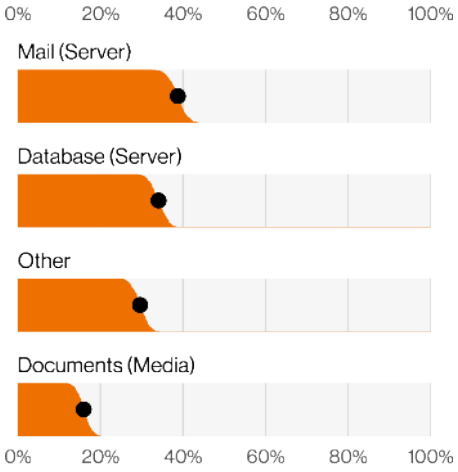


Figure 62. Top Asset varieties in Miscellaneous Errors breaches (n=513)

Denial of Service

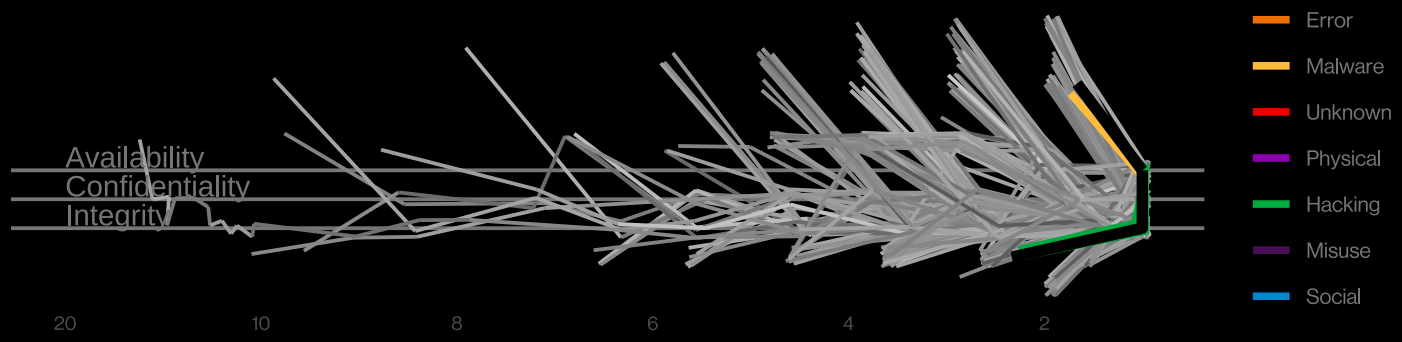


Figure 63. Denial of Service incident paths (n=3)

Heavy traffic ahead

Welcome to the Denial of Service pattern—one that is perhaps all too familiar to many of you, as it continues to be the top type of incident in our dataset. This pattern consists of those annoying attacks where botnets or compromised servers are leveraged in order to send junk data to target computers with the hopes of denying that service by creating a "traffic jam in the pipes."

Summary

While these attacks are a nuisance impacting a large range of organizations, some organizations face these attacks on a regular basis which may potentially impact their business function.

What is the same?

Denial of Service continues to be one of the most common types of cybersecurity incidents.

Frequency	8,456 incidents, 4 with confirmed data disclosure
Threat Actors	External (100%) (incidents)

These types of irksome incidents aren't isolated to any one industry. As Figure 64 demonstrates there are a wide range of companies from Information Services, Professional Services, Manufacturing and Government (which happens to cover many of the industries we write about).

However, while they may be ubiquitous within industries, it does not mean that organizations in these industries are perpetually bombarded with DoS attacks. We found that the median Denial of Service attack lasted less than four hours (Figure 65) and that the vast majority of organizations that are monitored for these attacks experience less than 10 attacks a year. If, on the other hand, you're one of those unlucky 1% of companies that experience more than 1,000 DDoS attacks a year, you're already aware of this and most likely have a service to help you manage the traffic.

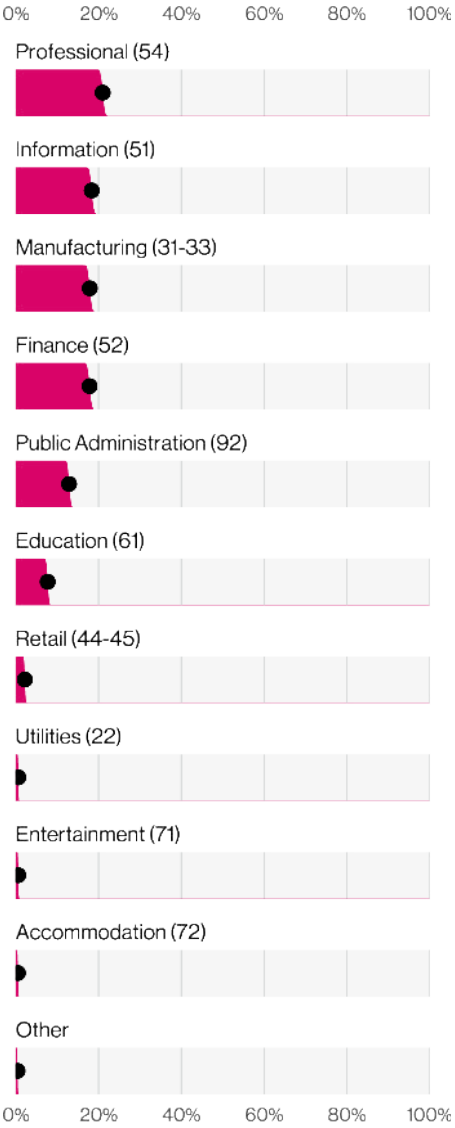


Figure 64. Top industries in Denial of Service incidents (n=8,330)

My, how big your DDoS have gotten

We first became acquainted with DDoS in the 2013 DBIR and it has since become a regular topic of discussion. It is interesting to look back and see how things have changed over the years. For 2013 era DDoS, the median attack was clocking in around 422 Mbps, with a very small number hitting the 100Gbps mark. By 2016, the median value was 1.1 Gbps (doubling from three years prior) and today the median is around 1.3 Gbps.

We can also see how DDoS has become narrowly centered. From 2013, through 2016, and on to 2021, DDoS has become tightly clustered around the median. We speculate[21] that back in 2013, DDoS attacks were ad hoc, whereas today's DDoS infrastructure is far more formalized and repeatable.

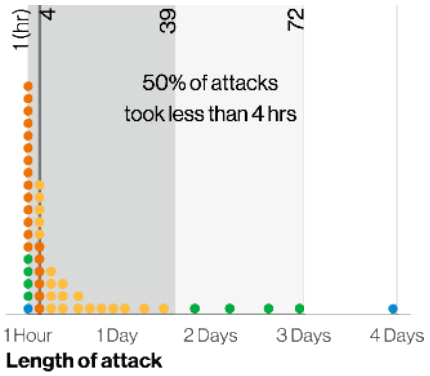
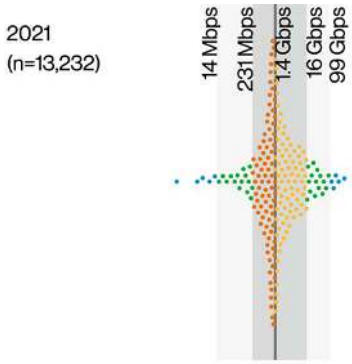
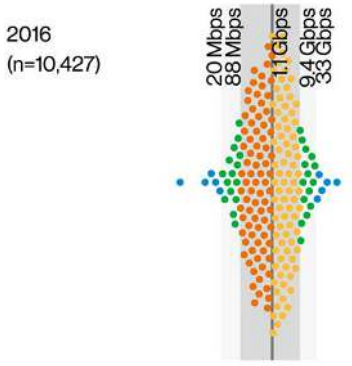


Figure 65. DDoS attack duration (n=15,059 log scale)





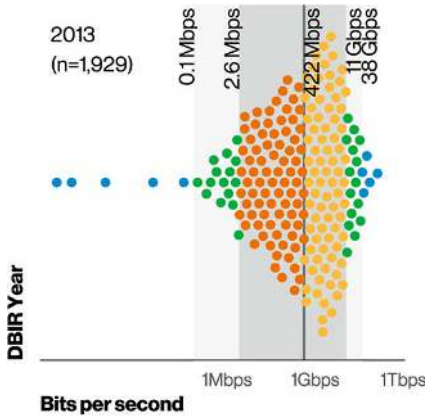


Figure 66. DDoS BPS over time (log scale)

21 Read "guess."

Lost and Stolen Assets

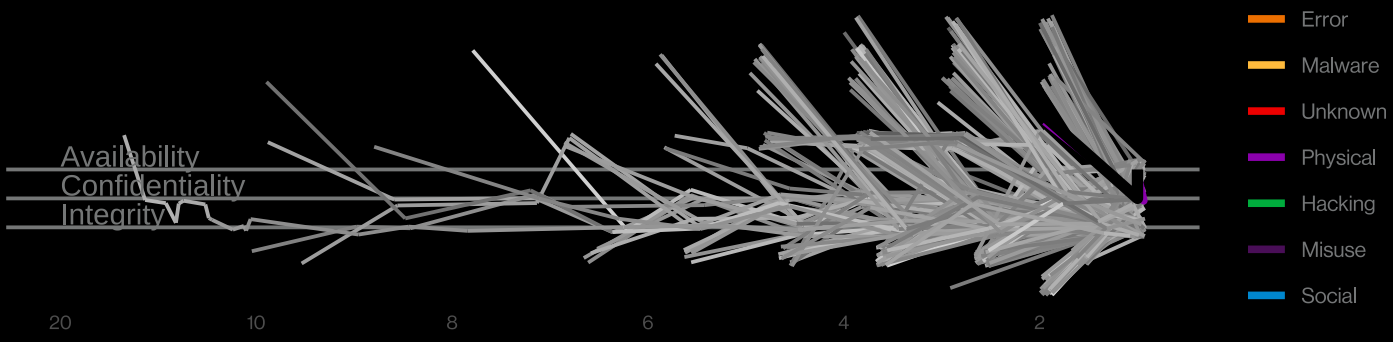


Figure 67. Lost and Stolen Assets incident paths

Losing it

In last year's report, we mentioned that for security incidents (not confirmed breaches), assets were far more likely to be lost by employees than stolen by someone who does not work for the organization. However, when looking at breaches, we see the opposite is true.

Summary

Most of the cases in this pattern are classified as "incidents" rather than "breaches, because the nature of the devices stolen makes it difficult to confirm data access. The prevalence of theft in this pattern is driven by the Financial motive—we believe many of the perpetrators of theft are committing the crime with the intention of an immediate payoff by selling the stolen asset.

What is the same?

The type of data affected by these incidents is the same (almost exactly) as last year. External actors typically perpetrate the thefts, while employees are responsible for losing track of their assets.

Frequency	885 incidents, 81 with confirmed data disclosure
Threat Actors	Internal (94%), External (6%) (incidents)
Actor Motives	Financial (98%), Ideology (2%) (incidents)
Data Compromised	Personal (77%), Medical (43%), Other (15%), Bank (9%) (incidents)

Stolen assets are more likely to be the causes of cases where we can confirm that data compromise occurred. Still, this is a pattern where most (approximately 90%) of the cases are classified as "security incidents" rather than "breaches," because confirming that the data was compromised is difficult based on the assets stolen.

We found it interesting that, despite the pandemic and the resulting lessening of travel, the Lost and Stolen Assets remained a common pattern in our dataset. It shows that if you entrust portable devices to employees, a certain percentage of them will either misplace their devices or leave them somewhere that they are vulnerable to theft. Leaving items in personal vehicles is a recurring theme in the data. People may just do it closer to home than before.

Figure 69 shows the devices most often lost or stolen. User devices (including desktops, laptops and mobile phones) are most frequently the type of item that is either lost or stolen. However, Documents still account for a good percentage of these breaches. This occurs most often in the Public Administration and Healthcare industries, which goes some way toward explaining the prevalence of Medical data compromised in these incidents. The government (of almost any country) administers large programs that manage health-related data, as of course do the members of the Healthcare industry. Industries that handle Protected Health Information (PHI) tend to have higher regulatory requirements for reporting breaches, and therefore we have better visibility into these events as well.

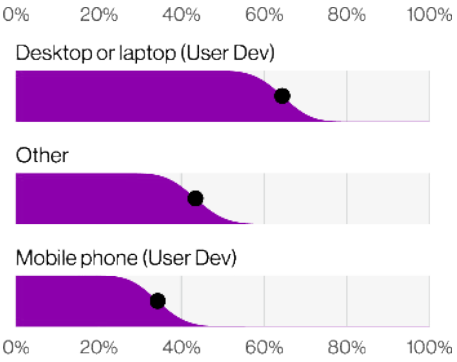


Figure 69. Top Asset varieties in Lost and Stolen Assets breaches (n=76)

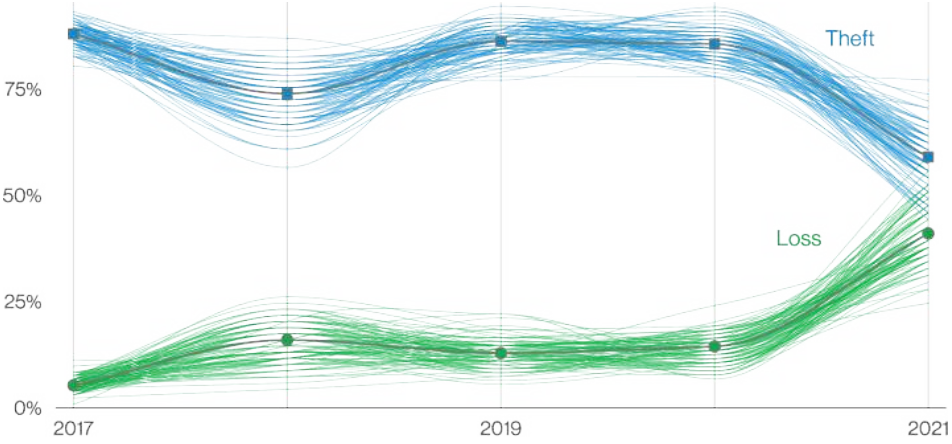


Figure 68. Top Action varieties over time in Lost and Stolen Assets breaches

Organic free-range data

Mobile data is something that appears only sparingly in our data, which seems ironic considering who we are.

Unfortunately (or fortunately), mobile phones hover around 1% or less in our breach dataset with the associated causes being somewhat random. This is likely due to bias in the data; when a phone is used to phish creds, it's likely the email server that gets reported, not the device used to access it. When we see breaches involving malware on mobile phones, it is not uncommon for the malware to be there to collect data. And if that's your goal, it helps to be quiet and not get caught, especially considering the difficulty it takes to get on the devices in the first place.

However, when we look at non-incident data, we get a clearer view of the role mobile plays in the security ecosystem. Figure 70 gives an idea of the threats that mobile phones see.

Only 42% of devices avoided blocking access to any URL while 84% of devices avoided an unwanted app. However that means the other 58% of devices had at least one malicious URL clicked and 16% of devices had at least one malware or riskware app installed. While that may not sound like a lot, a quick look at your Mobile Device Management console (or a company headcount) will tell you those numbers can add up rapidly.

And it's not just texts tempting the telephonic users. Phone honeypot data reveals that 5% of honeypots get at least one call a day, and we're about 90% sure the honeypots don't need to refinance their student loans or even own a car with an extended warranty (they prefer leasing). Figure 71 gives an idea about the content of those calls. About a third of them have little to no audio or are silent, which sounds to us[22] like vishing (voice phishing) for live numbers.

Another 29% are known scams (with 7% of the 29% known to be targeting businesses specifically) and the rest being other stuff or simply unknown.

Thankfully it's not as if the targeting of mobile devices is a big surprise to the security community. Sandboxed OSes and high prices for vulnerabilities suggest mobile security inherited a lot of hard-fought lessons learned from personal computers (PCs[23]) and so security has been incorporated into mobile devices from the get-go.

We point out in the Social Engineering pattern that 82% of breaches involve the human element—something the silicon isn't going to be mitigating. Eighteen percent of clicked phishing emails come from a mobile device. Admittedly, we can't say if more folks click on mobile vs PC since no one's phone is narc'ing on them. Still, since almost a fifth of phishing successes came from mobile devices, that should be good enough confirmation that it needs to be within your security estate.

Part of the problem is trying to get users to improve their security behavior. One such approach is providing access to key security information knowledge quizzes within reach of their thumbs in the form of a mobile app. For one such security dashboard app, 66% of users who accepted the terms and conditions

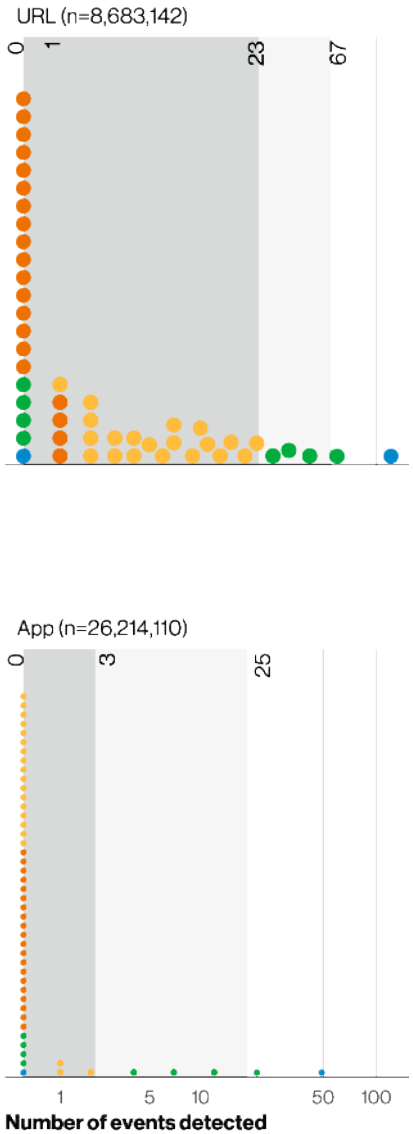


Figure 70. Events detected on mobile devices by type (log scale)

22 Well, not sounds sounds. Well ... you get the picture.
23 Yes, we spelled out "PC." Look, we both know what a PC is, but the kids these days, with their mobile phones and metaverses. Who knows?!

never interacted with the dashboard. Of those that did, 99% interacted more than once, but as you can see in Figure 72, the median interaction time was 15 seconds. Still, about half of folks came back after minutes, hours, or even months.

Making information available to the user about their specific security risks is the first step in the journey to changing behavior. The next is helping the user envision the impact of those risks on themselves. Finally, you need to give users the means to improve, which is where training comes in.[24] It may feel like throwing spaghetti at the wall to see what sticks, but sometimes that's what is required to make it better.

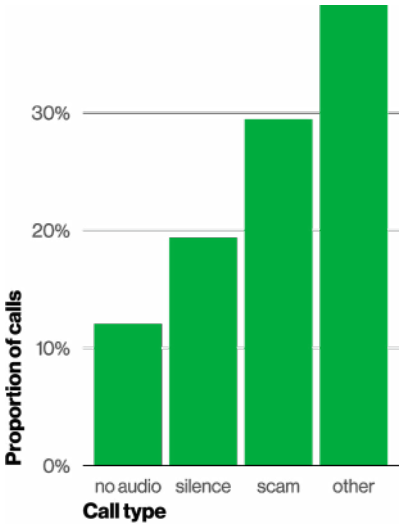


Figure 71. Phone honeypot calls by type (n > 10,000)

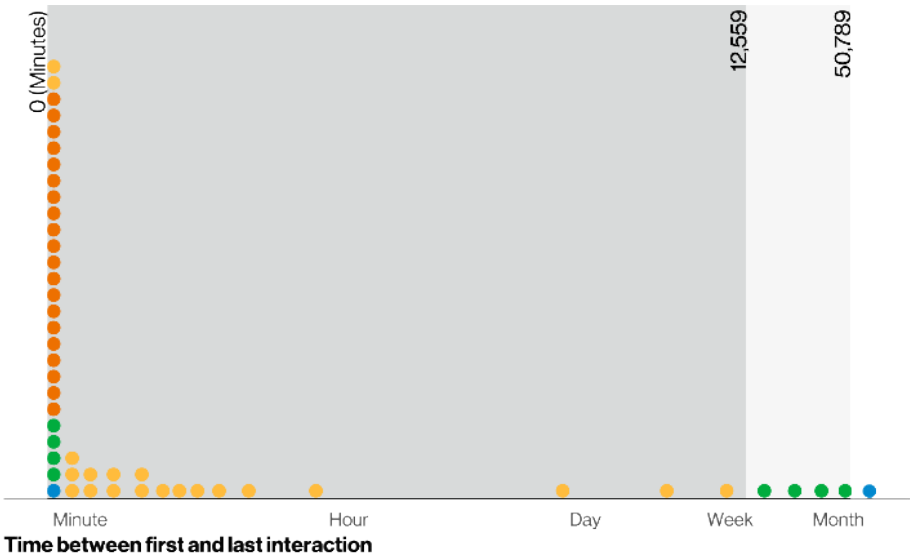


Figure 72. Length of interaction with a mobile security dashboard (n=22,086, log scale)

24 And if you're wondering about how, check out the "Changing Behavior" Appendix!

Privilege Misuse

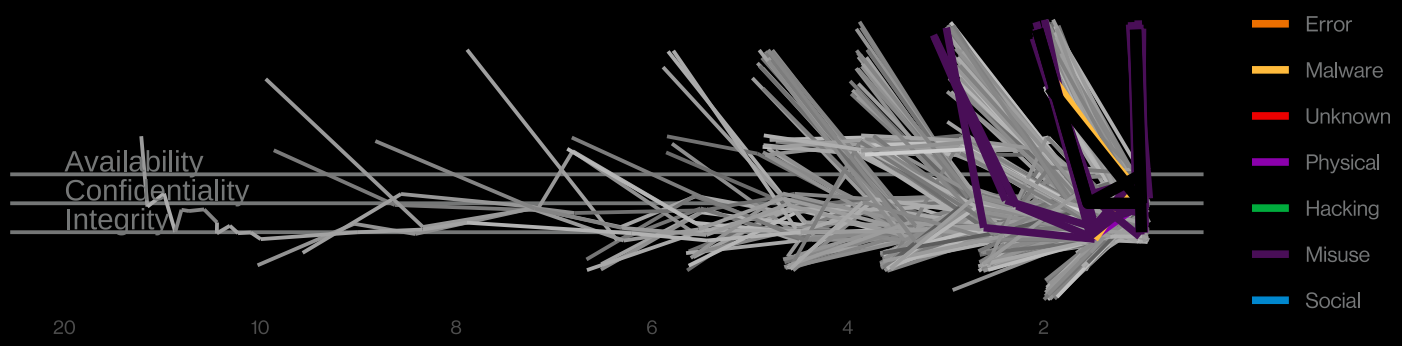


Figure 73. Privilege Misuse incident paths (n=33)

The best laid plans of Mice and Men

We get it. You've honed your hiring processes to a fine edge. You're well prepared to ensure that you onboard only the most qualified people to join your organization. And yet, things somehow go wrong despite your best efforts. Privilege Misuse is the pattern where people use the legitimate access granted to them as employees to steal data. Often, they act alone, but they sometimes act in concert with others. Either way, you have a data breach and must deal with the fallout.

Summary

This pattern is almost entirely insiders using their access maliciously to cause breaches. While Financial is still the leading motive, Espionage, Convenience and just plain Grudges are still represented. Personal data remains the most common data type for these breaches, but Medical data continues to be sought.

What is the same?

Most of the incidents in this pattern result in successful data breaches. These actors are still motivated by greed (financial gain), and are stealing Personal data because it is easy to monetize.

Frequency	275 incidents, 216 with confirmed data disclosure
Threat Actors	Internal (100%), External (4%), Multiple (4%) (breaches)
Actor Motives	Financial (78%), Grudge (9%), Espionage (8%), Convenience (6%) (breaches)
Data Compromised	Personal (70%), Other (28%), Medical (22%), Internal (12%) (breaches)

It's not that easy

Far and away the most common action in this pattern is Privilege abuse. However, Data mishandling also shows up, albeit to a much lesser degree, and is typically associated with the motive of Convenience. Sometimes people do unsafe things to get around a security control designed to protect the data from exposure. While some controls may make it harder for people to get their jobs done, it is important to pair these controls with education to at least let people know the "why" behind the process. Regardless, offering a less laborious process that remains secure would be something to consider if your organization repeatedly suffers this kind of event.

In this pattern the threat actor already has access to perform their day-to-day duties, therefore, we do not see Credentials as the data type affected. Instead, Personal data (whether of customers, employees, or even partners) is of the highest interest to those looking to capitalize on their access.

Medical data is still taken in 22% of breaches in this pattern. When you realize that the most common industry represented in this pattern is Healthcare, that makes sense. In fact, Healthcare has had an ongoing problem with Internal actors accessing their data without a valid reason for a long time. And while it is no longer in the top tier of the patterns in Healthcare, it should not be discounted as a solved problem.

