verizon

DBIR2020

DBIR

2020 Data Breach Investigations Report

verizon

verizon

3,950 breaches

That is what you are seeing. Each of these squares is organized by the 16 different industries and four world regions we cover in this year's report. Each square represents roughly one breach (1.04 to be more exact), for a total of 4,675 squares since breaches can be displayed in both their industry and region.

We also analyzed a record total of 157,525 incidents, 32,002 of which met our quality standards. The data coverage this year is so comprehensive that it shines through the monochromatic front cover, reinforcing the mission of the DBIR as being a data-driven resource. Turn the page to dig into the findings.

Table of contents

DBIR Cheat sheet

Hello and welcome to the *2020 Data Breach Investigations Report* (DBIR)! We have been doing this report for a while now, and we appreciate that all 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 a lot. 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 and 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/2020** includes DBIR facts, figures and figure data.
- **veriscommunity.net** features information on the framework with examples and enumeration listings.
- **github.com/vz-risk/veris** features the full VERIS schema.
- **github.com/vz-risk/vcdb** provides access to our database on publicly disclosed breaches, the VERIS Community Database.
- **http://veriscommunity.net/veris_webapp_min.html** allows you to record your own incidents and breaches. Don't fret, it saves any data locally and you only share what you want.

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. 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 classification system is available here:

https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012

Dotting the charts and crossing the confidence

Last year, we introduced our now (in)famous slanted bar charts to show the uncertainty due to sampling bias.[1] One tweak we added this year was to roll up an "Other" aggregation of all the items that do not make the cut on our "Top (whatever)" charts. This will give you a better sense of the things we left out.

Not to be outdone this year, our incredible team of data scientists decided to try dot plots[2] to provide a better way to show how values are distributed.

The trick to understanding this chart is that the dots represent organizations. So if there are 100 dots (like in each chart in Figure 1), each dot represents 1% of organizations. In Figure 1, we have three different charts, each representing common distributions we may find in this report. For convenience, we have colored the first half and the second half differently so it's easier to locate the median.

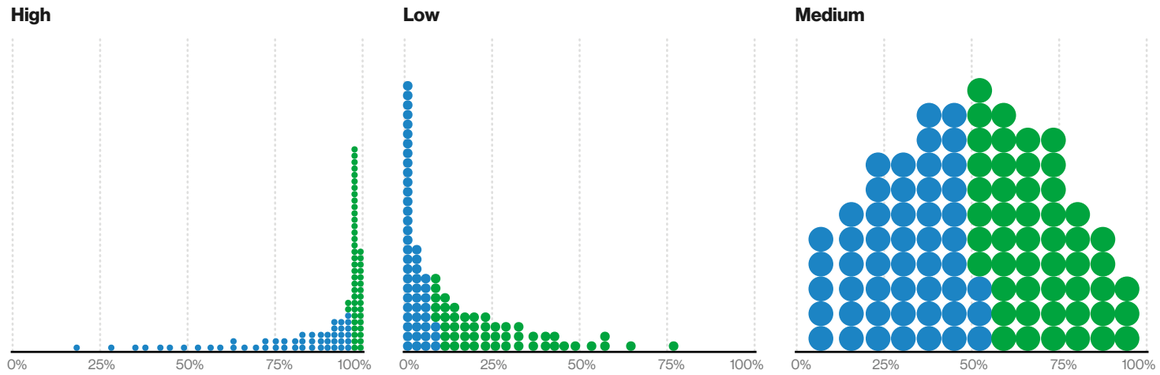


Figure 1. Example dot plots

In the first chart (High), you see that a lot of companies had a very large value[3] associated with them. The opposite is true for the second one (Low), where a large number of the companies had zero or a low value. On the third chart (Medium), we got stuck in the middle of the road and all we can say is that most companies have that middle value. Using the Medium chart, we could probably report an average or a median value. For the High and Low ones, an average is statistically undefined and the median would be a bit misleading. We wouldn't want to do you like that.

Questions? Comments? Still mad because VERIS uses the term "Hacking"?

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

1 Check "New chart, who dis?" in the "A couple of tidbits" section on the inside cover of the 2019 DBIR if you need a refresher on the slanted bar charts.
2 To find out more about dot plots, check out Matthew Kay's paper: http://www.mjskay.com/papers/chi2018-uncertain-bus-decisions.pdf
3 Don't worry about what the value is here. We made it up to make the charts pretty. And don't worry later either, we'll use a real value for the rest of the dot plots.

Introduction

Experience is merely the name men gave to their mistakes.

—Oscar Wilde, *The Picture of Dorian Gray*

Here we are at another edition of the DBIR. This is an exciting time for us as our little bundle of data turns 13 this year. That means that the report is going through a lot of big changes right now, just as we all did at that age. While some may harbor deeply rooted concerns regarding the number 13 and its purported associations with mishap, misadventure and misfortune, we here on the team continue to do our best to shine the light of data science into the dark corners of security superstition and dispel unfounded beliefs.

With that in mind, we are excited to ask you to join us for the report's coming-of-age party. If you look closely, you may notice that it has sprouted a few more industries here and there, and has started to grow a greater interest in other areas of the world. This year, we analyzed a record total of 157,525 incidents. Of those, 32,002 met our quality standards and 3,950 were confirmed data breaches. The resultant findings are spread throughout this report.

This year, we have added substantially more industry breakouts for a total of 16 verticals (the most to date) in which we examine the most common attacks, actors and actions for each. We are also proud to announce that, for the first time ever, we have been able to look at cybercrime from a regional viewpoint—thanks to a combination of improvements in our statistical processes and protocols, and, most of all, by data provided by new contributors—making this report arguably the most comprehensive analysis of global data breaches in existence.

We continue to use the VERIS framework to classify and analyze both incidents and breaches, and we have put additional focus on this process in order to improve how VERIS connects and interacts with other existing standards. We also aligned with the Center for Internet Security (CIS)[4] Critical Security Controls and the MITRE ATT&CK®[5] framework to improve the types of data we can collect for this report, and to map them to appropriate controls.

A huge "thank you" is in order to each and every one of our 81 contributors representing 81 countries, both those who participated for the first time in this year's report, and those tried-and-true friends who have walked this path with us for many years. This document, and the data and analysis it contains, would not be possible without you, and you have our most sincere thanks and heartfelt gratitude. And while we are on that topic, the way to continue to grow and improve is to have more quality organizations like yours join us in this fight against the unknown and the uncertain. Therefore, we urge you to consider becoming a data contributor and help us to continue to shed light into dark places.

Finally, thank you, our readers, for sticking with us these many years and for sharing your expertise, advice, encouragement and suggestions so that we can continue to make this report better each year.

Sincerely,
The DBIR Team

(in alphabetical order)

Gabriel Bassett
C. David Hylender
Philippe Langlois
Alexandre Pinto
Suzanne Widup

4 https://www.cisecurity.org/
5 https://attack.mitre.org/

Summary of findings

Figure 2. What tactics are utilized?

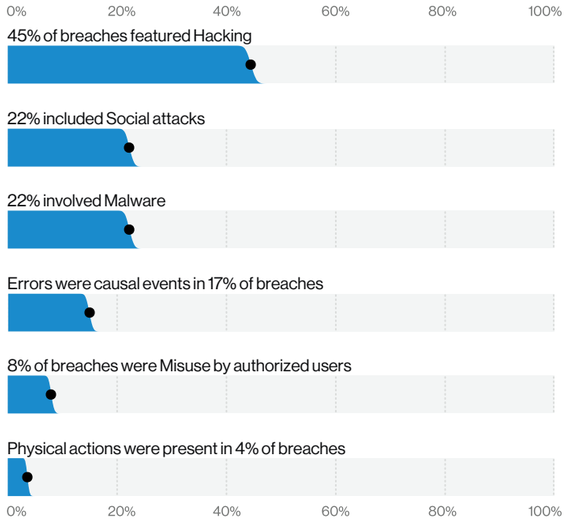


Figure 3. Who's behind the breaches?

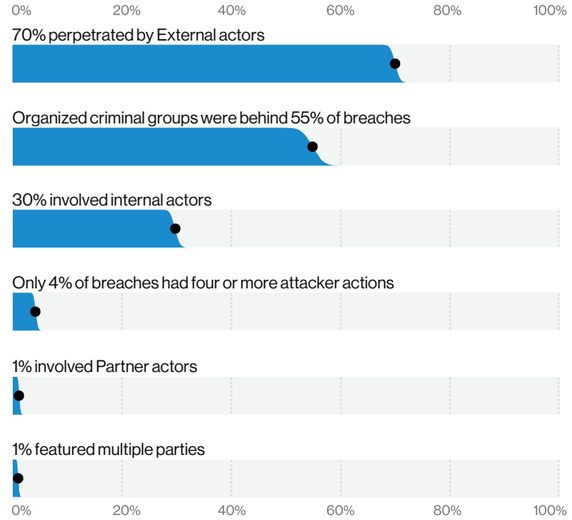


Figure 4. Who are the victims?

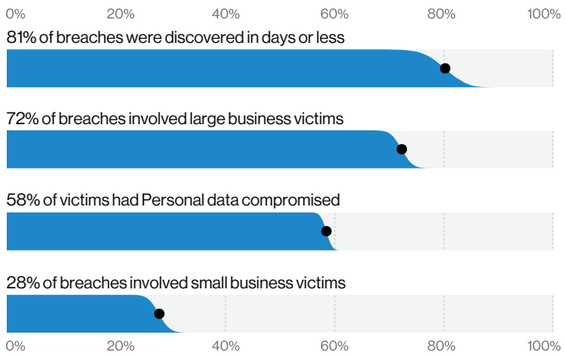
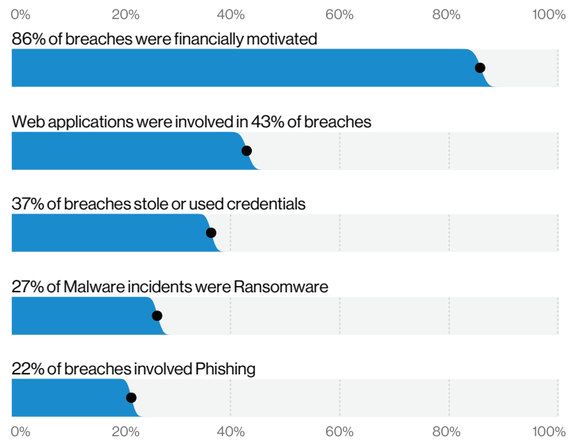


Figure 5. What are the other commonalities?



02

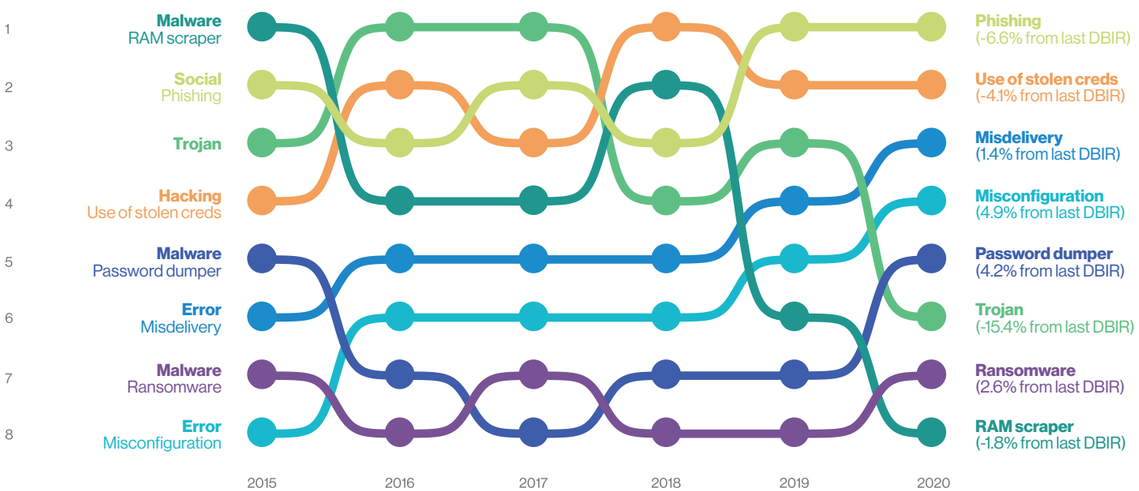
Results and analysis

Results and analysis

The results found in this and subsequent sections within the report are based on a dataset collected from a variety of sources, including cases provided by the Verizon Threat Research Advisory Center (VTRAC) investigators, cases provided by our external collaborators and publicly disclosed security incidents. The year-to-year data will have new incident and breach sources as we continue to strive to locate and engage with additional organizations that are willing to share information to improve the diversity and coverage of real-world events. This is a sample of convenience,[6] and changes in contributors—both additions and those who were not able to contribute this year—will influence the dataset. Moreover, potential changes in contributors' areas of focus can shift bias in the sample over time. Still other potential factors, such as how we filter and subset the data, can affect these results. All of this means that we are not always researching and analyzing the same population. However, they are all taken into consideration and acknowledged where necessary within the text to provide appropriate context to the reader. Having said that, the consistency and clarity we see in our data year-to-year gives us confidence that while the details may change, the major trends are sound.

Now that we have covered the relevant caveats, we can begin to examine some of the main trends you will see while looking through this report. When looking at Figure 6 below, let's focus for a moment on the Trojan[7] line. When many people think of how hacking attacks play out, they may well envision the attacker dropping a Trojan on a system and then utilizing it as a beachhead in the network from which to launch other attacks, or to expand the current one. However, our data shows that this type of malware peaked at just under 50% of all breaches in 2016, and has since dropped to only a sixth of what it was at that time (6.5%). Likewise, the trend of falling RAM-scraper malware that we first noticed last year continues. We will discuss that in more detail in the "Retail" section. As this type of malware decreases, we see a corresponding increase in other types of threats. As time goes on, it appears that attackers become increasingly efficient and lean more toward attacks such as phishing and credential theft. But more on those in the "Social" and "Hacking" subsections respectively. Other big players this year, such as Misconfiguration and Misdelivery, will be examined in the "Error" subsection.

Figure 6. Select action varieties over time



6 Convenience sampling is a type of nonrandom sampling that involves the sample being drawn from that part of the population that is close to hand or available. More details can be found in our "Methodology" section.

7 This year, we added a Trojan category to Malware. This is a combination of Malware RAT, Malware C2 and Backdoor, Hacking Use of backdoor or C2, and Malware Spyware/Keylogger.

Actors

Let us begin by disabusing our readers of a couple of widely held, but (according to our data) inaccurate beliefs. As Figure 7 illustrates, in spite of what you may have heard through the grapevine, external attackers are considerably more common in our data than are internal attackers, and always have been. This is actually an intuitive finding, as regardless of how many people there may be in a given organization, there are always more people outside it. Nevertheless, it is a widely held opinion that insiders are the biggest threat to an organization's security, but one that we believe to be erroneous. Admittedly, there is a distinct rise in internal actors in the dataset these past few years, but that is more likely to be an artifact of increased reporting of internal errors rather than evidence of actual malice from internal actors. Additionally, in Figure 8, you'll see that Financially motivated breaches are more common than Espionage by a wide margin, which itself is more common than all other motives (including Fun, Ideology and Grudge, the traditional "go to" motives for movie hackers). There is little doubt that Cyber-Espionage is more interesting and intriguing to read about or watch on TV. However, our dataset indicates that it is involved in less than a fifth of breaches. But don't let that keep you away from the cinema, just make sure to save us some popcorn.

With regard to incidents, Figure 9 illustrates that Financial is still the primary motive, but it must be acknowledged that the Secondary motivation is not far behind. As a refresher (or fresher for our new readers), the compromised infrastructure in Secondary incidents is not the main target, but a means to an end as part of another attack. In fact, if we had included the Secondary Web application breaches (we removed this subset as mentioned in the "Incident classification patterns and subsets" section), the Secondary motive category would actually be higher than Financial.

When we look at criminal forums and underground data, 5% refer to a "service." That service could be any number of things including hacking, ransomware, Distributed Denial of Service (DDoS), spam, proxy, credit card crime-related or other illicit activities. Worse still, that "service" may just be hosted on your hardware. The simple fact is this: If you leave your internet-facing assets so unsecured that taking them over can be automated, the attackers will transform your infrastructure into a multitenant environment.

Figure 7. Actors over time in breaches

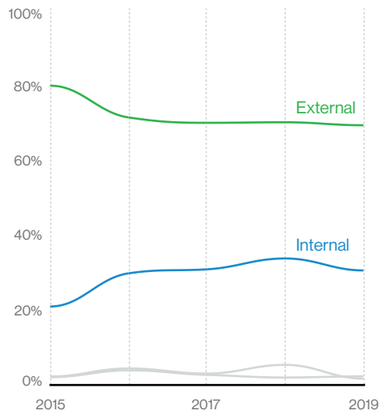


Figure 8. Actor motives over time in breaches

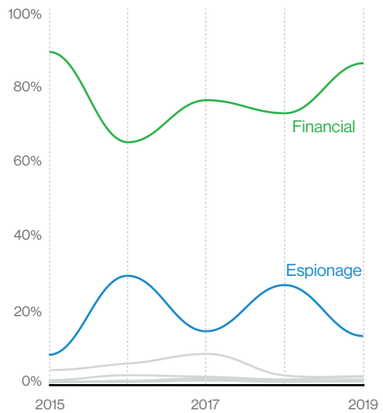
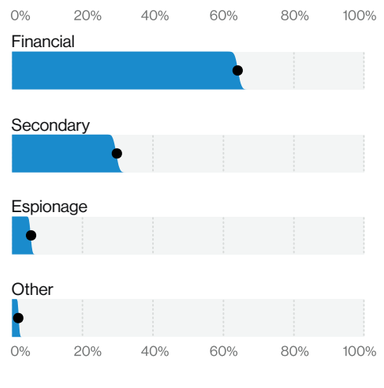


Figure 9. Top Actor motives in incidents (n = 3,828)



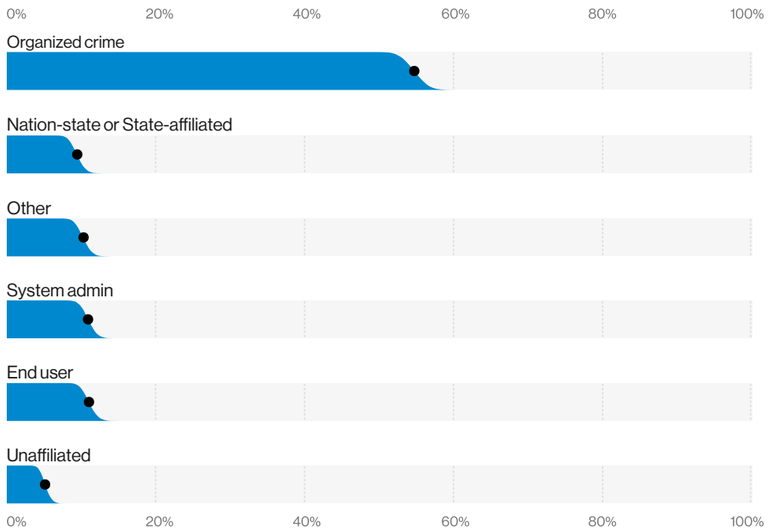


Figure 10. Top Actor varieties in breaches (n = 977)

A good follow-up question might be "where are these unwanted occupants coming from?" Figure 10 shows that Organized crime[8] is the top variety of actor for the DBIR. After that, we see a roundup of the usual suspects: State-aligned actors who are up to no good, internal End users and System admins making errors as though they were paid to do it, and, at the very bottom, the Unaffiliated. Although they may sound like the title of a book series for young adults, they are actually an interesting group. These are people from areas unknown and their motivation is not always readily apparent. One potential origin for these actors might be gleaned from looking at the criminal forum and marketplace data we referenced above. About 3% of the forum threads related to breach and incident cybercrime[9] were associated with training and education.[10]

These are would-be hackers who are still serving out their apprenticeship, for lack of a better term. In fact, as noted by the United Kingdom's National Crime Agency, "Offenders begin to participate in gaming cheat websites and 'modding' (game modification) forums and progress to criminal hacking forums without considering the consequences."[11] In other words, this is a group of individuals with a certain skill set but no clear sense of direction, who could perhaps, given the right amount of persuasion and incentive, be kept from the dark side and thereby added to the talent pool for our industry. Giving them a career and a future rather than a jail sentence is, in the long run, better for all concerned. Although it is handy to know a game cheat every now and again.

Another thing you might be wondering is where the attackers are coming from. Based off of computer data breach and business email compromise complaints to the FBI Internet Crime Complaint Center (IC3), 85% of victims and subjects were in the same country, 56% were in the same state and 35% were even in the same city. In part, this is driven by many of the complaints coming from high-population areas such as Los Angeles, CA, and New York City, NY. So, the proverbial call is almost coming from inside the building.

8 When we say "Organized crime," we mean "a criminal with a process," not "the mafia."

9 Cyber, cyber.

10 Matched a search for guide, tutorial, learn or train in the title or body.

11 Pathways into Cyber Crime, NCA, 2017 (https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file).

Actions

When we analyzed the high-level actions on Figure 11, we found that it mirrors Figure 6. The only action type that is consistently increasing year-to-year in frequency is Error. That isn't really a comforting thought, is it? Nevertheless, there is no getting away from the fact that people can, and frequently do, make mistakes and many of them probably work for you.

Physical breaches have stayed relatively level and infrequent, but Misuse, Hacking, Malware and Social have all decreased since last year's report. While Hacking and Social are down as a percent, they have remained close to the levels we have seen for the past few years. On the other hand, Malware has been on a consistent and steady decline as a percentage of breaches over the last five years.

Why is this? Has malware just gone out of fashion like poofy hair and common courtesy? No, we think that other attack types such as hacking and social breaches benefit from the theft of credentials, which makes it no longer necessary to add malware in order to maintain persistence. So, while we definitely cannot assert that malware has gone the way of the eight-track tape, it is a tool that sits idle in the attacker's toolbox in simpler attack scenarios.

It is important to keep in mind that the points made above are in reference to breaches and not incidents. The incidents tell us a somewhat different story. Ransomware—which in our dataset rarely results in a confirmed breach[12] unless paired with credential use—is on the rise. Still, as malware tools continue to evolve and improve, there appears to be a sense that malware prevalence is decreasing somewhat, as this causes fewer instances that rise to the status of "incident" for our data contributors. This seems to have the effect on our dataset of a polarization: malware being either part of advanced attacks or the simpler (yet still effective) smash-and-grab compromises.

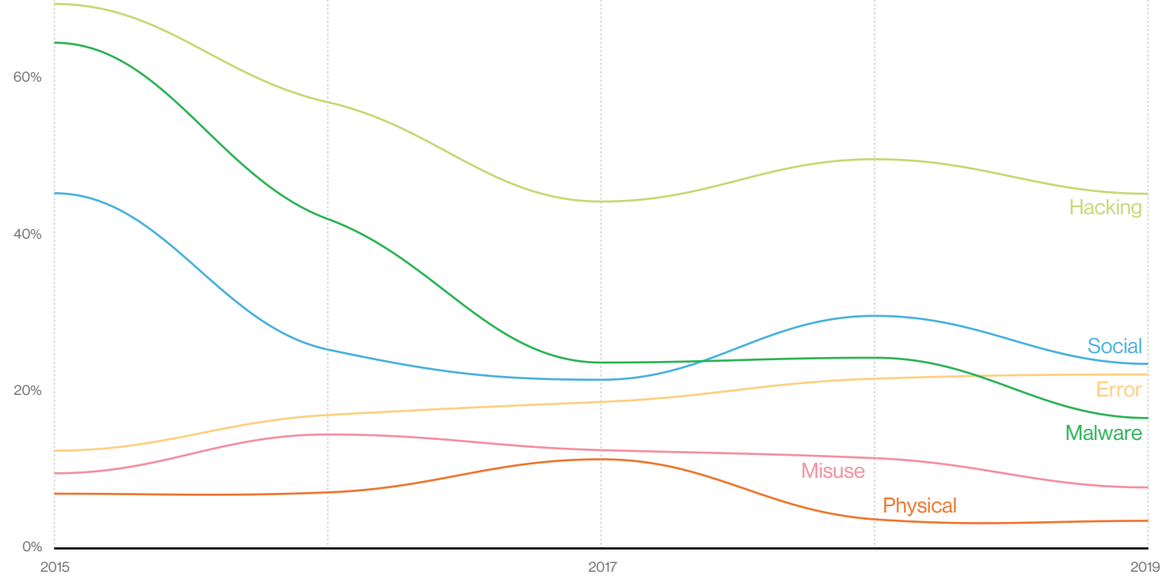


Figure 11. Actions over time in breaches

12 We are aware of reports of ransomware families that are now capturing data before encrypting so the actors can threaten to also expose the data if the ransom is not paid. However, the cases logged were documented after October 31, 2019, the close date of the data scope for this issue.

Threat action varieties

Taking a peek at threat action varieties allows us to dig a bit deeper into the bad guy's toolbox. Figure 12 provides an idea of what action varieties drive incident numbers and, shocker, Denial of Service (DoS) plays a large part. We also see a good bit of phishing, but since data disclosure could not be confirmed, they remain incidents and do not graduate to breach status (but maybe they can if they take a couple of summer classes). In sixth overall, we see ransomware popping up like a poor relation demanding money—which, in many cases, they get.

When we again switch back to looking at the top Action varieties for breaches in Figure 13, we see our old foes, Phishing, Use of stolen credentials and Misconfiguration in the top five. Misdelivery is making an impressive showing (mostly documents and email that ended up with the wrong recipients) this year. While we don't have data to prove it, we lean toward the belief that this is an artifact of breach disclosure becoming more normalized (and increasingly required by privacy laws around the world), especially for errors.

Finally, you'll notice "Other" in the mix. As we mentioned in the "DBIR Cheat sheet" section at the very beginning of this report, "Other" represents any enumeration not represented by one of the categories in the figure. It turns out there are a lot of breaches (675 to be specific) that didn't contain any of the top varieties. Breaches (like people and problems) come in many shapes and sizes and are never too far away from your front door.

Figure 12. Top threat Action varieties in incidents (n = 23,619)

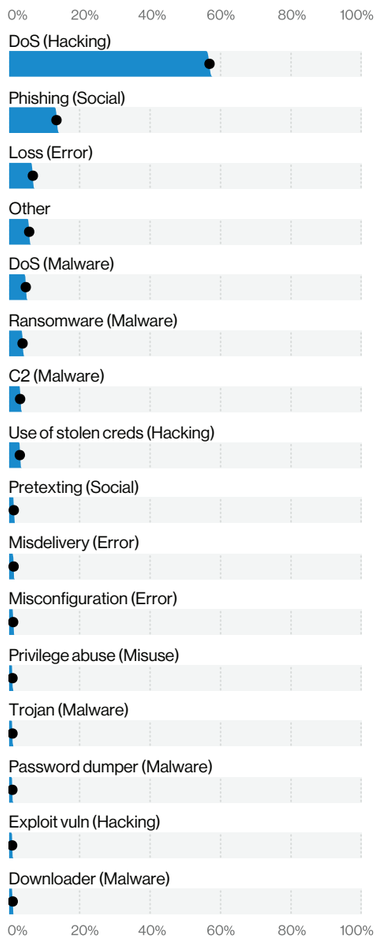


Figure 13. Top threat Action varieties in breaches (n = 2,907)

Error

Errors definitely win the award for best supporting action this year. They are now equally as common as Social breaches and more common than Malware, and are truly ubiquitous across all industries. Only Hacking remains higher, and that is due to credential theft and use, which we have already touched upon. In Figure 14 you can see that since 2017, Misconfiguration errors have been increasing. This can be, in large part, associated with internet-exposed storage discovered by security researchers and unrelated third parties. While Publishing errors appear to be decreasing, we wouldn't be surprised if this simply means that errors formerly attributed to publishing a private document on an organization's infrastructure accidentally now get labeled Misconfiguration because the system admin set the storage to public in the first place.

Finally, it is also worth noting what isn't making the list. Loss is down among the single digits this year as opposed to over 30% in 2010. Disposal errors are also not really moving the needle. Errors have always been present in high-ish numbers in the DBIR in industries with mandatory reporting requirements, such as Public Administration and Healthcare. The fact that we now see Error becoming more apparent in other industries could mean we are getting better at admitting our mistakes rather than trying to simply sweep them under the rug.

Of course, it could also mean that since so many of them are caught by security researchers and third parties, the victims have no choice but to utter "mea culpa." Security researcher has become the most likely Discovery method for an Error action breach by a significant amount (Figure 15), being over six times more likely than it was last year. However, we here on the DBIR team are of an optimistic nature, so we will go with the former conclusion.

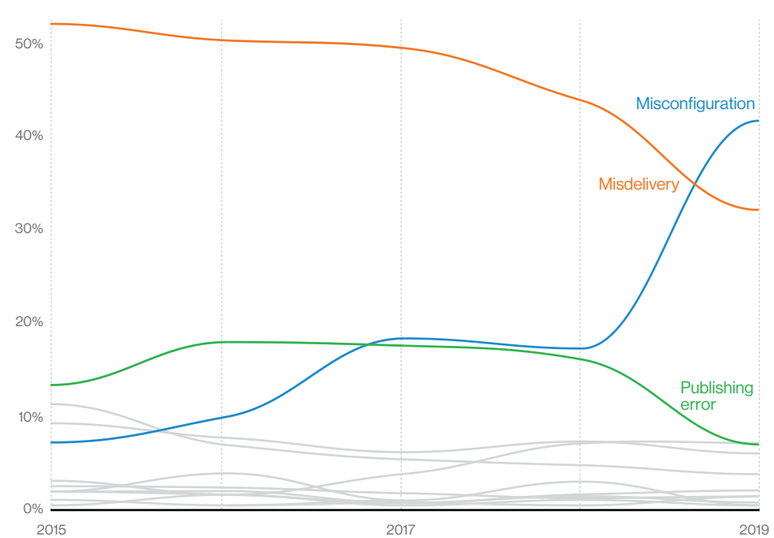


Figure 14. Top Error varieties over time in breaches

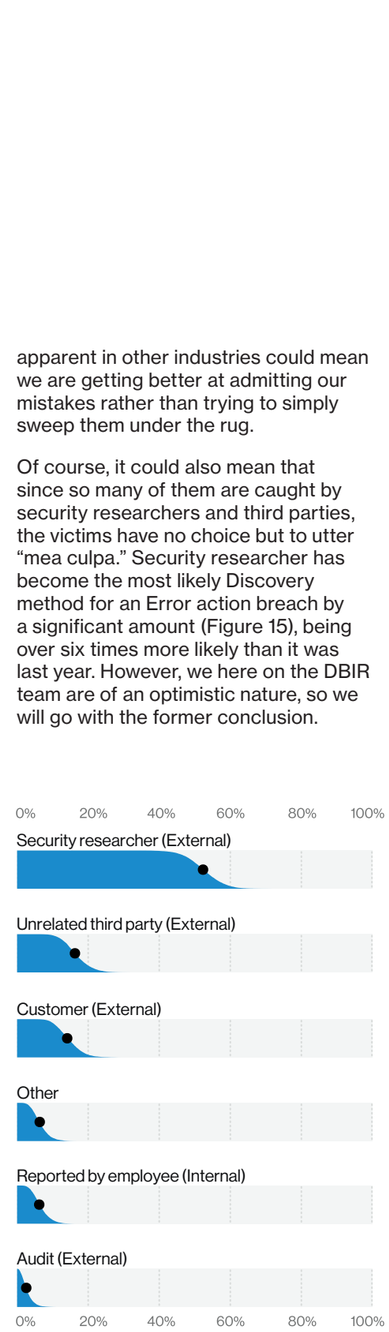


Figure 15. Top discovery methods in Error breaches (n = 95)

Malware

Our Malware findings further reinforce the trends of phishing and obtaining credentials with regard to breaches. As Figure 16 illustrates, Password dumper (used to get those sweet, sweet creds) has taken the top spot among breach Malware varieties. Email (usually associated with Phishing) and Direct install (an avenue generally—but not always—requiring credentials) are the top vectors.

Ransomware is the third most common Malware breach variety and the second most common Malware incident variety. Downloaders follow closely behind Ransomware, and they are clearly doing their jobs, not only moving Ransomware, but also Trojans.[13] It is perhaps worth noting that Cryptocurrency mining doesn't even make the top 10 list, which we know is sure to disappoint all our HODL readers.

However, it is important to acknowledge that the relative percentage of Malware that we see present in breaches and incidents may not correspond to your experiences fighting, cleaning and quarantining malware throughout your own organization. With that in mind, we would like to spend some time talking about bias, more precisely survivorship bias regarding those varieties.

Password dumper (used to get those sweet, sweet creds) has taken the top spot among breach Malware varieties.

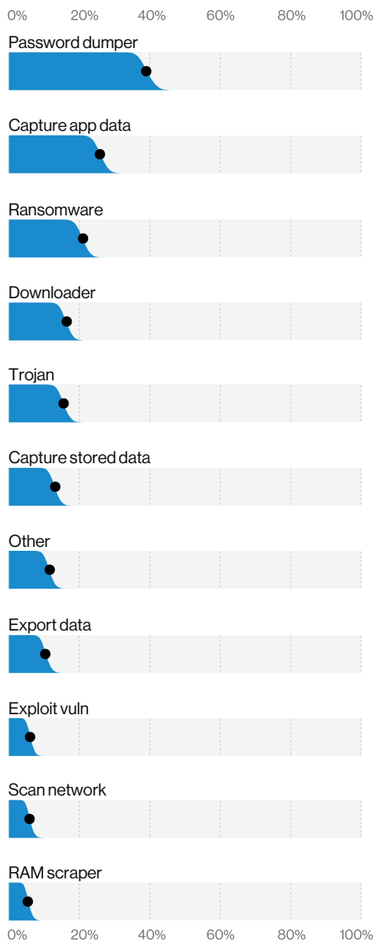


Figure 16. Top Malware varieties in breaches (n = 506)

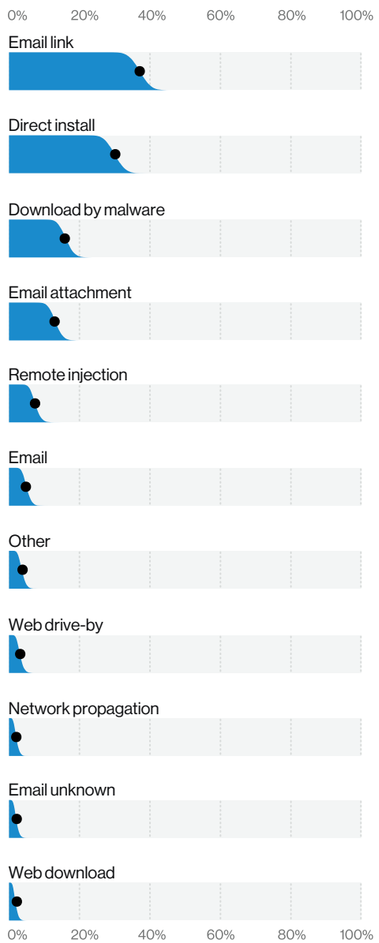


Figure 17. Top Malware vectors in breaches (n = 360)

Survivorship bias

We talk about survivorship bias (or more formally selection bias) in the "Methodology" section, but this is a good place for a call out. You, us, everyone looks at a lot of malware data. Our incident corpus suffers from the opposite of survivorship bias. Breaches and incidents are records of when the victim didn't survive.

On the other hand, malware being blocked by your protective controls is an example of survivorship bias where the potential victim *didn't* get the malware. Since we have both types of data at our disposal in the DBIR, it can highlight four possible situations:

1. **Large numbers in both blocks and incidents:** This is something big. It's being blocked but also happening a lot
2. **Large numbers in incidents but not blocks:** This is potentially happening more than it's being caught
3. **Large numbers in blocks but not incidents:** We're doing well at this. It's getting caught more than it's getting through
4. **Small numbers in both blocks and incidents:** This just ain't happening much

Ransomware

Traditionally, Ransomware is categorized as an incident in the DBIR and not as a breach, even though it is considered a breach in certain industries for reporting purposes (such as Healthcare) due to regulatory guidance. The reason we consider it only an incident is because the encryption of data does not necessarily result in a confidentiality disclosure. This year, however, ransomware figures more prominently in breaches due in large part to the confirmed compromise of credentials during ransomware attacks. In still other cases, the "breach" designation was due to the fact that personal information was known to have been accessed in addition to the installation of the malware.

Ransomware accounted for 3.5% of unique malware samples submitted for analysis, not such a big number overall. At least one piece of ransomware was blocked by 18% of organizations through the year,[14] even though it presented a fairly good detection rate of 82% in simulated incident data.

However, it shows up heavily in actual incidents and breaches, as discussed previously. This indicates that it falls into category #2 in the survivorship bias callout. It's a big problem that is getting bigger, and the data indicates a lack of protection from this type of malware in organizations, but that can be stopped. Part of its continued growth can be explained by the ease with which attackers can kick off a ransomware attack. In 7% of the ransomware threads found in criminal forums and market places, "service" was mentioned, suggesting that attackers don't even need to be able to do the work themselves. They can simply rent the service, kick back, watch cat videos and wait for the loot to roll in.

It's a big problem that's continuing to get bigger.

Droppers and Trojans

As we pointed out earlier, Trojans, although still in the top five malware varieties, have been decreasing over time. However, their backdoor and remote-control capabilities are still a key functionality for more advanced attackers to operate and achieve their objectives in more intricate campaigns. Downloaders are a common way to get that type of malware on the network, and they made up 19% of malware samples. Nineteen percent were classified as backdoors and 12% were keyloggers.

Droppers and Trojans seem to fall into category #3 in the survivorship bias callout. We see them quite frequently in malware, but they do not necessarily appear in a large number of incidents and breaches. One possible explanation for this is that we might be simply getting better at blocking the cruder and more commoditized versions of this type of malware, thereby pushing unsophisticated attackers increasingly to smash-and-grab tactics. Additionally, the shift to web interfaces for most of our services may simply mean Trojans have a smaller attack surface to exploit.

13 A combination of multiple malware varieties: RAT, Trojan, C2, Backdoor and Spyware/keylogger

14 Please bear in mind that incidents that would result in a Ransomware attack can also be stopped before the malware even manifests itself, so this is maybe an underestimation.

Malware with vulnerability exploits

If Droppers and Trojans are examples of category #3, then Malware that exploits vulnerabilities falls under category #4. It ranks at the bottom of malware varieties in Figure 16. Figure 25 (ahead in the "Hacking" section) shows that exploiting vulnerabilities in Malware is even more rare than in Hacking (where it's already relatively scarce). While successful exploitation of vulnerabilities does still occur (particularly for low-hanging fruit as in Figure 22—also in the "Hacking" section), if your organization has a reasonable patch process in place, and you do not have a state-aligned adversary targeting you, then your time might be better spent attending to other threat varieties.

