2017 Data Breach Investigations Report

10th Edition

verizon

Tips on Getting the Most from This Report

In the 2009 report, we wrote:

"These findings relate specifically to the occurrence (likelihood) of security breaches leading to data compromise ... not attacks, not impact, not general security incidents and not risk."

The study has since evolved to include security incidents and not just breaches for many findings, but the rest of the statement holds true to this day. The information, provided in aggregate, is filtered in many ways to make it relevant to you (e.g., by industry, actor motive). It is a piece of the information security puzzle – an awesome corner piece that can get you started – but just a piece nonetheless. The rest is filled in by you. You (hopefully) know the controls that you do or do not currently have to mitigate the effectiveness of the threat actions most commonly taken against your industry. You know the assets that store sensitive data and the data flow within your environment. If you don't – get on that. You also know your own incident and data-loss history. Use your own knowledge combined with the data from our report; they complement each other.

First-time reader?

Don't be shy – welcome to the party. As always, this report is comprised of real-world data breaches and security incidents – either investigated by us or provided by one of our outstanding data contributors.

The statements you will read in the pages that follow are data-driven, either by the incident corpus that is the foundation of this publication, or by non-incident datasets contributed by several security vendors.

We combat bias by utilizing these types of data as opposed to surveys, and collecting similar data from multiple sources. We use analysis of non-incident datasets to enrich and support our incident and breach findings. Alas, as with any security report, some level of bias does remain, which we discuss in Appendix D.

Incidents vs breaches

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.

VERIS resources

VERIS is free to use and we encourage people to integrate it into their existing incident response reporting, or at least kick the tires.

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.

Cybercrime case studies

This report doesn't focus on individual events – if you want to dive deeper into breach scenarios check out the cybercrime case studies collected in the Verizon Data Breach Digest[1]. This is a collection of narratives based on real-world investigations and from the perspective of different stakeholders involved in breach response.

Read now >

[1] http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/

Contents

Hope is the pillar of the world

– Pliny the Elder

Welcome to the 10th anniversary of the Data Breach Investigations Report (DBIR). We sincerely thank you for once again taking time to dig into our InfoSec coddiwomple that has now culminated in a decade of nefarious deeds and malicious mayhem in the security world. 2016 was an extremely tumultuous year, both in the United States and abroad. Political events, such as a divisive presidential election and the United Kingdom European Union membership referendum (aka Brexit), raised many a blood pressure reading, while memes focused on getting through the year without the loss of another beloved celebrity flooded social media. Despite the tumult and clamor, cybercrime refused to take a year off, and added to the feelings of uncertainty with numerous breaches being disclosed to the public – thereby debunking the "no such thing as bad publicity" myth.

Why the "hope" quote you ask? Isn't this report about doom and gloom and when things go wrong with real-world consequences? There is no doubt that you can view this report, throw up your arms in despair, and label us (the risk management and information security community) as "losing." All of us (authors, analysts and readers alike) must take a realistic approach to this and similar reports by our peers and acknowledge that we can do better. Yet we do firmly believe there is great cause for hope.

It is true that the DBIR will never be blank as – choose your cliché – "there is no such thing as 100% secure" or "perfection is the enemy of good enough". It is also true that due to the nature of the report we admittedly have a lack of success stories. After all, this is at its core a report about confirmed data breaches. However, we are aware that there are numerous success stories out there – it is not all bad news for the good guys. Our hope comes from the fact that we have been able to present these findings to the public for 10 years running. Our hope comes from how we have grown this publication from only one organization to include contributions from 65 sources, providing a solid corpus sample of security incidents and data breaches from which to learn.

Our hope is that while this report will not be able to definitively answer the macro-level question of "are we getting better?" you the readers, can leverage the combined efforts (thank you again data contributors!). Use the results of this study as a platform to improve your organization's awareness of tactics used by the adversary, to understand what threats are most relevant to you and your industry, and as a tool to evangelize and garner support for your information security initiatives.

So what is new in the 2017 publication? One of our favorite evolutions in the DBIR series was the definition of nine incident classification patterns and the ability to map them against industry. We felt, and still feel, that it was a boost that made the DBIR more actionable. The report goes one step further this year and includes sections that are specific to key industries. These sections dive deeper into who targets specific verticals, how they go about reaching their goal and discuss why particular industries are in the crosshairs of certain threat actors. We examine what is unique about each industry and how that influences the results we find in our dataset. It is our hope (there's that word again) that these industry sections will resonate with the security professionals and will provide a lens into our data that is beneficial to you personally.

So the report will follow this path: It starts off with an executive summary comprised of high-level findings in this year's data. As in other reports, we will then look back into history and discuss what has (and hasn't) changed over the years. Next, we will hop to the aforementioned industry sections, and then focus on the human element in information security and this ransomware thing all the kids are talking about. The nine incident classification patterns make their annual appearance, and we will wrap this party up with a review of the good, the bad and the ugly of 2016.

Executive Summary

Who's behind the breaches?

75% perpetrated by outsiders.

25% involved internal actors.

18% conducted by state-affiliated actors.

3% featured multiple parties.

2% involved partners.

51% involved organized criminal groups.

What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

Who are the victims?

24% of breaches affected financial organizations.

15% of breaches involved healthcare organizations.

12% Public sector entities were the third most prevalent breach victim at 12%.

15% Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66% of malware was installed via malicious email attachments.

73% of breaches were financially motivated.

21% of breaches were related to espionage.

27% of breaches were discovered by third parties.

Breach Trends

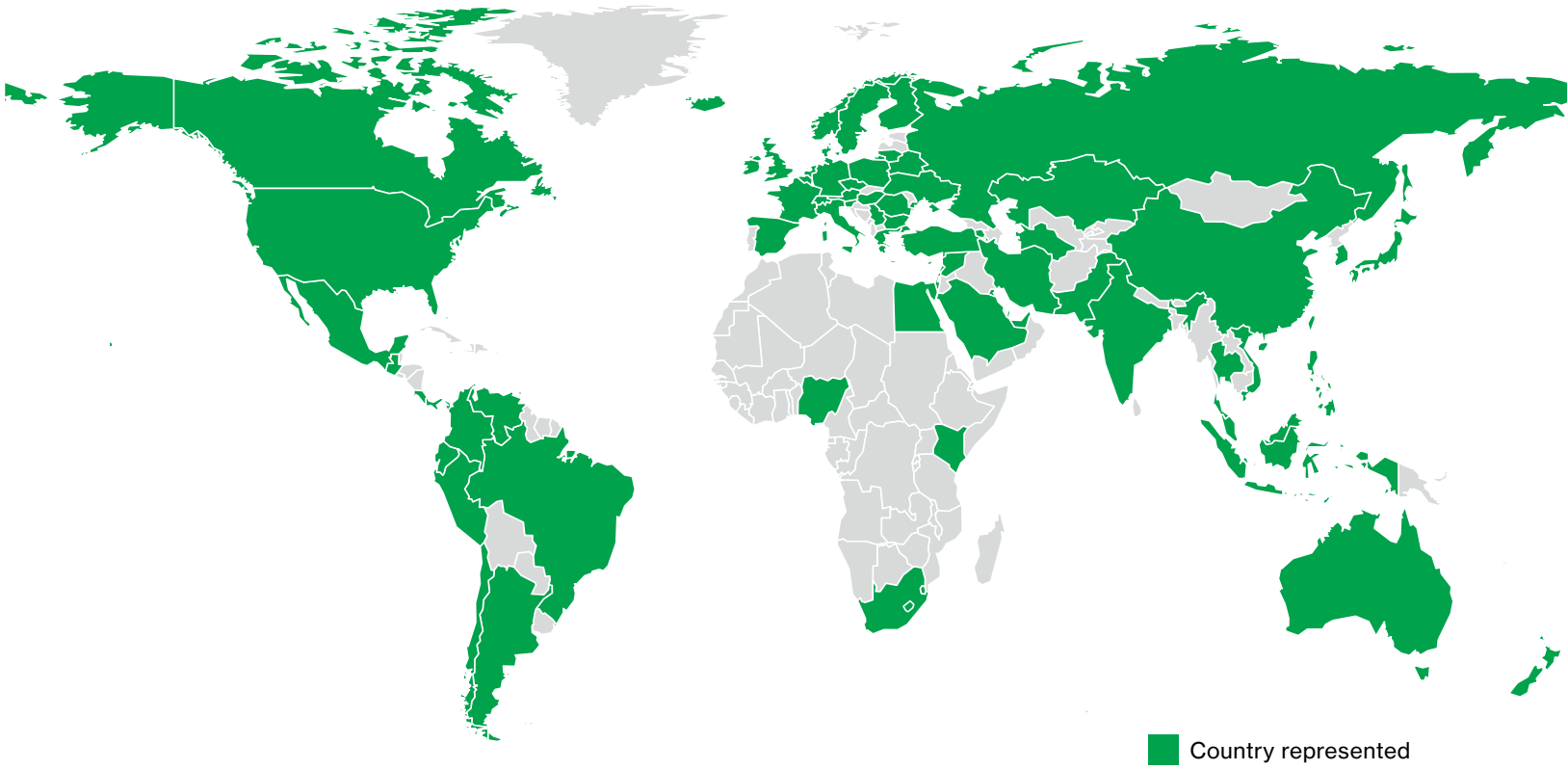


Figure 1: Countries represented in combined caseload

In 2014, we pointed out that “we’re not very good at maintaining the status quo. The sources of data grow and diversify every year. The focus of our analysis shifts. The way we visualize data and organize results evolves over time.” There are changes, both in addition and subtraction, of external organizations that are able to provide data year to year (as well as shifts in the types of incidents investigated by the community). These can influence the results as much, if not more, than changes in threat actor behavior.

We will disclose when changes or findings of interest are a product of the former. For example, a spike in data received associated with Dridex botnet breaches in last year’s report was responsible for several spikes in certain enumerations. This year we will see many of those come down to levels seen in prior years.

However, in 2014 we also said “measuring deltas has value and we know readers appreciate some level of continuity between reports.” And this section is an attempt to do so.

Figure 2 shows a downtick in the percentage of breaches involving external actors, which causes a corresponding increase in internal actors. In absolute numbers, however, breaches driven by internal parties have remained relatively constant, with an increase of around 12%.

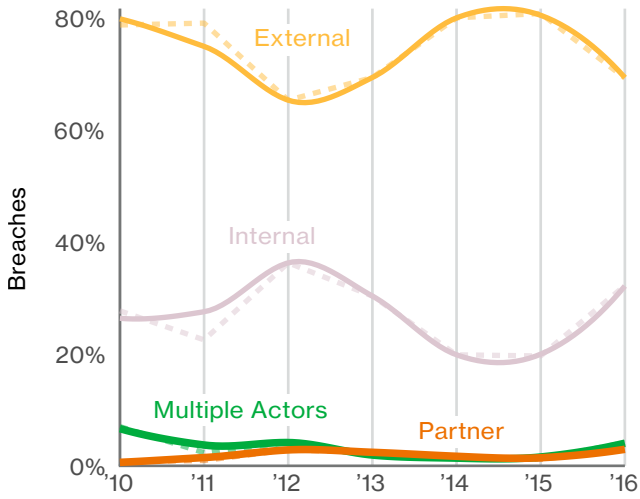


Figure 2: Threat actor categories over time

In other words, we will not be making any proclamations about internal threats on the rise and would not bet the farm that this line will continue to trend upward. The convergence of the two lines in 2016 is due to a decrease of two types of external attack that commonly feature a high actor-to-victim ratio: password-stealing botnets and opportunistic point-of-sale (POS) intrusions. Breaches involving multiple parties and/or business partners[2] exist but are much less frequent and have maintained their lower profile year to year.

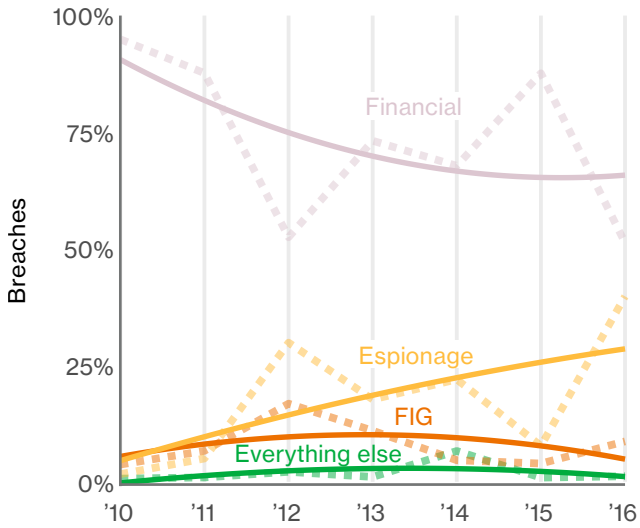


Figure 3: Threat actor motives over time

In 2016, financial and espionage were still the top two motives combining to account for 93% of breaches. Fun, Ideology and Grudge are motives we have combined and labeled as FIG in Figure 3, and other graphs throughout the report. The rise in espionage is partially due to the simple fact that we featured more of these breaches in our dataset this year, but also due to the previously discussed drop in banking Trojan botnets and POS. Organized criminal groups continue to utilize ransomware to extort money from their victims, and since a data disclosure in these incidents is often not confirmed, they are not reflected in Figure 3.

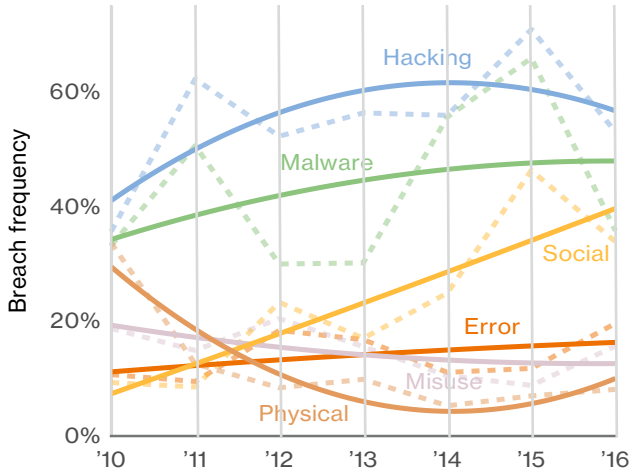


Figure 4: Percentage of breaches per threat action category over time

For many of us, 2016 was a year in which we were afraid to even accept dinner invitations due to the fear that someone would demand we discuss current events. So much upheaval and change on a global scale is difficult to take in. For that reason, Figure 4 above is oddly comforting. The triple threat of hacking, malware and social has been on top and trending upward for the last few years, and it does not appear to be going away any time soon. It represents a potent mixture for cyber-attacks, but at least it is something we can all agree on. We actually did see a decrease in numbers of these three actions in this year's dataset, due (yet again) to the reduction of POS and botnet-driven breaches.

[2] Note: for Partner to be selected as a threat actor, they need to be behind the action(s) that are causal to the breach. If a business partner is hacked and it affects an upstream organization in the chain, we still apply the actor tag to the party that is behind the hacking.

The actions taken and assets compromised are influenced heavily by the actors and their motives. Numerous areas of concentration are quickly observable in Figure 5 (e.g., use of keylogging malware by financially motivated actors).

The associations between actors, their motives, and their modus operandi are found in several industry and incident pattern sections throughout this report. The specific actors and motives represented in Figure 5 are: FIG (Fun, Ideology, Grudge motives OR activist group threat actors), ESP (Espionage motive OR state-affiliated OR nation-state actors), FIN (Financial motivation OR organized criminal group actors).

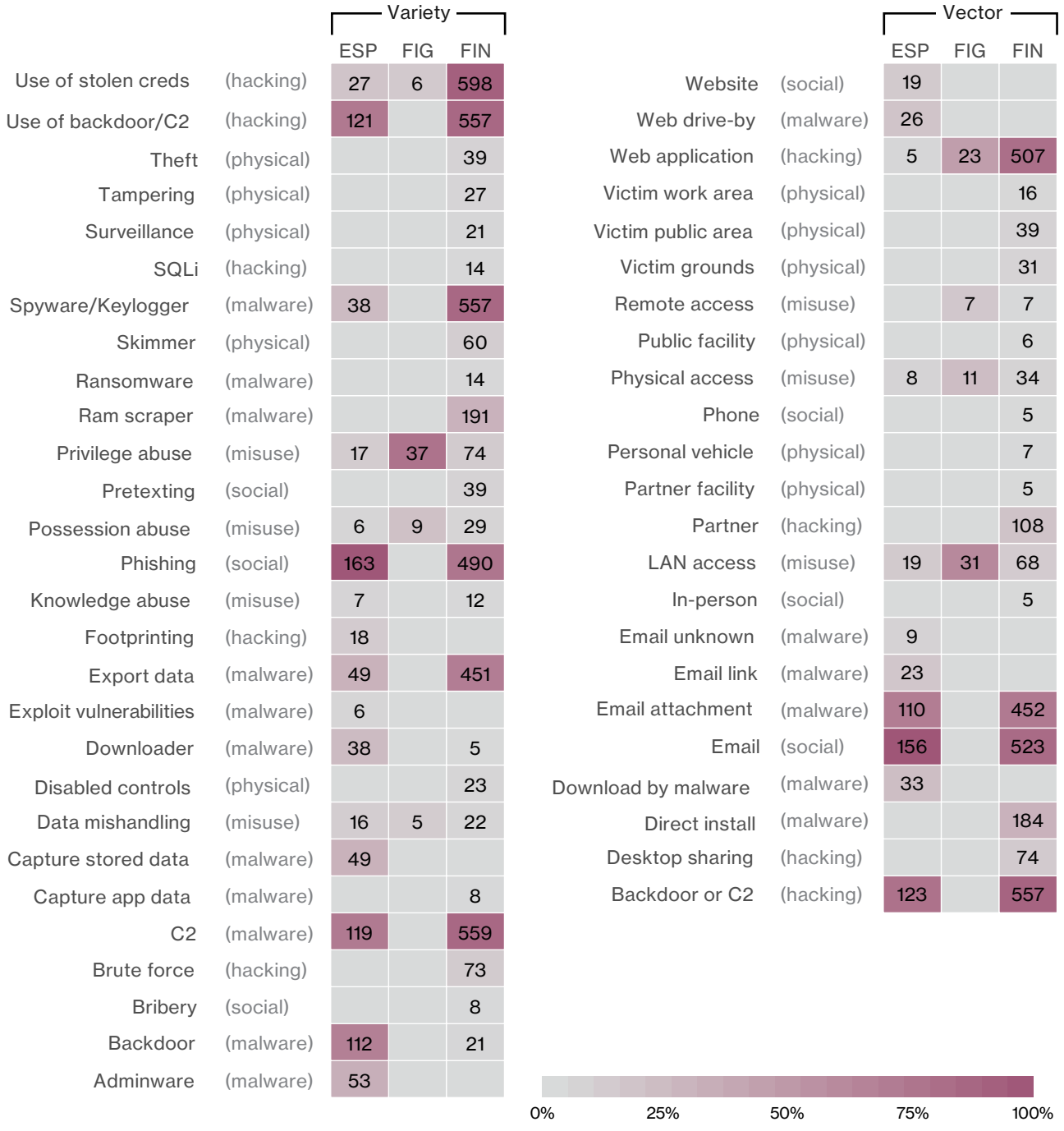


Figure 5: Action varieties and vectors by actor/motive groupings in breaches

Remember the 2011 DBIR when the number of records lost went down from 144 million to 4 million?[3] Mega-breaches of PCI data, which were front and center in prior reports, were absent that year, and didn't make a big comeback until a couple of years later. In the meantime, we began expanding our data sources – including publicly disclosed breaches – and found that million-record losses were not going away. Personal information harvested by activists from online websites and databases, then dumped to sites like Pastebin, was the biggest bounty of stolen records in the 2012 report and a sign of things to come. Keeping in mind that the numbers in Figure 6 below are aligned to the actual incident date, many were not part of the DBIR corpus until years after the initial compromise (as discovery of breaches is not an instantaneous revelation).

Fast forward to the present day and Figure 6 highlights the fact that data types that are apt to be stored in bulk have some monster numbers associated with them, with personal data and credentials totaling in the billions some years. It should be noted that some of the credentials may be hashed, and some may be salted to strengthen the encryption, but the sheer volume of records speaks … well volumes.

This year, the heavy hitters from a record-loss standpoint are from victims in the Information industry, specifically NAICS 519, which includes web portals and sites that are not online retail. Consumers are logging into a multitude of websites with single-factor authentication and providing names, addresses etc. as part of the enrollment process. When millions of people are members of a website and said site suffers a data breach, the word "newsworthy" comes to mind[4].

And we aren't trying to throw out these splashy numbers just to get folks riled up for no purpose. There are several reasons why we should at least be aware of these breaches. Obviously, if your organization has an external login for customers or members then you are not wanting for external forces that are aiming to capitalize by stealing those details. Even if you are not breached, there are armies of botnets with millions (or billions) of credentials attempting to reuse them against other sites. In other words, even though components of authentication weren't compromised from you, it doesn't mean they were not compromised. Again, if you are relying on username/email address and password, you are rolling the dice as far as password re-usage from other breaches or malware on your customers' devices are concerned. Those are two things you shouldn't have to worry about.

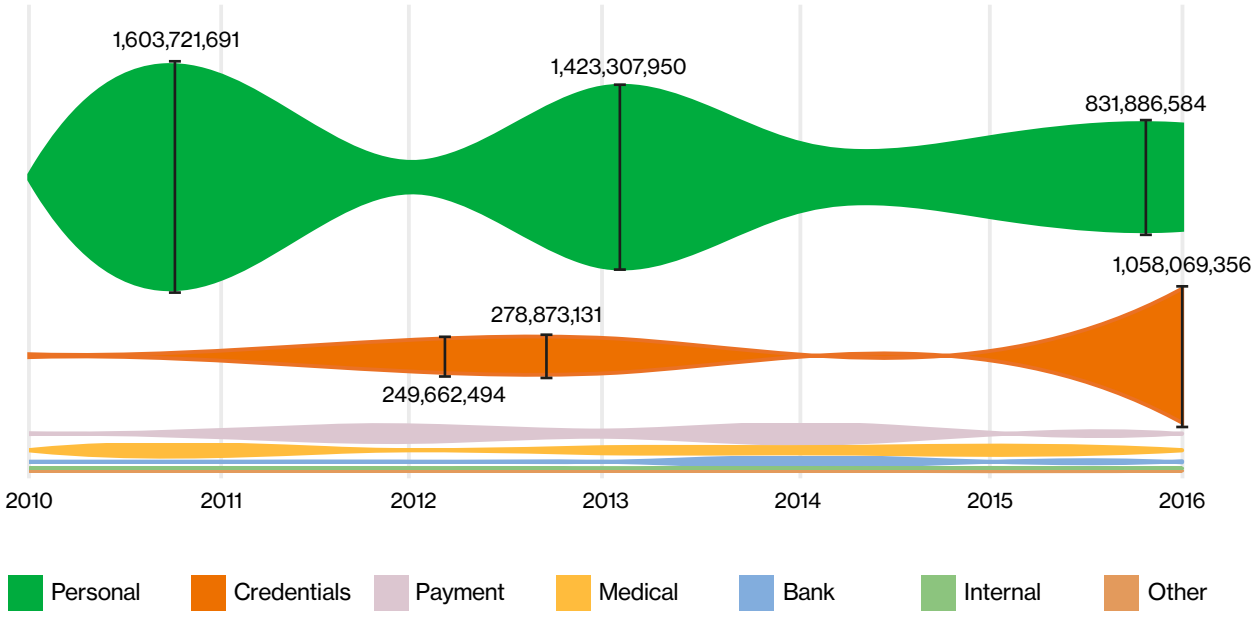


Figure 6: Number of records per data variety over time

[3] Pepperidge Farm remembers.

[4] For those that just have to know gory details, go take a look at the raw public data in the VERIS Community Database: https://github.com/vz-risk/VCDB/tree/master/data and you can read more into the individual breaches. Tactics and methods used can be found in the Information industry and Web Application Attacks pattern sections.

One of the metrics that seems to be most volatile is the method of breach discovery. Figure 7 shows that 2016 brought a sharp correction from the 2015 spike in law enforcement disclosure caused by the Dridex botnet takedown. Decreases in card skimming and POS crime sprees also influence the massive decrease in law enforcement and fraud detection. Employee notifications were the most common internal discovery method for the second straight year and there was also an uptick in detection through internal financial audits, associated with business email compromise (BEC). Third-party disclosure is up due to an increase in numbers of breaches disclosed by the affected customer or an external threat actor bragging or extorting their victims.

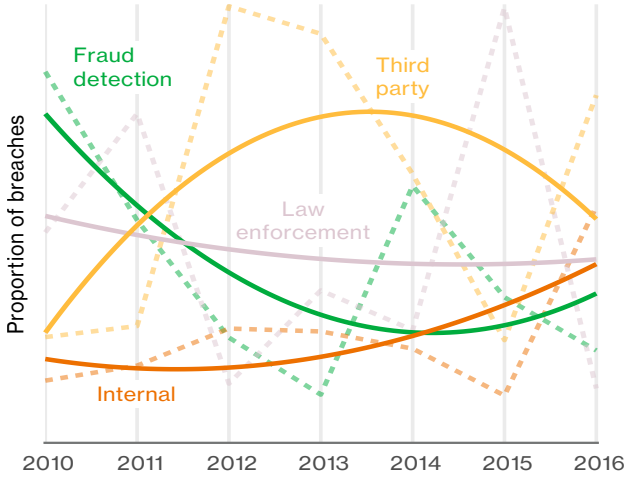


Figure 7: Breach discovery methods over time

Figure 8 examines breach timeline trends. The reduction of botnet and POS breaches results in a corresponding reduction in the number of compromises that took seconds or minutes. Even so, compromises[5] are measured in minutes or less 98% of the time.

Long-time readers might be wondering "where is the 'Detection Deficit' figure?" It compared the percentage of breaches where the time-to-compromise was days or less against the percentage of breaches where the time-to-discovery was days or less. After much thought, we determined that comparing time-to-compromise to time-to-discovery when **only looking at confirmed breaches** is unlikely to ever show any improvement. The reasons are two-fold: First, we cannot expect to see much improvement in the time-to-compromise – when the common methods of compromise work, they work quickly. When they don't, there is no compromise. Secondly, if discovery is done quickly (e.g., outbound traffic back to a C2 server is identified and blocked), then there's a much better chance that the event would be defined as an incident, not a breach, and therefore not applicable.

The increases in breaches discovered in minutes, hours, or days must be caveated with disclosing that almost two-thirds of those are associated with the Miscellaneous Errors or Physical Theft and Loss patterns. Breaches that are taking months or longer to discover in this year's dataset are likely to fall into Point of Sale Intrusions, Privilege Misuse, Everything Else or Cyber-Espionage.

To turn this somber story into a catalyst for action, track these metrics internally. Focus on increasing time-to-exfiltration and lowering time-to-discovery. By so doing, hopefully you can stop incidents from becoming breaches.