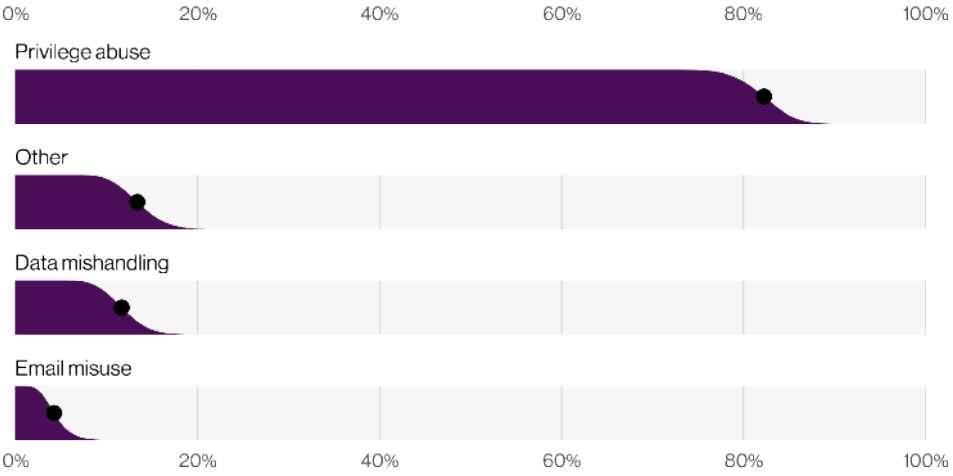
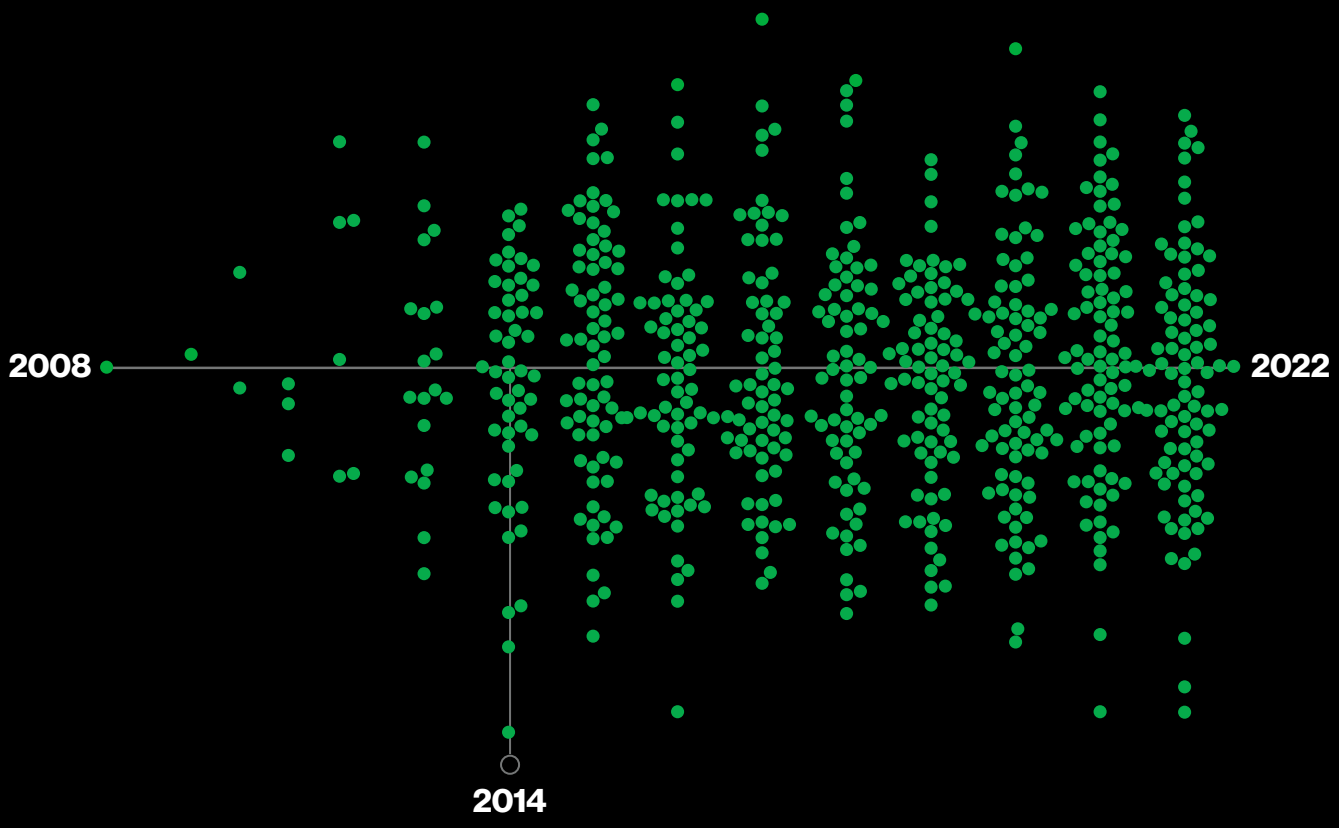
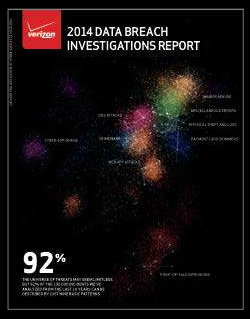


Figure 74. Top Action varieties in Privilege Misuse breaches (n=176)





4 Industries

Introduction

If you are a long-time reader this introduction may be redundant, but for new readers it is worth perusing. This year we looked at 23,896 incidents, which boiled down to 5,212 confirmed data breaches. As always, we break these incidents and breaches into their respective industries to illustrate that all industries are not created equal. At least not when it comes to attack surfaces and threats. The type of attacks suffered by a particular industry will have a great deal to do with what infrastructure they rely upon, what data they handle and how people (customers, employees and everyone else) interact with them.

A large organization whose business model focuses entirely on mobile devices where their customers use an app on their phone will have different risks than a small Mom and Pop shop with no internet presence, but who use a point-of-sale vendor that manages their systems for them. The infrastructure, and conversely the attack surface, largely drives the risk.

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

When examining industries with a small sample, we will provide ranges where the actual value may reside. This allows us to maintain our confidence interval while giving you an idea of what the actual number might be, given a large enough sample. For example, instead of stating "In the Accommodation industry, 92% of attacks were financially motivated," we might state that "financially motivated attacks ranged between 86% and 100%." Check out our riveting Methodology section for far more information about the statistical confidence background used throughout this report.

If you are reading this only for a glimpse of your industry, our recommendation is to verify what the top patterns are on the summary table accompanying each industry and also spend some time with those pattern sections. In addition, we provide a description of what Center for Internet Security (CIS) Critical Security Controls) to prioritize in each industry section for ease of reading if you want to get straight to strategizing your security moves.

	Incidents				Breaches			
Industry	Total	Small (1-1,000)	Large (1,000+)	Unknown	Total	Small (1-1,000)	Large (1,000+)	Unknown
Total	23,896	2,065	636	21,195	5,212	715	255	4,242
Accommodation (72)	156	2	1	153	69	1	1	67
Administrative (56)	39	5	7	27	19	3	5	11
Agriculture (11)	243	1	1	241	39	1	0	38
Construction (23)	127	21	7	99	57	8	5	44
Education (61)	1,241	112	48	1,081	282	57	15	210
Entertainment (71)	215	12	5	198	96	6	3	87
Finance (52)	2,527	103	50	2,374	690	56	32	602
Healthcare (62)	849	36	14	799	571	14	10	547
Information (51)	2,561	59	25	2,477	378	27	10	341
Management (55)	8	1	2	5	2	0	0	2
Manufacturing (31-33)	2,337	168	74	2,095	338	54	22	262
Mining (21)	231	0	0	231	132	0	0	132
Other Services (81)	180	16	1	163	101	8	1	92
Professional (54)	3,566	1,095	144	2,327	681	263	52	366
Public Administration (92)	2,792	110	88	2,594	537	74	25	438
Real Estate (53)	118	31	5	82	76	19	2	55
Retail (44-45)	629	157	68	404	241	54	35	152
Transportation (48-49)	305	26	38	241	137	17	23	97
Utilities (22)	172	20	14	138	47	14	3	30
Wholesale Trade (42)	166	79	33	54	68	38	8	22
Unknown	5,434	11	11	5,412	651	1	3	647
Total	23,896	2,065	636	21,195	5,212	715	255	4,242

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

Breaches

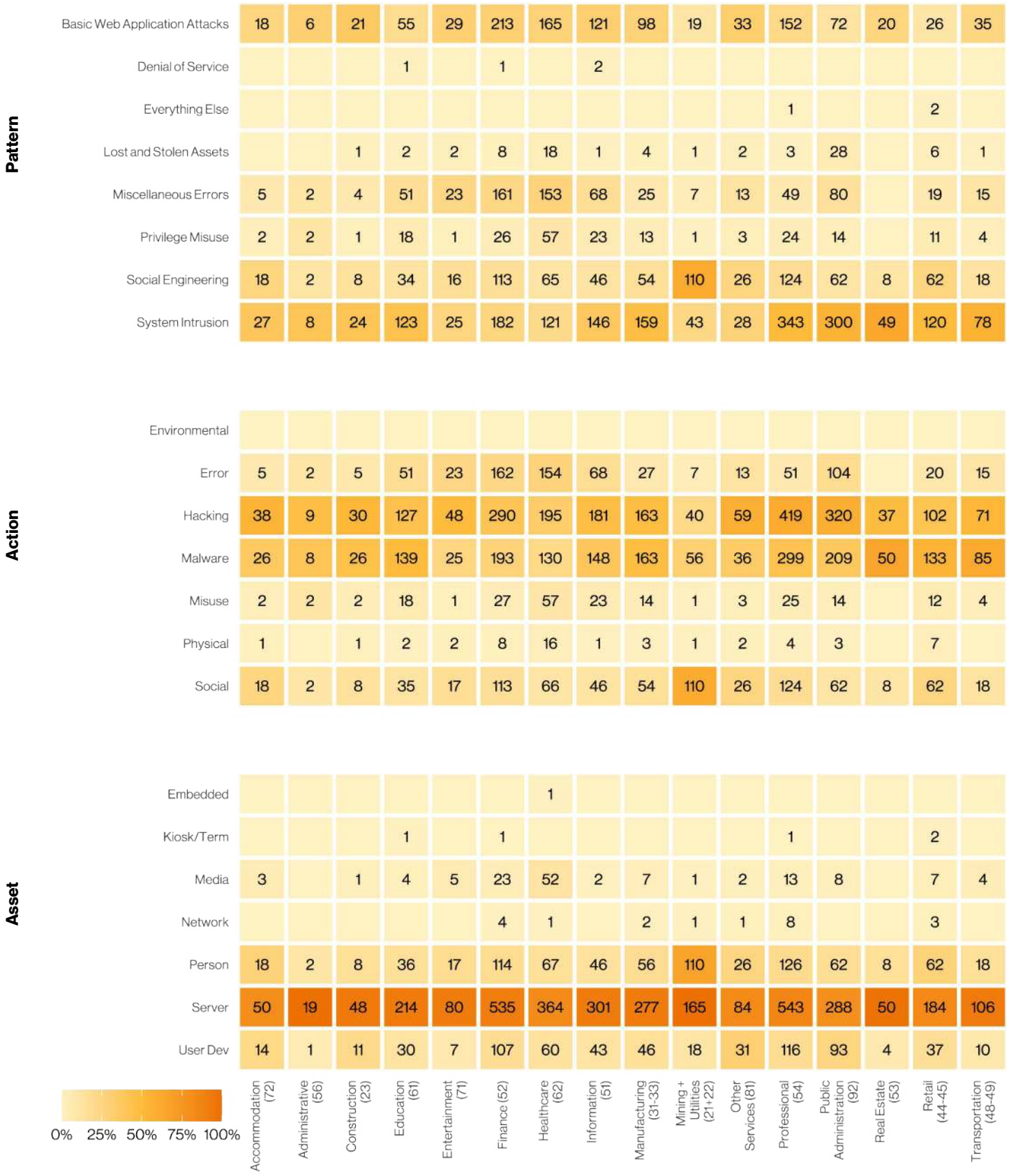


Figure 75. Breaches by industry

Incidents

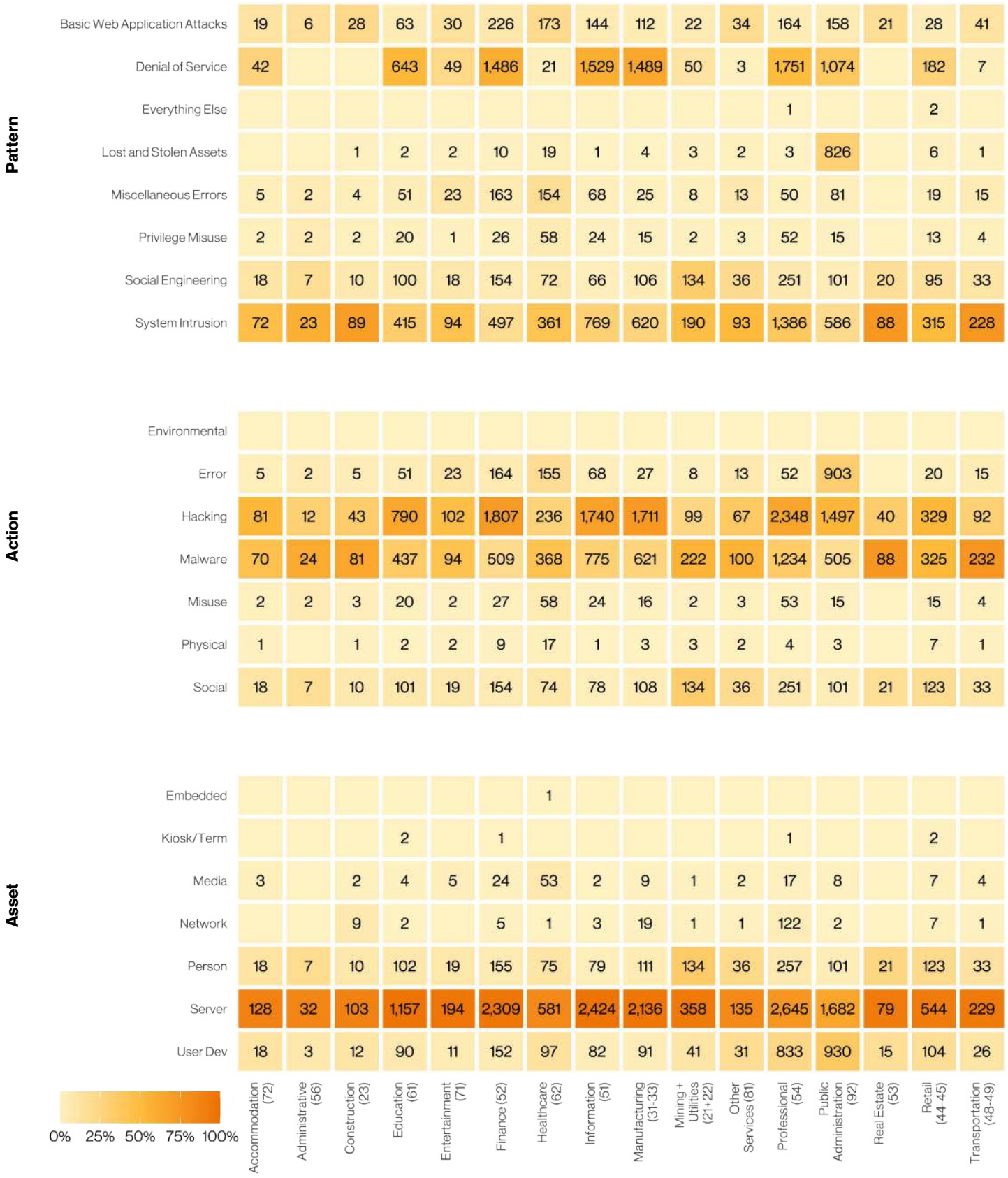


Figure 76. Incidents by industry

Accommodation and Food Services NAICS 72

Frequency	156 incidents, 69 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 90% of breaches
Threat actors	External (90%), Internal (10%) (breaches)
Actor motives	Financial (91%), Espionage (9%) (breaches)
Data compromised	Credentials (45%), Personal (45%), Payment (41%), Other (18%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	This industry continues to be targeted by financially motivated criminals going after Payment and Personal data.

Summary

Accommodation and Food Services, while having seen a decrease of System Intrusion since 2016, is still victimized by Malware via email and the Use of stolen credentials used against Web application.

Patterns in years	5-year difference	3-year difference	Difference with peers
System Intrusion	Less	Less	No change
Social Engineering	Greater	No change	No change
Basic Web Application Attacks	Greater	Greater	No change

The Accommodation and Food Services industry is one of the few industries that saw a drop in terms of System Intrusion. However, it shows similar trends to other industries in regard to Basic Web Application Attacks and Social Engineering. They have been on the increase over the last 5 years, and are now a bit closer to the same baseline for the types of attacks that the other industries are experiencing.

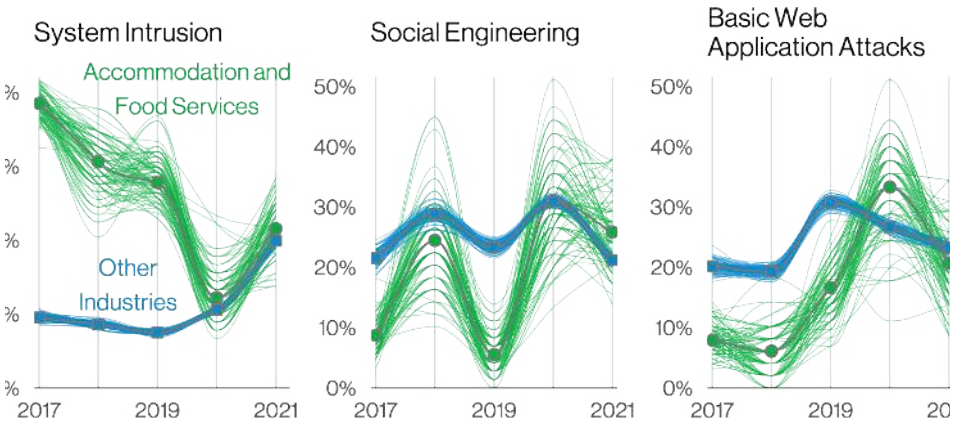


Figure 77. Top patterns over time in Accommodation and Food Services breaches

Figure 78 captures the top Action varieties found in this industry. This is one of the few industries that is extremely long tailed, with over 80% of the breaches including Actions not captured in the top five varieties. While that might seem imposing, keep in mind that the vectors are still the usual suspects found in the other industries: Email, Web apps and Desktop sharing software.

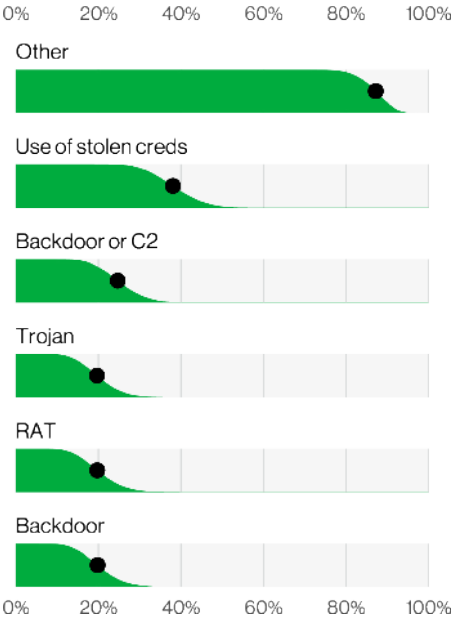


Figure 78. Top Action varieties in Accommodation and Food Services breaches (n=58)

Looking back

In the 2012 DBIR, Accommodation and Food Services represented over 54% of our cases and has since dropped to less than 2% of our incidents. This represents both a total drop in cases but also a rather dramatic drop in incidents and may be representative of a larger shift in the criminal ecosystem to target and victimize not only the organizations with credit card data but any organization.

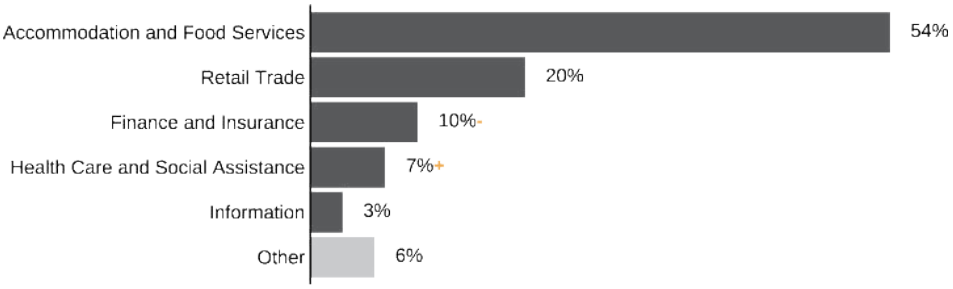


Figure 79. Industry groups represented by percent of breaches (2012 DBIR Figure 3)

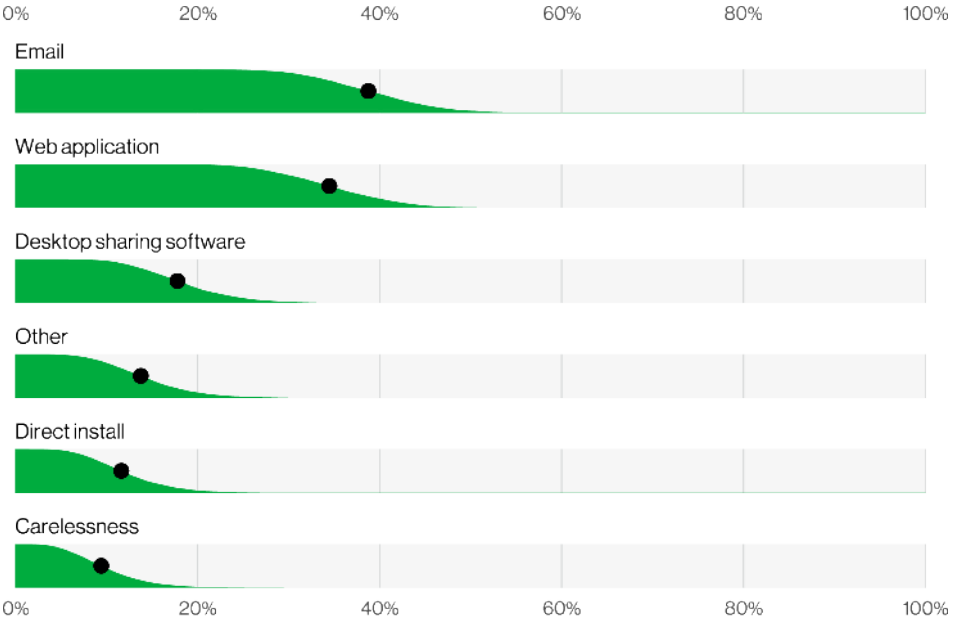


Figure 80. Top Action vectors in Accommodation and Food Services breaches (n=47)

Arts, Entertainment and Recreation NAICS 71

Frequency	215 incidents, 96 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, System Intrusion and Miscellaneous Errors represent 80% of breaches
Threat actors	External (74%), Internal (26%) (breaches)
Actor motives	Financial (97%), Grudge (3%) (breaches)
Data compromised	Personal (66%), Credentials (49%), Other (23%), Medical (15%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6)
What is the same?	The patterns are the same, but the order is not. Medical data continues to be compromised in this industry.

Summary

The System Intrusion and Basic Web Application Attacks patterns exchanged positions, but the Miscellaneous Errors pattern held on to 3rd place on the podium. For incidents, Denial of Service attacks remain a problem in the sector, particularly for the Gambling industry.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	No change	No change
System Intrusion	No change	No change	Less
Miscellaneous Errors	No change	No change	Greater

This industry mainly covers live performances, and whether dance, theater or sporting events, the common thread is that none are pre-recorded for later broadcast. It also includes the gambling industry. One can only imagine the different attack surfaces that are present for the myriad organization types belonging to this NAICS code. Something many of them have in common, however, is that at least a portion of their infrastructure relies on the internet to perform critical functions, whether that is ticket sales or taking orders (or bets as the case may be). In any event, when a Denial of Service attack comes calling, it is a very unwelcome guest. Nevertheless, it is a frequent guest in this sector (particularly in the Gaming organizations in the APAC region), and represents over 20% of incidents.

With regard to breaches, the three patterns listed in the At-a-Glance table show the vulnerability of the infrastructure beyond disruption of services. Once the attackers get in, they can wreak havoc in earnest. These attackers are largely External actors, with a Financial motive, although there are a small amount of Grudge-motivated attacks in this sector as well.

The inclusion of the Basic Web Application Attacks is concerning, given the less complex nature of these attacks. Conversely, the attackers have to try much harder to gain their prize in the System Intrusion attacks, where ransomware is always a favored tool. As we have seen in the past, every attacker loves credentials, and will use them to masquerade as a legitimate employee to evade capture for as long as it takes to get what they are after.