Cryptocurrency mining

The cryptocurrency mining malware variety falls squarely into category #4. It accounted for a mere 2.5% of malware among breaches and only 1.5% of malware for incidents. Around 10% of organizations received (and blocked) Cryptocurrency mining malware at some point throughout the course of the year.[15]

The breach simulation data clues us in on what might be happening, as it indicates that the median block rate for cryptocurrency mining malware was very high. Another valid theory is that cryptomining occurrences rarely rise to the level of "reported incident" unless we are talking about instances running on stolen cloud infrastructure. These cost your organization a lot of money while generating less loose change than the threat actor could have found in their couch cushions.

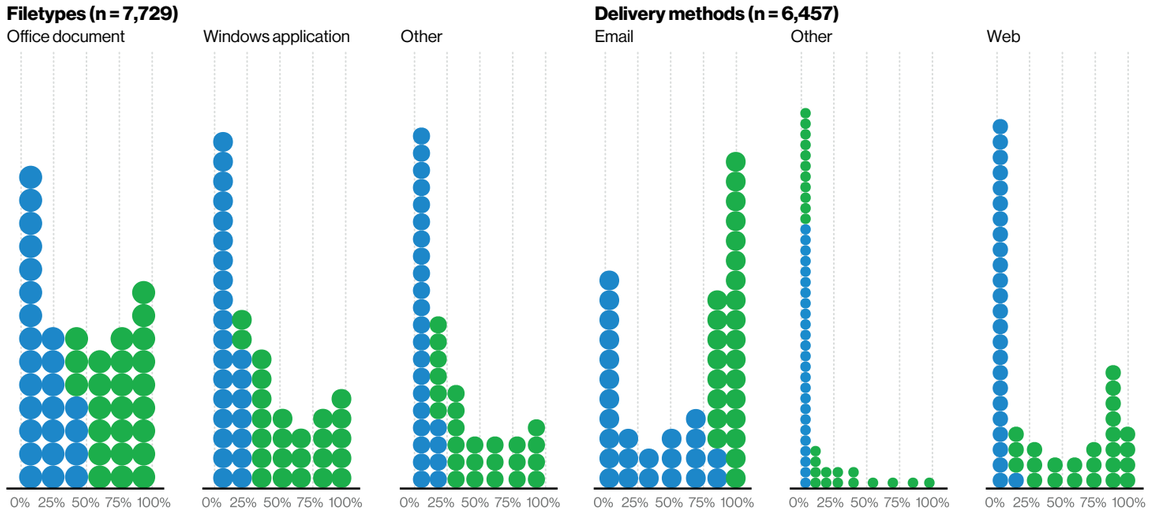


Figure 18. Top malware filetypes and delivery methods

15 The potential underestimation from incidents being stopped before the malware manifests itself is also valid here.

Malware delivery

Finally, this year we've dug a bit deeper into the malware delivery methods. Office documents and Windows® apps still tend to be the malware filetype of choice; however, the "Other" category has also grown relatively large. Most malware is still delivered by email, with a smaller amount arriving via web services, and almost none by other services (at least when detected).

One takeaway from Figure 18 is that the "average" really doesn't represent a great many companies. For example, approximately 22% of organizations got almost none of their malware via email, while about 46% got almost all of theirs that way. If you look at the Office documents part of the malware filetypes chart, other than a spike of organizations near 0%, all the other dot piles are almost the same—meaning that type of delivery is almost uniformly distributed. When attempting to determine what percentage of malware your organization would receive as an Office document, you would be as likely to be correct by throwing a dart at that figure[16] as by basing it on data. This is not to indicate that it is low, just that it is simply all over the map.

Speaking of maps, Figure 19 provides a glimpse at the other filetypes of malware organizations typically see. It lacks the detail of Figure 18, but still serves as an adequate visual reminder that malware comes in a variety of types, most of which apparently look like lengths of hardwood flooring. Thankfully, as we stated previously, malware is not showing up as frequently in incidents and breaches. So, if you obtain a good tool to block it where possible you can focus your attention on more pressing matters.[17]

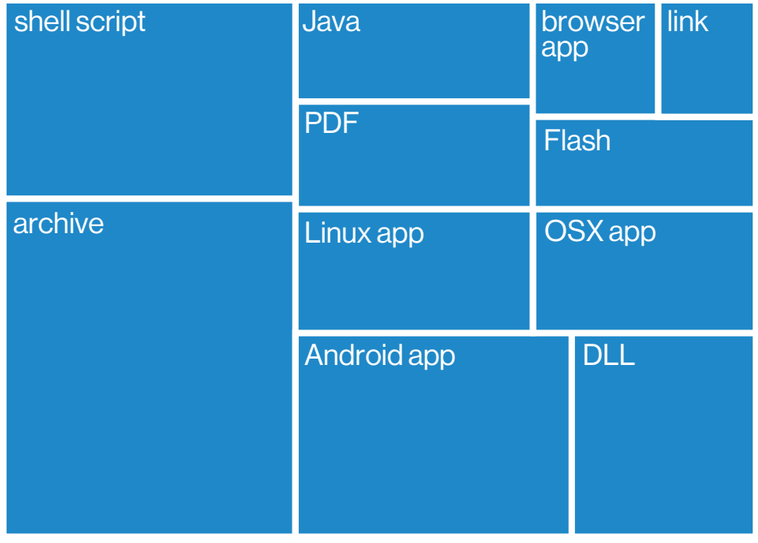


Figure 19. Other malware filetypes (n = 13.6 million)

16 Other than zero obviously. And please exercise caution with sharp objects around coworkers, family members and pets if you attempt this.
17 Credential theft and use, Phishing and Errors.

Hacking

At a high level, Hacking can be viewed as falling into three distinct groups: 1) those utilizing stolen or brute-forced credentials; 2) those exploiting vulnerabilities; and 3) attacks using backdoors and Command and Control (C2) functionality.

However, it must be said that Hacking and even breaches in general (at least in our dataset) are driven by credential theft. Over 80% of breaches within Hacking involve Brute force or the Use of lost or stolen credentials. These Hacking varieties (Figure 20 below), along with exploitation of a vulnerability (of which SQLi is a part), are associated in a major way with web applications as illustrated in Figure 21. We have spent some time on this over the last year, and it is important to reassert that this trend of having web applications as the vector of these attacks is not going away. This is associated with the shift of valuable data to the cloud, including email accounts and business-related processes.

Use of backdoor or C2 (checking in at third place) are both associated with more advanced threats, since, for more intricate campaigns and data exfiltration missions, there is nothing quite like the human touch. For better or worse, the promise of fully autonomous Artificial Hacking Intelligence (AHI) is still at least 15 years away,[18] along with flying cars.

Over 80% of breaches within Hacking involve Brute force or the Use of lost or stolen credentials.

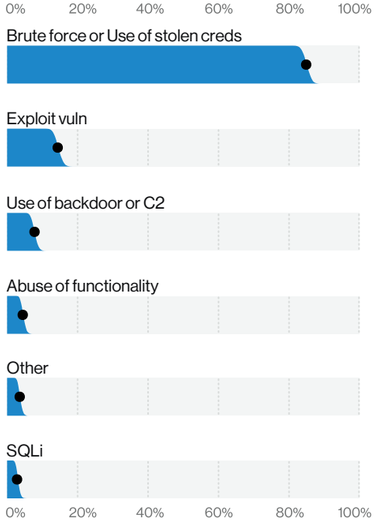


Figure 20. Top Hacking varieties in breaches (n = 868)

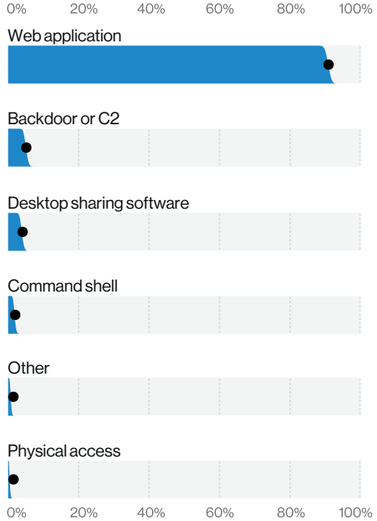


Figure 21. Top Hacking vectors in breaches (n = 1,361)

18 [citation needed] I read this in some vendor marketing copy somewhere, I'm sure. OK, I didn't, but doesn't it sound like something I would?

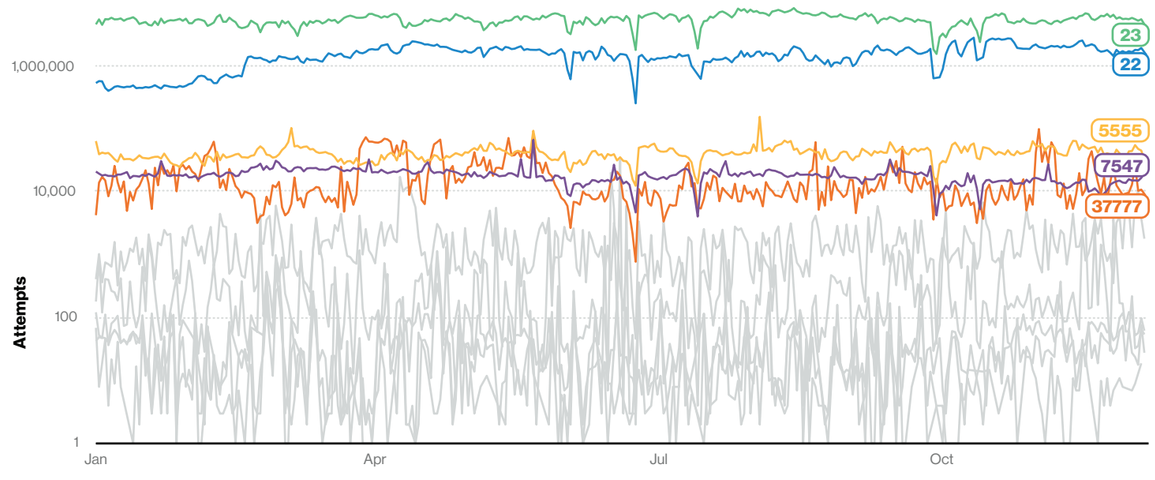


Figure 22. Connection attempts by port over time in honeypot data (n = 2.55 billion)

Using and abusing credentials

Criminals are clearly in love with credentials, and why not since they make their jobs much easier? If you refer back to Figure 6 at the very beginning of the Results and Analysis section, it is apparent that use of credentials has been on a meteoric rise. Figure 22 represents connection attempts by port over time based on contributor honeypot data, and provides another take on the topic. As it depicts, SSH (port 22) and Telnet (port 23) connection attempts are two orders of magnitude[19] above the next cluster of services. Let's explore credential stuffing and then move on to exploiting vulnerabilities.

Additional contributor data sheds light onto the credential stuffing attacks criminals are attempting. Figure 23[20] shows the number of attempts orgs who had any credential stuffing attempts typically received. As you will notice, it is a relatively smooth bell curve with a median of 922,331. Granted, a good number of those login/password combos attempted will be as complex as "admin/admin" or "root/hunter2" but those sustained attacks over time are succeeding according to our incident dataset.

Something you might be wondering is "Do credential leaks lead to more credential stuffing?" We took a look at a dataset of credential leaks and compared it to the credential stuffing data we had. You can see in Figure 24 that the answer is no.[21] We found basically no relationship between a credential leak and the amount of credential stuffing that occurred the week after. Instead it appears to be a ubiquitous process that moves at a more or less consistent pace: Get a leak, append to your dictionary, continue brute forcing the internet. Rinse, repeat.

19 They may seem close, but that is a log scale (https://en.wikipedia.org/wiki/Logarithmic_scale).
20 If this figure is confusing, see the dot plot explanation in the "DBIR Cheat sheet" section.
21 Where are my negative result experiment fans? A toast to science, my colleagues!

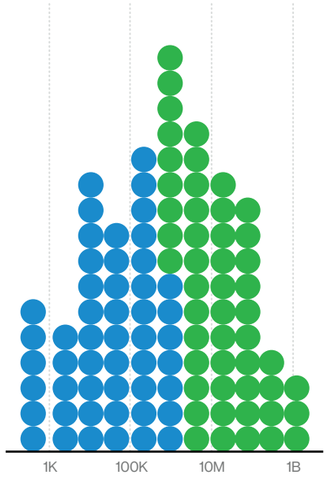


Figure 23. Credential attempts per org per year (n = 631)

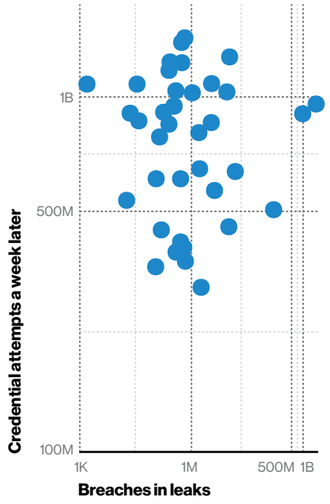


Figure 24. Relationship between credential leads and credential attempts one week later. $R^2 = 0.006$ (n = 37)

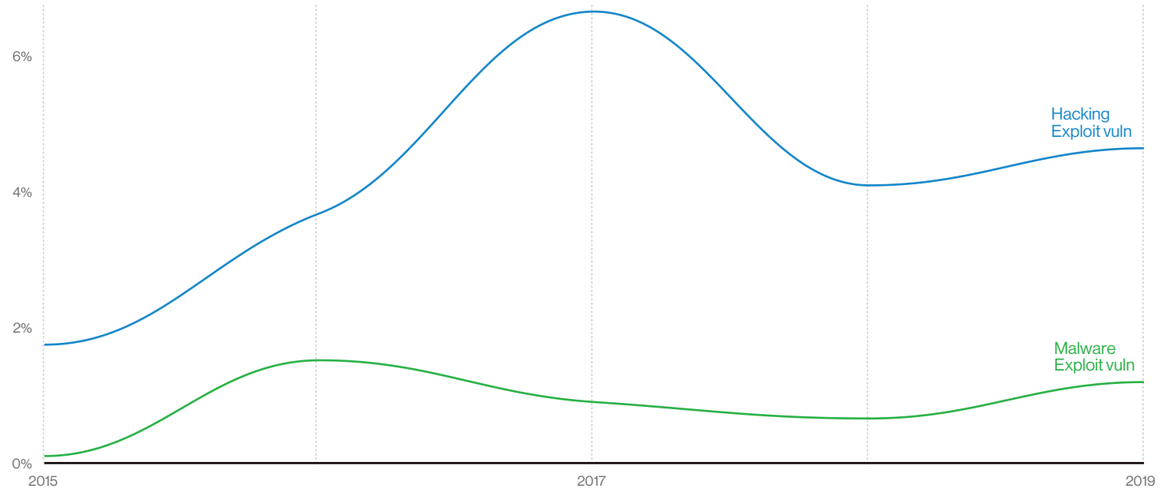


Figure 25. Vulnerability exploitation over time in breaches

Exploiting vulnerabilities

Vulnerabilities occupy a huge amount of mind-share in information security. Yet, harkening back to that bit about survivorship bias in the "Malware" section, it's more of situation #3 than situation #1. There are lots of vulnerabilities discovered, and lots of vulnerabilities found by organizations scanning and patching, but a relatively small percentage of them are used in breaches, as you can see in Figure 25. Although exploiting vulnerabilities is in second place in breach Hacking varieties, it has not played a major role within incidents found in the DBIR over the last five years. In fact, it reached its peak at just over 5% as a Hacking variety in 2017. In our security information and event management (SIEM) dataset, most organizations had 2.5% or less of alerts involving exploitation of a vulnerability.[22]

But that doesn't mean that the attackers don't give it a try anyway. Clearly, the attackers are out there and if you leave unpatched stuff on the internet, they'll find it and add it to their infrastructure.[23] We hear a lot about new vulnerabilities and their prevalence both on the internet and within organizations. Does the internet as a whole become more vulnerable with every new vulnerability that gets discovered?[24] And are those unpatched vulnerabilities that are adding to the problem likely to be present on *your* systems?

To test whether that[25] is true, we conducted a little investigation this summer. We looked at two sets of servers hosted on public IP addresses: ones vulnerable to an Exim vulnerability discovered in 2019[26] and randomly chosen IPs. As we see in Figure 26, hosts that were vulnerable to the Exim vulnerability were also vulnerable to 10-year-old SSH vulnerabilities[27] much more frequently than the random sample.

The takeaway is that it wasn't just the Exim vulnerability that wasn't patched on those servers. NOTHING was patched. For the most part, no, the internet as a whole does not seem to be getting less secure with each new vulnerability, at least not after the short window before organizations that are on top of their patch management update their systems.[28] You can just as easily exploit those vulnerable servers with that l33t 10-year-old exploit you got from your h4x0r friend on Usenet.

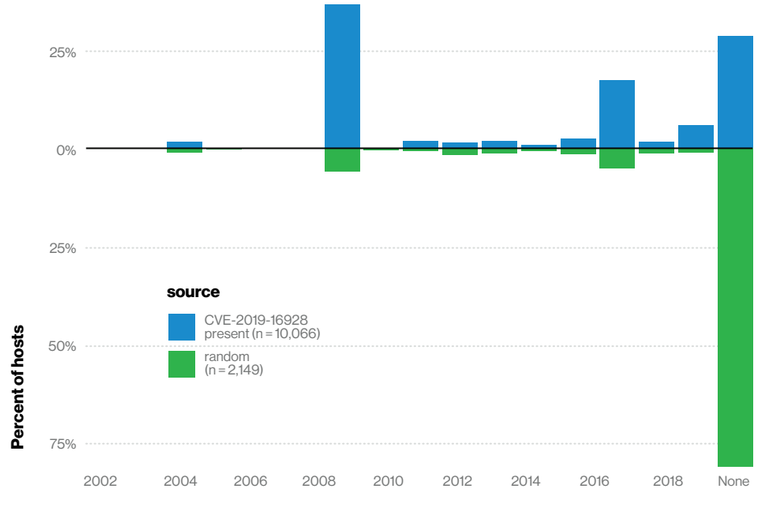


Figure 26. Comparing oldest other vulnerability for internet-facing hosts with EXIM CVE-2019-16928 vs randomly selected hosts

22 Caveat emptor, to do this we used existing contributor mappings to MITRE ATT&CK and traced to our VCAF mapping as discussed in Appendix B.
23 Granted, I don't have any studies that show that stealing CPU cycles is a lot cheaper than traditional infrastructure as a service (IaaS), but given my last cloud services bill, I don't see how it couldn't be.
24 TL;DR: Mostly no. Not for long anyway.
25 Does the internet as a whole get more vulnerable with each new vulnerability?
26 CVE-2019-16928
27 And basically, every vulnerability since then
28 Shout-out to our summer intern Quinnan Gill who did this research for us. You're awesome!

But what about the second question: Are those likely to be *your* systems that are vulnerable?[29] To test this, we took two samples from vulnerability scan data: organizations with the Eternal Blue vulnerability[30] present on their systems and those without. In Figure 27,[31] we see the same thing as in Figure 26. The systems that were vulnerable to Eternal Blue were also vulnerable to everything from the last decade or two. Once again, no, each new vulnerability is not making you that much more vulnerable. Organizations that patch seem to be able to maintain a good, prioritized patch management regime.

Still, we're not in the fourth survivorship bias situation here. Attackers *will* try easy-to-exploit vulnerabilities if they encounter them while driving around the internet. Since you just came from the "Credentials" section, you may remember that Figure 22, which illustrates that once you get below the SSH and Telnet lines on the chart, the next three services that we conveniently highlighted are port 5555 (Android Debug Bridge, or adb—really popular lately), port 7547 (common router RPC port) and port 37777 (popular with IP cameras and DVRs).

If you will allow us a mixed metaphor, there is no outrunning the bear in this case, because the bears are all being 3D-printed in bulk and automated to hunt you.

So, carry on my wayward son and keep doing what you're doing (you know, patching), and perhaps skip over to the "Assets" section to get an inkling of what you might be missing.

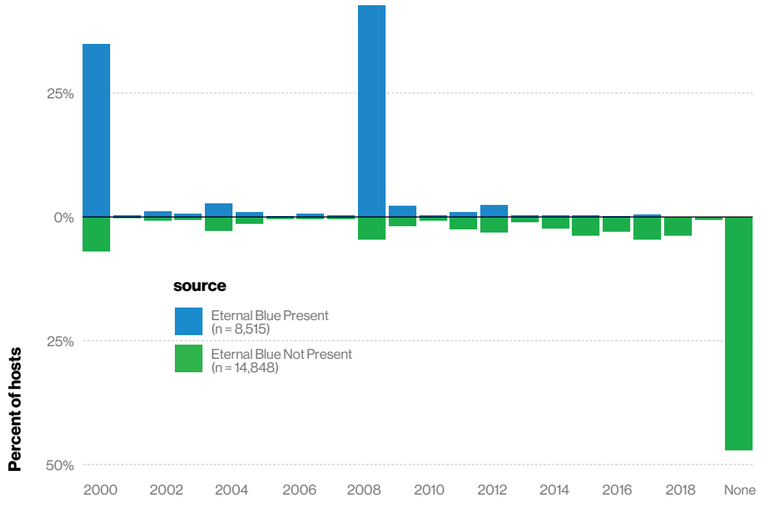


Figure 27. Comparing oldest other vulnerability for hosts with Eternal Blue vs hosts without

29 TL;DR: Again, probably not. If you are patching, of course.
30 CVE-2017-0144
31 We use Eternal Blue here and the Exim vulnerability in Figure 26 because the analysis for Figure 26 came from the summer while Figure 27 data is from last year, potentially before CVE-2019-16928.

Social

If action types were people, you would probably give Hacking, Malware and Error a wide berth because they just sound like they would be less than friendly. But Social sounds as though it would be much more happy-go-lucky. More likely to house-sit for you, invite you to play bunko and include you in neighborhood barbecues. You'd be wrong though. Social comes with a devious attitude and a "take me to your manager" haircut. Figure 28 shows Social broken down into two types of incidents: Phishing and Pretexting.[32] When it comes to breaches, the ratio remains quite similar, only with slightly lower numbers.

Social actions arrived via email 96% of the time, while 3% arrived through a website. A little over 1% were associated with Phone or SMS, which is similar to the amount found in Documents. If you take a glance at Figure 29, you'll notice that while credentials are by far the most common attribute compromised in phishing breaches, many other data types are also well represented. Phishing has been (and still remains) a fruitful method for attackers. The good news is that click rates are as low as they ever have been (3.4%), and reporting rates are rising, albeit slowly (Figure 30).

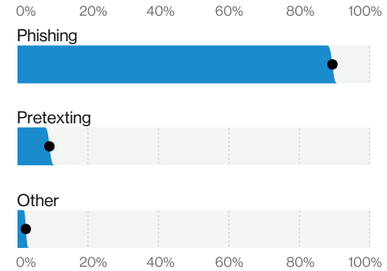


Figure 28. Top Social varieties in incidents (n = 3,594)

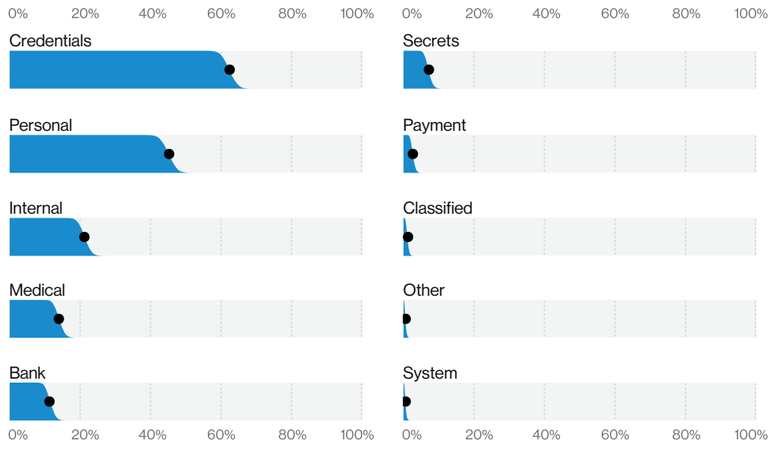


Figure 29. Top data varieties compromised in Phishing breaches (n = 619)

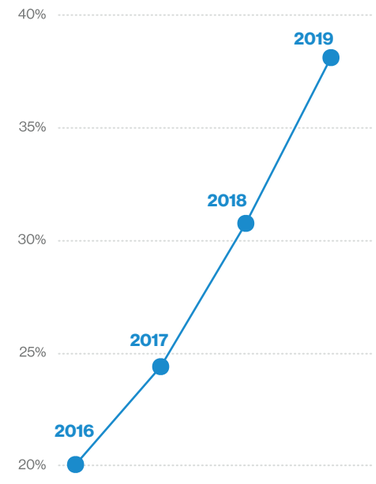


Figure 30. How many phishing test campaigns are reported at least once

32 Often business email compromises (BECs), but given that it works even if you don't compromise an email address, you might see us referring to Financially Motivated Social Engineering or FMSE.

Financially Motivated Social Engineering

Financially Motivated Social Engineering (FMSE) keeps increasing year-over-year (Figure 31), and although it is a small percentage of incidents, in raw counts, there were over 500 in our dataset this year. These attacks typically end up in our Everything Else pattern, as they are purely social in nature. There is no malware component, as you would see in the more advanced nation-state scenario, nor is there any effort to gain a foothold and remain persistent in the victim's network. These are simply a "get what you can when you can" kind of attack.

This is not to say that they cannot be sophisticated in the lengths the adversary is willing to go to for success. In prior years, they would impersonate CEOs and other high-level executives and request W-2 data of employees. They have largely changed their tactics to just asking for the cash directly—why waste time with monetizing data? It's so inefficient. Their inventiveness in the pretext scenario to lend a level of believability to their attempt is a measure of how good these people are at their jobs.

Last year, we looked at the median impact cost for incidents reported to the FBI IC3. With regard to business email compromises (BEC), we noticed that most companies either lost $1,240 or $44,000 with the latter being slightly more frequent (Figure 32).

Also, last year we stated that when "the IC3 Recovery Asset Team acts upon BECs, and works with the destination bank, half of all U.S.-based business email compromise victims had 99% of the money recovered or frozen; and only 9% had nothing recovered." They continued to record that metric and this year it improved slightly, indicating that 52% recovered 99% or more of the stolen funds and only 8% recovered nothing.

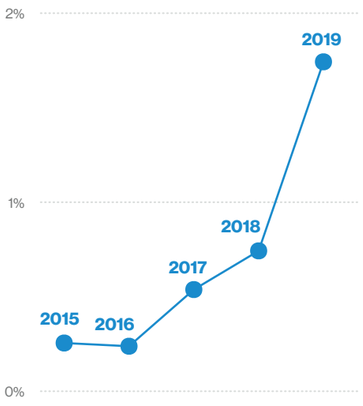


Figure 31. Financially Motivated Social Engineering (FMSE) over time in incidents

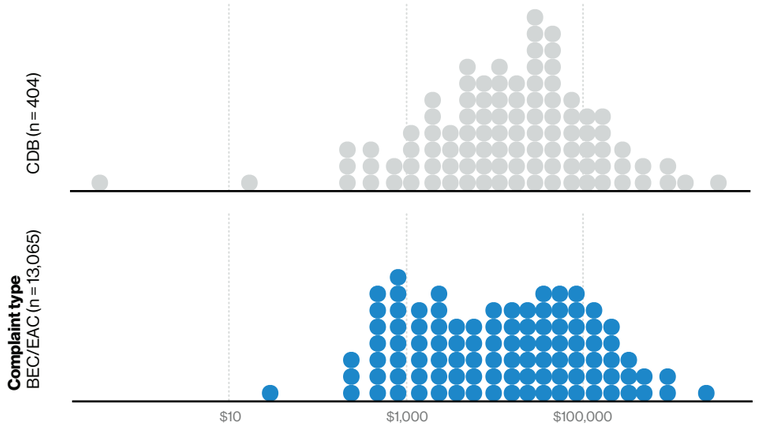


Figure 32. Loss amount in Corporate Data Breaches (CDB) and business email compromises/(individual) email account compromises (BEC/EAC) (Excludes complaints with zero loss amount)

Assets

Figure 33 provides an overview of the asset landscape. Servers are the clear leader and they continue to rise. This is mainly due to a shift in industry toward web applications (the most common asset variety in Figure 34) with system interfaces delivered as a software as a service (SaaS), moving away from that seven-year-old spreadsheet with those great macros that Bob from accounting put together. Person[33] holds second place for the second year in a row, which is not surprising given how Social actions have stayed relevant throughout this period.

Kiosks and Terminals continued to decline as they did last year. This is primarily due to attackers transitioning to "card not present" retail as the focus of their efforts, rather than brick-and-mortar establishments.

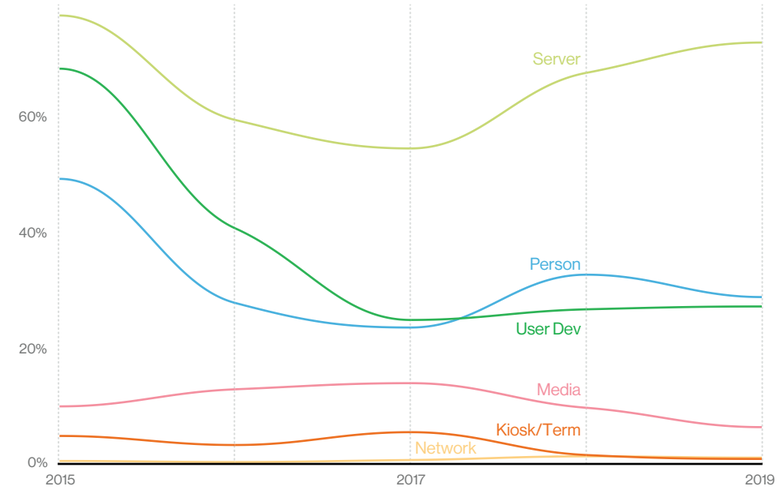


Figure 33. Assets over time in breaches

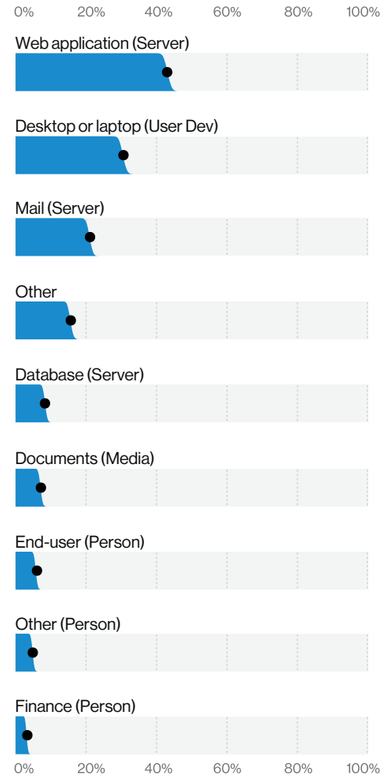


Figure 34. Top Asset varieties in breaches (n = 2,667)

33 I know it is weird, maybe even dehumanizing, to think of a Person as an asset but this is meant to represent the affected party in an attack that has a social engineering component. People have security attributes too!

Head in the clouds

Cloud assets were involved in about 22% of breaches this year, while on-premises assets are still 71%[34] in our reported incidents dataset. Cloud breaches involved an email or web application server 73% of the time. Additionally, 77% of those cloud breaches also involved breached credentials. This is not so much an indictment of cloud security as it is an illustration of the trend of cybercriminals finding the quickest and easiest route to their victims.

Information Technology vs. Operational Technology

Last year we started tracking embedded assets, but that turned out to be less insightful than we anticipated. So, this year we began tracking Information Technology (IT) vs Operational Technology (OT) for assets involved in incidents instead. We hope to be able to do a more comprehensive analysis in the following years, but for now our findings were not particularly surprising: 96% of breaches involved IT, while 4% involved OT. Although 4% might not sound like a lot, if you happen to be in an industry that relies on OT equipment in your means of production, it's certainly adequate cause for concern.

Mobile devices

This year we were minding our own business, eating some plums we found in the icebox, when over a thousand cases of Loss involving Mobile Devices showed up in our dataset. We would make this incredible spike in incidents one of our key findings, but we are pretty sure "forgetting your work mobile phone in a hipster coffee shop" is not a new technique invented in 2019. Turns out data collection is partially to blame here. We updated the collection protocols with a few of our contributors, and voilà, there they were. Those Error cases made up roughly 97% of the incidents we had on Mobile Devices.

The other 3% are very interesting, though. Those incidents are split almost evenly between Espionage and Financial motives, which is incredibly significant when our overall breakdown of motives is of 64% Financial and only 5% Espionage. And while the financially motivated ones vary from Theft to the use of the device as a vessel for Pretexting, the espionage-related cases are exclusively Malware-based compromises of mobile devices to further persistence and exfiltration of data by advanced State-affiliated actors.

34 The remainder were breaches where cloud was not applicable, such as where the asset is a Person.

Asset management

We mentioned back in the "Hacking" section that hosts susceptible to major new vulnerabilities tend to also still be defenseless against many older vulnerabilities. That finding is a bit of a double-edged sword in that, while it seems to suggest that patching is working, it also suggests that asset management may not be. We found that it was most often the case that organizations have approximately 43% of their internet-facing IPs in one network.[35] However, the most common number of networks that an organization occupies is five, and half of all organizations are present on seven or more (Figure 35). If you don't know what all those networks are, you might have an asset management problem. Therefore, it might not just be an asset management problem, but also a vulnerability management problem on the assets you did not realize were there.

In over 90% of organizations, less than 10% of their internet-facing hosts had any significant vulnerabilities. In half of all orgs, less than 1% of hosts had internet-facing vulnerabilities (Figure 36). That suggests that the vulnerabilities are likely not the result of consistent vulnerability management applied slowly, but a lack of asset management instead.

Figure 35. Number of additional networks per organization (n = 86)

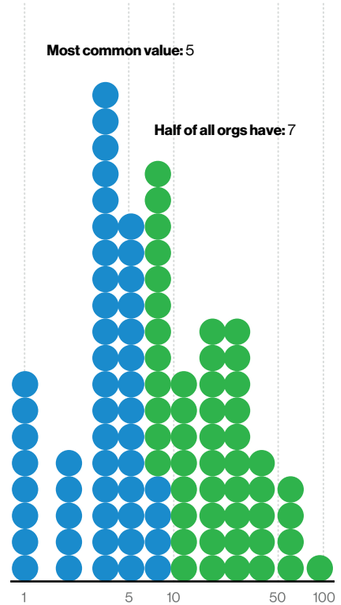
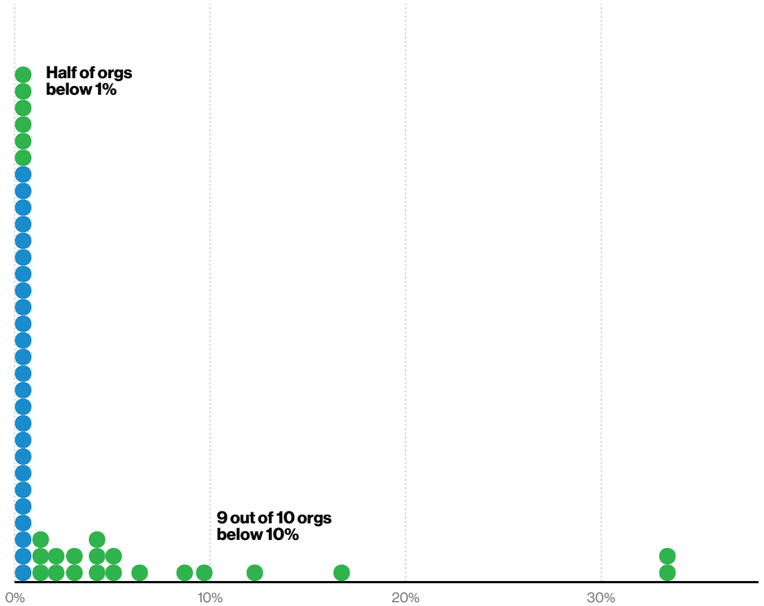


Figure 36. Percent of organizations' public IPs with significant vulnerabilities (n = 110)



35 By "network," we mean an autonomous system, represented by an autonomous system number (ASN): https://www.apnic.net/get-ip/faqs/asn/

Attributes

The compromise of the Confidentiality of Personal data leads the pack among attributes affected in breaches, as shown in Figure 37. But keep in mind that this contains email addresses and is not just driven by malicious data exfiltration, but also by "benign" errors. The one-two punch of Hacking and Error puts email addresses (and by extension personal information) at the front of the pack. Certainly, Personal information goes way beyond just email addresses, but that is the designation where those reside.

In second place, we see Credentials, which should come as no surprise since we have covered that topic sufficiently already. Alter behavior appears next and is a result of Social breaches affecting the Integrity of our victims' Person assets. Finally, we see Malware-related breaches causing the integrity violation of Software Installation.

One other notable observation from Figure 37 is that Bank and Payment data are almost equal. Five years ago, Payment information was far more common, but while compromise of bank information has stayed relatively level, Payment has continued to decline to an equivalent level.

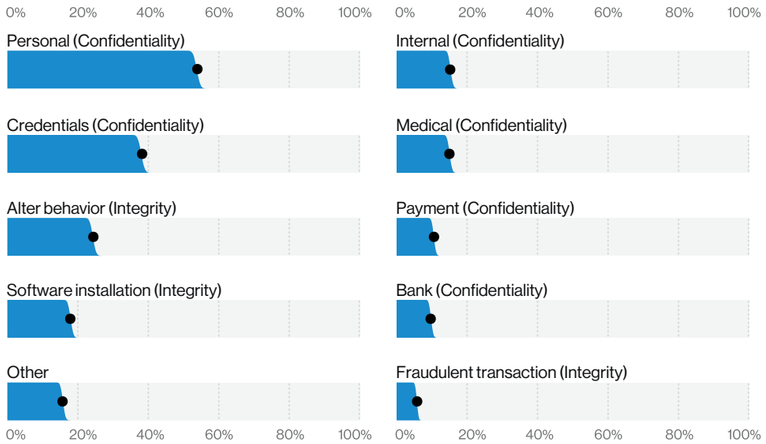


Figure 37. Top compromised Attribute varieties in breaches (n = 3,667)

Email address compromises

Given that email addresses are Personally Identifiable Information (PII) and that Personal is the most common variety of data to be breached in this year's report, we looked a bit more closely at some of the email leaks we have seen over the last 10 years. Figure 38 gives you a feel for what email top-level domains (TLDs) are being compromised the most. The "Other" category includes TLDs with less than 1% of emails, by the way.