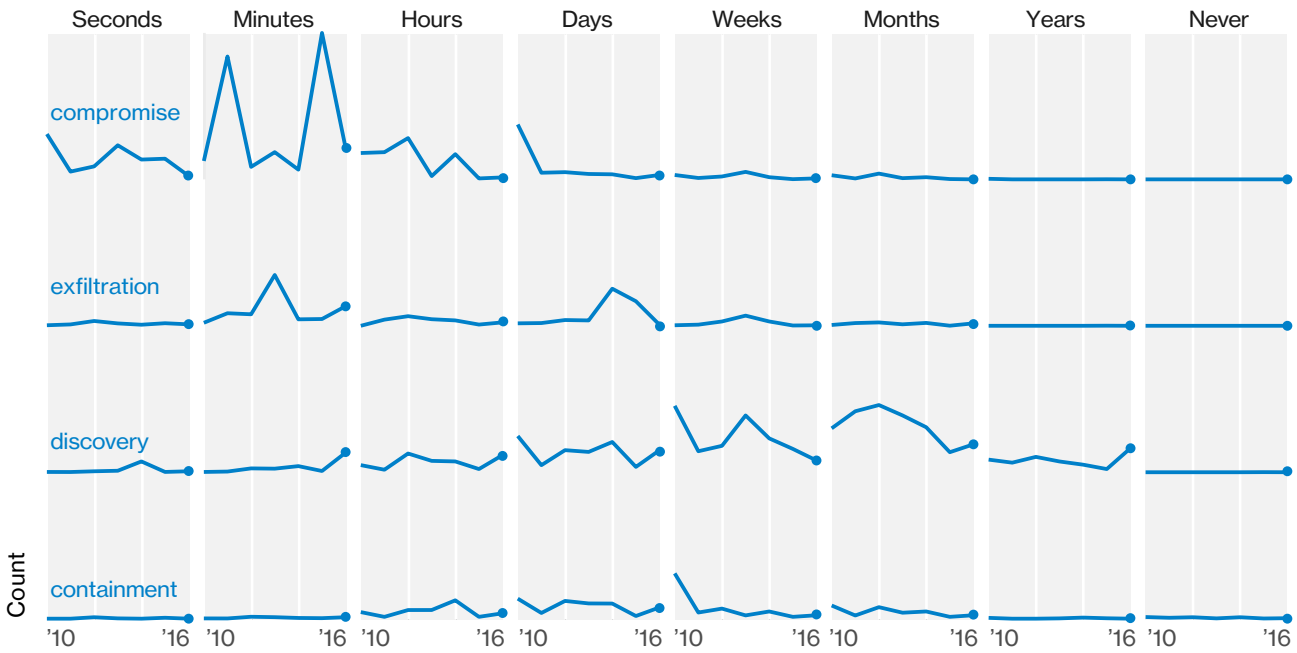


Figure 8: Timespan of breach events over time

[5] We do not record a time-to-compromise when the incident involves a lost device or misuse of privileges.

Introduction to Industries

In previous years, we have released separate industry reports for key verticals. As mentioned in the Introduction, this year we opted to focus even more on industry-specific findings in the main report. We're going to take a deeper look at them as a whole in this section, examining some of the differences in industry findings.

The next couple of pages provide an overview of the industries, followed by individual sections examining the differences in detail. We've selected a few specific industries to focus on because of both readership interest and statistical significance[6].

The totals within Table 1 provide information on the sample size for this year's study and are not indicative of one industry being more or less secure than another. It is more of an indication of how well an industry is represented by our data contributors[7]. With only one recorded breach of a large construction company, that's a good sign we probably won't be able to draw any conclusions based on it. However, if, as is the case with Financial Services, there are 471 breaches, that's a solid sample size for some statistical fun.

Think of Table 1 as opening up the fridge to see just what ingredients you have to cook with, and if you have enough of an industry to "make the bread rise."

	Incidents				Breaches			
	Total	Small	Large	Unk	Total	Small	Large	Unk
Total	42,068	606	22,273	19,189	1,935	433	278	1,224
Accommodation (72)	215	131	17	67	201	128	12	61
Administrative (56)	42	6	5	31	27	3	3	21
Agriculture (11)	11	1	1	9	1	0	1	0
Construction (23)	6	3	1	2	2	1	0	1
Education (61)	455	37	41	377	73	15	15	43
Entertainment (71)	5,534	7	3	5,524	11	5	3	3
Finance (52)	998	58	97	843	471	39	30	402
Healthcare (62)	458	92	108	258	296	57	68	171
Information (51)	717	57	44	616	113	42	21	50
Management (55)	8	2	3	3	3	2	1	0
Manufacturing (31-33)	620	6	24	590	124	3	11	110
Mining (21)	6	1	1	4	3	0	1	2
Other Services (81)	69	22	5	42	50	14	5	31
Professional (54)	3,016	51	21	2,944	109	37	8	64
Public (92)	21,239	46	20,751	442	239	30	59	150
Real Estate (53)	13	2	0	11	11	2	0	9
Retail (44-45)	326	70	36	220	93	46	14	33
Trade (42)	20	4	10	6	10	3	6	1
Transportation (48-49)	63	5	11	47	14	3	4	7
Utilities (22)	32	2	5	25	16	1	1	14
Unknown	8,220	3	1,089	7,128	68	2	15	51
Total	42,068	606	22,273	19,189	1,935	433	278	1,224

Table 1: Number of security incidents by victim industry and organization size, 2016 dataset.

[6] If your favorite industry isn't listed, ping us at dbir@verizon.com and we'll help you out!
[7] To quote the 2015 report, "Don't give much credence to the huge number for the public sector; we have many government Computer Security Incident Response Teams (CSIRTs) participating in this report, and they handle a high volume of incidents."

Figure 9: Industry comparison (left: all security incidents, right: breaches only)

Figure 9 is far more useful for comparing verticals. We are going to let the figures speak for themselves and invite you to identify the “hot spots” for your industry, which are explained in greater detail in the individual sections.

In addition to our incident data, we extracted a lot of good information from our non-incident datasets that can add to our industry focus. If the above is what we cooked from our fridge, what follows is the spice rack.

Industry DDoS

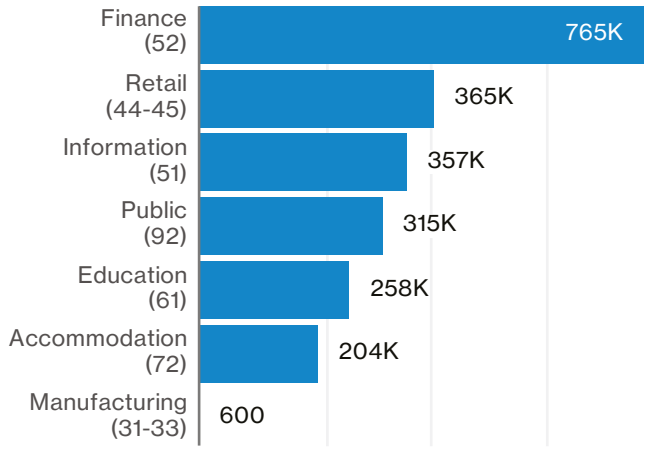


Figure 10: Median DDoS size (pps) by industry (n=2,133)

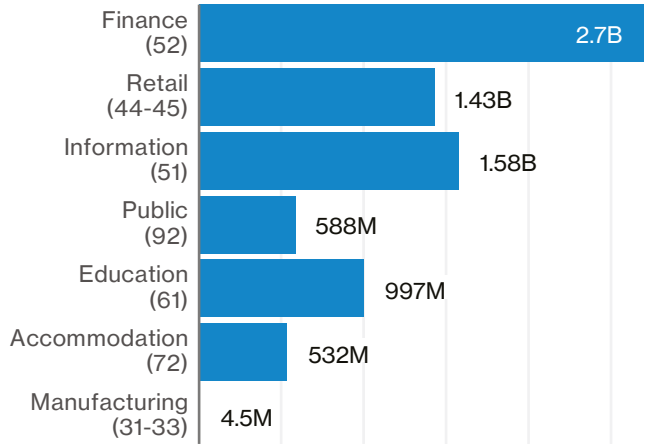


Figure 11: Median DDoS size (bps) by industry (n=2,133)

In Figures 10 and 11 we see that industries that rely on their internet presence for doing business or communications seem to suffer larger Distributed Denial of Service (DDoS) attacks. In our incident dataset, numerous industries feature Denial of Service as their most prominent pattern.

Even for those that don't, such as Manufacturing, it doesn't mean they are immune, simply that it is not represented in our data. Check out the Denial of Service pattern to get a full rundown on the lifecycle of these attacks against availability.

Industry Phishing

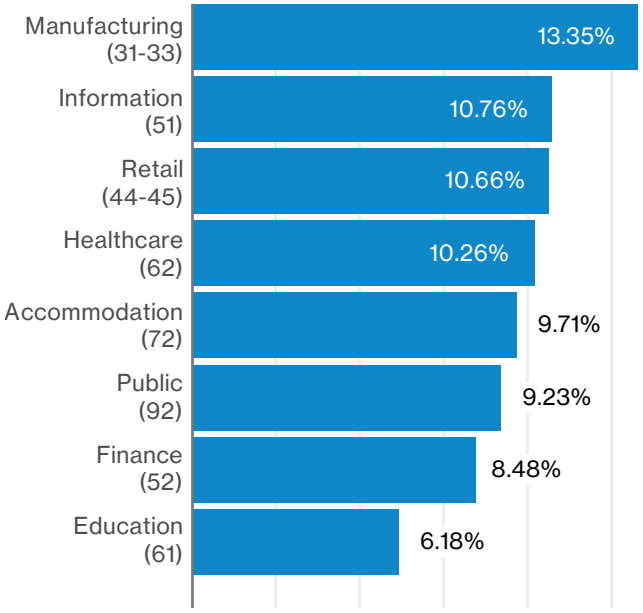


Figure 12: Median click rate per campaign by industry (n=7,153)

Figure 12 gives an idea of how susceptible industries are to phishing attacks. The results from security-awareness training exercises show us that no industry is at 0% and the majority of industries are not significantly different with regard to the percentage of users that click on phishing links or attachments. For more information on phishing, cast your line into the Attack the Humans! section.

Industry malware

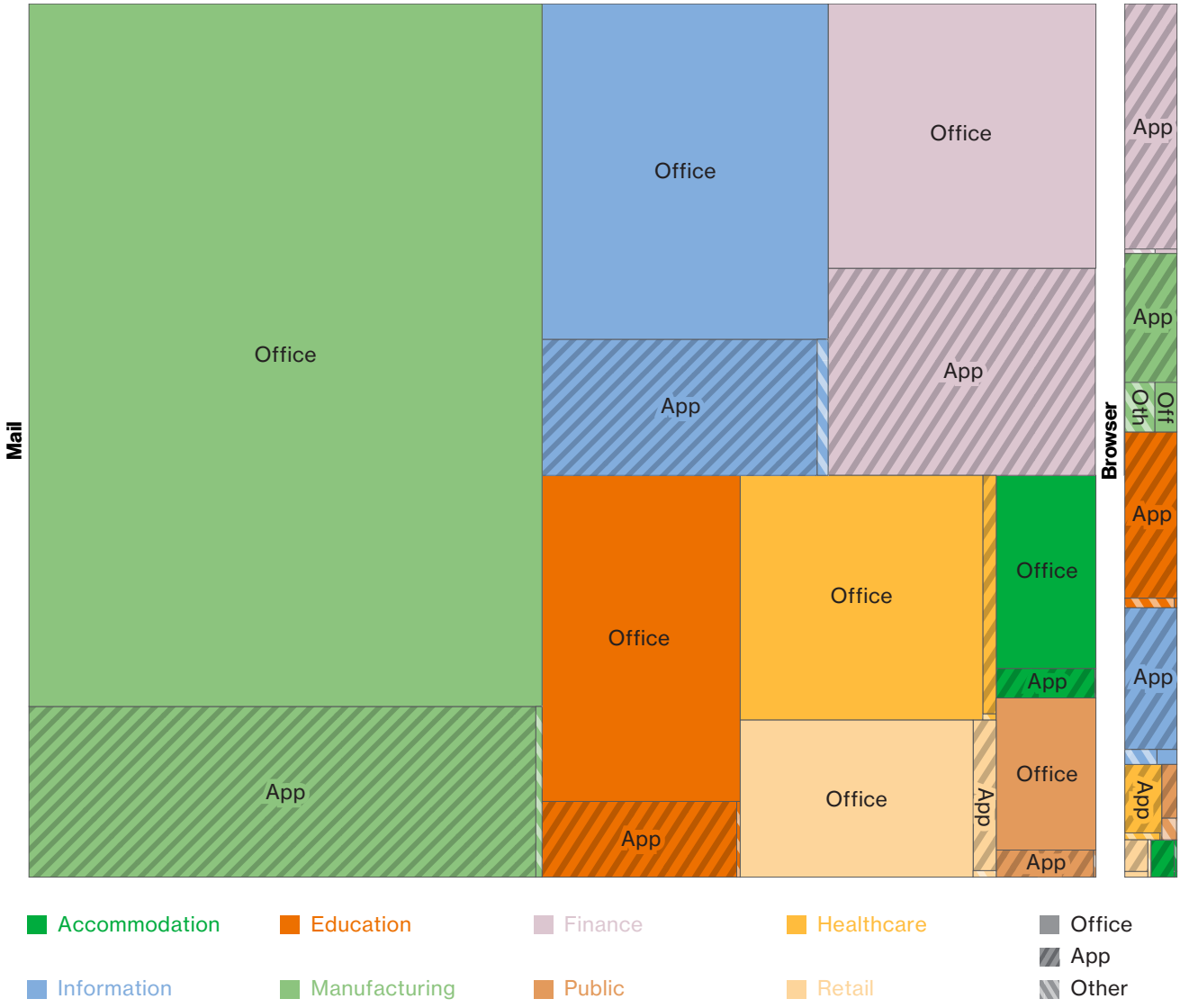


Figure 13: Malware detection details per industry (n=42,821,799)

Figure 13 allows us to compare malware from 50 million on-the-wire detections[8]. We normalized the data so as not to be influenced by the number of organizations in a particular industry within the sample. The amount of space represents the amount of malware detonations in each category per industry. This dataset is not part of the incident corpus, but the vectors of malware installation align with our real-word data.

For example, the finding that manufacturing organizations are often the intended recipients of email-based malware supports the incident data we will discuss in that industry section and also ties in with the click rates in Figure 12. Across industries, email is the road most traveled to deliver malware into organizations. The vectors of mail and web browser are further broken down into malware packaged in an Office document, an executable application, or 'Other'.

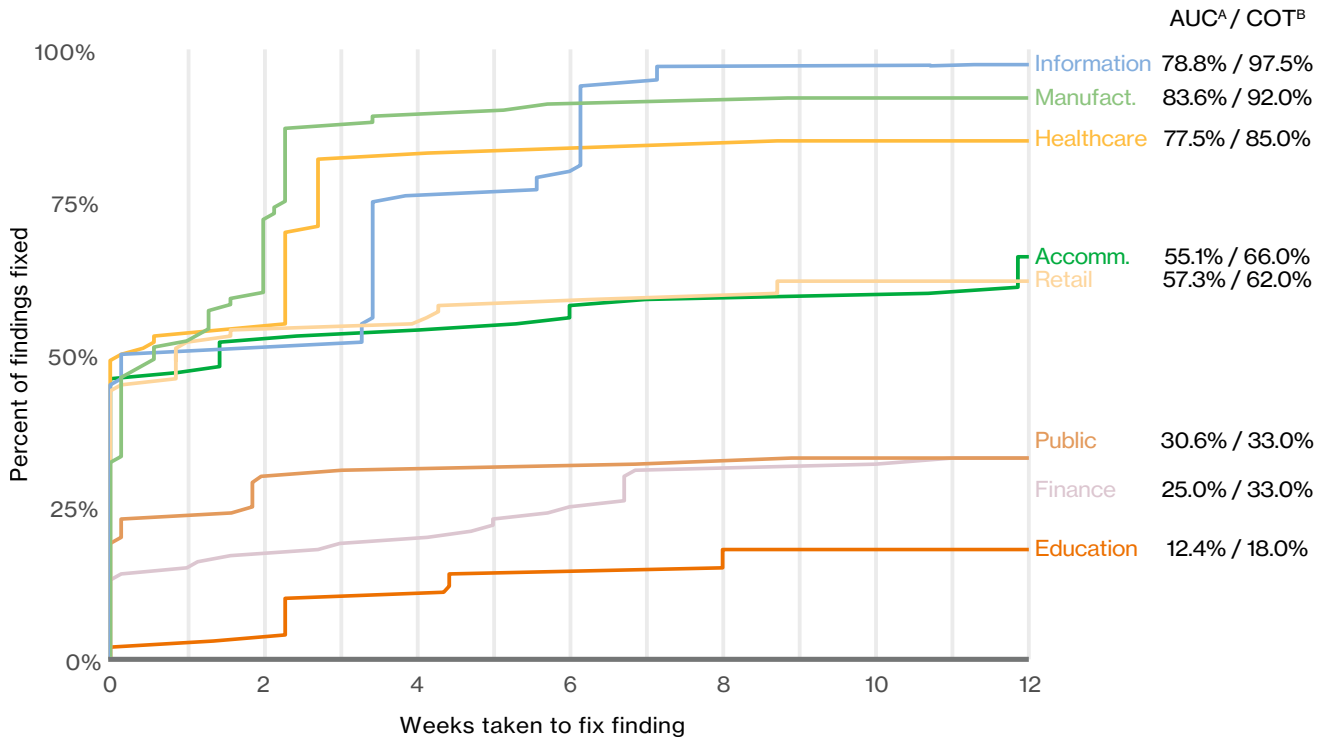
[8] JavaScript malware is prominent in the Crimeware pattern. However, while 50 million samples, the dataset used to generate Figure 13 did not measure JavaScript malware.

Industry patching

We received vulnerability-scanning data from six contributors, and are thankful for the opportunity to roll up our sleeves and find some interesting talking points in the combined dataset. Our research focused on time-to-patch, and the amount of findings that are "left over" or not addressed. We geek out with statistically-sound abandon in Appendix B: The Patch Process Leftovers, but wanted to give you a preview here with a comparison of patching per industry. Before you dive brain first into the visual below (and who wouldn't?), let's clarify some things.

In your environment, you may have longer or shorter patch cycles that are dependent on the particular vulnerabilities discovered as well as the assets on which the findings are triggered. The vulnerabilities are treated as 'equals' in the chart below – organizations will need to factor in threat rates as well as potential impact to establish their own time-to-patch duration to review COT[B].

So, based on Figure 14, the Information industry is the greatest and the Education industry is just the worst right? Not necessarily. Prior research has shown that vulnerabilities are either patched during that initial cycle or tend to hang around for a long time. There are several valid reasons for this phenomenon and the continued existence of vulnerability findings could be expected. Potential justifications are that other controls are in place, or the vulnerabilities may not be exploitable, or even a false positive. It is, however, interesting to see how some industries trend towards a big early push and others are more slow and steady. It is important for organizations to understand what their leftover findings are. And we reheat those leftovers in Appendix B and stuff our faces by looking into how they are laid out across devices and asset types.



A. Area under the curve (AUC)
A measurement of how much potential vulnerability is addressed during the patch process[9]. More simply, if you patch a large percentage of findings immediately you will have a higher percentage in AUC than if you address those findings on day 80.

B. Completed on time (COT)
Represents the percentage of findings that are addressed at some point within a patch cycle. The "leftovers" are findings that are still present in scans after a patch cycle is over. In the figure above we see all industries level off by week 12, so that is the duration for "on time" used for this example.

Figure 14: Comparison of industry patch cycles

[9] Note to professional data wonks: our usage of area under a curve is not the same as area under a ROC curve

Accommodation and Food Services

Frequency	96% External, 4% Internal (breaches)
Top 3 patterns	Point of Sale Intrusions, Everything Else and Privilege Misuse represent 96% of all data breaches within Accommodation
Threat actors	96% External, 4% Internal (breaches)
Actor motives	99% Financial, <1% Grudge (breaches)
Data compromised	96% Payment, 2% Personal, 1% Credentials
Summary	This vertical was dominated by POS breaches. Most of them are opportunistic and financially motivated and involve primarily malware and hacking threat actions. Time-to-compromise is quick but time-to-discovery and containment remains in the months category. Fraud detection is increasing compared to previous years.

Be our guest

The hospitality industry continues to be inhospitable, at least when it comes to POS breaches, which continue to be as ubiquitous and unsatisfying as the continental breakfast. While hotels likely come to mind first, restaurants also fall into this industry and comprise the majority of the victim population. Often food service victims are smaller businesses without IT departments, CISOs etc., but they do accept payment cards and are therefore a target for opportunistic attack.

Let's begin by reviewing the incident patterns most relevant to Accommodation. As Figure 15 illustrates, the POS trend has decreased compared to the previous two years, but remains the forerunner, while Everything Else and Privilege Misuse patterns have both increased, but only slightly. Thus, we will focus on POS breaches below.

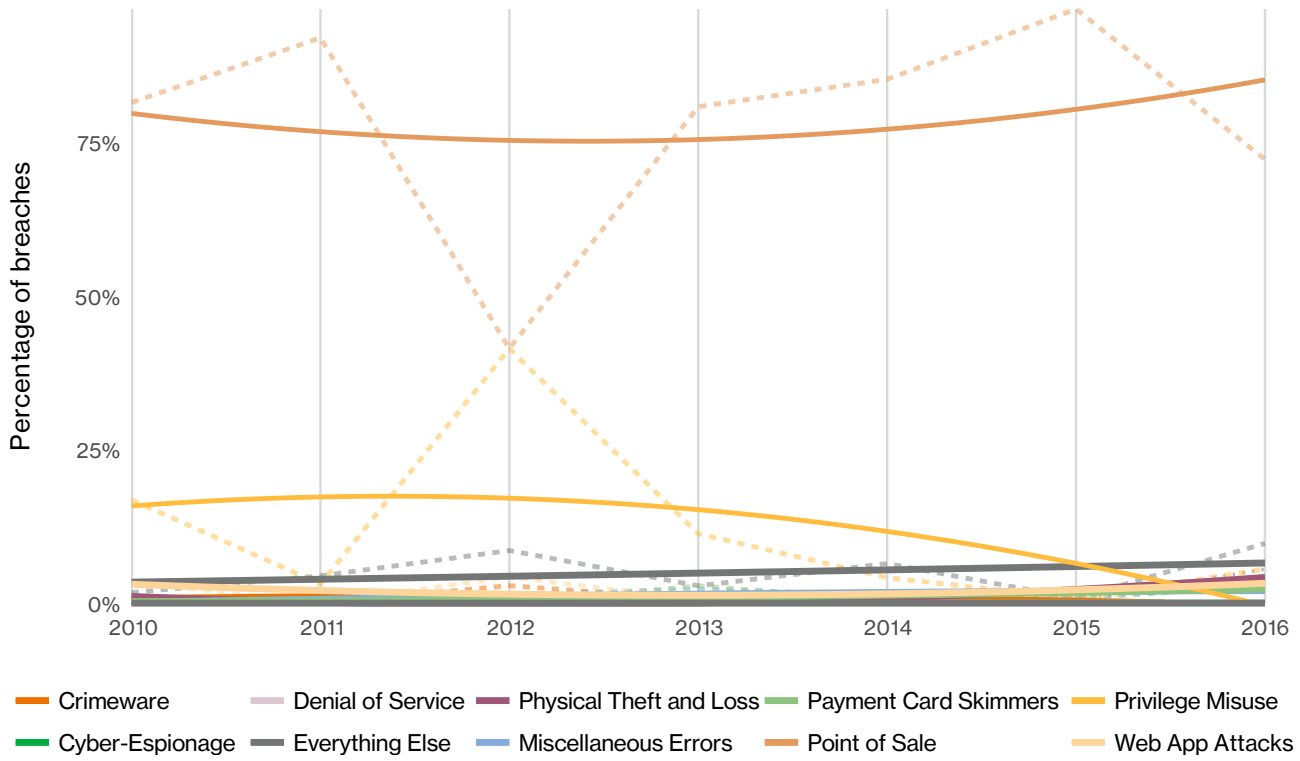


Figure 15: Frequency of incident classification patterns over time across Accommodation industry breaches

As mentioned above, 96% of breaches involved external actors – almost all by financially-motivated organized criminal groups attacking targets of opportunity and compromising payment card data. The threat action categories of malware and hacking were ubiquitous in attacks against this industry, with third-party managed POS devices (both terminals and controllers) accounting for the majority of the assets that were compromised.

The specific threat action varieties in Figure 16 present the chef's special of cage-free RAM scrapers sautéed with C2, and served over keyloggers and credentials with a balsamic brute force reduction[10].

[10] Gluten-free keyloggers available, ask your server.

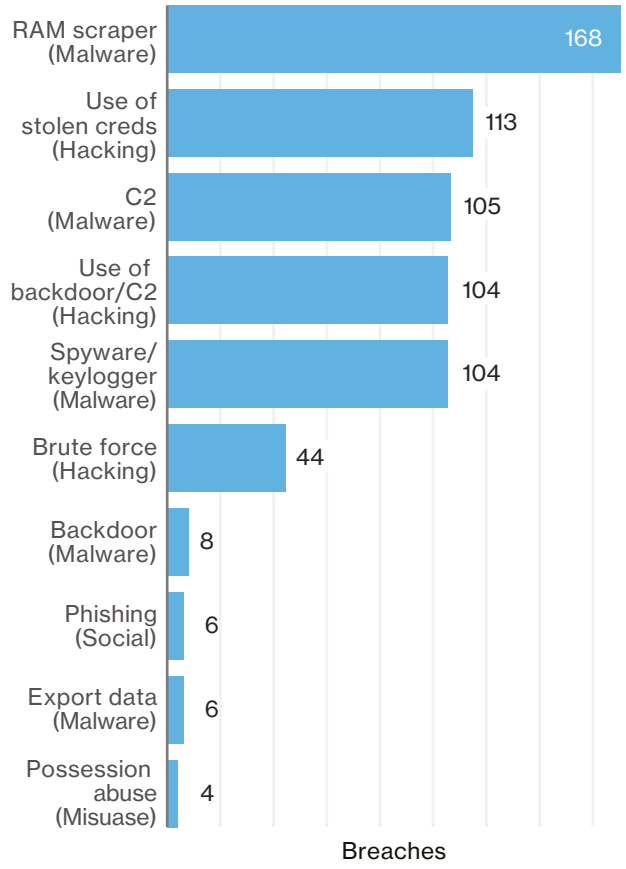


Figure 16: Top threat action varieties within Accommodation industry breaches (n=197)

With regard to malware-related breaches, 96% represented RAM scrapers, while 60% featured C2 and spyware/ keyloggers – all of which were installed after an initial access was gained. Out of the 170 breaches specifically containing these three top malware varieties, 102 contained all three in a given breach. This implies that over half of these breaches (that contain at least one of the three varieties) are a product of a mature, multidimensional variant of POS malware with C2 capabilities. We must point out that this is more of a characteristic of a particular type of POS breach and not necessarily a sweeping trend (we just tell the data's story).

Use of stolen credentials and backdoor/C2 were the most prominent hacking varieties (represented in over half of the breaches), with brute force attacks reporting just under a third. Many of these attacks involved actors using valid partner credentials and backdoors, while a third of them represented desktop sharing as the hacking vector.

> **"You can check out any time you like, but you can never leave..."**

Apparently, it is not only The Eagles that are destined for a long stay at the hotel. The hackers continue to be checked in indefinitely as well. Breach timelines continue to paint a rather dismal picture – with time-to-compromise being only seconds, time-to-exfiltration taking days, and times to discovery and containment staying firmly in the months camp. Not surprisingly, fraud detection was the most prominent discovery method, accounting for 85% of all breaches, followed by law enforcement which was seen in 4% of cases.

To wrap it up, let's focus on the obvious. POS attacks are absolutely rampant in this industry; Accommodation was the top industry for Point of Sale Intrusions in this year's data, with 87% of breaches within that pattern. Feel free to skip to that incident pattern section for even more details.

Things to consider:

Killing me softly with malware – The level of software installation occurring in this industry needs to decrease as this particular variety of integrity compromise represents 94% of breaches this year.

Remove this tab before use – Don't use default passwords as doing so makes criminals' lives much easier.

You can't get there from here – Filter remote access to your POS network. Only allow connections from whitelisted IP addresses.

Don't be outdated – Patch promptly and consistently and make certain all terminals and servers are running the most recent version of software.

Educational Services

Frequency	455 incidents, 73 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Miscellaneous Errors and Everything Else represent 67% of all data breaches within Education
Threat actors	71% External, 30% Internal, 3% Partner (breaches)
Actor motives	45% Financial, 43% Espionage, 9% Fun (breaches)
Data compromised	56% Personal, 27% Secrets, 8% Credentials
Summary	This section will focus on confirmed data breaches, but Education remains a consistent target of Denial of Service (DoS) attacks also. 2016 results reflect a substantial increase in the number of espionage-related breaches.

"A" for effort, right?

Espionage and errors were definitely in the backpacks of the Education industry this past year. Cyber-Espionage was present in 26% of breaches, with Miscellaneous Errors closely following at 22%. Last year the Cyber-Espionage pattern accounted for under 5% of breaches while Web Application Attacks dominated the chalkboard. Figure 17 shows how espionage has been increasing over time. So college isn't just pizza and tailgates – research studies across myriad disciplines conducted at universities put them in the sights of state-affiliated groups.