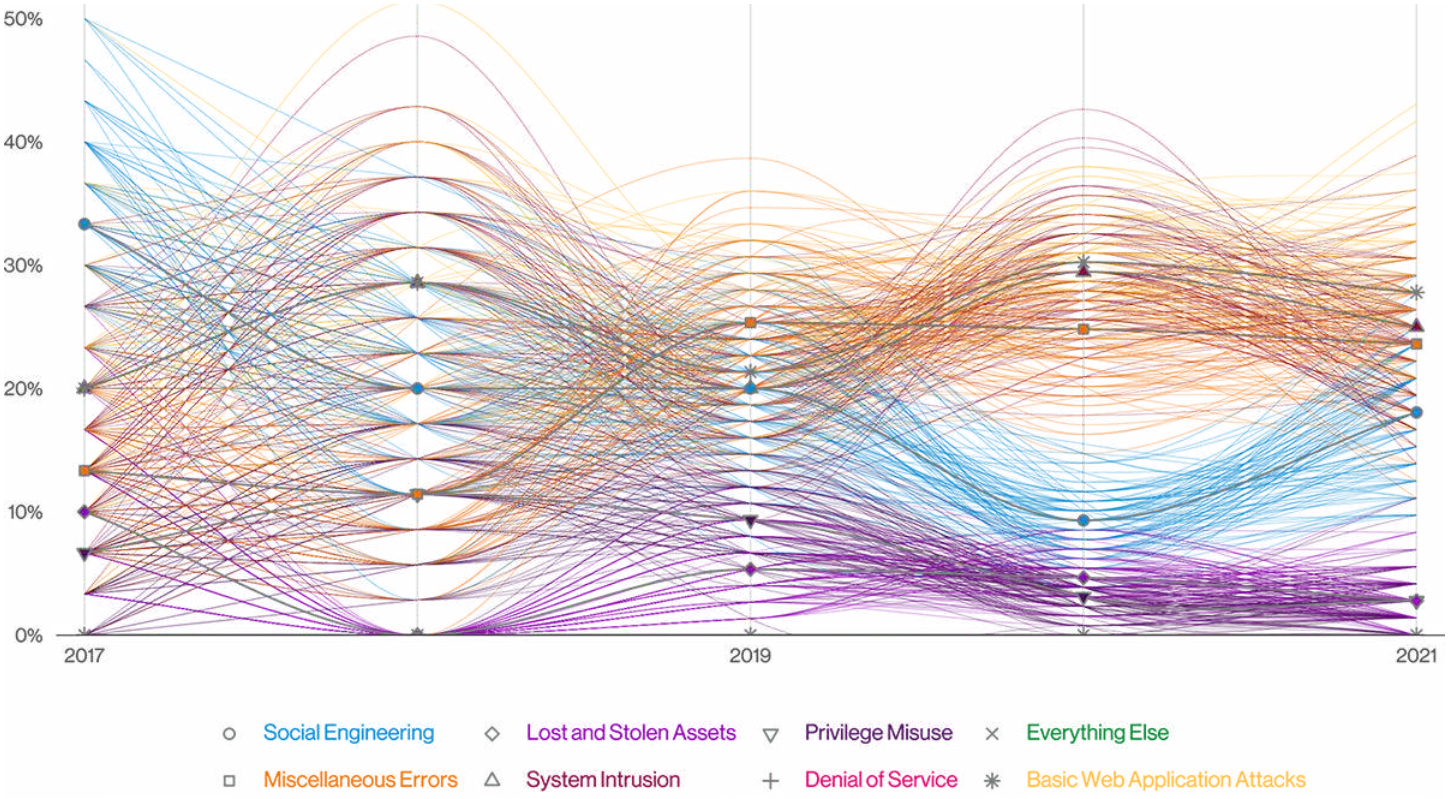


Figure 81. Patterns over time in Arts and Entertainment breaches

The most commonly taken data is Personal information (although it is down from a high last year of 83%) and Credentials. Oddly enough, Medical data is still being snarfed up (technical term) in 15% of the breaches in this sector. This was similar to last year (at 26%), but it remains a puzzling data type to find in a sector that has no medical affiliation. It may be that the data taken is from companies that are self-insured for their employee medical needs, and so have a need to store that kind of data, or it could possibly be from some form for Workers Compensation data (on the job injuries). Additionally, this NAICS code includes sports teams which could account for a certain number of stolen medical records. Regardless, it is a rather counterintuitive finding.

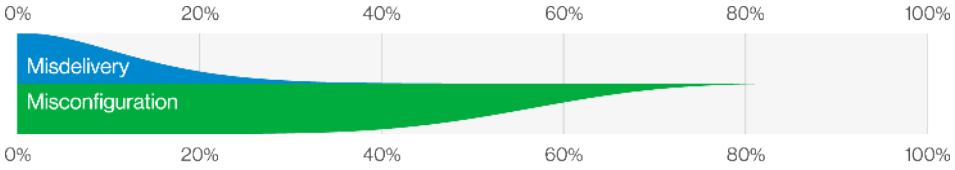


Figure 82. Misdelivery vs Misconfiguration in Arts and Entertainment industry Error breaches (n=16)

Miscellaneous Errors remain in the top three patterns again this year (25%). The Misconfiguration error was the most common, representing approximately 15% of the breaches. It appears this sector simply traded one problem for another as Misdelivery errors (the most common last year) have dropped considerably.

Educational Services NAICS 61

Frequency	1,241 incidents, 282 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 80% of breaches
Threat actors	External (75%), Internal (25%) (breaches)
Actor motives	Financial (95%), Espionage (5%) (breaches)
Data compromised	Personal (63%), Credentials (41%), Other (23%), Internal (10%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	This industry continues to be impacted by attacks targeting their external infrastructure and are largely targeted by External actors with Financial motives. However, Educational Services also faces errors as one of the top causes of breaches.

Summary

Educational Services follows an eerily similar trend to the majority of the other industries; it is experiencing a dramatic increase in Ransomware attacks (over 30% of breaches). In addition, this industry needs to protect itself against stolen credentials and phishing attacks potentially exposing the personal information of its employees and students.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	Greater	Less
System Intrusion	Greater	Greater	Greater
Miscellaneous Errors	No change	Less	Greater

Alright, class is back in session, put away your NSYNC Trapper Keeper and get out a number two pencil, cause you're about to get schooled on the breaches and incidents impacting the Educational Services industries. System Intrusion, Social Engineering and DoS are the leading causes of incidents and System Intrusion, BWAA and Errors lead the way with regard to breaches. Falling along the peak of the grading curve, this industry also has Use of stolen creds and Ransomware as the top two action varieties, which is a very dangerous combination. The rumor is stolen creds and ransomware quit school due to recess, because they don't play around.

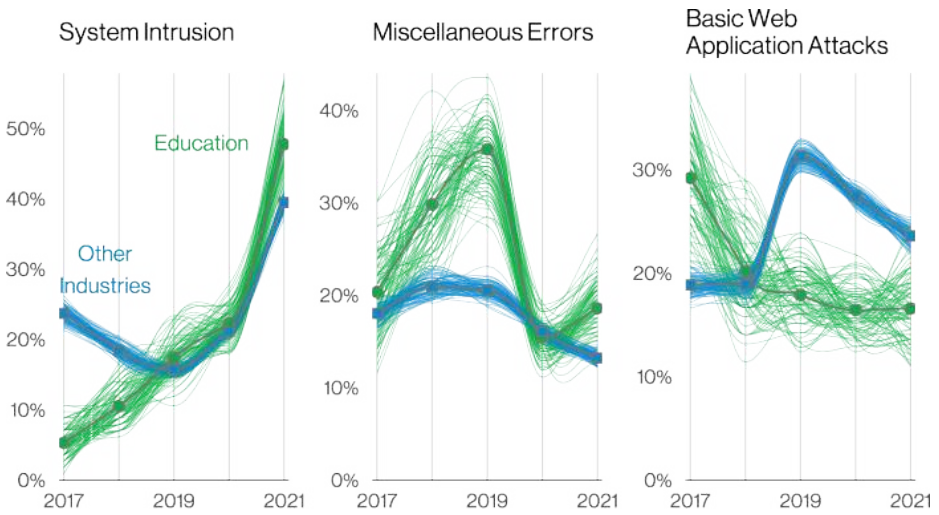


Figure 83. Top patterns over time in Education breaches

While an erroneous number in a calculation might result in a few points off of your homework, the erroneous end user might result in a data breach. Thirty four percent of the errors found in this industry were from an email sent to the wrong people, or with the wrong attachment.

While errors may have decreased over the past three years, they're still a relatively normal occurrence that should be taken seriously, especially considering the various troves of data schools handle, we would hate to have our poor little Bobby Tables' data leaked.[25]

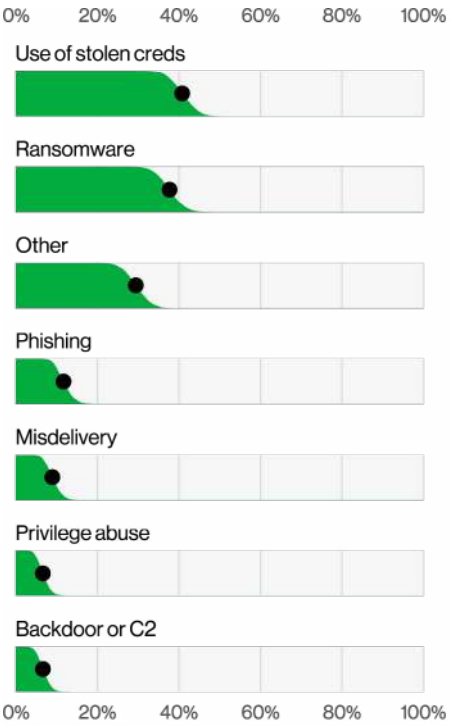


Figure 84. Top Action varieties in Educational Services breaches (n=218)

2017 Yearbook

There's nothing quite like the feeling of nostalgia that hits you when you're looking over your old yearbook. Signatures and notes from friends long ago, ahh, the good old days. We get that same feeling when looking back at the 2017 DBIR and see Cyber-Espionage as the top breach pattern for this industry. No worries though, Espionage has not graduated and moved away yet. It shows up in 34% of incidents this year. Figure 85 captures the shifts in data and the somewhat dramatic rise of Espionage that is still all too present today. Unfortunately, unlike your opinionated high school friends on social media, you can't just block espionage from cluttering up your feed.

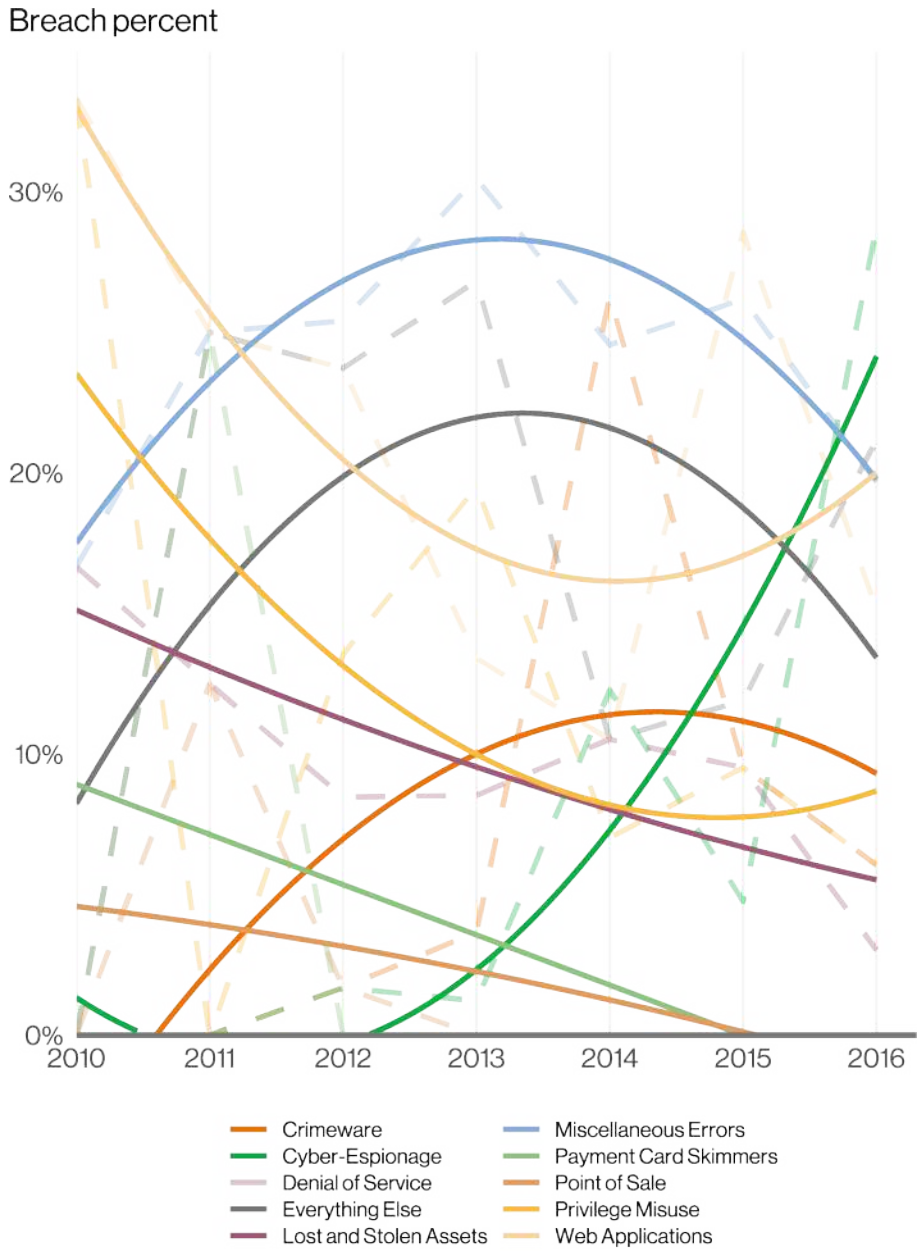


Figure 85. Percent of breach classification patterns over time within the Education industry (DBIR 2017 Figure 17)

25 https://xkcd.com/327, a classic.

Financial and Insurance NAICS 52

Frequency	2,527 incidents, 690 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, System Intrusion and Miscellaneous Error represent 79% of breaches.
Threat actors	External (73%), Internal (27%) (breaches)
Actor motives	Financial (95%), Espionage (5%) (breaches)
Data compromised	Personal (71%), Credentials (40%), Other (27%), Bank (22%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Data Protection (CSC 3)
What is the same?	Basic Web Application Attacks and Miscellaneous Errors continue to play a large part in breaches for this vertical as they did last year.

Summary

The Financial sector continues to be victimized by financially motivated organized crime, often via the actions of Social (Phishing), Hacking (Use of stolen credentials) and Malware (Ransomware). Finally, Miscellaneous Errors, often in the form of Misdelivery, is still very common as it has been for the past three years in a row.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	Greater	Greater	Less
System Intrusion	Greater	Greater	Greater
Miscellaneous Errors	Greater	Greater	Greater

In 2016 servers were involved in 50% of Financial breaches, as opposed to 90% currently. However, the specific variety of "Server–Web application" has increased from 12% to 51% over that same timeframe, thus accounting for Basic Web application Attacks' position in the top three patterns. A key component of these attacks is that they usually involve the Use of stolen credentials, which is the number one Action variety in this vertical. These creds may have been obtained in any number of ways, but brute force hacking and credential stuffing are the most likely culprits. One thing is certain, stolen creds and web apps go together like peanut butter and chocolate.

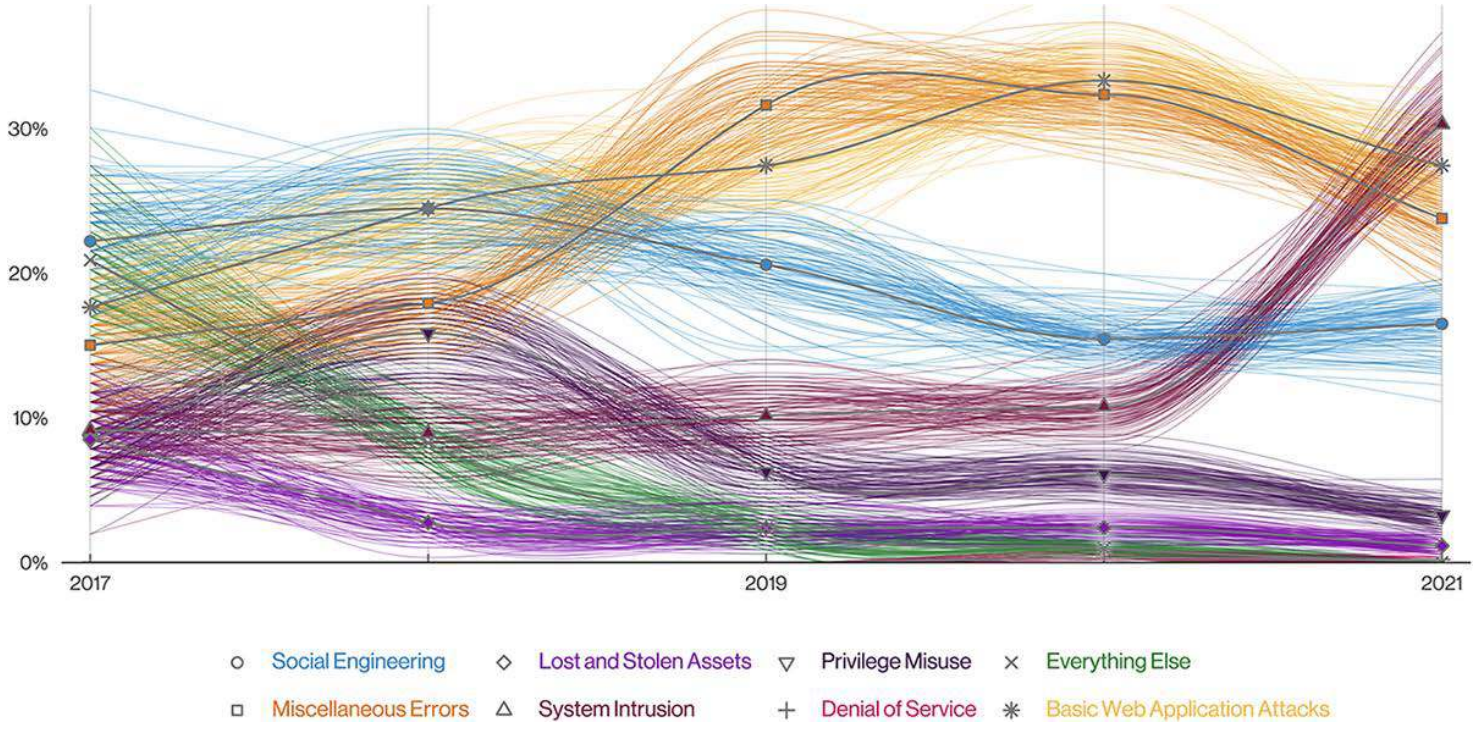


Figure 86. Patterns over time in Financial and Insurance industry breaches

"I'll show you mine if you show me yours"

The Error variety of "Misdelivery" (16%) is the second most common action variety in this vertical. Misdelivery is exactly what it sounds like, delivering PII or other sensitive information to the wrong recipient. One might expect to see that variety more often in Public Sector or Healthcare because, by their very nature, they send a great deal of mail. Instead, our data indicates that Misdelivery is approximately three times higher in Financial than in the other industries. We here on the DBIR team were taken aback by this finding, as it would be embarrassing if any unauthorized person were to view our checks and learn that we make countless millions for writing this report each year.[26]

"Through the years..."

System Intrusion has doubled from 14% in 2016 to 30% this year. Organized crime was responsible for only 49% of breaches in 2018 vs the 79% we see in this report. Availability was affected in only 6% of breaches back in 2016, vs 14% today, and the discovery method of Actor disclosure was 5% (in 2016) as opposed to the 58% in this year's report. We need hardly say that this is mainly due to ransomware attacks, but to be on the safe side, we will say it anyway:

This is mainly due to ransomware attacks. As long as ransomware continues to be a high profit, low risk attack, criminals will continue to utilize it.

Finally, we would be remiss if we did not mention that DoS attacks continue to be a huge problem and account for 58% of security incidents in this vertical. That is approximately twice as much as we see in the other industries.

26 If only.

Healthcare NAICS 62

Frequency	849 incidents, 571 with confirmed data disclosure
Top patterns	Basic Web Application Attacks, Miscellaneous Errors and System Intrusion represent 76% of breaches
Threat actors	External (61%), Internal (39%) (breaches)
Actor motives	Financial (95%), Espionage (4%), Convenience (1%), Grudge (1%) (breaches)
Data compromised	Personal (58%), Medical (46%), Credentials (29%), Other (29%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6)
What is the same?	The top three patterns are the same, but the order is not. The threat actors were exactly the same as last year (down to the percentage point).

Summary

The Basic Web Application Attacks have overtaken the Miscellaneous Errors in causing breaches in this sector. Errors are still a significant problem.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	Greater	Greater	Greater
System Intrusion	Greater	Greater	Less
Miscellaneous Errors	Less	Less	Greater

Insiders? What Insiders?

Healthcare is the industry where the internal actor has figured prominently in breaches since we first began collecting and reporting data. While the make-up of the insider breach has moved from being largely malicious Misuse incidents to the more benign (but no less reportable) Miscellaneous Errors, we have always been able to rely on this industry to tell the insider threat story. With the rise of the Basic Web Application Attacks pattern in this vertical, those inside actors no longer hold sway. Move over Insiders, the big dogs are here.

Make no mistake (no pun intended) your employees are still causing breaches, but they are more than 2.5 times more likely to make an error than to maliciously misuse their access. Misdelivery and Loss are the most common errors (and they are so close, we'd need a photo finish to determine a winner).

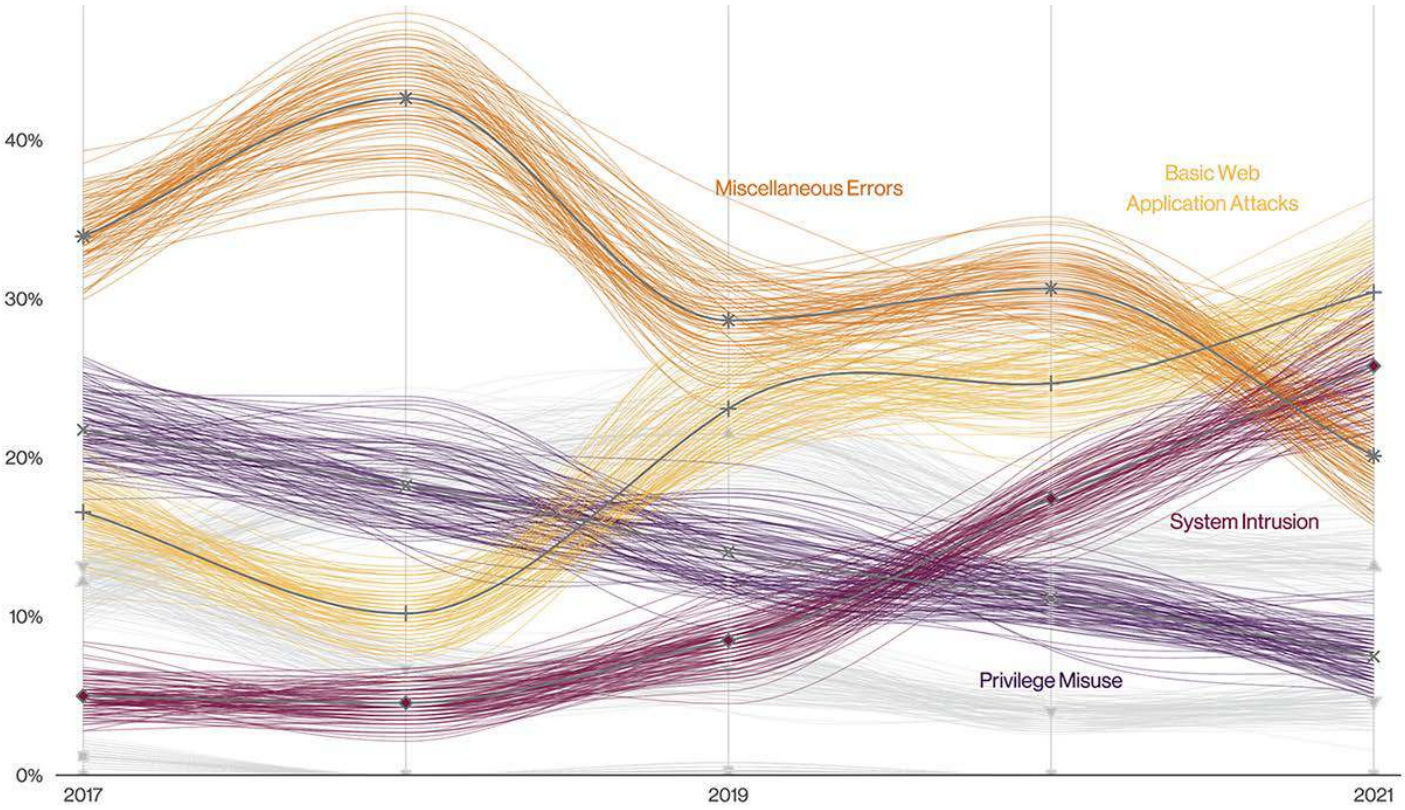


Figure 87. Patterns over time in Healthcare industry breaches

Figure 87 illustrates the change over time in patterns for Healthcare. Back in 2015, the top pattern was Privilege Misuse, followed by Miscellaneous Errors. It wasn't until 2019 that we started to see the rise of Basic Web Application Attacks, and they have clearly become a serious problem for everyone, not just this industry. Healthcare has increasingly become a target of run-of-the-mill hacking attacks and the more impactful ransomware campaigns (both from the System Intrusion pattern, which came in third). With the increase in ransomware, comes the associated increase of the discovery method of Actor Disclosure. It is a bad day when that ransom note pops up after the encryption has been triggered, providing convenient methods of payment for these customer service-focused threat groups. (And really, who doesn't want to make it easy for their "customers" to pay them?)