Since .com accounts for approximately 59% of leaked emails, we focused in on that a bit. The first 150 domains that we looked at showed that most were mail registration services. That accounted for about 97% of the breaches, and provides hope that most emails compromised aren't your employees' corporate addresses. However, the little matter of the remaining 3% was comprised of tens of millions of addresses.

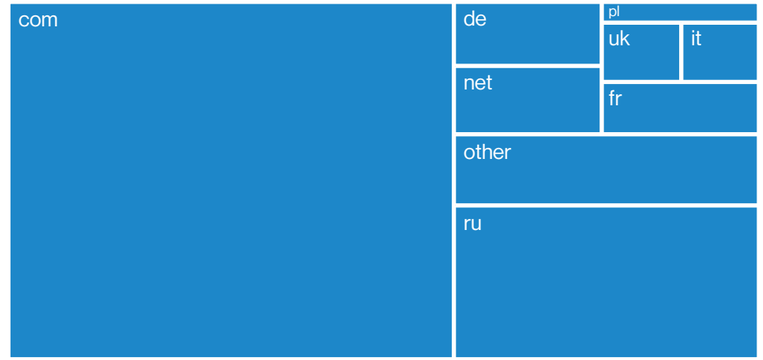


Figure 38. Prevalence of top-level domains (TLDs) in leaked emails (n = 3.94 billion)

What's that attribute going to cost you?

As reported in FBI IC3 complaints, the most common loss was $32,200 this year, up from about $29.3k last year. That's still basically in the preowned car range, and while no one wants to lose that much money, it could certainly be much worse.

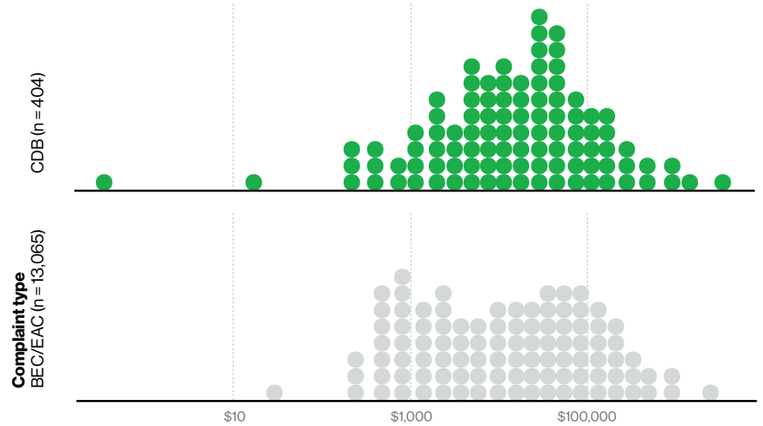


Figure 39. Loss amount in Corporate Data Breaches (CDB) and business email compromises/(individual) email account compromises (BEC/EAC)
(Excludes complaints with zero loss amount)

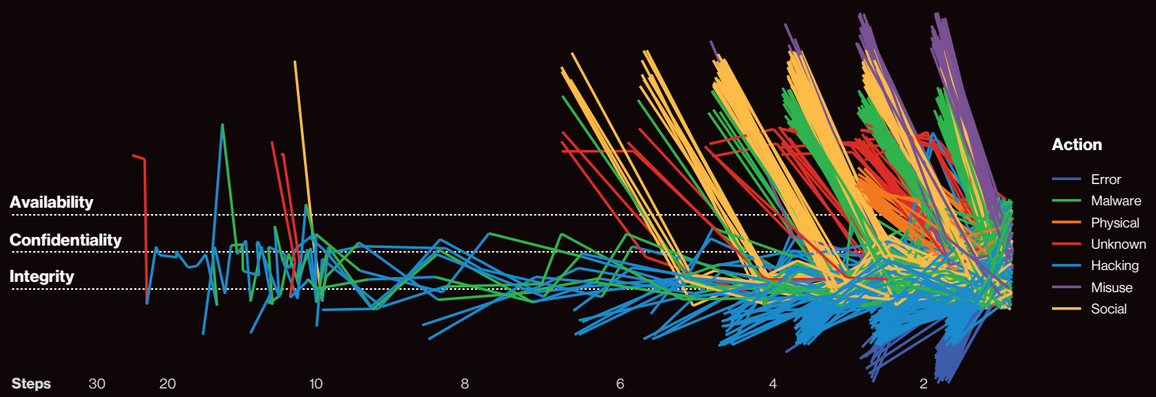
How many paths must a breach walk down?

We tend to think about incidents and breaches as a point in time. You snap your fingers and all the attacker actions are complete, the stolen data is in the attacker's saddlebags and they are off down Old Town Road and away into the sunset. Still, we all know that is not quite what actually happens. Many of the attacks studied in this report fall somewhere between a stickup and the Great Train Robbery in terms of complexity. The good news is that defenders can use this to their advantage.

As you can see in Figure 40, attacks come in numerous forms and sizes, but most of them are short, having a small number of steps (you can notice that by how the volume of line segments thin out between the four and six steps markers). The long ones tend to be Hacking (blue) and Malware (green) breaches, compromising Confidentiality (the middle position) and Integrity (the lower position) as the attacker systematically works their way through the network and expands their persistence. The benefit in knowing the "areas" (threat actions—colors/compromising specific attributes—positions) attackers are more likely to pass through in their journey to a breach gives you first advantage, because you can choose where to intercept them. You may want to stop their initial action or their last. You may not want to go near them, so you don't have to listen to "Old Town Road." All of these options are understandable in accordance with your response strategy.[36]

36 Or to how susceptible you are to ubiquitous earworms.

Figure 40. Attack paths in incidents
(n = 652. Two breaches, 77 and 391 steps respectively, not shown.)



Figures 41 and 42 provide us with our next defensive advantage. Attackers prefer short paths and rarely attempt long paths. This means anything you can easily throw in their way to increase the number of actions they have to take is likely to significantly decrease their chance of absconding with the data. Hopefully by now we have driven home the significance and prevalence of credential theft and use. While we admit that two-factor authentication is imperfect, it does help by adding an additional step for the attacker. The difference between two steps (the Texas two-step) and three or four steps (the waltz) can be important in your defensive strategy.

The difference between two steps (the Texas two-step) and three or four steps (the waltz) can be important in your defensive strategy.

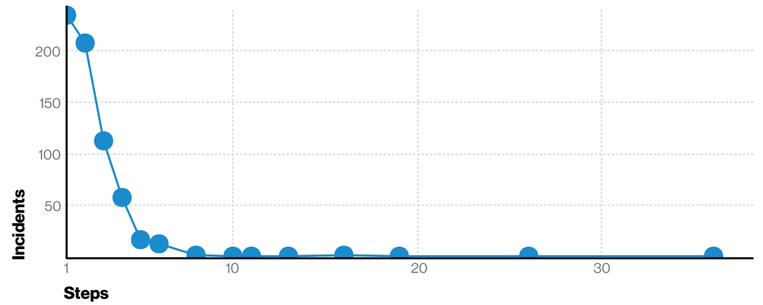


Figure 41. Number of steps per incident
(n = 654. Two breaches, 77 and 391 steps respectively, not shown.)

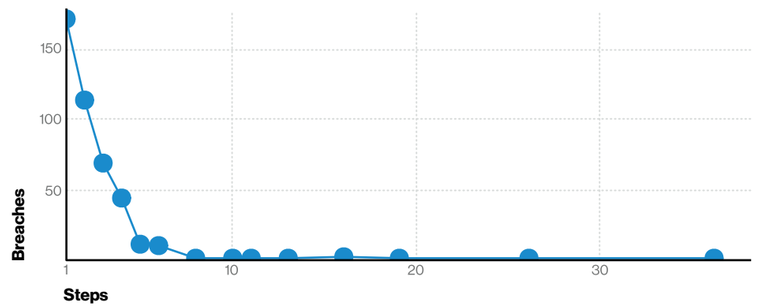


Figure 42. Number of steps per breach
(n = 429. Two breaches, 77 and 391 steps respectively, not shown.)

OK, take a deep breath and look at Figure 40. No, a butterfly did not just vomit on your report. Don't worry about trying to understand all the graphic has to tell. Instead, let us convey the concept of what you are seeing here. This abstract work of art contains a line (a "path") for each of several hundred breaches. In the way a bar chart summarizes numbers, this graph summarizes paths taken by the attacker.

Each colored line segment (a "step") represents an action taken by the threat actor along with the associated attribute that was compromised. The color of each step represents the VERIS threat action of the step, and the position where the step ends represents the attribute compromised. But the real trick to understanding this chart is that the paths start *from the left and move to the right*—the first step on a path will either come from the top of the chart or the bottom (because they have to come from somewhere) and "land" on the appropriate attribute.

So, if you pick any yellow step coming from the top of the chart starting at 4 on the horizontal axis and ending on the lower position of the chart, you just found yourself at the beginning of a four-step incident that started with a Social action that compromised the Integrity attribute. Also, notice how Error actions (the dark blue lines coming from the bottom of the chart) are usually part of very short paths and land on the Confidentiality attribute.

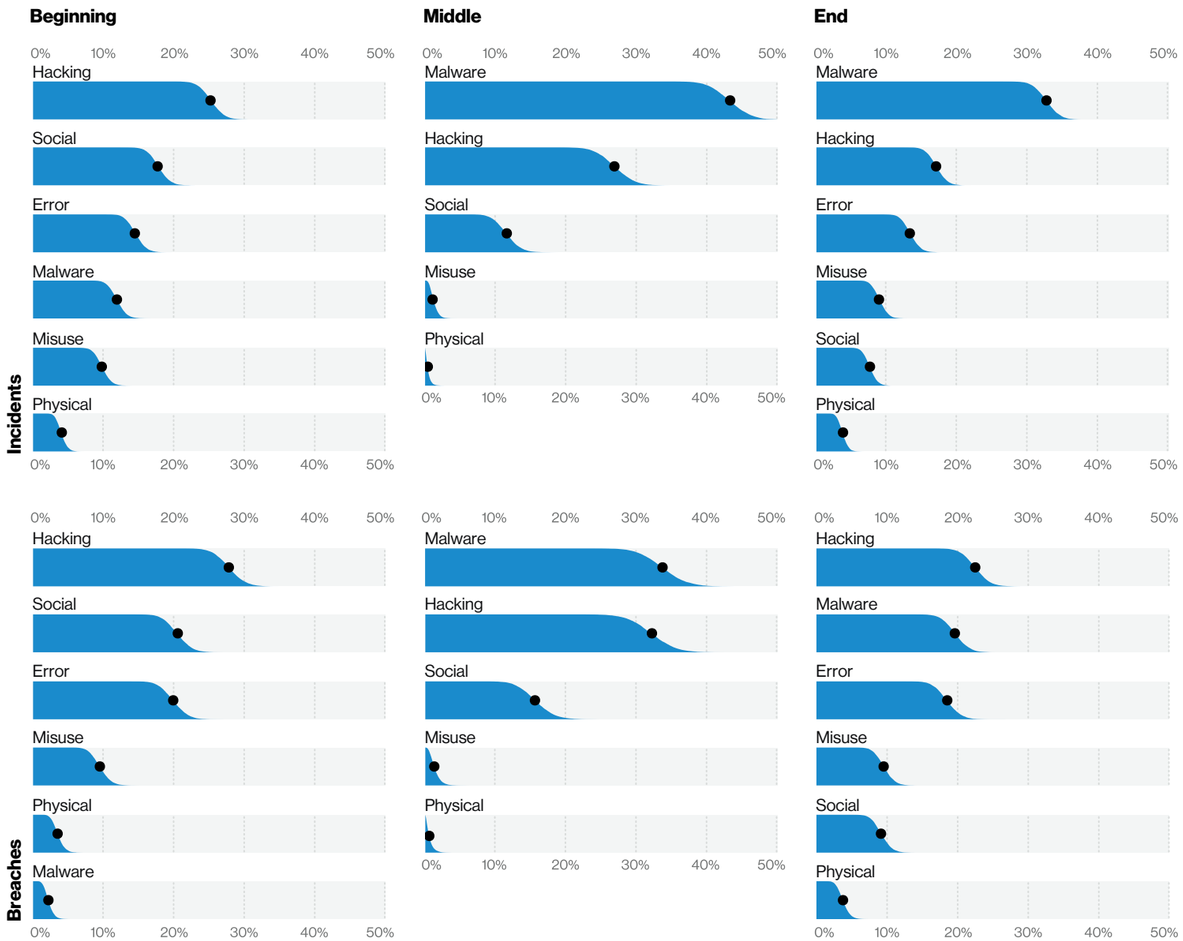
There's a small amount of noise put into the positions of the lines, since otherwise the same lines would be exactly on top of each other and we wouldn't be able to see a lot here. But mostly we did it for the art.

Finally, take a look at Figure 43. It shows what actions happen at the beginning, middle and end of both incidents and breaches. It is not what is on top that's interesting (we already know "Social–Phishing" and "Hacking–Use of stolen creds" are good ways to start a breach and "Errors" are so short that the beginning of the path is also the end). The interesting bit is what's near the bottom.

Malware is rarely the first action in a breach because it obviously has to come from somewhere. Conversely, Social actions almost never end an attack. In the middle, we can see Hacking and Malware providing the glue that holds the breach together. And so, our third defensive opportunity is to guess what you haven't seen based on what you have. For example, if you see malware, you need to look back in time for what you may have missed, but if you see a social action, look for where the attacker is going, not where they are.

All in all, paths can be hard to wrap your head around, but once you do, they offer a valuable opportunity not just for understanding the attackers, but for planning your own defenses.

Figure 43. Actions at the beginning, middle and end of incidents and breaches



Timeline

As we analyze how breach timelines have evolved over time, Discovery in days or less is up (Figure 44) and Containment in that same timeframe has surpassed its historic 2017 peak (Figure 45). However, before you break out the bubbly, keep in mind that this is most likely due to the inclusion of more breaches detected by managed security service providers (MSSPs) in our incident data contributors' sampling, and the relative growth of breaches with Ransomware as collateral damage, where Discovery is often close to immediate due to Actor disclosure.[37]

Discovery in Months or more still accounts for over a quarter of breaches. We are obligated to point out that since this is a yearly report, this is usually a trailing indicator of the actual number, as there are potentially a significant number of breaches that occurred in 2019 that just have not been discovered yet.

All in all, we do like to think that there has been an improvement in detection and response over the past year and that we are not wasting precious years of our life on a completely pointless battle against the encroaching void of hopelessness. Here, have a roast beef sandwich on us.

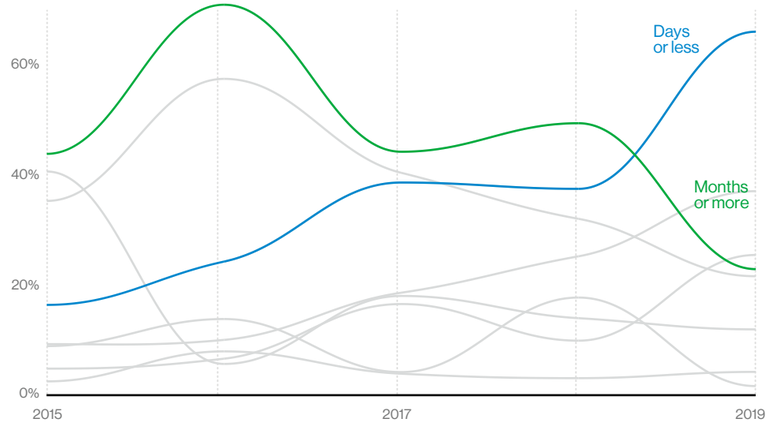


Figure 44. Discovery over time in breaches

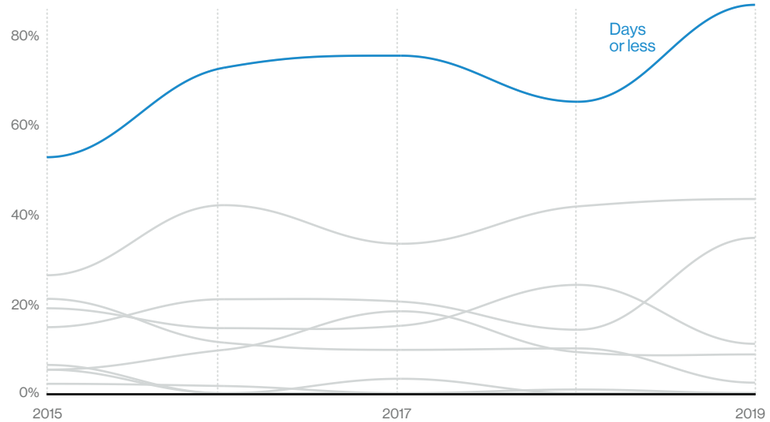


Figure 45. Containment over time in breaches

37 Nothing quite like a rotating flaming skull asking for cryptocurrency on your servers to help you "discover" a breach.

Incident classification patterns and subsets

For the uninitiated, VERIS and the DBIR may seem overwhelming when you consider both the amount of data we possess (now over 755,000 incidents over the years) and the depth of that data (over 2,400 values we are able to track on each incident). To help us better understand and communicate this vast arsenal of information, we started to leverage what we call "Patterns" in 2014, which are essentially different clusters of "like" incidents. We won't go too much into the data science-y aspect,[38] but the outcome was the identification of nine core clusters, our Incident Classification Patterns. This allows us to abstract upward and discuss the trends in the patterns rather than the trends in each of our different combinations: Actions, Assets, Actors and Attributes.

Looking over our 409,000 security incidents and almost 22,000 quality data breaches since the inception of the report, the numbers reveal that 94% of security incidents and 88% of data breaches fall neatly in one of the original nine patterns. However, when we focus our lenses on just this year's data, the percentages drop to 85% of security incidents and 78% of data breaches.

Nothing better demonstrates this than our category of "Everything Else," effectively designed to be our spare-USB-cable drawer of breaches, having risen to one of the top patterns due to the rise of Phishing, while some of the other patterns have drastically fallen since their initial inception. It seems that time waits for no pattern, and the only breach constant is breaches changing over time.

The patterns will be referenced more in the "Region" and "Industry" sections, but to get acquainted with them or to rekindle a prior relationship, they are defined here.

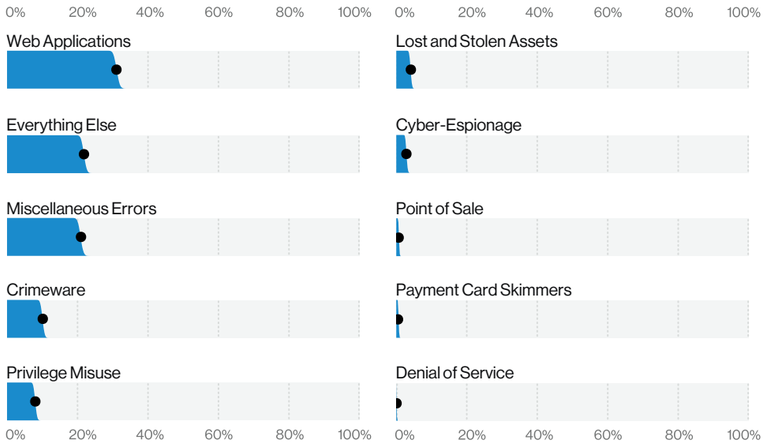


Figure 46. Patterns in breaches (n = 3,950)

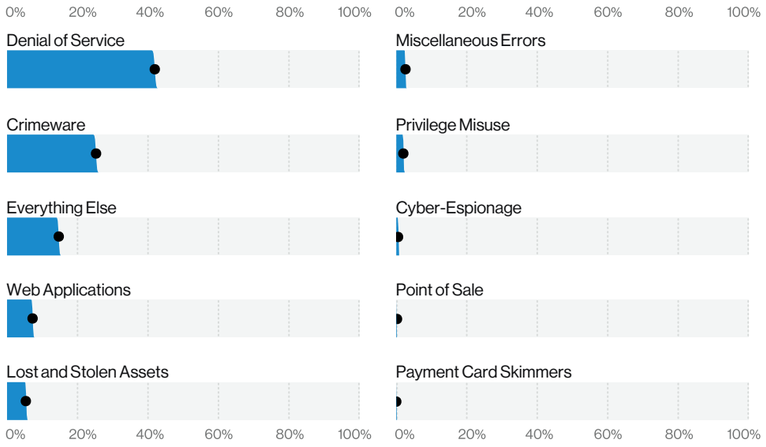


Figure 47. Patterns in incidents (n = 32,002)

38 We recommend taking a glance at the 2014 report if you are curious about the nerdy stuff.

Patterns

Crimeware

One of the oldest games in town, Crimeware includes all the malware that doesn't fall into the other patterns. Think of these as the common type of commodity malware that everyone has probably seen on some email claiming to be a fax or a missed delivery package. These incidents and breaches tend to be opportunistic and financially motivated.

Notable findings: This year has continued the trend of modest increases in incidents and breaches involving Crimeware, now up to about 300, which is higher than last year and roughly matches the highest levels that were reached in 2014. Unsurprisingly, these types of attacks normally propagate through email, either as a link or as an attachment, dropping something nasty like a downloader, password dumper, Trojan or something that's got C2 functionality. These types of attacks rely heavily on Social and Malware combined vectors, using Phishing in 81% of the incidents and some form of malware in 92%.

Denial of Service

These attacks are very voluminous (see what we did there) in our dataset at over 13,000 incidents this year. Attacks within this pattern use differing tactics, but most commonly involve sending junk network traffic to overwhelm systems, thereby causing their services to be denied. The system can't handle both the incoming illegitimate traffic and the legitimate traffic.

Notable findings: While the amount of this traffic is increasing as mentioned, in DDoS, we don't just look at the number of attacks that are conducted. We also look at the bits per second (BPS), which tells us the size of the attack, and the packets per second (PPS), which tells us the throughway of the attack. What we found is that, regardless of the service used to send the attacks, the packet-to-bit ratio stays within a relatively tight band and the PPS hasn't changed that much over time, sitting at 570 Mbps for the most common mode (Figure 48).

When it comes to defending against DDoS, a layered approach is best, with some of the attacks being mitigated at the network level by internet service providers and the others being handled at the endpoint or a content delivery network (CDN) provider. These attacks are prevalent because of their ease of use and the fact that internet-facing infrastructure can be targeted; however the impact to your organization and the decision of whether to mitigate will be based entirely on your business.

Cyber-Espionage

This pattern consists of espionage, enabled via unauthorized network or system access, and largely constitutes nation-states or state-affiliated actors looking for those oh-so-juicy secrets.

Notable findings: This is one of our patterns that has decreased this year, both in raw numbers and also as a percentage from 13.5% of breaches in 2018 to 3.2% of breaches in 2019. The drop in raw numbers could be due to either under-reporting or failure to detect these attacks, but the increase in volume of the other patterns is very much responsible for the reduction in percentage.

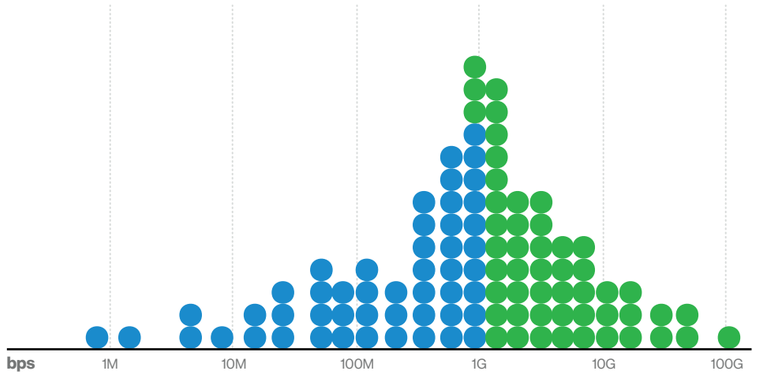


Figure 48. Most common distributed denial of service (DDoS) bits per second (BPS) (n = 195)

Privilege Misuse

This pattern consists of "Misuse" actions, which are intentional actions undertaken by internal employees that result in some form of security incident.

Notable findings: Misuse is down as a percentage of incidents, as the other patterns increase by association. However, that could be attributed to lower granularity data this year and may rise back to previous levels in 2021. On the other hand, breaches are showing a legitimate drop, which appears to be associated with less misuse of databases to access and compromise data.

Miscellaneous Errors

Life is full of accidents and not to disappoint Bob Ross, but not all of them are happy little trees. This pattern captures exactly that, the unintentional (as far as we know) events that result in a cybersecurity incident or data breach.

Notable findings: The majority of these errors are associated with either misconfigured storage or misdelivered emails, committed by either system admins or end users. We'll let you figure out which actor is associated with which action. In terms of discovery, these are often found by trawling security researchers and unrelated third parties who may have been on the receiving end of those stray emails. The Results and Analysis Error section goes into even more detail for those of you with this unique predilection.

Payment Card Skimmers

This pattern is pretty self-explanatory: These are the incidents in which a skimmer was used to collect payment data from a terminal, such as an ATM or a gas pump.

Notable findings: Our data has shown a continuous downward trend of incidents involving Point of Sale (PoS) Card Skimmers, which are now down to 0.7% of our incident data. At approximately 30 incidents, it is showing a relatively marked decline from its peak of 206 back in 2013. This decrease could be attributed to a variety of different causes, such as less reporting to our federal contributors or shifts in the attacker methodology.

Point of Sale (PoS)

This pattern includes the hacking and remote intrusions into PoS servers and PoS terminal environments for the purpose of stealing payment cards.

Notable findings: Much like the Payment Card Skimmers, this pattern has received a notable decrease in the last few years, making up only 0.8% of total data breaches this year. The majority of these incidents include the use of RAM scrapers, which allow the adversaries to scrape the payment cards directly from the memory of the servers and endpoints that run our payment systems. However, the majority of payment card crime has moved to online retail.

Lost and Stolen Assets

These incidents include any time where an asset and/or data might have mysteriously disappeared. Sometimes we will have confirmation of theft and other times it may be accidental.

Notable findings: This pattern tends to be relatively consistent over the years, with approximately 4% of breaches this year (the previous two years fluctuating from 3% to 6% of breaches). These types of incidents occur in various different locations, but primarily occur from personal vehicles and victim-owned areas. Don't forget to lock your doors.

Web Applications

Incidents in this pattern include anything that has a web application as the target. This includes attacks against the code of the actual web application, such as exploiting code-based vulnerabilities (Hacking–Exploit Vuln) to attacks against authentication, such as Hacking–Use of Stolen Creds.

Notable findings: In the data provided by contributors who monitor attacks against web applications (Figure 49), SQL injection vulnerabilities and PHP injection vulnerabilities are the most commonly exploited. This makes sense since these types of attacks provide a quick and easy way of turning an exposed system into a profit maker for the attacker. However, in vulnerability data, cross-site scripting (XSS), the infamous ding popup vulnerability, is the most commonly detected vulnerability and SQLi attacks are only half as common as XSS.

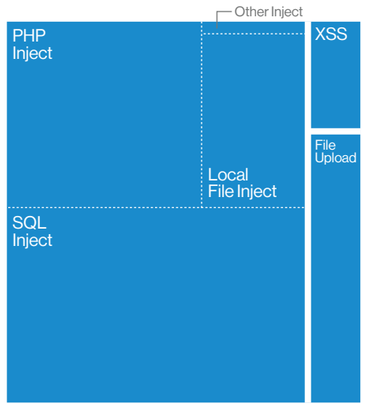


Figure 49. Web applications attack blocks (n = 5.5 billion)

Everything Else

This pattern is our graveyard of lost incident souls that don't fall into any of the previously mentioned patterns.

Notable findings: The majority of these incidents are Phishing or Financially Motivated Social Engineering where attackers try to commit fraud via email. Rather than go into detail here, we'll point you to the Results and Analysis–Social section, which goes into great detail on Financially Motivated Social Engineering and Phishing.

Subsets

In addition to the main nine Patterns, there is another level of patterns that we examine separately due to different factors that might skew our results and analysis, such as an extremely high volume of low-detailed incidents. This year, like the previous one, the subpatterns we examined separately are divided into the Botnet subset and Secondary motives.

Botnet subset

This subset consists of 103,699 incidents from various occurrences of Trojans and malware being installed on desktops and servers. The majority of these incidents tend to be low quality and limited in detail, coming from multiple incident sources.

Notable findings: In Figure 50, we see that botnets primarily affect the Financial, Information and Professional Services verticals. All these industries should focus on their customers' security as well as their own. The absolute numbers on this subset have more or less doubled from the previous year. Also, be mindful that these types of incidents impact everyone, with 41% of victims originating outside North America.

Secondary webapp subset

This subset examines those security incidents in which the victim web application was a means to an end for a different attack. This is often seen in the form of servers being compromised and used as part of a botnet or to DDoS other systems.

Notable findings: The Secondary subset represents a total of 5,831 incidents, with about 90% of them involving some form of hacking, malware and impacting servers. As we point out in the Actor section of Results and Analysis, if you give the bad guy the opportunity to add your infrastructure to theirs, they won't hesitate.

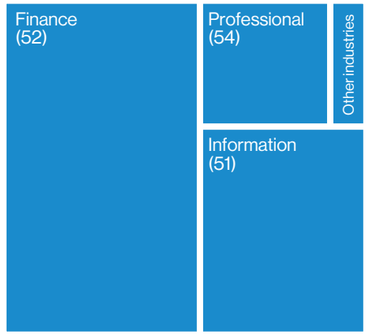


Figure 50. Botnet infections (n = 103,699)

03

Industry analysis

Introduction to industries

This year we collected 157,525 incidents and 108,069 breaches. That may sound impressive until you realize that 100,000+ of those breaches were credentials of individual users being compromised to target bank accounts, cloud services, etc. We break those out into the Secondary motive subset in the "Incident classification patterns and subsets" section. After filtering for quality and subsetting, we are left with the incidents and breaches in Table 1.

Our annual statement on what not to do with this breakout will now follow. Do not utilize this to judge one industry over another; a security staffer from an Administrative organization waving this in the face of their peer from the Financial sector and trash-talking is a big no-no. The number of breaches or incidents that we examine is heavily influenced by our contributors. These numbers simply serve to give you an idea of what we have to "work with," and is part of our pledge to the community to be transparent about the sourcing of the data we use in the report.

Figures 51 and 52 come with yet another warning. The numbers shown here are simply intended to help you to get your bearings with regard to industry. The smaller the numbers in a column, the less confidence we can provide in any statistic derived from that column.

Incidents:	Total	Small	Large	Unknown
Total	32,002	407	8,666	22,929
Accommodation (72)	125	7	11	107
Administrative (56)	27	6	15	6
Agriculture (11)	31	1	3	27
Construction (23)	37	1	16	20
Education (61)	819	23	92	704
Entertainment (71)	194	7	3	184
Finance (52)	1,509	45	50	1,414
Healthcare (62)	798	58	71	669
Information (51)	5,471	64	51	5,356
Management (55)	28	0	26	2
Manufacturing (31–33)	922	12	469	441
Mining (21)	46	1	7	38
Other Services (81)	107	8	1	98
Professional (54)	7,463	23	73	7,367
Public (92)	6,843	41	6,030	772
Real Estate (53)	37	5	4	28
Retail (44–45)	287	12	45	230
Trade (42)	25	2	9	14
Transportation (48–49)	112	3	16	93
Utilities (22)	148	5	15	128
Unknown	6,973	83	1,659	5,231
Total	32,002	407	8,666	22,929

Breaches:	Total	Small	Large	Unknown
Total	3,950	221	576	3,153
Accommodation (72)	92	6	7	79
Administrative (56)	20	6	10	4
Agriculture (11)	21	1	0	20
Construction (23)	25	1	10	14
Education (61)	228	15	22	191
Entertainment (71)	98	3	1	94
Finance (52)	448	32	28	388
Healthcare (62)	521	31	32	458
Information (51)	360	32	32	296
Management (55)	26	0	25	1
Manufacturing (31–33)	381	5	185	191
Mining (21)	17	0	5	12
Other Services (81)	66	6	1	59
Professional (54)	326	14	13	299
Public (92)	346	24	50	272
Real Estate (53)	33	3	3	27
Retail (44–45)	146	7	18	121
Trade (42)	15	1	6	8
Transportation (48–49)	67	3	6	58
Utilities (22)	26	2	4	20
Unknown	688	29	118	541
Total	3,950	221	576	3,153

Table 1. Number of security incidents by victim industry and organization size

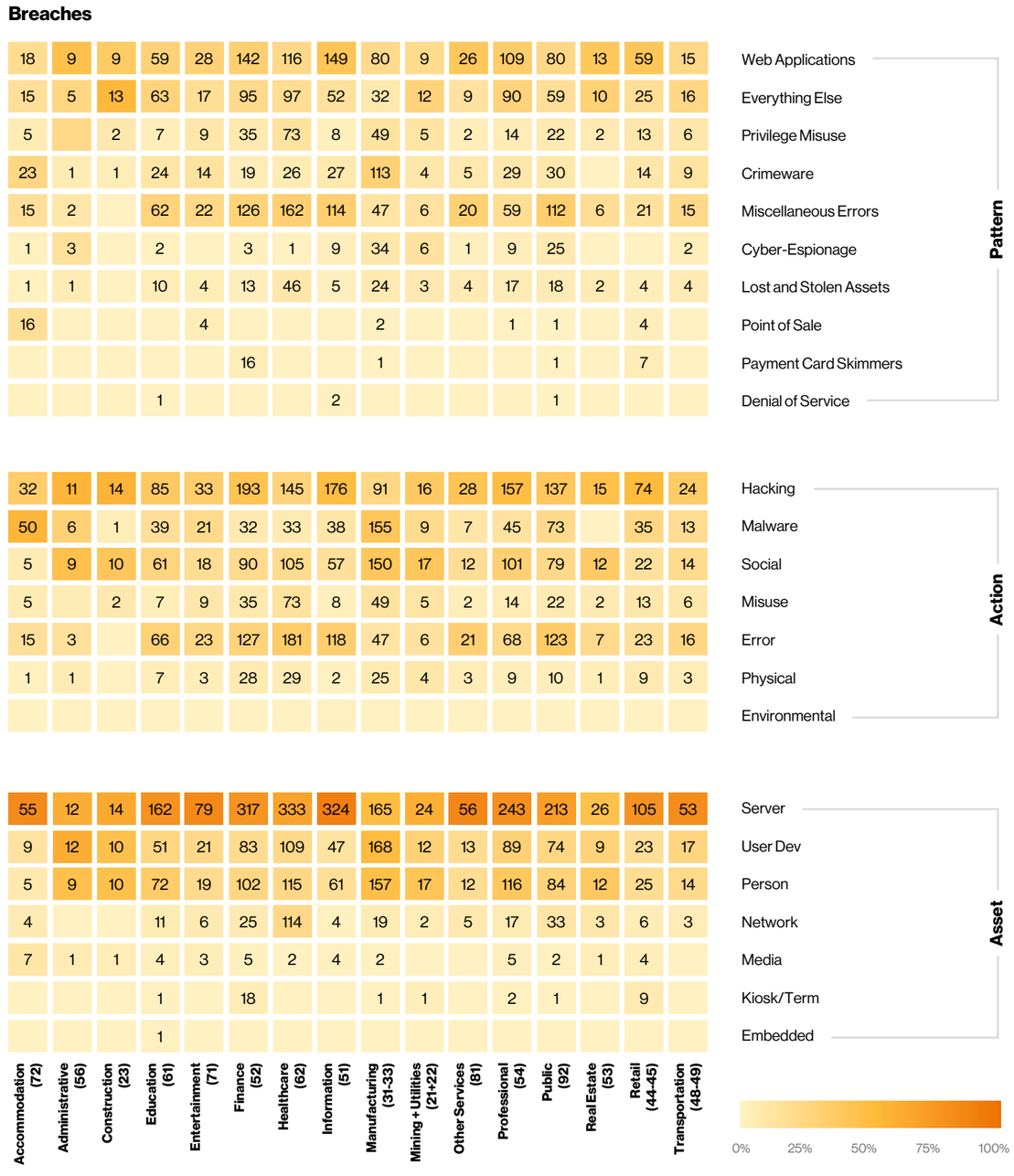


Figure 51. Breaches by Industry

Incidents

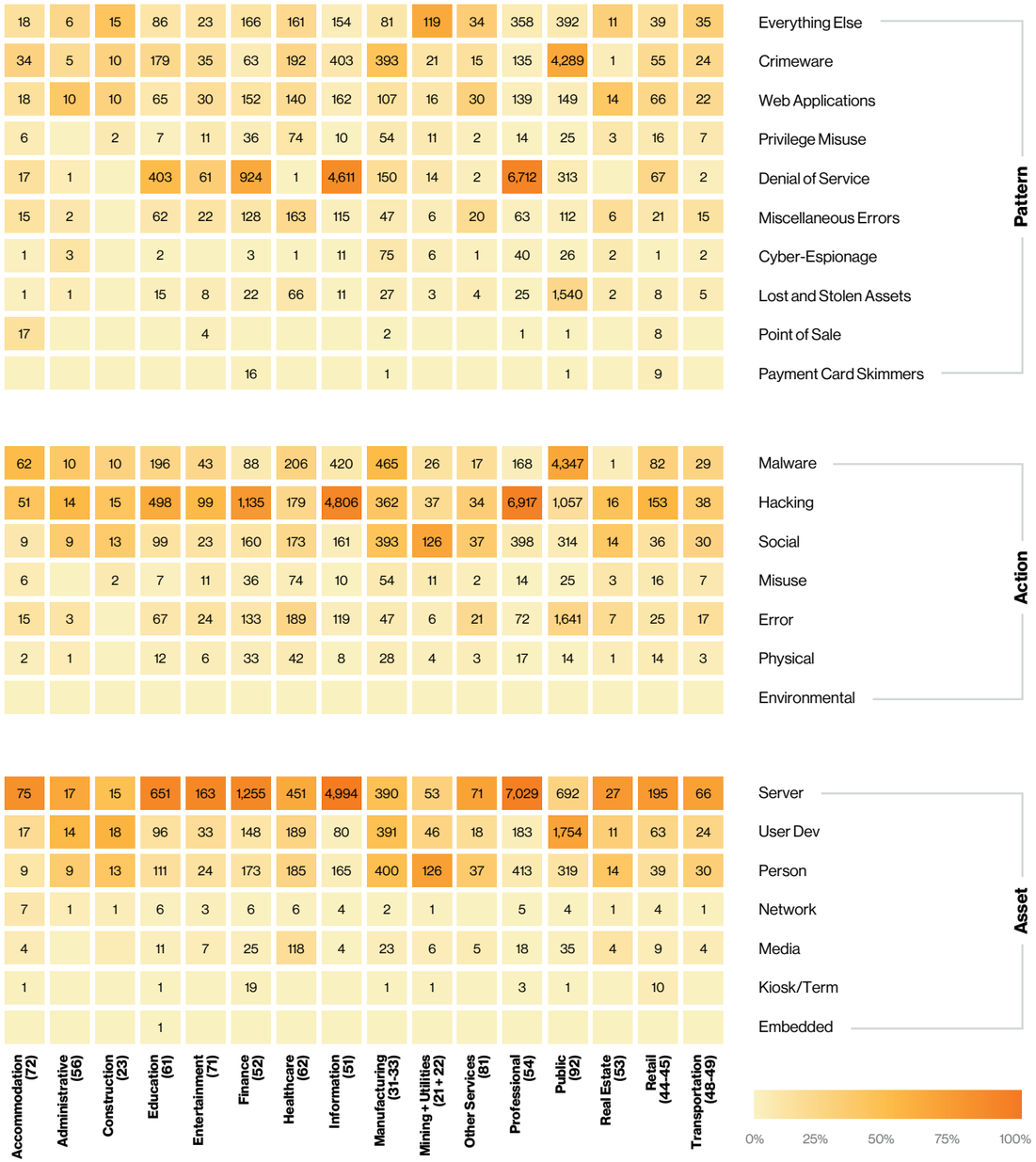


Figure 52. Incidents by Industry

For example, there are 35 total assets involved in Construction (NAICS 23) breaches. Of those, multiple assets may be contained in a single breach, meaning there are potentially fewer breaches (25) than our asset count. Considering how few breaches we have in this sector, our confidence in any statistic derived from them will be relatively low. However, in an attempt to bring our readers information on more industries, we have upped our statistical game. For example, instead of making a statement such as "64% of Construction breaches involved a server," we would state "between 44% and 82% of breaches in Construction involved servers." This is not an attempt to be coy,[39] we simply want to give you as much information as possible without being misleading and, in industries with such a small sample, that means using statistical ranges. You may notice something similar in bar charts where the black median dot is removed. Please keep an eye out for the "Data Analysis Notes" at the bottom of the Summary table in each section. We will be pointing out things such as small sample sizes and other caveats there. Check out the "Methodology" section for more information on the statistical confidence background used throughout this report.

