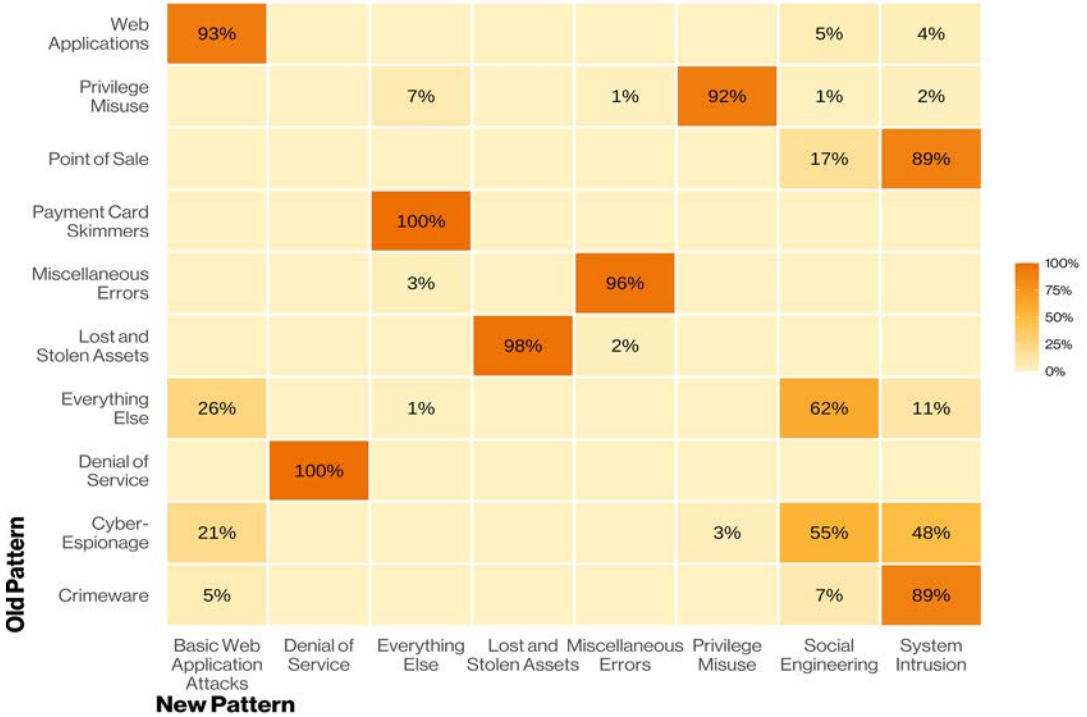

DBIR
2021 Data Breach Investigations Report
Suzanne Widup, DBIR Co-Author
verizon