For the second year, Personal data is compromised more often than Medical. Do we consider this the norm now for the one industry with a plethora of medical data? Is this because the actors are just getting in and getting their encryption game on without regard to the type of records they are rendering inaccessible? Only those in the industry know for certain if they have increased their controls around their Medical data but left Personal data in the waiting room.

Information NAICS 51

Frequency	2,561 incidents, 378 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Miscellaneous Errors represent 81% of breaches
Threat actors	External (76%), Internal (24%) (breaches)
Actor motives	Financial (78%), Espionage (20%), Ideology (1%), Grudge (1%) (breaches)
Data compromised	Personal (66%), Other (35%), Credentials (27%), Internal (17%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Secure Configuration of Enterprise Assets and Software (CSC 4), Access Control Management (CSC 6)
What is the same?	Surprisingly, over the last five years Social breaches have remained roughly the same. This may be because Social breaches are targeting customers resulting in Hacking breaches (which have also stayed pretty level) to the company due to stolen credentials.

Summary

System Intrusion moves ahead of Errors and Basic Web Application Attacks to claim the top spot this year in breaches, meanwhile DDoS maintains its top position in incidents. Malware has seen a noticeable rise over the past two years, while Errors appear to be on the down swing since their rise five years ago.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	No change	Greater
Miscellaneous Errors	Greater	Less	Greater
System Intrusion	Greater	Greater	Greater

Last year, not unlike your boss at your last performance review, we highlighted the Errors in the Information industry. However, as we can see in Figure 88, there has been clear progress that we can put on the mid-year review. Errors have experienced a decline since their upswing half a decade ago in 2017.

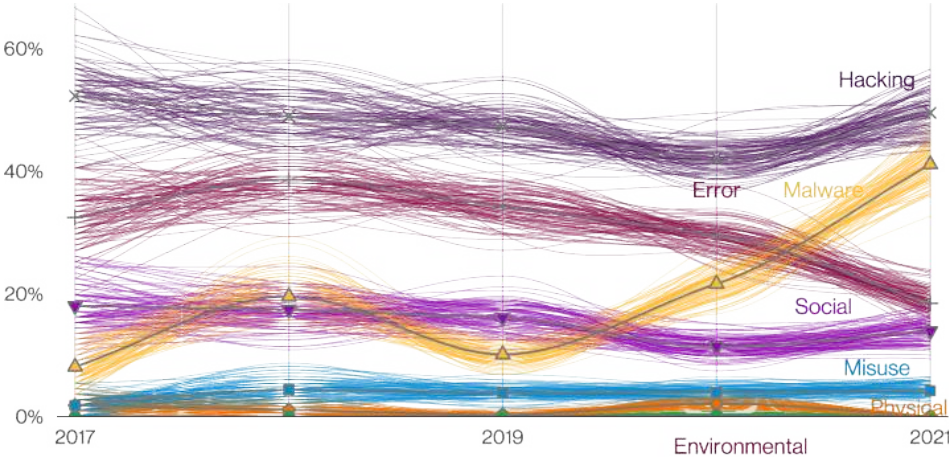


Figure 88. Actions over time in Information industry breaches

To maintain the balance however, Malware has seen a measurable increase over the past two years. That is reflected in Figure 89. System Intrusion has jumped to the top in this vertical, even rising above Basic Web Application Attacks.

One interesting effect of having System Intrusion in the number one position is that the Information industry contains a smorgasbord of Action varieties. Use of stolen creds is the most common, but after that, a legion of varieties are present, with Ransomware, Misconfiguration, Backdoor or C2, and Export Data appearing in more than 4% of breaches. In fact, Information is tied for 2nd place in industries by number of varieties above 4% at 17 different Action varieties.

Figure 90 illustrates the top incidents, dominated by DDoS attacks and System Intrusions (which are driven by Ransomware). Please be sure not to forget about DDoS–while it is relatively easy to mitigate, it has certainly not gone away.

Finally, Figure 91 provides a look into something else that's easy to forget: botnets. The information industry takes the top spot in botnets for the second year running. Botnet breaches are often masked at the victim organization because they only see the malicious login, and not that the bot also stole the credentials.

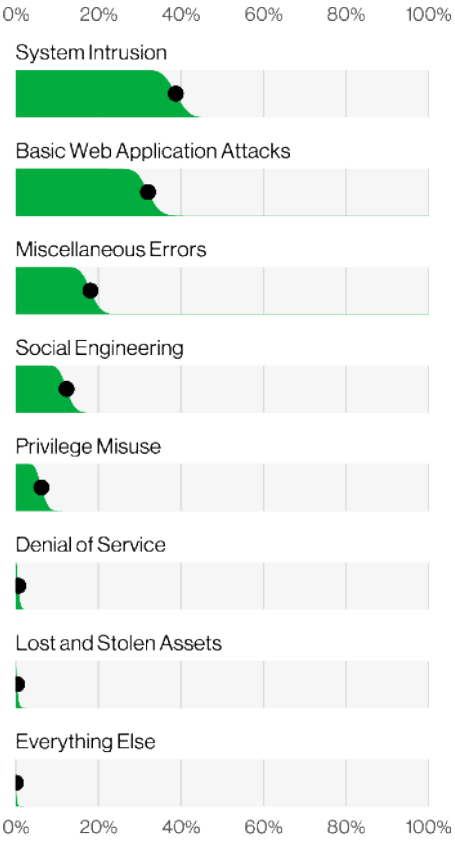


Figure 89. Patterns in Information industry breaches (n=378)

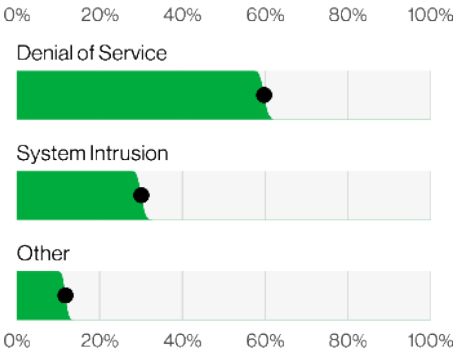


Figure 90. Top patterns in Information industry incidents (n=2,561)

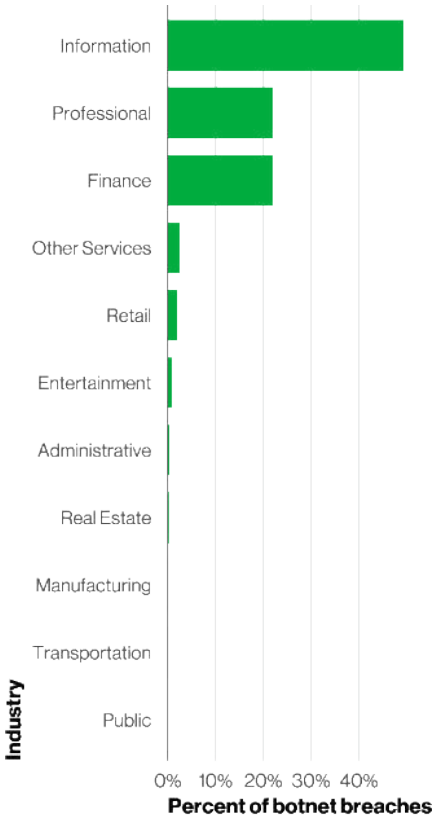


Figure 91. Evil Corp botnet breaches by industry (n=7,072)

Manufacturing NAICS 31-33

Frequency	2,337 incidents, 338 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 88% of breaches
Threat actors	External (88%), Internal (12%), Partner (1%) (breaches)
Actor motives	Financial (88%), Espionage (11%), Grudge (1%), Secondary (1%) (breaches)
Data compromised	Personal (58%), Credentials (40%), Other (36%), Internal (14%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	System intrusion and Basic Web Application Attacks continue to be among the main patterns this industry faces.

Summary

Manufacturing continues to be a lucrative target for espionage, but is also increasingly being targeted by other criminals via the use of Denial of Service attacks, credential attacks and Ransomware.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	Greater	Greater	Greater
Social Engineering	Less	Less	Less
System Intrusion	Greater	Greater	Greater

Manufacturing, with its hum of machinery churning out the key components that make our modern life possible, continues to be a valued target for espionage (mostly due to recent indiscriminate supply chain attacks covered in a previous section). However, it has also become a lucrative target for financially motivated criminals looking to make a quick dollar.

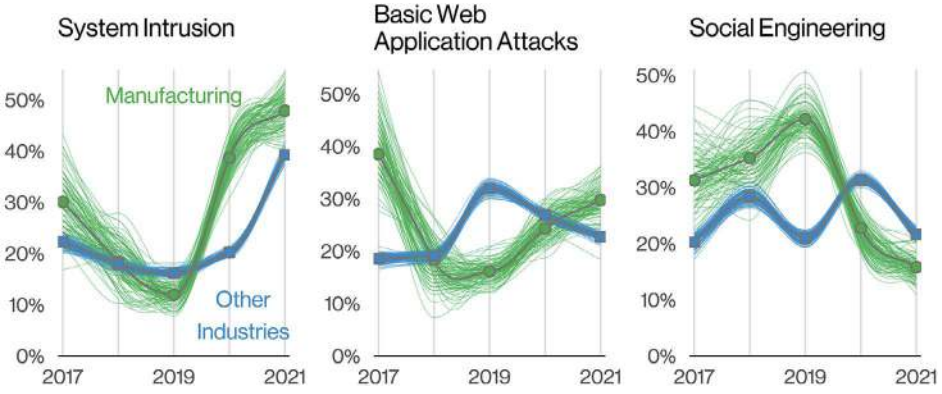


Figure 92. Top patterns over time in Manufacturing breaches

In previous reports, Manufacturing was largely targeted for their juicy schematics and secrets. For example, in 2016 over 55% of the incidents in this vertical involved Espionage (Figure 93), but that has been lower over the last few years. Or, conversely, the spies have upped their game to the point that they are no longer exposed.

DoSing against the machine

For an industry where availability equals productivity, it's interesting to see the yo-yo pattern that has been taking place with DoS attacks over the years. While DoS attacks initially reached its former peak in the 2018 report (over 40% of incidents), it's been increasing since 2019 and now accounts for approximately 70% of incidents, which puts it more in line with what we see in other industries. This rise of DoS, while unlikely to prevent those key assets from actually running the manufacturing process, is still worth keeping in mind as integration increases between the OT side of the house and the IT side.

With regard to the breaches impacting this sector, one can find the usual suspects, such as stolen credentials (39%), Ransomware (24%) and Phishing (11%) demonstrated in Figure 95. These types of breaches appear to be impacting everyone regardless of industry. Implementing safeguards, such as the ones listed in the At-a-Glance table, should be a priority for this vertical. Otherwise, you might find your organization unexpectedly seizing up due to a certain someone with an anime girl avatar.

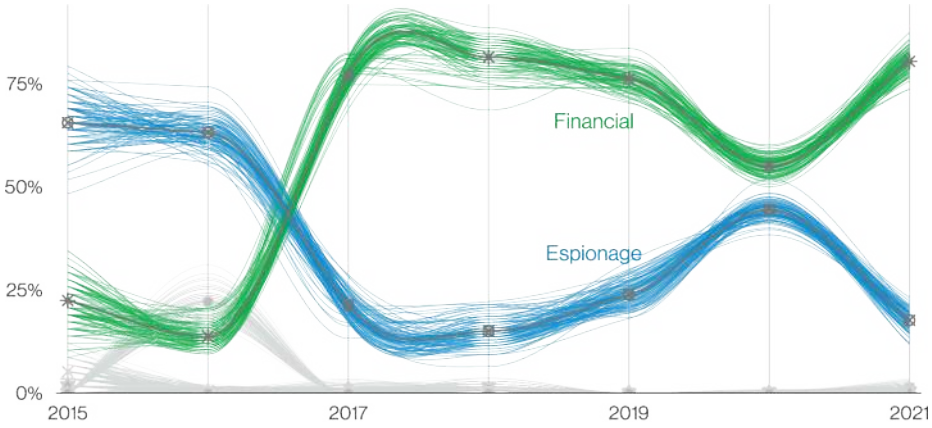


Figure 93. Motives over time in Manufacturing industry incidents

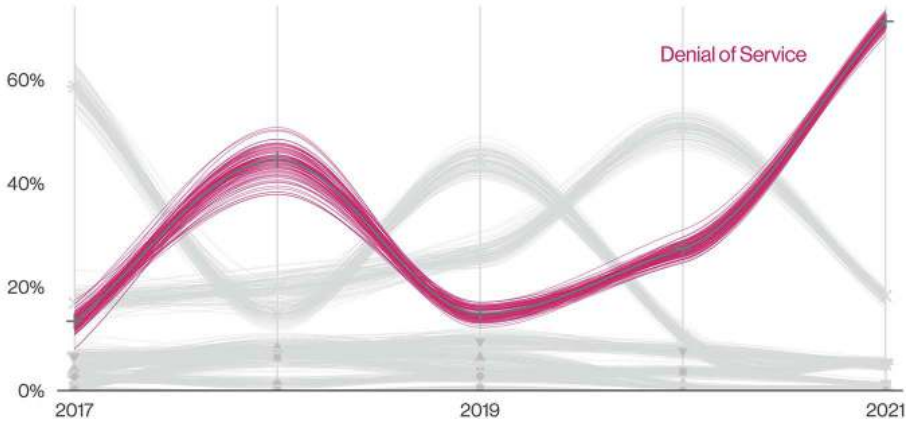


Figure 94. Patterns over time in Manufacturing industry incidents

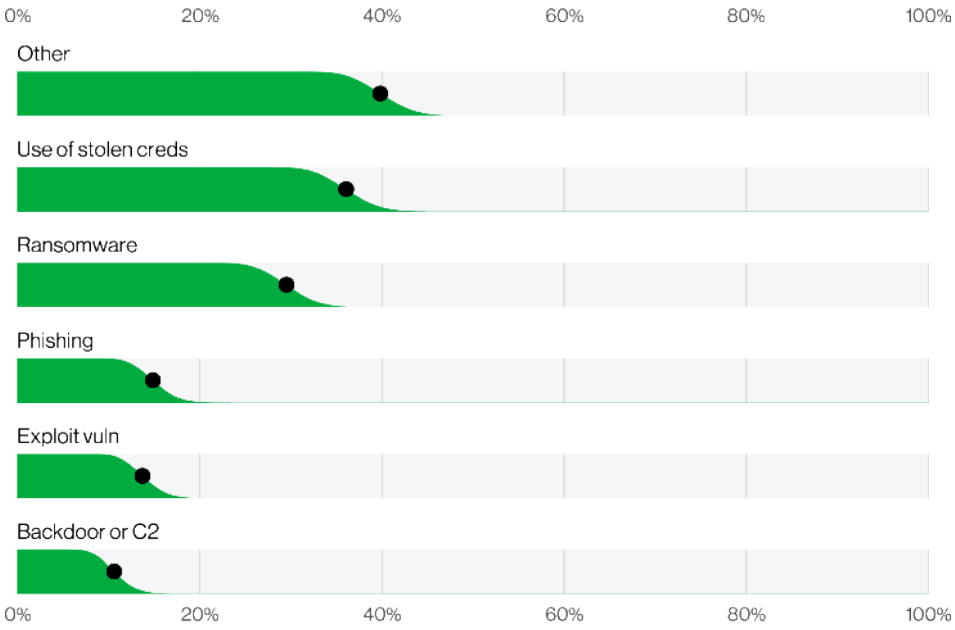


Figure 95. Top Action varieties for Manufacturing industry breaches (n=259)

Mining, Quarrying, and Oil & Gas Extraction + Utilities

NAICS 21+22

Frequency	403 incidents, 179 with confirmed data disclosure
Top patterns	Social Engineering, System Intrusion and Basic Web Application Attacks represent 95% of breaches
Threat actors	External (96%), Internal (4%) (breaches)
Actor motives	Financial (78%), Espionage (22%) (breaches)
Data compromised	Credentials (73%), Personal (22%), Internal (9%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Account Management (CSC 5)
What is the same?	This industry continues to be targeted by financially motivated actors as well as actors committing espionage.

Summary

The Mining and Utilities industry faces similar types of attacks as other industries such as those targeting credentials and leveraging Ransomware, but in addition has a high rate of social engineering attacks like Phishing.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	No change	Less
Social Engineering	No change	No change	No change
System Intrusion	No change	No change	Less

Mining, Quarrying, and Oil & Gas Extraction + Utilities (or MQOGEU as we like to say) simply rolls off the tongue. It is an interesting "combined" industry has had a higher number of engineers. This is perhaps fitting as it seems to be under barrage from the other form of "engineers"—the Social Engineers. This industry has had a higher rate of Social Engineering breaches than their peers.

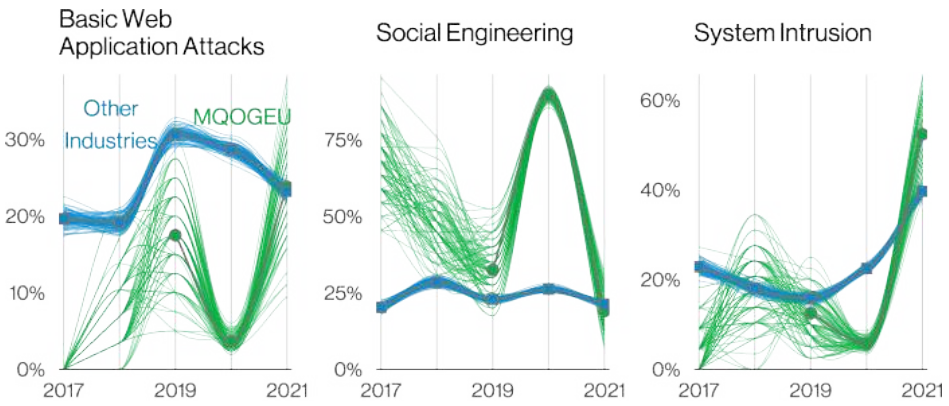


Figure 96. Top patterns over time in MQOGEU breaches

And it shows, as more than 60% of all breaches are Phishing (Figure 97), followed by stolen credentials (potentially gathered by Phishing) and Ransomware (potentially tangential to Phishing). Given the key importance of this industry to our everyday well-being, we certainly hope that those credentials aren't the only thing keeping our utilities and mining operations safe, especially since that's one of the most commonly breached data types.

Considering the high prevalence of Phishing and credential attacks, it's not too surprising to have Email servers as this industry's most commonly breached asset, followed by Web application and Desktop. Even though the infrastructure that runs these complex systems isn't traditional IT infrastructure, the company can still be exposed to the very same threats as any other organization.

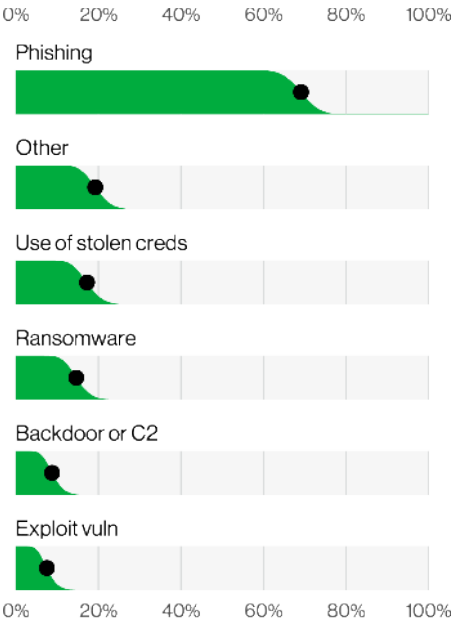


Figure 97. Top Action varieties in MQOGEU breaches (n=153)

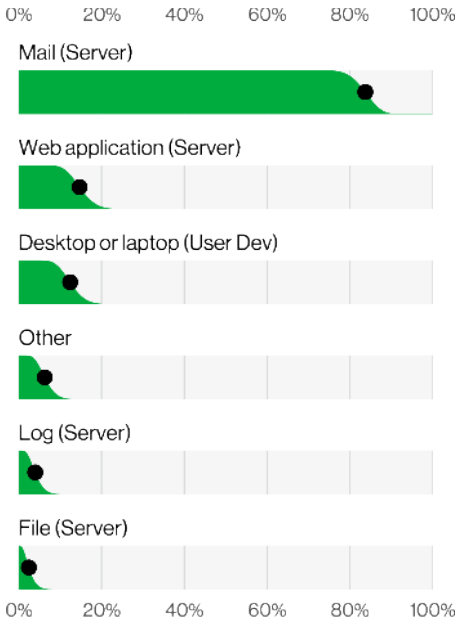


Figure 98. Top Asset varieties in MQOGEU breaches (n=130)

Professional, Scientific and Technical Services NAICS 54

Frequency	3,566 incidents, 681 with confirmed data disclosure
Top patterns	System Intrusion, Basic Web Application Attacks and Social Engineering represent 89% of breaches
Threat actors	External (84%), Internal (17%), Multiple (1%) (breaches)
Actor motives	Financial (90%), Espionage (10%) (breaches)
Data compromised	Credentials (56%), Personal (48%), Other (26%), Internal (14%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	The top three attack patterns remain System Intrusion, Basic Web Application Attacks and Social Engineering, but they have changed order compared to last year's report.

Summary

Denial of Service attacks are a serious problem in this industry, and while they rarely result in a data breach, they can still have a significant impact. The System Intrusion attack pattern is in the first position again this year, while Social attacks are less prominent, but still in the top three.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	No change	No change
Social Engineering	Less	Less	No change
System Intrusion	Greater	Greater	No change

Services denied

As a NAICS code with the name of Professional, Scientific and Technical Services might imply, this sector relies on their internet presence to provide their highly skilled offerings to their customers. This means that when they are hit with a DoS attack, particularly the higher volume distributed varieties, they definitely feel the impact. This past year has been a hard one for this sector, with the DoS attacks accounting for almost half of the incidents recorded. And even though this type of attack rarely leads to a reportable data breach, it can still do significant damage to the victim.

The devil you know

Moving to breaches, the System Intrusion pattern remained at the top of our pyramid, while Basic Web Application Attacks and Social Engineering switched places. So, the same players remain on the field, they are simply playing different positions.

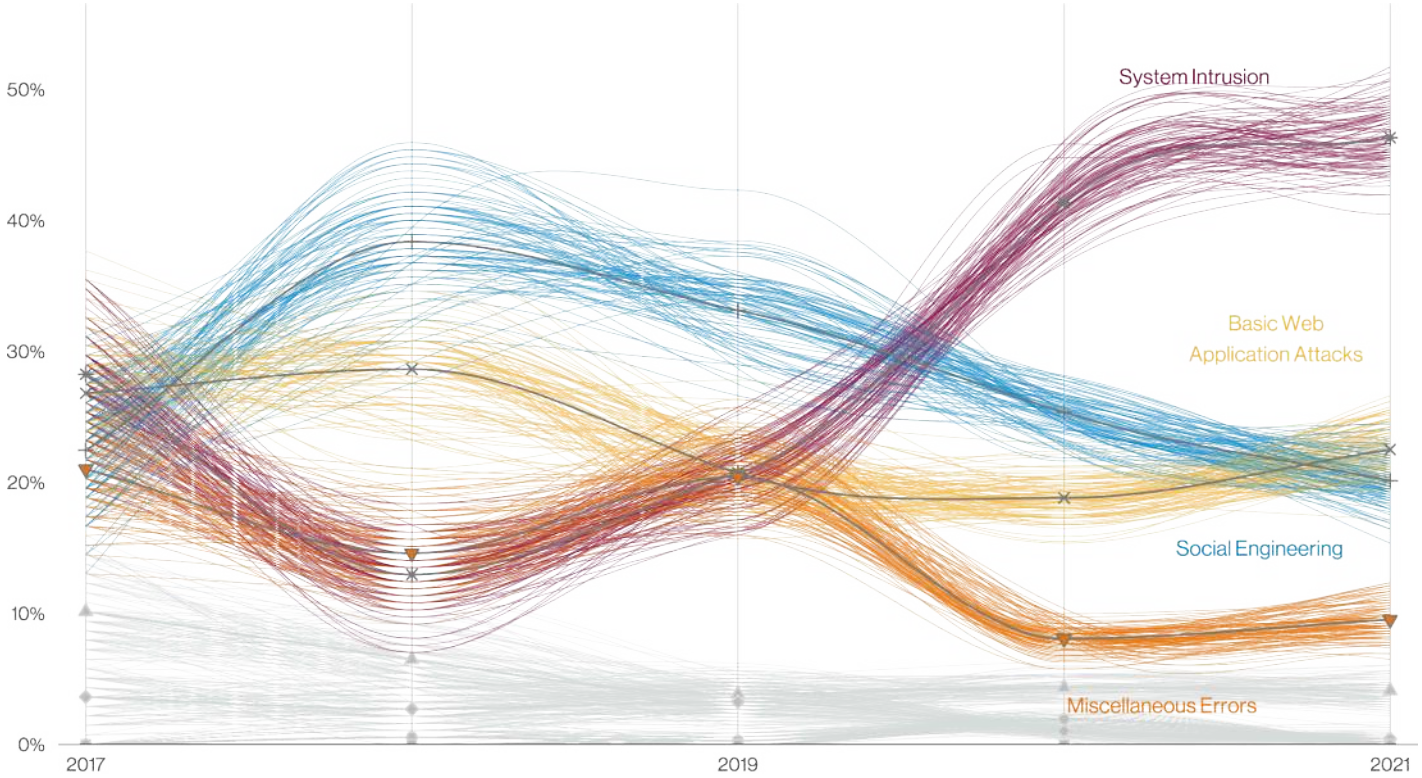


Figure 99. Patterns over time in Professional, Scientific and Technical Services breaches

The perpetrators of these top three attack patterns tend to be External. The Internal actor breaches were down this year by comparison to last year's report. Surprisingly we saw a small uptick in the multiple actor breaches in this sector this year. These are when an external actor recruits an internal or partner actor to help them out with the breach activities. Sometimes they are paid for their troubles, and sometimes it is a more subtle form of influence by an acquaintance or significant other exerting pressure on the person with the access to data. Either way, the result is a breach that can be more difficult to detect, since it is someone on the inside facilitating the access under the guise of conducting their regular duties.