Our breach findings showed that over half involved the compromise and disclosure of stored personal information – of both students and employees, while a little over a quarter resulted in the disclosure of intellectual property. This industry faces numerous challenges that are unique when it comes to keeping sensitive information secure. Not least among these is the very nature of the vertical itself which is, and always has been, based on the free and open exchange of ideas and information. Add to that the student/user population whose varying degrees of technical skills and curiosity must be taken into account, not to mention their roles as data subjects, whose personally identifiable information (PII) and other information must be protected. Implementing security controls while still maintaining the culture of openness is practically MIT Course Number 16.512.

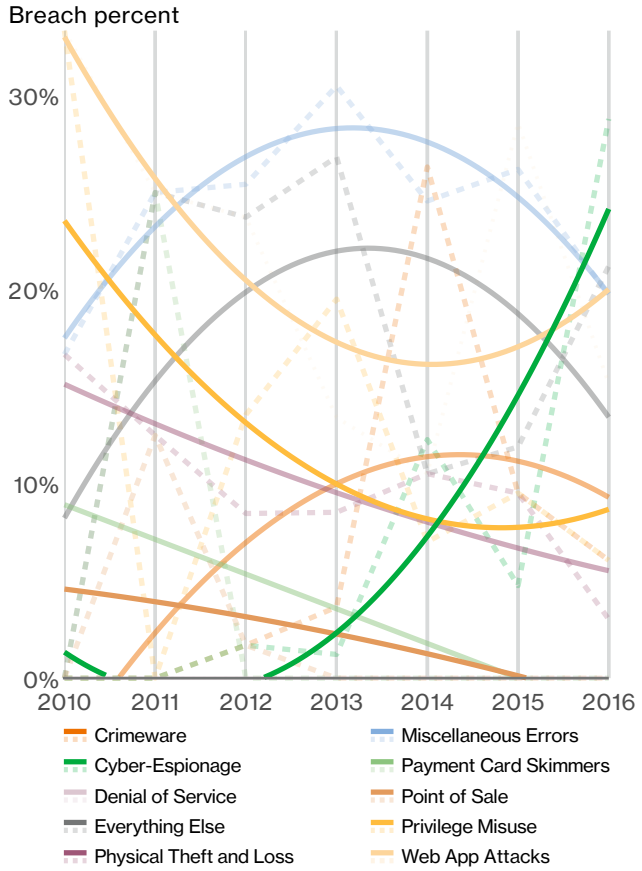


Figure 17: Frequency of incident classification patterns over time within Education breaches

Next you may be asking, "Who is behind these breaches? Are they targeted or more opportunistic in nature?" Good questions – here's a gold star. The data showed that state-affiliated actors (involved in over half of the breaches) were targeting these educational institutions. We also saw a handful of breaches where organized criminal groups were involved with their mind on the money (and the money on their mind). The breaches involving internal actors were mostly attributable to human error – notably misdelivery of sensitive data and publishing errors, as opposed to malicious intent.

Now that we have covered the "what" and "who", let's briefly discuss the "how".

The threat categories that were the real troublemakers within the patterns mentioned above were hacking, social and malware. We saw more breaches involving social and malware attacks compared to last year, where social was represented in almost 44% of breaches and malware featured in a little over a third. Phishing via email was the most prevalent variety of social attacks, while use of stolen credentials against web applications was the dominant hacking tactic. We wanted to look into the representation of the breaches that had an explicit link between our top three actions (hacking, social and malware). In other words, we were interested in how often breaches had at least two of these three categories as threat actions are certainly not mutually exclusive. As you can see in Figure 18, a little over a third of the breaches posted to social media that they're "in a relationship" and are indicative of multi-faceted attack methods.

Although we focused on breaches in this section, the fact remains that DDoS attacks are a significant threat to educational institutions, representing one half of all security incidents. These attacks are akin to a realization that your 30-page research paper is due the next morning, while you thought you had another week to conquer your procrastination and churn out something brilliant. Panic sets in, your brain shuts off, and you crawl into a dark corner and assume the fetal position. Just as this nightmare is a type of availability degradation, so too were the DDoS incidents against this vertical.

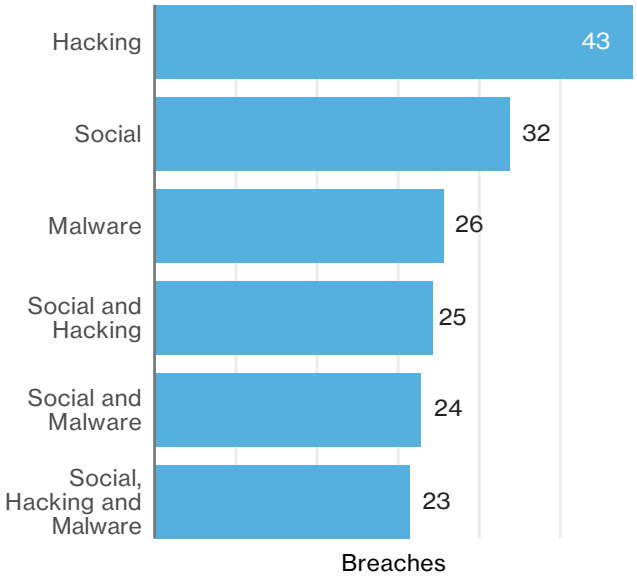


Figure 18: Relationships between actions within Education breaches (n=73)

Things to consider

"All aboarddd" – Train your employees and students on security awareness, and encourage/reward them for reporting suspicious activity such as potential phishing or pretexting attacks.

Classes are cancelled – Be sure to develop a response plan and practice your disaster and recovery plans annually/biannually to make sure you are adequately prepared for any unreasonably high traffic densities.

Financial and Insurance

Frequency	998 Incidents, 471 with confirmed data disclosure
Top 3 patterns	Denial of Service, Web Application Attacks and Payment Card Skimming represent 88% of all security incidents within Financial Services
Threat actors	94% External, 6% Internal, <1% Partner (all incidents)
Actor motives	96% Financial, 1% Espionage (all incidents)
Data compromised	71% Credentials, 12% Payment, 9% Personal
Summary	DoS attacks were the most common incident type. Confirmed data breaches were often associated with banking Trojans stealing and reusing customer passwords, along with ATM skimming operations.

While there are no traditional bank robbers in our dataset, the summary section above calls out that external parties are still looking to make a (dis)honest dollar.

The Financial Services umbrella is comprised of many subsectors and not all share similarities in threat actor tactics. For instance, having to worry about dudes in hoodies and track pants installing skimmers and cameras on ATMs is a commercial bank or credit-union reality, but not so for insurers and investment bankers. The charts that follow will exclude that niche attack as it is unique enough to have its own pattern if you want to learn more. DoS, on the other hand, while an equal opportunity attack method, will also be removed from the following analysis so we can focus more on confirmed (non-ATM skimming) data breaches in the industry.

And you know what, while we are in a spring-cleaning kind of mood, let's acknowledge again that banking Trojans are a "thing", but the sheer amount of those breaches, if we allowed them to remain, would dominate the conversation like a telemarketer phoning a Trappist monastery. We will filter those out as well in efforts to uncover more interesting findings.

A bit about botnets

Botnets continue to be a powerful tool built and utilized (either by renting out or direct use) by organized criminal groups for financial gain. One type of zombie herd that is leveraged in attacks against banking institutions is DoS botnets, which use strength in numbers to spew unwanted traffic at their victims' infrastructure. These gained national attention in 2012 with ideology-driven attacks against US banks. Another threat worthy of note is consumer devices infected with banking Trojans. Banking Trojans are not new on the cybercrime scene, but are still omnipresent and ever evolving. The difficulty for banking institutions is that many of the nefarious acts or, in VERIS lingo, "Threat Actions" are against their customers, not internally-managed devices.

A common event chain is:

1. Send malicious attachment to consumer.
2. Malware installs on consumer device and identifies when they are accessing a banking site.

3a. Keyloggers capture user credentials to be reused fraudulently. Or,

3b. User web request is redirected to a fake site where credentials are entered and captured.

4. Threat actor issues legitimate credentials to application acting as the customer potentially triggering an SMS second factor authorisation code.
5. The second factor is presented to the fake website and step 4 is repeated.
6. Account balances get smaller.

In July 2016, the National Institute of Standards and Technology listed the above scenario, as well as malicious code on mobile endpoints designed to capture second factors delivered via SMS, as reasons for recommending moving away from texting codes as a second authentication factor. We are not suggesting using two-factor authentication via SMS is akin to building a house of sticks (as opposed to a straw house) for the mitigation of wolf attacks, but it is a window into the thinking of the adversary. When faced with defeating multi-factor authentication they will pragmatically try to devise a way to capture both factors for reuse.

After filtering ATM skimming, DoS, and botnets, Figure 19 uncovers:

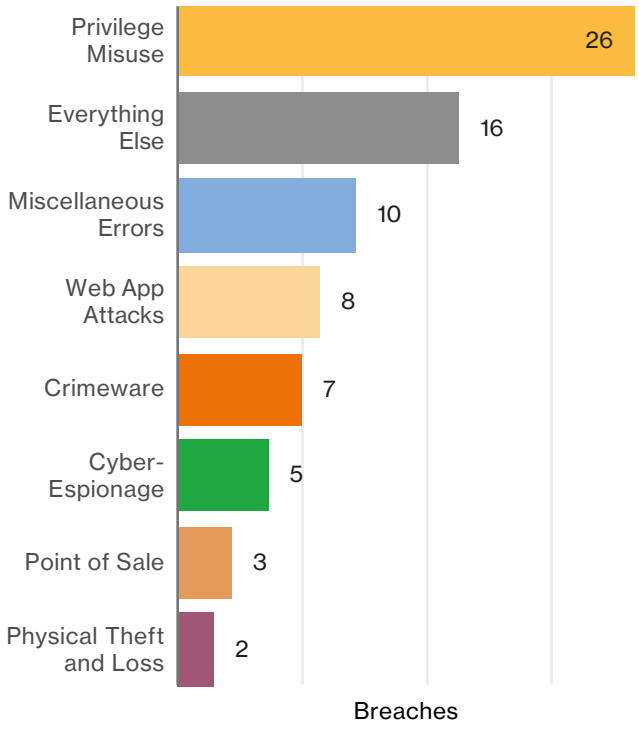


Figure 19: Incident classification patterns within select Financial industry breaches (n=71)

Banking employees have access to data in their normal work day that can absolutely be used to give themselves that bonus that they feel they so richly deserve. Accessing systems to fraudulently transfer money or using personal information of customers for identity theft are two financially-motivated examples of misuse. Interestingly, personal information is found to be the desired data more often than banking information. Perhaps they are more aware of the breadcrumb trail left behind when you transfer money, and would prefer to use personal information to open up lines of credit or to conduct other fraud that occurs outside of their own workplace.

There is a saying "Don't fraud where you work" (or something similar) that may be adhered to due to the risk of being caught.

Accessing systems to fraudulently transfer money or using personal information of customers for identity theft are two examples of financially-motivated misuse.

Not only does the financial industry need to protect data that is easy to monetize, but investment banks and other non-commercial entities have information surrounding investment strategies, mergers and acquisitions, and market influencers that would be sought after by actors motivated by espionage. Skip over to the Cyber-Espionage pattern to learn more about the tactics associated with that motive.

If you are curious about the breaches in the Everything Else category, many featured hacking and/or phishing attacks without further descriptors to draw any actionable conclusions or allow for them to be categorized in one of our nine patterns.

Things to consider

Taunt them a second time – Use two-factor or multi-factor authentication to help secure all web applications.

Make a new plan, Stan – In this industry you are likely to be the target of DoS attack. Have a DoS protection and mitigations service in place and make it your job to know the details of the agreement with the provider.

It's not that I don't trust you, but... – Keep an eye on employees and periodically monitor their activities. Do not give them permissions they do not need to do their job, and make sure you disable accounts immediately upon termination or voluntary departure.

An alternative solution to tackling cyber fraud

– Mishcon de Reya

The majority of fraud today takes place online, and the police are simply unable to keep pace with the rate at which, and the scale on which, it is being committed. The public sector is under-resourced, meaning that money stolen is rarely recovered and cybercrimes go unpunished. As cybercriminals become more sophisticated, this kind of crime shows no sign of slowing down.

A creative solution is now being piloted by the City of London Police in the UK. It will see law enforcement working with Mishcon de Reya and others in the private sector in a new two-year initiative to identify, seize and recover assets from criminals under normal civil law remedies rather than criminal law.

It is anticipated the fraud panel will make it possible for victims of crime to recover their losses from the assets of fraudsters in circumstances where they may otherwise have been unable to. If the claim is financially and legally viable, the panel will prepare the case to be offered to the victims and use the police evidence for recoveries.

The sharing of information between the police and the private sector will enable law enforcement to introduce groups of victims of the same perpetrator(s) to the possibility of forming a joint instruction that considers the civil route – in addition to the criminal route – under a joint criminal and civil steering group. In these matters, the victims obtain third-party disclosure orders, Search Orders and Freezing Orders in the UK and similar types of orders abroad to track down wrongdoers, freeze assets and seize evidence. Through this civil route, the process can be rapid, giving victims the best chance of recovering their losses.

Going forward, this joint strategy could have huge implications for the future of enforcement, as cybercriminals are pursued through civil as well as criminal courts. In a world where no business or individual is immune to cyber fraud, the ability to act quickly to identify wrongdoers and quickly regain control of assets is critical.

Healthcare

Frequency	458 incidents, 296 with confirmed data disclosure
Top 3 patterns	Privilege Misuse, Miscellaneous Errors and Physical Theft and Loss represent 80% of breaches within Healthcare
Threat actors	32% External, 68% Internal, 6% Partner (breaches)
Actor motives	64% Financial, 23% Fun, 7% Grudge (breaches)
Data compromised	69% Medical, 33% Personal, 4% Payment
Summary	Healthcare has the unenviable task of balancing protection of large amounts of personal and medical data with the need for quick access to practitioners. Internal actors are well represented with employees accessing patient data out of curiosity, or to commit identity fraud.

Far from a piece of cake

Being an information security professional for a healthcare organization is not easy. You have to deal with a multitude of medical records, stored electronically (in centralized databases and laptops alike), and possibly still on paper. Those records also have personal information (name, address, social security number) often riding along. This information needs to be accessible quickly for patient care, so draconian access control mechanisms may do more harm than good. Another item to add to the "Things-that-stress-out-healthcare-CISOs" list is the disclosure requirements for the industry.

Insider misuse is a major issue for the Healthcare industry; in fact it is the only industry where employees are the predominant threat actors in breaches. Interestingly enough, Figure 20 shows the insiders' motives are almost equally divided between financial and fun[11]. This is a product of a lot of sensitive data that may be accessed by legions of staff members containing PII – that is perfect for identity theft – and medical history (sometimes of friends or relatives), that is very tempting for enquiring minds (that want to know!).

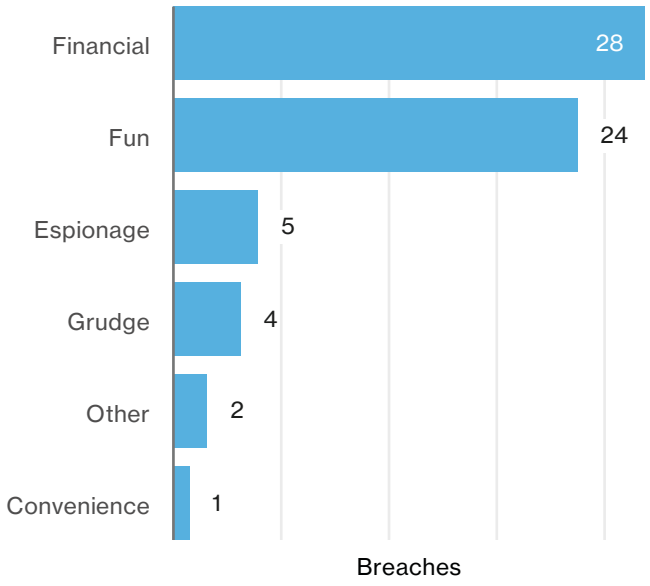


Figure 20: Internal actor motive breaches within the Healthcare industry (n=64)

[11] Errors, which are discussed later, do not have a motive associated with them.

A comedy of errors

Doctors losing laptops, X-rays accidentally ending up in landfills, and employees giving J. Tinker's discharge papers to J. Evers (and Evers' to Chance) all help Miscellaneous Errors remain a top 3 pattern again this year. The breach counts in Figure 21 show that misdelivery, disposal errors and lost assets combine for almost 30% of all Healthcare breaches – showing that it isn't just malicious insiders that you need to worry about.

Tall, dark and ransom

In our dataset, ransomware attacks are not counted as breaches because typically we cannot confirm that data confidentiality was violated. However, the US Department of Health and Human Services (HHS) has given guidance that ransomware incidents should be treated as a breach for reporting purposes[12]. This year, ransomware accounts for 72% of malware incidents in the Healthcare industry.

Timelines

The discovery timeline for Healthcare, Figure 22, appears healthier than the overall dataset. Unfortunately, when we got lab results back (by digging into the breaches discovered in days or less) we found out that the majority of them were breaches involving misdeliveries of information or stolen assets. In the future, we hope that we find more instances of quick identifications of improper access of medical records based on correlation of records viewed and patients under direct care of that employee.

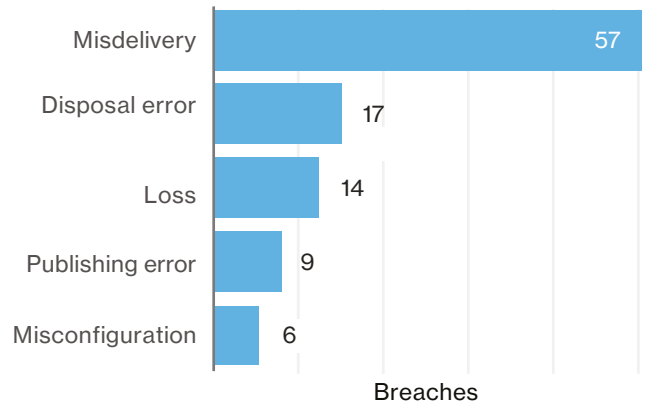


Figure 21: Top varieties of error within Healthcare industry breaches (n=113)

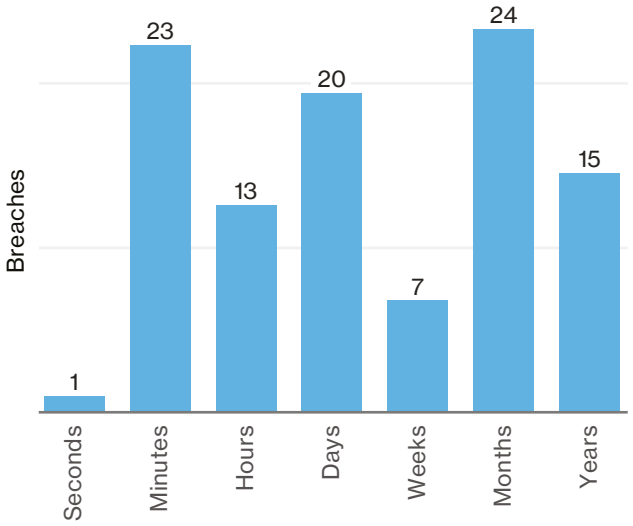


Figure 22: Time-to-discovery within Healthcare industry breaches (n=103)

Things to consider

Achtung, baby – Pay attention to what you are doing. Many of the problems in Healthcare are errors that could have been prevented. Have a process that mandates a second individual must sign off on any online changes to avoid publishing errors. Have a policy in place for disposal of any PII and make sure that it is monitored for compliance. Encrypt all mobile devices to limit the impact of lost or stolen devices.

I love it when a backup plan comes together – Although not discussed in detail in this section, ransomware is increasingly prevalent in the Healthcare vertical. Backup all systems routinely and have them ready to fall back on in case of such an attack.

See a doctor and get rid of it – As misuse is so common, routinely check on employee activity to make sure they are not viewing, downloading or printing information that they have no business need for. Use warning banners that make it clear that monitoring is taking place and it isn't worth it to snoop around.

Token of my appreciation – Where feasible, tokenize sensitive information (such as social security number) when it is only used to identify a record and the employee doesn't need it for billing purposes or patient care.

[12] https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Information

Frequency	717 incidents, 113 with confirmed data disclosure
Top 3 patterns	Denial of Service, Web Application Attacks and Crimeware represent 90% of all security incidents within Information
Threat actors	97% External, 3% Internal (all incidents)
Actor motives	75% Financial, 18% Fun/Ideology/Grudge, 6% Espionage (all incidents)
Data compromised	56% Credentials, 45% Personal, 6% Internal
Summary	Both incidents and breaches within the information sector have a strong association with internet-facing web servers.

That's just TMI

The Information industry (NAICS 51) encompasses everything from software publishers to telecommunication carriers; from cloud providers to social media sites, and even online gambling. Speaking of gambling, the evidence provided by the pattern breakout shows that information organizations, much like James "Wild Bill" Hickok, have suffered significant availability issues (but not necessarily while holding aces and eights). Historical references aside, the fact that the results gravitate toward hacking – specifically Denial of Service (71% of all incidents) – is a common-sense finding indicative that most of the incidents are based on disruption of access to web-based sites/applications.

When the situation escalates from a security incident to a confirmed data breach, it is most often credentials and personal data that are harvested via web applications, where the number of members affected is often measured in the millions. Our data shows that almost 60% of breaches involved web applications either as the asset affected, and/or a vector to the affected asset[13]. Directing our focus to these breaches[14], what are the tactics used and what are the unique issues within the organizations in this industry that influence the results?

[13] It is quite possible, and actually common, for a breach to feature a web application as the vector and the asset affected.

[14] Where asset variety OR hacking vector is a web application.

Figure 23 reveals a strong grouping of the top six threat action varieties that follow the well-traveled path of phishing users to install C2 and keylogging software in order to capture credentials that are used to authenticate into, and exfiltrate data out of, organizations. It should be noted that this group is followed by unknown hacking (not shown) and SQL injection (SQLi), so attacks against application code are alive, well, and possibly underrepresented.

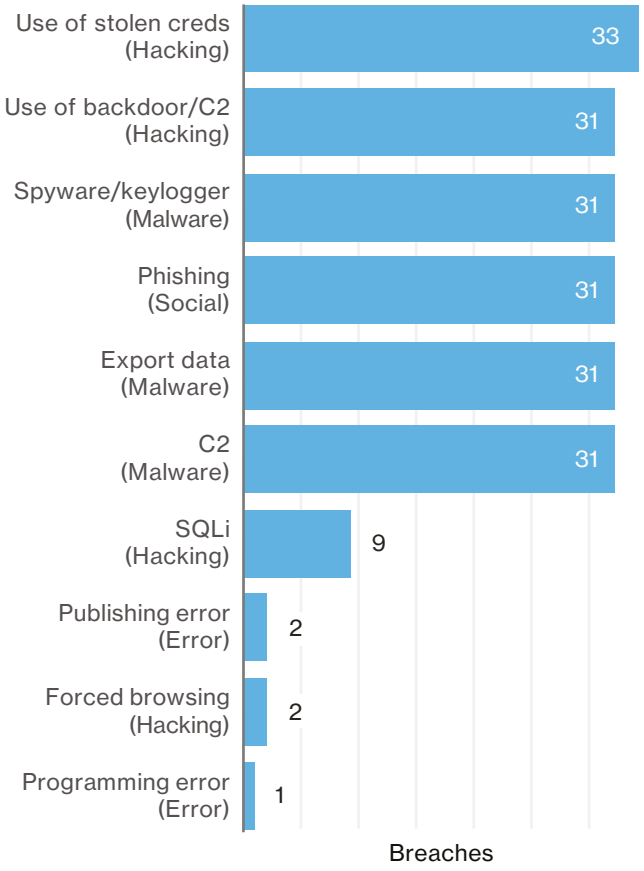


Figure 23: Top threat action breach varieties within Information involving web applications, (n=48)

When we have enough demographic information available to extrapolate the victim NAICS code to six digits, over a third fall into category 519130 (Internet Publishing and Broadcasting and Web Search Portals). This is a catch-all category for web-based organizations that are not retailers. Their business is their web presence and thus the web application is the prime target of compromise to harvest data, frequently some combination of usernames, passwords (sometimes encrypted, sometimes not), and email addresses.

So, they are a web-based entity storing user information and hackers go after the web applications for user information – got it. Another commonality is the organization size – over three-quarters of these victims are small businesses and may not have dedicated security staff and/or processes. The data-loss numbers can be massive, but they are (typically) considered less sensitive than regulated data varieties (e.g., Payment Card Information, Protected Health Information). The site administrators may not be as concerned about disclosure of usernames and passwords, and it may be easier for them to notify and force password changes than to implement two-factor authentication, conduct penetration testing, or ensure the Content Management Platform is up to date.

"Well, I'm not running a forum for macramé enthusiasts operating on outdated WordPress," you say? Fair enough. When we filter out breaches that involved web applications the results are all over the place. The Everything Else pattern rises to the top, and further exploration uncovers breaches where we know a database was hacked, but not enough additional details are available for it to be categorized further. It is certainly feasible that a web app was involved, but we cannot make that leap of faith.

Things to consider:

Establish your cred(entials) – Implement two-factor authentication for administrative access to web applications and any other devices that are data stores. Reduce the effectiveness of stolen credentials being reused to unlock the door to member or customer information. If feasible, extend the use of strong authentication to your user base.

Don't be denied – Develop a DDoS response plan and make fast friends with your business continuity/disaster recovery guru. Monitor capacity usage and prepare for spikes in traffic that are a product of larger than normal legitimate usage.

All sysadmins must update server software before returning to work – A drum that has been beaten to oblivion: security hygiene. The act of keeping server software (OS, web applications, plug-ins) up to date, and a method of becoming aware when security vulnerabilities are disclosed and patches made available, isn't mind blowing. But the results of Shodan searches show that there are still plenty of misconfigured servers in this imperfect world of ours.

Manufacturing

Frequency	620 incidents, 124 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Privilege Misuse and Everything Else represent 96% of breaches within Manufacturing
Threat actors	93% External , 7% Internal (breaches)
Actor motives	94% Espionage, 6% Financial (breaches)
Data compromised	91% Secrets, 4% Internal, 4% Personal
Summary	Gains in strategic advantage via espionage-related actions comprise the majority of breaches within this industry. Most are conducted by state-affiliated actors, but instances of internal espionage pilfering trade secrets are present as well.

Spies like us

In our salad days, one of the chief complaints we received on the report went like this: “That is great if you are a bank, a restaurant or in retail, but I know the APT is after my secrets and this does not help me”. Years ago, our breach data expanded from payment card hauls to the common issues experienced by those protecting intellectual property as their main security focus. The NAICS code for Manufacturing comprises “establishments engaged in the mechanical, physical, or chemical transformations of materials, substances, or components into new products.”[15] In other words, they make stuff. And when you make stuff, there is always someone else who wants to make it better, or at least cheaper. A great way to make something cheaper is to let someone else pay for all of the R&D and then simply steal their intellectual property. With that in mind, it will probably be of no surprise that Cyber-Espionage is by far the most predominant pattern associated with breaches in Manufacturing as evidenced by Figure 24.