Another improvement on this year's report is that we have standardized our control recommendations through a mapping between VERIS and the CIS Critical Security Controls. Each industry will have a "Top Controls" list on their Summary table. You can find more details about our mapping in our "CIS Control recommendations" section.

Please note: Based on feedback from our readers, we know that while some study the report from cover to cover, others only skip to the section or industry vertical that is of direct interest to them. Therefore, you may notice that we repeat some of our definitions and explanations several times throughout the report, since the reader who only looks at a given section won't know the definition or explanation that we might have already mentioned elsewhere. Please overlook this necessary (but possibly distracting) element.

39 Like a Gameboy.

Accommodation and Food Services

NAICS 72

Summary

Point of Sale (PoS)-related attacks no longer dominate breaches in Accommodation and Food Services as they have in years past. Instead, responsibility is spread relatively evenly among several different action types such as malware, error and hacking via stolen credentials. Financially motivated attackers continue to target this industry for the payment card data it holds.

Frequency	125 incidents, 92 with confirmed data disclosure
Top Patterns	Crimeware, Web Applications and Point of Sale represent 61% of data breaches.
Threat Actors	External (79%), Internal (22%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (98%), Secondary (2%) (breaches)
Data Compromised	Payment (68%), Personal (44%), Credentials (14%), Other (10%) (breaches)
Top Controls	Limitation and Control of Network Ports, Protocols and Services (CSC 9), Boundary Defense (CSC 12), Data Protection (CSC 13)

Breaches served with a smile

The Accommodation and Food Services industry is one that we have been tracking for quite a while. There's just something welcoming about it that keeps us coming back. One lesson that we learned from all our time spent here is that malware plays a relatively large role in this industry. Crimeware and PoS (both malware dependent) represent two of the top three patterns this year. These are joined by this year's darling of Web applications attacks, which covers both the Use of stolen credentials and the Exploitation of vulnerabilities, as seen in Figure 53.

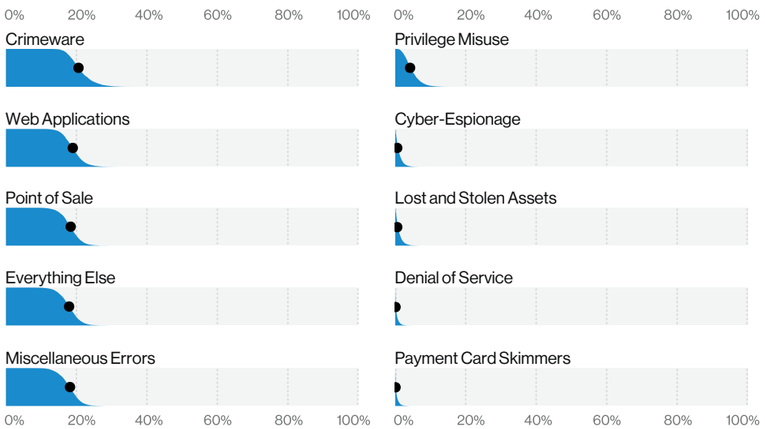


Figure 53. Patterns in Accommodation and Food Services industry breaches (n = 92)

86 the PoS breaches.

We reported last year on the decrease in different attacks targeting the PoS, either the malware-based remote attacks or the skimmers, and this trend has continued this year as well (Figure 54). Even though PoS intrusions are still relatively common, accounting for 16% of breaches in this industry, they are nowhere near their high-water mark back in 2015. This may be (and probably is) indicative of the trend of adversaries to more quickly monetize their access in organizations by deploying ransomware rather than pivoting through the environment and spreading malware—a more time-costly endeavor.

Do you want malware with that?

In spite of the decline in PoS intrusions, we're still seeing Crimeware being leveraged to capture payment card and other types of data at a higher rate than in our overall dataset, accounting for a quarter of the breaches this year. The malware is found on desktops and servers alike. With regard to type, Figure 55 shows a decrease of RAM scrapers and an increase of malware that enables access to the environment, such as Trojans, Backdoors and C2. There is also a continued rise in Ransomware, which has been known to leverage existing infections to access the environment. While Ransomware is not the top malware variety in breaches, or showing up in scans, it should be on your radar.

More than just dollar bills, y'all

This is an industry rich in payment data, and that makes for an easy dollar for bad guys. But Payment data isn't the only type of data being compromised. Instead, we also see Personal data being compromised, often as a byproduct of attacks, so be sure to pay proper attention to your security program outside of your payment card environment.

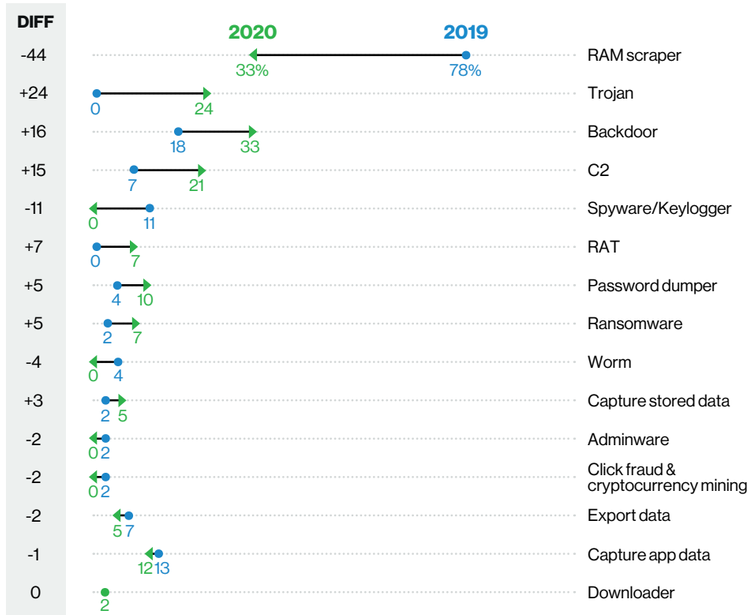


Figure 55. Top Malware over time in Accommodation and Food Services industry breaches; n = 45 (2019), n = 42 (2020)

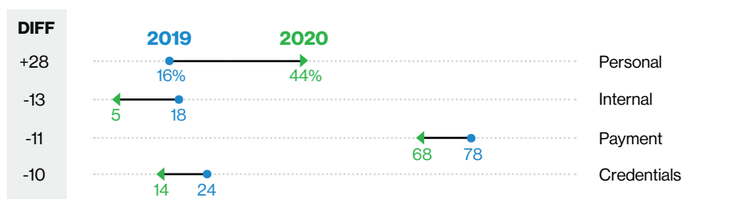
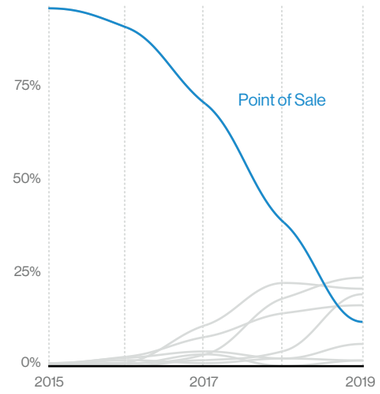


Figure 56. Top compromised data type over time in Accommodation and Food Services industry breaches; n = 51 (2019), n = 87 (2020)

Figure 54. Patterns over time in Accommodation and Food Services industry breaches



Arts, Entertainment and Recreation NAICS 71

Summary

Web applications attacks led to many breaches in this sector. Denial of Service attacks had higher bits-per-second volume in this industry than in the overall dataset. Social engineering attacks and errors also figure prominently in this vertical.

Frequency	194 incidents, 98 with confirmed data disclosure
Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 68% of data breaches.
Threat Actors	External (67%), Internal (33%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (94%), Convenience (6%) (breaches)
Data Compromised	Personal (84%), Medical (31%), Other (26%), Payment (25%) (breaches)
Top Controls	Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11), Implement a Security Awareness and Training Program (CSC 17)

Wake up in a good mood and start hacking.

While hackers were once described as being "like an artist," organizations in this industry that have been on the receiving end of some of these artistic endeavors might have a slightly different opinion. Although creativity and novelty are the hallmarks of this industry, the majority of the breaches in this sector may suffer from artistic criticisms such as "derivative" or "this has been done before" given that the top breach patterns are Web Applications, Miscellaneous Errors and Everything Else (Figure 57).

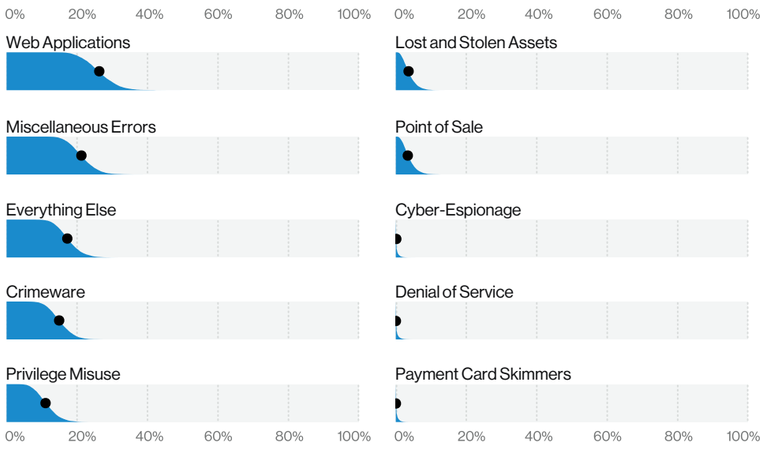


Figure 57. Patterns in Arts and Entertainment industry breaches (n = 98)

Fraudulent forgers fool frequently.

Much like how the authenticity of art can be difficult to establish, humans also struggle with determining the legitimacy of electronic communications. This accounts for the prevalence of the Everything Else pattern, where social engineering takes the wheel. In 2019, a Social action was found in approximately 18% of breaches. But to return to the topic of human nature, accidents and errors such as Misconfigurations and Misdeliveries remain a common issue for this sector. The growth in accidental breaches can been seen in Figure 58, where there has been a converging of Internal and External actors over the last few years. While this rise could be due to changes in breach reporting, it has remained consistent since 2016.

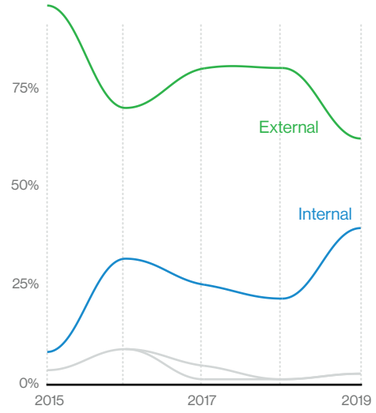


Figure 58. Actors over time in Arts and Entertainment industry breaches

Untitled Work II

Companies want to be able to maintain their data's integrity, and cybercriminals know that. This year, the top Malware varieties (Figure 59) included functionality, such as "Capture app data." This and the others listed allow bad actors to steal quietly into your systems and siphon your data while leaving worms to spread across your environment and ransomware to lock away your key data. These are either introduced on web servers via a vulnerability, or on desktops through the tried and true method of email phishing.

The DDoS-er

One very interesting result from our research this year was that this industry experienced the highest rate of DDoS attacks (Figure 60), beating out even the Information sector—our usual winner—by a wide margin. This NAICS code contains the online gambling industry as a member, and they are likely the ones driving this trend. Apparently, DDoSing your business rival is a thing in that realm. Who knew?

Figure 59. Top Malware variety changes over time in Arts and Entertainment industry incidents; n = 14 (2015), n = 35 (2020)

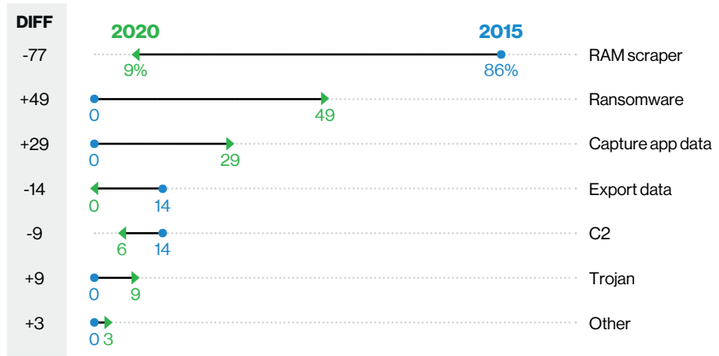
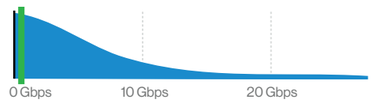


Figure 60. Most common BPS in Arts and Entertainment industry DDoS (n = 5 organizations); all industries mode (green line): 565 Mbps



Construction NAICS 23

Summary

This vertical suffers from Web App attacks and social engineering, and the use of stolen credentials remains a problem. However, it boasts a low submit rate for phishing and exhibits a surprisingly low number of employee errors.

Frequency	37 incidents, 25 with confirmed data disclosure
Top Patterns	Everything Else, Web Applications and Crimeware represent 95% of all incidents.
Threat Actors	External (95%), Internal (5%) (incidents)
Actor Motives	Financial (84%–100%), Grudge (0%–16%) (incidents)
Data Compromised	Personal and Credentials
Top Controls	Secure Configurations (CSC 5, CSC 11), Boundary Defense (CSC 12), Account Monitoring and Control (CSC 16)
Data Analysis Notes	Actor Motives are represented by percentage ranges, as only 10 breaches had a known motive. We are also unable to provide percentages for Data Compromised.

Rob the builder

Having delved a bit deeper into our data, we were able to build sections on several new industries this year, and Construction is among them. Although the Construction industry may not be the first thing that comes to mind when you think of data breaches, it is a critical industry that generates a great deal of economic growth and helps to sustain the nation's infrastructure. When viewed from that perspective, one question that may come to mind is, "What motivates the attacks in this industry?" Most cases were financially motivated and were typically carried out by organized criminal groups. The majority of these attacks were opportunistic in nature (75%), which means that the actors who perpetrated them had a very well-calibrated hammer they knew how to make work, and were just looking for some unprotected nails.

Since this is the first time we've all sat down together at the Construction industry table, we should take a moment to talk about the top attack patterns from the Summary table on the left. The Everything Else pattern is basically our bucket for attacks that do not fit within the other patterns. There are quite a bit of social engineering attacks in it, and they frequently come in the form of either a pretext attack (invented scenarios to support the attacker's hope that the victim will do what they are asking them to do) or general phishing, for the less industrious criminal who doesn't want to expend all that effort. Web Applications attacks are what they sound like: people hacking into websites to get to the data. Crimeware is your basic malware attack; ransomware falls in here and is increasingly popular. While a ransomware attack usually doesn't result in a data breach, threat actors have been moving toward taking a copy of the data before triggering the encryption, and then threatening a breach to try to pressure the victims into paying up.

How they do that voodoo they do

We mentioned social engineering as a common approach in this industry (and in the dataset as a whole). The bad guys use this approach simply because it works. Whether the adversary is trying to convince the victims to enter credentials into a web page, download some variety of malware or simply wire them some cash, a certain percentage of your employees will do just that (Figure 61). What is a proactive security person to do? We've talked about how important it is to know you're a target—and while the click rate shows that people in this industry fall for the bait slightly more often than the average Joe, it is important for them to report that they've been targeted. While the submission rate after clicking is quite low for the sector, so is the reporting rate. You can tell by all the stacked companies at 0% in the Figure 62 dot plot.

Figure 61. Median click rate in Construction industry phishing tests (n = 532); all industries median (green line): 3.6%

For the Web Applications attacks, the most common hacking variety was the use of stolen credentials. Sometimes these were obtained from a phishing attack, and sometimes they were just part of the debris field from other breaches. Employees reusing their credentials for multiple accounts (both professional and personal) increases risk for organizations when there are breaches and the stolen credentials are then used for credential stuffing. The key to reducing this risk is to ensure that the stolen credentials are worthless against your infrastructure by implementing multifactor authentication methods.

We love our employees.

One thing that really stood out when we looked at this sector was how low the Internal actor breaches were. Internal actor breaches come in two flavors: Misuse (malicious intent) and Error (accidental). This sector had very few breaches involving either, as shown in Figure 63.

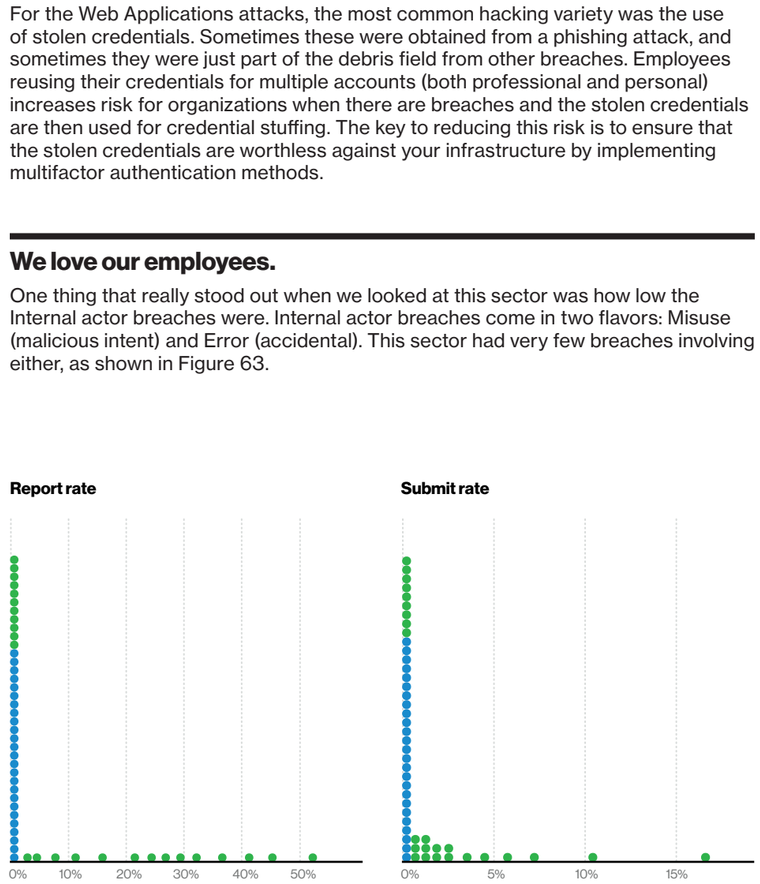


Figure 62. Median rates in Construction industry phishing tests (n = 532)

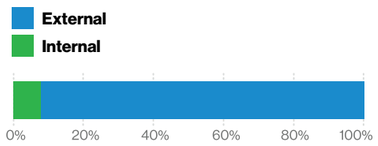


Figure 63. Actors in Construction industry breaches (n = 25)

Educational Services

NAICS 61

Summary

This industry saw phishing attacks in 28% of breaches and hacking via stolen credentials in 23% of breaches. In incident data, Ransomware accounts for approximately 80% of Malware infections in this vertical. Educational Services performed poorly in terms of reporting phishing attacks, thus losing critical response time for the victim organizations.

Frequency	819 incidents, 228 with confirmed data disclosure
Top Patterns	Everything Else, Miscellaneous Errors and Web Applications represent 81% of breaches.
Threat Actors	External (67%), Internal (33%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (92%), Fun (5%), Convenience (3%), Espionage (3%), Secondary (2%) (breaches)
Data Compromised	Personal (75%), Credentials (30%), Other (23%), Internal (13%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configuration (CSC 5, CSC 11)

An island of misfit breaches

You may be wondering, "What is this Everything Else pattern that is top of the class in this sector?" It sounds like the kitchen drawer where all the odds and ends wind up, and in a way, it is. If an attack doesn't meet the criteria of one of the other attack patterns, it ends up here, with that olive pit remover you got from your Secret Santa.

Phishing dominates the Everything Else pattern by a comfortable margin, not unlike many other industries. However, the Educational Services sector stands out by also getting a failing grade in phishing reporting practices. Of all industries, according to our contributor data, only 24% of organizations had any phishing reporting at all, and none of them had at least 50% of the emails reported in phishing awareness campaigns. It is exceedingly important to encourage your user base to let you know when your organization is being targeted. If they don't report it, you miss out on your early warning system.

Similarly, the prevalence of the Web Applications pattern is mostly because of the use of stolen creds on cloud email accounts. Although we cannot say this is the organizations' fault, according to our non-incident data analysis, Educational Services have the longest[40] number of days in a year—28—where they had credential dumps run against them. The global median here is eight days. The overall number of credentials attempted is also one of the highest of all industries we analyzed for this year's report (Figure 64).

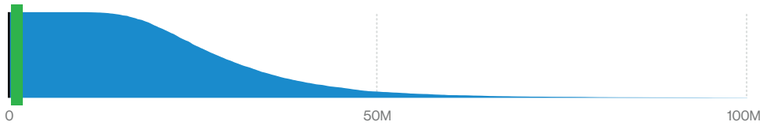


Figure 64. Credential stuffing attempts in Education industry web blocks (n = 8); all industries mode (green line): 1.11 M

40 Mode of industry

Outside of those two patterns, sadly, the news is still not great. Ransomware is really taking hold of Education vertical incidents, and has been responsible for 80% of the Malware-related incidents, up from 48% last year (Figure 65). All of those Ransomware cases have also played a role in the increase we have seen on financially motivated incidents for the past two years.

One additional concern in this sector is the fact that, according to our analysis, this is the only industry where malware distribution to victims was more common via websites than email. This information doesn't really seem to make sense until you consider malware being distributed via unmonitored email (such as personal mail accounts from students on bring-your-own devices connected to shared networks), and all of those infections obviously endanger the larger organization.

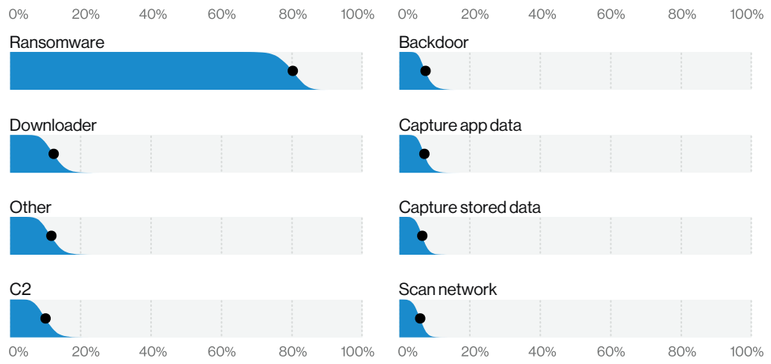


Figure 65. Top Malware varieties in Education industry incidents (n = 129)

Financial and Insurance

NAICS 52

Summary

The attacks in this sector are perpetrated by external actors who are financially motivated to get easily monetized data (63%), internal financially motivated actors (18%) and internal actors committing errors (9%). Web Applications attacks that leverage the Use of stolen credentials also continue to affect this industry. Internal-actor-caused breaches have shifted from malicious actions to benign errors, although both are still damaging.

Frequency	1,509 incidents, 448 with confirmed data disclosure
Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 81% of breaches.
Threat Actors	External (64%), Internal (35%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (91%), Espionage (3%), Grudge (3%) (breaches)
Data Compromised	Personal (77%), Other (35%), Credentials (35%), Bank (32%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11)

Why is everybody always picking on me?

The Financial and Insurance sector has always had a target on its back due to the kinds of data it collects from its customers. The data shows that the sector remains a favorite playground for the financially motivated organized criminal element again this year. Web Applications attacks are in competition with the Miscellaneous Errors pattern for the top cause of most breaches, as shown in Figure 66. It is a bit disturbing when you realize that your employees' mistakes account for roughly the same number of breaches as external parties who are actively attacking you. Apparently, it really is hard to get good help these days, and you can take that to the bank.

The Misuse action was among the top three causes of breaches for this vertical in last year's report, but it dropped from 21.7% in the 2019 report to only 8% this year. While this pattern saw a decline in our overall dataset, we are not of the opinion that all employees have suddenly become virtuous with regard to abusing their access. It is more likely that this is simply reflective of a change in contributor visibility rather than a sign of extreme moral rectitude in the workforce.

We switch our focus from malicious actions to those that were unintentional in Figure 67. The most common Error was Misdelivery, which is pretty much exactly what it sounds like: sending information to the wrong person. This can be with electronic data, such as an email sent to the incorrect recipient by an autofill in the "To:" field. Or it can be paper documents, such as a mass mailing that is incorrectly addressed. Both can result in a large breach, depending on what file(s) were attached to the email, or how large the mass mailing was.

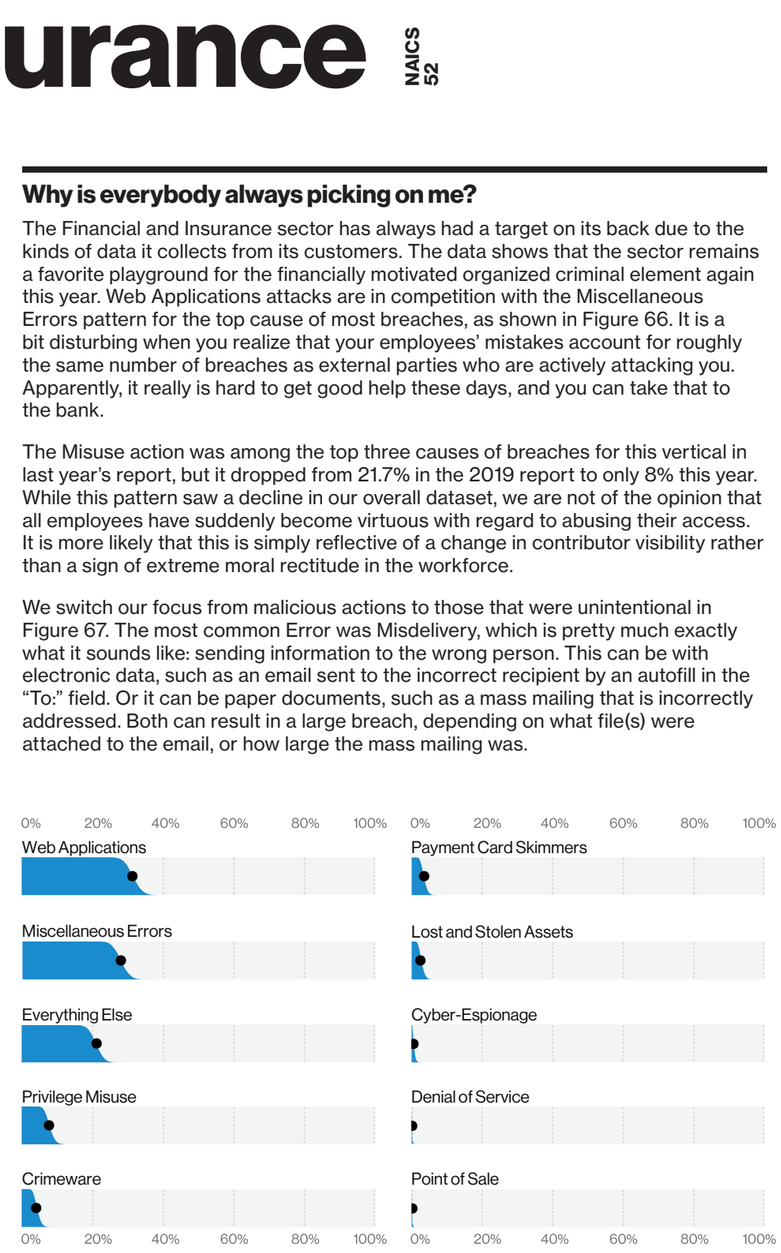
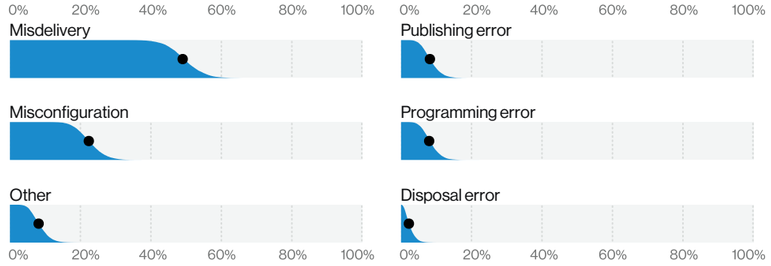


Figure 66. Patterns in Finance and Insurance industry breaches (n = 448)

Figure 67. Top Error varieties in Finance and Insurance industry breaches (n = 109)



The second most common Error is one that has been experiencing a surge in popularity—the Misconfiguration. This occurs when someone (often a system administrator) fails to secure a cloud storage bucket or misconfigures firewall settings. In the case of both Misdelivery and Misconfiguration, the motivation was overwhelmingly carelessness. Good security practices? Ain't nobody got time for that.

The wallflowers of the breach world

Like the shy creatures that line the walls of the middle school dance, those attacks that are shy in providing sufficient detail end up in the Everything Else pattern. Here languish the average, yet successful, phishing attacks, and the increasingly common business email compromise in its various forms. Among its many incarnations is the phishing email masquerading as coming from someone in the executive level of the company asking for something of monetary value.

Keep on playing those mind games together.

We also see invented scenarios (Pretexting) manufactured in order to plausibly convince the target to transfer money to the attacker's bank account. Figures 68 and 69 illustrate the popularity of these common social attacks. One key takeaway is that the weakest link in many organizations is their staff. Is it likely that the average user (who was targeted based on their access to data) will challenge a request that appears to be coming from someone who has the authority to fire them? Our ~~Magic 8-Ball~~ data indicates that signs point to no.

The majority of attacks in this sector are perpetrated by external actors who are financially motivated to access easily monetized data stored by the victim organizations. While there remains a small amount of Cyber-Espionage by nation-state actors in this industry, most attacks are perpetrated by someone who is all about the shekels.

#somefilter

As stated in past versions of this report, we utilize filters in our data analysis for a variety of things, including focusing on a given industry, threat actor type, etc. We also use them to exclude certain subsets of data in order to reduce skew and to help us find trends that might otherwise be missed. However, we do not ignore this data; we analyze it separately in other sections of this report. You can read more about it in our "Incident classification patterns and subsets" section. Specifically, for Finance, there were tens of thousands of incidents on the Botnet subset analyzed separately.

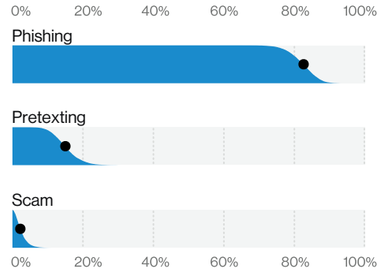


Figure 68. Social varieties in Finance and Insurance industry breaches (n = 86)

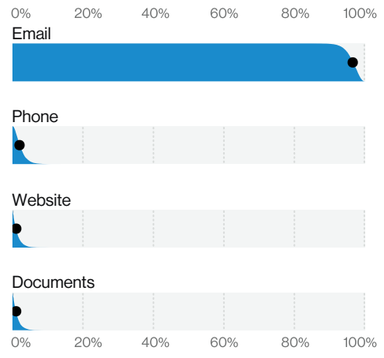


Figure 69. Social vectors in Finance and Insurance industry breaches (n = 86)

Healthcare NAICS 62

Summary

Financially motivated criminal groups continue to target this industry via ransomware attacks. Lost and stolen assets also remain a problem in our incident dataset. Basic human error is alive and well in this vertical. Misdelivery grabbed the top spot among Error action types, while internal Misuse has decreased.

Frequency	798 incidents, 521 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Web Applications and Everything Else represent 72% of breaches.
Threat Actors	External (51%), Internal (48%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (88%), Fun (4%), Convenience (3%) (breaches)
Data Compromised	Personal (77%), Medical (67%), Other (18%), Credentials (18%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Data Protection (CSC 13)

As contributors come and go, our dataset will change, and that change will be visible in both the types of attacks and the overall number of breaches we include in this report.

This year, we saw a substantial increase in the number of breaches and incidents reported in our overall dataset, and that rise is reflected within the Healthcare vertical. In fact, the number of confirmed data breaches in this sector came in at 521 versus the 304 in last year's report. Given that this is the *Data Breach Investigations Report*, we tend to put more focus on actual confirmed breaches. But in Healthcare, given the Department of Health and Human Services' (HHS) guidance on ransomware cases for example,[41] the incidents hold higher relevance than they might in a different vertical despite the data being simply "at-risk" rather than a confirmed compromise.

Figure 70 shows the breakdown of the patterns for incidents in Healthcare. The Crimeware pattern includes Ransomware incidents, and as one might expect, that pattern accounts for a large portion of the incidents in this sector. If we drop further down the list in this chart, we see that one pattern that tends to get lost in the shuffle is Lost and Stolen Assets. Because the asset is not available, proving whether the data was accessed or not is no simple matter. Therefore, we code these as incidents with data being "at-risk" rather than as a confirmed compromise. Our caution to the reader is not to assume that because the attacks aren't showing up as confirmed breaches in our dataset, you won't have to declare a breach according to the rules that govern your industry.

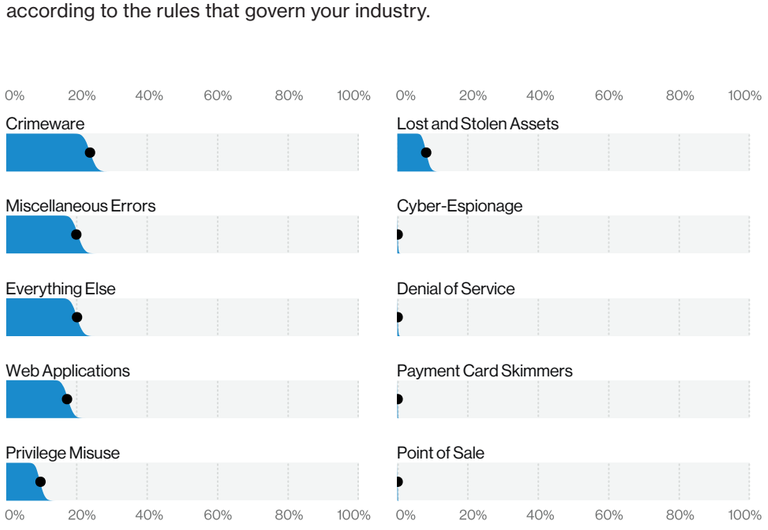


Figure 70. Patterns in Healthcare industry incidents (n = 798)

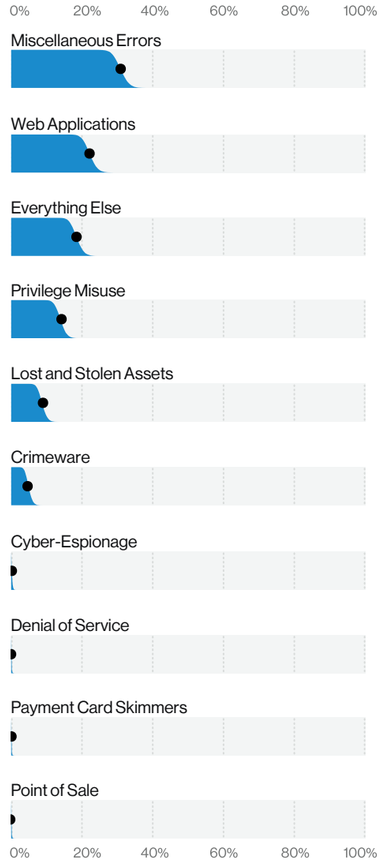


Figure 71. Patterns in Healthcare industry breaches (n = 521)

Take three patterns and call me in the morning.

If you've been following the "Healthcare" section for some time, you may notice a big change in the breach pattern rankings on Figure 71. This is the first year that the Privilege Misuse pattern is not in the top three. However, this pattern saw a significant proportional drop in our dataset overall—not just in the Healthcare vertical. In the 2019 report, we showed Privilege Misuse at 23% of attacks, while in 2020, it has dropped to just 8.7%. Does that indicate that insiders are no longer committing malicious actions with the access granted to them to accomplish their jobs? Well, we wouldn't go quite that far. However, it will be interesting to see if this continues as a trend when next year's data comes in.

Another change that goes along with decreased insider misuse breaches is the corresponding drop in multiple actor breaches. The Healthcare sector has typically been the leader in this type of breach—which usually occurs when External and Internal actors combine forces to abscond with data that is then used for financial fraud. The multiple actor breaches last year were at 4% and this year we see a drop to 1%. The 2019 DBIR reported a first in that the Healthcare vertical had Internal actor breaches (59%) exceeding those perpetrated by External actors (42%). This year, External actor breaches are slightly more common at 51%, while breaches perpetrated by Internal actors fall to 48%. However, this is a small percentage and Healthcare remains the industry with the highest amount of internal bad actors.

As with many things in life, as one attack grows more prevalent, others begin to decrease. So the story goes with the Miscellaneous Errors pattern. While it has frequently graced the top three patterns in this sector, it took the gold this year. In case you are curious, the top mistake within Healthcare is our old friend, Misdelivery.