Days gone by

Looking back over the years in this sector, the Miscellaneous Errors pattern was in the top three. However, as Figure 99 shows, in 2019, the System Intrusion pattern began its meteoric rise to the top, eventually far surpassing Errors. This sector mirrors the overall dataset in terms of the top attack patterns. The top three here are the top three patterns in the full dataset, so clearly, these patterns are holding sway in a number of business categories.

Public Administration NAICS 92

Frequency	2,792 incidents, 537 with confirmed data disclosure
Top patterns	System Intrusion, Miscellaneous Errors and Basic Web Application Attacks represent 81% of breaches
Threat actors	External (78%), Internal (22%) (breaches)
Actor motives	Financial (80%), Espionage (18%), Ideology (1%), Grudge (1%) (breaches)
Data compromised	Personal (46%), Credentials (34%), Other (28%), Internal (28%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Account Management (CSC 5)
What is the same?	Miscellaneous Errors remain in the top three patterns in the same place as last year.

Summary

The System Intrusion pattern is the newest big dog to arrive on the scene in this sector. Employees continue to be a cause of breaches in this vertical, although Internal actors are seven times more likely to make a mistake than to commit a malicious act that causes a breach.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	Greater	Less
Miscellaneous Errors	No change	Less	Less
System Intrusion	Greater	Greater	Greater

Here and now

The System Intrusion pattern has drop-kicked the Social Engineering pattern right out of the "top three" club. This was quite the coup, considering the Social Engineering pattern was in the top spot last year. In part, this may be attributed to some prominent and far-reaching supply chain breaches that came to light last year.

As the Social Engineering pattern fell, the Basic Web Application Attacks stepped in to fill the vacuum. Miscellaneous Errors remained in the middle spot, with the trio of Misconfiguration, Misdelivery and Loss nearly tied for what caused the most error-based breaches in this sector.

The occurrence of errors in this industry accounts for the prevalence of breaches caused by the Internal actor. While there was a smattering of Misuse breaches in this sector, Internal actors are about seven times more likely to make a mistake that causes a breach than they are to do something malicious.

We have said before how popular Credentials are as a data type to be raided. However, this year's data showed a drop from 2021's report, when it was 80% in this industry. Personal was only 18% last year, but has now catapulted into the top spot.

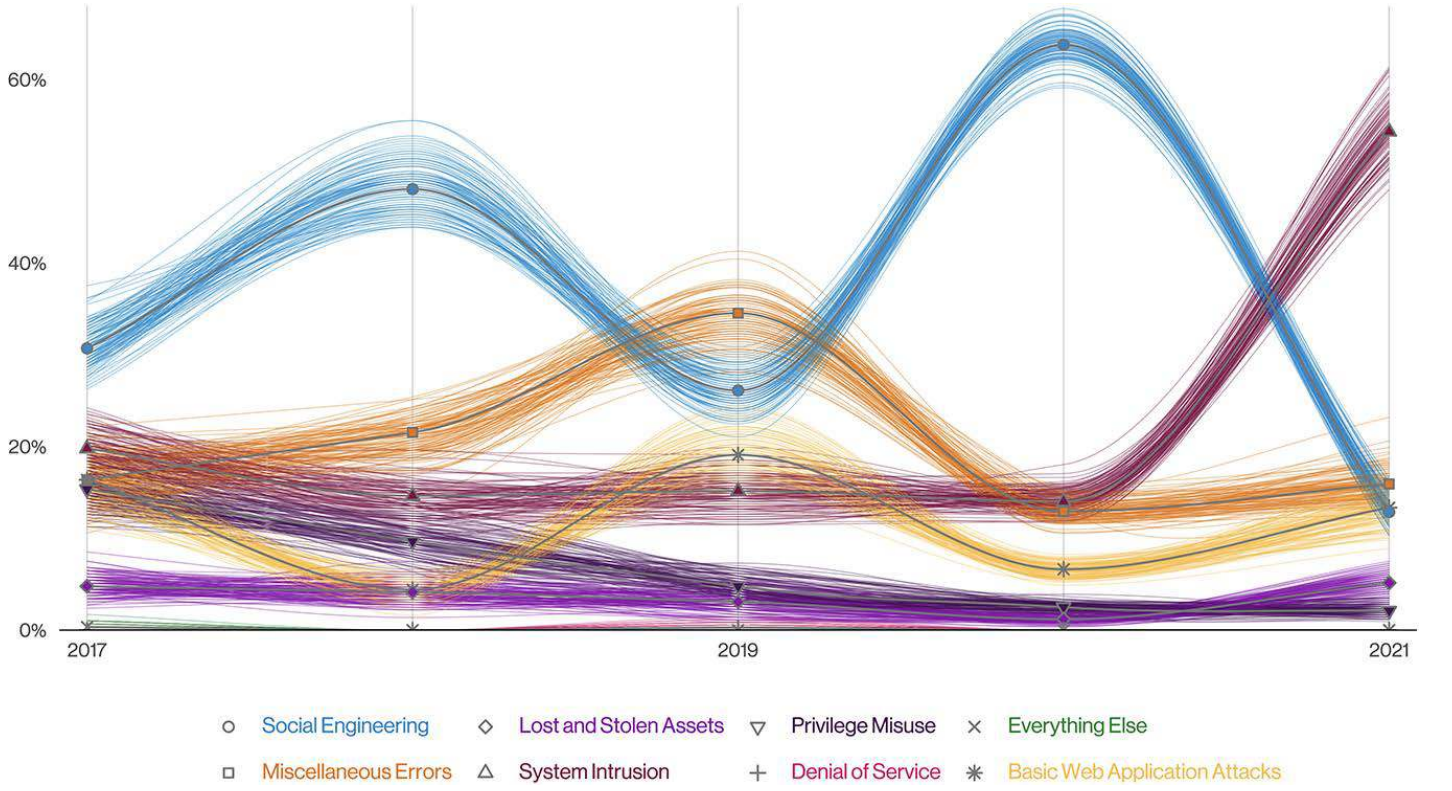


Figure 100. Patterns over time in Public Administration breaches

Step into my raggedy DeLorean

In honor of our 15-year anniversary, we wanted to take a look back in time at what has changed in this sector. Just three years ago, the top motive was Espionage, at 66% of breaches. Five years ago, it was 64%, which illustrates that it has been a persistent challenge for Government entities. This makes sense, when you consider that regardless of which Government entity we are talking about, someone wants to know what they're up to. Speaking of malicious—we found that the Espionage motive is up from 4% from last year to 18% this year. Internal breaches also increased from last year, and we have the motive of Grudge popping up in our list for a change.

Figure 101 illustrates the change in the Espionage-motivated actors in this industry since 2017. As you can see, when the Espionage motive fell, the Financial-motivated attacks rose. It appears that the Public Administration sector has joined the rest of us in being targeted by criminals looking to make a buck. Welcome to the party, pal![27]

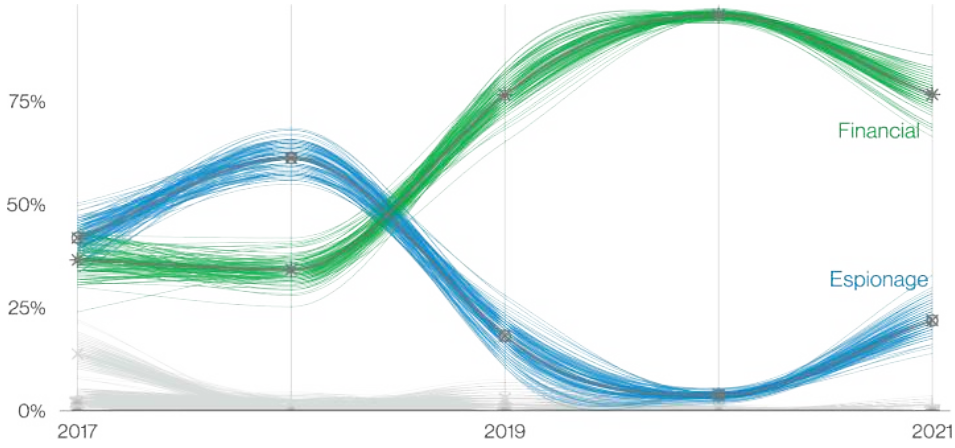


Figure 101. Actor motives over time in Public Administration breaches

27 Admit it, you read this in John McClane's voice.

Retail NAICS 44-45

Frequency	629 incidents, 241 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 84% of breaches
Threat actors	External (87%), Internal (13%) (breaches)
Actor motives	Financial (98%), Espionage (2%) (breaches)
Data compromised	Credentials (45%), Personal (27%), Other (25%), Payment (24%) (breaches)
Top IG1 protective controls	Security Awareness and Skills Training (CSC 14), Access Control Management (CSC 6), Secure Configuration of Enterprise Assets and Software (CSC 4)
What is the same?	These organizations continue to be impacted by a variety of threat actors that leverage a range of tactics such as deploying malware to capture credit cards being processed by webforms and more common tactics like phishing.

Summary

The Retail industry is experiencing the same types of attacks they suffered last year: Use of stolen credentials, Phishing and Ransomware.

Patterns in years	5-year difference	3-year difference	Difference with peers
Basic Web Application Attacks	No change	Less	Less
Social Engineering	No change	Greater	Greater
System Intrusion	Greater	No change	Greater

Our society, indeed the entire globe, has seen an astounding amount of change over the last couple of years. The Retail industry, on the other hand, has not, at least when it comes to breaches. As tempting as it was to simply cut and paste our findings for this industry from last year's report, we bravely refrained from doing so. Nevertheless, while the needle has not moved very much from when we last looked at it, there are a few noteworthy findings.

Social attacks, roughly split between Phishing (53%) and Pretexting (47%), have been on the rise over the last few years in the Retail industry: 7% in 2016, 13% in 2018, 29% this year. This accounts for Social Engineering's position in the top three patterns. Therefore, as one might expect, Credentials are the top data type compromised in this vertical. In many cases those Credentials are later utilized to hack into servers and load ransomware (47%). Then the criminals sit back and wait for a big payday.

One interesting finding this year is that the Malware enumeration of "Capture app data" in the Retail industry is 7 times higher than the other industries. This goes some way to explain why the System Intrusion pattern is ranked at first place in this industry. The "Capture app data" functionality is one that we commonly see in Magecart-type attacks, in which the attacker will typically exploit a vulnerability, use stolen credentials to gain access to an e-commerce server and then just chill there and take a little sumpin' sumpin' for themselves, almost always payment card data.

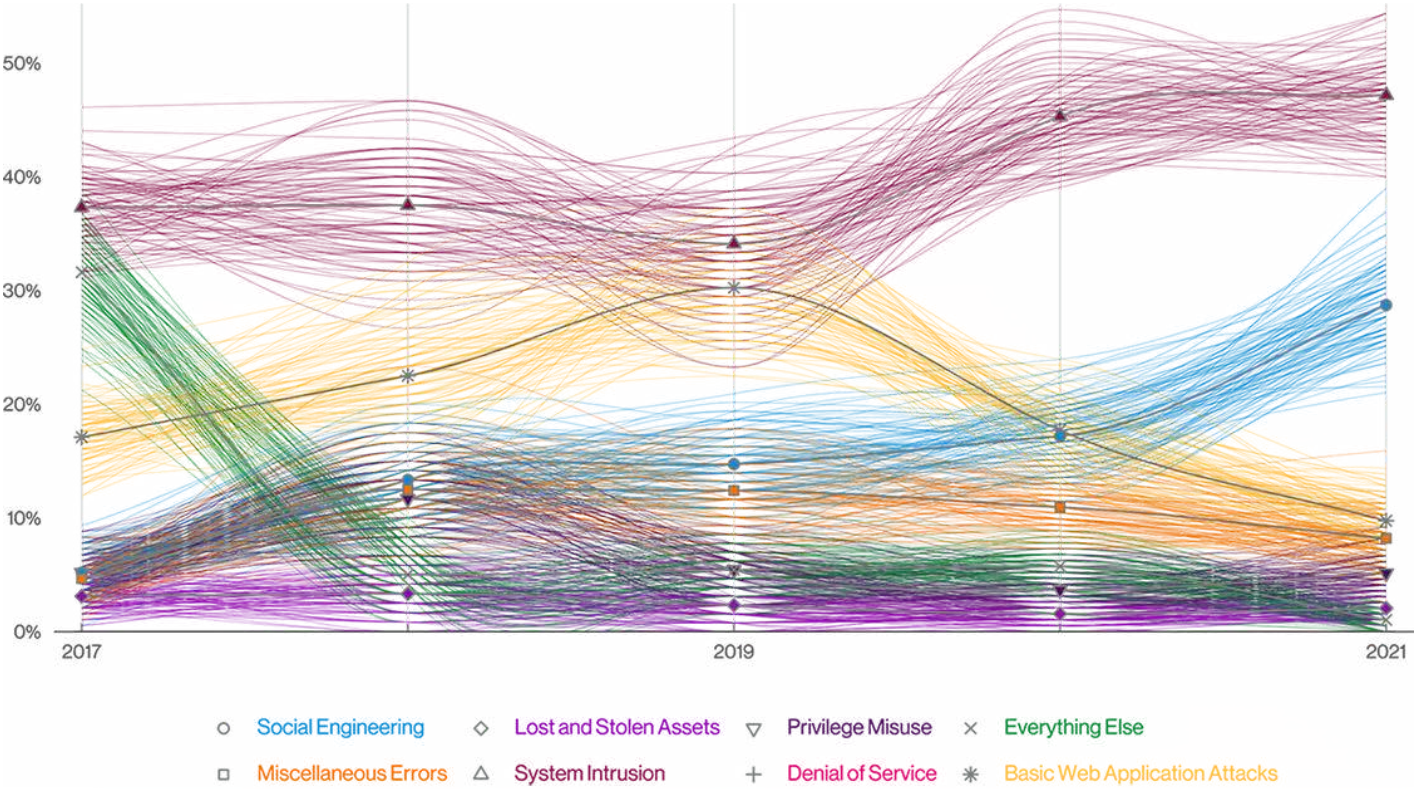


Figure 102. Patterns over time in Retail industry breaches

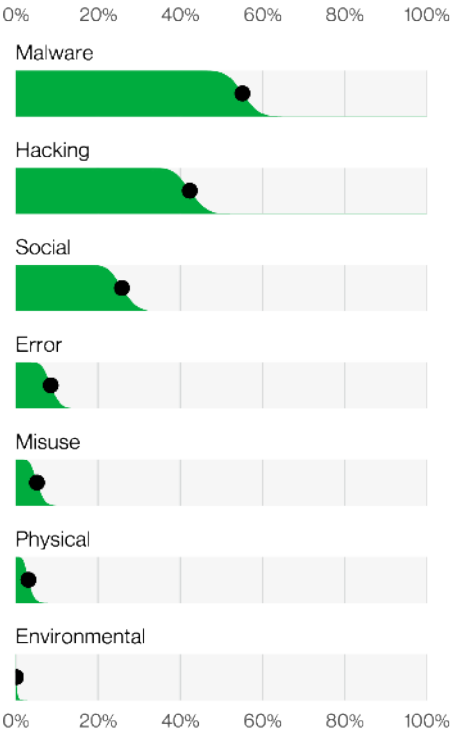


Figure 103. Actions in Retail industry breaches (n=241)

Finally, when a company in the Retail industry learns that they have become a victim, it's via fraud detection mechanisms (e.g., Common Point of Purchase [CPP] or law enforcement) more than any other industry. This is perhaps a rather intuitive finding given the fact that Retail is responsible for so many transactions, but it is noteworthy nonetheless.

Very Small Business Cybercrime Protection Sheet

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

When cybercrime makes the news, it is typically because a large organization has fallen victim to an attack. However, contrary to what many may think, very small organizations are just as enticing to criminals as large ones, and, in certain ways, maybe even more so. Threat actors have the "we'll take anything we can get" philosophy when it comes to cybercrime. These incidents can and have put small companies out of business. Therefore, it is crucial that even very small businesses (10 employees or less) should take precautions to avoid becoming a target. Large organizations have large resources, which means they can afford Information Security professionals and cutting-edge technology to defend themselves. Very small businesses on the other hand have very limited resources and cannot rely on a trained staff. That is why we wrote this section.

If you own or manage a very small business, we offer the following recommendations or best practices. We suggest you print out or tear out this section and refer to it when a concern appears.

What are the most common threats facing my business?

The number one action type in our dataset for very small businesses are ransomware attacks. Ransomware is a type of malicious software that encrypts your data so that you cannot view or utilize it, and once the ransomware is triggered the threat actor demands a (frequently large) payment to unencrypt it. This is where having those offline[28] backups come in handy.

The second most common is the Use of stolen credentials. Attackers can get your credentials (username and password) via many different methods. Brute force attacks (where attackers use automation to try numerous combinations of letters, symbols and numbers to guess your credentials), various types of malware (thus the value of having an up-to-date Antivirus), reused passwords from another site that has been hacked and last but not least, social attacks such as Phishing and Pretexting.[29]

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

Phishing is a type of social attack

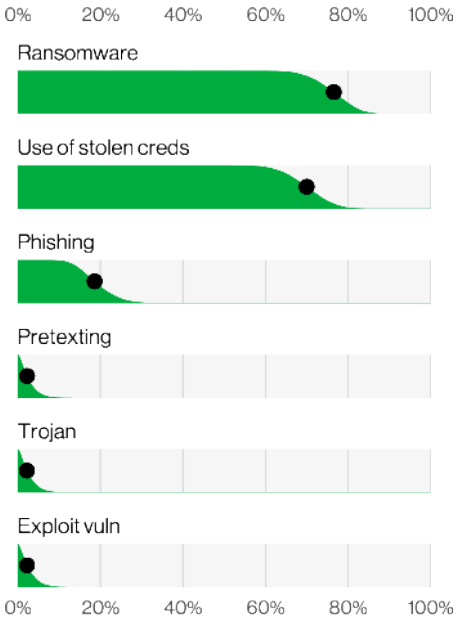


Figure 104. Action varieties in 1 to 10 employee organization breaches (n=61)

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

(usually via email) in which the attacker tries to fool you into doing something you should not, such as providing them with your user name and password or clicking on a malicious link. Examples include "click here to reset your password" or download an invoice, view the pdf attachment, verify your bank account number, etc. These attacks can be extremely realistic and are often very hard to identify.

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

How do I know I have become a victim?

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

What to do to avoid becoming a target

1. Use two-factor authentication[30]
2. Do not reuse or share passwords[31]
3. Use a password keeper/generator app
4. Be sure to change the default credentials of the Point of Sale (PoS) controller or other hardware/software
5. Ensure that you install software updates promptly so that vulnerabilities can be patched
6. Work with your vendors to be sure that you are as secure as you can be, and that they are following these same basic guidelines
7. Keep a consistent schedule with regard to backups and be sure to maintain offline backups—meaning that they are not on a device connected to a computer
8. Ensure that the built-in firewall is switched on for user devices such as laptops and desktops ("on" may not be the default)
9. Use antivirus software, for all your devices. Smart phones, tablets and credit card swipers are just as important as laptops and computers. It won't catch everything, but it will help
10. Do not click on anything in an unsolicited email or text message
11. Set up an out of band method for verifying unusual requests for data or payments
12. Make sure the computer used for financial transactions is not used for other purposes such as social media or email
13. Use email services that incorporate phishing and pretexting defenses and use a web browser that warns you when a website may be spoofed

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

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

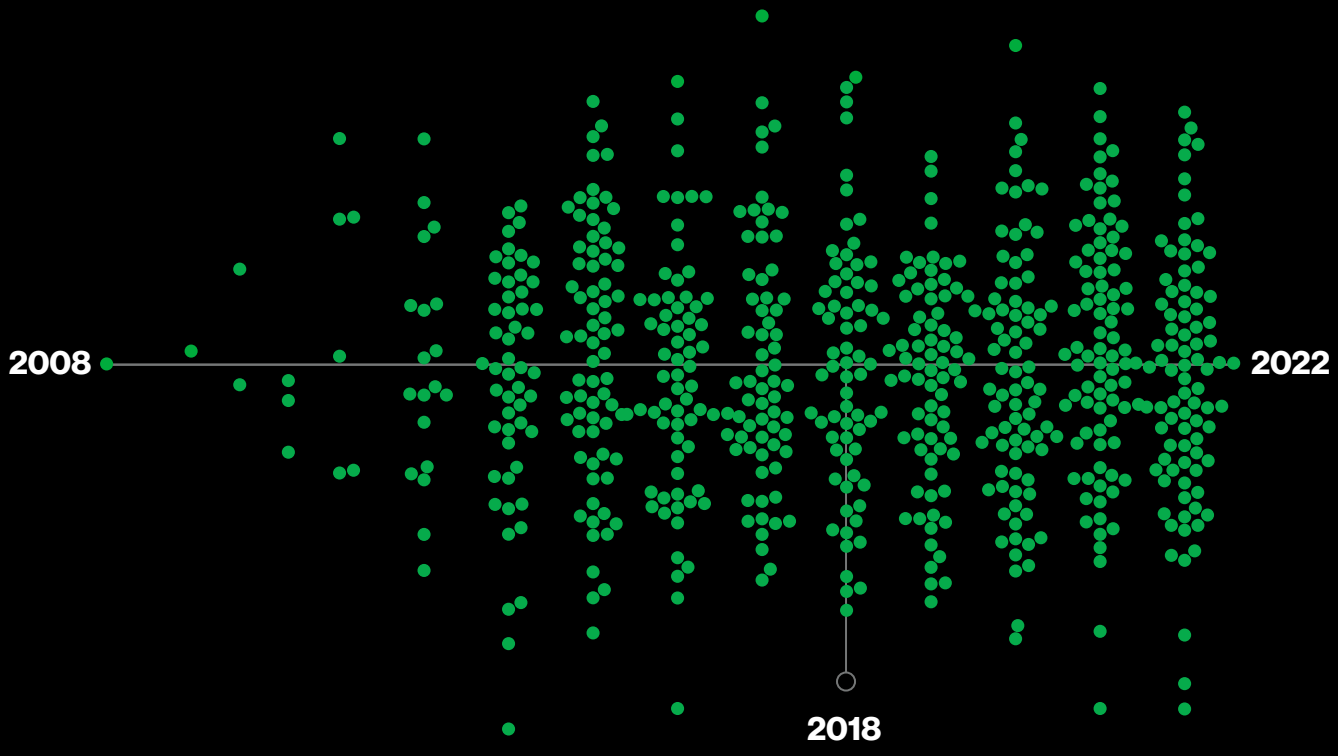
Familiarize yourself with these resources, and draw up a plan for what steps you will take if you find your organization has become a victim. Plan this ahead of time instead of waiting until your company's "hair" is on fire. Even if it is just a document that contains the contact information for all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

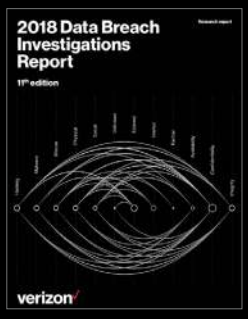
Some planning on your part, along with a bit of educating the people most likely to encounter these kinds of attacks, can go a long way in helping to make your small company safer.

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

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

5 Regions


2008
2022
2018


2018 Data Breach Investigations Report
11th edition
verizon

Introduction to Regions

This edition of the DBIR marks the third year that we have analyzed incidents and presented them from a macro-region perspective. It is our hope that our readers find this more global view of cybercrime helpful and informative. As we have mentioned in the past, we have greater or lesser visibility into a given region based on numerous factors such as contributor presence, regional disclosure regulations, our own caseload and so on.

If you reside and work in a part of the world that is not mentioned in the following pages, please contact us about becoming a data contributor and encourage other organizations in your area to do the same, so that we may continue to expand and refine our coverage each year. It is important to keep in mind that if you do not see your region represented here it does not necessarily mean that we have no visibility at all into the region, but simply that we do not have enough incidents in that geographic location to be statistically relevant for a stand-alone section.