2021 DBIR in a nutshell



Old Patterns Mapped to New Patterns in Incidents

14 years

88 countries

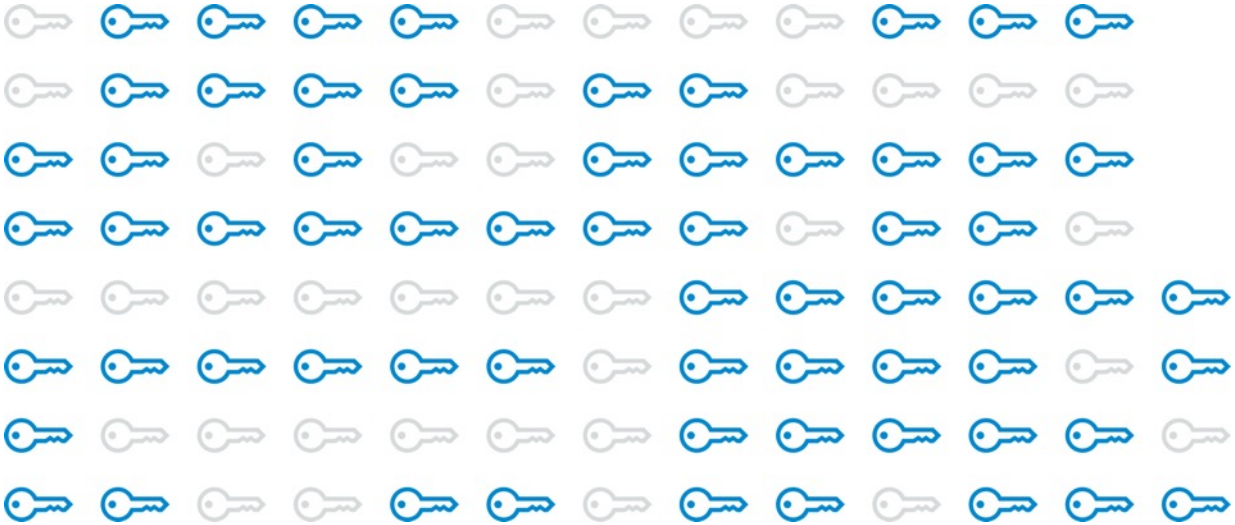
83 contributors

79,635 incidents

5,258 data breaches

61% of breaches involved credential data.

While missing credentials were ubiquitous, error-based breaches are more likely to leak personal data.



Each key represents 10 breaches.

Ransomware appears in 10% of breaches.

This increase is influenced by new tactics, where some ransomware now steals the data as it encrypts it.

Ransomware is now in third place among actions causing breaches.

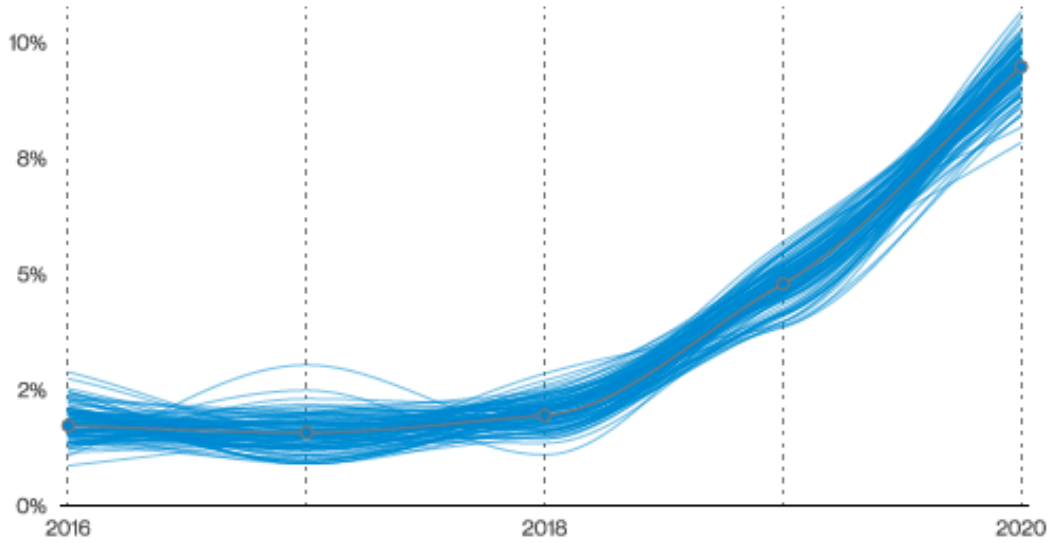
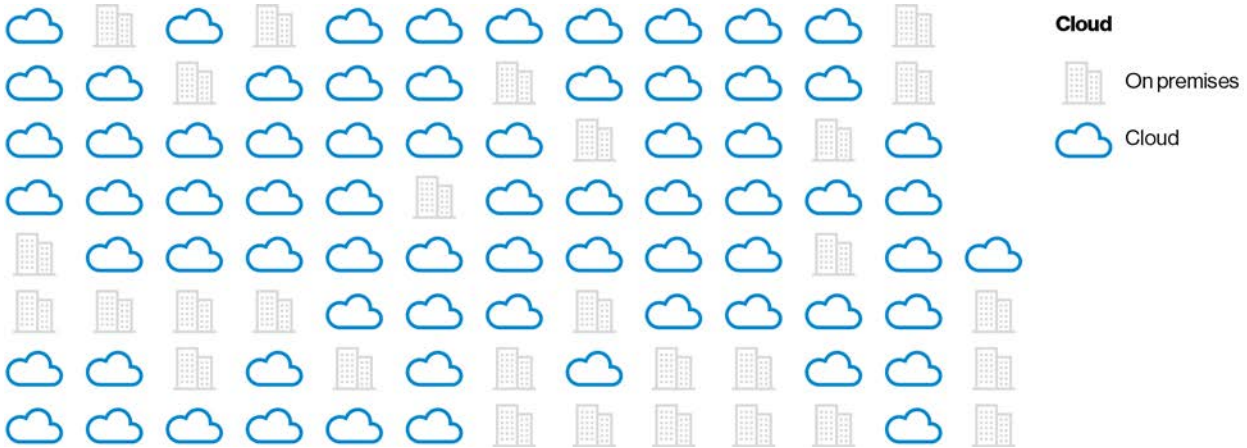


Figure 84. Ransomware in breaches over time

Cloud assets were more common than on-premises ones.