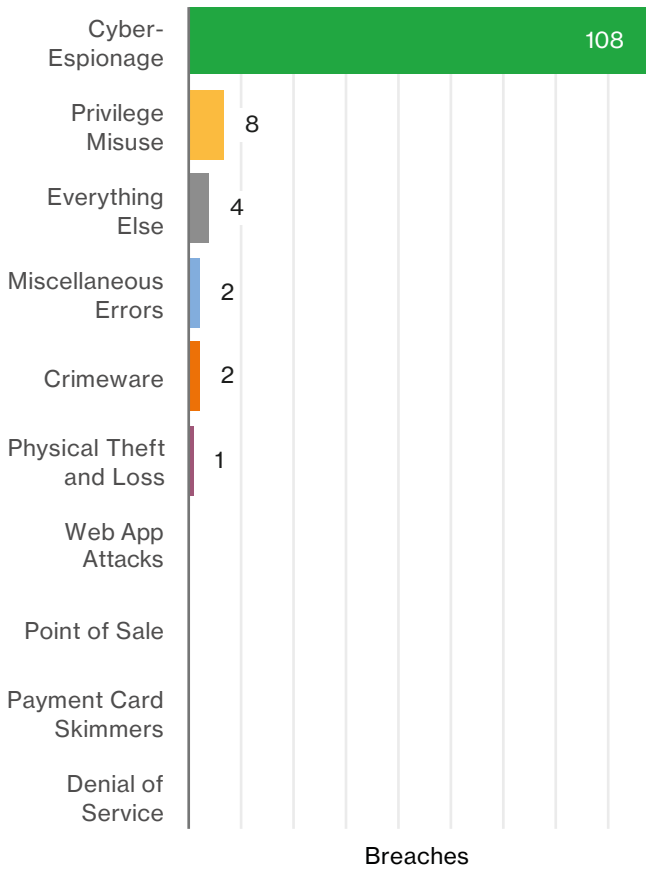


Figure 24: Frequency of incident classification patterns within Manufacturing industry breaches (n=124)

[15] https://www.bls.gov/iag/tgs/iag31-33.htm

Can you keep a secret?

Benjamin Franklin said, "Three may keep a secret if two are dead." If you are in Manufacturing, it is a safe bet that you worry quite a bit about hanging on to secrets. A whopping 90% of data stolen in Manufacturing was of the "Secrets" variety. Figure 25 does nothing to ease those concerns.

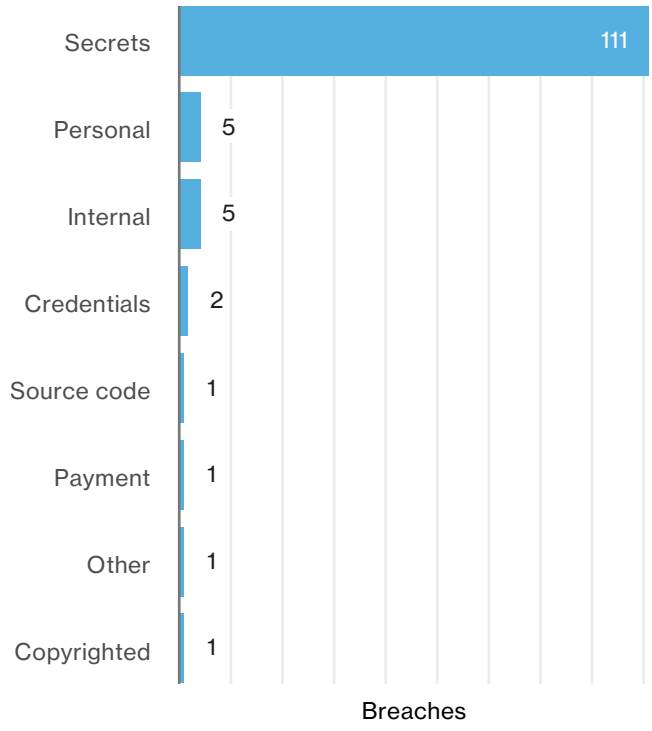


Figure 25: Varieties of data breached within the Manufacturing industry (n=122)

For a manufacturer, the intellectual property it possesses is of the utmost importance – whether it is a secret recipe, a creative new concept or a less expensive way to make a widget, it makes a tempting target for thieves. Unlike the more run of the mill, "grab-the-loot-and-scram" attacks we see in other verticals, espionage attacks are typically aimed at more long-term results. The criminals want to infiltrate the network, find out where the secrets are kept, and then sit and slowly siphon off the nectar for as long as they can. In many cases these attacks begin with a move against the carbon layer. An employee of the organization receives a phishing email, and clicks on the malicious link or attachment it contains. Then malware is installed in the form of a backdoor or C2, and the bad guys return at their leisure to footprint the network and take what they need. In fact, the social and malware combination occurred in 73% of these breaches.

When state-affiliated actors are involved, their operations are targeted attacks, rather than opportunistic. In other words, the criminals are coming directly for a particular organization with a specific purpose in mind.

The next most common incident pattern, Privilege Misuse, (while only a very small sample size) is in some ways akin to the external espionage breaches discussed above. It often occurs when a disgruntled employee is tired of being kept down by the man and sets off to make their fortune elsewhere – but wants to take as much data as possible with them.

Things to consider:

Keep 'em separated – If you have highly-sensitive information, keep that data segregated and only allow access to those who require it to perform their job.

Click not, lest ye be phished – Many attacks against this vertical are initiated via a phishing email. Train your employees with regard to phishing, and provide them with a quick and easy way to report suspicious emails.

Just look at yourself – Internal monitoring of networks, devices and applications is critical. Attempt to implement account monitoring, audit log monitoring and network/IDS monitoring.

No parting gifts – Implement data loss prevention (DLP) controls to identify and block improper transfers of data by employees.

Public Administration

Frequency	21,239 incidents, 239 with confirmed data disclosure
Top 3 patterns	Cyber-Espionage, Privilege Misuse and Miscellaneous Errors represent 81% of breaches within Public Administration
Threat actors	62% External, 40% Internal, 4% Multiple parties, 2% Partner (breaches)
Actor motives	64% Espionage, 20% Financial, 13% Fun/Ideology/Grudge (breaches)
Data compromised	41% Personal, 41% Secrets, 14% Credentials, 9% Medical
Summary	Almost one half of attacks resulting in confirmed data disclosure are state-affiliated. Timeline for breach to discovery is over 50% in the “years” category.

First, we kill all the incidents...

As we have mentioned ad infinitum already in this report, our data is in large part dependent on our contributors for the year. What they investigated or witnessed, what they had the resources to provide to us and so on. Certain contributors tend to give us particular types of data, and this is probably nowhere more marked than in the public sector. The government is required to report up the chain on incidents that would remain unremarked upon in many organizations. Governments are also very large and due to these two factors, Public Administration continues to feature a large number of incidents. Many of these were comprised mostly of “unknown” events, or nebulous “policy violations.”

Consequently, there is little value in examining them in depth. If we were guessing, we would hazard that many of the policy violations were issues such as web-content filters reporting on inappropriate web usage, or employees utilizing effective but unauthorized workarounds, but you don’t pay us to speculate so we won’t. Also, there were a great number of lost and stolen assets reported, but since that is already covered adequately in the Physical Theft and Loss section (and there is no way of proving definitively that data was actually compromised or simply at risk), we will move on to what we do know a bit more about. Namely, the 239 cases that resulted in confirmed data disclosure.

The breakdown of Public breaches across patterns has remained relatively constant for the last few years with Cyber-Espionage, Privilege Misuse and Miscellaneous Errors usually in the top three. Approximately 41% of the breaches in this vertical were related to espionage, which should come as no surprise, since it stands to reason that other governments want to know what our government is thinking regarding important issues, such as aliens, crop circles and microwave surveillance. As is generally the case when external espionage is conducted, the actors lean heavily towards the state-affiliated side of the spectrum as shown in Figure 26.

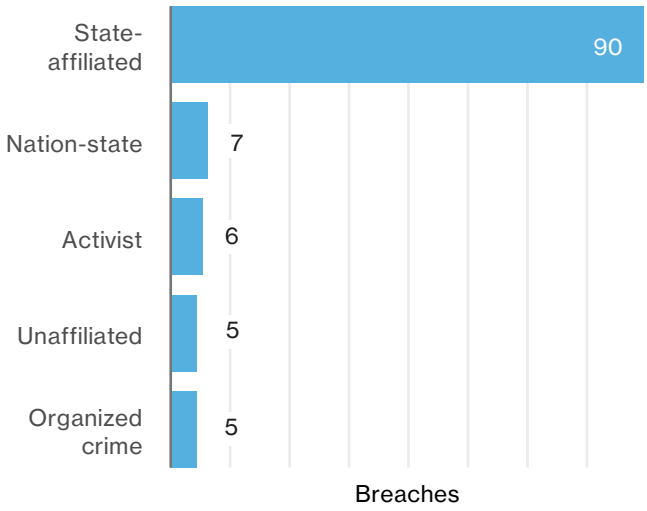


Figure 26: External actor varieties within Public breaches (n=113)

At this point the reader might wonder, "Am I reading the Manufacturing section again"? No, you aren't but there are some very definite similarities between the two. Both deal in secrets, and both appeal to a certain type of criminal who, by the way, tends to use very similar tactics.

Speaking of similarities, let us now turn to an interesting difference. For Manufacturing the actor was 93% external and they went after trade secrets 91% of the time. Here, we see a much greater number of internal actors making up a sizeable 40%[16], and the data variety was roughly equal between trade secrets and personal information. The insiders represented here in many instances fall into scenarios such as a police officer who misuses his or her ability to access criminal databases inappropriately. This scenario helps to explain the 13% of breaches with fun/curiosity as the motive.

[16] The 40% representation of internal actors is not all malicious activity – about half of insider representation stems from errors.

Finding your inner breach

As a rule, the government is only in a hurry if you owe them something. Otherwise their mills may grind fine, but they grind very slowly. Certainly, it would appear that is the case when it comes to breach discovery. In almost 60% of cases in Figure 27 (when discovery is known) it takes them years to learn that they have been breached. This may be due to the high number of espionage-related attacks, which often aim to cloak themselves in the victim network and remain hidden for a lengthy period of time. Or, it may be more representative of smaller government agencies that do not have the resources to spot the problem sooner. Either way, it is bad news for us humble citizens.

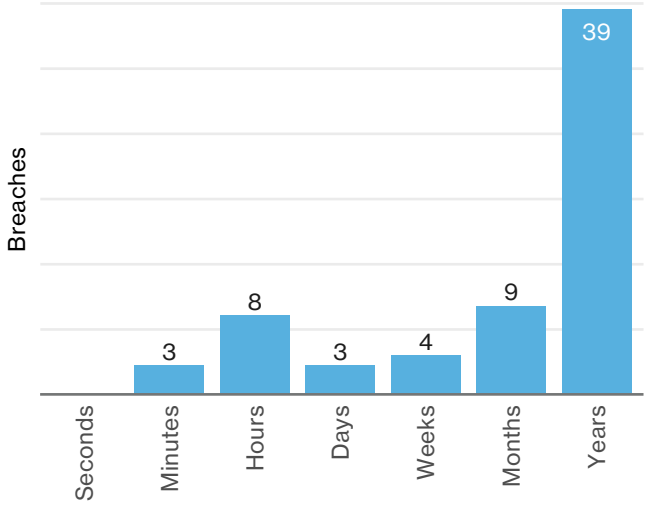


Figure 27: Time-to-discovery within Public breaches (n=66)

Things to consider:

Is that my data? – Know your own data, particularly the more sensitive type. Know where it resides, who has access to it, and who, in fact, does access it.

Exits are located above the wings – To prevent your data from flying out of your organization, set up controls to monitor data egress. If data leaves, you need to know about it and where it is headed.

Know your enemy – The public sector includes everything from organizations responsible for national security to local zoning boards. Understand what type of threat actor will be most interested in your department.

Retail

Frequency	326 incidents, 93 with confirmed data disclosure
Top 3 patterns	Denial of Service, Web Application Attacks and Payment Card Skimming represent 81% of all security incidents within Retail
Threat actors	92% External, 7% Internal, <1% Partner (incidents)
Actor motives	96% Financial, 2% Espionage, 2% Curiosity (incidents)
Data compromised	57% Payment, 27% Personal, 17% Credentials
Summary	Online retailers are consistent targets of DoS attacks, and POS environments continue to be compromised for financial motivations.

Ye olde e-commerce shoppe

The Retail industry, in terms of this report, is best segmented into brick-and-mortar retailers and online shopping (understanding that a retailer can be both). When analyzing incidents that involved a web application, we find that DoS attacks represent over 80% of incidents and are behind the majority of the 209 hacking incidents displayed in Figure 28. Breaches involving e-commerce sites typically involve hacking the web application – fairly straightforward. What is interesting is the varieties of hacking involved; credentials stolen from customers as part of phishing attacks are the predominant method of web application compromise. We are not convinced that retailers across the globe have cleared up all input validation vulnerabilities, but they are not landing in our combined dataset in significant numbers.

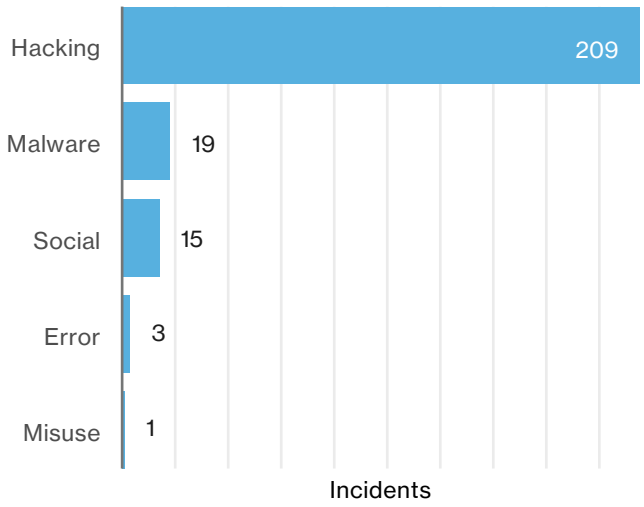


Figure 28: Frequency of threat action categories within Retail incidents involving web applications (n=214)

Are you being served?

Traditional storefront retailers have an entirely different attack surface; installation of skimmers inside gas pump terminals and ATMs account for almost 60% of non-e-commerce retailer breaches. We were surprised at the data found in Figure 29, specifically the lack of POS breaches within Retail. We will keep an eye on this as we don't have an enlightening explanation for it.

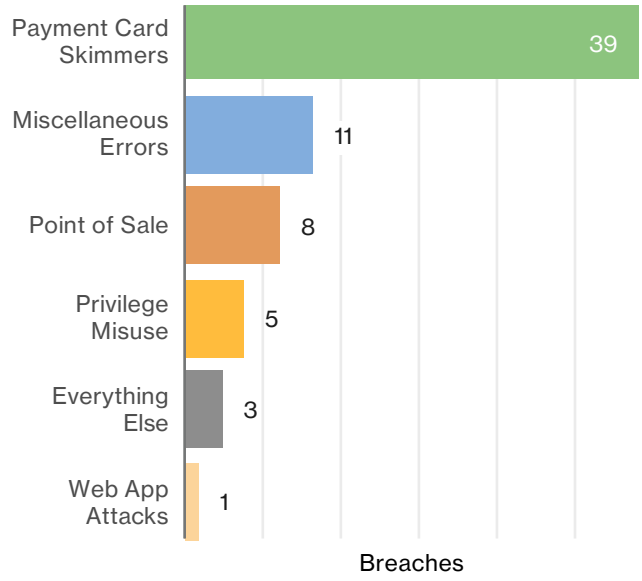


Figure 29: Frequency of incident classification patterns within Retail breaches not involving web application assets (n=67)

Size matters not?

Small retailers have historically been well represented in the Point of Sale Intrusions pattern. In the 2013 DBIR we called the scalable and automated attacks on internet-facing POS systems "smash-and-grab" operations. Large retailers were (thankfully) not being victimized due to rampant exposure of POS assets to the entire internet combined with default passwords. The 2014 DBIR focused on large retailers that began to disclose sizable breaches associated with POS attacks, and many times these involved credentials that were stolen, not guessed. This year we do not have any large retailers in the Point of Sale Intrusions pattern, which is hopefully an indicator of improvements and lessons learned. We are interested in finding out if smaller retailers also learned this lesson, or if single small breaches just aren't making it into our dataset.

Things to consider:

What do we want? Uptime! When do we want it? Now! – Make certain that you have DoS mitigation plans, know the limitations of your protection and the details of your provider agreement in the event of an attack.

No man is an island – But perhaps your assets should be. Keep critical assets on separate network circuits. The flatter the network, the easier it is to jump from an initial foothold to the promised land. Using default or easily-guessable passwords simply will not cut it in today's world. Implement multi-factor authentication across your enterprise but especially for remote access into payment card processing networks.

Attack the Humans!

Frequency	1,616 incidents, 828 with confirmed data disclosure
Top 3 patterns	Web Applications Attacks, Cyber-Espionage and Everything Else represent 96% of all security breaches involving social attacks
Threat actors	99% External, 1% Internal, <1% Partner (breaches)
Actor motives	66% Financial, 33% Espionage, <1% Grudge (breaches)
Data compromised	61% Credentials, 32% Secrets, 8% Personal
Summary	Social attacks were utilized in 43% of all breaches in this year's dataset. Almost all phishing attacks that led to a breach were followed with some form of malware, and 28% of phishing breaches were targeted. Phishing is the most common social tactic in our dataset (93% of social incidents).

Grifters and marks

Eagerness. Distraction. Curiosity. Uncertainty. All of these are drivers of human behavior, and one or more can be leveraged to influence someone to disclose information, click a link or wire money to a "vendor" account. Although there are a number of different types of social engineering attacks, we will be focusing on phishing and pretexting in this section given that together, they represented almost 98% of both incidents and breaches that involved a social action. Specifically, we will examine financial pretexting as it pertains to business email compromise (BEC). Then we will add some additional context by discussing some findings from the non-incident data acquired from security awareness training exercises.

Wings of reason

First, let's take a step back and examine the picture as a whole. There were a little over 1,600 incidents and more than 800 breaches featuring social actions in this year's corpus (all external actor driven). Phishing was again the top variety, found in over 90% of both incidents and breaches. Once successfully phished, a number of things can happen: software installation, influencing disclosure of sensitive data, repurposing of assets and so on. In last year's report, we discussed how the majority of remote breaches began with the same chain of events; phishing to gain a foothold via malware, then leveraging stolen credentials to pivot off of the foothold. It also holds true this year – 95% of phishing attacks that led to a breach were followed by some form of software installation.

The actor/motive combinations that represent the vast majority of phishing breaches fall into two categories: three-quarters were financially-motivated organized criminal groups, and a quarter were state-affiliated actors conducting espionage operations. A significant amount of the financially-motivated phishing was associated with banking Trojan botnets. In Figures 30 and 31, we remove the subset of botnet-driven phishing, and focus on human targets under the victim organizations' employ.

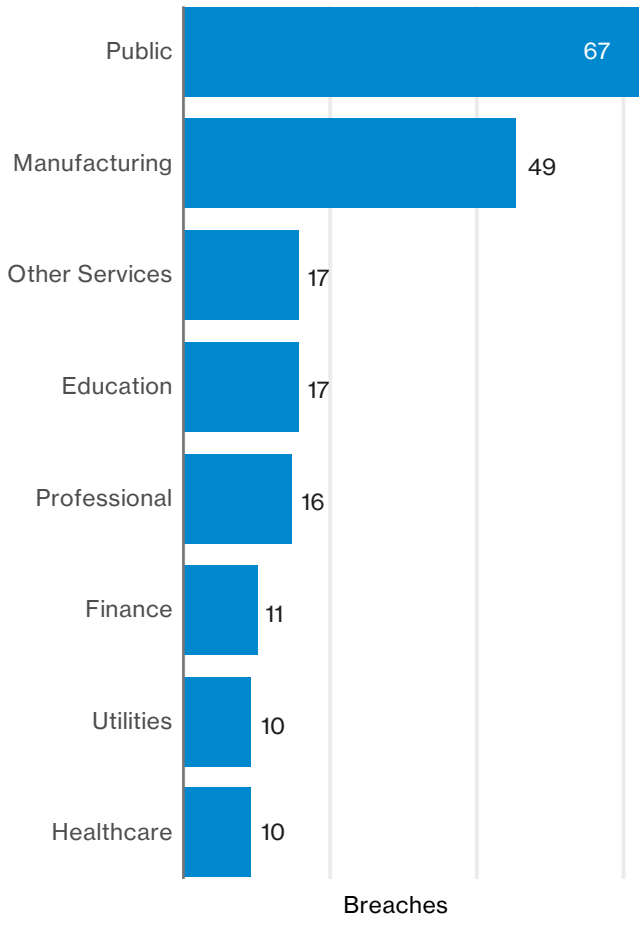


Figure 30: Top victim industry within social breaches, excluding botnet-driven campaigns (n=216)

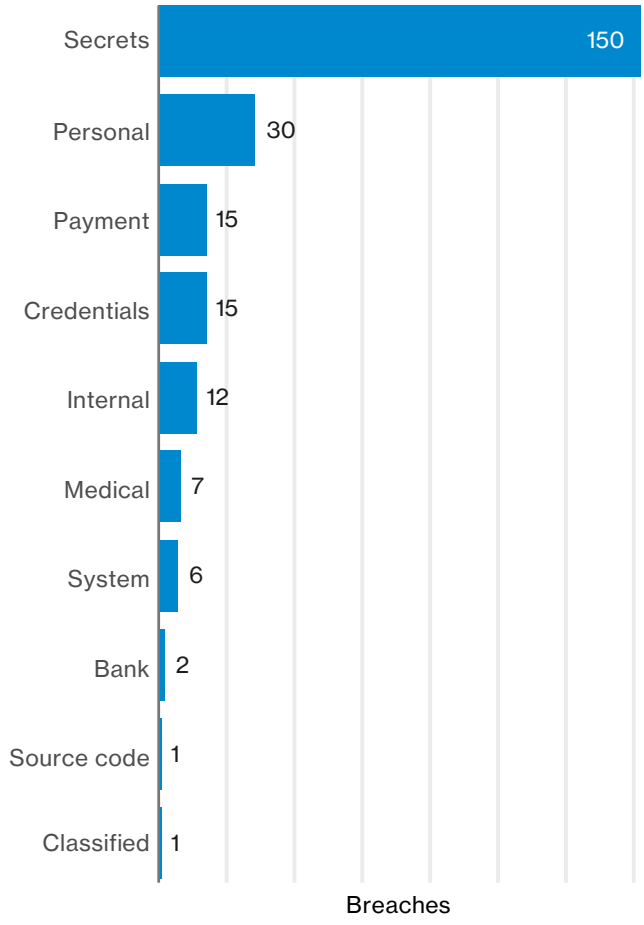


Figure 31: Compromised data variety within phishing breaches, excluding botnet-driven campaigns (n=211)

Public Administration and Manufacturing represent over half of the victims in this subset of data (where the industry was known). But since you've read the industry sections already, you probably guessed that. This is yet another example of how our data illustrates the strong association between cyber-espionage and phishing. Figure 31 adds to this story, with trade secrets as the top data variety targeted, followed by personal information.

Security through education

The main focus of this report has, and always will be, the breach data. However, we also review results from our non-incident datasets not only to glean what we can from them on their own merit, but also to provide context for our breach corpus. Our non-incident phishing data is comprised of 7.3 million records (campaign data down to user level), over 14,000 campaigns, and over three million unique users across 2,280 different organizations.

Clicks

7.3% of users across multiple data contributors were successfully phished – whether via a link or an opened attachment. That begged the question, "How many users fell victim more than once over the course of a year?" The answer is, in a typical company (with 30 or more employees), about 15% of all unique users who fell victim once, also took the bait a second time. 3% of all unique users clicked more than twice, and finally less than 1% clicked more than three times.

Reporting

Now that we have an idea of how many people were phished – and how many were phished repeatedly – let's see how many reported the event. In other words, those who "saw something and said something." This is paramount. You're never going to completely stop phishing emails getting through and being clicked, but if you have a good process for detecting and handling them, they're less likely to impact your organization. Some (but not all) of the sanctioned phishing campaigns provided a mechanism for users to report the email. Of those that had recorded instances of reporting, the percentage of users who reported was 20%. So, there are approximately 1 in 5 good Samaritans out there who upon noticing something odd, follow policy and report it. Ah, faith in humanity is restored! Reporting is key to limiting the effectiveness of phishing that makes it past your email filters. We are happy that the reporting percentages from the aforementioned subset of campaigns are higher than the overall click percentage, but this is definitely a number we hope to see increase in the future[17].

You sit on a throne of lies!

Pretexting is a form of social engineering focused on creating a scenario, or pretext, to influence your target. Yes, it's a bit like dating in high school only more cyber-y. The real pros seem to be organized criminal groups who are masters at tall tales aimed at financial gain. Although pretexting was not as common as phishing, there are a few important things to note. It was almost always targeted in nature (and hence over half of the marks were from the finance department), which means actors are doing their research to identify the right employee, and invent a believable story.

This year's data features numerous incidents involving the impersonation of an executive to trick someone to transfer money (sometimes six-figure amounts) from the corporate accounts. Many of these pretexting incidents were discovered by internal financial audits and a few by fraud detection. In these cases, external fraud detection is actually the preferred method as it typically means the transfer was blocked, whereas internal audits discovered the fraud after the proverbial horse had left the stable. Email was the top vector of communication, accounting for 88% of financial pretexting incidents[18], with phone communications in second place with just under 10%.

Areas of focus

The data shows simulated phishing makes a difference, but someone will always click. Focus on detection and reporting of clicks rather than just prevention. Implement and test a phishing response plan that:

- Empowers users to alert on "phishy" emails.
- Identifies phishing recipients and recalls the email.
- Identifies phishing recipients who clicked the link or opened the attached file.
- Expires credentials accessed from compromised hosts.
- Investigates post-click communications from the infected hosts.
- Isolates the system so that the malware cannot spread.
- Identifies and removes the malware.
- Considers the use of sandboxing technologies, including operating systems that sandbox applications natively. Also discounts cloud applications that sandbox emails and Office documents from the user device.

Prepend external emails with [External] or [E] or [Not from the CEO!] in the subject header to help detect spoofed messages purporting to be coming from a big wig. That's not enough though, as some BEC involves hacked email accounts. So while the email is not coming from the executive, it is coming from his/her legitimate email address. Have a process for approving payments that includes some form of communication other than email. Train the employees who can pull the trigger on money transfers that they will never ever be asked over email to transfer funds outside of the documented approval policy. Work with your banking institution to block and alert on large or anomalous transfers of funds.

[17] From campaigns that featured at least one tracked instance of reporting. Most campaigns did not contain a reported phish. This could be because there isn't a trackable reporting tool built in, or it was not implemented by the customer. It could also be because the users did not report it. We cannot say for sure, but are optimistically inferring in those cases that reporting was not tracked.

[18] We use phishing for emails with a particular hook in the form of a link or attachment as the "bait", whereas pretexting involves a persona and dialogue between the actor and victim.

Ransom Notes are the Most Profitable Form of Writing

Ransomware is the latest scourge of the internet, extorting millions of dollars from people and organizations after infecting and encrypting their systems. It has moved from the 22nd most common variety of malware in the 2014 DBIR to the fifth most common in this year's data. It is our pleasure to turn this section over to McAfee, who leverage their threat intelligence to shed some light on significant ransomware technical enhancements that are transforming both the nature of the threat and ways in which the security industry is fighting back.

The rise of ransomware

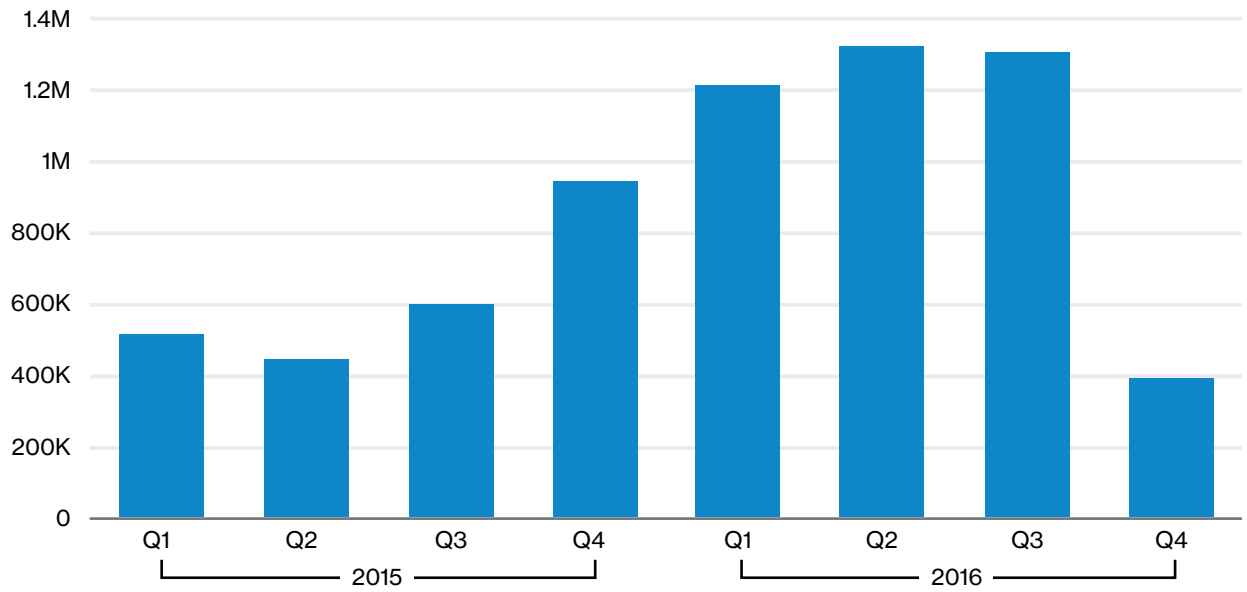


Figure 32: New ransomware samples per quarter – Source: McAfee Labs

While ransomware dates back to 1989[19], in the past year we have seen more technical and process innovation in ransomware than we have seen since the invention of Bitcoin-enabled anonymous payments. Fueled by the success of early attacks, the number of ransomware incidents increased to 228 in this year's report from 159 in the 2016 DBIR. Figure 32 above supports the DBIR findings.