This Error tends to fall into two major categories:

- Someone is sending an email and addresses it to the wrong (and frequently wider) distribution—it's an added bonus if a file containing sensitive data was attached
- An organization is sending out a mass mailing (paper documents) and the envelopes with the addresses become out of sync with the contents of the envelope. If sampling is not done periodically throughout the mailing process to ensure that they remain *NSYNC, then it's bye, bye, bye to your patients' sensitive information

41 "The presence of ransomware (or any malware) on a covered entity's or business associate's computer systems is a security incident under the HIPAA Security Rule." https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

When thinking of the Healthcare vertical, one naturally thinks of Medical data. And, unsurprisingly, this is the industry in which that type of data is the most commonly breached. However, we also see quite a lot of both Personal data (which can be anything from basic demographic information to other covered data elements) and Credentials stolen in these attacks. The second most common pattern for Healthcare is the Web Applications attack. As more and more organizations open patient portals and create new and innovative ways of interacting with their patients, they create additional lucrative attack surfaces.

Finally, we see a good deal of the Everything Else pattern, which is not unlike a lost and found for attacks that do not fit the criteria of any other attack pattern. It is within this pattern that the business email compromise resides. If you're not familiar with this attack, it is typically a phishing attack with the aim of leveraging a pretext (an invented scenario to give a reason for the victim to do what the attacker wants) to successfully transfer money (by wire transfer, gift cards or any other means). Although these are common attack types across the dataset, it is a good reminder to Healthcare organizations that it isn't only patient medical data that is being targeted.

When did you first notice these symptoms?

The time required to compromise and exfiltrate data has been getting smaller in our overall dataset. Unfortunately, the time required for an organization to notice that they have been breached is not keeping pace. There is a discrepancy there somewhat akin to how long it takes you to earn your wages vs how long it takes for them to be taxed. Some attacks, by their very nature, will both happen quickly and be detected quickly. A good example is a stolen laptop—how long does it take someone to smash a car window and make off with the loot? (That is a rhetorical question, so don't mail in answers, there is no prize for getting it right.) Likewise, it also doesn't take much time for the owner to come back to their car and see the break-in.

Both of these will have a short duration due to the nature of the crime. In contrast, an insider who has decided to abuse their access to copy a small amount of data each week and sell it to their buddy, who in turn utilizes it for financial fraud, may not be caught for a very long time.

Information NAICS 51

Summary

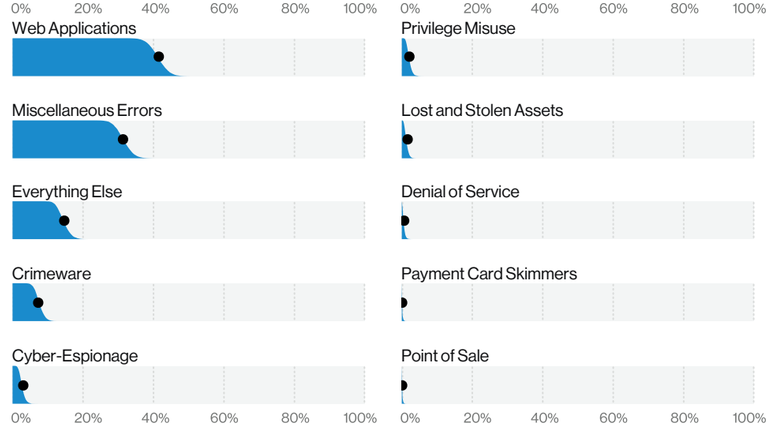
Web App attacks via vulnerability exploits and the Use of stolen credentials are prevalent in this industry. Errors continue to be a significant factor and are primarily made up of the Misconfiguration of cloud databases. Growth in Denial of Service attacks also remains a problem for the Information sector.

Frequency	5,741 incidents, 360 with confirmed data disclosure
Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 88% of data breaches.
Threat Actors	External (67%), Internal (34%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (88%), Espionage (7%), Fun (2%), Grudge (2%), Other (1%) (breaches)
Data Compromised	Personal (69%), Credentials (41%), Other (34%), Internal (16%) (breaches)
Top Controls	Secure Configurations (CSC 5, CSC 11), Continuous Vulnerability Management (CSC 3), Implement a Security Awareness and Training Program (CSC 17)

Come one, come all!

Welcome to the Information industry portion of the DBIR, and boy are you in for a treat! This section has it all: web applications attacks, errors, phishing and even some malware. The main three patterns witnessed in the NAICS 51 sector for 2019 were Web Applications with over 40% of breaches, followed by Miscellaneous Errors and, at a distant third, Everything Else (Figure 72).

Figure 72. Patterns in Information industry breaches (n = 360)



Since 2019, Web Applications attacks have increased significantly, both in terms of percentage of breaches and in raw number of incidents. This is one that organizations in this industry should keep an eye out for, as adversaries are dividing their effort equally between utilizing web exploits and stolen credentials to gain access to your web applications. Considering this vertical has a high dependence on external services and the internet, one shouldn't be too shocked to learn that this industry has a higher percentage of web application exploitations than other industries. However, based on our non-incident data, Information also has one of the highest percentages of vulnerability patching completed on time (Figure 73).

An anthem to errors

Errors are everywhere and the technical wizards that run our information infrastructure are not immune. This is why Errors are the second most common type of breach, maintaining relatively similar levels to previous years (this is not an area where consistency is a good thing). Misconfigurations are by far the most common type of errors, and largely relate to databases or file storages not being secured and directly exposed on a cloud service. These are the types of incidents that you hear security researchers discovering through simple trawling of the internet to see what's exposed. The optimist in us hopes that as these new technologies become more commonly used, people will stop (or at least slow down) making these types of mistakes. On the other hand, the realist in us wouldn't put any money on it.

You, sir, are a phish.

Technical issues are not the only thing impacting this technology-based sector. Organizations in this vertical have fallen prey to the same type of social engineering attacks that affect everyone else. Most of these attacks fall into our Everything Else pattern and account for 14% of the breaches we saw in 2019. In terms of social attacks, there is a relatively even split between phishing and pretexting (the bad guy just asks for information via email or uses some existing conversation in order to make a more convincing request). One of the common techniques we've seen is the use of typo-squatted domains of partners that are used to send existing email threads or request an update to a bank account.

Fast speeds and full bandwidths

Big interweb pipes are a key part of this industry since consumers demand that videos load fast and website content gets updated at the speed of an unladen European swallow. Unfortunately, cybercriminals know how important that is, and have been persistently targeting this industry with DoS attacks to disrupt their services and capabilities. The 2019 data showed continued growth in terms of the percentage of DDoS incidents (Figure 74). Not only does this industry get targeted more than a red barrel in a first-person shooter, they're also facing attacks with the second highest median BPS – meaning these attacks tend to pack a punch. Unfortunately for many companies, these attacks often need a helping hand to mitigate, so it helps to have a Player 2 in your corner.

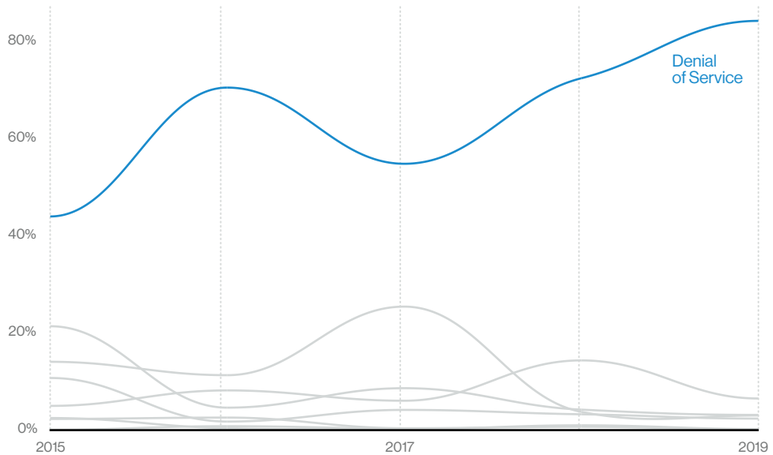
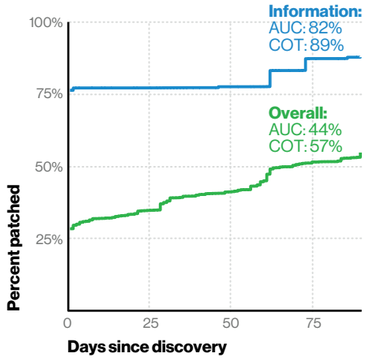


Figure 74. Patterns over time in Information industry incidents

Figure 73. Patching in Information industry vulnerabilities (n = 36,255)



Manufacturing NAICS 31–33

Summary

Manufacturing is beset by external actors using password dumper malware and stolen credentials to hack into systems and steal data. While the majority of attacks are financially motivated, there was a respectable showing of Cyber-Espionage-motivated attacks in this industry as well. Internal employees misusing their access to abscond with data also remains a concern for this vertical.

Frequency	922 incidents, 381 with confirmed data disclosure.
Top Patterns	Crimeware, Web Applications and Privilege Misuse represent 64% of breaches.
Threat Actors	External (75%), Internal (25%), Partner (1%) (breaches)
Actor Motives	Financial (73%), Espionage (27%) (breaches)
Data Compromised	Credentials (55%), Personal (49%), Other (25%), Payment (20%) (breaches)
Top Controls	Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17), Data Protection (CSC 13)

Bad actors, bad actions, bad puns

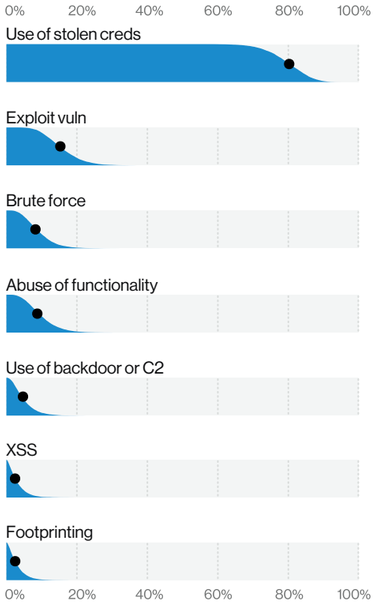
It has been said that the proper study of mankind is Man(ufacturing), or at least we are pretty sure that is how the adage goes. We hope so at least, because we have been giving a lot of thought to that topic. The Manufacturing vertical is very well represented this year with regard to both incidents and breaches. As always when we see a large increase, it could be indicative of a trend or simply a reflection of our caseload. In this instance, it is certainly the latter.

However, NAICS 31–33 has long been a much-coveted target of cybercrime and this year is no exception. Whether it is a nation-state trying to determine what its adversary is doing (and then replicate it) or just a member of a startup who wants to get a leg up on the competition, there is a great deal of valuable data for attackers to steal in this industry. And steal it they do. The predominant means they employ for this theft falls under the Crimeware pattern, as shown in Figure 75. Namely, the Password dumper, Capture app data and Downloader varieties.

This combination of obtain password, infiltrate network, download software and then capture data paints a very clear picture of what's going on in this vertical, but it may not be a picture you want hanging on your wall if you do business in this area. But while we are on the topic of malware in general, keep in mind that ransomware (while not considered a breach in this report) is still a very present danger for this industry at 23% of all malware found in incidents.

Figure 75. Patterns in Manufacturing industry breaches (n = 381)

Figure 76. Hacking varieties in Manufacturing industry breaches (n = 44)

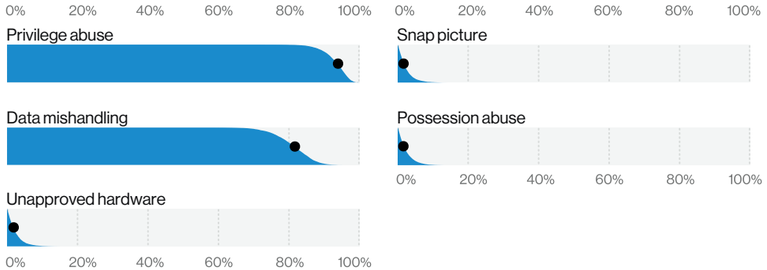


Web Applications attacks took the number-two place this year and are dominated by the Use of the stolen credentials to compromise a variety of web apps used in enterprises. Sometimes these credentials are obtained via malicious links served up in successful phishing attacks, sometimes they are obtained via desktop sharing and sometimes it is unclear how the victim is infected. Regardless of how they are compromised, these credentials, often of the cloud-based email variety, are very successful as a means to an end in this vertical, as you can see in Figure 76.

There are several patterns that are closely grouped around the third-place position for Manufacturing: Misuse (13%), which by definition involves insiders, and is mostly Privilege abuse—the actor has legitimate access but they use those privileges to do something nefarious—and Data mishandling, of which prime examples are sending company data via personal email or placing it on cloud drives in order to work from home (Figure 77).

Error is ubiquitous in all of the verticals this year, and in Manufacturing it is in keeping with the trend of Misdelivery and Misconfiguration that we see in other industries. Finally, we would be remiss to not say a word or two regarding cyber-espionage-related attacks.

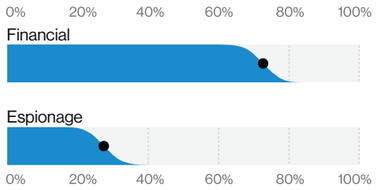
Figure 77. Misuse varieties in Manufacturing industry breaches (n = 49)



As a glance at Figures 78 and 79 reveals, 38% of actors were of the Nation-state variety, and 28% of breaches were motivated by Espionage. As we have mentioned in previous reports, it is cheaper and simpler to steal something than to design it yourself. And while large organizations are often willing to outsource their help-desk functions, they are, as a rule, not as eager to ship off their intellectual property and research-and-design generation to foreign locales.

Figure 78. External actor varieties in Manufacturing industry breaches (n = 83)

Figure 79. External actor motives in Manufacturing industry breaches (n = 121)



Mining, Quarrying, and Oil & Gas Extraction + Utilities

NAICS 21+22

Summary

Breaches are composed of a variety of actions, but Social attacks such as Phishing and Pretexting dominate incident data (no confirmation of data disclosure). Cyber-Espionage-motivated attacks and incidents involving OT assets are also concerns for these industries.

Frequency	194 incidents, 43 with confirmed data disclosure
Top Patterns	Everything Else, Web Applications and Cyber-Espionage represent 74% of breaches.
Threat Actors	External (75%), Internal (28%), Multiple (2%) (breaches)
Actor Motives	Financial (63%–95%), Espionage (8%–43%), Convenience/Other/Secondary (0%–17% each), Fear/Fun/Grudge/Ideology (0%–9% each) (breaches)
Data Compromised	Credentials (41%), Personal (41%), Other (35%), Internal (19%) (breaches)
Top Controls	Secure Configurations (CSC 5, CSC 11), Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17)
Data Analysis Notes	Actor motives are represented by percentage ranges, as only 21 breaches had a known motive.

It's an NAICS mashup!

This new section combines the Mining, Quarrying, and Oil and Gas Extraction (NAICS 21) with the Utilities (NAICS 22) industries for a joint view of the incidents and breaches that affected them. We really dug deep, but we were unable to strike oil for an exclusive section for NAICS 21 on this year's report. (There must be a minimum number of incidents for the statistics to be valid.) However, we believe that this blended section with NAICS 22 will be an electrifying read and hopefully not too dry.

If you review Figure 80, you can see that while Everything Else, Web Applications and Cyber-Espionage seem to be the top three patterns in breaches, it is statistically impossible to tell which one is more prevalent—they simply overlap too much. It's exciting to have such a diversity of breaches in a brand-new industry section, but it also makes it difficult to focus on precise recommendations beyond "Note to all CISOs: Secure all the things!"

Even so, it is important to point out that the Everything Else pattern, both in incidents and breaches, is dominated by Phishing with mostly financial gain as a motive, including pretexting attacks that were clearly FMSEs.

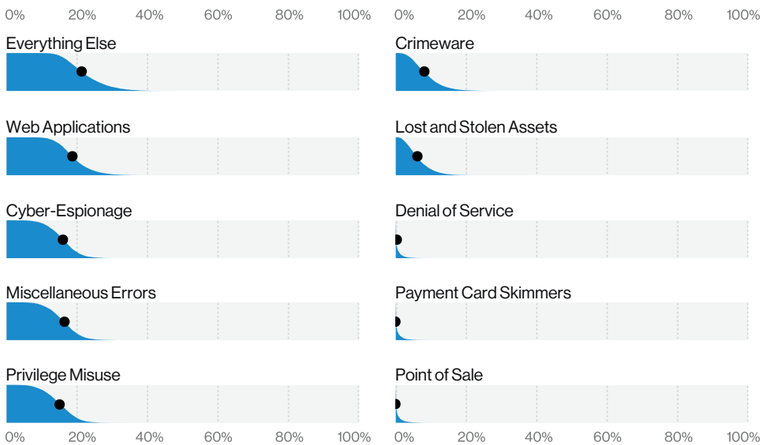


Figure 80. Patterns in Mining and Utilities industry breaches (n = 43)

If I closed my eyes, was it still a breach?

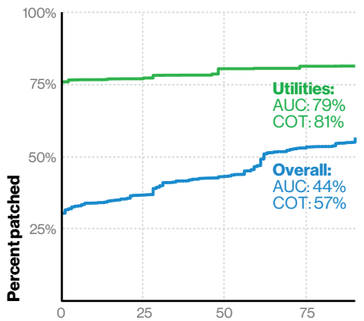
Since the Everything Else pattern is the largest for incidents (cases in which there was potential data disclosure but it was not confirmed), special attention is needed here. There were about as many incidents with potential data disclosure as there were confirmed breaches in these industries. This is especially concerning for a vertical with a broad range of possible percentages for Espionage-motivated breaches (between 8% and 43%), while in all incidents it accounts for 10% of the motives.

Wrapping up the top patterns, Web Applications is filled with the Use of stolen creds that were gathered by Phishing. Meanwhile, Miscellaneous Errors favors Misconfiguration and Publishing Errors, both action varieties that can be mitigated with stronger processes and personnel training.

Unpatched vulnerabilities in your web application infrastructure may lead to them being found by someone with a set of tools to exploit them in an automated fashion. Keeping your infrastructure patches up to date is certainly a security best practice. In looking at our non-incident data surrounding time to patch (Figure 81), we found the Utilities sector had a better-than-average score. This is good news because our research has found that the patches that do not get applied within the first quarter of being released frequently don't get applied at all. This gives the adversaries time to build tools that will make it easy even for a novice to attack the infrastructure that remains vulnerable.

Also, as these industries have become a focus of our reporting, we have added OT-specific fields to track incidents involving OT equipment in the latest version of VERIS. The total number of cases we have for this year are few, but they are mainly concerned with this sector along with Manufacturing (NAICS 31–33).

Figure 81. Patching in Mining and Utilities industry vulnerabilities (n = 151,658)



Other Services NAICS 81

Summary

Financial gain is the highest motive for External actors, with Web Applications being 39% of breaches. Error among employees is another issue for this sector, particularly with regard to Misconfiguration and Misdelivery. While Credentials are a desirable target, it is Personal data that is most frequently stolen here.

Frequency	107 incidents, 66 with confirmed data disclosure
Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 83% of breaches.
Threat Actors	External (68%), Internal (33%), Multiple (2%) (breaches)
Actor Motives	Financial (60%–98%), Espionage (0%–28%), Convenience/Fear/Fun/Grudge/Other/Secondary (0%–15% each) (breaches)
Data Compromised	Personal (81%), Other (42%), Credentials (36%), Internal (25%) (breaches)
Top Controls	Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17), Secure Configurations (CSC 5, CSC 11)
Data Analysis Notes	Actor Motives are represented by percentage ranges, as only 12 breaches had a known motive. Some charts also do not have enough observations to have their expected value shown.

Break on through to the other side.

The Other Services (NAICS 81) industry is also new to the report this year. This NAICS code is one of several that are surprisingly broad, covering everything from various personal and repair services to non-profit religious and social benefit organizations. Oddly enough, it even includes a subcode (814) for private households, but those are not represented in this dataset. For an incident to be eligible for inclusion in the DBIR, there must be a victim organization, since that is where the laws focus, and where the controls are most likely to have good effect. As we have mentioned in the other new sections, while this is the first year we are including this industry in the report, we have data going back a few years on this sector.

Jockeying for that top spot

The top breach patterns in this industry were Web Applications attacks, Miscellaneous Errors and Everything Else. When looking at the incident patterns (not confirmed data breaches), the patterns remain the same, albeit in a different order.

The main change from last year's data for this vertical is the drop in the Cyber-Espionage pattern. Last year it held the first place slot in the footrace, and you can see from Figure 82 that is has since told the other patterns "go on ahead, I'll catch up" as it struggles to catch its breath. Consistent with this change, we've seen the variety and motivation of the External actor breaches transform from State-affiliated/Espionage into Organized crime/Financial. It seems the people who like to go after data for the sheer joy of monetizing it have found a friend in this sector.

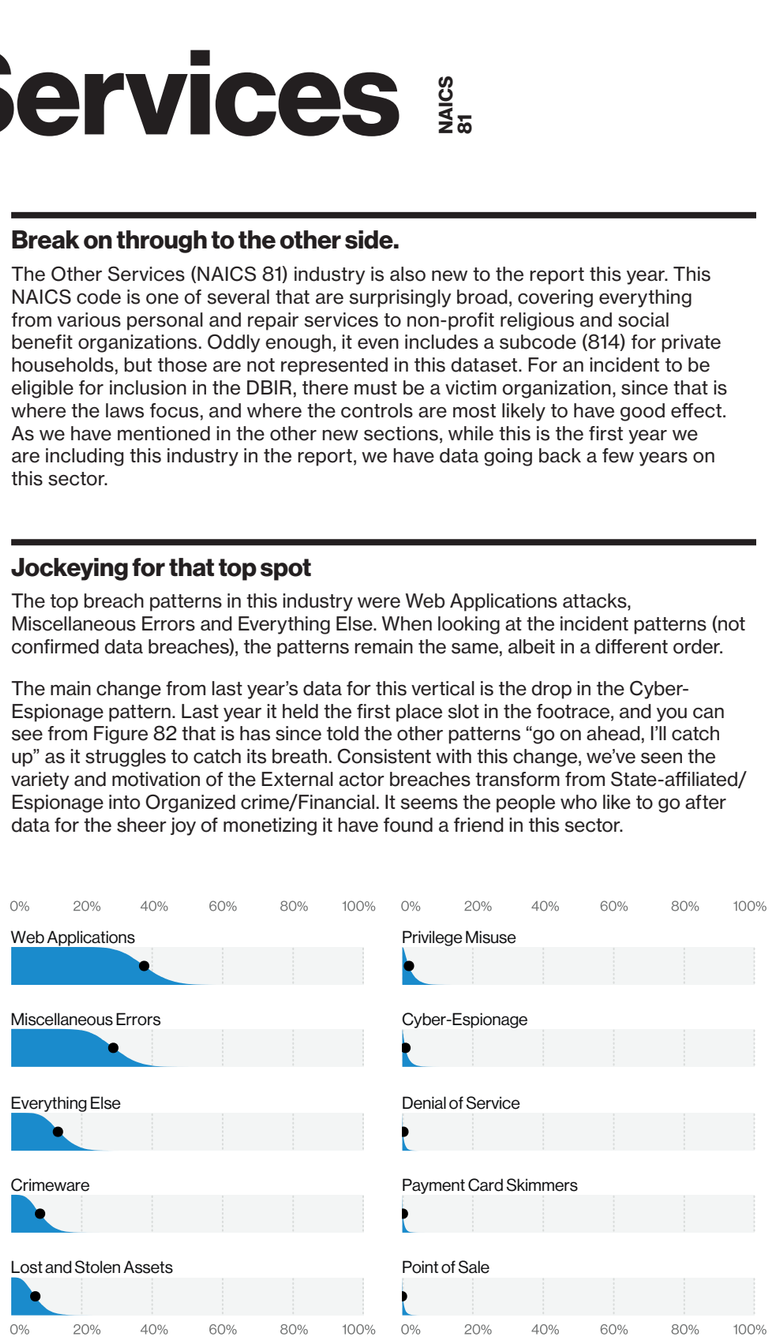


Figure 82. Patterns in Other Services industry breaches (n = 66)

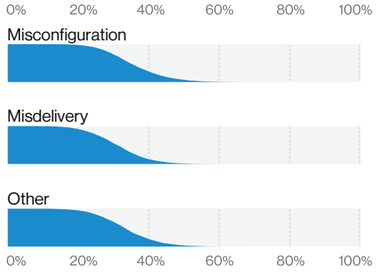


Figure 83. Top Error varieties in Other Services industry breaches (n = 21)

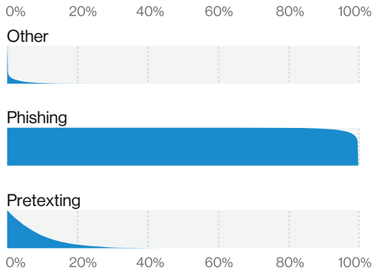


Figure 84. Top Social varieties in Other Services industry breaches (n = 12)

The Web Applications attack pattern includes the Hacking actions, and the favored action variety tends to be the Use of stolen credentials. It makes sense—who wouldn't like credentials when trying to break into some else's computer? What burglar would say no to a set of free keys? And while the use of a backdoor or Command and Control (C2) infrastructure is always nice, if you can just waltz in the front door, why exert yourself? Do you enjoy being asked questions?

What can go wrong will happen to me.

The Miscellaneous Errors pattern is all about the mistakes your employees make. Two stand out from the rest in the field of errors for Other Services: Misconfiguration and Misdelivery (Figure 83). Misconfiguration errors are the frenemies of Information Security. These breaches are caused by Internal actors (frequently a system admin or DBA, as they have access to large amounts of data) doing things such as standing up an instance of the data on a cloud platform, but neglecting to put in any security controls to limit access. Once that happens, it is a matter of time before the intrepid security researchers out there find it via their search tools and someone gets a call.

Misdelivery—when sensitive data goes to the wrong recipient(s)—is the other most common Error in this sector. A good example is when the autocomplete in an email "To:" or "Cc:" field occurs and directs to the incorrect party. In other instances, it is the mass-mailing misstep where the addresses are no longer paired with the correct contents. It is never good to have your customer open a letter only to find someone else's Personally Identifiable Information (PII) inside.

Finally, we have the Everything Else pattern, which is our version of potpourri. This is where the attacks that do not meet the criteria of the other patterns end up. Not exactly the fragrant flowers of the security breach world, these attacks are frequently made up of phishing attacks in which not a great deal of detail was provided.

The business email compromises also live within this pattern. They typically come in two main flavors: the pretext and the C-level impersonation. For the pretext, there is an invented scenario and usually an attempt to get either an invoice paid or a direct wire transfer to an adversary-controlled bank account. They may compromise the mail account of the executive and wait until the person is traveling to elevate the sense of urgency, and to minimize the ability to contact the person in order to verify the legitimacy of the request. The latter type is when the actor pretends to be a member of the executive suite, but they ask for data rather than a wire transfer. Figure 84 illustrates that phishing and pretexting are still thriving in this vertical. Both of these social engineering actions typically arrive via email.

Professional, Scientific and Technical Services

NAICS 54

Summary

Financially motivated attackers continue to steal credentials and leverage them against web application infrastructure. Social engineering in the form of Phishing and Pretexting is a common tactic used to gain access. This industry also suffers from Denial of Service attacks regularly.

Frequency	7,463 incidents, 326 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 79% of breaches.
Threat Actors	External (75%), Internal (22%), Partner (3%), Multiple (1%) (breaches)
Actor Motives	Financial (93%), Espionage (8%), Ideology (1%) (breaches)
Data Compromised	Personal (75%), Credentials (45%), Other (32%), Internal (27%) (breaches)
Top Controls	Secure Configuration (CSC 5, CSC 11), Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12)

This industry is made up of a wide range of companies primarily offering service directly to customers. They range from lawyers, accountants and architects to research labs and consulting firms. They share some common traits: Their internet presence is very important to the livelihood of the organization, and their employees are human and make mistakes.

We mentioned the importance of their internet presence to the members of this industry. This is why the Web Applications attack pattern was seen so frequently this year (Figure 85). These attacks are driven by the use of stolen credentials (frequently obtained in phishing attacks, but also may be laying around on the web from another company's breach, just waiting for some enterprising hacker to find). These attacks drive the theft of personal data in the sector, and given that there are always people willing to try their luck at using stolen credentials against whatever web infrastructure they encounter, are unlikely to end anytime in the near future.

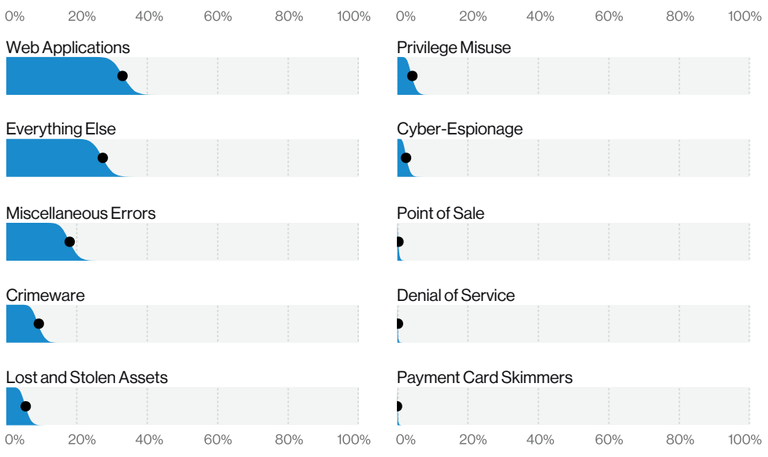


Figure 85. Patterns in Professional Services industry breaches (n = 326)

I feel attacked.

Why would organizations in this sector be targets of attacks? You have heard the expression "Location, location, location"? This sector is the location of lots of useful personal data (in fact, apart from Credentials, Personal information is the most targeted data type in these breaches). This isn't necessarily an industry full of financial information or payment card records, but personal information can be quite lucrative for a number of different kinds of financial fraud, hence the attraction. Figure 86 shows the continued growth of Financially motivated breaches at the expense of Espionage (and even Errors).

The Everything Else pattern is our scrap bin of unwanted attacks—if they do not fit the criteria of the other patterns, they end up here. They are largely low-detail phishing attacks, but sometimes the social engineering perpetrator puts a bit of actual effort into their work and invents a likely scenario to entice their prey. If you're familiar with the business email compromise, this is where that lives. Professional Services is middle of the road when it comes to being on the receiving end of phishing attacks. But this attack isn't just about receiving the attack—it is about whether the victim clicks, and if they submit their data. It is also about whether they raise a flag with their internal security people to let them know "what they done did."

The news about phishing in this sector is a bit of a mixed bag. In Figure 87, we see that click rate is right on the overall median. You can also see in Figure 88 that submit rates are low (notice the large stack of companies on the 0% of the right chart—Submit rate), which is the good news—you want the number of people giving out their credentials to be low. Sadly, the bad news is that the reporting rate is low as well (there is also a large stack of companies on the 0% of Report rate), meaning that your people are not telling you they've fallen victim to a phish. That second measure—the Report rate—is critical so that the organization's security response team can mitigate the effects of the breach.

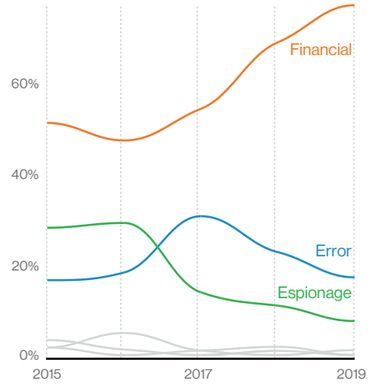


Figure 86. Motives over time in Professional Services industry breaches

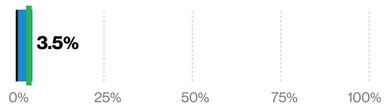


Figure 87. Median click rate in Professional Services industry phishing tests; all industries median (green line): 3.6%

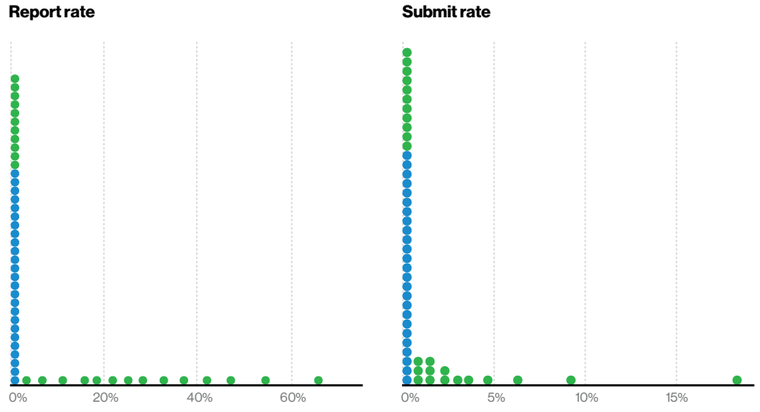


Figure 88. Median rates in Professional Services industry phishing tests (n = 2,583)

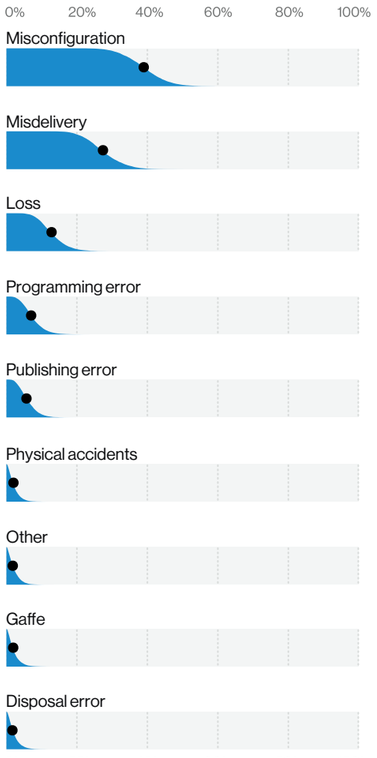


Figure 89. Error varieties in Professional Services industry breaches (n = 67)

I should not have done that.

Miscellaneous Errors figure prominently in this industry, but really any industry is susceptible to their employees' mishaps causing a breach. Figure 89 shows the errors that are on top in this industry—namely Misconfiguration, Misdelivery and Loss. Misconfiguration has become increasingly reported, primarily because there are people out there actively looking for this type of breach. This happens when someone drops some of their data into a cloud database instance but fails to put any protective measures in place. We mentioned people are actively searching for this, right? Yeah, then hilarity ensues—not really.

Misdelivery is frequently via paper documents in the mail, when person A gets person B's paperwork, but it can also happen via email when people are careless about addressing emails and what they attach. Loss is a bit of a different animal. When the item lost is electronic, like a laptop, this would not be counted as a breach in our dataset. For it to be counted, there must be a confirmed compromise of the confidentiality aspect of the data—and confirming access is difficult when you don't have the asset anymore. While the Loss error appears in our dataset, it is most frequently an incident, not a breach. However, here it is a breach, so what gives? Well, it would have to be an asset that is in human-readable format, like paper documents. We count them as a breach since there are no protections at all on printed matter. This is why people put caution signs on printers to give people an extra heads-up that, once printed, documents need to be treated carefully if they contain sensitive information.

Final deliverables

Left out of the breach patterns is Denial of Service, since it also does not typically result in an actual confidentiality breach. DDoS was over 90% of incidents in Professional Services and Figure 90 shows us that this sector has slightly above average DDoS bits per second.

To wrap up with some good news, Figure 91 shows that Professional Services has a better-than-average patch rate, completing 67% of patches in the first quarter from those being first made available from the manufacturer. If you've read the Results and Analysis—Action—Hacking section, you know that it's not the slow patching that's the problem; it's the systems in the remaining third that never get patched that are likely to come back to haunt you.

Figure 90. Most common BPS in Professional Services industry DDoS (n = 30 organizations); all industries mode (green line): 565 Mbps

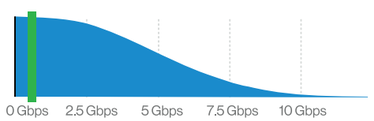
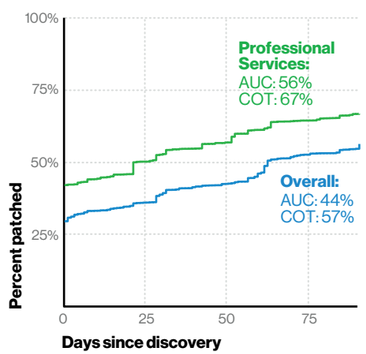


Figure 91. Patching in Professional Services industry vulnerabilities (n = 87,857)



Public Administration NAICS 92

Summary

Ransomware is a large problem for this sector, with financially motivated attackers utilizing it to target a wide array of government entities. Misdelivery and Misconfiguration errors also persist in this sector.

Frequency	6,843 incidents, 346 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Web Applications and Everything Else represent 73% of breaches.
Threat Actors	External (59%), Internal (43%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (75%), Espionage (19%), Fun (3%) (breaches)
Data Compromised	Personal (51%), Other (34%), Credentials (33%), Internal (14%) (breaches)
Top Controls	Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11)

I can see clearly now.

The "Public Administration" section is an illustration of what good partner visibility into an industry looks like. The bulk of our data in this vertical comes from partners inside the United States federal government who have a finger on the pulse of data breaches inside Public Administration. As we have stated elsewhere in this report, in order to meet the threshold for our definition of a data breach, the compromise of the confidentiality aspect of data must be confirmed. However, reporting requirements for government are such that run-of-the-mill malware infections or simple policy violations still must be disclosed. Therefore, we see an inordinately large number of incidents and a correspondingly small number of breaches.

When we look at the difference in the attack patterns in this sector, for example, the top three for breaches are Miscellaneous Errors, Web Applications attacks and Everything Else. When we look at the same data for incidents, the top three patterns are Crimeware (malware attacks), Lost and Stolen Assets, and Everything Else.

With regard to malware in the incident dataset, Figure 92 indicates that Ransomware is by far the most common, with 61% of the malware cases. This malware is most commonly downloaded by other malware, or directly installed by the actor after system access has been gained. However, ransomware isn't typically an attack that results in a confidentiality breach. Rather, it is an integrity breach due to installation of the software, and an availability breach once the victim's system is encrypted. Thus, these attacks do not typically appear when we discuss data breaches.