Conversely, there is a decline in user devices (desktops and laptops) being compromised.

This makes sense when we consider that breaches are moving towards Social and Web application vectors, and those are becoming more server-based, such as gathering credentials and using them against cloud-based email systems.



146 of 171 breaches were listed as cloud assets.
However, cloud status was unknown for an additional 4,684 breaches.

Breaches continue to be mostly due to external, financially motivated actors.

These findings were the norm, but there is a long tail of less prominent causes and types of attacks. We recommend that you build your security program around the norm, but be sure your team is properly trained to also respond to the exceptions.

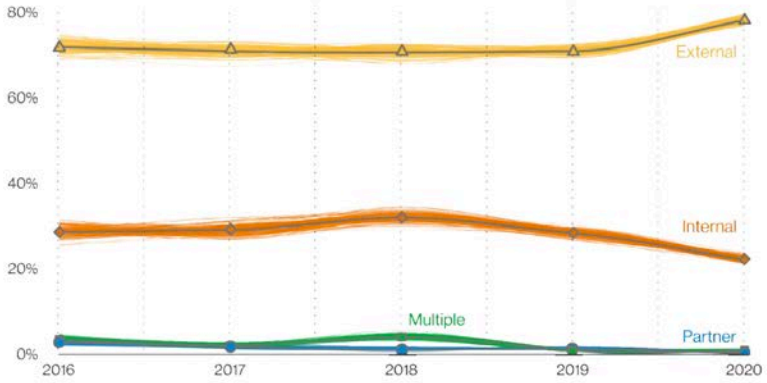


Figure 14. Threat actor over time in breaches

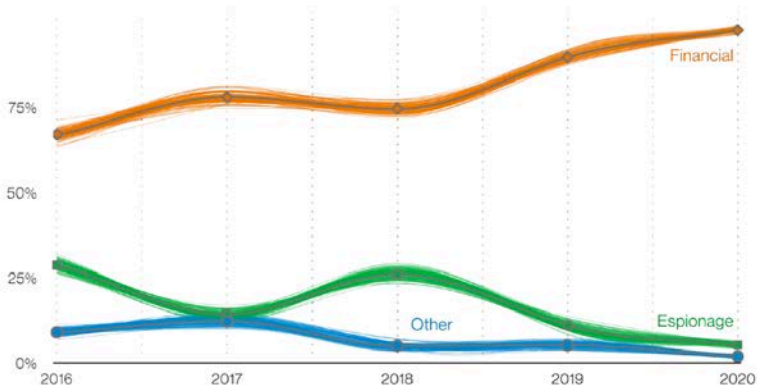
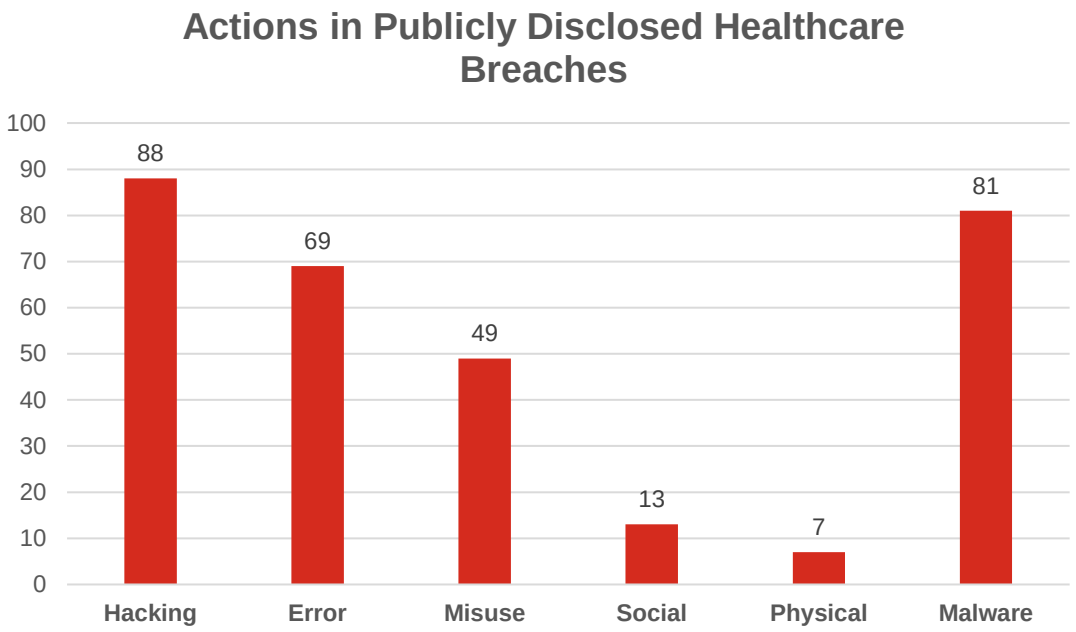