Through most of 2015 and 2016, telemetry at McAfee Labs recorded a steady increase in new ransomware samples, as bad actors modified code and implemented new attack forms, encryption methods, exploit kits and evasion techniques. However, there was a slight decline in new samples in Q3 2016, and a drastic 70% drop in Q4. This big decline is mostly due to a reduction in generic ransomware detections, as well as a decrease in Locky and CryptoWall variants.

[19] https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/

Technical and process innovations

Last year we saw impressive innovation in ransomware technology and extortion methods. Moving on from file encryption – the standard practice of ransomware authors – attackers introduced master boot record locking, and partial and full disk encryption in an effort to make it more difficult to recover systems without paying. They also experimented with a variety of methods to avoid detection by security sandboxes. These included execution time differences between real and virtual machines, unexpected command-line arguments and an abnormally short list of Microsoft Office recent files. Mid-year, we witnessed a sudden shift in exploit kits used for ransomware from Angler to Neutrino, followed by another shift in September from Neutrino to RIG. Tracking these kits helps identify which vulnerabilities are targeted, which patches to prioritize and how to strengthen defenses.

Encouraged by the profitability of ransomware, criminals began offering ransomware-as-a-service, enabling anyone to extort their favorite targets, while taking a cut of the action. This approach was followed by a variety of experiments in ransom demands. Criminals introduced time limits after which files would be deleted, ransoms that increased over time, ransoms calculated based on the estimated sensitivity of filenames, and even options to decrypt files for free if the victims became attackers themselves and infected two or more other people. Multi-level marketing at its finest!

Changes to targeting and attack vectors

Perhaps the most significant change to ransomware in 2016 was the swing away from infecting individual consumer systems toward targeting vulnerable organizations. Overall, ransomware is still very opportunistic, relying on infected websites and traditional malware delivery for most attacks. Looking again through the lens of DBIR data, web drive-by downloads were the number one malware vector in the 2016 report, but were supplanted by email this year. Social actions, notably phishing, were found in 21% of incidents, up from just 8% in the 2016 DBIR. These emails are often targeted at specific job functions, such as HR and accounting – whose employees are most likely to open attachments or click on links – or even specific individuals.

Healthcare ransomware campaigns got the most publicity in 2016, due in part to the potential impact that obscuration of medical data can have on patient care. The DBIR data reveals that Public Administration organizations were the number one industry target, with Healthcare number two and Financial Services number three. Ransomware campaigns targeting organizations often have additional characteristics, such as credential theft to spread the attack throughout the organization, delayed encryption to infect as many machines as possible before detection, and code that targets corporate servers as well as user systems.

The fall of ransomware, or how the security industry is fighting back

The security industry is not taking the rise in ransomware lying down. Security vendors are working on multiple fronts to: detect ransomware before infections become critical, protect individuals and organizations from criminal campaigns, and help rescue ransomed systems without enriching attackers.

Security software

The expected response from the security industry to most threats is enhancing tools to enable earlier detection. Combating ransomware is no exception. Endpoint protection systems can now detect millions of ransomware samples, with more added as they are discovered. Because this process is obviously insufficient to stop all attacks, the security industry has also added detection techniques such as sandboxes that can mimic a user environment to catch obfuscated ransomware, behavioral analysis to prevent ransomware from executing completely and file creation blocks to prevent ransomware from writing encrypted files. Although these actions have increased detection and prevention rates, the volume of ransomware variants and the criminals' speed of adaptation mean the techniques are unlikely to be 100% effective, thus necessitating further actions.

Threat intelligence sharing

In addition to catching criminals in the act, security vendors, law enforcement agencies and organizations of all sizes are increasingly sharing threat intelligence information to help detect ransomware (and other malicious activities) before they reach systems. The rapid sharing of threat information acts like a vaccine; immunizing systems and organizations from known and suspected ransomware attacks, before they can cause lasting damage.

Working with law enforcement

The security industry is also collaborating with law enforcement agencies to disrupt and take down malicious infrastructure and, when possible, to identify and arrest those responsible. Several takedowns took place in 2016 and more are underway.

nomoreransom.org

Perhaps the most significant action taken to combat ransomware in the past year is the creation and ongoing development of the No More Ransom! collaboration. Begun by four founding members in July 2016, this group now comprises 57 members, including security vendors, consultants, law enforcement agencies, incident response groups, insurance companies, information sharing centers, and hosting companies that provide necessary web services. The group's goal is to share information, educate users and help victims recover their encrypted data without having to pay ransomware attackers[20].

To that end, nomoreransom.org currently hosts 27 decryption tools, which can recover files from a wide range of ransomware families. No More Ransom! calculates that they have successfully diverted more than US$3 million from criminals by offering free decryption tools to thousands of victims around the world.

[20] Verizon is now part of the No More Ransom! collaboration.

Introduction to Incident Classification Patterns

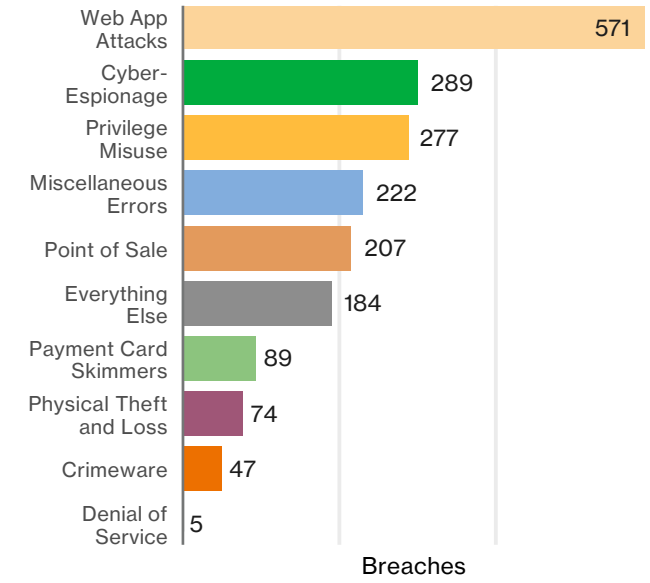


Figure 33: Percentage and count of breaches per pattern (n=1,935)

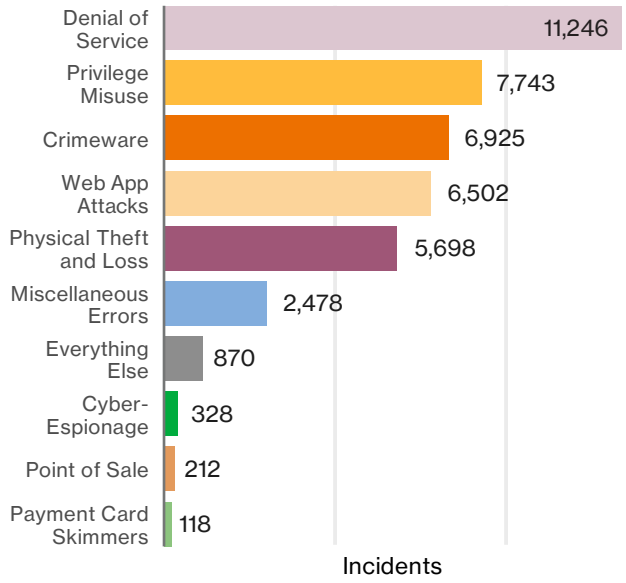


Figure 34: Percentage and count of incidents per pattern (n=42,068)

Legend has it that Sir Isaac Newton discovered gravity when an apple fell on his head. Likewise, Einstein was purported to have come up with the theory of relativity in a dream. Inspiration can strike anywhere. A few years ago, we on the DBIR team noticed as a result of a casual conversation that most breaches seemed to fall into a few broad categories or patterns that kept repeating themselves. Thus was created the nine patterns that we have showcased in subsequent reports. Naturally, we are not comparing this observation to the genius of Einstein or Newton, because clearly our inspiration is of much greater importance[21].

We first included the incident patterns in the 2014 report when over 90% of confirmed breaches fell into one of them. This year 88% of breaches fall into those same basic patterns. Web Application Attacks remains the most prevalent, helped again by a multitude of botnet data that skews the data toward that pattern (see Figure 33). If we were to rank this year's set of breaches without that botnet, then Cyber-Espionage would assume the top spot and Web Application Attacks would fall to sixth place.

Examining all incidents (Figure 34) rather than breaches shows that DoS attacks dethroned Miscellaneous Errors (last year's #1) by a large margin in 2016.

As we state each year, the real value of the incident patterns is not in how they compare to each other, but as guidance on what is most likely to negatively impact your organization. For example, if you are in the Accommodation industry your main areas of concern center on POS intrusions. On the other hand, retailers have less of a worry about espionage than manufacturers. Does that mean that those are the only areas that you should protect against if you find yourself in one of those demographics? Of course not, but understanding these areas of concern goes a long way to help struggling security professionals gain insight on where and how to invest their limited resources. The patterns provide a quick and easy way to assess a baseline of where the most likely danger will arise – you are less likely to be bitten by a snake in Antarctica than Arizona.

Think of the patterns as reading your security horoscope (only based on data rather than celestial movements). Of course, this report can only inform the reader of the trends we observe and not actually foretell your entire future. However, our data does indicate that 7, 29 and 60 are your lucky numbers, and you will find love and riches on Flag Day.

[21] What?!

Crimeware

All instances involving malware that did not fit into a more specific pattern. The majority of incidents that comprise this pattern are opportunistic in nature and are financially motivated. This pattern will often affect customers and is where “typical” malware infections are placed.

At a glance

Top Industries
Public and Manufacturing
Frequency
6,925 total incidents, 47 with confirmed data disclosure
Key Findings
Ransomware has continued to increase for the last few years and is now the number one malware variety within this pattern. When examining non-incident data, 99% of malware is sent via email or webserver.

The Crimeware pattern has always been a bit like having a rich uncle who constantly drops hints that he will give you part of his fortune on your birthday, but it is always on your next birthday. In other words, he appears to have the money, he appears to want to give it to you, but, alas, he never does. Year after year, this pattern is comprised of thousands of incidents, but only a handful of actual data breaches or incidents that provide enough information to be actionable or even very useful for analysis.

Typically they come to us from Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs), which derive the data from a large variety of contributors and are very loosely categorized in aggregate. Nevertheless, we soldier on and, in spite of the lack of detail, we can glimpse useful data points from time to time.

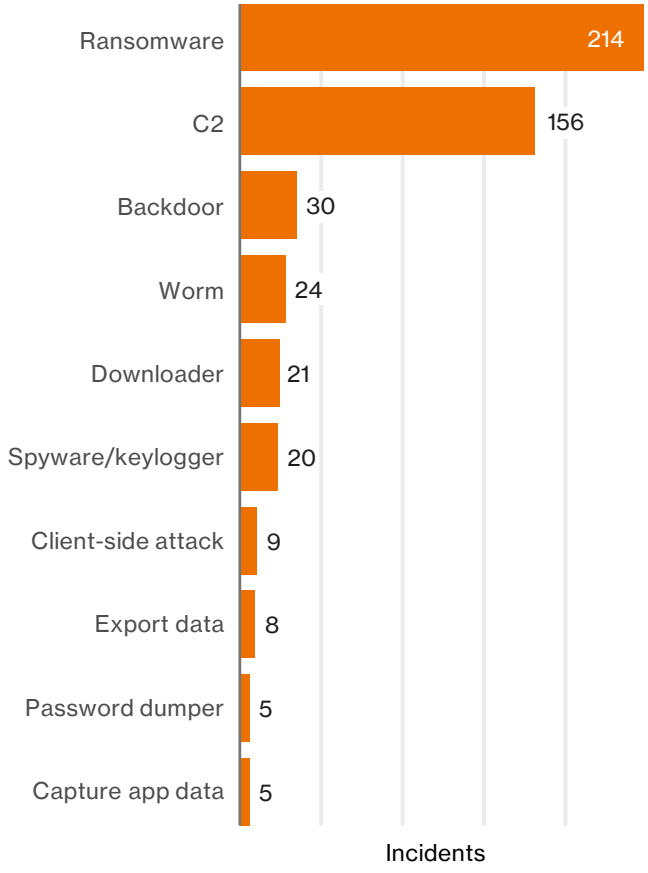


Figure 35: Top malware varieties within Crimeware incidents (n=430)

Ransomware! Why didn't I think of that?

Ransomware, as you no doubt know, is a type of malware that can infect your system and then be used to encrypt your data until you pay the "ransom" the criminal demands to give you the data back. If you are an unscrupulous villain it is a great way to make a living. In the overall dataset, there are actually more botnet malware incidents than ransomware. However, bots tend to fall in the Web Application Attack pattern as they routinely steal credentials for use against financial websites. That leaves ransomware as the reigning champion in the Crimeware patterns shown in Figure 35. This isn't out of nowhere like Leicester City, ransomware has been increasing each year. This is likely a trend we should expect to continue as it offers the criminal a number of benefits. Ransomware short-circuits the normal attack path, so the actor doesn't have to persist. It's easily monetizable, very fast and represents a low risk for the attacker.

When things go right

There is some good news, however. When we look at our non-incident data (malware detonations – a sample of 50 million on-the-wire detections), over 99% of malware is sent by either email or web server. This means it's coming through your mail server or web proxy where you can take steps to squash it. This dataset of successfully squashed malware supports the data taken from our incident corpus that also shows that almost 80% of crimeware is email-based and drive-by downloads check in at 8%.

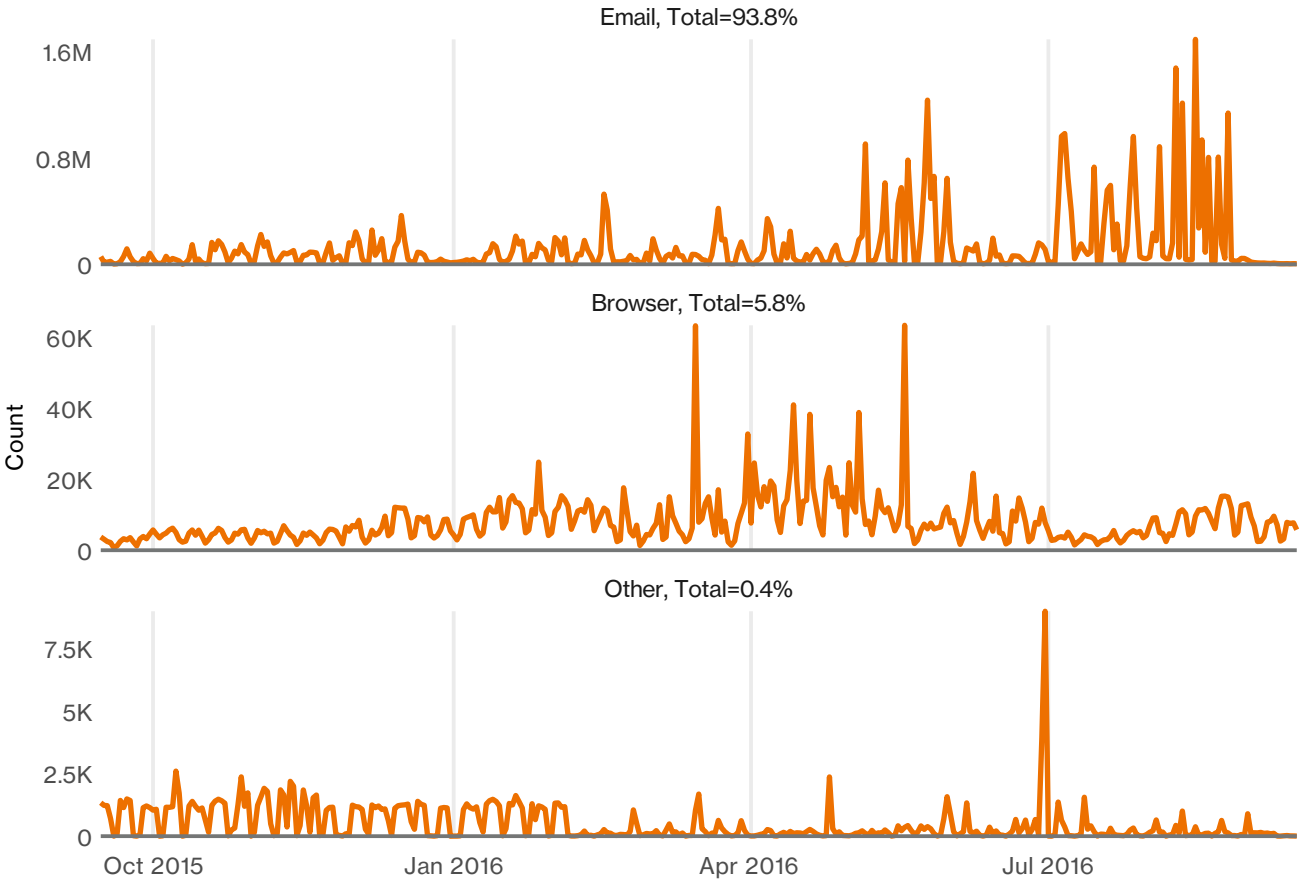


Figure 36: Malware count per day by vector (n=50,366,956)

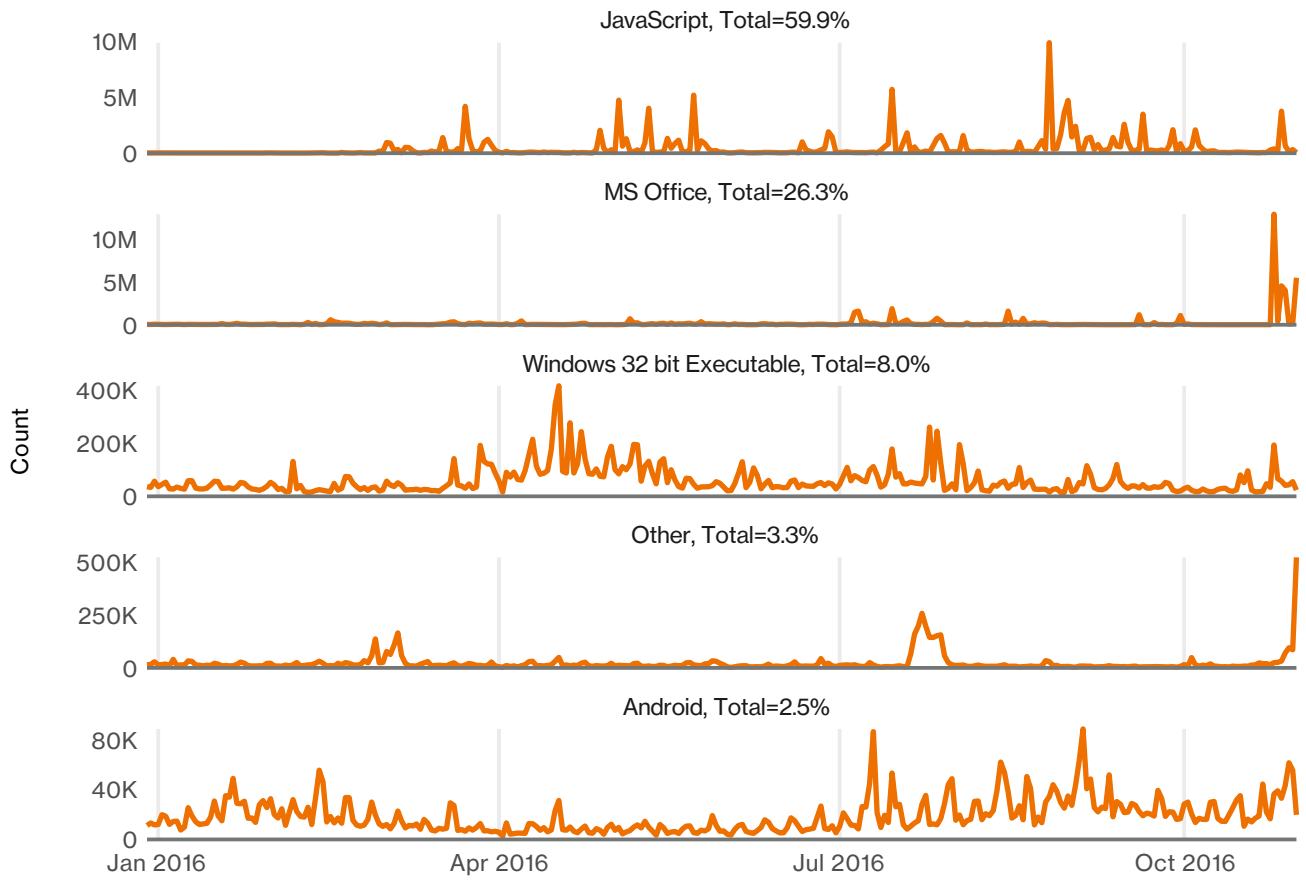


Figure 37: Malware count per day by file type (n=227,109,781)

It's also streaky, as we can see in Figure 36. It's very cyclical, likely driven by the work week, with significantly larger weeks between March and August, with peaks differing between the delivery methods.

Shifting gears a bit and diving into another non-incident dataset, Figure 37 sheds light on how malware is packaged. The main takeaway is the prominence of JavaScript malware, followed by malicious Office documents and 32 bit Windows executables.

While the VERIS framework has enumerations for both malware variety and vector, this data gives us information on what file types are most often used to smuggle it in.

Areas of focus

Unless your organization mails around software updates, you need to block executables at your email gateway. Disable macro-enabled office documents[22], specifically MS Word and Excel, for anyone who doesn't explicitly need it. Stopping malicious JavaScript starts with blocking .js via email and keeping browser software up to date.

Implement a robust malware defense strategy that incorporates client-based malware detection, application whitelisting, sandboxing and network defenses to detect communications from infected hosts.

Prioritize patching vulnerabilities associated with browser exploitation. This includes the browser software, but also plug-ins.

[22] https://decentsecurity.com/block-office-macros/

Cyber-Espionage

Incidents in this pattern include unauthorized network or system access linked to state-affiliated actors and/or exhibiting the motive of espionage.

At a glance

Top Industries
Public, Manufacturing, Professional Services, Education
Frequency
328 incidents, 289 with confirmed data disclosure
Key Findings
Targeted phishing campaigns continue to be the tip of the spear for espionage-related breaches. Educational organizations made a bigger appearance in the victim base this year.

Strategic manoeuvres in the dark

Acquisition of information to obtain a strategic advantage has been around since the days of Sun Tzu, who wrote of five classes of spies: local, inward, converted, doomed and surviving. We are not quite sure what class a dude crafting a malicious PDF is, so we will create a sixth class – comfy spies.

Unlike organized criminal groups, who are typically after directly monetizable data, state-affiliated actors are playing the long game and are more selective of their targets. Figure 38 lists what industries represent the unfortunate chosen ones.

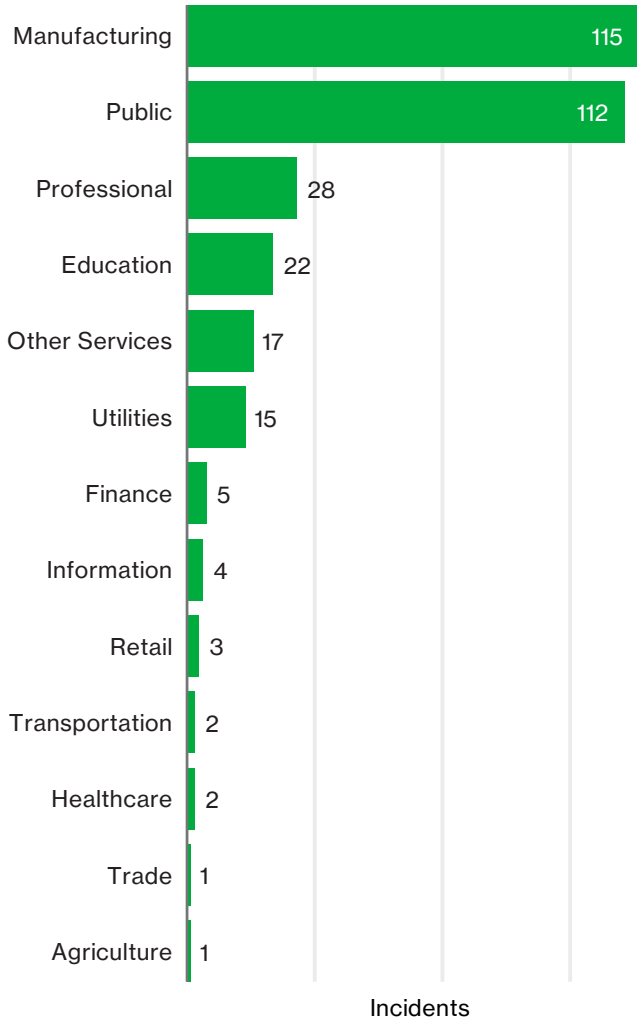


Figure 38: Count and percentage of breaches within Cyber-Espionage (n=271)

Manufacturing and Public Administration lead the pack of targeted industries yet again, and Professional Services take the bronze for the second straight year. The interesting change is the rise of academia as a target of these attacks. Colleges are centers of innovation and are building technologies that would certainly be targeted by state-affiliated groups. The chemical laser prototype designed by Pacific Technical University students in support of the 1985 Crossbow project is an excellent, albeit completely fictional example. It is important to understand that these attacks with higher levels of pre-attack research, sophistication, patience and targeting will not be documented at the rate of opportunistic attacks. Even if your industry is not well represented in the statistics in Figure 38, if you have – or may be perceived to have – useful information, then you are a potential target.

The spy who phished me

Over 90% of breaches were attributed to state-affiliated groups, with nation-states, competitors and former employees present, but not nearly as common. The tactics used have remained consistent, with phishing remaining a favorite technique of attackers[23]. Typically, an attacker will send a malicious email with an attachment to their intended victim. If the attachment is opened, it will drop command and control malware to establish and maintain control of the device. From there the methods used by the actor are more about blending in with the crowd. They have accomplished the first phase of their mission, and typically avoid noisy approaches like launching a barrage of exploits to escalate privileges. Unlike millennials binge-watching shows on Netflix, instant gratification does not influence post-compromise actions.

Figure 39 sheds a bit of light on the types of activities that occur once the beachhead is established, such as downloading additional malware, mapping out the internal network, and using keylogging and password dumping malware to advance towards the finish line of exportation of data. Seven of the top 15 threat action varieties are functionalities of malware, and the data shows that the malicious payloads are commonly delivered via email (73%) and drive-by downloads (13%).