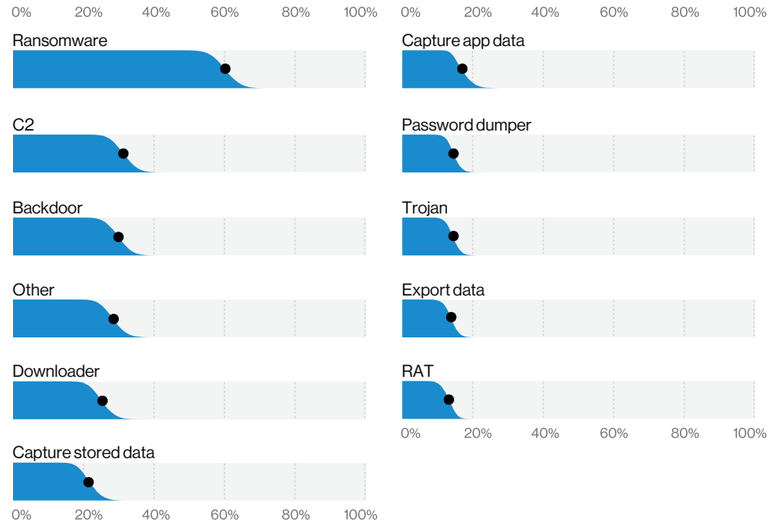


Figure 92. Top Malware varieties in Public Administration incidents (n = 198)

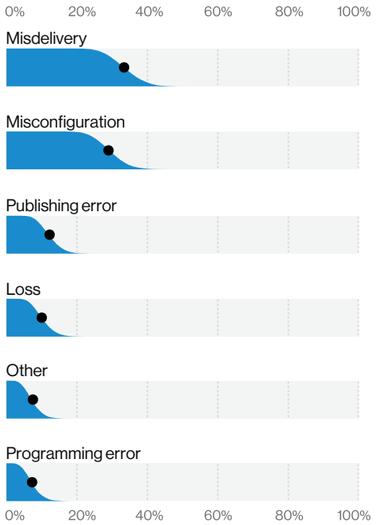


Figure 93. Top Error varieties in Public Administration breaches (n = 92)

The same is true of Lost and Stolen Assets. These are unencrypted devices or they wouldn't be considered even at risk of a data breach. Unless, of course, the decryption key is also lost at the same time in human-readable format (before you jeer, keep in mind that we have actually seen this). The data on these devices is most likely protected only by a password, and is therefore considered at-risk in our dataset, and not a confirmed data breach.

No Regerts[42]

In the red corner, Miscellaneous Errors is the most prominent pattern in this industry when looking at confirmed data breaches. Figure 93 shows us that Misdelivery remains a big problem for the public sector. This is when sensitive information goes to the wrong recipient. It may be via electronic means, such as emails that are misaddressed, or it may be old-fashioned paper documents. Those mass mailings (and nobody can hold a candle to the volume of paper sent out by government entities) where the envelopes and their contents become out of sync can be a serious problem.

In the blue corner, weighing in at 30% of breaches, we have Misconfiguration, the other contender for the top variety of Error. A Misconfiguration data breach is when someone (usually a system administrator or someone in another privileged technical role) spins up a datastore in the cloud without the security measures in place to protect the data from unauthorized access. There are security researchers out there who spend their time looking for just this kind of opportunity. If you build it, they will come.

Looking back at changes from last year to this, the top three patterns have altered composition quite a lot. The 2019 report showed the top three breach patterns as Cyber-Espionage, Miscellaneous Errors and Privilege Misuse. You can see the difference in the rankings in Figure 94. Both Cyber-Espionage and Privilege Misuse declined in our dataset overall this year, and have dropped into the single digit percentages in this sector.

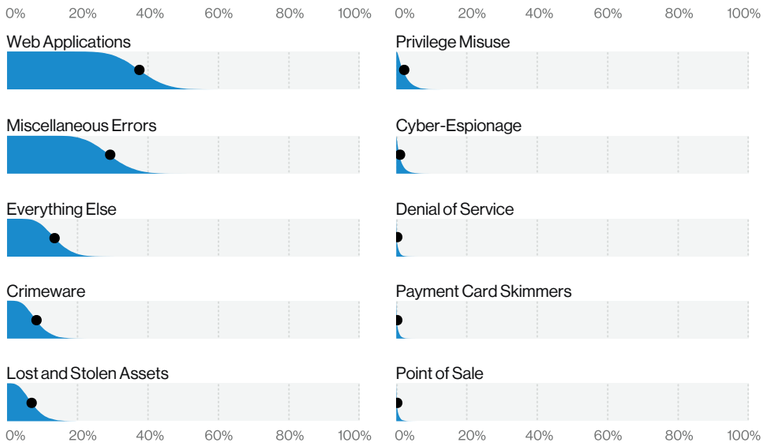


Figure 94. Patterns in Public Administration breaches (n = 346)

42 Well, except for these ugly tattoos we got on a dare last year.

Real Estate and Rental and Leasing

NAICS 53

Summary

Web Applications attacks utilizing stolen credentials are rife in this vertical. Social engineering attacks in which adversaries insert themselves into the property transfer process and attempt to direct fund transfers to attacker-owned bank accounts are also prevalent. Like many other industries, Misconfigurations are impacting this sector.

Frequency	37 incidents, 33 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 88% of data breaches.
Threat Actors	External (73%), Internal (27%) (breaches)
Actor Motives	Financial (45%–97%), Convenience/ Espionage (0%–40% each), Fear/Fun/ Grudge/Ideology/ Other/Secondary (0%–21% each) (breaches)
Data Compromised	Personal (83%), Internal (43%), Other (43%), Credentials (40%) (breaches)
Top Controls	Top Controls: Secure Configuration (CSC 5, CSC 11), Implement a Security Awareness and Training Program (CSC 17), Boundary Defense (CSC 12)
Data Analysis Notes	Actor motives are represented by percentage ranges, as only eight breaches had a known motive. Some charts also do not have enough observations to have their expected value shown.

SOLD!

There is nothing quite like that feeling of owning your first home. Moving in, enjoying the smell of fresh paint and reflecting on all the memories you'll make. Our data for this vertical indicates that cybercriminals are also being allowed to move right in and make themselves at home. Whether they are attending a showing of your data via Web Applications attacks, utilizing social engineering in the Everything Else pattern or simply being asked to drop in by your employees through an assortment of Miscellaneous Errors, they are certainly being made welcome. As you can see in Figure 95, it is difficult to state conclusively which of these three patterns is the statistical leader but we can assert that they are all in the running.

Don't leave the key under the welcome mat.

Although we saw a rather small number of breaches in this sector over the last year, there are some interesting high-level findings to discuss. As in many other sectors, criminals have been actively leveraging stolen credentials to access users' inboxes and conduct nefarious activities. In fact, across all industries, credential theft is so ubiquitous that perhaps it would be more accurate to consider them time-shares rather than owned. Meanwhile, other external actors are relying on social engineering to get the job done. Some of these activities are simply aimed at stealing your data, but in other cases these attacks can be used to tee up a separate assault, as seen in many of the attacks that leverage pretexting.

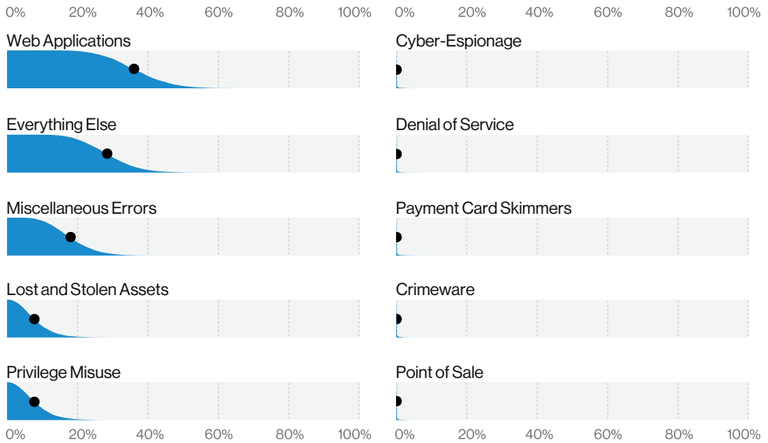


Figure 95. Patterns in Real Estate industry breaches (n = 33)

Figure 96. Top integrity impacts in Real Estate industry incidents (n = 16)

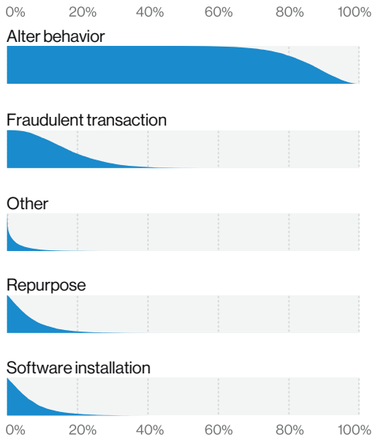


Figure 97. Top Error varieties in Real Estate industry incidents (n = 7)

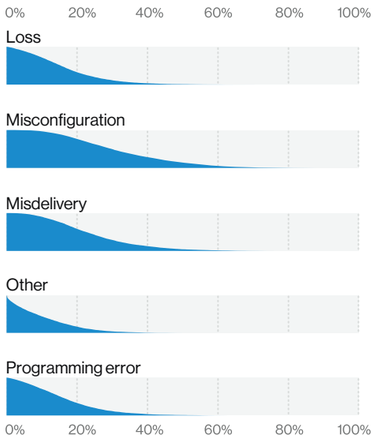


Figure 96 shows how Bad Guys™[43] exploit the milk of human kindness to dupe well-meaning employees into assisting them to achieve their objectives. They use pretexts to alter someone's behavior in such a manner that the employee divulges sensitive information, or otherwise unwittingly helps them to commit fraud. One example of this type of social engineering is when the attacker inserts themselves into an email thread regarding the sale or purchase of a new home and convinces the victim organization to transfer funds to attacker-owned bank accounts. It's worthwhile to make a phone call to confirm details before making this type of significant transaction.

You sent that to who?!

Even though this is the first time we have written an industry section for "Real Estate," we have been collecting data on this industry for a number of years. This enables us to analyze how the patterns have evolved over time in this vertical. This year, one of the more interesting findings was the continuity in volume of Errors. These Error-related breaches involve Misconfigurations (forgetting to turn those restrictive permissions on), Misdeliveries (email and/or paper documents sent to the incorrect recipient) and Programming errors (mistakes in code) as seen in Figure 97. These Error actions accounted for 18% of data breaches in the Real Estate vertical. If you do business in this industry, we urge you to take time for security awareness training and the implementation of sound policies and procedures.

43 Surely someone has trademarked this, right?

Retail NAICS 44–45

Summary

Attacks against e-commerce applications are by far the leading cause of breaches in this industry. As organizations continue to move their primary operations to the web, the criminals migrate along with them. Consequently, Point of Sale (PoS)-related breaches, which were for many years the dominant concern for this vertical, continue the low levels of 2019's DBIR. While Payment data is a commonly lost data type, Personal and Credentials also continue to be highly sought after in this sector.

Frequency	287 incidents, 146 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 72% of breaches.
Threat Actors	External (75%), Internal (25%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (99%), Espionage (1%) (breaches)
Data Compromised	Personal (49%), Payment (47%), Credentials (27%), Other (25%) (breaches)
Top Controls	Boundary Defense (CSC 12), Secure Configurations (CSC 5, CSC 11), Continuous Vulnerability Management (CSC3)

I'll buy that for $1.

We are sure it comes as no surprise to anyone in this sector, but the Retail industry is a frequent target for financially motivated actors. Retail as an industry is almost exclusively financially motivated too, so it is only fair. This sector is targeted by criminal groups who are trying to gain access to the wealth of payment card data held by these organizations. Last year's trend of transitioning from card-present to card-not-present crime continued, which drove a similar decrease since 2016 in the use of RAM-scraper malware. Personal data figures prominently in Retail breaches and is more or less tied with Payment for the top data type compromised. Certainly, if the attacker cannot gain access to Payment data, but stumbles across Personal data that is lucrative for other types of financial fraud, they will not file a complaint.

To the web with you!

Figure 98 provides us with a good view through the display case as it were in the "Retail" section. Over the last few years (2014 to 2019), attacks have made the swing away from Point of Sale devices and controllers, and toward Web Applications. This largely follows the trend in the industry of moving transactions primarily to a more web-focused infrastructure. Thus, as the infrastructure changes, the adversaries change along with it to take the easiest path to data.[44] Attacks against the latter have been gaining ground. In the 2019 DBIR, we stated that we anticipated Retail breaches were about to lose their majority to web-server-related breaches, and in Figure 99, we can see that has in fact occurred. Be sure to play the lucky lotto numbers printed on the back cover. Winner, winner! Chicken dinner!

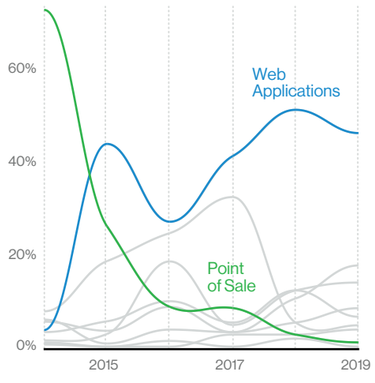


Figure 98. Patterns over time in Retail industry breaches

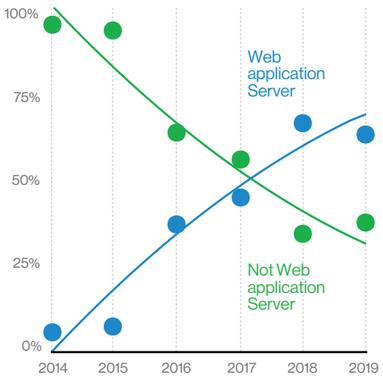


Figure 99. Web application Server vs Not Web application Server assets in Retail Payment data breaches over time

44 Of course, if you haven't made this transition, your PoS infrastructure remains at risk.

The Web Applications pattern is composed of two main action varieties: the use of stolen credentials and the exploitation of vulnerable web app infrastructure. Figure 100 shows that Exploit vuln and Use of stolen creds are close competitors for first place in the Hacking varieties category and there is not a great deal to distinguish between them from a percentage point of view. In a perfect world, someone else's data breach would not raise the risk to your own. However, that is increasingly not the case, with the adversaries amassing datastores of credentials from other people's misfortune and trying them out against new victims.

You hold the key to my heart.

Our non-incident data tells us that in this vertical (Figure 101), credential stuffing is a significant problem. While it is slightly below the most common value for all industries this year, it is not likely that people who have so many keys (credentials) will stop trying them on whatever locks they can find.

When the bad actors are not using other people's keys against your infrastructure, they are using unpatched vulnerabilities in your web apps to gain access. Based on the vulnerability data in Figure 102, only about half of all vulnerabilities are getting patched within the first quarter after discovery. It is best not to put those patches on layaway but go ahead and handle them as soon as possible. We know from past research that those unpatched vulnerabilities tend to linger for quite a while if they aren't patched in a timely manner—people just never get around to addressing them. Our analysis found that SQL, PHP and local file injection are the most common attacks that are attempted in this industry (Figure 103).

Figure 100. Top Hacking varieties in Retail industry breaches (n = 48)

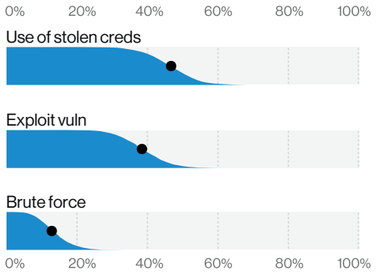


Figure 101. Credential stuffing attempts in Retail industry web blocks (n = 284); all industries mode (green line): 1.11 M

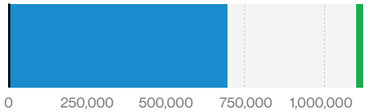


Figure 102. Patching in Retail industry vulnerabilities (n = 35,098)

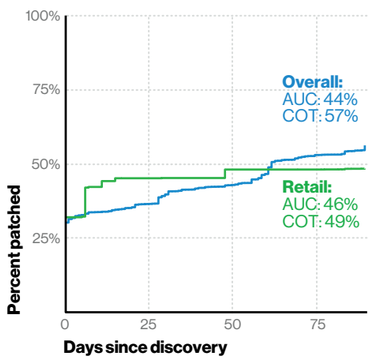
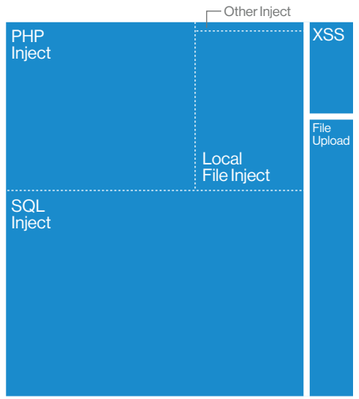


Figure 103. Varieties in Retail industry Web Application attacks (n = 2.22 billion)



Data types

If we were to create a ranking of the most easily monetizable data types, surely Payment card data would be at the top. After all, who doesn't have the urge to try out that brand new credit card and "break it in" when it first arrives? Figure 104 shows us that the attackers feel the same way, and likely want to build upon their sweet gaming rig with someone else's money. However, Personal data is tied with Payment data as the reigning champion. It's easy to forget that as web apps increasingly become the target of choice, the victims' Personal data is sometimes boxed up and shipped off right along with the Payment data as a lagniappe.

Figure 105 lists the top terms in hacking data from criminal forum and marketplace posts. It stands to reason that they would (like any good SEO effort) tailor their terms to what is most in demand. Clearly banking and payment card data is high on everybody's wish list, although those who are doing this type of trade do not need to go to the lengths of finding a dusty lamp to have those wishes granted.

Figure 104. Top data varieties in Retail industry breaches (n = 135)

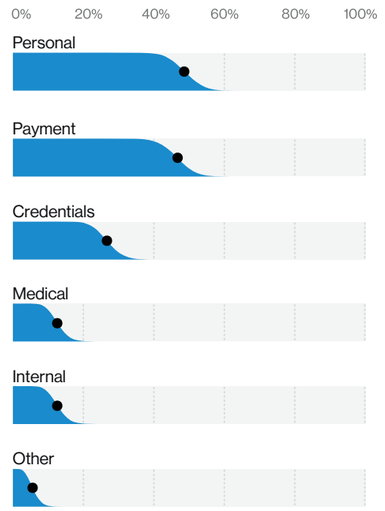
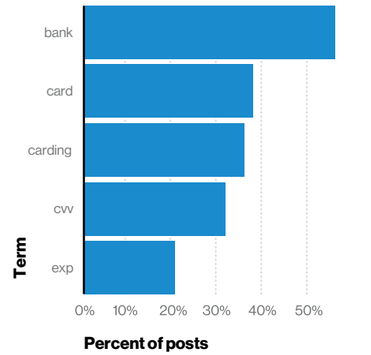


Figure 105. Top terms in hacking-related criminal forum posts (n = 3.35 million)



Transportation and Warehousing

NAICS 48–49

Summary

Financially motivated organized criminals utilizing attacks against web applications have their sights set on this industry. But employee errors such as standing up large databases without controls are also a recurring problem. These, combined with social engineering in the forms of phishing and pretexting attacks, are responsible for the majority of breaches in this industry.

Frequency	112 incidents, 67 with confirmed data disclosure
Top Patterns	Everything Else, Web Applications and Miscellaneous Errors represent 69% of breaches.
Threat Actors	External (68%), Internal (32%) (breaches)
Actor Motives	Financial (74%–98%), Espionage (1%–21%), Convenience (0%–15%) (breaches)
Data Compromised	Personal (64%), Credentials (34%), Other (23%) (breaches)
Top Controls	Boundary Defense (CSC 12), Implement a Security Awareness and Training Program (CSC 17), Secure Configurations (CSC 5, CSC 11)
Data Analysis Notes	Actor motives are represented by percentage ranges, as only 26 breaches had a known motive. Some charts also do not have enough observations to have their expected value shown.

The Transportation and Warehousing industry is a new one for our report. If you're reading this report for the first time for just this reason, pull up a chair, we're glad to have you! As you know, this industry is all about getting people and goods from point A to point B, and about storing those goods until they're needed. Once transported, the people are usually good enough to find their own places to stay, but that's another industry entirely.

All roads lead to pwnd.

What is causing breaches in this sector? Our data shows us that Web Applications attacks and Miscellaneous Errors are quite common, and the Everything Else pattern is also prevalent, but more on that later (Figure 106). Web applications are a common attack across the dataset, and a fact of life in this era is that if you have an internet-facing application, someone out there will eventually get around to testing your controls for you. The Hacking and Social actions were the most common in this industry, which supports the Web Applications pattern's prominence.

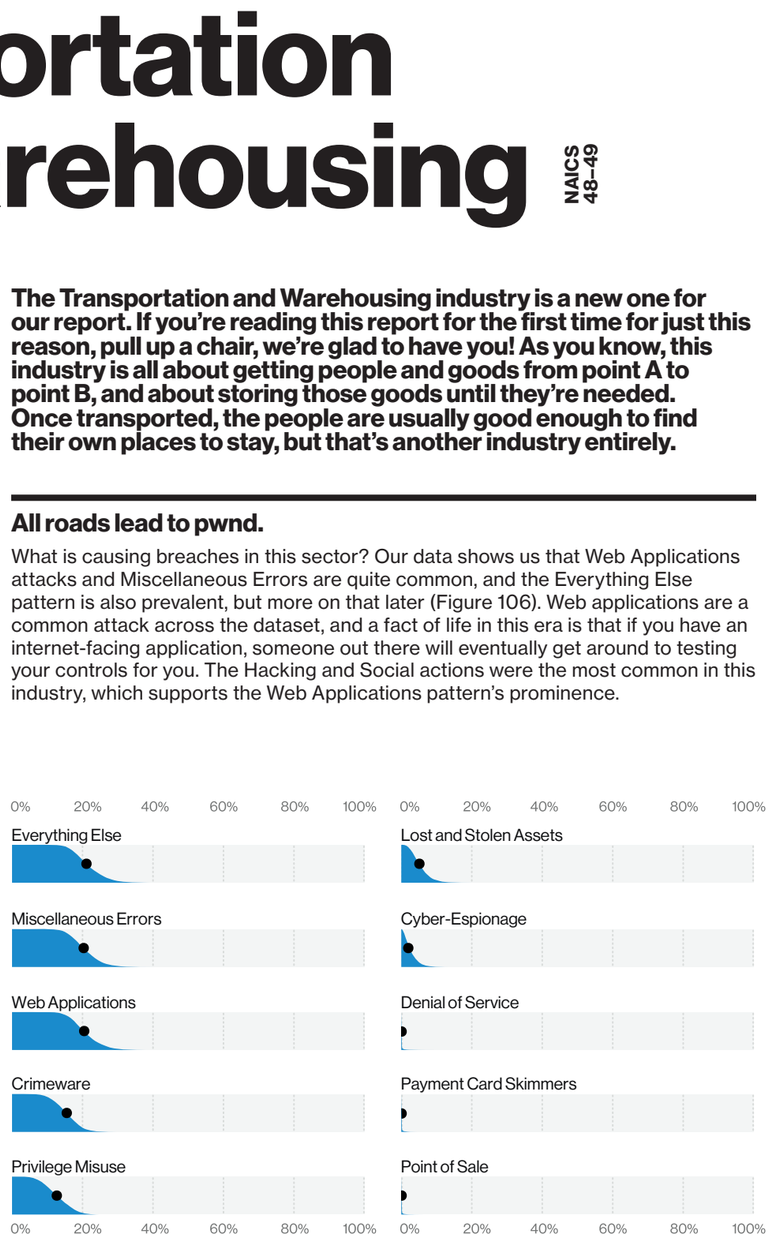


Figure 106. Patterns in Transportation industry breaches (n = 67)

Keep your eyes on the road.

Miscellaneous Errors are simply a byproduct of being human—we make mistakes. The most common error in this industry was Misconfiguration, as shown in Figure 107. A typical misconfiguration error scenario is this: An internal actor (frequently a system admin or DBA) stands up a database on a cloud service without any of those inconvenient access controls one would expect to see on sensitive data. Then, an enterprising security researcher finds this instance using a search engine that is made to spot these unprotected datastores and poof, you have a breach.

That Everything Else pattern mentioned earlier—it is a place we store odds and ends for attacks that don't fit into the other attack patterns, and within this pattern lives the business email compromise (BEC). These usually come in as a phishing email, although they can also be done over the phone. The goal of the attacker is either to get data or facilitate a wire transfer to their conveniently provided bank account. These attacks are perpetrated largely by organized criminal actors with a financial motive.

You can see in Figure 108 the most common motive of the external actors in this sector. While there are some espionage-motivated actors, they are few and far between when compared to financially motivated attackers. The data type of choice in this vertical appears to be Personal, which is being closely tailgated by Credentials.

Figure 107. Top Error varieties in Transportation industry breaches (n = 15)

Figure 108. Top Actor motives in Transportation industry breaches (n = 25)

04

Does size matter? A deep dive into SMB breaches

Does size matter? A deep dive into SMB breaches

Summary

While differences between small and medium-sized businesses (SMBs) and large organizations remain, the movement toward the cloud and its myriad web-based tools, along with the continued rise of social attacks, has narrowed the dividing line between the two. As SMBs have adjusted their business models, the criminals have adapted their actions in order to keep in step and select the quickest and easiest path to their victims.

Frequency	Small (less than 1,000 employees)	Large (more than 1,000 employees)
	407 incidents, 221 with confirmed data disclosure	8,666 incidents, 576 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 70% of breaches.	Everything Else, Crimeware and Privilege Misuse represent 70% of breaches.
Threat Actors	External (74%), Internal (26%), Partner (1%), Multiple (1%) (breaches)	External (79%), Internal (21%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (83%), Espionage (8%), Fun (3%), Grudge (3%) (breaches)	Financial (79%), Espionage (14%), Fun (2%), Grudge (2%) (breaches)
Data Compromised	Credentials (52%), Personal (30%), Other (20%), Internal (14%), Medical (14%) (breaches)	Credentials (64%), Other (26%), Personal (19%), Internal (12%) (breaches)

A trip down memory lane

Several years ago (the 2013 edition of the report to be precise), we took a look at some of the differences and similarities between small businesses (under 1,000 employees) and large businesses (1,000+ employees). Since a lot can change in seven years, we thought we would once again compare and contrast the two and see what story the data tells us. After all, now more than ever due to the proliferation of services available as commodities in the cloud, including platform as a service (PaaS), software as a service (SaaS) and any other *aaS of which you can conceive, a small business can behave more like a large one than ever before. Therefore, we asked ourselves the question, "Have the differences in capabilities evened the playing field out a bit between the two with regard to the detection of and response to security incidents?" Since you're reading this section, you've probably already guessed that the answer is "Yes!" Let's dive in and examine how much has changed, and in what ways the song remains the same.

The first thing we noticed when populating the Summary table is the wide chasm between the two when it comes to numbers of incidents and breaches. Breaches are more than twice as common in the larger companies than in the small ones. Does this mean the small organizations are flying under the radar, or are they simply not aware they've received visitors of the uninvited variety? And the inequality between the two when it comes to number of incidents is staggering. Is it an obvious case of "mo' money, mo' problems" for large enterprises? Is it due to increased visibility or perhaps a much wider attack surface? We find ourselves in the same position that some professional sports referees have been in recently as we realize it's hard (maybe more so in the Big Easy) to make the right call.

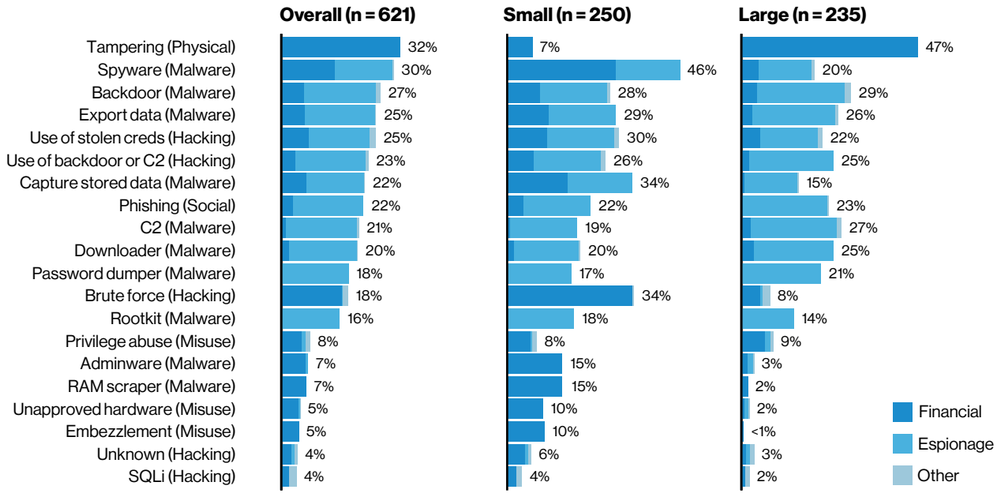


Figure 109. Top 20 threat actions (referencing the 2013 DBIR)

We call out the beginning attack patterns in the table at the beginning of this section, but the pattern concept wasn't born yet the last time we focused on organization size. In looking back, we can tell you there have been some changes in the most frequent causes (or as we like to call them in VERIS, action varieties) since 2013. The top 20 threat actions figure from the 2013 DBIR (Figure 109) lists the top 20 threat action varieties of the year, broken out into small and large organizations.

You can see that for large organizations, the top action was Physical tampering (wait, what?). For small organizations, in contrast, it was Spyware, although Brute-force hacking and Capturing stored data was not far behind. Skipping ahead seven years to our current dataset, we see that both large (Figure 110) and small (Figure 111) organizations have a top threat action of Phishing, with the Use of stolen credentials and Password dumpers in the top three for both (only in reverse order). Regardless, the same three contestants are leading the pack in both and that is an interesting finding. Phishing was considerably further down the list in 2013, as compared to the prime position it holds now.

Give me your keys and your wallet.

In 2013, far and away the favorite data type to steal was Payment card information. Back in those days, criminals would walk a long way (barefoot, in the snow, uphill both ways) to obtain this type of data (and they were thankful for the opportunity!). Following that, Credentials were a fan favorite, and Internal and Secret data were also very much in vogue. Examining the types of data stolen today, in both small and large organizations, we see that Payment card data is so last year. Today's criminal (lacking the work ethic of 2013) is primarily concerned with obtaining Credentials, regardless of the target victims' size. Personal data also seems to be highly sought after, irrespective of the size of an organization. After those two heavy hitters, it becomes too close to call between Medical, Internal or Payment data.

Another change from 2013 is the types of assets commonly attacked (Figure 112). The top asset for large companies (47%) was an ATM, while Point of Sale (PoS) controllers (34%) (followed closely at 29% by the Point of Sale terminal) were the top assets for small organizations. All of those assets have now fallen entirely off the list for both org types. Nowadays, organizations regardless of size are troubled with attacks on User devices, Mail servers and People (social attacks).

Figure 110. Top action varieties in large organization breaches (n = 448)

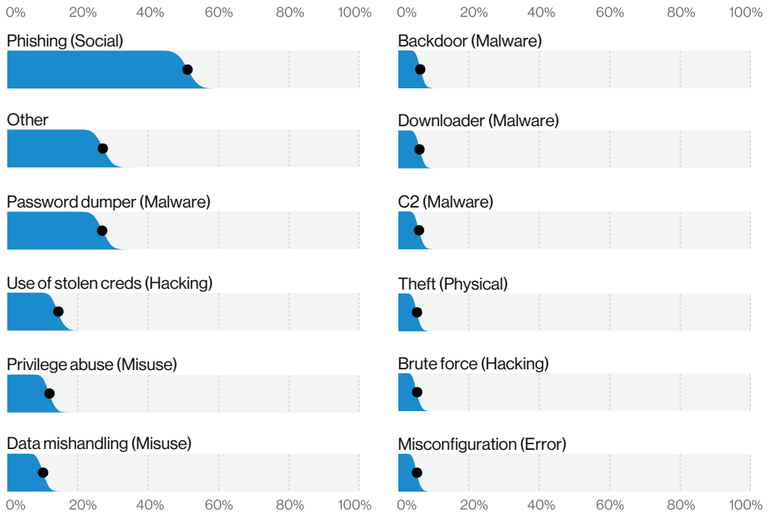
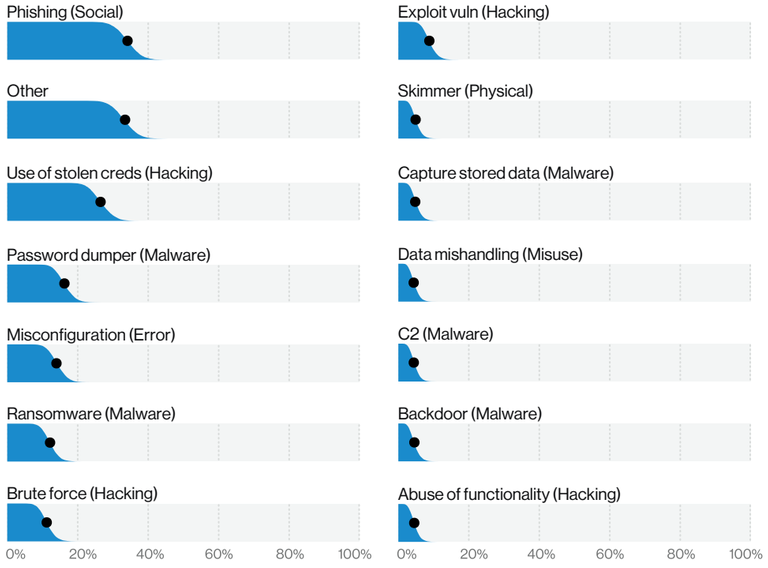


Figure 111. Top action varieties in small organization breaches (n = 194)



No time like the present

Moving on to the differences in the dataset for this year alone (otherwise we can't talk about patterns), the top attack patterns for small organizations were Web Applications, Everything Else and Miscellaneous Errors, with none of them emerging as the obvious winner. Meanwhile, large organizations are contending with Everything Else, Crimeware and Privilege Misuse as their main issues. Web Applications attacks are self-explanatory, while the Everything Else pattern is a pantechnicon stuffed with bits and bobs that do not fit anywhere else. Packed away in here you will find attacks such as the business email compromise—a social attack in the form of phishing, purporting to be from a company executive who is requesting data or a wire transfer. Miscellaneous Errors is a wide-ranging pattern that encompasses the many means (and they are legion) by which someone you employ can hurt your organization without malicious intent. The Crimeware pattern is your garden-variety malware and tends to be deployed by criminals who are financially motivated. Finally, Privilege Misuse is an act (usually malicious in nature) in which an Internal actor can ruin both your day and your brand.

When examining Timeline data, we noticed that the number of breaches that take months or years to discover is greater in large organizations (Figure 113) than in small organizations (Figure 114). This seems a bit counterintuitive. On the one hand, large organizations have a much larger footprint and could possibly be more likely to miss an intrusion on an internet-facing asset that they forgot they owned, but small orgs have a reduced attack surface so it might be easier to spot a problem. On the other hand, large orgs typically have dedicated security staff and are able to afford greater security measures, whereas small businesses often do not. Whatever the reason, there is a rather marked disparity between them with regard to Discovery.

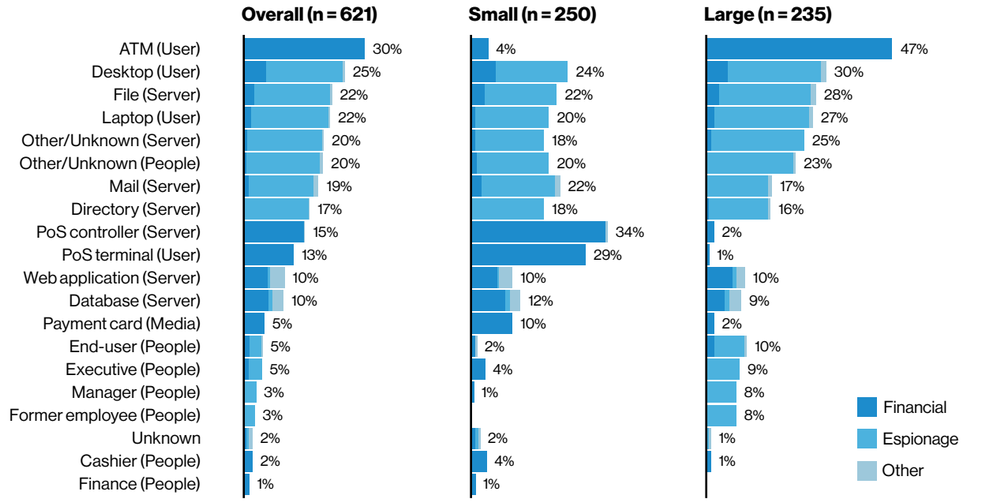


Figure 112. Varieties of compromised assets (referencing the 2013 DBIR)

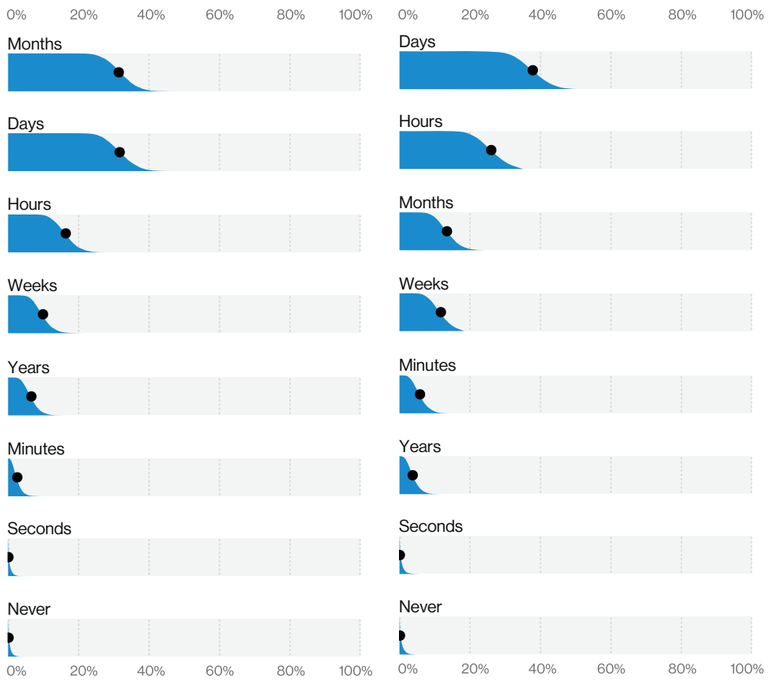


Figure 113. Discovery time in large organization breaches (n = 121)

Figure 114. Discovery time in small organization breaches (n = 102)

05

Regional analysis

Introduction to regions

Incidents	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	32,002	407	8,666	22,929
APAC	4,055	27	33	3,995
EMEA	4,209	57	88	4,064
LAC	87	14	10	63
NA	18,648	231	6,409	12,008
Unknown	5,003	78	2,126	2,799
Total	32,002	407	8,666	22,929

Breaches	Total	Small (1–1,000)	Large (1,000+)	Unknown
Total	3,950	221	576	3,153
APAC	560	22	24	514
EMEA	185	41	53	91
LAC	14	5	5	4
NA	920	130	209	581
Unknown	2,271	23	285	1,963
Total	3,950	221	576	3,153

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

We present for the first time a focused analysis on macro-regions of the world, thanks to the diligent work of the team this year to increase the diversity of our data contributors and the more precise statistical machinery we have put in place.