Figure 15. Top threat actor motive over time in breaches

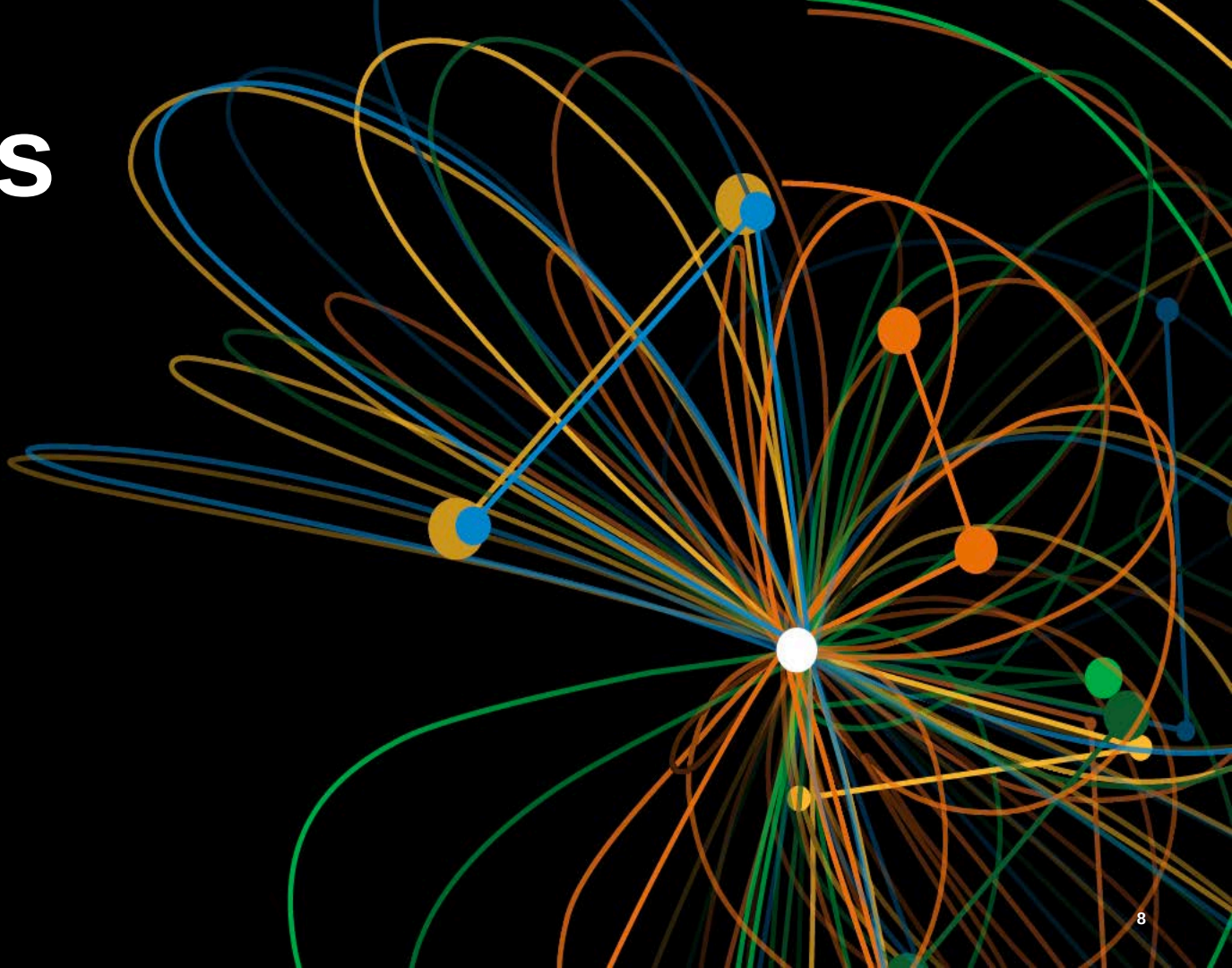
Data from Nov 2020 to present

The VERIS Community Database Project is where we track publicly disclosed data breach reports. This data is from the cutoff of data collection from the 2021 DBIR to present.