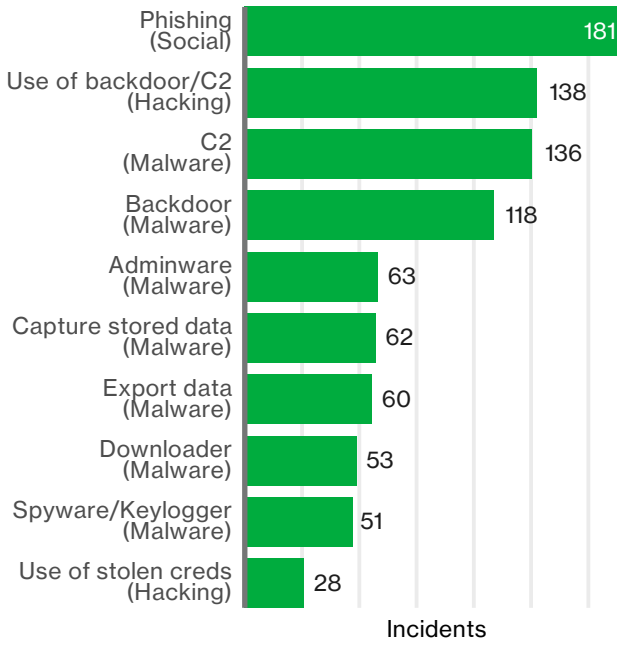


Figure 39: Top threat action varieties within Cyber-Espionage, (n=271)

Areas of focus

Make it difficult to establish a foothold in your internal network. Anti-malware protection at the email gateway, security awareness training and keeping web browsers (and plug-ins) up to date are essential controls. Test and implement Data Execution Prevention (DEP) and Endpoint Threat Detection and Response (ETDR) technologies.

If a potential phish is identified, formalize a process for users to bring it to the attention of the security team, and for your organization to gather the necessary information regarding the behavior of their device. Find out who they have been talking to both internally and externally. Ensure you have the monitoring and logging enabled to review account and device activity.

Reduce the impact of a compromised user device. If a username and password is the only barrier to escalating privilege or compromising the next device, you have not done enough to stop these actors. Network segmentation establishing more granular security zones that require multi-factor authentication may require the attackers to shift their tactics and stand out from the crowd.

[23] If you skipped to this section before reading "Attack the Humans!" flip to that page next.

Denial of Service

Any attack intended to compromise the availability of networks and systems. Includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.

At a glance

Top Industries
Entertainment, Professional Services, Public, Information, Finance
Frequency
11,246 incidents, five with confirmed data disclosure
Key Findings
When we knew the organization size, DDoS attacks were disproportionately (98%) targeted at large organizations. Most attacks are not sustained for more than a couple of days.

HTTP 503 Error: Service Unavailable

For people in charge of keeping their web presence up and running on all cylinders, DDoS attacks (or the threat thereof) can be in equal parts frustrating and annoying. Like self-diagnosing the root cause of a headache by reading internet forums[24], you research the newest, biggest, attack in the news and officially become a worrywart.

There is a lack of ultimate control associated with this attack. You can't prevent attempts, and likely need to rely on help from some upstream allies to defend if/when attempts are made. If someone points their botnet at you, hopefully you have a plan of action to engage your ISP(s) and DoS mitigation service to thwart the attack with minimal interruption or service degradation. Either way, it's akin to watching the end of the salmon run. Sure, there are a lot of salmon, but you never think about where they all came from or how many ended up as bear food.

The salmon/packet analogy extends to the beginning stages of the DDoS process. Our ocean is the internet filled with compromised devices being monetized as worker bees in botnets. The creation of Mirai botnets using devices hacked via default telnet credentials[25] is a timely example.

[24] It's (likely) not a tumor!

[25] Much of the focus was around the Internet of Things (IoT) aspect. If you are on the other end of an availability attack, you don't care that the botnets are cameras versus desktops. Also these devices with remote-access ports open to the internet and default credentials resemble an early 90s insecure server, just in a smaller plastic box. Don't focus on the buzzword, but on the vulnerability that made compromise so darn easy.

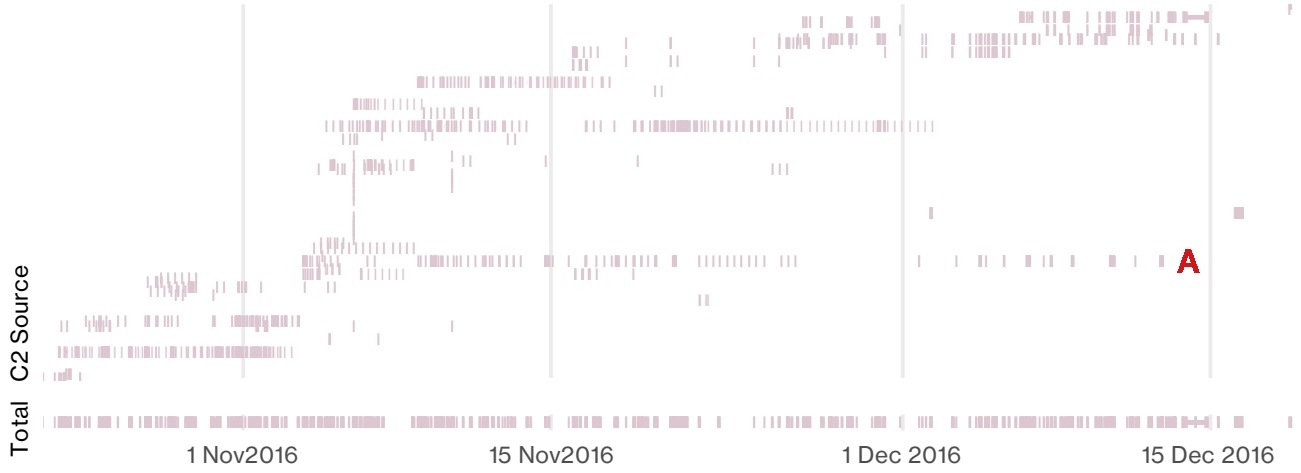


Figure 40: Taskings of Mirai botnet per C2 source over time

Running the numbers

After the botnet is created, devices are tasked to send the packets from the four corners of the internet, up the stream, and to their target. Figure 40 displays the tasking of various Mirai botnets by roughly 50 C2 sources from October 22, 2016 to December 18, 2016. It's a bit anecdotal, but it does demonstrate one thing. While we heard a lot about Mirai, it's not this juggernaut that is continuously attacking the world. Many C2 sources tasked it for a period of time and then never again. It appears only one source **A** was continuously active between the beginning of November and mid-December. Only the total aggregate begins to approach a constant use of the botnet.

The net is vast and infinite

From there, the packets must cross the ocean of the internet. Along the way, some get "eaten" by network infrastructure blocking packets exceeding rate limits on certain protocols. Others are swallowed by DDoS mitigation equipment used to minimize traffic. Still, many make it upstream to their intended target.

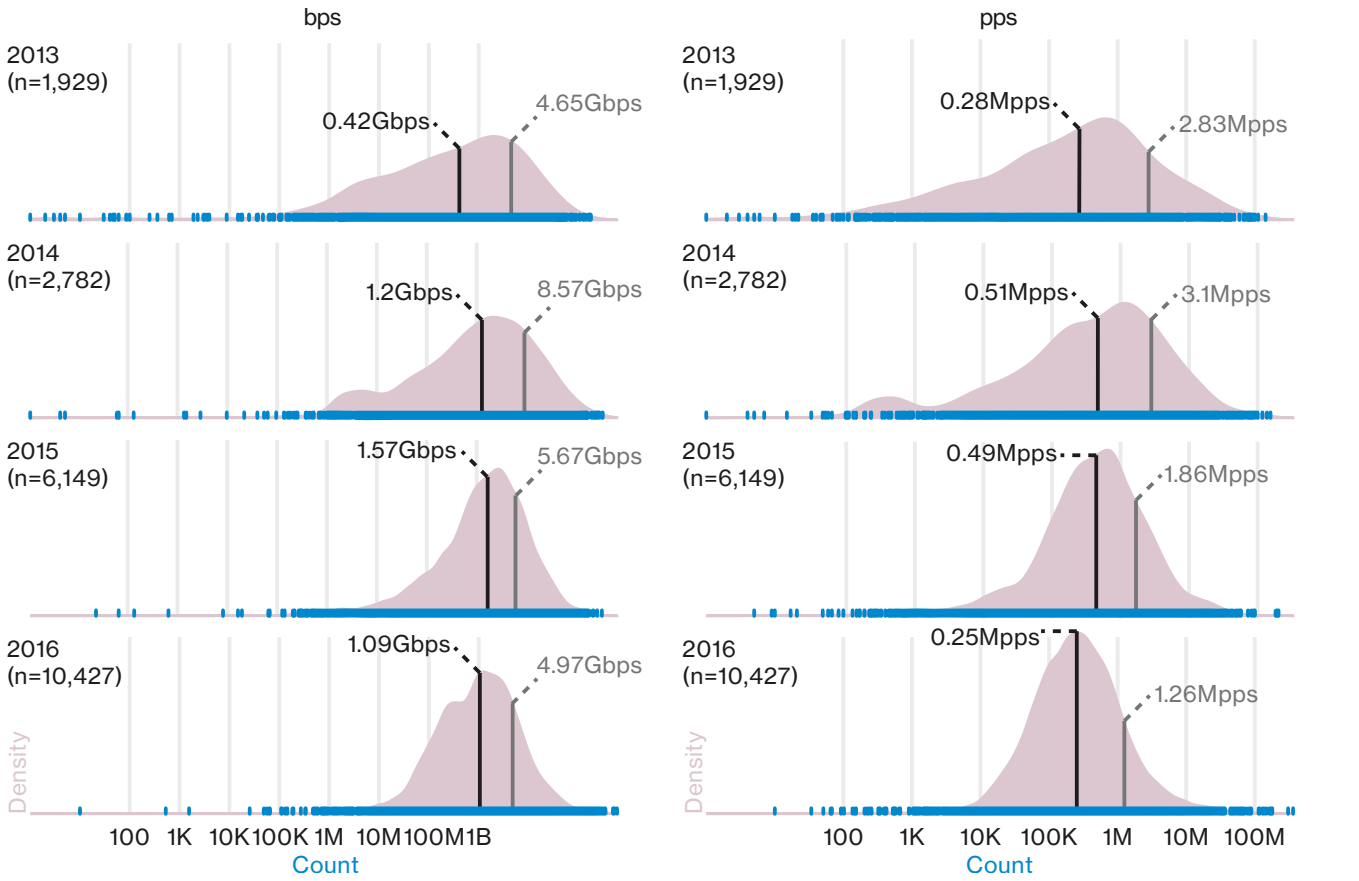


Figure 41: DoS attack bandwidth and packet count levels

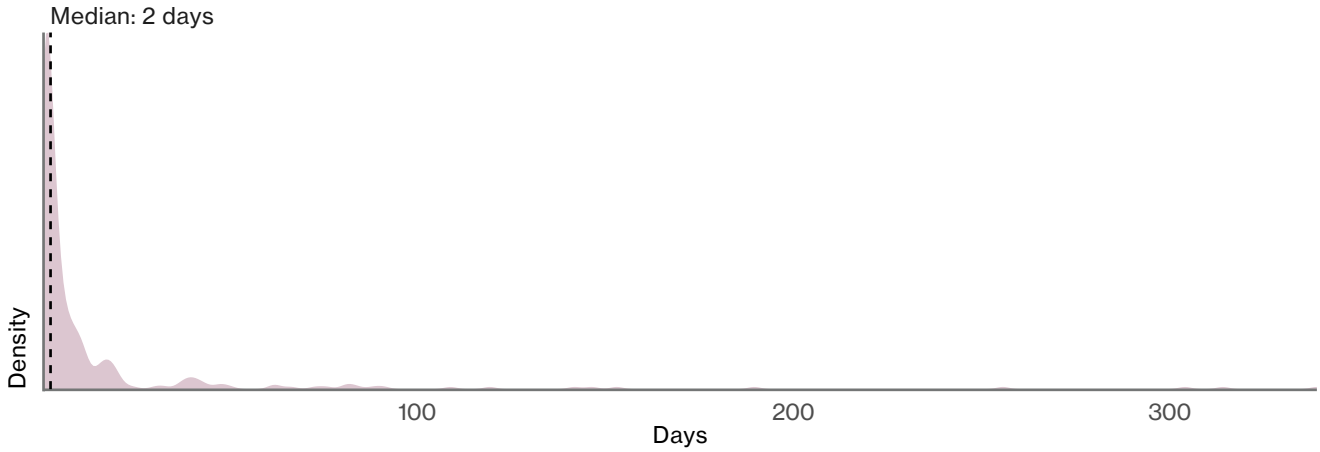


Figure 42: Density plot of days per year under attack by organization

Figure 41 shows that the median attack size of DDoS incidents measured by mitigation services has actually decreased. There's also a wide range for how long organizations are attacked.

In Figure 42, we can see that only a few companies get attacked constantly throughout the year. However, the majority are only dealing with these barrages for a few days.

Areas of focus

Understanding the types and levels of mitigation you need is key. What assets do you have exposed to potential DDoS? What is the impact of not having those assets? Business as usual? End of the world? DDoS services all have different capacities, detection methods and types of services. Do you need to resist the median attack (both in size and duration) or do you want to be safe from the bigger and longer attacks that are possible?

TDoS – Because you didn't have enough problems already

Packet-based DDoS isn't the only type of DoS around. Telephone Denial of Service (or TDoS) is another attack type made possible by the rise of Voice over Internet Protocol (VoIP) calling systems.

Like traditional DDoS, TDoS can be a real threat to organizations. Services exist to help mitigate the risk and are improving with advancements in data science and machine learning. So, just like DDoS, weigh the business impact of not having defenses vs. the cost of acquiring them. If you're going to need them, it's better to know how to get them before the attack starts.

Figure 43 provides an anecdotal example of a single TDoS attack and does not imply anything about all TDoS, the average TDoS, or anything else. It is interesting (in our humble opinion) and can help give you an idea about what this attack can look like.

- **A** represents a normal day.
- At **B** the TDoS starts.
- For a while it looks like things are keeping up.
- But at **C**, the call volumes increase from the existing sources.
- And at **D** a second source is added to the attack.
- The attack stops for about a day, but returns at **E** and to a lesser extent, **F** (without the source from **D**).

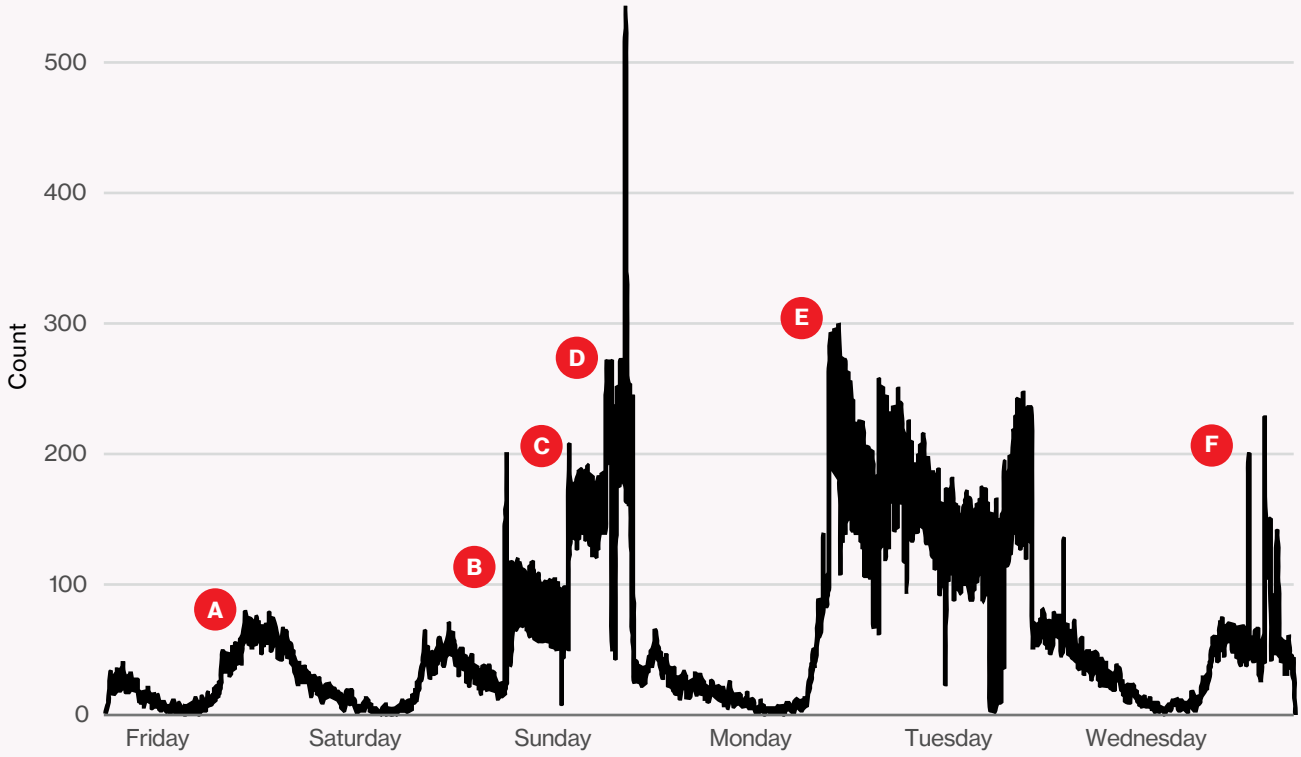


Figure 43: Call volumes during TDoS attack

Insider and Privilege Misuse

All incidents tagged with the action category of Misuse—any unapproved or malicious use of organizational resources—fall within this pattern. This is mainly insider-only misuse, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well.

At a glance

Top Industries
Public, Healthcare, Finance
Frequency
7,743 total incidents, 277 with confirmed data disclosure
Key Findings
When the threat actor is already inside your defenses, they can be quite a challenge to detect – and most of the incidents are still taking months and years to discover. Most of these perpetrators are financially motivated, but don't rule out those who want to use your data for competitive advantage.

With employees like these, who needs enemies?

Malicious insiders are not always the people snarfing up vast troves of data and packing it off to WikiLeaks tied up with a bow. Those breaches are the ones that get the headlines, the glory and, potentially, land the actor in a prison cell. What is more common is the average end-user absconding with data in the hope of converting it to cash somewhere down the line (60%). Sometimes employees let their curiosity get the better of them and they engage in some unsanctioned snooping (17%). These misuse scenarios are reflected in the types of data compromised. Personal information and medical records (71%) are targeted for financial crimes, such as identity theft or tax-return fraud and occasionally just for gossip value.

This pattern also features espionage motives (15%) involving data stolen to either start up a competing company or take to a new employer. In those cases, sensitive internal data and/or trade secrets were stolen (24%), which could include sales projections, marketing plans, the Glengarry leads, or other intellectual property.

Threat actors within this pattern are kicking back inside your perimeter, plundering your databases (57%), rifling through your printed documents (16%) and accessing other employees' email (9%).

Figure 44: Percentage of breaches per threat actor category within Insider and Privilege Misuse (n=277)

In this pattern, you'd expect the internal actor to feature prominently – and they do. But while internal actors accounted for 89% of the incidents, we see in Figure 44 that External and Partner actors were also represented. That is the pattern where we most commonly see multiple actors that are potentially colluding (8%).

The insider threat, while not as common in breaches as external actors, is still very significant, accounting for 15% of breaches (across all patterns, not including errors). The practice of limiting, logging and monitoring internal account usage extends beyond rogue employees. One of the main goals of external adversaries is to gain access to legitimate internal credentials to advance their assault.

Even if everyone on your payroll is a model employee devoid of greed, dishonesty or malice, the same security controls that are designed to identify employee misuse can also detect external attackers masquerading as privileged users.

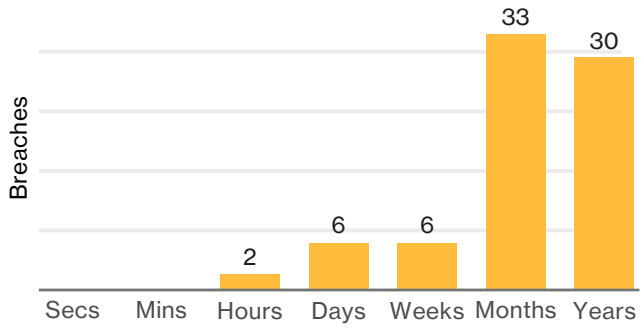


Figure 45: Breach discovery timeline within Insider and Privilege Misuse (n=77)

The discovery timeline for this pattern, displayed in Figure 45, shows that these breaches are more likely to take months and years to detect rather than weeks or less. When it takes years to discover your organization has lost control of sensitive data, it is a bit like watching a celestial nova – the original event occurred far back in the past, but we're just now learning the details.

Areas of focus

This section has touched on the following commonalities: Public Administration and Healthcare industries, inappropriate access of databases, financial motivation, as well as curiosity. If we take those data points we can tell three common stories.

- Healthcare workers are accessing medical databases either to steal PII for identity theft, or snooping on patient medical histories.
- Public administration breaches often involve workers employed in law enforcement that are accessing criminal databases to get dirt on somebody.
- Acceptable use training, and a banner that makes it clear that any access of personal information without a legitimate need will be flagged and dealt with can deter snooping.

Some of the breach discovery stems from forensic investigations of employees' devices after their departure from the company. While important, organizations should also focus on monitoring designed to capture (and prevent) data transfers or USB usage closer to real time to reduce the potential impact.

Miscellaneous Errors

Incidents in which unintentional actions directly compromised an attribute of a security asset. This does not include lost devices, which are grouped with theft.

At a glance

Top Industries
Healthcare, Public, Education, Professional Services (breaches only)
Frequency
2,478 incidents, 222 with confirmed data disclosure
Key Findings
Misdelivery of information in either electronic or paper format continues to be the primary form of error. Publishing and disposal errors also make a respectable showing.

Mistakes were made

Alexander Pope wrote that "To err is human, to forgive is divine," but he wrote it long before the advent of breach notification laws. You can rest assured that we all continue to be human, but we now have a much larger stage on which to showcase our folly.

It is important to make two distinct points with regard to error. Firstly, according to VERIS, error is only selected when that error itself is the proximate cause of the breach. One could persuasively argue that all breaches have an error somewhere in the chain of events, but if it did not directly lead to the breach, it is classified under some other pattern. Secondly, the results of this report are based largely on the data derived from contributing organizations, and those organizations do not remain consistent year after year. New ones join, some depart or take a temporary hiatus.

The majority of errors in our corpus come from the government organizations that contributed to the report, not because they are more prone to mistakes than the rest of us, but because they have more stringent reporting requirements than most other industries. This year, the data from those organizations was substantially smaller than in previous years. This may be due to a myriad of causes, but most of them have more to do with the samples we were provided with than any massive change in human behavior.

See, what had happened was....

Figure 46 confirms that error varieties this year fall mostly into the same camps they always do, misdelivery, publishing errors, disposal errors and misconfiguration. The most common form of misdelivery by far is mailing paper documents to an unintended recipient (sadly, we did not have one instance of a clay tablet or a papyrus scroll going astray).

Publication errors occur when information becomes available or viewable electronically to an unintended audience, e.g., the document you intended for your intranet page is open to the internet at large. Disposal error may be in third place with regard to Figure 46, but it is always the Blue Ribbon winner when it comes to jaw-dropping disbelief and downright comedy.

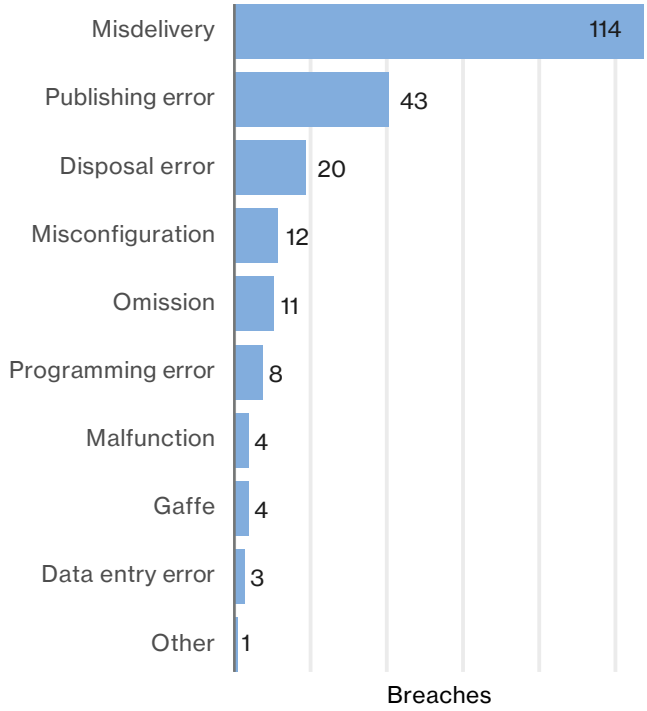


Figure 46: Top 10 threat action varieties within Miscellaneous Error breaches (n=212)

Our corpus is rife with such antics as selling filing cabinets that are full of medical records, and even organizations attempting to surreptitiously discard PII at a city dump while a reporter from a major newspaper looked on – unbeknownst to them. Perhaps we should create a Darwin Award for data disposal screw-ups?

Bringing up the rear is misconfiguration, similar to publishing error but different. A couple of examples are when your admin mistypes a firewall rule that allows certain private information to be viewable to everyone rather than a select audience as intended. Or an administrator turns on debug logging thus dumping sensitive information into clear-text files.

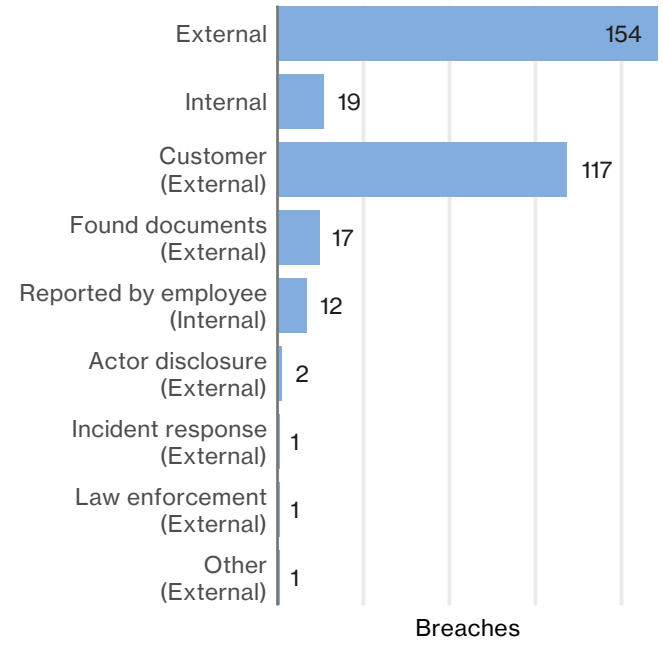


Figure 47: Breach discovery methods within Miscellaneous Errors (n=174)

Figure 47 shows it is usually the customer (76%) who lets you know you messed up. If they find their information on display on your website, or get someone else's medical records delivered to their house, they will typically give you a shout out to let you know about it.

Coming in at the number two spot "like a game show contestant with a parting gift" at 11% are documents found by external parties. These are notifications from people like the guy who received the filing cabinets from the auction site mentioned above. If we were to disclose all the various ways and means external parties find sensitive documents, the reader would lose faith in humanity, so we will draw a veil over this and move on.

To end on a positive note, in about 8% of cases the error was found by a conscientious and attentive employee who noticed something odd and reported it.

Areas of focus

There are no firewall rules for human inattentiveness, no alerting system for carelessness. But, there are a few basic policy and procedure-related steps to minimize human error.

Have a formal procedure for discarding ANYTHING that might have the slightest chance of containing sensitive information. This includes everything from desktops to wastepaper baskets. Then make sure that the policy is enforced and there are records kept to prove they were enforced.

Keep records of past mistakes and use them in security training. Leaving PII on a park bench could be just as damaging, and as costly, to your organization as spear phishing, so don't forget to cover the basics of handling, storage, delivery and disposal of anything that could be or has been an issue in the past.

Ensure there is a second reviewer who approves anything that is published or posted to company servers and web pages. Monitor webpages to catch publishing errors before an external party does.

Payment Card Skimmers

All incidents in which a skimming device was physically implanted (tampering) on an asset that reads magnetic stripe data from a payment card (e.g. ATMs, gas pumps, POS terminals, etc.).

At a glance

Top Industries
Retail, Finance
Frequency
118 total incidents, 89 with confirmed data disclosure
Key Findings
ATMs continue to account for the majority of incidents, however, the number of ATM attacks fell by 25%, while the number of gas pump terminal-related attacks more than tripled. Attackers are mostly from Eastern Europe and Cuba.