After the filtering and subset creation described in the "Introduction to industries" section, we are left with a similar result on Table 2. We define regions of the world in accordance with the United Nations M49[45] standard, joining the respective super-region and subregion of a country together. By combining them even further, the subjects of our global focus are:

- **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 Africa (002), Europe including Northern Asia (150) and Western Asia (145)
- **LAC –** Latin America and the Caribbean (419), also including for redundancy due to potential different encodings South America (005), Central America (013) and Caribbean (029)
- **NA –** Northern America (021), mainly consisting of breaches in the U.S. and Canada, as well as Bermuda, which has also been busy lately for some reason

As the table clearly shows, we have better coverage in some regions than in others. However, we did not want to leave anyone out of our around-the-world tour, and this is where a lot of our estimative language and percentage ranges will come in handy.

This is also a great opportunity for us to ask for our readers to help us by sharing your data so we have more data breaches to report on. Please don't take this as an invitation to create data breaches by either malicious intent or by accident! However, by suggesting new potential data contributors from the regions where you, our readers, would like more detailed analysis, and by encouraging organizations in those areas to contribute data to the report, we can continue expanding our coverage and providing better analysis each new year.

The same caution with small sample numbers we discussed in the "Introduction to industries" section applies to Figure 115 – some of them are so small that you can easily step on them like the Lego pieces your kid leaves lying around. Believe us when we tell you that a biased statement that does not take into consideration the small sample size (n value) is just as painful. Be on the lookout for "Data Analysis Notes" in the "Latin America and the Caribbean" section where we will be calling out those "small samples" and check out the "Methodology" section for more information on the statistical confidence background used throughout this report.

Please note: Based on feedback from our readers, we know that while some study the report from cover to cover, others only skip to the section or region that is of direct interest to them. Therefore, you may notice that we repeat some of our definitions and explanations several times, since the reader who only looks at a given section won't know the definition or explanation that we might have already mentioned elsewhere. Please overlook this necessary (but possibly distracting) element.

45 https://en.wikipedia.org/wiki/UN_M49

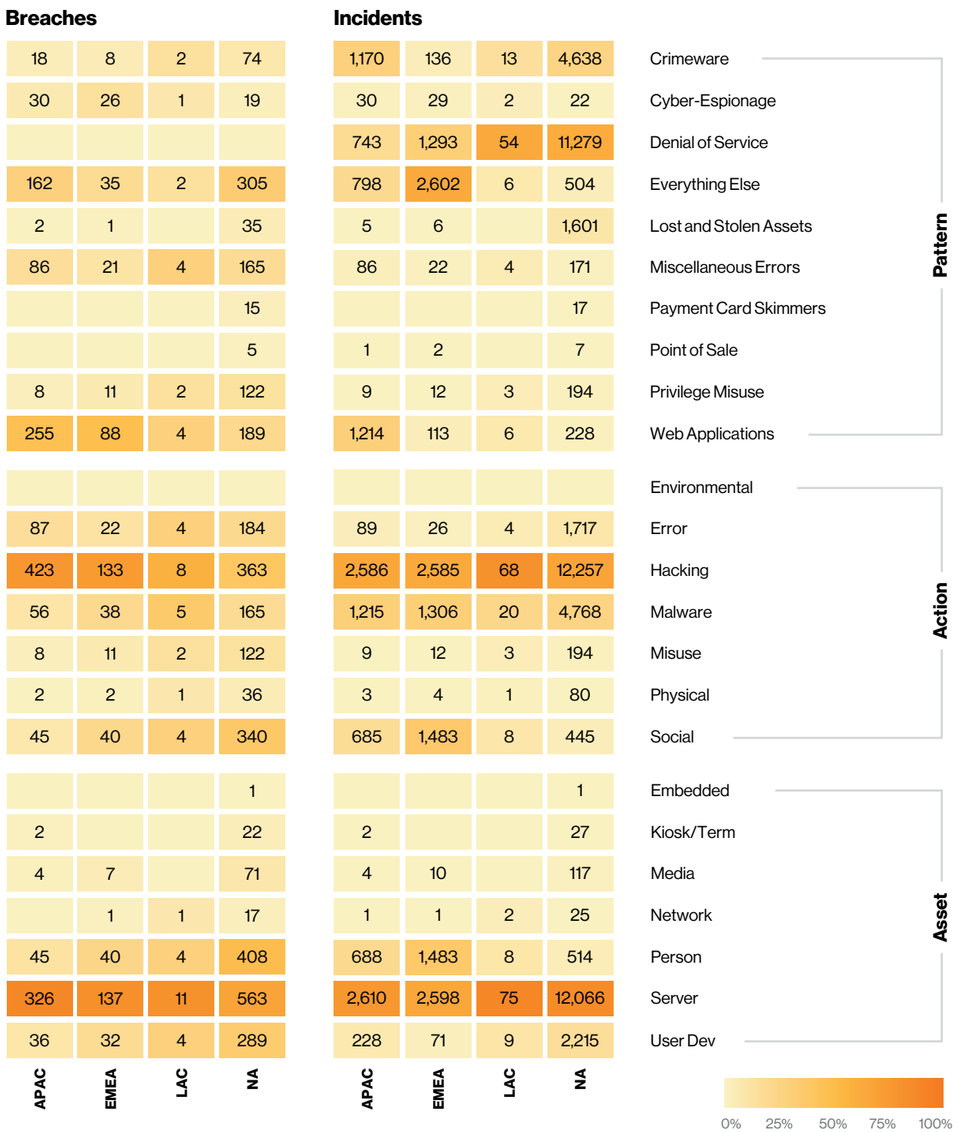
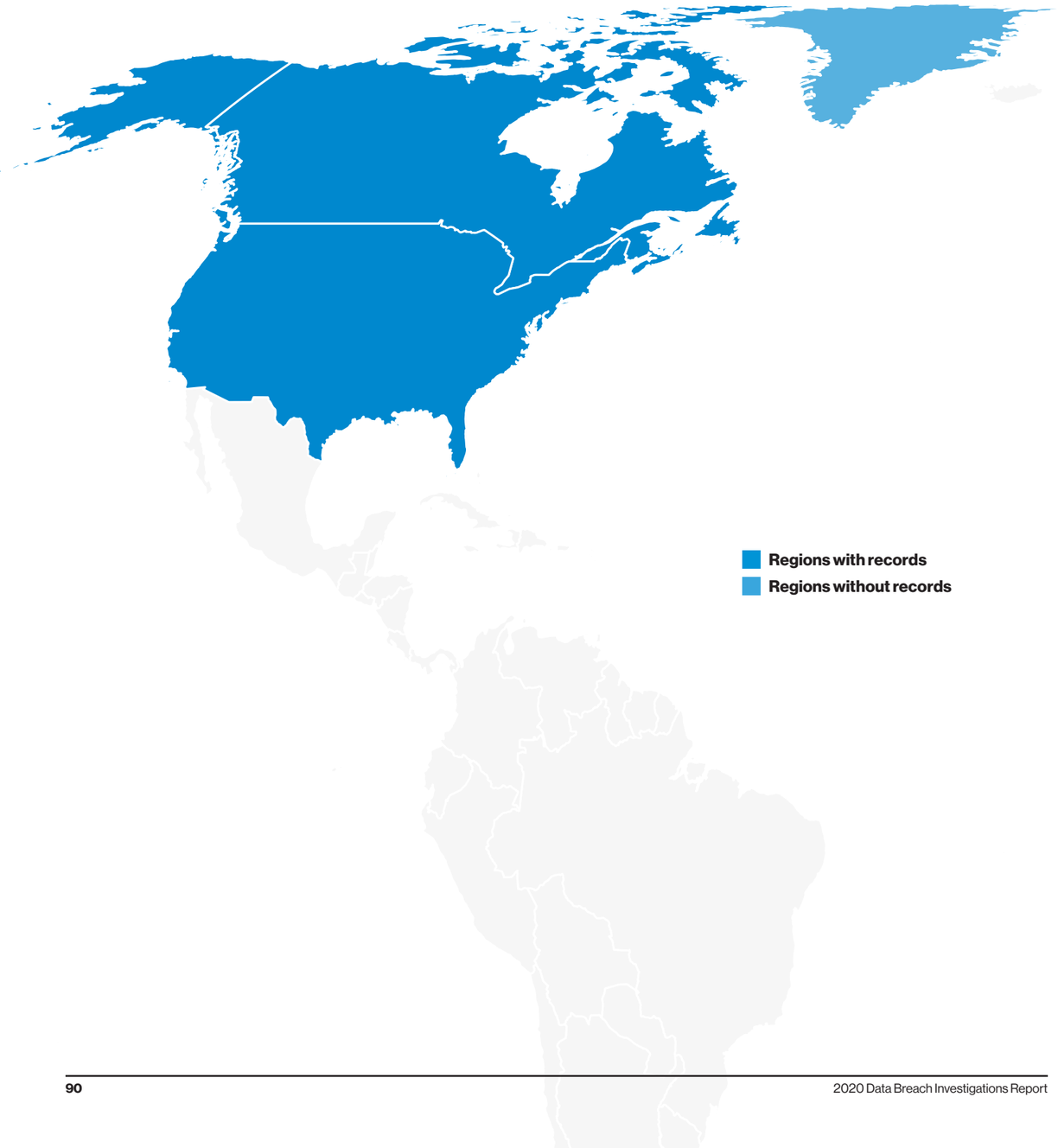


Figure 115. Breaches and incidents by region

Northern America (NA)

Figure 116. Northern America (NA) region



The region designated as Northern America consists of the United States and Canada, as well as some outlying islands such as Bermuda.

There are a couple of factors that need to be kept in mind when looking at the findings below. First of all, this region accounts for 70% of all incidents and 63% of all breaches in our dataset this year. That does not mean that good security practice has disappeared into the Bermuda Triangle, though. Northern America has arguably some of the most robust data reporting standards[46] in existence, particularly in Healthcare and Public administration. Therefore, the number of incidents and breaches are likely to be higher than in areas with less stringent disclosure requirements. Also, it must be admitted that while this report is becomingly increasingly global in scope, many of our contributors are located in and are primarily concerned with Northern American organizations. As a result of these factors, outcomes for this region are not too dissimilar from the findings for the overall dataset. Nevertheless, there are a few interesting differences and highlights worthy of discussion.

Phish and whistle, whistle and phish[47]

Everything Else is the top pattern for this region (Figure 117). That is due in large part to the number of financially motivated phishing attacks that we see across so many industries (Figure 118). In the past, we have observed that security awareness training can help limit the frequency and/or impact of phishing attacks. However, in some instances, this training appears to be either not carried out at all or delivered in an insufficient or inadequate manner. Whatever the reason, telling employees not to click phishing emails can be as effective as yelling “ear muffs” when you don’t want your child to hear something unpleasant.

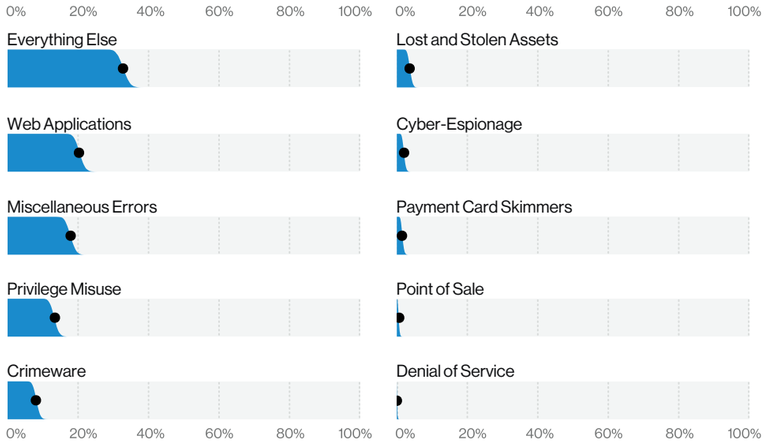


Figure 117. Patterns in Northern American breaches (n = 920)

Summary

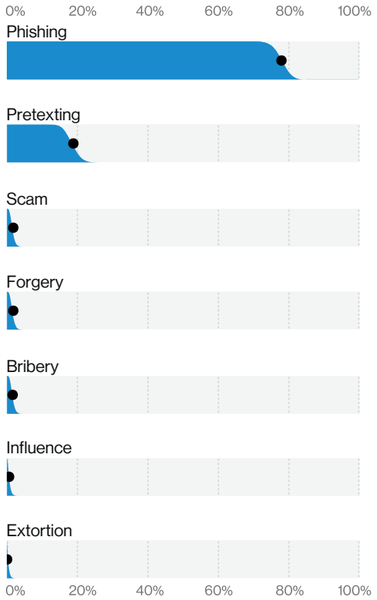
Northern American organizations suffered greatly from financially motivated attacks against their web application infrastructure this year. Hacking via the Use of stolen credentials was most commonly seen, with social engineering attacks that encourage the sharing of those credentials following suit. Employee error was also routinely observed in our dataset.

Frequency	18,648 incidents, 920 with confirmed data disclosure
Top Patterns	Everything Else, Web Applications and Miscellaneous Errors represent 72% of all data breaches in Northern America.
Threat Actors	External (66%), Internal (31%) Partner (5%), Multiple (1%) (breaches)
Actor Motives	Financial (91%), Espionage (5%), Grudge (3%) (breaches)
Data Compromised	Personal (43%), Credentials (43%), Other (35%), Internal (21%) (breaches)

46 This is largely due to the robust data breach notification laws passed over the years, such as California S.B. 1386 passed in 2002, which served as a blueprint for other states in the U.S. and has now been augmented by the California Consumer Privacy Act (CCPA) in the Golden State.

47 We hope you will allow us a paraphrase of the words of the great John Prine. He will be sorely missed.

Figure 118. Social varieties in Northern American breaches (n = 322)



Get your head out of your ... cloud.

Web app attacks also loom large in Northern America. The majority of these attacks are carried out via the Use of stolen credentials (Figure 119), which are then used to hack into web-based email and other web applications utilized by the enterprise (Figure 120). We have mentioned in past reports that, with the growing trend of businesses moving toward cloud-based solutions, we could expect the Use of stolen credentials to increase proportionally. This does seem to be the case.

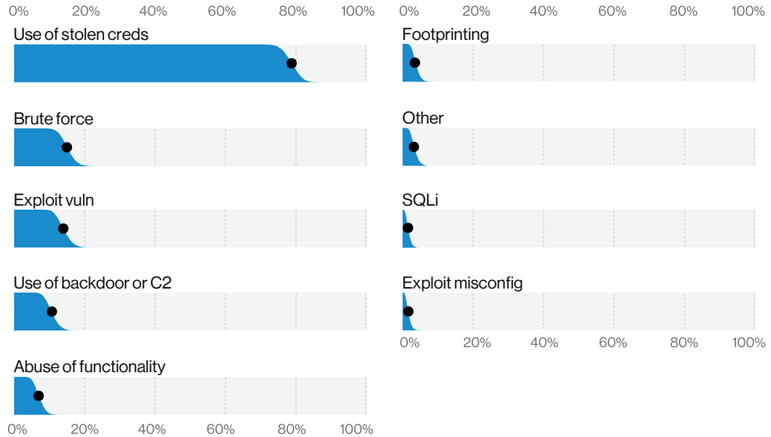


Figure 119. Top Hacking varieties in Northern American breaches (n = 268)

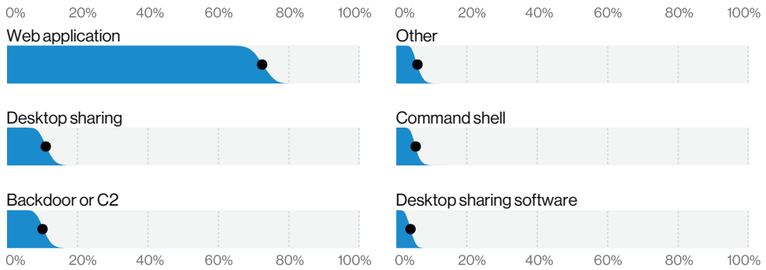


Figure 120. Top Hacking vectors in Northern American breaches (n = 260)

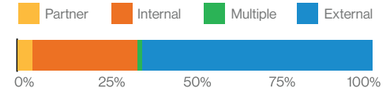


Figure 121. Actors in Northern American breaches (n = 908)

See! This is why we can't have anything nice.

You don't need External actors to harm your organization as long as your employees are willing to do their work for them. The number of Internal actors is somewhat high (30%) this year for this region and for the dataset as a whole (Figure 121). This is explained by the prevalence of Error and Privilege Misuse actions. Both are caused by Internal actors and both can be very damaging to an organization, but while Error is unintentional, Misuse can be (and often is) malicious in nature.

Let's take a quick look at the Error actions. As you can see in Figure 122, the vast majority of all error-related breaches are caused by Misdelivery (sending data to the incorrect recipient) and Misconfiguration (i.e, forgetting to secure to a storage bucket). For whatever reason, these Error types seem to be the peanut-butter-and-jelly sandwich of the breach world this year. Perhaps Internal actors are simply too busy trying to perfect their Renegade dance on TikTok these days; we do not know for sure. Whatever the reason, these errors are found in every industry and region, and in alarmingly large percentages. As mentioned elsewhere in this report, the vector for these errors is almost entirely carelessness on the part of the employee.

Turning our attention to Misuse, we see a proliferation of Privilege abuse (56%). This is using legitimate access for an illegitimate purpose. Somewhat farther down the ladder, we see approximately equal percentages of Data mishandling and Possession abuse (Figure 123). No matter how you view it, this region would benefit from increased controls for Internal actors.

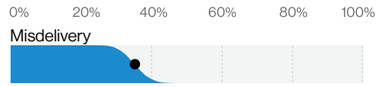


Figure 122. Top Error varieties in Northern American breaches (n = 166)

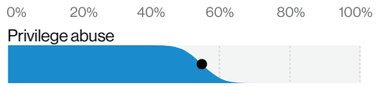
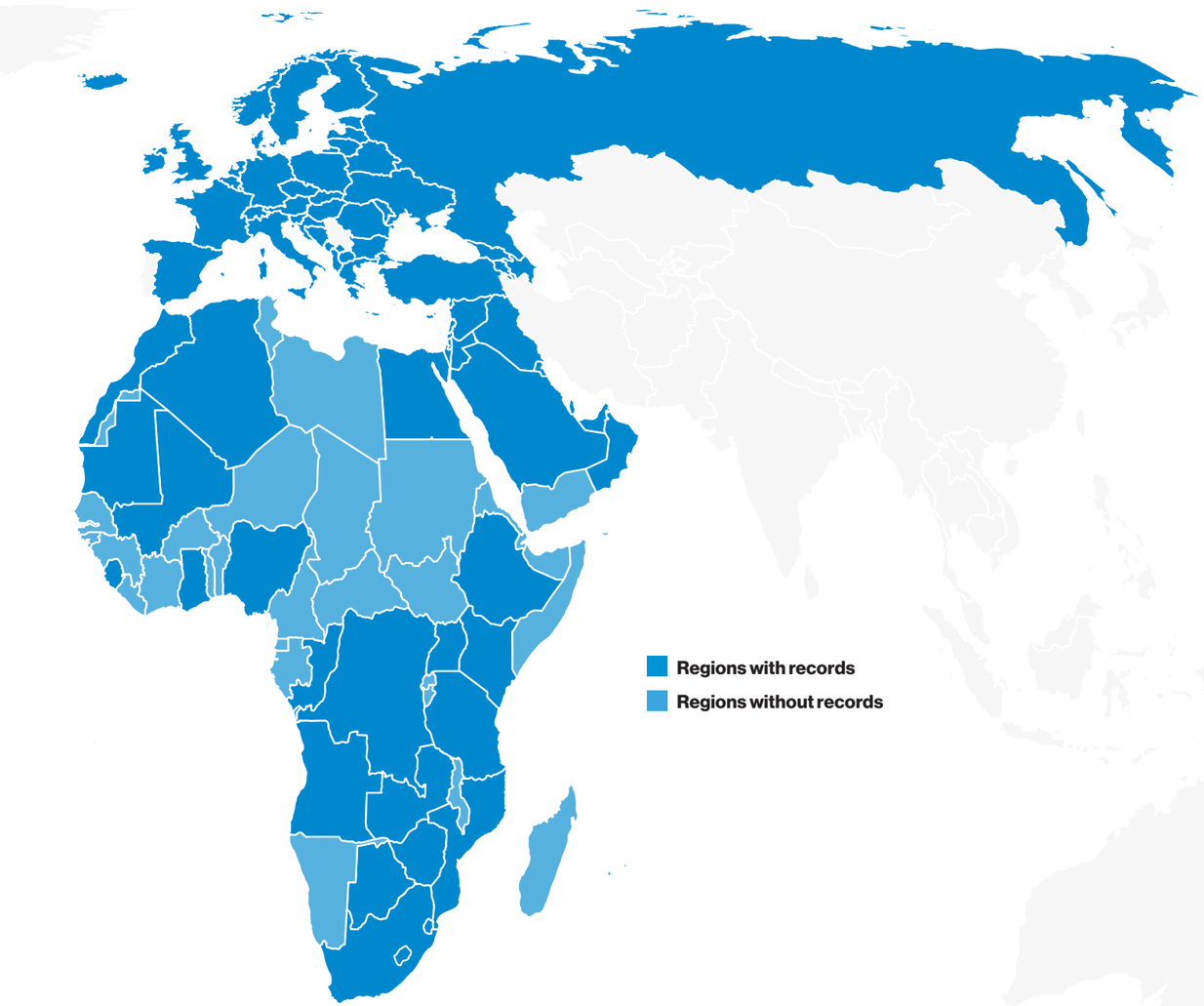


Figure 123. Top Misuse varieties in Northern American breaches (n = 121)

Europe, Middle East and Africa (EMEA)

Figure 124. Europe, Middle East and Africa (EMEA) region



As our world has become increasingly smaller over the years, it seems that the scope of our report has done the opposite.

In that spirit of growth and exploration, we will examine data from Europe, the Middle East and Africa (EMEA) in this section. While some readers may consider it "over there," the types of attacks and cybersecurity incidents experienced by those in EMEA are quite similar to what we observe elsewhere. In this region, Web Applications, Everything Else and Cyber-Espionage are the top patterns associated with the 185 breaches that we tracked this year (Figure 125).

The Web Applications pattern encompasses two major attacks that greatly affect this region. The first is Hacking via the Use of stolen credentials, which accounts for approximately 42% of data breaches. This scenario usually plays out in the following manner: An attacker uses credentials, typically gathered either through phishing or malware, to access a web application platform owned by the organization and commit wickedness of one type or another. This year, we've seen adversaries target assets such as outward-facing email servers, but also other platforms such as business-related applications. The second type of attack associated with this pattern is the use of exploits against web-facing applications to either gain access to the system data itself, or to repurpose the server for something more nefarious. These attacks account for close to 20% of our breaches in EMEA this year. If you haven't checked your external-facing websites recently for unpatched vulnerabilities or missing multifactor logins, you might want to get on that.

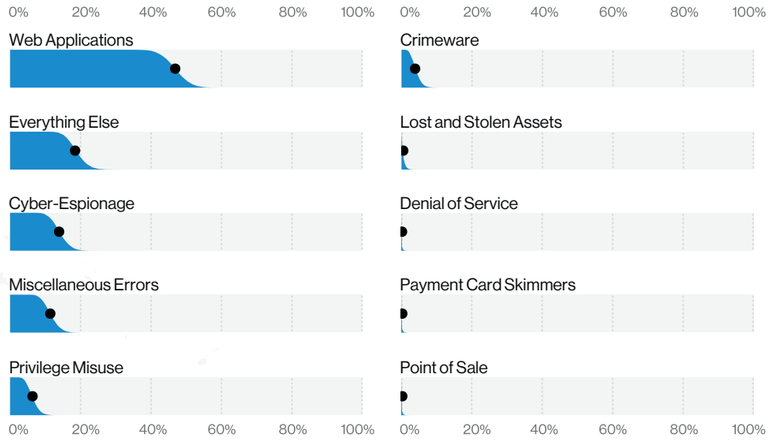


Figure 125. Patterns in EMEA breaches (n = 185)

Summary

Attackers are targeting web applications in EMEA with a combination of hacking techniques that leverage either stolen credentials or known vulnerabilities. Cyber-Espionage attacks leveraging these tactics were common in this region. Denial of Service attacks continue to cause availability impacts on infrastructure as well.

Frequency	4,209 incidents, 185 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Cyber-Espionage represent 78% of data breaches in EMEA.
Threat Actors	External (87%), Internal (13%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (70%), Espionage (22%), Ideology (3%), Fun (3%), Grudge (3%), Convenience (1%) (breaches)
Data Compromised	Credentials (56%), Internal (44%), Other (28%), Personal (20%) (breaches)

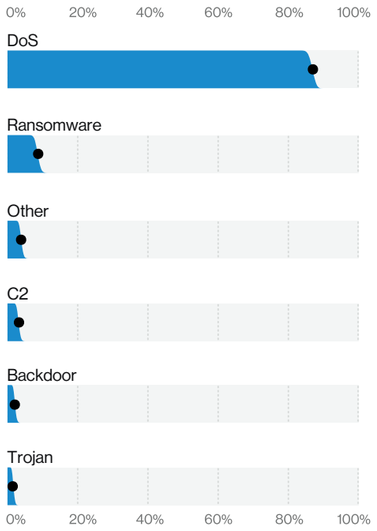


Figure 126. Top Malware varieties in EMEA incidents (n = 1,298)

The next pattern, Everything Else, is a catch-all category for breaches and incidents that do not readily fit into one of the other patterns. In this instance, it mostly consists of typical business email compromises (BEC) and represents 19% of the data breaches within this region. In this type of incident, fraudsters will mimic a business partner, client, executive, etc., in order to get an organization to transfer a payment over to an attacker-owned bank account. These attacks vary in degree of sophistication between spear-phishing and pretexting (where a bad actor hijacks an existing thread and inserts themselves into the conversation, thereby making it much harder to catch the fraudulent action).

I spy.

In third place was the Cyber-Espionage pattern, accounting for 14% of the region's breaches, which is substantially higher than the average of 3% for the overall dataset. This is an interesting finding, and there is not a clear-cut reason for it. The most likely explanation is that it may be an artifact of our data contributors and the cases they happen to encounter in these locales. But then again, James Bond is British after all. In this sort of incident, one should expect to see the hallmarks of the Advanced Persistent Threat (APT) attack—combinations of social attacks (phishing) to gain access, along with malware being dropped and deployed in the environment in order to maintain persistence and remain unobserved.

Zooming out

If we take a step back and look at the larger class of incidents, we see that Denial of Service (DoS) attacks topped the regional charts for malware varieties (Figure 126). An interesting point is that while DoS attacks accounted for a very high percentage of incidents in this area's overall corpus, they actually had one of the lowest rates of bits per second (BPS) of any region. The second most common incident for the region was ransomware, which continues to be ubiquitous globally. In fact, if we remove DoS attacks, ransomware accounts for 6% percent of all incidents here, and is commonly associated with C2/backdoors, Brute forcing and Password dumpers. All the more reason we should keep our endpoints malware free and our servers locked down.

Asia-Pacific (APAC)

Figure 127. Asia-Pacific (APAC) region

Summary

The APAC region is being targeted by financially motivated actors deploying ransomware to monetize their access. This region is also beset by phishing (often business email compromises), internal errors and has a higher-than-average rate of Cyber-Espionage-related breaches. Web application infrastructure is being targeted both by Denial of Service attacks affecting the availability of the assets, and by hacking attacks leveraging stolen credentials.

Frequency	4,055 incidents, 560 with confirmed data disclosure
Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 90% of breaches.
Threat Actors	External (83%), Internal (17%), Partner (0%) (breaches)
Actor Motives	Financial (63%), Espionage (39%), Fun (4%) (breaches)
Data Compromised	Credentials (88%), Internal (14%), Other (9%), Personal (6%) (breaches)

The Asia-Pacific (APAC) region includes a vast amount of territory, including most of Asia, what many refer to as Oceania (e.g., Australia and New Zealand), and numerous island nations in and around the Pacific.

An incident does not a breach make ... or does it?

In Figure 128, we can see the patterns that account for the majority of incidents in this region. It is important to note that some of those patterns, while prevalent, do not usually result in a confirmed breach. For instance, in the Crimeware pattern, the second most common Malware variety is Ransomware incidents. These are both an Integrity violation (Software Installation) and an Availability violation (Obscuration) as they encrypt the data, but instances where the data is known to be viewed and stolen (Confidentiality) remain relatively rare. However, in our data collection for next year's report,[48] cases are surfacing in which certain groups of actors are using the tactic of "naming and shaming" their victims in an attempt to exert additional pressure on them to pay the ransom. In other cases, the actors will copy some or all of the data prior to encrypting it, and then post excerpts on their websites[49] in order to further incentivize their victims to pay up.

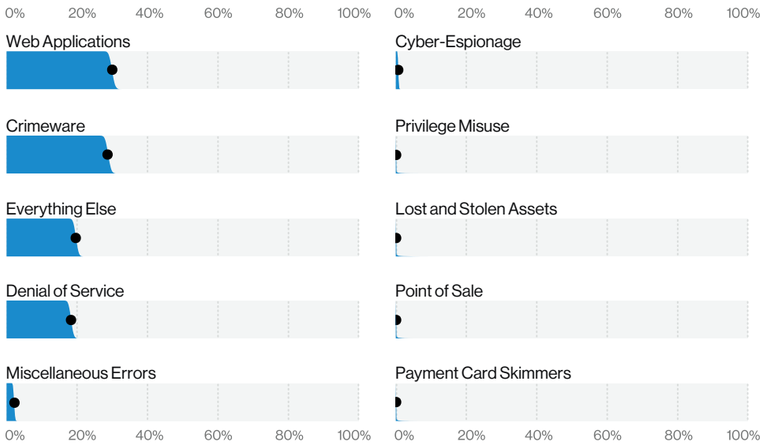


Figure 128. Patterns in APAC incidents (n = 4,055)

Web Applications attacks were the top pattern for both incidents and confirmed breaches in APAC. These attacks are most frequently someone testing their trusty store of stolen credentials against your web-facing infrastructure and crossing their fingers they will see success. Not surprisingly, with the problem of credential reuse and the vast treasure trove of resulting credential dumps, there are a fair number of hackers laughing all the way to the bank. If that strategy does not work for our hoodie-clad friends, the use of social engineering will frequently gain them the keys to the kingdom. Clearly, something is working, since Credentials were the top stolen data type in the region's breaches.

The second most common pattern was Everything Else (Figure 129). This serves as a category for breaches that do not fit the criteria for the other attack patterns. There are a couple of common attacks that live within this pattern. One of them, the business email compromise (BEC), is an attack that starts with a phishing email. The attacker is frequently masquerading as someone in the executive suite of the company and is trying to influence the actions of someone who would not normally be comfortable challenging a request from them. For example, a payroll clerk believes they are being told to reroute deposits to a different account by the CEO of the organization and so they do as instructed—only to find later that the request did not actually come from that executive.

Sometimes this comes in the form of a pretext (an invented scenario). One common example is asking for money via a wire transfer to a specific (never before used) account. In either case, unless there is a process in place to handle these kinds of unusual requests from someone in high authority, the organization will likely see an incident.

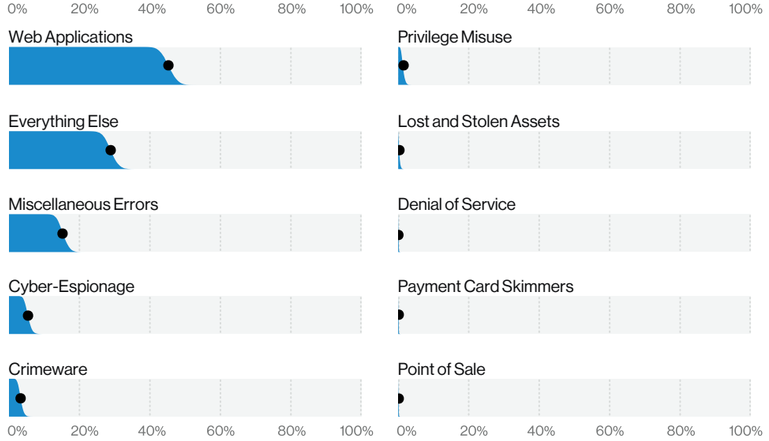


Figure 129. Patterns in APAC breaches (n = 560)

48 Sisyphus has nothing on us!
49 Some examples from publicly disclosed incidents: https://github.com/vz-risk/VCDB/issues?q=is%3Aopen+is%3Aissue+label%3ARansomeware-N%26S

Oops, did I do that?

A word of warning: What you are about to hear may shock you, but people are not perfect. Yes, we know, we didn't believe it at first either. But our dataset certainly indicates that it is the case, and neither organization type nor region seems to make much difference. In fact, the Miscellaneous Errors pattern comes in third in the APAC regional data. What are these errors? Why are they happening to me? Hop in and we will take you on a tour of the many ways the people who make up an organization can cause a breach without actually meaning to.

Figure 130 shows the bulk of these are Misconfiguration errors, and are due to Carelessness. Misconfiguration errors have long been a boon companion of this report. They occur when an employee—typically a system administrator or some other person with significant access to scads (yes that is a technical term) of data—stands up a database in the cloud without the usual security controls. "This will be fine. Surely nobody will locate this here," they think to themselves. Or perhaps the lunch special ends at two and they leave with the intention of putting those controls in place at the very next convenient moment. But often that moment only arrives after a security researcher, or much worse an attacker, has already found them. Yes, believe it or not there are truly a sizeable number of people who are employed (and some who are freelance) to find these nuggets of data strewn about on the internet just waiting to be unearthed. What comes next depends on the motives of the person who found the data. Most security researchers will notify the organization (if they can figure out who it belongs to). However, sometimes it isn't a person with motivations of notification, but rather an intention to monetize this tasty find on the dark web.

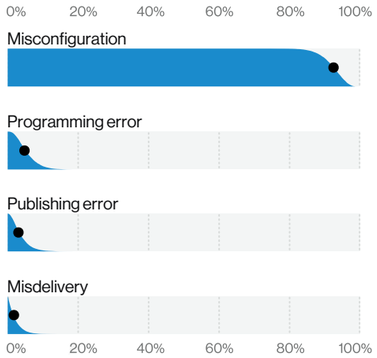


Figure 130. Error varieties in APAC breaches (n = 55)

Latin America and the Caribbean (LAC)

Figure 131. Latin America and the Caribbean (LAC) region

Summary

Even though there are a relatively small number of incidents and breaches recorded in the region, the results clearly show consistency with the global dataset. Denial of Service attacks are seen with a higher intensity than expected, and ransomware incidents are a serious problem.

Frequency	87 incidents, 14 with confirmed data disclosure
Top Patterns	Denial of Service, Crimeware and Web Applications represent 91% of incidents.
Threat Actors	External (93%), Internal (7%), Partner (1%), Multiple (1%) (incidents)
Actor Motives	Financial (52%–87%), Espionage/Ideology (2%–27% each), Fun/Grudge (0%–15% each), Convenience/Fear/Other/Secondary (0%–8% each) (incidents)
Data Compromised	Credentials, Personal, Internal, Secrets and System (incidents)
Data Analysis Notes	Actor motives are represented by percentage ranges, as only 22 incidents had a known motive.

It's the law—or not.

Before we begin, it is important to point out that not all of the countries in this region have a legal requirement to notify of a data breach either to the government or to those affected, with the notable exceptions of Mexico, Brazil (whose data protection law is only effective since February 2020) and Colombia (where only the government is required to be notified). As such, we can surely expect a significant under-reporting of incidents and breaches here. It should be interesting to see if, as in other areas of the world where new disclosure laws are passed, the reporting ramps up and we find that it was just the tip of the iceberg being reported before. Hopefully, we can entice new contributors in LAC to increase the quality of our data. (Is this you? Let's talk.)

All things considered, we see a clear mirroring of the data we have available for this region in the global dataset. The majority of actors in all incidents are External, with the 93% in the region being very similar to the 92% of the entire dataset. Likewise, 52% to 87% of incidents were Financially motivated in LAC, while 64% were so motivated in the global data.

The top patterns for incidents are also consistent with the larger dataset, with Denial of Service representing between 50% to 70%, while Crimeware, Web Applications and Everything Else are tightly grouped (Figure 132). Crimeware is largely made up of incidents involving Ransomware, which have a very strong showing in this region in relation to other action varieties.

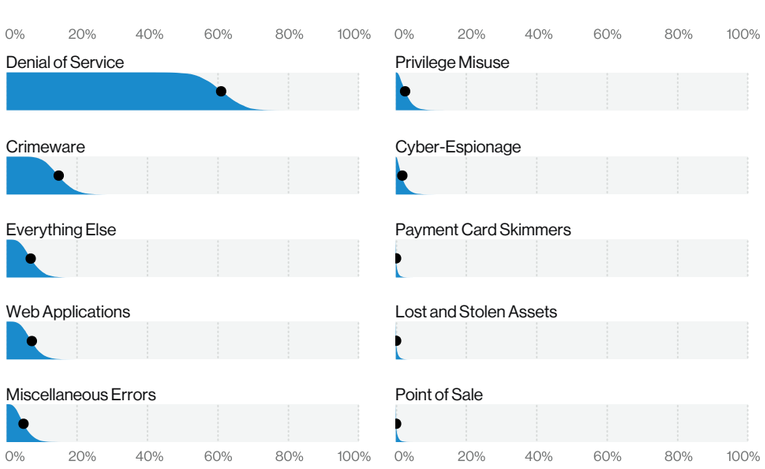


Figure 132. Patterns in LAC incidents (n = 87)

For all those similarities, this region had the largest median bits per second (BPS) by far—with 9 Gbps—where the global median was just a little over 500 Mbps (Figure 133). This higher intensity is in line with what one would expect from Denial of Service attacks against Financial organizations, which were over-represented in our regional DDoS data.

One of the things that has been reinforced in analyzing the data across the different locales is that, regardless of whether a specific country is represented in the dataset from year to year, all countries are seeing similar types of attacks. Time and again, we see that the adversaries are not adjusting their tactics based on the geographic location of their victims. They adjust their attacks based on what they need to do to gain access. So, while we have seen some differences across the regions, we are consistently finding that the kinds of attacks are common to all.