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

APAC: Asia 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 North Africa (002), Europe and Northern Asia (150) and Western Asia (145)

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

LAC: Latin America and Caribbean, which consists of breaches in South America (005), Central America (013) and Caribbean (029)

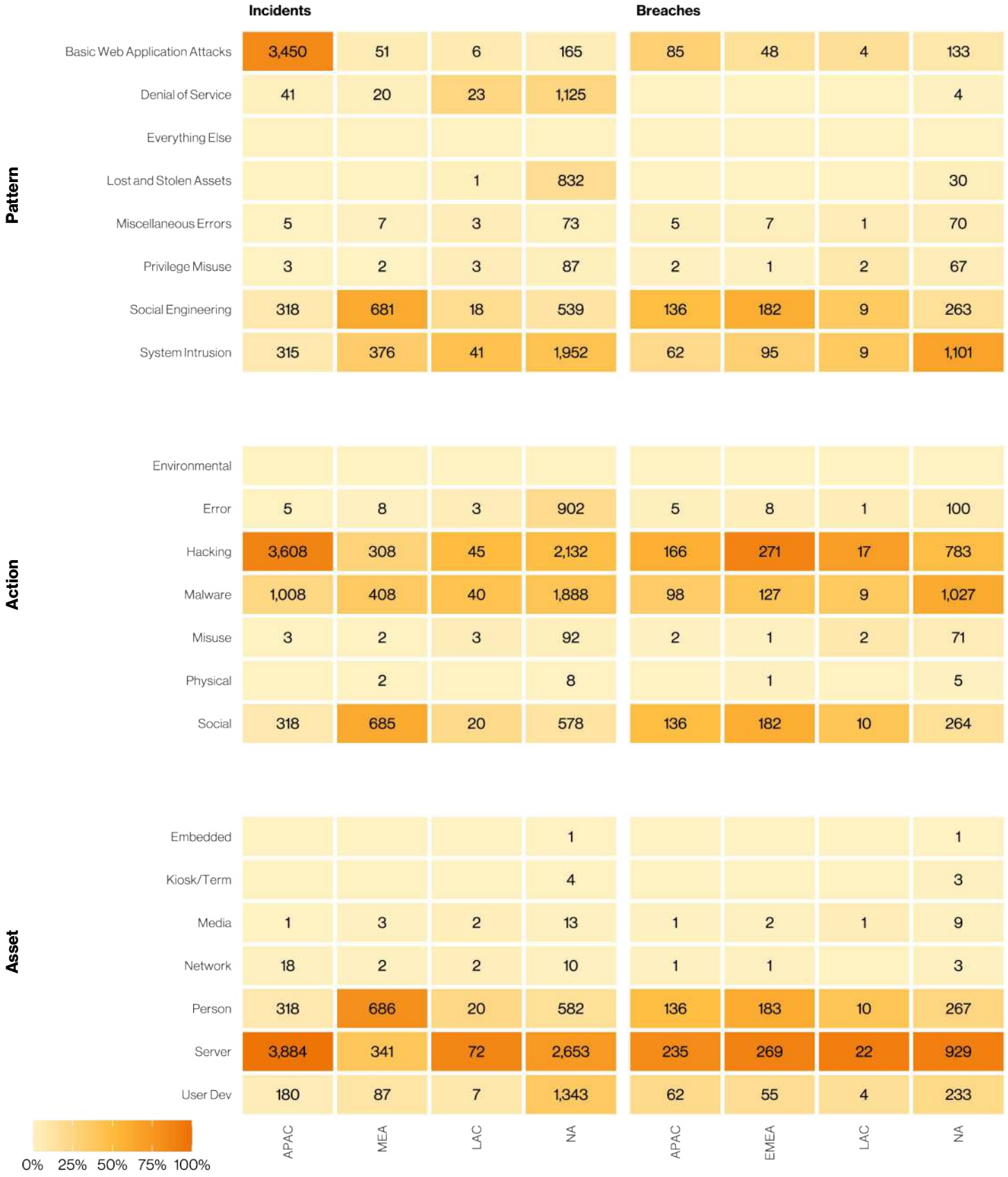


Figure 105. Incidents and breaches by region

Asia Pacific (APAC)

Frequency	4,114 incidents, 283 with confirmed data disclosure
Top patterns	Social Engineering, Basic Web Application Attacks and System Intrusion represent 98% of breaches
Threat actors	External (98%), Internal (2%) (breaches)
Actor motives	Financial (54%), Espionage (46%), Secondary (1%) (breaches)
Data compromised	Credentials (72%), Internal (26%), Secrets (18%), Other (11%) (breaches)
What is the same?	Basic Web Application Attacks and Social Engineering continue to be persistent threats for this region.

Summary

APAC experiences a high number of Social and Hacking related attacks, but has a much lower number of Ransomware cases than other areas.

This year in APAC we see the well-known trifecta of Hacking (58%), Social (48%) and Malware (36%) taking center stage. The majority of incidents were perpetrated by attackers with Financial (81%) motives. However, State-affiliated (19%) and Nation-state (1%) actors with the motive of Espionage (19%) were rather common in APAC as well.

The predominant Hacking action was 'Use of stolen credentials' (83%) being mostly used to compromise a web application (60%). The social attacks in this region accounted for approximately twice the number we saw in other regions, and consisted almost exclusively of Phishing (99%). Similar to last year, we saw a comparatively low number of ransomware cases in APAC. Ransomware was involved in 10% of breaches in APAC as opposed to the overall dataset average of 25%.

There were a substantial number of defacement attacks in this region this year (over 2,800), which pushed the attribute of "Integrity" up to 75% of incidents. This is interesting in that our data does not reflect a high number of defacements in other areas of the world. And while a nuisance, they usually have a lesser impact than a ransomware case for example.

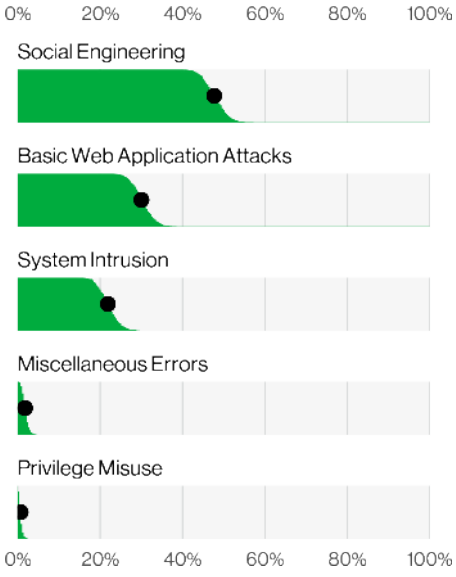


Figure 106. Top patterns in Asia Pacific breaches (n=283)

Europe, Middle East and Africa (EMEA)

Frequency	1,093 incidents, 307 with confirmed data disclosure
Top patterns	Social Engineering, System Intrusion and Basic Web Application Attacks represent 97% of breaches
Threat actors	External (97%), Internal (3%) (breaches)
Actor motives	Financial (79%), Espionage (21%) (breaches)
Data compromised	Credentials (67%), Internal (67%), Secrets (20%), Other (18%) (breaches)
What is the same?	The patterns are the same top three, but they have rearranged themselves in order. External actors continue to perpetrate the vast majority of breaches in this region.

Summary

The rise of the Social Engineering pattern in this region illustrates the need for controls to detect this type of attack quickly. Credential theft remains a large problem as well, as illustrated in the continued persistence of the Basic Web Application Attacks pattern in EMEA.

The EMEA region, covering Europe, the Middle East and Africa, has seen a sharp increase in the Social Engineering pattern in the past year (to almost 60% of breaches). While the same three patterns continue to afflict the region, Social Engineering was in third place in last year's data. At the same time, we saw Basic Web Application Attacks plummet (Figure 108 on the next page). In last year's report, they accounted for over 50% of the breaches in this region, but have now dropped to the 15% range. The more complex System Intrusion pattern, however, continues to thrive and still holds second place at 30%.

Credential theft remains a problem in this region, and regardless of how threat actors obtain those credentials (the rise of Social Engineering provides a likely answer), once they are acquired they use them against your infrastructure. With the foothold this provides, attackers are then able to leverage their access to obtain more Credentials via Phishing, or utilize details gained from company emails to craft realistic pretexts as part of BEC attacks.

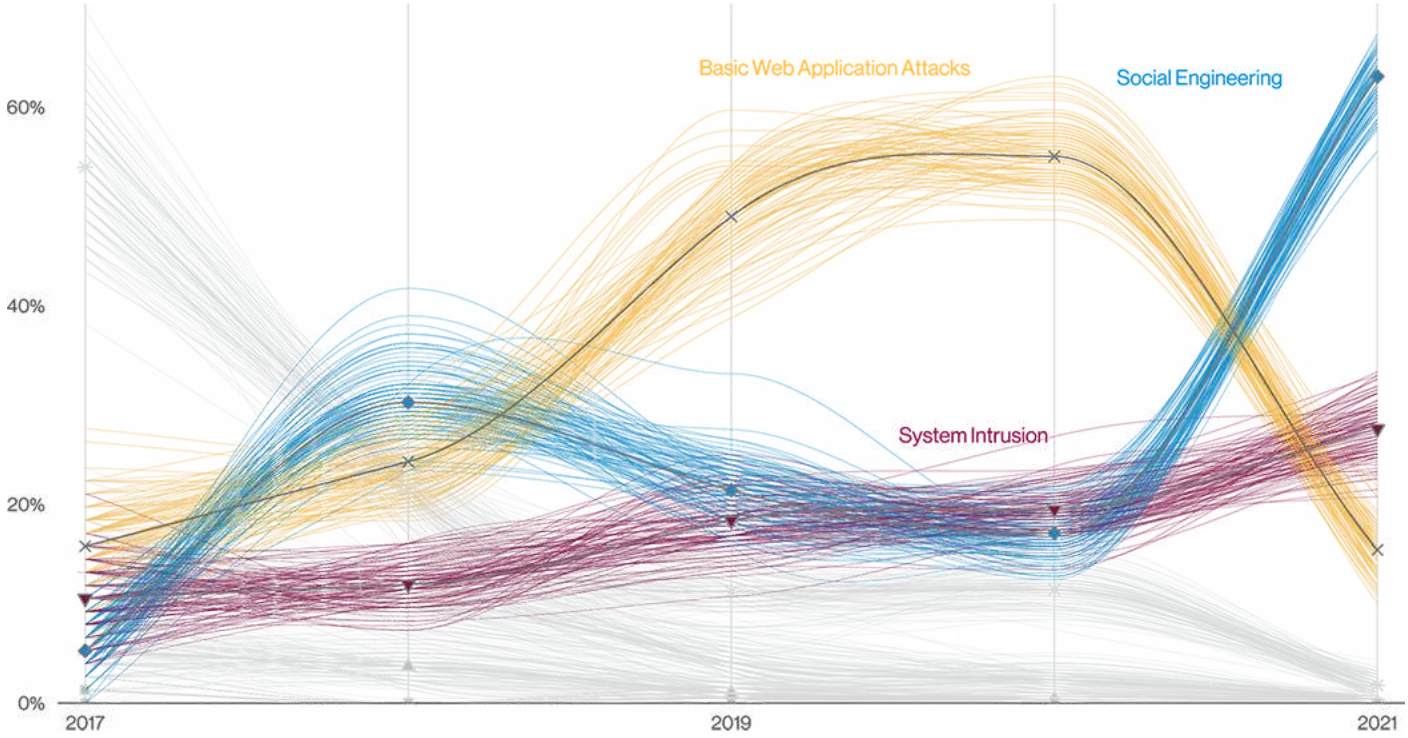


Figure 108. Patterns over time in Europe, Middle East and Africa breaches

Threat actors are most commonly attacking Web application servers as a means to gaining access (since it is the most easily reached via the internet) along with Email servers. Email servers provide both an opportunity to mine the account's contents for interesting internal company data for espionage, and a venue to gain more access via phishing other employees. In terms of the people being targeted, unsurprisingly, phishers like to compromise people in Finance since they have convenient access to the organization's money transfer capabilities. If they can convince one of those targets to send them currency under the guise of a legitimate transaction, they don't need to worry about monetizing data.

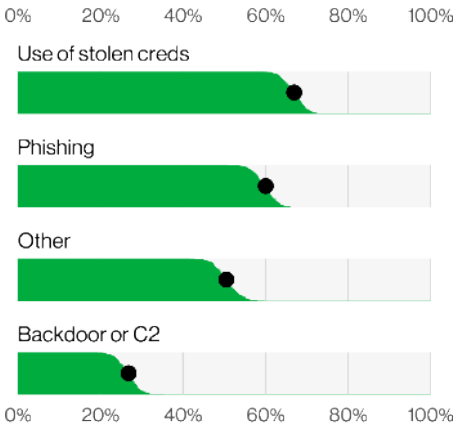


Figure 107. Top Action varieties in Europe, Middle East and Africa breaches (n=283)

Northern America (NA)

Frequency	4,504 incidents, 1,638 with confirmed data disclosure
Top patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 90% of breaches
Threat actors	External (90%), Internal (10%), Multiple (1%) (breaches)
Actor motives	Financial (96%), Espionage (3%), Grudge (1%) (breaches)
Data compromised	Credentials (66%), Internal (21%), Personal (20%), Other (20%) (breaches)
What is the same?	The top three patterns remain the same, only their order has changed. External actors continue to hold sway in breaches in this region.

Since our dataset shows a strong Northern American (NA) bias, we find that as this region goes, so goes the dataset. This is nowhere more evident than when looking at the top three patterns for Northern America. These three mirror the top patterns for the full dataset. The bias is due to a combination of things. First of all, the breach disclosure laws in NA are quite robust, and they continue to evolve. Determining all the places you must report a breach to in Northern America almost requires a decoder ring and Magic 8 Ball. In addition to this, most of our data sharing contributors have excellent visibility into the NA region, in both private and public sectors. And, frankly, our English is excellent, our French and Portuguese passable, but beyond that our linguistic facilities falter. All of this means we have very good data on this region–more so than any other.

Summary

The System Intrusion pattern has become the dominant pattern in this region. Social Engineering gave way as System Intrusion increased, but there remains a large problem with social actions such as Phishing in Northern America. Basic Web Application Attacks continue to beset organizations here as well.

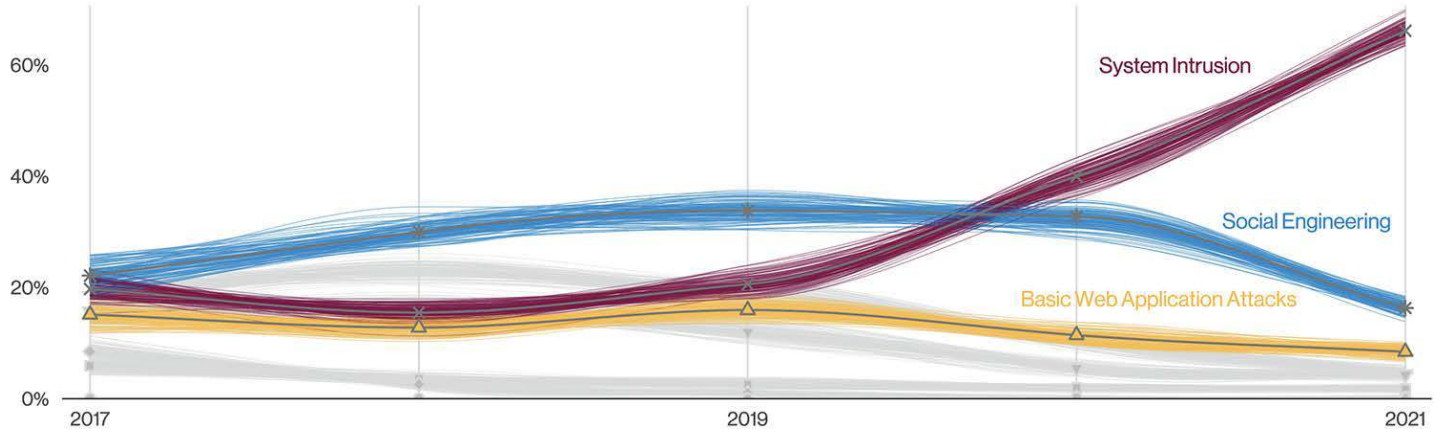


Figure 109. Patterns over time in Northern America breaches

We can see in Figure 109, that while the Social Engineering pattern has held sway for some time as the top pattern in breaches, last year showed a change. The top pattern is now System Intrusion, which is also where most of the Ransomware cases reside. It is surely no secret that Ransomware has been rising for several years and has become quite prominent in our data.

In fact, for cases where malware is present, Ransomware is by far the most common variety (Figure 110). Increasingly over the past several years, this attack has the one-two punch of causing both a loss of access to the data, and the need to report a data breach as the actors have also taken a copy of the organization's data.

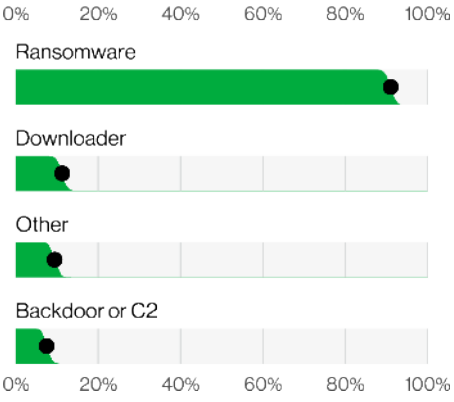


Figure 110. Top Malware varieties in Northern America breaches (n=647)

With our Social Engineering pattern comes Social actions, of course. The most common is a straight-up Phish, with Pretexting coming in second (Figure 111).

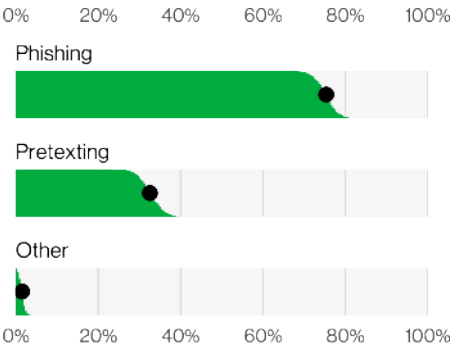


Figure 111. Top Social varieties in Northern America breaches (n=264)

Pretexting takes more work, so it may be employed against higher-value targets. We see this in cases where a Business Email Compromise attack offers up a fake invoice or something similar to attempt to get either money or banking info from the target. As expected, people in the Finance function of the organization are likely to be the target of more advanced attacks.

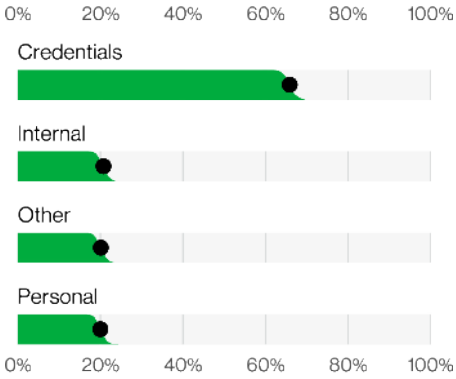


Figure 112. Top Confidentiality data variety in Northern America breaches (n=944)

In attacks that result in confirmed data breaches, the data type most frequently stolen is, unsurprisingly, Credentials. They are stolen more often than the next two most common varieties combined. Perhaps Credentials are like popcorn, you cannot steal just one.

Latin America and the Caribbean (LAC)

Frequency	92 incidents, 24 with confirmed data disclosure
Top patterns	System Intrusion Denial of Service and Social Engineering represent 88% of incidents
Threat actors	External (95%), Internal (7%), Multiple (1%) (incidents)
Actor motives	Financial (92%), Convenience (3%), Espionage (2%), Grudge (2%), Other (2%) (incidents)
Data compromised	System (51%), Credentials (40%), Internal (21%), Other (12%) (incidents)
What is the same?	Financially motivated actors continue to be the main threat actors in this region.

Summary

Much like the rest of the world, Latin American businesses face attacks targeting the functioning of their businesses, such as Ransomware and Denial of Service attacks. These attacks account for 37% and 27% of incidents respectively.

Water might spin in the opposite direction in the Southern Hemisphere, but breaches and incidents seem to go down just as they do elsewhere. Unfortunately, our data collection for this section of the world is still very sparse, and we continue to be in need of partners to help us round out our understanding of what's going on with our friends in the South. If your organization operates in this region please reach out and join us.

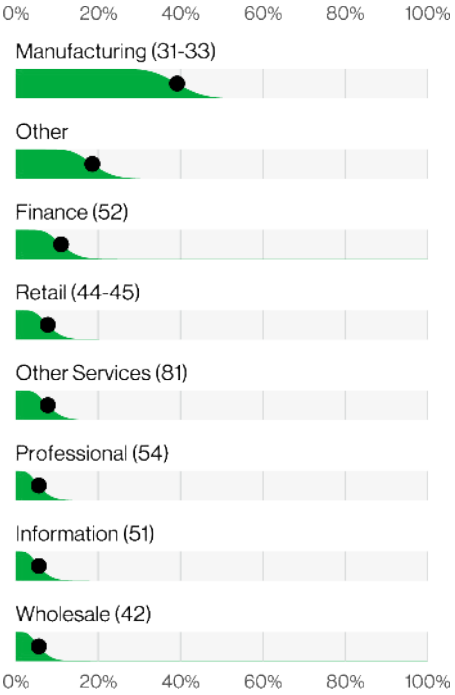


Figure 113. Top industries in Latin America and the Caribbean incidents (n=92)

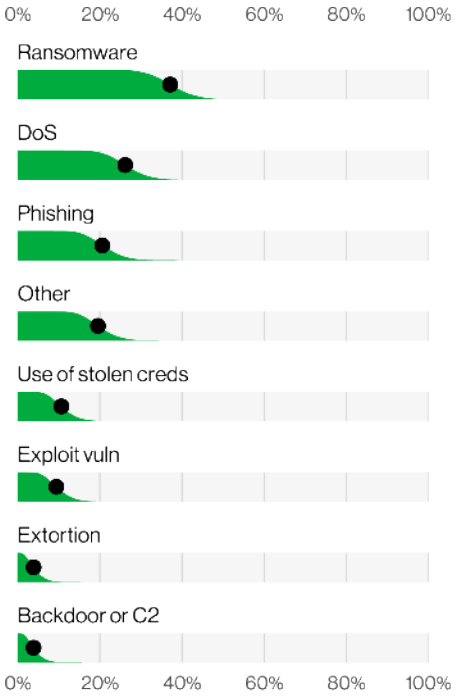
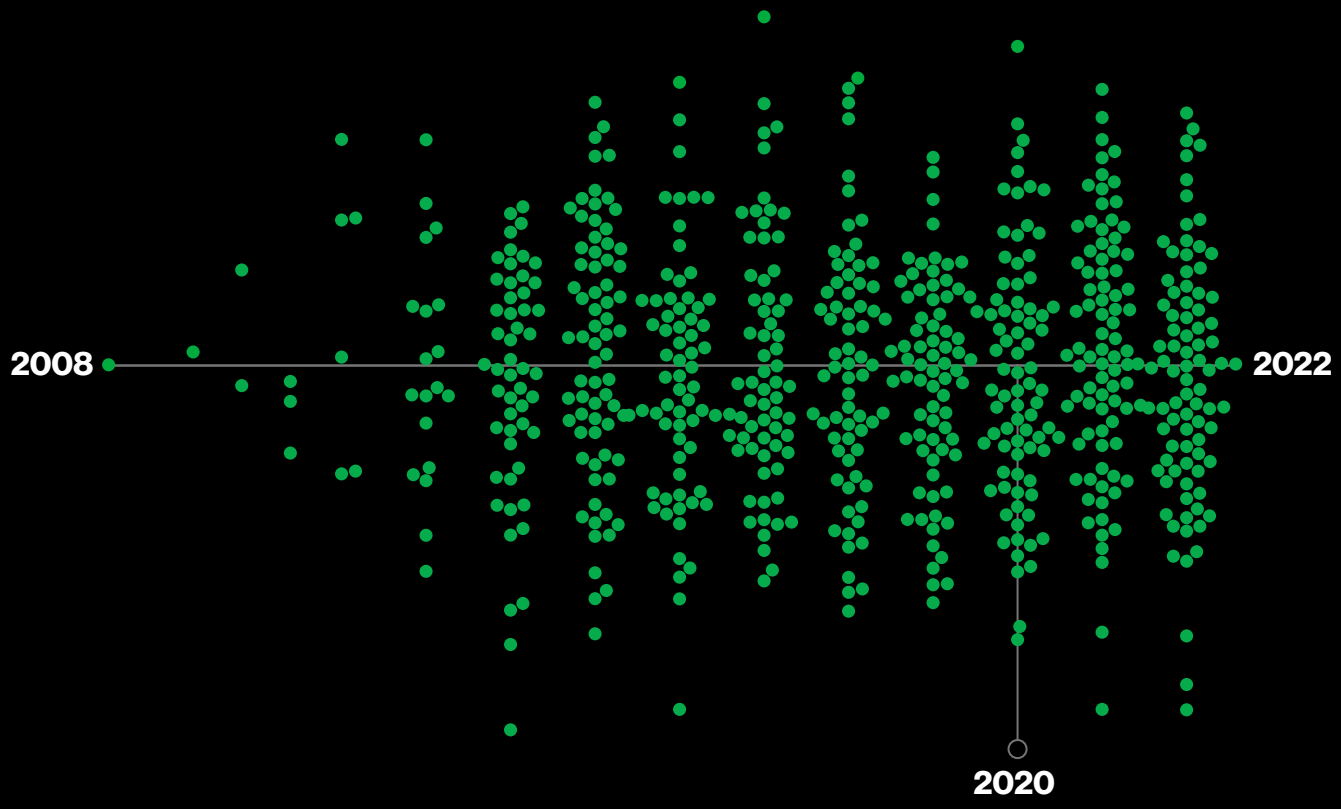


Figure 114. Top Action varieties in Latin America and the Caribbean incidents (n=89)

Figure 113 provides a breakdown of what industries have been breached in Latin America. While we don't necessarily have a large number of breaches, we certainly have a diverse collection of compromised organizations, with approximately 20% of victims not from the top seven.