The song remains the same ... almost

Payment Card Skimmers continue to be a lucrative method of obtaining cash for criminals, and as we have pointed out before, those criminals clearly do not want to rock the boat by changing their methods. No doubt you, gentle reader, have seen the videos on YouTube in which an ATM skimmer is installed quicker than Superman can change clothes in a phone booth. The speed and ease with which these attacks are carried out, the potential for relatively high yield results, and the comparatively low chance of being caught all combine to make skimming a very popular threat action type in our dataset.

Generally speaking, the findings in this area do not change a great deal from year to year. However, this year we saw one particular shift from previous years that is worthy of remark. The number of incidents involving gas pump terminals increased over three-fold from last year, while at the same time, there was approximately a 25% decrease from last year in the number of incidents with ATMs as the affected asset. This may simply be a result of the number and type of cases our contributors provided us for this year, or it may be a developing trend, but either way we will keep a weather eye out to see if it continues.

Nobody's fault but thine

One of the basic human needs is the need to have someone to blame. Which brings us to the next question, who is responsible for these crimes? As we have stated in the past, due to the organizations who contribute the relevant data for this section, it is almost entirely US-centric from a victim standpoint. However, from a perpetrator point of view it can be laid squarely at the door of organized crime. As in previous reports, Eastern Europe continues to loom large when it comes to payment card skimming, with 60% of attacks attributed to actors from Romania when the criminal's origin could be definitively determined. Cuba is making an appearance this year, with approximately 16% of skimming cases. Naturally, the heads of these criminal groups aren't canoeing over here and installing them themselves, they have local helpers that do the physical labor.

Chip and pin – the shot heard across the living room

Back in 2015, we included a brief section in anticipation of the adoption of EMV (Chip and Pin) that was mandated for the US by October of that year. So, now that we are two years further along we thought it only fair to look back at how the technology may have changed things with regard to skimming. At the time, we reminded readers that they should "curb their enthusiasm" as the primary change taking place (at first anyway) was simply a shift in liability. Namely, whomever had the lesser technology in place at the time of a breach, be it merchants who had yet to upgrade terminals or banks that failed to issue shiny new EMV cards would bear the blame. So, having said all that, the jury is still out. It is not often, (well, ok, almost never) that one sees an ATM that is EMV-ready, while there are substantially more reports of Bigfoot sightings than there are gas pumps with a chip reader[26]. So, given their relative scarcity, it is not likely that Chip and Pin technology has to any great degree changed our findings within this pattern. However, chip readers are "slowly" becoming more prevalent and it will be interesting to see how the tactics used by criminals change when that happens. According to creditcards.com[27], as of late 2016 approximately 25% of US ATMs are chip-ready. However, it is important to remember that these ATMs are primarily those owned by the very large consumer banks that see a great deal of traffic. The relatively high cost of installation on the one hand, and the financial liability for non-compliance on the other, may combine to make lower-traffic convenience store ATMs a thing of the past.

Your time is gonna come

External parties continue to account for almost all breach discovery. It is noteworthy that discovery by law enforcement has increased from last year and has almost caught up with fraud detection via Common Point of Purchase (CPP) algorithms. Figure 48 indicates that internal discovery is lagging behind. Hope and optimism allows us to speculate that when discovered by internal mechanisms the situation is handled in such a way that it does not end up in our corpus. However, with small gas stations we also must be realists – the attendant is more concerned with selling lotto tickets and tree-shaped air fresheners and can't be expected to be everywhere at once.

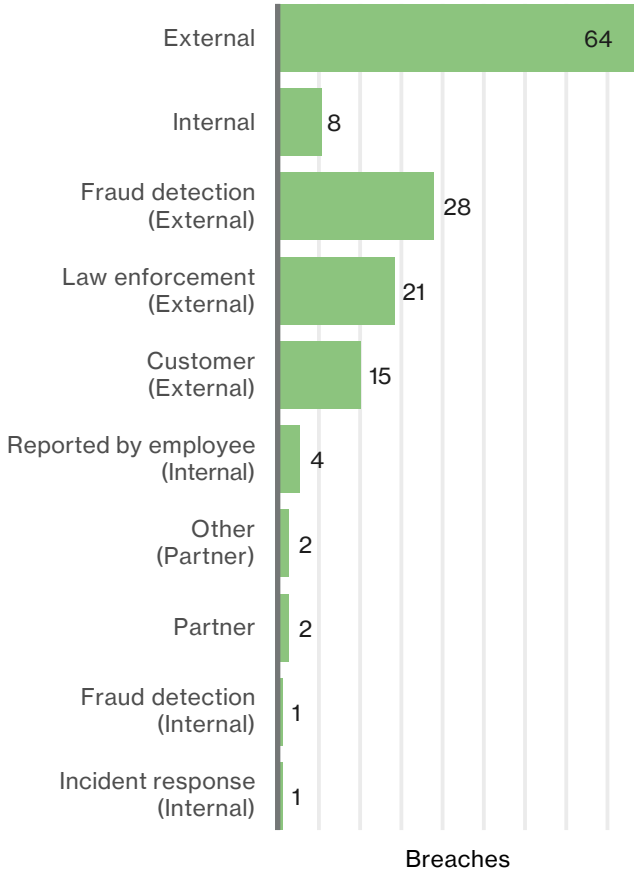


Figure 48: Discovery methods for Payment Card Skimmer breaches (n=74)

Areas of focus

Monitor your outdoor terminals via video surveillance and make a point to review the tapes periodically. This may enable you to learn of tampering sooner and thereby reduce the impact. Check the machinery as part of routine closing or opening procedure. Include a visual inspection of all terminals as part of your schedule and train your employees to know what to look for.

Use tamper-evident controls when possible. For example, place tamper resistant tape over the doors of the gas pump terminals and check physically each day to see if the tape has been disturbed. Also check the inside of the terminal for evidence of foreign objects.

[26] In fairness, ATMs and gas terminals have yet to reach their liability shift deadline. https://usa.visa.com/visa-everywhere/security/emv-at-the-pump.html

[27] www.creditcards.com/credit-card-news/atm-change-accept-emv-chip-1273.php

Point of Sale Intrusions

Remote attacks against the environments where card-present retail transactions are conducted. POS terminals and POS controllers are the targeted assets. Physical tampering of PIN entry device (PED) pads or swapping out devices is covered in the Payment Card Skimmers section.

At a glance

Top Industries
Accommodation and Food services, Retail
Frequency
212 total incidents, 207 with confirmed data disclosure
Key Findings
Accommodation, specifically restaurants, was the most prevalent victim of POS Intrusions. Use of stolen credentials to access POS environments continues to rise and is almost double that of brute force for hacking actions. RAM scraping continues to be very pervasive, but keylogging/spyware malware increased substantially as part of multi-function malware targeting POS systems. Continuing the trend over the last several years, the sprees (single threat actor, many victims) represented in this data are a byproduct of successful attacks against POS vendors and cannot be attributed to automated attacks targeting poorly configured, internet-facing POS devices.

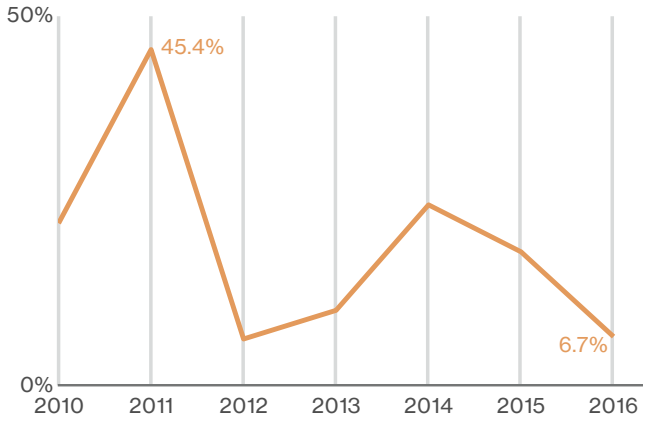
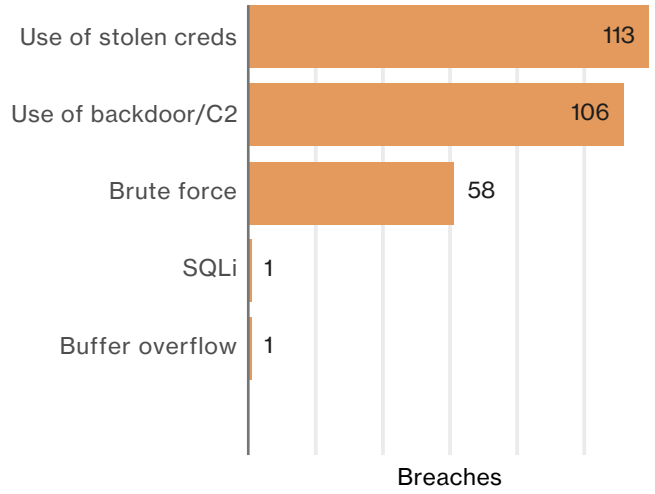


Figure 49: Point of Sale Intrusions pattern as a percentage of all breaches over time

The point we are trying to get across

POS breaches – primarily opportunistic and external-actor-driven – represented a little over 10% of all breaches this year. As you can see in Figure 49 POS breaches have declined over the years.

Back in our 2011 report, our findings were dominated by scalable, automated attacks targeting internet-visible POS servers with default credentials. We saw this method of compromise over and over again in primarily small organizations. Fast forward to the 2014 report where 2013 was referred to as the “year of the retailer breach”, not because of how many organizations fell victim, but the fact that POS intrusions were affecting big retailers with significant impacts. The good news is that this pattern has (for this year at least) gone back to being primarily a small business problem.



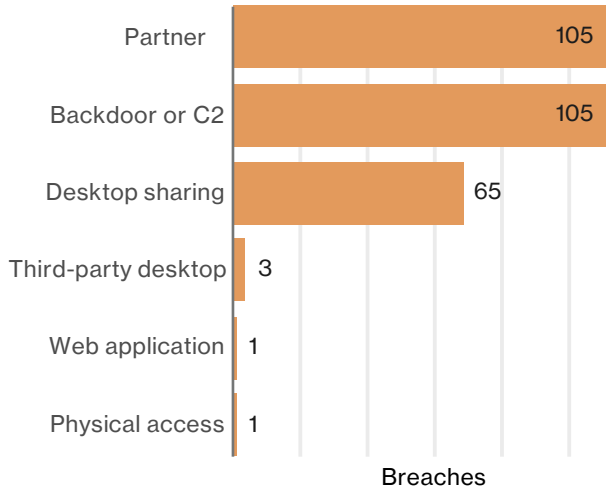


Figure 50: Hacking varieties (n=175) and vectors (n=176) within Point of Sale Intrusions

Figure 50 focuses on some specifics around POS hacking. Almost 65% of breaches involved the use of stolen credentials as the hacking variety, while a little over a third employed brute force to compromise POS systems. Following the same trend as last year, 95% of breaches featuring the use of stolen credentials leveraged vendor remote access to hack into their customer's POS environments.

Malware almost always scraped data from running memory (95%), while a little over half of POS breaches featured keyloggers. This is a significant increase from last year. We'd like to caveat this by saying this finding came from a spree that featured POS malware with both RAM scraping and keylogging functionalities. We expect POS malware families to continue to perform multiple jobs, including communications to C2 infrastructure along with the capture and exporting of data.

Finally, let's move onto discovery. Figure 51 shows that most breaches were discovered via fraud detection – a 25% increase on last year. While law enforcement dropped to nine times less and customers fell to six times less when comparing years. Regardless of which external discovery method is present, the means in which that external party made the discovery is almost always related to the post-compromise fraud or in the case of law enforcement, additional victims are notified after one victim is identified via CPP or customer notification.

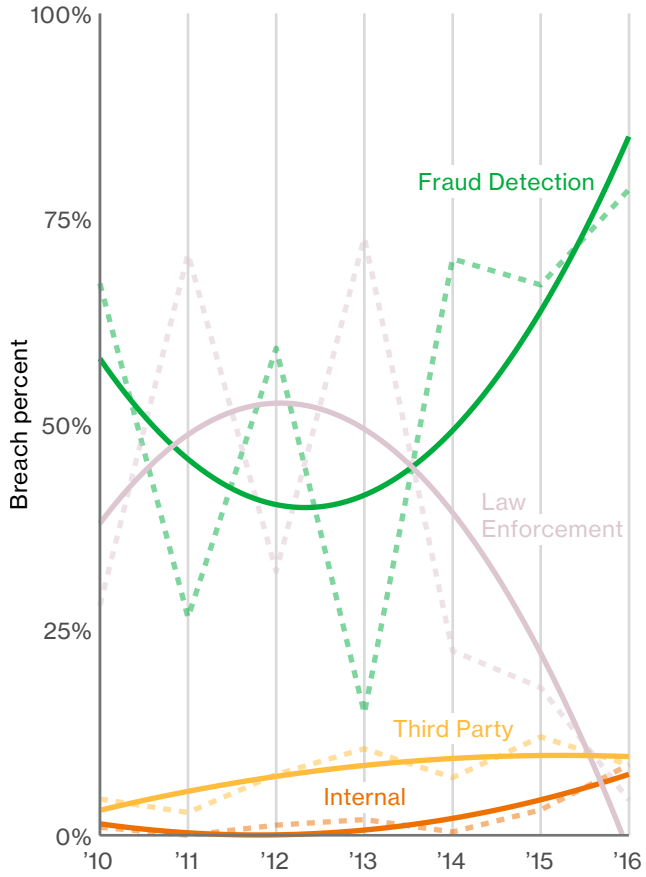


Figure 51: Select discovery methods within Point of Sale Intrusion breaches over time

Areas of focus

We continue to hope that POS vendors apply more efforts in securing their remote access mechanisms to their customers. We recommend all businesses, small and large, ask the right questions to any third-party management vendors about their security practices, specifically about use of two-factor authentication.

Strengthening authentication and limiting remote access into the POS environments is essential. For a small mom-and-pop operation it may be merely ensuring that the systems are not internet-visible. For larger targets, it will be a more arduous task, but as our data shows this year, it is not an impossible one.

Physical Theft and Loss

Any incident where an information asset went missing, whether through misplacement or malice.

At a glance

Top Industries
Public, Healthcare
Frequency
5,698 Incidents, 74 with confirmed data disclosure
Key Findings
Consistent with prior reports, misplacement is more common than theft. Top industries are influenced by our data contributors and regulatory requirements rather than a higher likelihood of loss.

Hasta la vista, assets

This pattern is the yin to the Cyber-Espionage yang. Big in terms of number of incidents – but not a heck of a lot to talk about. We can rehash recommendations around security-awareness training to educate your user base to not leave laptops in cars, or being more careful to not leave their tablets on a subway. But the best take-away from this section is to understand that people will inevitably lose things. Oscar Wilde once quipped "To lose one parent may be regarded as a misfortune; to lose both looks like carelessness." His witticism does, in a circuitous manner, apply to theft and loss: people are often careless. We can, however, take appropriate measures to significantly reduce the impact of the physical loss of assets.

It starts with encryption. Full disk encryption is available natively on both Windows (BitLocker) and Mac (FileVault). Implementation is simple, and is either a three or four-step process respectively for an individual device[28]. For a community of mobile devices, these technologies can be part of the standard build, and implemented and validated via centralized management.

Not all assets can be encrypted – paper documentation in particular. The majority of confirmed breaches involve lost documents (several with record-loss totals in the thousands). We don't assume a confidentiality loss for every lost device, but we can be more liberal in inferring disclosure when the data is literally printed in black and white. This requires adjusting corporate culture to not print out sensitive data if not necessary for business operations, or tokenizing data when printing is required. This will also help with disposal errors covered in another pattern.

We do have instances where the misuse action category is present, such as cases where a user either prints or downloads sensitive data to an external drive, which is then subsequently lost or stolen. Hammer home data-handling policies and monitor for inappropriate data transfers.

Areas of focus

We can't eliminate losing assets, but we can do a better job of putting ourselves in a defensible position to avoid the unpleasant experience of breach notifications.

[28] https://support.apple.com/en-us/HT204837

Web Application Attacks

Any incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms.

At a glance

Top Industries
Finance, Public, Information
Frequency
6,502 total incidents (3,583 additional with secondary motivation) 571 with confirmed data disclosure
Key Findings
The breaches within this pattern are heavily influenced by information gathered by contributors involved in the Dridex botnet takedown. Hundreds of breaches involving social attacks on customers, followed by the Dridex malware and subsequent use of credentials captured by keyloggers dominate the actions.

Compared to last year, we saw a higher number of web application incidents, yet a lower number of breaches. Specifically, a majority of the incidents in this pattern involved website defacements reported by several CERTs, where data disclosure was not confirmed. Honing in on the incidents that were not defacement or repurposing (see secondary motives call-out below), the data reflects that, once again, use of stolen credentials, phishing and C2/backdoors were the lead action varieties this year – present in over 60% of the remaining incidents.

Battling the bots

Moving on to breaches, 77% were the targets of botnet activity, which has been a prominent and repeating trend in this pattern (Hello, Dridex my old friend). So we decided to examine web application breaches with and without the botnet subset to get the full picture and accommodate for bias. With botnets included, 93% of breaches were associated with organized crime. The actions taken tell the same story as last year; hundreds of breaches involving social attacks on customers via email attachments, followed by banking Trojans, and the subsequent use of stolen credentials captured by keyloggers or form grabbers.

Removing the bot bias

When we analyzed the data with the botnet breaches excluded to uncover any hidden treasures, we found that many things had shifted for the remaining 131 breaches compared to what we mentioned above. The top external actor became unaffiliated persons (42%), which bumped organized crime down to second place (32%). The use of stolen credentials still leads the way from a hacking variety standpoint, but our old friend SQL injection (SQLi) makes a solid showing as well in Figure 52.

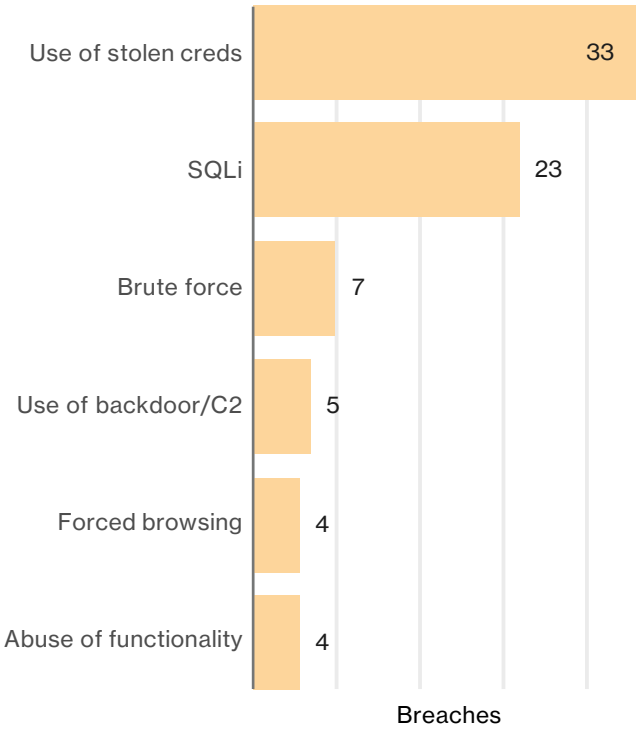


Figure 52: Top hacking varieties within Web Application Attack breaches – botnet activity excluded (n=72)

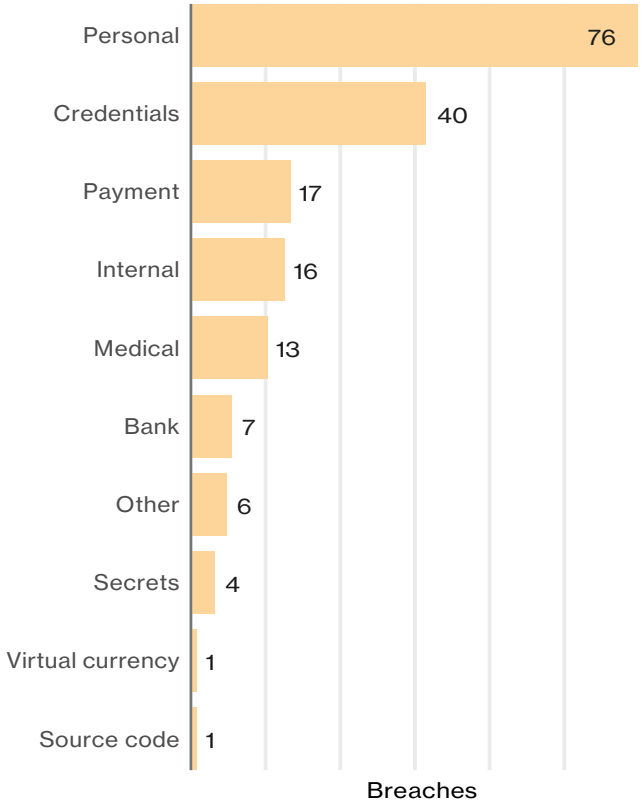


Figure 53: Varieties of compromised data within Web Application Attack breaches – botnet activity excluded (n=161)

Figure 53 clues us into the types of data targeted and captured via web applications. Personal data takes the place of credentials as the most frequently compromised type of data, found in more than half of breaches.

A means to an end

Let's not disregard the secondary characters in our story, they too have a purpose. As we mentioned in the 2015 DBIR, we noticed utilitarianism in the works; there were high-profile instances of hackers targeting web servers as a means to set up an attack on a different target, a tactic known as a Strategic Web Compromise. When modeling the incident from the standpoint of the site affected, the motive is secondary. The primary motive of espionage was applied to the visitors to the website. An even more common occurrence is opportunistic compromises of websites to build an attacker's infrastructure (e.g., C2 server, serve up malware, turn into a phishing site). We now have over 34,000 total incidents in our corpus that had a secondary motive, almost all of which are associated with organized criminal groups. As in previous years, we are limited in the details of these attacks, which is the primary reason we again culled them from our main analysis. It is good to have situational awareness of the adversary infrastructure, but the usefulness of these incidents in this study ends there.

Areas of focus

As websites are becoming more interactive and versatile – and thus complex – to provide a solid user experience, we should focus more on the underlying infrastructure, logic, and functionality of these assets and the data that they store.

- Limit the amount of personal information or site credentials stored on a web application or backend databases to the minimum needed to run your operation, and protect the rest via encryption.
- Use a second factor of authentication into a web application that would require a completely different attack pattern to compromise than the initial password.
- Patch CMS and plug-ins consistently and ensure you are notified when out-of-cycle patches are made available.
- Yes, SQLi is still around; perform web application scanning and testing to find potential SQLi and other input validation weaknesses.

Everything Else

Any incident that did not classify as one of the nine patterns.

At a glance

Top Industries
Manufacturing, Education, Public (incidents)
Frequency
870 total incidents, 184 with confirmed data disclosure
Key Findings
Participants in DoS bots, social engineering and information gathering via network footprinting comprise the majority of incidents in this pattern.

Details, details...

Everything else is the catch-all pattern; particularly for incidents and breaches that have some information, but are lacking enough information to help classify them better. We can wish all we want for those details to fall out of the sky, but a better activity is to utilize what we do have. When we do, we can uncover some useful findings. The first three bars in Figure 54 represent distinct attack narratives.

The first bar represents low-fidelity phishing breaches where we know phishing was involved and the bait was taken, but not much else. Since most phishing involves malware, we can infer that at least some of the phishing incidents went down that path.

The second bar represents footprinting incidents and these were mostly from the same data contributor. We just don't know what threat actions preceded or followed the network mapping. We know, the suspense is killing us too!

The third and most interesting bar represents business email compromises (BEC). These incidents involve communications, typically via email and from "THE CEO" ordering a wire transfer, and providing a scenario that is believable and requires quick attention.

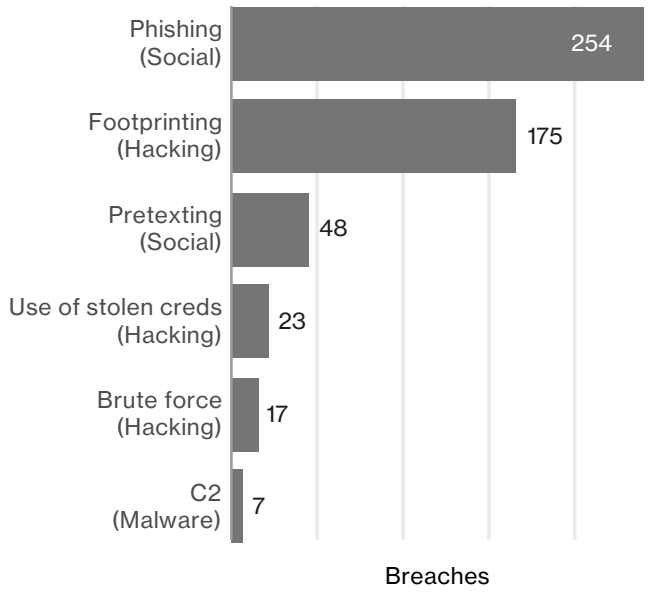


Figure 54: Top threat action varieties within Everything Else (n=529)

Wrap Up

So, that wraps up our 10th installment of this report. Ten years is a long time. It took 10 years to build the Brooklyn Bridge, Michelangelo spent roughly 10 years working on the Sistine chapel, and 10 years is the average length of time required to play a standard game of Monopoly. No, not really, but it sometimes feels like it. A lot can happen in a decade. In that time, the DBIR went from a brief report totally comprised of breaches investigated by one entity (Verizon), which were primarily focused on Financial and Retail verticals, to a collaborative effort with as many as 70 organizations spanning the globe. Over the last decade our scope has broadened to encompass a bit of almost everything cyber-related that is occurring in enterprises around the world.

Many new threats have emerged or evolved in that time span: hacktivism moving from availability attacks to full-blown data breaches, the prevalence of nation-state and state-affiliated espionage, the rise and dominance of phishing, DDoS attacks, more sophisticated and polymorphic malwar – the list goes on.

Likewise, the DBIR has evolved and matured along with the industry and the threats that it must combat. From its more humble and simplistic beginnings the DBIR has become more robust and expansive over the years. The addition of the United States Secret Service as a contributor in the 2010 report helped to open the floodgates for other organizations to feel comfortable sharing breach-related data – something that was more or less unheard of prior to that event. The addition and refinement of the VERIS framework, the inclusion of non-incident data to enrich our view of data breaches, the introduction of the nine patterns in 2014, and the creation of specific industry vertical sections have combined to help organizations prepare to meet the challenges that each new year brings.

From the beginning our primary goal was, and still remains, to help organizations understand the threats they are facing, and enable them to make sound evidence-based risk management decisions. Again, we thank you, our readers, and our contributors for helping to make this report a success, and we hope that it continues to provide you with insight and helpful, actionable data.

> **We are stronger together.**

At the end of the day, we are stronger together than any one of us is alone, so we encourage you to continue to share your data, your ideas and your feedback. Due in large part to your support, we have enjoyed 10 years of publishing in-depth analysis and sharing. Here is hoping for number 11, because as the great sage Nigel Tufnel once so eloquently stated, 11 “is one louder” than 10.

Appendices

Appendix A:

Countering an Evolving Transnational Cybercrime Threat

Robert Novy
Deputy Assistant Director
United States Secret Service

Transnational cybercrime has steadily evolved over the past 20 years, requiring continued adaptation to strategically counter this threat. In the late 1990s and early 2000s, websites like Boa Factory, Carder Planet and ShadowCrew were established to coordinate this transnational cybercrime activity. However, these websites were just the visible manifestations of a complex network of cybercriminals, located primarily in Eastern Europe, that were being formed to exploit cyberspace for their illicit financial gain. US financial and payment systems were, and remain, the natural target for much of this criminal activity – for the simple reason, as the bank robber Willie Sutton was once reported to have quipped, "That's where the money is at."

> **That's where the money's at.**

The Secret Service has a long history of safeguarding financial and payment systems from criminal exploitation. In 1865, the threat we were founded to address was that of counterfeit currency. As our financial payment systems have evolved, from paper to plastic to, now, digital information, so too has our investigative mission. Today, our modern financial system depends heavily on information technology for convenience and efficiency. Accordingly, criminals have adapted their methods and are increasingly using cyberspace to exploit our nation's financial payment system by engaging in fraud and other illegal activities.