Figure 133. Most common BPS in LAC region DDoS (n = 52 DDoS); all regions mode (green line): 565 Mbps

06

Wrap-up

Well, that's it, folks! Thank you for joining us again. We hope you enjoyed reading the report and found the contents informative. As always, we send our most sincere thanks to our readers, supporters and contributors. This job can be a bit of a heavy lift at times, but it is also a labor of love. We feel very fortunate to be able to create this report and share the findings with you. We are grateful to all of you who have supported this endeavor with your time and resources. We hope to meet you all back here again next year, and in the meantime, be well, be prosperous and be prepared for anything.

CIS Control recommendations

CIS Critical Security Controls (CSCs)

CSC 1	Inventory and Control of Hardware Assets
CSC 2	Inventory and Control of Software Assets
CSC 3	Continuous Vulnerability Management
CSC 4	Controlled Use of Administrative Privileges
CSC 5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
CSC 6	Maintenance, Monitoring and Analysis of Audit Logs
CSC 7	Email and Web Browser Protections
CSC 8	Malware Defenses
CSC 9	Limitation and Control of Network Ports, Protocol and Services
CSC 10	Data Recovery Capabilities
CSC 11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
CSC 12	Boundary Defense
CSC 13	Data Protection
CSC 14	Controlled Access Based on the Need to Know
CSC 15	Wireless Access Control
CSC 16	Account Monitoring and Control
CSC 17	Implement a Security Awareness and Training Program
CSC 18	Application Software Security
CSC 19	Incident Response and Management
CSC 20	Penetration Tests and Red Team Exercises

For all the years of hard work, the DBIR can finally have some standardized controls, as a treat.

To be fair, this is simply a new take on an old approach. If you were to take out the 2014 version of the DBIR, blow the dust off of the cover and glance through the findings, you'll see an effort that we undertook to help standardize our approach to talking about defense and controls.

In this effort, we aligned our findings with the Center for Internet Security (CIS) Critical Security Controls (version 6 at the time) to provide you, our most devoted and loyal readers, with a way to match our findings to your security efforts. You may (or may not) be happy to hear that we've revisited our earlier attempt to help provide you with the same types of integration and assist you with tying your security program prioritization to our data.

Why CIS?

Most of us probably have our own preferences regarding security frameworks and guidance, and the authors of this report are certainly not without theirs (hint: one of us may have contributed to the CIS Critical Security Controls [CSCs] at one point or another), but there are several empirical reasons why we chose this specific collection of controls. In brief, they provide sufficient levels of detail to meaningfully tie back between our Actions and Vectors, and there's a multitude of different mappings between the CIS CSCs and other standards freely available online. Also, it helps that we jibe with their non-profit community approach.

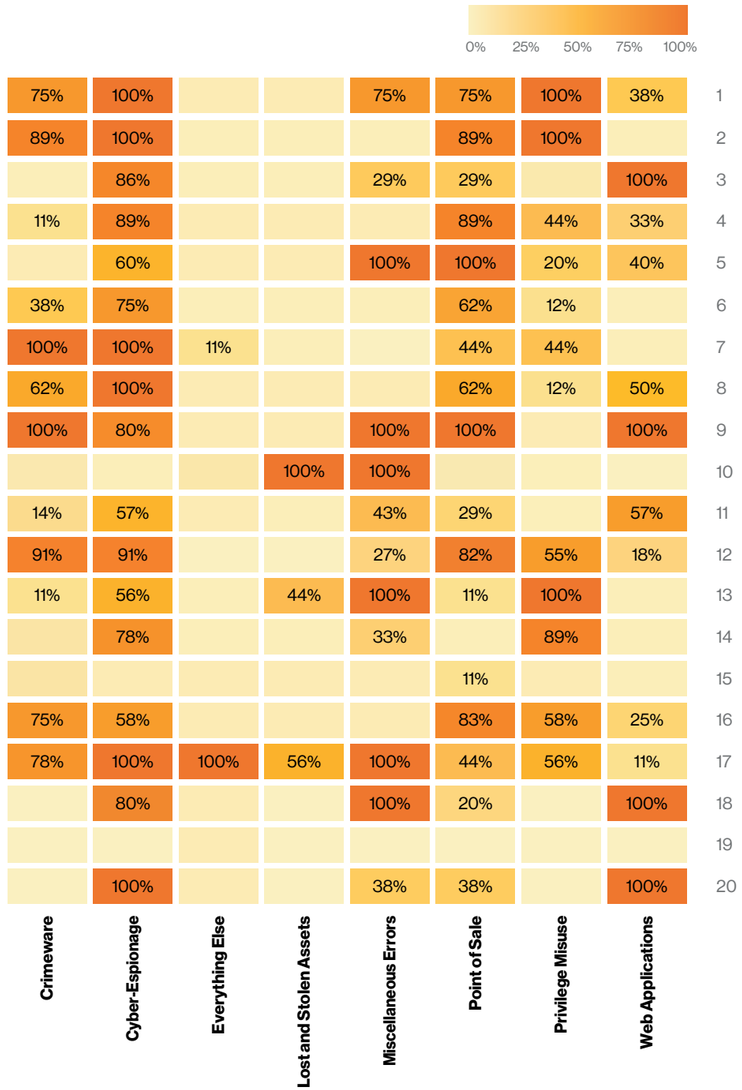


Figure 134. Percentage of Safeguards mapped to Patterns by Critical Security Control

For those who are unacquainted with the CIS CSCs, they are a community-built, attacker-informed prioritized set of cybersecurity guidelines that consist of 171 safeguards organized into 20 higher-level controls. One of the unique elements of the CIS CSCs is their focus on helping organizations understand where to start their security program. This prioritization is represented in two ways:

- Through the ordering of the Critical Security Controls so that they allow a loose prioritization (Critical Security Control 1: Inventory of Hardware is probably a better place to start than Critical Security Control 20: Penetration Testing)
- Introduced in version 7.1[50] is the concept of Implementation Groups, in which the 171 safeguards are grouped based on the resources and risks the organizations are facing. This means that a smaller organization with fewer resources (Implementation Group 1) shouldn't be expected to implement resource- and process-intensive controls such as Passive Asset Discovery even if it is within Critical Security Control 1, while an organization with more resources and/or a higher risk level may want to consider that control.

50 https://www.cisecurity.org/blog/v7-1-introduces-implementation-groups-cis-controls/

How we used it

The more observant among you may notice that we included a new item on our Summary tables in our industry sections that identify the Top Controls for the breaches found in that specific industry. To get those Top Controls, we developed a mapping between the VERIS Actions and the safeguards and then aggregated them at the Critical Security Control level. This allows you to get a rough approximation of some of the controls that you should consider prioritizing for your security program.

Figure 134 is based on the initial mapping we did and captures the percentage of safeguards per Critical Security Control that play a role in mitigating the patterns identified.[51] Below is also a quick description of some of the top controls identified across all the industries analyzed. Additional information on the actual Critical Security Controls can be found on the CIS website.[52]

Continuous Vulnerability Management (CSC 3)

A great way of finding and remediating things like code-based vulnerabilities, such as the ones found in web applications that are being exploited and also handy for finding misconfigurations.

Secure Configuration (CSC 5, CSC 11)[53]

Ensure and verify that systems are configured with only the services and access needed to achieve their function. That open, world-readable database facing the internet is probably not following these controls.

Email and Web Browser Protection (CSC 7)

Since browsers and email clients are the main way that users interact with the Wild West that we call the internet, it is critical that you lock these down to give your users a fighting chance.

Limitation and Control of Network Ports, Protocols and Services (CSC 9)

Much like how Control 12 is about knowing your exposures between trust zones, this control is about understanding what services and ports should be exposed on a system, and limiting access to them.

Boundary Defense (CSC 12)

Not just firewalls, this Control includes things like network monitoring, proxies and multifactor authentication, which is why it creeps up into a lot of different actions.

Data Protection (CSC 13)

One of the best ways of limiting the leakage of information is to control access to that sensitive information. Controls in this list include maintaining an inventory of sensitive information, encrypting sensitive data and limiting access to authorized cloud and email providers.

Account Monitoring (CSC 16)

Locking down user accounts across the organization is key to keeping bad guys from using stolen credentials, especially by the use of practices like multifactor authentication, which also shows up here.

Implement a Security Awareness and Training Program (CSC 17)

Educate your users, both on malicious attacks and the accidental breaches.

The future is under control.

To aid us both in our continuous improvement and transparency, we'll be adding our mapping of Critical Security Controls to our VERIS GitHub page at https://github.com/vz-risk/veris. We encourage you to use it as well and provide feedback on how you think we can improve. This is really our first step toward making this more accessible and easier for others to leverage, and while we acknowledge that this first version may have room for improvement, we plan to iterate rapidly on it. The more we share a common language, the easier it will be for us to work together toward more secure environments and organizations.

51 One thing of note is that the CIS Controls are focused on cybersecurity best practices and don't touch upon things like physical security (Payment Card Skimmers pattern) or availability practices (Denial of Service pattern), so we did not include them in our diagram.

52 https://www.cisecurity.org/controls/cis-controls-list/

53 We combined both Secure Configuration for Desktops, Servers and Workstations (CSC 5) AND Secure Configuration for Networking Devices (CSC 11), for two reasons. For one, it's difficult to know if it's a networking issue or a system issue that is the ultimate cause of the breach and for another, it's become increasingly more difficult to separate the network from the device in certain environments.

Year in review[54]

January

The first intelligence collection in 2019 was an FBI Liaison Alert System on APT10 intrusion activities targeting cloud-based managed service providers. Throughout the month, the Verizon Threat Research Advisory Center (VTRAC) intelligence collections reflected a continuation of some of 2018's trends and emerging developments that would occupy us throughout the new year. New intelligence linked two Russian APT-grade actors, GreyEnergy and APT28 (Sofacy). Two months since we began tracking "the DNSpionage campaign," new collections revealed its global span and complexity. GandCrab and Ryuk ransomware surged in January, in part to occupy the vacuum left after the SamSam operators were indicted and ceased operations. The VTRAC continued to track and report Magecart payment card scripting skimmer attacks on e-retailers, a threat that would resurface several more times in 2019. The Indian subsidiary of Milan-based Tecnimont SpA, fell prey to a fraud after US$18.6 million (₨130 crore) was stolen by Chinese hackers. The attackers breached the email system of the Mumbai branch to learn the "rhythm" of the business, identifying key players, vocabulary and customs. A series of staged conference calls with executives in Italy and a Swiss lawyer convinced the head of the Indian office to transfer funds to Hong Kong banks.

February

Australia's parliament revealed that its computer network had been compromised by an unspecified "security incident." Norwegian cloud computing company Visma attributed a breach to the menuPass threat actor. A whaling campaign was observed that was probably aiming for Office 365 credentials to be used for a business email compromise operation. The Bank of Valetta in Malta was the victim of a €13 million fraud. Analysis of weaponized documents used by APT-grade actors in APAC sought to determine if a shared "digital quartermaster" was supplying multiple actors, including multiple state-aligned ones. It found links among some Chinese actors but that "the current exchange of offensive cyber tools remains opaque," and requires more research.

March

The successful exploitation of new vulnerabilities was a recurring problem in March, including vulnerabilities in Cisco Adaptive Security Appliances, Cold Fusion, Drupal, Microsoft Exchange Server and the Windows kernel. Attacks on two "zero-day" vulnerabilities were mitigated among 36 patches on "Patch Tuesday." "Operation ShadowHammer" by the Chinese Winnti threat actor tampered with software updates from PC maker ASUSTeK Computer to install malware on victims' computers. Aluminum manufacturer Norsk Hydro was attacked with LockerGoga ransomware. Citrix disclosed a data breach after the FBI warned them the attackers probably used a password spraying attack to gain a foothold. We collected intelligence about three separate campaigns targeting point-of-sale systems.

54 Thanks to David M. Kennedy from the VTRAC for this contribution.

April

Pharmaceutical company Bayer announced it had prevented an attack by the Winnti threat actors targeting sensitive intellectual property. The Indian IT services giant Wipro was breached in order to attack its customers. The ultimate aim of the group behind the attack appeared to be gift-card fraud. The Vietnam-aligned APT32 (Ocean Lotus) actor targeted foreign automotive companies to acquire IP. The U.S. Department of Energy reported grid operators in Los Angeles County, California, and Salt Lake County, Utah, suffered a DDoS attack that disrupted their operations, but did not cause any outages. The US-CERT warned that multiple VPN applications store the authentication and/or session cookies insecurely in memory and/or log files. Cisco, Palo Alto Networks, F5 Networks and Pulse Secure products were affected. A new DNS hijacking campaign, "Sea Turtle," was discovered targeting private and public organizations primarily located in the Middle East and North Africa.

May

Patch Tuesday in May included patches for CVE-2019-0708, a vulnerability in Remote Desktop Protocol that was nicknamed "BlueKeep." A hue and cry to patch so as to avoid an imminent WannaCry-like worm went hyperbolic. The City of Baltimore, Maryland, was paralyzed by RobbinHood ransomware. A new ransomware, "Sodinokibi" appeared to be spreading from unpatched Oracle WebLogic servers. Magecart groups continued to deploy payment card scraping scripts. They expanded their targeted platforms beyond Magento to the PrismWeb and OpenCart e-commerce platforms. A vulnerability in Magento patched in March became the target of mass scanning and SQLinjection attacks.

June

LabCorp disclosed that a breach at a third-party billing collections firm exposed the personal information of 7.7 million Americans. Chinese intelligence services hacked into the Australian National University to collect data they could use to groom students as informants before they were hired into the civil service. U.S. grid regulator NERC issued a warning that Xenotime, a major hacking group with suspected Russian ties, was conducting reconnaissance into the networks of electrical utilities. "Operation Soft Cell" ran over the course of seven years by the APT10 Chinese espionage actor. They hacked into 10 international mobile phone providers operating across 30 countries to track dissidents, officials and suspected spies. The operators behind GandCrab ransomware announced they were shutting down. Most analysts assessed they were simply shifting from GandCrab to Sodinokibi.

July

Capital One revealed a hacker accessed data on 100 million credit card applications, including Social Security and bank account numbers. Improperly secured Amazon cloud storage was at the heart of the theft of 30 GB of credit application data by a single subject. Microsoft revealed that it had detected almost 800 cyberattacks over the past year targeting think tanks, non-governmental organizations and other political organizations around the world, with the majority of attacks originating in Iran, North Korea and Russia. Several major German industrial firms, including BASF, Siemens and Henkel, announced that they had been the victim of a state-sponsored hacking campaign by the Chinese Winnti group.

August

On Friday, August 16, 22 Texas towns were infected with Trickbot followed by Sodinokibi ransomware after attackers breached their managed service provider (MSP), TSM Consulting, and employed the MSP's ConnectWise Control remote management tool to distribute the malware. The following week, malware researchers observed revived activity in Emotet distribution networks. In June, the Emotet crew seemed to suspend operations. By mid-September, Emotet seemed to be fully operational. Emotet had been linked to multiple Russian threat actors, including Mummy Spider, TA542 and TA505. Emotet mal-spam had been delivering other malware payloads, including Dridex, Ursnif, Trickbot and Ryuk.

September

At the end of August and early in September, multiple sources began reporting strategic web compromises targeting Tibetan rights activists and ethnic minority Uyghurs using iOS and Android Trojans. Operation Soft Cell reported in June was probably part of this campaign. Another new Chinese APT-grade actor, APT5, emerged and was discovered attacking vulnerable VPN servers. Two zero-day Windows vulnerabilities were included in September's Patch Tuesday and before the end of the month, Microsoft released an out-of-cycle patch for a third zero-day. A breach at social video-game developer Zynga affected over 175 million players.

October

In October, the VTRAC was swamped by intelligence covering APT-grade actors, including TA505, FIN6, FIN7 and RTM cybercrime actors. FIN4, FIN6 and Carbanak were linked to different Magecart groups. Intelligence was received on cyber-espionage and cyber-conflict actors included Charming Kitten, Turla, Winnti and APT29 actors. We learned of a September attack on India's Kudankulam Nuclear Power Plant (KNPP) by the Lazarus group. The attack did not affect either the nuclear power plant control system or the electricity-generating power plant control system. A new spin on business email compromises emerged and was dubbed "Vendor Email Compromises."

November

Facility services company Allied Universal suffered a Maze ransomware infection. The miscreants demanded about US$2 million in bitcoin and threatened to release 5 GB of stolen internal files if they weren't paid. They did release at least 700 MB. Before the end of the year, criminals behind at least four ransomware families had begun to exfiltrate internal files before triggering file encryption. They threatened to make the data public to add leverage on the victims to pay. The Iranian APT33 had been targeting industrial control system (ICS) equipment that is used in oil refineries, electrical utilities and manufacturing.

December

The U.S. government warned of malicious spam-spreading Dridex banking Trojans that were used to gain a foothold to infect networks with BitPaymer ransomware. Petróleos Mexicanos (Pemex) was the victim of DoppelPaymer, a variant of Dridex and BitPaymer. One of 36 vulnerabilities Microsoft patched was being exploited in watering-hole attacks before December's Patch Tuesday. Microsoft released another out-of-cycle security bulletin and patch for a SharePoint vulnerability that was being exploited in the wild. The Gallium threat actor was linked to Operation Soft Cell and the watering-hole attacks on Tibetans and Uyghurs.

07 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 that 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. In order to continue to increase the transparency of our work, we introduced a couple of new features we are including in the report this year.

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://enterprise.verizon.com/resources/reports/dbir/2020/report-corrections/

Second, we check our work. The same way the data behind the DBIR figures can be found in our GitHub repository,[55] for the first time we're also publishing our fact-check report there as well. It's highly technical, but for those interested, we've attempted to test every fact in the report.[56]

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 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 confidence in this grows as we gather more data and compare it to that of others), bias undoubtedly exists.

While we may not be perfect, we believe we provide the best obtainable version of the truth and a useful one at that. Please review the "Acknowledgement and analysis of bias" section below for more details on how we do that.

The DBIR process

Our overall process remains intact and largely unchanged from previous years. All incidents included in this report were individually reviewed and converted (if necessary) into the VERIS framework to create a common, anonymous aggregate dataset. If you are unfamiliar with the VERIS framework, it is short for Vocabulary for Event Recording and Incident Sharing; it is free to use and links to VERIS resources that 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 contributors using VERIS
3. Converting contributors' existing schema into VERIS

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

Reviewed spreadsheets and VERIS WebApp JavaScript Object Notation (JSON) are ingested by an automated workflow that converts the incidents and breaches 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 contributors providing the data, the data is cleaned and reanalyzed. This process runs nightly for roughly three months as data is collected and analyzed.

55 https://github.com/vz-risk/dbir/tree/gh-pages/2020
56 Interested in how we test them? Check out Chapter 9, Hypothesis Testing, of ModernDive: https://moderndive.com/9-hypothesis-testing.html

Incident data

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

Another important point is that when looking at the findings, "Unknown" is equivalent to "unmeasured." Which is to say that if a record (or collection of records) contain 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 no information. Because they are "unmeasured," they are not counted in sample sizes. The enumeration "Other" is, however, counted as it means the value was known but not part of VERIS or not included, as is the case with "top" figures. Finally, "Not Applicable," (normally "NA"), may be counted or not counted depending on the hypothesis.

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

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

Incident eligibility

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

The details of what is a "quality" incident are:

1. 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
2. The incident must have at least one known VERIS threat action category (hacking, malware, etc.)

In addition to having the level of details necessary to pass the quality filter, the incident must be within the time frame of analysis (November 1, 2018, to October 31, 2019, for this report). The 2019 caseload is the primary analytical focus of the report, but the entire range of data is referenced throughout, notably in trending graphs.[57] We also exclude incidents and breaches affecting individuals that cannot be tied to an organizational attribute loss. If your friend's laptop was hit with Trickbot, it would not be included in this report.

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

57 Our line figures use the calendar year the incident occurred in as they are continuous, while our dumbbell charts use the year of the DBIR report, as they are ordinal.

Figure 135. Individual contributions per Action

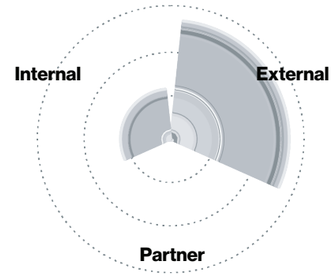


Figure 136. Individual contributions per Actor

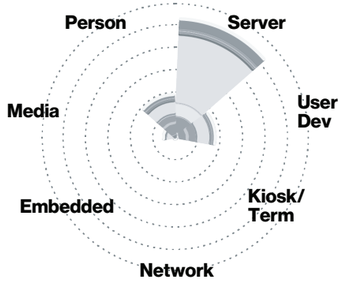


Figure 137. Individual contributions per Asset

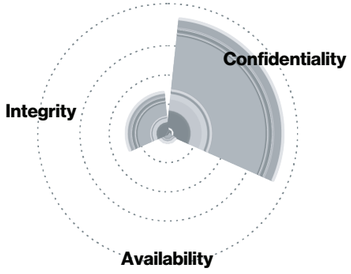


Figure 138. Individual contributions per Attribute

Acknowledgement and analysis of bias

Many breaches go unreported (though not in our sample). 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.[58] Unfortunately, this process introduces bias.

The first type of bias is random bias introduced by sampling. This year, our maximum confidence is +/-1.5%[59] for incidents and +/-0.5% 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 conditional probability bar charts (the "slanted" bar charts) that we have been using since the 2019 report.

The second source of bias is sampling bias. We strive for "the best obtainable version of the truth"[60] by collecting breaches from a wide variety of contributors. Still, it is clear that we conduct biased sampling. For instance, some breaches, such as those publicly disclosed, are more likely to enter our corpus, while others, such as classified breaches, are less likely.

The four figures at left are an attempt to visualize potential sampling bias. Each radial axis is a VERIS enumeration and we have stacked bar charts representing our data contributors. Ideally, we want the distribution of breaches to be roughly equally divided between contributors in the stacked bar charts along all axes. Axes only represented by a single source are more likely to be biased. However, contributions are inherently thick tailed, with a few contributors providing a lot of data and many 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 axes.

You'll notice a rather large single contribution on many of the axes. While we'd generally be concerned about this, it represents a contribution aggregating several other sources, so not an actual single contribution. 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 both exploratory analysis as well as hypothesis testing, we inherently test our hypotheses on the same data we used to make them. Until we develop a good collection method for data breaches or incidents from Earth-2 or any of the other Earths in the multiverse,[61] 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.[62] 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 (as called out in the relevant sections). 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 separately analyzed the last three 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 earlier and excludes the aforementioned two subsets.

Non-incident data

Since the 2015 issue, the DBIR includes data that requires the analysis that did not fit into our usual categories of "incident" or "breach." Examples of non-incident data include malware, patching, phishing, 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.

58 Interested in sampling? Check out Chapter 7, Sampling, of ModernDive: https://moderndive.com/7-sampling.html
59 This and all confidence intervals are 95% confidence intervals determined through bootstrap simulation. Read more in Chapter 8, Bootstrapping and Confidence Intervals, of ModernDive: https://moderndive.com/8-confidence-intervals.html
60 Eric Black, "Carl Bernstein Makes the Case for 'the Best Obtainable Version of the Truth,'" by way of Alberto Cairo, "How Charts Lie" (a good book you should probably read regardless)
61 The DBIR is a pre-Crisis on Infinite Earths work environment.
62 A unique finding is more likely to be something mundane (such as a data collection issue) than an unexpected result.

Appendix B: VERIS Common Attack Framework (VCAF)

VERIS was developed as a solution to the need for consistent definitions of incident and breach data for analysis.

With its close ties to the DBIR and data analysis, it was created to remove the ambiguity inherent in terms surrounding breaches and provide a data-driven structure capable of quantifying the majority of breaches. While VERIS covers a lot of different detailed information about an incident, including things such as Victim demographics and Timeline, the core of VERIS is captured in what we call the four "A's" of an incident: Actor, Action, Asset, Attribute.

However, VERIS was not designed to represent precise and detailed tactical and technical minutiae around attackers' techniques, chosen methods of persistence or methodology for executing malicious code on a compromised asset. Thankfully, it doesn't need to because there is something else that has come along to help address that need.

Massive (adoption of) ATT&CK

MITRE privately developed the original Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework starting in 2013 as a means of codifying adversarial behavior and released it publicly in 2015.[63] ATT&CK has become a well-established way for describing the tactical actions used by attackers (including a heavy focus on advanced threats). Much like VERIS, ATT&CK is subdivided into a handful of key components, but the core of the framework are the "Techniques," which describe the atomic means of how an attacker achieves an objective called a "Tactic." The 260+ Techniques in ATT&CK for Enterprise are logically grouped with their corresponding 11 Tactics, which describe the different objectives an adversary might take as part of their intrusion.

We're better when we're together.

While both VERIS and ATT&CK grew out of different needs and different objectives, VERIS to codify incidents and ATT&CK to codify adversary technique, there is without a doubt an overlap between the two that could be leveraged to improve the value of both standards. To get a better understanding of the relationships between these two frameworks, the team spent some time researching to see if they could map the VERIS framework to the ATT&CK techniques and vice-versa, the results of which you can see in Figure 139.

What is this, a crossover episode?

Our solution to bridge the gap and help operationally connect the relationships between ATT&CK and VERIS is through the creation of an extension that we call the VERIS Common Attack Framework (VCAF).

VCAF serves as a bridge to ATT&CK, covering the portions of VERIS not in ATT&CK with the aim of creating a holistic framework. At its very core, VCAF is made of two components: one is the conceptual mapping between VERIS and ATT&CK, and another is the extension of ATT&CK with techniques that cover all possible Threat Actions present in VERIS. As much as we would have liked to leverage a default "meteor falling from the sky" technique in ATT&CK, those events are definitely quite rare.[64]

This approach should be flexible enough to accommodate both general categories found in VERIS (such as Ransomware) and some of the more specific attack types found either in VERIS or ATT&CK. Aside from expanding the scope of what is covered and can be tracked, using VCAF can help provide essential context to these incidents. Below is a list that includes a variety of the different benefits of leveraging this powerful combination:

- Understand the technical details associated with an incident
- Prioritize mitigations based on previous all incident types (not just the malware or hacking kind)
- Better understand the junction of targeting and capabilities
- Capture incident context that goes beyond technical artifacts
- Ease communication of cybersecurity concepts with non-cybersecurity experts

63 https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf
64 But they sure have a large impact!

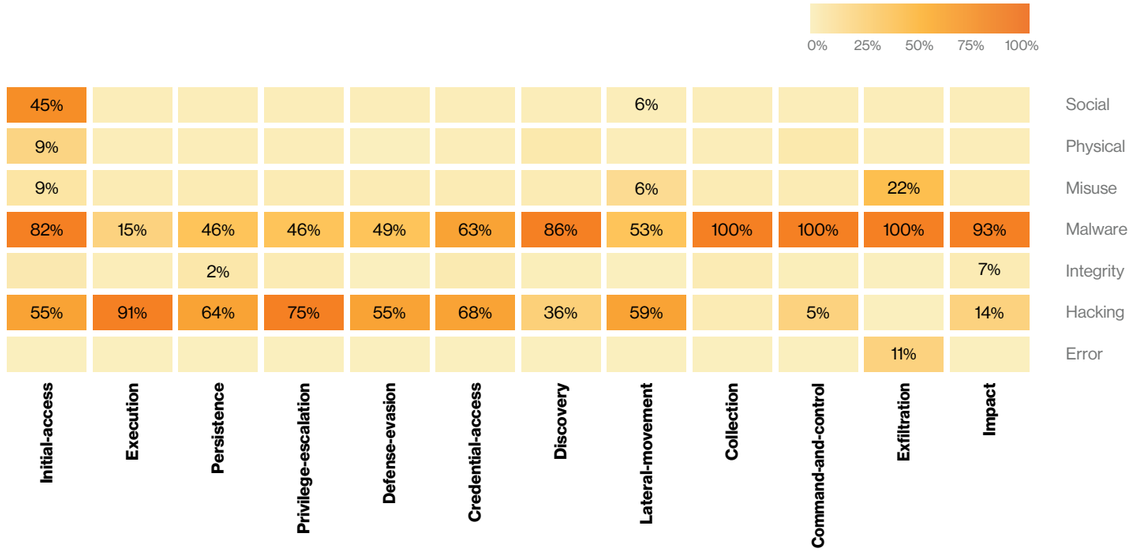


Figure 139. Percentage of MITRE Techniques covered by VERIS

In this issue of the DBIR, we used VCAF to map simulated breach data, SIEM data and malware features to VERIS action categories to compare and draw conclusions in conjunction with our incident corpus.

The beginning of something great

Clearly, VCAF is not the end-all be-all of cybersecurity frameworks. It is a modest step toward having an integrated way for the community to discuss security incidents and attackers. As the number of cybersecurity frameworks grows and the field of knowledge surrounding cybersecurity topics deepens, there is a need for us as a community to integrate our own languages and understanding in an effort to help us communicate to the larger community of non-cybersecurity experts. Keep your eyes peeled for future developments and information on VCAF by visiting[65] our VERIS GitHub page at https://github.com/vz-risk/veris.

65 And don't forget to smash that like and subscribe button!

Appendix C

Michael D'Ambrosio
Assistant Director
U.S. Secret Service

Jonah Force Hill
Senior Cyber Policy Advisor
U.S. Secret Service

Following the money—the key to nabbing the cybercriminal

This year's DBIR has once again highlighted the principal motive for the vast majority of malicious data breaches: the pursuit of profit. This is surprising to some, given the extensive media coverage of national security-related breaches. However, it should not be. Most malicious cyber actors are not motivated by national security or geopolitical objectives, but rather by simple greed. Cybercriminals primarily profit through fraud and extortion. They target financial and payment systems, steal information to use in various fraud schemes, and hold IT systems hostage through ransomware and other means. Whatever their criminal scheme, they then depend upon a money movement and laundering apparatus to transfer and liquidate their proceeds.

That is why the U.S. Secret Service was first assigned responsibility for investigating cybercrimes in the early 1980s, before it was even called "cyber," and why we continue to do so today. Secret Service agents are financial crimes investigators, skilled not only at "following the money," but at preventing criminals from profiting from their activities and at recovering the stolen assets of victims. When investigating any criminal cyber incident, a data breach, an "unlimited ATM cash-out" conspiracy, a ransomware attack or any other diverse, financially motived crime committed via the internet, the heart of the Secret Service's approach is following the money.

We have learned over the decades that it is through the movement of funds—from the victim to the criminal, between and among criminals, and through the process of money laundering—that investigators are able to generate the greatest insights and criminal leads. Malware samples and indicator sharing are useful, no doubt, but it is the money and where it moves that leads to arrests, asset seizures and the recovery of assets stolen from victims of fraud.

For example, in a typical business email compromise (BEC) scheme, a victim is lured into sending a payment, usually via a wire transfer, to a bank account maintained under a criminal's control. The methods used in the deception part of the crime can range from highly sophisticated (such as deploying tailor-made malware) to shockingly simple (such as impersonating a vendor on the phone). How the fraudsters fool the victim is often insignificant; what is important is how they move and liquidate their proceeds.

Smart criminals understand this. They know that the accounts, shell companies and processes they use to move their stolen funds contain a wealth of location data and other information that can lead to their arrest. As a result, criminals try to distance themselves and their identities from all accounts and institutions that might be associated with their crimes.

There are number of ways criminals do this, but one of the principal mechanisms is the use of "mules," outside individuals recruited to participate in the scheme. Mules can be either witting or unwitting participants. Some mules join the scheme with full knowledge of the criminal nature of their involvement; others are recruited through what appear to be legitimate job postings. Still others are victims themselves of ancillary frauds, often romance scams, in which they are conned into believing that they are sending money to a romantic partner, when in fact they are just moving money for crooks.

A similar dynamic exists in cases of ransomware and in other crimes in which cryptocurrencies play a role. When an organization pays a ransom to unlock its IT systems, for instance, the criminal generally instructs the victim to send a bitcoin payment to a cryptocurrency wallet. These wallets are hosted either on a cryptocurrency exchange, which can be either legitimate or illegitimate, or on a device operated by the criminal or an associate. Here too, the criminals seek to obscure the location of the wallets and to limit access to any other information that might tie their activities to a specific wallet or account.

Criminals engaged in ransomware attacks employ many of the same techniques as BEC scammers to cover their tracks. They may pay mules to set up crypto wallets, or con unwitting mules into thinking they have landed a legitimate job in the cryptocurrency industry. They may use cryptocurrency tumblers and mixers to swap funds from one form of cryptocurrency to another (for instance, from bitcoin to ether), to keep law enforcement from tracking their movements on the blockchain. They may set up shell companies, open overseas bank accounts and move money repeatedly from one country to the next, all with the aim of making their financial movements as difficult as possible to trace.

Yet there is always a chokepoint. If cybercriminals want to enjoy the fruit of their criminal labor, they must convert their profits into a form of money they can actually use, without being tracked by law enforcement. These chokepoints create the greatest opportunities to counter cybercriminal activity.

The Secret Service focuses on these chokepoints to disrupt these financial flows, whether they are explicitly illicit services or legitimate businesses that are exploited by criminals. Through undercover operations, confidential informants and partnerships with industry and the broader law enforcement community, the Secret Service excels at identifying and interdicting these illicit financial flows. In 2019, the Secret Service prevented $7.1 billion of cybercrime losses and returned over $31 million in stolen assets to victims of fraud.

The lessons for industry are simple: Invest in the defense of your networks and, in the event of a breach, collect as much evidence as you can. When shared with law enforcement partners, that evidence can lead not only to the arrest of the criminal, but also to the seizure of their assets. In many cases, the recovered money can be returned to the victim. This is how we prevent cybercriminals from operating with impunity. It is a collective struggle. Let's work together.

Appendix D

Diego Curt
Chief Compliance Officer
State of Idaho, Office of the Governor—Information Technology Services

State of Idaho enhances incident response program with VERIS.

We hear it all the time. We need to share incident and breach information for improved decision-making. The State of Idaho was facing the same issue, trying to get different agencies to share incident and breach information for improved decision-making and better cyber-defense investment. In order to address this, the State of Idaho designed a program that gained approval from various stakeholders, including the legal department. The program consists of two fundamental components and three core components.

The two fundamental components are:

1 **Cyber Kill Chain®[66] developed by Lockheed Martin, Inc.**—used to promote actionable intelligence-process thinking and serves as a blueprint for building an effective cybersecurity program

2 **National Institute of Standards and Technology (NIST) Cybersecurity Framework[67]**—a risk reporting framework used to assess the readiness and maturity of cybersecurity controls throughout the enterprise

The three core components of the program are:

1 **NIST SP 800-53[68] Incident Response Control Family**—used to govern and ensure all control processes are addressed and matured on a continuous basis

2 **Vocabulary for Event Recording and Incident Sharing (VERIS)**—an easy-to-use, systematically structured language/taxonomy used to gather intelligence from incidents and breaches for better decision-making and information sharing

3 A commercial web-based application that brings together first responders, emergency management, National Guard, cyber-incident response handlers, etc., into one platform that houses the VERIS language/taxonomy

66 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
67 https://www.nist.gov/cyberframework
68 https://nvd.nist.gov/800-53

At the heart of the program is the VERIS taxonomy. VERIS is a language/taxonomy designed to help an organization hurdle over the issues many organizations are concerned about—sharing confidential data with outsiders. Without the capability to incorporate a common language (VERIS) designed to share incident information, the State of Idaho would never have been able to gain approval from various stakeholders (including the legal department) to share incident and breach information both internally (other agencies) and externally (DHS, FEMA, etc.).

Some of the areas in which VERIS has helped improve the State of Idaho's ability to share information are:

- It has created awareness and interest that there is a better way to gather and use intelligence information from adverse events that we respond to from time to time
- It is an open source framework that works well with other incident response frameworks
- It is an easy-to-use full-schema taxonomy/language designed to be incorporated and implemented within a short period of time
- It provides a way for business executives to get involved with their organization's cybersecurity efforts and simplifies intelligence gathering by repetitively asking four basic questions: Whose actions affected the asset? What actions affected the asset? Which asset was affected? How was the asset affected?

VERIS provides a solid language foundation that can be used to build a strong intelligence-driven incident response program. Couple that with other open source frameworks and you have one heck of an incident response program.

Appendix E: Contributing organizations

A

Akamai Technologies

Apura Cyber Intelligence

AttackIQ

Australian Federal Police

B

BeyondTrust

Bit Discovery

Bit-x-bit

BitSight

C

Center for Internet Security

CERT European Union

CERT Insider Threat Center

CERT Polska

Check Point Software Technologies Ltd.

Chubb

Cisco Talos Incident Response

Coalition (formerly BinaryEdge)

Computer Incident Response Center Luxembourg (CIRCL)

CrowdStrike

Cybercrime Central Unit of the Guardia Civil (Spain)

CyberSecurity Malaysia, an agency under the Ministry of Science, Technology and Innovation (MOSTI)

D

Defense Counterintelligence and Security Agency (DCSA)

Dell (formerly EMC-CIRC)

DFDR Forensics

Digital Shadows

Dragos, Inc.

E

Edgescan

Elevate Security

Emergence Insurance

F

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

Financial Services Information Sharing and Analysis Center (FS-ISAC)

G

Government of Telangana, ITE&C Dept., Secretariat

Government of Victoria, Australia—Department of Premier and Cabinet (VIC)

GreyNoise

H

Hasso-Plattner Institut

Hyderabad Security Cluster

I

ICSA Labs

Irish Reporting and Information Security Service (IRISS-CERT)

J

JPCERT/CC

K

Kaspersky Lab

KnowBe4

L

Lares Consulting

LMG Security

M

Malicious Streams

Micro Focus (formerly Interset)

Mishcon de Reya

mnemonic

Moss Adams (previously AsTech Consulting)

MWR InfoSecurity

N

National Cybersecurity and Communications Integration Center (NCCIC)

NetDiligence

NETSCOUT

P

Paladion Networks Pvt Ltd.

Palo Alto Networks

ParaFlare Pty Ltd

Proofpoint (formerly Wombat Security)

Q

Qualys

R

Rapid7

Recorded Future

S

S21sec

SecurityTrails

Shadowserver Foundation

Shodan

SISAP—Sistemas Aplicativos

SwissCom

T

Tetra Defense (formerly Gillware Digital Forensics)

Tripwire

U

United States Computer Emergency Readiness Team (US-CERT)

U.S. Secret Service

V

VERIS Community Database

Verizon Cyber Risk Programs

Verizon DDoS Shield

Verizon Digital Media Services

Verizon Managed Security Services—Analytics (MSS-A)

Verizon Network Operations and Engineering

Verizon Professional Services

Verizon Threat Intelligence Platform Service (VTIPS)

Vestige, Ltd.

VMRay

W

Wandera

WatchGuard Technologies

Z

Zscaler