Just like their Northern America counterparts, Latin America industries face the looming threat of Ransomware. This attack type accounts for more than 30% of their incidents. This is followed by the ever-present DoS attack. This region of the world also experiences its fair share of Phishing attacks and Stolen credentials, which we realize may be beginning to sound like a broken record. Or, erg ... would a buffering looping advert be the modern equivalent? At this point we're beginning to get the feeling that some of these attacks are universal to anyone who has some form of internet presence.


2008
2022
2020


DBIR
Data Breach Investigations Report
verizon

6 Wrap-up

This concludes another installment of the Data Breach Investigations Report.

As always, it is our hope that you have found the information herein to be informative, actionable and enjoyable to read. While we do our best to bring the occasional smile to our readers, we assure you that we take cybercrime seriously indeed. The five of us on the DBIR team feel truly fortunate to be in this fight alongside each and every one of you. We will do our best to keep providing you with whatever insight we can from our data, and we wish all of you the greatest success. Here is to a brighter tomorrow! We hope to see you all again next year. We will close with a line from a former report that we feel is particularly apropos:

"Be well, be prosperous, and be prepared for anything."

Year in review

January

As the New Year began, the Verizon Threat Research Advisory Center (VTRAC) was still tracking the SolarWinds-related campaigns. Tools emerged for security teams to use in Azure/Microsoft O365 environments. January's patch Tuesday included one remote code execution vulnerability in Windows Defender that was already being exploited in the wild (zero-day). SonicWall was investigating an attack exploiting "probable zero-day vulnerabilities" in certain secure remote access products. Researchers reported a fourth malware used in the SolarWinds operation. "Raindrop" is a digital cousin to the Teardrop malware. Raindrop was installed only on select targets and delivered Cobalt Strike. After zero-day attacks, Apple released security updates for three vulnerabilities in iOS/iPadOS. The best news in January came when Europol closed down Emotet's infrastructure redirecting 1.6 million victim systems to servers controlled by law enforcement.

February

Google kicked off February with Chrome browser updates to mitigate one zero-day. SonicWall, Cisco, Fortinet and Palo Alto Networks all released patches and updates to VPN and remote access products. SonicWall's CVE-2021-20016 was already being exploited. Two more zero-day vulnerabilities were patched on patch Tuesday, one each by Microsoft and Adobe. CERT-FR reported a supply-chain compromise of Centrion by the Russian Sandworm threat actor that exhibited commonalities with the 2020's SolarWinds Orion and Accellion attacks. Two days before the Super Bowl, the fresh water plant for a small city in Florida was briefly breached. One processing chemical was manipulated but quickly detected and corrected. IT security at the plant did almost everything wrong: the attacker entered via TeamViewer with a shared static password on a Windows 7 computer.

March

March roared in with out-of-cycle updates for four zero-day vulnerabilities in Microsoft Exchange that had been initially exploited in January. At least 30,000 Exchange servers were reported to be victims of Hafnium, a newly-labeled APT-grade threat actor aligned with the national security interests of China. The flaws were dubbed, "ProxyLogon." Scanning and exploitation quickly surged. Other APTs and other threat actors breached unpatched Exchange servers. Microsoft patched 89 vulnerabilities including CVE-2021-26411, a zero-day in Internet Explorer exploited by a North Korean threat actor targeting security researchers. The month closed with Apple releasing patches for a zero-day vulnerability in Apple iOS/iPadOS/WatchOS.

April

In early April, the VTRAC collected reports of attacks by APTs from China and Russia targeting Japanese manufacturing and the German Bundestag respectively. The most significant shift in risk was due to zero-day exploitation of an authentication bypass vulnerability in Ivanti Pulse Secure SSL VPN appliances. Microsoft patched 114 vulnerabilities, one of which was exploited before patch Tuesday. The US government formally attributed the SolarWinds Orion operation to the Russian SVR intelligence service and their APT29 or Nobelium threat actor. SITA, a communications and IT vendor for almost all of the world's airlines, was the victim of a data breach that compromised data for millions of passengers. It was among the largest data breaches of the year.

May

May began with one of 2021's milestone breaches: Colonial Pipeline was compelled to shut down operations of their pipeline to contain a DarkSide ransomware attack. Several states suffered from fuel shortages. Even after paying the 75 Bitcoin (~US$5 million) ransom, the closure lasted six days. On the same day Colonial resumed operations, DarkSide announced they were ceasing operations, releasing decryptors to their affiliates and claiming that a portion of the group's infrastructure was disrupted by an unspecified law enforcement agency. A month later, the FBI seized 63.7 Bitcoin (~US$2.3 million due to declining Bitcoin valuation). May's zero-day vulnerabilities were one vulnerability in MacOS, one in Adobe Reader and four vulnerabilities in Android. A threat actor self-identifying as "Fancy Lazarus," a tongue-in-cheek combination derived from names of a Russian and a North Korean APT, began an extortion DDoS campaign. Japanese conglomerate, FujiFilm and the world's largest meat packer, JBS Foods, both suffered business interruptions caused by REvil ransomware.

June

North Korean APT Kimsuky breached the network of the South Korean Atomic Energy Research Institute in June. Threat actors stole source code from Electronic Arts by first infiltrating the company's support channel on Slack to bypass the company's multi-factor authentication. Microsoft reported APT29 targeted IT, think tanks and government organizations using credential harvesting attacks. Six zero-day vulnerabilities were among 50 patched on Microsoft Tuesday. Apple patched two zero-days in iPadOS and iOS and Google patched one in Chrome browser.

July

Hours before the USA's Independence Day holiday, REvil ransomware abused Kaseya Virtual Systems Administrator (VSA) to attack Managed Security Service Providers that controlled the infrastructure of thousands of companies. No one knows how many of the millions of end point systems were encrypted. A few days later, the REvil threat actors closed their darknet website and ceased infecting new victims. Before the end of the month, the BlackMatter ransomware debuted announcing: "The project has incorporated in itself the best features of DarkSide, REvil, and LockBit." Attacks exploiting a total of 15 zero-day vulnerabilities in five product families were reported in July. Cloudflare mitigated a 17.2 million request per second DDoS attack on a financial industry customer. The attack was a 30 second burst launched from 20,000 bots. Microsoft discovered a Chinese threat actor targeting SolarWinds Serv-U software with a Zero-day exploit.

August

August 5th at Black Hat, a "researcher" revealed how he chained two April and one May vulnerabilities in Windows to create the "ProxyShell" attack. Mass scanning for vulnerable Exchange servers ensued. Cybereason reported on "DeadRinger," a campaign targeting Asian telecom providers. Cybereason found links to no less than five Chinese threat actor groups. Microsoft patched 51 vulnerabilities including "exploitation detected" for one zero-day. Italian energy company ERG and Accenture were the victims of LockBit 2.0 ransomware. T-Mobile reported a breach of PII from about 40 million former or prospective customers. The Poly Network, a "DeFi" or decentralized finance platform that works across blockchains, said that an attacker stole about $600 million in cryptocurrencies.

September

Just in time to ruin the Labor Day holiday in the United States, threat actors began exploiting a one-week old vulnerability in Atlassian Confluence servers. Most threat actors installed cryptominers but before the end of the month, VTRAC collected intelligence for payloads including webshells akin to the TTPs of APT actors. On Labor Day, Microsoft released an out-of-cycle advisory for zero-day exploitation of a vulnerability in the Windows browser rendering engine. Microsoft advised: "Keep antimalware products up to date," but did not release patches until a week later, on the eve of Patch Tuesday. Iowa farm services provider NEW Cooperative was hit with BlackMatter ransomware and a $5.9 million ransom demand. CISA and the FBI urged organizations to patch a vulnerability in Zoho ManageEngine ADSelfService Plus that APTs had been using as a zero-day exploit to target defense contractors, academic institutions, and other entities. Google patched five vulnerabilities being exploited in zero-day attacks on Chrome browser. Zero-day attacks drove Apple to patch three vulnerabilities in iOS/iPadOS and MacOS.

October

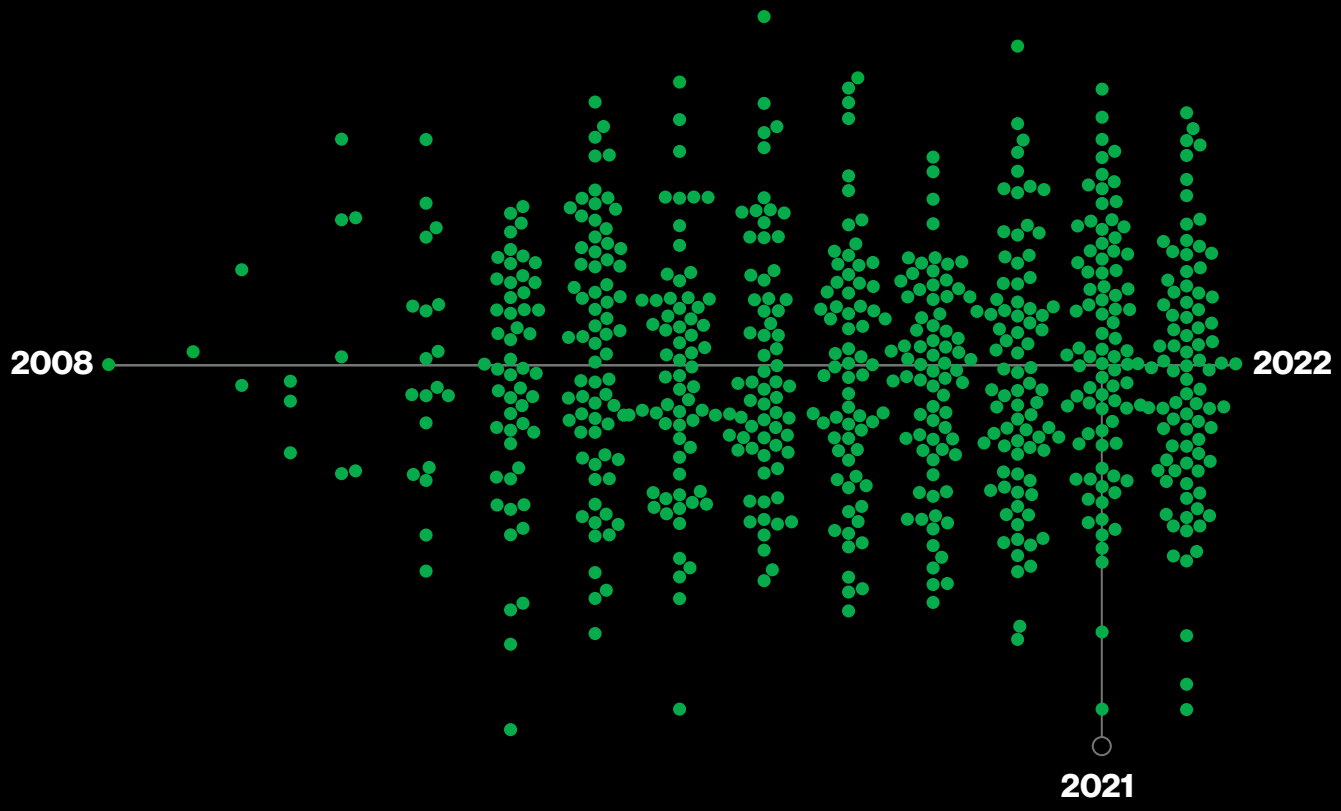
The month began with accelerated patching to mitigate zero-day attacks on a vulnerability in Apache HTTPD, the internet's #2 (after Nginx) web server. After the fix in Apache 2.4.50 was found to be "insufficient," and that it introduced a new vulnerability that was, in turn, exploited almost immediately. Apache released version 2.4.51. Zero-day attacks also struck Microsoft, Apple and the Chrome browser. The REvil ransomware operation shut down again after an unknown person hijacked their Tor payment portal and data leak blog. CrowdStrike published an analysis of the threat actor known as "LightBasin" which had been targeting companies in the telecommunications sector since 2016. CrowdStrike did not attribute LightBasin to a nation-state. A "cyber event" shuttered Schreiber Foods, a multibillion-dollar dairy company for three days. This would affect the availability of cream cheese in the United States for the holiday season. CISA/FBI/NSA issued a joint alert detailing the TTP of BlackMatter ransomware. The ransomware had been targeting multiple US critical infrastructure organizations since July 2021. Eighteen days later BlackMatter closed down after transferring its current victims to LockBit 2.0.

November

Robinhood Markets said a hacker tried to extort the financial services company following a breach of data for 7 million customers. The actor targeted 10 customers to collect "extensive account details." Emotet returned, using TrickBot for distribution and launched a worldwide email spam campaign delivering malicious documents. Researchers believe that the Conti ransomware gang was behind the botnet's return. Google's monthly Android update addressed a local privilege escalation vulnerability under "limited targeted exploitation." Microsoft released advisories for 55 vulnerabilities including two that were already being exploited. Ukraine's security service, the SSU, identified five Russian FSB officers as operators behind the Gamaredon threat actor.

December

The Apache Foundation patched a critical remote code execution vulnerability in the widely employed Log4j library. Within days, security researchers discovered indications of exploitation that began nine days before the patch announcement. The VTRAC collected intel about attacks exploiting two previously unknown vulnerabilities in Zoho ManageEngine. Zero-day attacks impacted one Windows and one Chrome browser vulnerability respectively. The APT29 (Nobelium) actor maintained the high operational tempo it reached for the SolarWinds compromise one year earlier. Reports detailed several cyber-espionage campaigns tied to the APT. "In most instances, post compromise activity included theft of data relevant to Russian interests."



7 Appendices

Appendix A: Methodology

One of the things readers value most about this report is the level of rigor and integrity we employ when collecting, analyzing and presenting data.

Knowing our readership cares about such things and consumes this information with a keen eye helps keep us honest. Detailing our methods is an important part of that honesty.

First, we make mistakes. A column transposed here; a number not updated there. We're likely to discover a few things to fix. When we do, we'll list them on our corrections page: https://www.verizon.com/business/resources/reports/dbir/2022/corrections/

Second, we check our work. The same way the data behind the DBIR figures can be found in our GitHub repository,[32] as with last year, we're publishing our fact check report there as well. It's highly technical, but for those interested, we've attempted to test every fact in the report.

Third, science comes in two flavors: creative exploration and causal hypothesis testing. The DBIR is squarely in the former. While 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.[33] All incidents included in this report were reviewed and converted (if necessary) into the VERIS framework to create a common, anonymous aggregate data set. If you are unfamiliar with the VERIS framework, it is short for Vocabulary for Event Recording and Incident Sharing, it is free to use, and links to VERIS resources are at the beginning of this report.

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

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

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

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

32 https://github.com/vz-risk/dbir/tree/gh-pages
33 As does this sentence.

Incident data

Our data is non-exclusively multinomial, meaning a single feature, such as "Action," can have multiple values (i.e., "social," "malware" and "hacking"). This means that percentages do not necessarily add up to 100%. For example, if there are 5 botnet breaches, the sample size is 5. However, since each botnet used phishing, installed keyloggers and used stolen credentials, there would be 5 social actions, 5 hacking actions and 5 malware actions, adding up to 300%. This is normal, expected and handled correctly in our analysis and tooling.

Another important point is that when looking at the findings, "Unknown" is equivalent to "Unmeasured." Which is to say that if a record (or collection of records) contains elements that have been marked as "Unknown" (whether it is something as basic as the number of records involved in the incident, or as complex as what specific capabilities a piece of malware contained), it means that we cannot make statements about that particular element as it stands in the record—we cannot measure where we have too little information. Because they are "unmeasured," they are not counted in sample sizes. The enumeration "Other," however, is counted, as it means the value was known but not part of VERIS. Finally, "Not Applicable" (normally "NA") may be counted or not counted depending on the claim being analyzed.

This year we have again 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. **Samples 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 makes a "quality" incident are:

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

In addition to having the level of details necessary to pass the quality filter, the incident must be within the timeframe of analysis, (November 1, 2020, to October 31, 2021, for this report). The 2021 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 Emotet 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 next.

Acknowledgement and analysis of bias

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

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

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.

Breaches

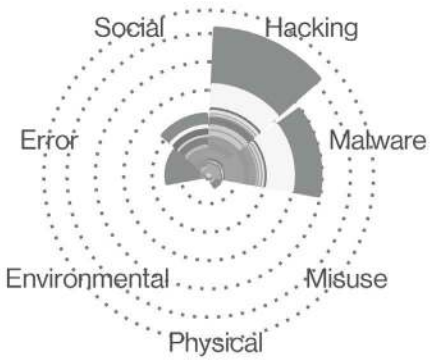


Figure 115. Individual contributions per action

Breaches

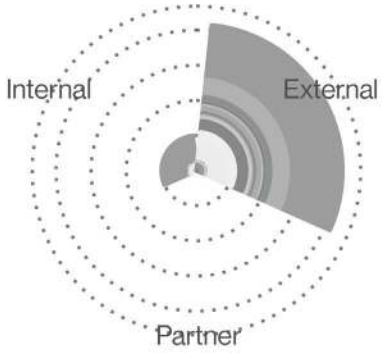


Figure 116. Individual contributions per actor

Breaches

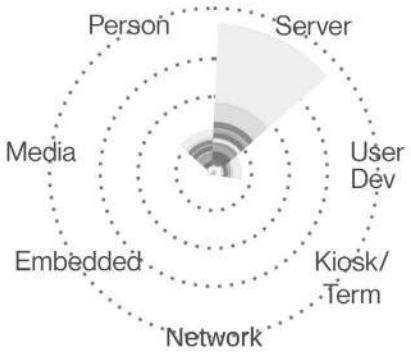


Figure 117. Individual contributions per asset

Breaches

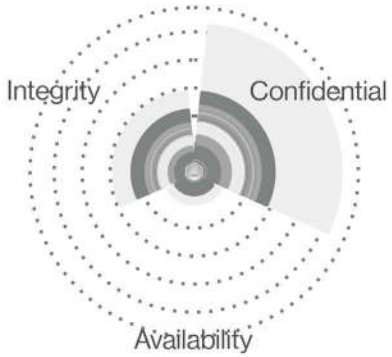


Figure 118. Individual contributions per attribute

The above four figures 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 represented by only 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 a rather large contribution on many of the axes. While we'd generally be concerned about this, they represent contributions aggregating several other sources, so 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 horse, not zebra.[34] 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 they 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 out the last five 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 two aforementioned 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, DDoS and other types of data. The sample sizes for non-incident data tend to be much larger than the incident data, but from fewer sources. We make every effort to normalize the data, (for example weighting records by the number contributed from the organization so all organizations are represented equally). We also attempt to combine multiple partners with similar data to conduct the analysis wherever possible. Once analysis is complete, we try to discuss our findings with the relevant partner or partners so as to validate it against their knowledge of the data.

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

Appendix B: VERIS and Standards

While the DBIR is celebrating its 15th birthday, VERIS (the data standard underlying the DBIR) is creeping up to the ripe old age of 12. The standard was born out of necessity as a means of cataloging in a repeatable manner the key components of an incident. This enables analysis of what happened, who was impacted and how it occurred. Since then it has grown and matured into a standard that can be adopted by many different types of stakeholders. VERIS is tailored to be a standard that provides not only ease of communication, but also a connection point to other industry standards and best practices, such as the Center for Internet Security (CIS) Critical Security Controls and MITRE Adversary Tactics, Techniques & Common Knowledge (ATT&CK). We realize that there isn't going to be one universal framework (or language or well, anything) to rule them all, but we certainly believe in the importance of peaceful co-existence between all the frameworks that have enabled the growth of this community. Below are some of the great projects and connection points that exist with VERIS and it is our hope that the standard will bring more players to the cybersecurity table.

CIS Critical Security Controls
The CIS Critical Security Controls[35] (CIS CSC) are a community-built, prioritized list of cybersecurity best practices that help organizations of different maturity levels protect themselves against threats. The CIS CSC aligns well with VERIS, as the DBIR is built to help organizations catalogue and assess cybersecurity incidents. This mapping connects the dots between the bad things that are happening and things that can help protect the organizations. Since 2019 we've published a mapping document that can help organizations crosswalk the patterns that are most concerning to them with the Safeguards that can protect them from the attacks within those patterns. Within each industry section, organizations can find the Implementation Group 1 set of controls that they can use as a starting point to improve their defenses based on the top patterns for that industry.

MITRE ATT&CK
MITRE's ATT&CK has become one of the defining ways of capturing technical tactical information in terms of what attackers do as part of their attack process. This rich dataset not only includes the specific techniques, but also the software, groups and mitigations associated with each technique, and as of earlier this year, the associated VERIS components. To assist organizations with translating the technical tactical information into strategic insights, Verizon collaborated with partners at the Center for Threat Informed Defense (CTID) and created the official VERIS to ATT&CK[36] mapping, available free of charge to anyone with an internet connection. The mapping data is represented in Structured Threat Information eXpression (STIX) STIX format, includes tools and scripts to update the mapping and also has a visualization layer that can be imported into ATT&CK[37] Navigator. By providing this mapping, we hope that the various stakeholders of the organization can communicate and share their needs in a consistent fashion.

Attack Flow
One thing you may notice in the DBIR is that outside of a few small areas such as the Timeline section, we do not discuss the path the attack takes. This is because non-atomic data (like paths and graphs of actions) is really hard, for us and the rest of the information security ecosystem. Whether it's describing breaches, writing signatures, creating repeatable pen tests or control validations, or communicating to leadership, attack paths and graphs are difficult to create, share and analyze.

The DBIR team, with MITRE CTID and its participants, hope to change that with the Attack Flow project. Attack Flow is a data schema for capturing both the causal path of an attack as well as the contextual data around it as it "flows." Because breaches fan out and then come back together, go down a path and come back to a server, Attack Flow supports arbitrary graphs of actions and assets interacting. Because we all need to know different things about the attack, it uses a knowledge graph structure to capture the context of the flow. And because we all organize differently, it supports multiple namespaces. So, for example, you could use VERIS Actions, MITRE ATT&CK actions, organization specific actions, or even a combination of all of the above as part of your attack path analysis.

With Attack Flow, we now have a format we can use to share non-atomic data. Digital Forensics and Incident Response (DFIR) folks could document an incident as a flow. Detection vendors could use it to create a signature. Control validation tools can use it to simulate the incident. The Security Engineering team can use it to build attack surface graphs and plan mitigations. And they all can use the structure to create communications to leadership, and all be able to share the same underlying data with each other in a standardized but flexible structure. If that sounds like something you could get behind, check out the MITRE project at https://github.com/center-for-threat-informed-defense/attack-flow and the DBIR team's graph based tools for working with it at https://github.com/vz-risk/flow.

35 https://www.cisecurity.org/controls
36 https://github.com/center-for-threat-informed-defense/attack_to_veris/
37 https://oasis-open.github.io/cti-documentation/stix/intro

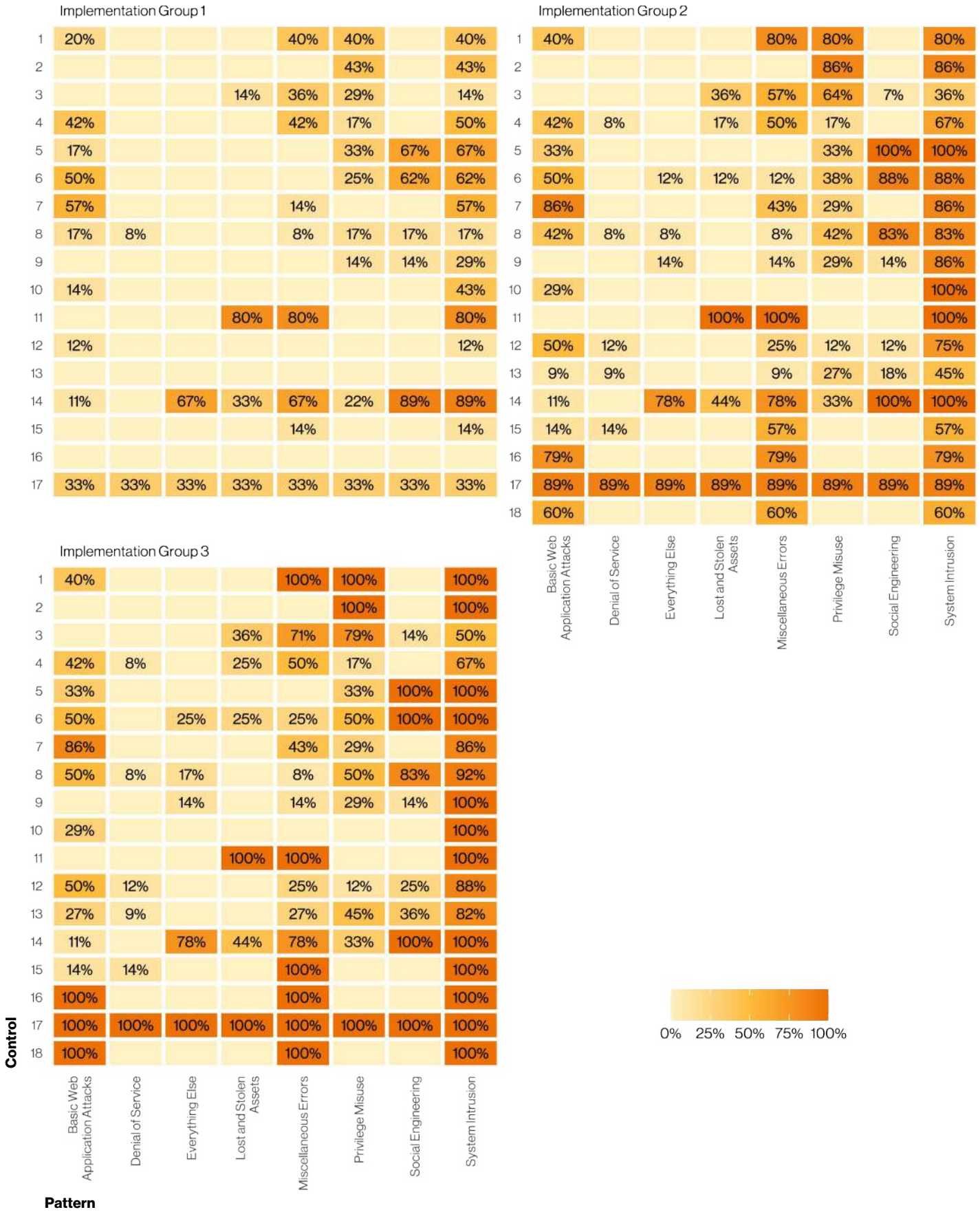


Figure 119. CIS to pattern mapping

Appendix C: Changing Behavior

In 2021 we reported that the human element impacted 85% of breaches, which decreased slightly to 82% this year. Unfortunately, strong asset management and a stellar vulnerability scanner aren't going to solve this one.