November 2020 to July 2021

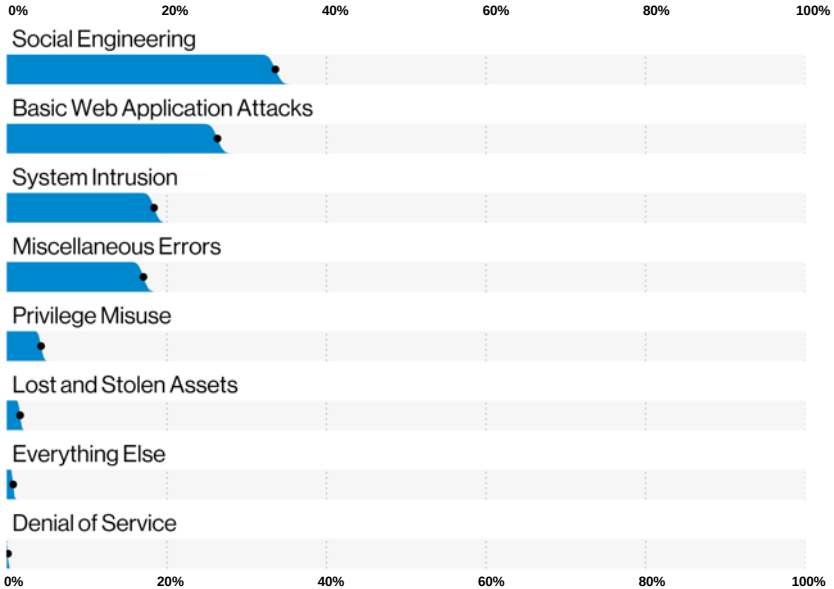
Patterns



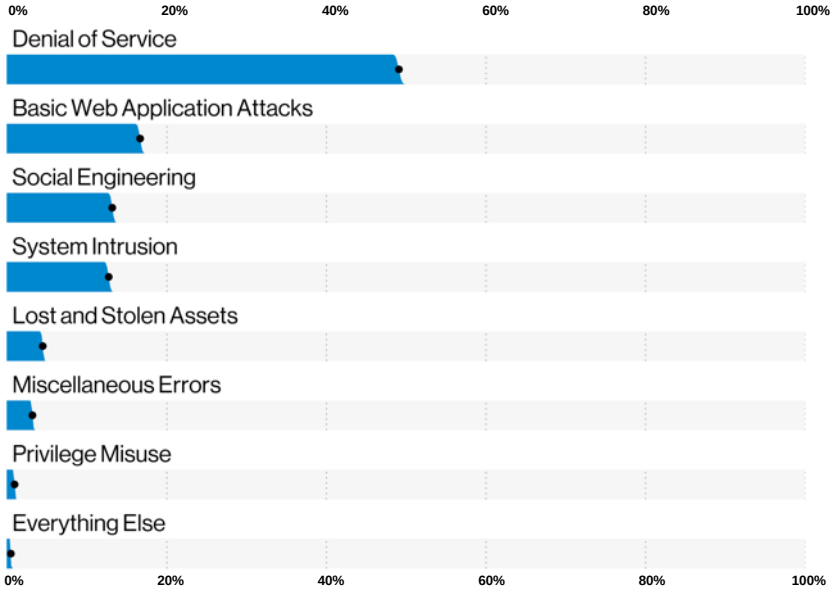
verizon

Updated DBIR patterns using machine learning

The updated patterns explain 99.7% of analyzed breaches and 99.8% of analyzed incidents over all time.