Secret Service cybercrime investigations have resulted in the arrest and successful prosecution of numerous cybercriminals that have been involved in some of the largest known data breaches, including many of the leaders of these early transnational cybercriminal groups.

Despite this, some of the participants in those early days of cybercrime have engaged in multi-year campaigns totaling hundreds of millions (if not billions) in financial fraud losses, in addition to other costs to victim businesses and their customers. These criminals have reinvested their proceeds to develop formidable criminal enterprises, and facilitated the development of a robust underground for a wide range of cybercrime services, which enable a wide range of illicit cyber activity.

However, some of the most significant cyber threat actors generally do not participate in these criminal marketplaces. Instead, they have developed organizations that have cartel-like qualities and coordinate their criminal activity through a closely trusted collective. These criminal organizations are rapidly growing in both technical and financial sophistication – as they find new ways to gain unauthorized access to networks and new ways to profit from that access.

Countering transnational criminal organizations like these has become a critical priority of the Secret Service as we work to safeguard the integrity of US financial and payment systems. The sophistication, capabilities, and financial incentives for these cyber criminal enterprises largely render network defenses and traditional efforts at deterrence insufficient. Instead, what is required is a proactive campaign for countering, degrading and containing their unlawful activities.

We believe such a campaign presents our best opportunity to reduce the substantial homeland security risks posed by these organizations, and to degrade the malicious cyber capabilities of a broad range of cyber threats – from nation-state organizations to less sophisticated criminals.

Such a campaign to counter transnational cybercrime involves numerous activities and objectives, most of which the Secret Service cannot accomplish in isolation. As a first step, we need to shift some of the current focus on preventing unauthorized access or damage to our computer networks, to preventing and minimizing the ability of criminals to profit from their malicious cyber activities. The Secret Service does this through a variety of means, from targeting the money laundering and digital currencies they use, like we did in our cases that shutdown Liberty Reserve and eGold, to notifying victims of ongoing network intrusions. Certainly one purpose of our victim notifications is to enable them to restore the security of their networks, but more importantly it is to minimize the cybercriminal's opportunity to profit from their activities and inflict financial harms on victim organizations.

Sadly, some companies continue to react to notifications of a cybersecurity incident with denial and are far too slow to take action to protect themselves, their customers, partners and other businesses from financial losses from the malicious cyber activity. To help prepare companies and their security, legal and IT departments to respond swiftly and responsibly to cybersecurity incidents, the Secret Service encourages organizations to develop and exercise a cybersecurity incident response plan that involves specialized expert legal counsel, outside cyber incident response and forensics organizations, and law enforcement.

Second, as a community we need to get better at sharing information on threats and incidents. This includes sharing not just the indicators of compromise (malware hashes, YARA rules and such), but also working with law enforcement to investigate and bring the perpetrators to justice. It also requires sharing the more general context of cybersecurity incidents to inform prioritization of cybersecurity actions and law enforcement efforts to counter particularly damaging threats.

The purpose of information sharing should not be narrowly considered in the context of cybersecurity – but rather, we need to broadly consider how to minimize the illicit gains for the perpetrator and financial harm to victims.

Through our network of Electronic Crimes Task Forces and trusted partnerships with private sector and other law enforcement agencies, the Secret Service has been able to effectively share critical information on cybercrime, while protecting privacy interests and our investigative sources and methods – including highly sensitive undercover operations and confidential informants that have penetrated some of the most sophisticated transnational cybercriminal organizations.

It is for this information sharing purpose that the Secret Service first partnered with Verizon for the Data Breach Investigations Report. We are proud to see so many organizations have also come to contribute data to this report, and we encourage more to do so. No organization can singlehandedly develop an understanding of the full range of cybersecurity threats, much less be effective at countering these threats.

> **"The DBIR has developed into a critical resource..."**

The DBIR has developed into a critical resource for assessing the nature of cybersecurity threats and drives our ability, collectively, to identify opportunities to effectively counter these threats. The Secret Service remains committed to working with all potential partners for the purpose of preventing, detecting and investigating cybercrimes.

Appendix B:

The Patch Process Leftovers

Only a single-digit percentage of breaches in this DBIR involved exploiting a vulnerability. That is comforting, but it doesn't mean we are condoning a moratorium on vulnerability scanning or patching vulnerabilities. Having a good patch process is a fundamental security practice. But how do you define what "good" is for you and how can you measure against it?

Figure 55 gives us a way to look at patching progress. It shows how, over time, the vulnerability scan findings[29] of an organization are fixed. The green line roughly represents a normal organization[30] while the orange line represents, (all other things being equal) an organization better than almost three-quarters of their peers. These examples demonstrate patching happens multiple times.

The top line patches some findings immediately and then again before the one-month scan. The bottom line patches before the one-week and one-month scans, after which they have patched everything they'll be patching. In reality, organizations have vastly different curves. Some patch a majority of what they plan to patch immediately. Others patch slowly over time.

Each organization's patching can be represented by two numbers: The area under the curve (AUC) and the percentage completed on time (COT). AUC is a representation of how protected you are while you are actively patching, knocking a majority of the findings out quickly will result in a higher AUC. COT is the amount of vulnerabilities patched at cut-off time (12 weeks in Figure 57). As we demonstrated in last year's DBIR[31], findings that aren't patched quickly tend to go unpatched for a long period of time. We call these the leftovers.

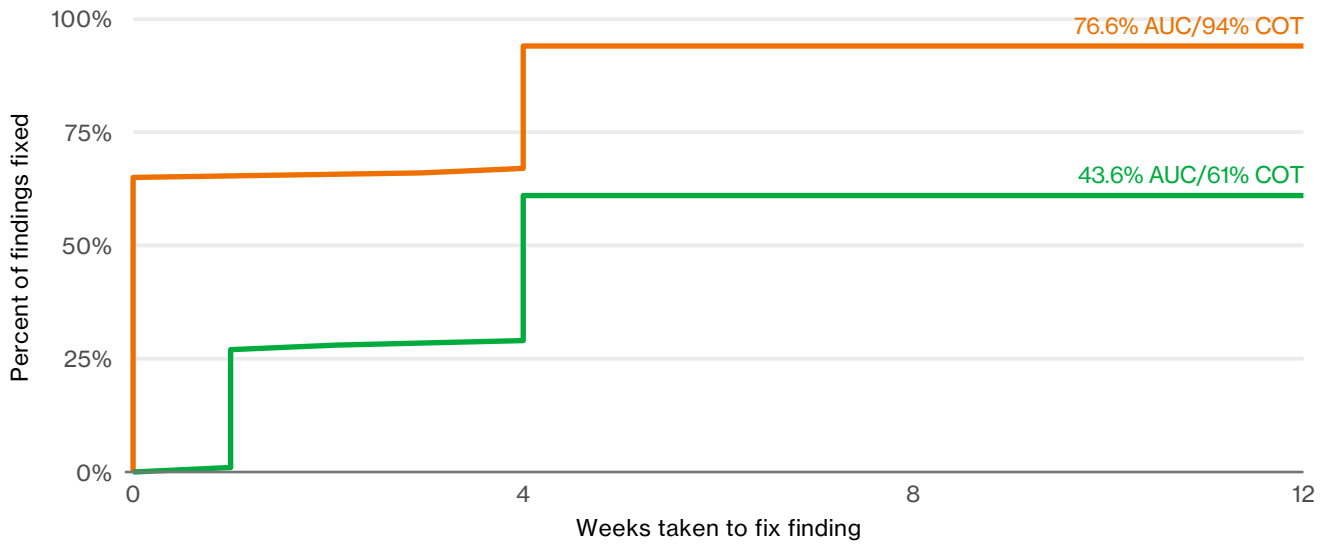


Figure 55: Comparison of organization area under the curve (AUC) percentage

[29] While all analysis in this section has informational findings removed, you need to consider findings in the context of your organization. "Telnet enabled" is informational until you find default creds on webcams.

[30] Technically it's the 55th percentile, not the 50th like the median would be, but you get the idea.

[31] 2016 Data Breach Investigations Report, Page 16, Paragraph 1 and Figure 13

Completed on what time?

We just mentioned completed on time, but what "time" is that? It's the cut-off time before which findings are actively worked. Your organizations patch cycle, if you will. We found 12 weeks was where most organizations had completed their patch process through analysis of roughly 116,000 vulnerabilities within organizations. This also aligns with a quarterly patch process. We used the phrase earlier "All things being equal" and we know they aren't. You should ground your process around the exploitability of the findings you are addressing.

Not all vulnerabilities get to experience the joy of exploitation in the wild so a universal patch cycle or "on-time metric" for all the findings is infeasible and inefficient. Ultimately you want to fix findings before the actors start exploiting. Findings that have real-world exploitation will have an escalated patch cycle, as well as vulnerabilities on identified critical assets. So "on time" may be seven days for those findings, where a quarterly patch cycle may be the "norm" for the rest. In other words, AUC and COT can be calculated for any subset of the findings.

Each subset can be prioritized by the exploitability of the finding, the business criticality of the asset, and/or its threat actor exposure. And just like the fourth Friday in November, leftovers can be fine. It is however, important for organizations to know what these unpatched findings are and how they have addressed the risk or documented their acceptance of it. We will analyze the leftover findings in this year's combined vulnerability scan dataset later in the section.

Going back to the overall numbers, if you need a starting point, half of all companies have an AUC below 51% and COT of 76%. The top quarter of companies have an AUC of about 80% and COT nearing 100%. In Figure 55, the upper line has an AUC of 76.8%, meaning they are only potentially vulnerable – we can't account for false positives within this dataset – to roughly 23% of the findings over the course of 12 weeks. The bottom line has a much lower AUC of 43.6% meaning they are vulnerable to over half of the findings across the duration of the patch cycle. At the cut-off time of 12 weeks, the upper line has a COT of 94% meaning they've fixed 94% of their findings. On the other hand, with a COT of 61%, almost 40% of the lower line's findings are leftovers.

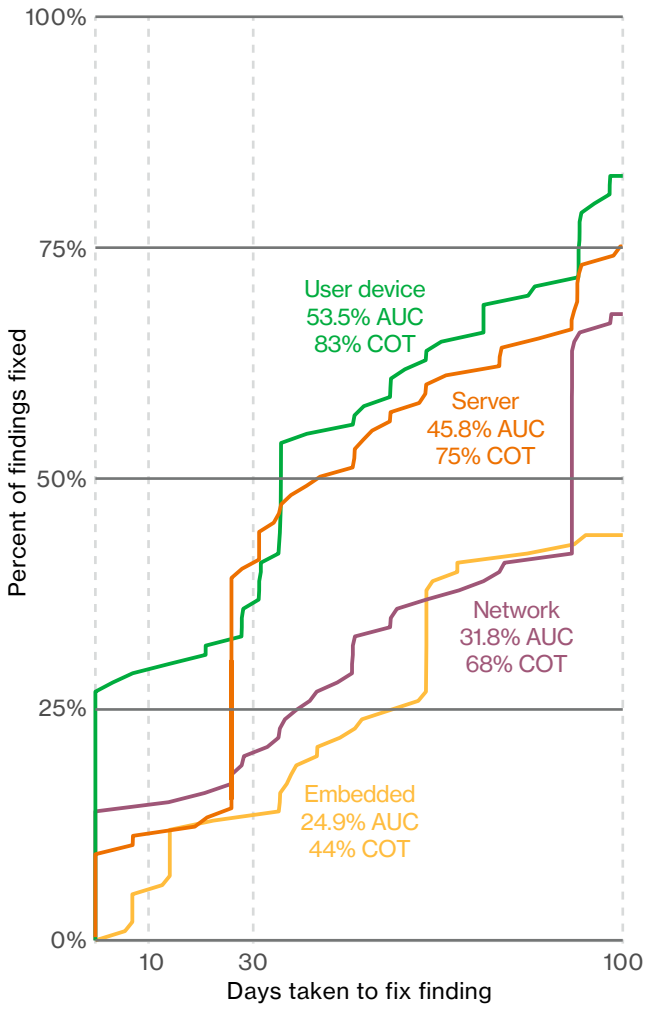


Figure 56: Comparison of patching per asset type

In Figure 56, we break the results out by asset type and use a cut-off time of 100 days. The graph illustrates user devices have a higher AUC and COT (53% and 83% respectively) vs. servers (46% AUC and 75% COT), network devices (32% AUC and 68% COT) and embedded devices[32] (25% AUC and 44% COT). User devices are patched quickly and then again after about a month, while servers receive their biggest jump closer to a month after discovery. Network devices aren't patched until the end of the quarter.

[32] These are mostly VOIP adapters and environmental monitors.

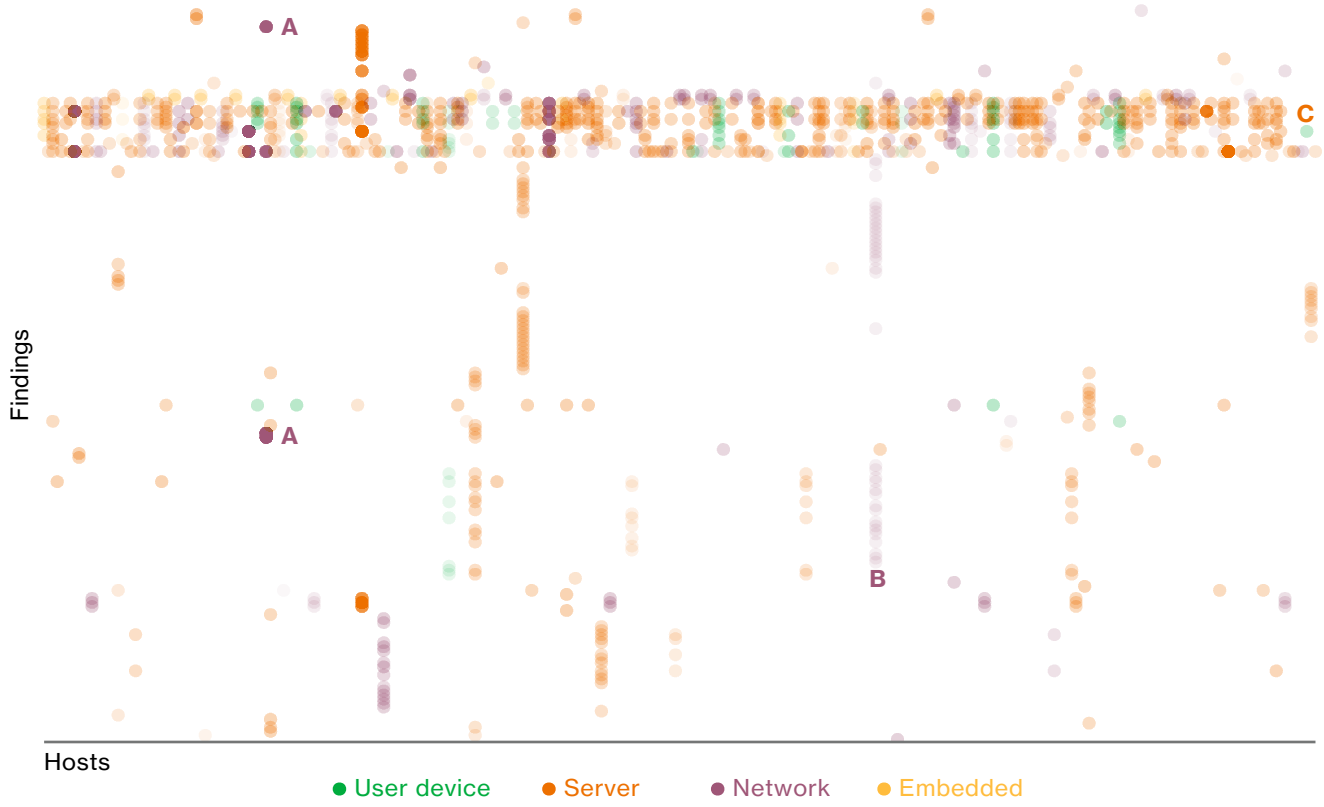


Figure 57: Analysis of leftover findings

Leftover analysis

So what exactly is up with the findings that are still hanging around? Figure 57 shows some patterns in the remaining or leftover findings. Each spot is a single finding on a single host. How dark a spot is indicates if the finding was found repeatedly.

- The **berry colored** dots **A** are an indication that a few network devices have repeat findings that are simply not being patched.
- On the other hand, the **B** column indicates a single device that has many vulnerabilities that appeared one or a few times. This is an opportunity to investigate why it was found vulnerable when other assets were not.
- Finally, **C** represents a suite of similar vulnerabilities – in this case SSL vulnerabilities – that are repeatedly found on multiple servers. Those findings could be false positives, or be determined to be low-risk by the organization and thus that scary orange bar could be a non-issue.

What is important is to understand what pockets of vulnerabilities are lingering in your environment and not be surprised by their existence.

In the end, this section provides some bars you can measure yourself by, but what's more important is understanding your AUC and COT and the leftover findings in the context of your organization. Measure the threat and impact to your organization to turn findings into risks. And, ultimately, put your risks in context with each other to understand your organization's full attack surface[33].

[33] For more information about attack surfaces, see the 2016 Verizon Data Breach Investigations Report, Appendix D.

Appendix C:

Year in Review

January

The Verizon Threat Research Advisory Center looks back on 2016 as being a year stacked with monumental events impacting information security risk. 2016 stands out in this respect more so than any other year since we launched the DBIR. The electricity blackout that struck Ukraine on December 23, 2015 became the first of these events as developing related intelligence became a priority tasking in January and through the first quarter. To be sure, as we experienced in past years, other trends developed as well. Austria-based aerospace manufacturer FACC AG was the victim of a €50 million business email compromise (BEC) attack. Over the next several days after the company announced the attack, it lost almost €45 million in market capitalization. Almost simultaneously, Belgian bank Crelan announced they were the victim of a €78 million BEC fraud.

February

Four milestones emerged in February: A collaborative effort by more than a dozen security companies and response teams produced the Operation Blockbuster report detailing the November 2014 cyberattack on Sony Pictures Entertainment (SPE). We began collecting the emerging reports of a US$80 million compromise of the central bank in Bangladesh. Attackers used social engineering and malware to abuse the SWIFT system. We would later learn the same threat actor was probably responsible for both SPE and Bangladesh Bank. Kaspersky led reporting on the Equation Group, a cyber-espionage threat actor most analysts link to the USA's National Security Agency. Ransomware attacks on healthcare organizations were the next milestone and trend. Ransomware caused Hollywood Presbyterian Medical Center to declare an internal emergency. They were successful in negotiating the ransom down from US$3.5 million to US$17K.

March

Ransomware in healthcare organizations continued in March, striking 10 hospitals and 250 outpatient centers in the MedStar network in the Washington DC area. Methodist Hospital in Henderson, KY was hit by Locky ransomware. Samsam ransomware struck two facilities in California, the Chino Valley Medical Center and Desert Valley Hospital in Victorville. 21st Century Oncology provides services across the US and reported a data breach that compromised 2.2 million patient records. As the US approached the deadline for income tax reporting, cybercriminals mounted a variation on BEC by targeting W-2 income statement forms. According to Cloudmark, 68 companies had W-2 phishing breaches in the first four months of the year. Top-tier websites including the New York Times, BBC, AOL and MSN exposed visitors to TeslaCrypt ransomware via malvertising with the Angler exploit kit.

April

Four major events set the tone for April beginning with revelations that over 11 million documents were stolen or leaked from the law firm Mossack Fonseca. The "Panama Papers" had a global impact on business and international relations similar to, but on a smaller scale than, Edward Snowden's leaks. The next event occurred when a GozNym malware campaign struck 22 US and Canadian banks to the tune of US$4 million. Every major website in the Netherlands suffered from a malvertising attack in April. About half the population of the Republic of the Philippines were victims of the data breach at the Commission on Elections.

May

The first major operation in 2016 by a cyber-espionage threat actor was May's milestone. The Turla group has been operating since 2008. In May, Switzerland's CERT reported a 20-month Turla operation targeting the Swiss defense company, RUAG. BAE Systems analyzed the malware used in the Bangladesh Bank fraud and linked it to the Lazarus threat actor. We learned The Tien Phong Joint Stock Bank in Vietnam and Banco del Austro in Ecuador had thwarted attempted SWIFT frauds similar to February's attack on Bangladesh Bank.

June

The good guys' greatest success of the year came in June when Russian law enforcement made 55 arrests of the Lurk group. Those arrests crippled the Angler and Nuclear exploit kits. A bank in Ukraine lost US$10 million to SWIFT fraud. On June 15, CrowdStrike published, "Bears in the Midst: Intrusion into the Democratic National Committee." In the US, for the remainder of 2016, information security and geopolitics became inseparable.

July

If only we could have known beforehand that July was the best month to schedule vacations. The customary Oracle and JavaScript critical patch update was the most significant security announcement. A new offering in the malware marketplace launched in the form of the Petya and Mischa ransomware-as-a-service. The attacks abusing the SWIFT network earlier in the year exemplified taking Sutton's law to an extreme. In July, a variation on that theme led the Union Bank of India to thwart an attack on a US dollar nostro account.

August

On August 1, the threat actor "Peace" listed 200 million Yahoo account logins on "The Real Deal" cybercrime marketplace. Miscreants stole almost 120,000 bitcoin, valued at that time at about $65 million from the bitcoin exchange Bitfinex. The "Shadow Brokers" began their campaign to peddle 250MB of files stolen or leaked from the NSA's Equation Group. The Anunak threat actor breached the customer support portal of Oracle's MICROS point-of-sale system. Leoni AG, the world's 4th largest manufacturer of wire and electrical cables lost €40 million in a BEC scam. Brisbane, Australia lost AUD $450,000 to a BEC attack.

September

In September, Yahoo announced a data breach from 2014 that compromised the accounts of 500 million. Three months later, it announced a different breach from 2013 had compromised one billion accounts. On September 20, the website of security journalist Brian Krebs suffered a 600+Gbps DDoS attack. Two days later, French hosting company OVH reported they had been the target of a 1Tb Gbps DDoS attack. We later learned both of these DDoS attacks were delivered using the Mirai worm that infected IoT devices.

October/November

Major events in autumn in the Northern Hemisphere included waves of "Internet of Things" DDoS malware attacks. Two with far-reaching impacts were DoS attacks on hosted DNS provider DYN on October 21 and on Deutsche Telekom on November 27. Palo Alto Networks released their "SilverTerrier" report and they characterized it as the next evolution in Nigerian cybercrime. Palo Alto analyzed 8,000+ malware samples to identify 500+ domains being abused by about 100 threat actors to launch 5,000-8,000 BEC and "419" fraud attacks per month.

December

Moscow-based security company Group-IB issued press releases claiming the "Cobalt" threat actor was infecting banks with ATM jackpotting malware. But we had no technical details on Cobalt ATM attacks until a December report from Positive Technologies. One of the worst cybercriminal groups, Anunak is almost certainly linked to the Cobalt gang's ATM jackpotting attacks. Trustwave reported Anunak, was targeting the hospitality sector. The Verizon Threat Research Advisory Center is still working to define the relationships between Anunak, Buhtrap and Cobalt. The best news of 2016 came in December with the takedown of the Avalanche cybercrime operation including five arrests and seizure of 39 infrastructure servers.

Appendix D:

Methodology

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

Our overall methodology 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 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 VERIS.

2. Direct recording by contributors using VERIS.

3. Converting contributor's existing schema into VERIS.

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

Incident eligibility

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

- The incident must have at least seven enumerations (e.g. threat actor variety, threat action category, variety of integrity loss and so on) across 34 fields OR be a DDoS attack. Exceptions are given to confirmed data breaches with less than seven enumerations.

- The incident must have at least one known VERIS threat action category (hacking, malware and so on).

In addition to having the level of details necessary to pass the quality filter, the incident must be within the time frame of analysis. The 2016 caseload is the primary analytical focus of the report, but the entire range of data is referenced throughout, notably in trending figures. 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 CryptoLocker it would not be included in this report.

Lastly, for something to be eligible for inclusion in the DBIR, we have to know about it, which brings us to sample bias.

Acknowledgement of sample bias

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 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. Unfortunately, we cannot measure exactly how much bias exists (i.e. in order to give a precise margin of error). We have no way of knowing what proportion of all data breaches are represented because we have no way of knowing the total number of data breaches across all organizations in 2016. Many breaches go unreported (though our sample does contain many of those). Many more are as yet unknown by the victim (and thereby unknown to us).

While we believe many of the findings presented in this report to be appropriate, generalization, bias and methodological flaws undoubtedly exist. However, with 65 contributing organizations this year, we're aggregating across the different collection methods, priorities and goals of contributors. We hope this aggregation will help minimize the influence of any individual shortcomings in each of the samples and the whole of this research will be greater than the sum of its parts.

Statistical analysis

We strive for statistical correctness in the DBIR. In this year's data sample, the confidence interval is at least +/- 1.4% for breaches and +/- 0.4% for incidents[34]. Subsets of the data (such as breaches within the Espionage pattern) will be even wider as the sample size is smaller. We have tried to treat every statement as a hypothesis (knowing they were made after seeing the data, which cannot be helped), and check that each statement is accurate at a given confidence level (normally 95%).

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

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

[34] Wilson method, 95% confidence level.

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, the only subset analyzed separately across the board consisted of web servers that were identified as secondary targets (such as taking over a website to spread malware).

Finally, we create some subsets to help further our analysis. This year we created a botnet subset that helps us analyze the impact of botnets on the data. As with last year, we left this subset in the data for the core analysis and removed it in some figures to allow the other results to present themselves. Anytime we did this it is noted in the figure header and/or supporting text.

Non-incident data

The 2016 DBIR includes sections that required the analysis of data 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 reporting on the median organization rather than the average of all data. We also attempt to combine multiple contributors with similar data to conduct the analysis wherever possible. Once analysis is complete, we try to discuss our findings with the relevant contributor(s) to validate it against their knowledge of the data.

Appendix E:

Contributing Organizations


INTERSET
The Science of Threat Detection


wombat
security technologies


CROWDSTRIKE


MWR
INFOSECURITY


WINSTON & STRAWN


RAPID7


LIFARS
your digital world, secured


Pavan Duggal Associates
Advocates

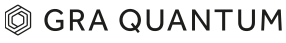

SOCIAL-ENGINEER


US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM


sparkcognition


JUNIPER
NETWORKS


DFDR
CONSULTING


GRA QUANTUM


panaseer


Skycure
Mobile Threat Defense


QUALYS


AsTech
SECURITY. GUAF


tripwire


DELL


CHUBB


GDT
GRUPO DE DELITOS TELEMÁTICOS


KRYPTOS LOGIC


CYLANCE


NetDiligence


LARES


KASPERSKY lab


JPCERT CC®


BeyondTrust
VISIBILITY. KNOWLEDGE. ACTION.


VESTIGE
Digital Investigations


V
C
D
B


mnemonic
- securing your business

Contributing Organizations

Akamai Technologies
Arbor Networks
AsTech Consulting
BeyondTrust
Center for Internet Security
CERT Insider Threat Center
Champlain College's Senator Patrick Leahy Center for Digital Investigation
Check Point Software Technologies LTD
Chubb
Cisco Security Services
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)
Cylance
Deloitte
DFDR Forensics
Digital Edge
DSS
EMC Critical Incident Response Center
Fortinet
GRA Quantum
Industrial Control Systems Cyber Emergency Response Team (ICS – CERT)
Interset
Irish Reporting and Information Security Services (IRISS – CERT)
ICSA Labs
JPCERT/CC
Juniper Networks
Kaspersky Lab
KnowBe4
Kryptos Logic
Lares Consulting
LIFARS
McAfee
Mishcon de Reya
mnemonic
MWR InfoSecurity
National Cybersecurity and Communications Integration Center (NCCIC)
NetDiligence
Palo Alto Networks
Panaseer
Pavan Duggal Associates
Pwnie Express
Qualys
Rapid7
S21sec
Skycure
Social-Engineer, Inc.
Spark Cognition
SwissCom
Tripwire
US Secret Service
US Computer Emergency Readiness Team (US – CERT)
Veracode
VERIS Community Database
Verizon Digital Media Services
Verizon DOS Defense
Verizon Fraud Team
Verizon Network Operations and Engineering
Verizon Enterprise Services
Verizon RISK Team
Vestige Ltd
WhiteHat Security
Winston & Stawn, LLP
Wombat Security Technologies

VerizonEnterprise.com