Instead, you're going to need to change the behavior of humans, and that is quite an undertaking. Regardless of how you plan on doing it (be it giving them a reason to change, providing training or a combination of the two), you will need a way to tell if it worked, and that normally means running a test. Here's a cheat-sheet of things that your internal department or vendor who is responsible for conducting the training should provide to you so you can determine if it is paying off:

- A population of people you are interested in. (If the test was run only in a healthcare company or in a specific division, the population should be "Employees of healthcare companies" not "Anyone.")
- A measurable outcome that can be proven or disproven. (Such as "More correct answers on a questionnaire about phishing delivered 1 day after training," or "Fewer people clicked the phishing email," etc.)
- An intervention to test to see if it changes the outcome. ("Watch a 15-minute video on not clicking phishing.")
- A control that provides a baseline for the outcome. ("Received no training," "Read a paragraph of text about phishing," "Read a comic book and took a nap," etc.)
- Random assignment. ("200 employees were picked to participate in the study. 100 were randomly assigned the control and 100 were randomly assigned the intervention.")
- The conditions of the test should also be shared. ("Participants were sent the control or intervention via the company training tool as annual mandatory training.")

This test may be something run specifically for you or a test the trainer already ran. As long as the population, outcome, etc. are close to yours, it doesn't matter.

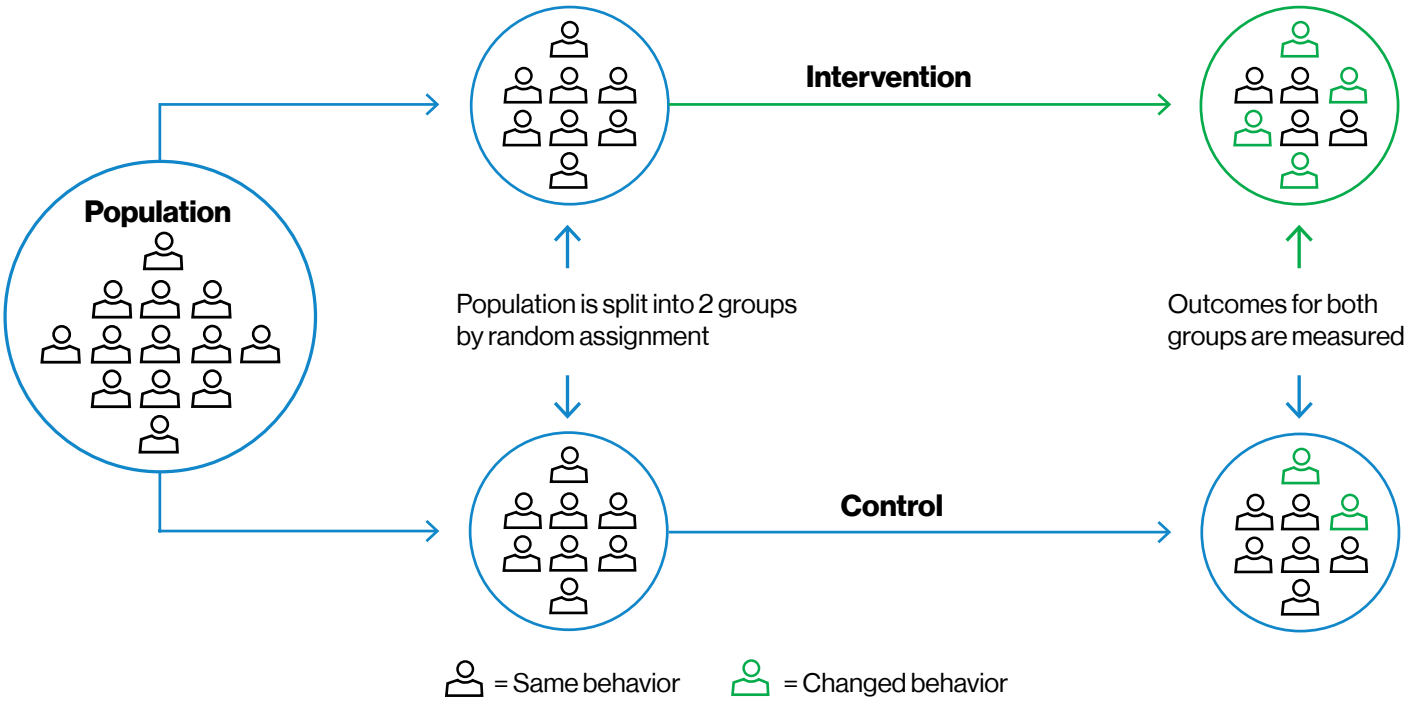


Figure 120. Randomized control test

The manner in which the results are reported is just as important as how the testing was conducted. Here are a few things you should expect in the results:

- A result with a confidence interval. (If 10 folks in the control clicked the phishing email and only 1 in the intervention, 10-1 = 9 people we thought would click, but didn't. That's a 9/10 or 90% effectiveness.) But that one number doesn't tell the whole story. What if some of those were flukes? The result should come with a range (such as 70% to 100% effective at 95% confidence) similar to the DBIR ranges. (Btw, if the range includes 0%, there's a chance the training didn't actually do anything.) If the outcome question was yes/no, then just a confidence level will do. ("People changed due to the intervention with 98% confidence.")
- Since results can vary over time, you should know when the result was measured. "The result was 30 days after the intervention."
- What if some folks just refused to take the training? That's called dropout and is important to the results. The results should show who dropped out (preferably by full name so they can be shamed in front of their peers – okay, not really). ("Twenty percent of technically savvy employees didn't take the intervention training, while only 2% didn't take the control training.") Dropout can occur for any of the other characteristics recorded (industry, world region, department, age, etc.) and if major differences are found, the results should be broken out by those characteristics as well. ("People changed 98% in tech savvy folks, but only 70% in non-tech savvy.")
- There should also be qualitative questions. Sometimes you don't know what you don't know.[38] In that case, there should be an open-ended question about the training in addition to the more objective outcomes. It also gives a chance to ask questions like "Do you have formal education or a job in a computer-related field?" And you can see the importance of this in the dropout bullet above. Asking "Is there anything else you'd like us to know?" might reveal that while the training was effective, many folks found it highly offensive.

Unfortunately, there's no way to guarantee something works. But, if you're getting the information above (Population, Outcome, Intervention, Control, Random, Conditions) and (Results, When, Dropout, Qualitative) you can be reasonably confident you're getting something for your effort. So, remember those easy acronyms: POICRC and RWDQ!

38 Often referred to as the Rumsfeld paradox.

Appendix D: U.S. Secret Service

David Smith
Assistant Director
U.S. Secret Service

Jason D. Kane
Special Agent in Charge
Criminal Investigative Division
U.S. Secret Service

Evolution of Investigative Methodology to Thwart an Everchanging Cybercriminal Landscape

The ways in which we live, work and interact with each other has changed dramatically the last few years. The increased use of Internet platforms during the COVID-19 pandemic clearly demonstrates our growing economic dependence on information technology, and with that increased risk of cybercrime. Transnational cyber criminals continue to expand their capabilities, and their ability to cause harm—regardless of if they are financially or politically motivated.

In terms of criminal activity, 2021 experienced a growth in crimes involving cryptocurrencies. This includes digital extortion schemes (including ransomware), theft of credentials or private keys that control substantial value in digital assets, manipulation of decentralized finance (DeFi) systems, and new money laundering methods that enable a wide variety of illicit activity. Transnational criminals are increasingly using cryptocurrency and other digital assets, rather than traditional physical assets or the intermediated financial system. Cryptocurrencies even found their way into Superbowl advertisements. What was once a niche market is now a growing part of modern life – investing, trading, and for illicit activity as well.

Since its creation in 1865, the U.S. Secret Service has continuously evolved its investigative strategies and methods to protect our nation's financial system. We are no longer chasing counterfeiters on horseback but are now focused on preventing cyber fraud by identifying and arresting cybercriminals worldwide. In 2010, when the Secret Service first joined in developing the DBIR, the foremost risk we were seeing was the theft of payment card and PII data for use in fraud. As this year's report shows that risk is still present, but we are seeing development of new schemes by those who illicitly exploit the Internet.

To keep pace with evolving criminal activity, the U.S. Secret Service focuses on partnering to enable businesses and law enforcement to take effective actions to mitigate risk. The DBIR is a key part of this—providing recommendations derived from analysis of aggregated incident reports. We also aid our partners and prevent cyber incidents through the work of our Cyber Fraud Task Forces, and the over 3,000 state, local tribal and territorial (SLTT) law enforcement personnel we trained at the National Computer Forensics Institute (NCFI) in FY 2021. We coordinate these activities globally through a dedicated group of investigators in our Global Investigative Operations Center (GIOC) focused on achieving the most effective outcomes—from recovering and returning stolen assets to victims to apprehending those responsible.

The U.S. Secret Service, while focused on thwarting criminal activity today, has already started to train and prepare for the cybercrimes of the future.

This past year clearly demonstrated the increasing impact ransomware is having on businesses, critical infrastructure and national security. The most prolific ransomware networks are Russian-speaking, though this crime is not limited to one country or region. According to one industry estimate, 74% of ransomware payments were Russian affiliated. We have also seen the use of destructive malware, which is functionally similar to ransomware, but lacks a means for payment. This dynamic, coupled with the limited cooperation of some states in countering ransomware, illustrates a growing risk which blurs distinctions politically and financially motivated cybercrimes. This risk reinforces why partnership is essential in improving cybersecurity by both improving the resilience of computer systems and apprehending the threat actors.

Despite transnational cybercrime being a daunting challenge, the U.S. Secret Service relentlessly pursues these cases. In 2021, the Secret Service led or participated in numerous multi-national operations to counter cyber criminal networks. For example, we conducted a multinational operation with Dutch Police and Europol to arrest multiple individuals responsible for ransomware attacks affecting over 1,800 victims in 71 countries. In total, Secret Service responded to over 700 network intrusions and prevented over $2.3 billion in cyber financial losses last fiscal year.

Identity theft and fraud continues to be a core activity of transnational cyber criminals—it provides a means to convert stolen personally identifiable information into profit. The COVID-19 pandemic created new opportunities for this sort of fraud, as criminals defrauded relief programs. In response, the U.S. Secret Service named a National Pandemic Fraud Recovery Coordinator to focus on partnering with financial institutions to prevent and recover fraudulent payments. These efforts resulted in the U.S. Secret Service recovering more than $1.2 billion, the return of more than $2.3 billion of fraudulently obtained funds, and over 100 arrests.

As the world becomes more digitized, in addition to being connected to each other through technology, we are connected to a wide array of devices, such as the internet of things (IoT). Other emerging technologies that may soon be the targets of cybercriminals include quantum cryptography, 5G wireless technology and Artificial Intelligence (AI). These technologies have the potential to improve lives and open new lines of communication. Conversely, cybercriminals will seek ways to use these technologies for malicious gains. The U.S. Secret Service, while focused on thwarting criminal activity today, has already started to train and prepare for the cybercrimes of the future.

Preventing cybercrime requires a multi-pronged strategy including increasing cybersecurity resilience and pursuing criminals and seizing illicit gains to deter and prevent future crimes. Both of these efforts are strengthened by the analysis of aggregated incident reports, and evidence-based recommendations the DBIR provides. In 2022, the U.S. Secret Service looks forward to further strengthening our partnerships, to stay ahead of our changing use of technology, the efforts of criminals to exploit it, and ensure there is no safe place for cyber criminals to hide.

Appendix E: Ransomware Pays

In past reports, we have talked at length about the cost of ransomware and other breaches to victims. However, we have never examined what the economics look like for the threat actor. This alternate point of view might provide some useful insights.

To that end, we have combined the value chain targeting and distribution data, phishing test success rate data, criminal forum data, and ransomware payment data to estimate what the business looks like from the criminal's side.

First, let's examine the cost of access. Figure 121 illustrates the cost of hiring (criminal) professional services to do the actor's dirty work. These (and larger criminal organizations with internal staff for access) are likely going for riskier, bigger-payout attacks.

The small-time criminal is less of a techie and more of a manager. They are trying to minimize costs so will not invest in professional services. Instead, they buy access products outright in the form of credentials, emails for phishing, vulnerabilities, or botnet access. Figure 122 gives an idea of the costs. Instead of $100,000, the majority of access doesn't even cost a dollar. This is because most access is email which is incredibly cheap, even when the median click rate is only 2.9%. While purchasing access directly in the form of access to a bot, login credentials, or knowledge of a vulnerability are also included, it's email that steers the ship.

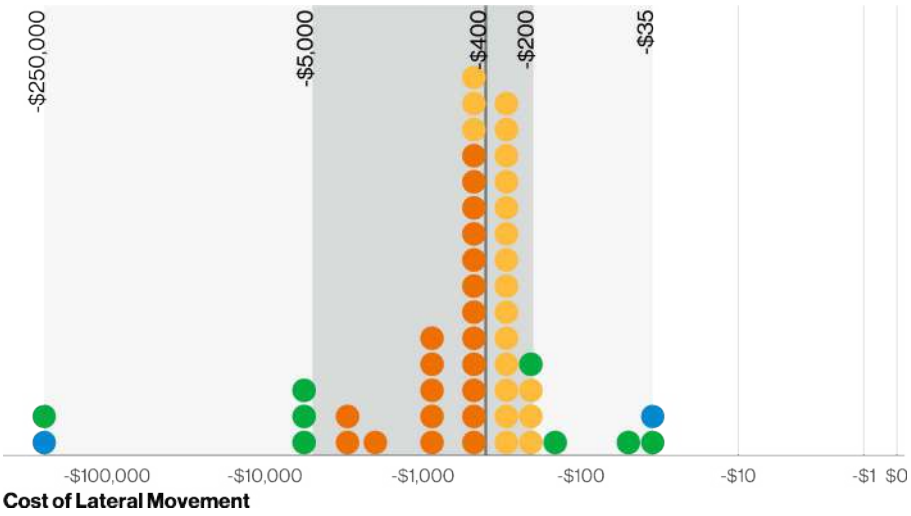


Figure 121. Cost of skilled intrusion services (log scale).
Based on 3,000 simulations of criminal forum data.

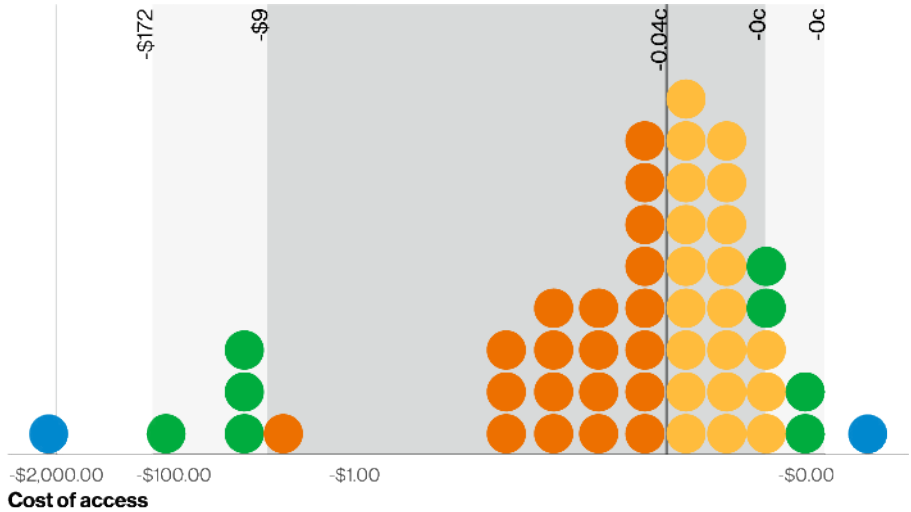


Figure 122. Simulated cost of access (log 100 scale)
(Phishing, Credentials, Vulnerabilities and Botnets)

Contrast Figure 122 with the profits in Figure 123. Sixty percent of ransomware incidents had no profit and aren't shown in the figure. A large portion had a profit near one dollar. However, the median is just over $100. Figure 124 shows what those same profits look like over time. After 300 simulated ransoms the actor has over $600,000 in income.[39]

To see if this was an anomaly, we simulated 500 ransomware actors and 1.4% of them showed a loss.[40] However, the median profit after 300 incidents was $178,465, with the top simulated earner making $3,572,211.

The takeaway is that ransomware is more of a lottery[41] than a business. You gamble on access, win the lottery 40% of the time, and get a payout from a few bucks to thousands of dollars. But for something more actionable, focus on the access. If an actor has to pay for services to break in rather than just an access product, you've made yourself much less of a target. Use antivirus to remove bots; implement patching, filtering and asset management to prevent exposed vulnerabilities; and standardize two-factor authentication and password managers to minimize credential exposure. Lastly, with email being the largest vector, you can't ignore the human element. Start with email and web filtering followed by training. (See the Changing Behavior Appendix for a recommendation on how to tell if your training is working.)

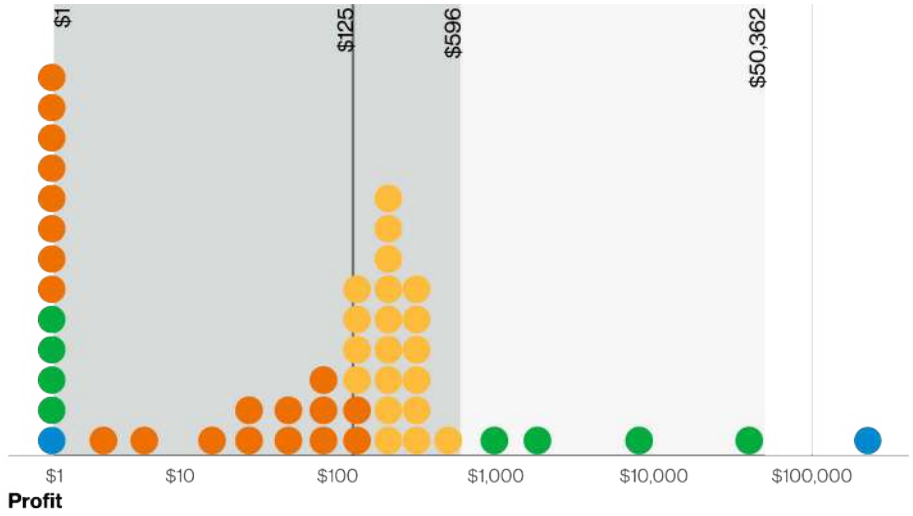


Figure 123. Simulated profit from ransomware incidents (log scale)

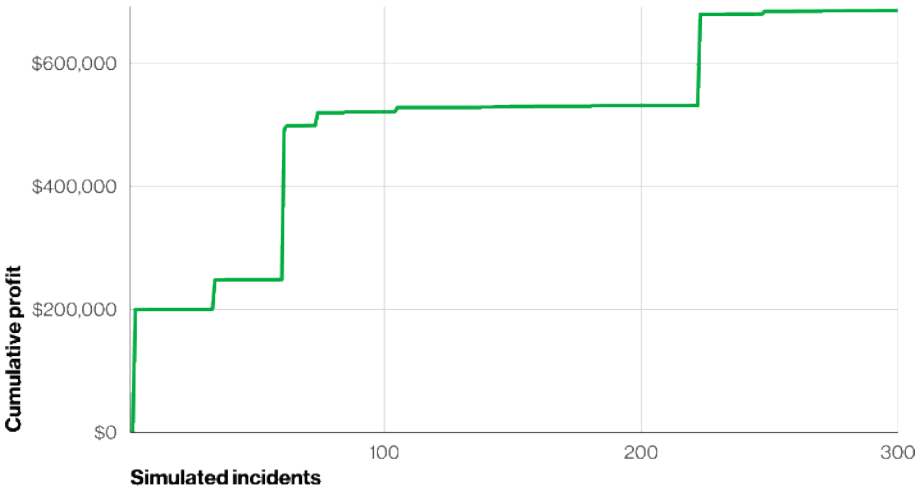


Figure 124. Profit for a simulated ransomware actor over time

39 We assume tax-free.

40 I suppose not everyone can be good at business. Even criminals.

41 As Erick Galinkin also suggests in "Winning the Ransomware Lottery: A Game-Theoretic Model for Mitigating Ransomware Attacks," https://doi.org/10.48550/ arXiv.2107.14578

Appendix F: Contributing Organizations

A

Akamai Technologies

Ankura

Anomali

Apura Cybersecurity Intelligence

AttackIQ

Atos

B

Bad Packets

bit-x-bit

Bitsight

Blackberry Cylance

C

Center for Internet Security

CERT European Union

CERT Division of Carnegie Mellon University's Software Engineering Institute

Checkpoint Software Technologies Ltd.

Chubb

Coalition

Computer Incident Response Center Luxembourg (CIRCL)

Coveware

Crowdstrike

Cybersixgill

Cybercrime Support Network

Cybersecurity and Infrastructure Security Agency (CISA)

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

D

Defense Counterintelligence Security Agency (DCSA)

Dell

Digital Shadows

Domain Tools (formerly Farsight Security)

Dragos, Inc.

E

EASE (Energy Analytic Security Exchange)

Edgescan

Elevate Security

Emergence Insurance

EUROCONTROL

F

Domain Tools (formerly Farsight Security)

Financial Services ISAC (FS-ISAC)

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

Fortinet

G

Global Resilience Federation

Grey Noise

H

HackedEDU

Hasso-Plattner Institut

I

Irish Reporting and Information Security Service (IRISS-CERT)

J

Jamf

JPCERT/CC

K

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

Kaspersky

Knowbe4

Kordamentha

L

Lares Consulting

Legal Services – ISAO

LMG Security

Lookout

M

Malicious Streams

Maritime Transportation System ISAC (MTS-ISAC)

Micro Focus

mnemonic

N

NetDiligence®

NETSCOUT

NINJIO Cybersecurity Awareness Training

P

Palo Alto Networks

Paraflare Pty Ltd

Proofpoint

PSafe

Q

Qualys

R

Ransomwhe.re

Recorded Future

S

S21sec

SecurityTrails

Shadowserver Foundation

Shodan

SISAP - Sistemas Aplicativos

Swisscom

U

U.S. Secret Service

V

VERIS Community Database

Verizon Cyber Risk Programs

Verizon DDoS Shield

Verizon Mobile Security Dashboard

Verizon Network Operations and Engineering

Verizon Professional Services

Verizon Sheriff Team

Verizon Threat Intelligence Platform

Vestige Digital Investigations

Verizon Threat Research Advisory Center (VTRAC)

W

WatchGuard Technologies

Z

Zscaler

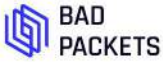

ankura

Akamai

apura

ANOMALI

Atos

ATTACKIQ

BAD
PACKETS

BITSIGHT

bit-x-bit

BlackBerry.
Intelligent Security. Everywhere.

CERT-EU

CIS
Center for
Internet
Security

CIRCL
Computer Incident
Response Center
Luxembourg

CROWDSTRIKE

Cybercrime
SUPPORT NETWORK

CHUBB

CHECK POINT

CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Carnegie
Mellon
University
Software
Engineering
Institute

CyberSecurity
MALAYSIA

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

COVEWARE

Coalition

cybersixgill

DELL Technologies

digital shadows_

DOMAINTOOLS

DRAGOS

EASE
Energy Analytic Security Exchange

edgescan

Elevate Security

emergence

EUROCONTROL

FBI

FORTINET

FS-ISAC

GLOBAL
RESILIENCE
FEDERATION

GREYNOISE

Hack_EDU

HPI
Hasso
Plattner
Institut

IRISS
Irish Reporting and
Information Security Service

jamf

Verizon Cyber Risk Programs

Verizon DDoS Shield

Verizon Mobile Security Dashboard

Verizon Network Operations and Engineering

Verizon Professional Services

Verizon Sheriff Team

Verizon Threat Intelligence Platform

Verizon Threat Research Advisory Center (VTRAC)

verizon