Patterns in breaches, n=5,257



Patterns in incident, n=29,206

Patterns Overview

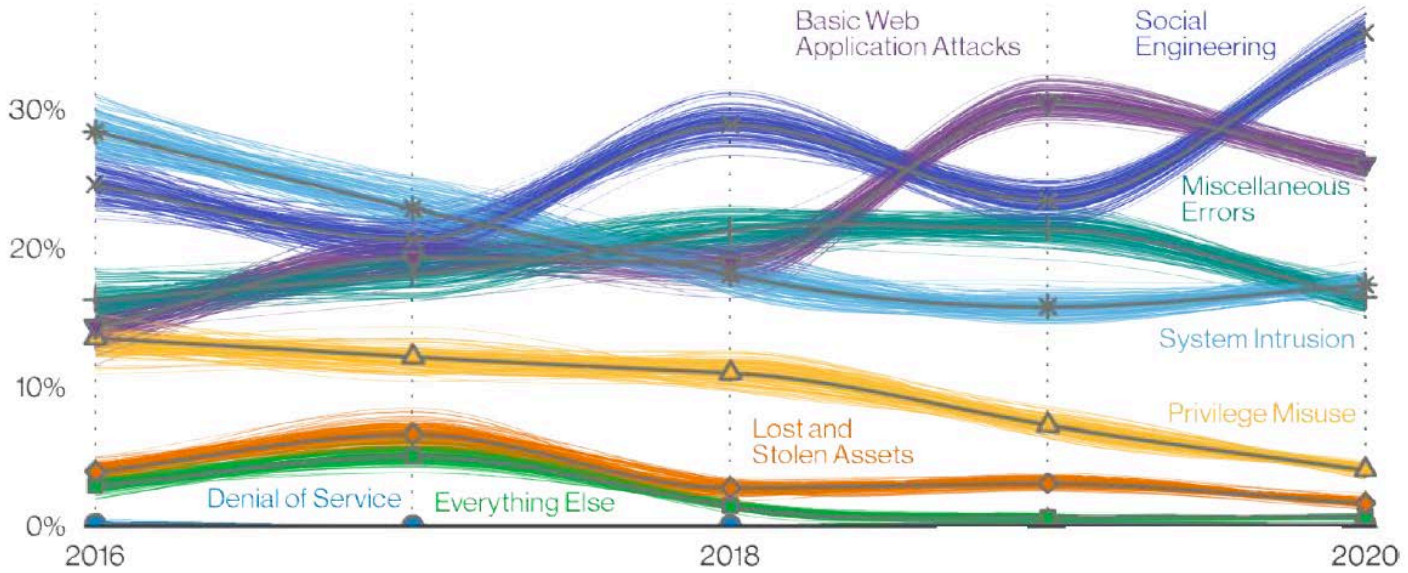


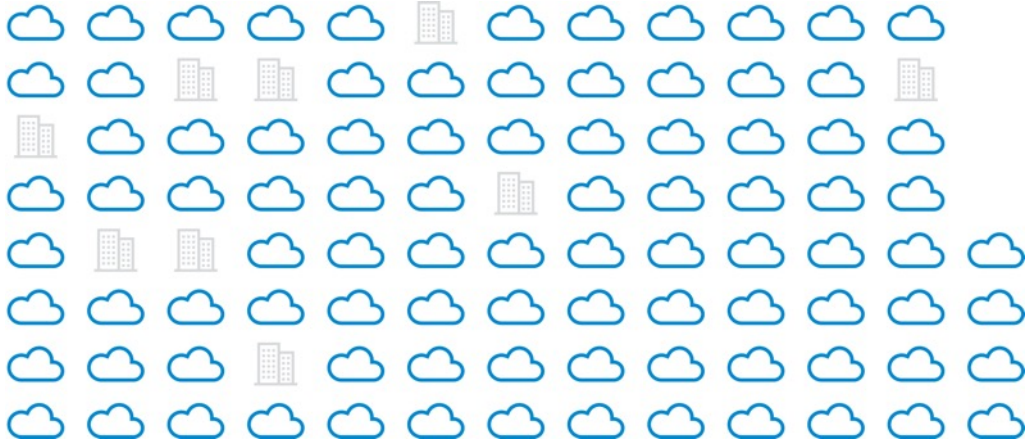
Figure 46. Patterns over time in breaches

Basic Web Application Attacks

This pattern overwhelmingly represents the use of single-step hacking actions against servers.

Most of these servers were cloud-based and were hacked via the Use of stolen credentials or Brute-force attacks.

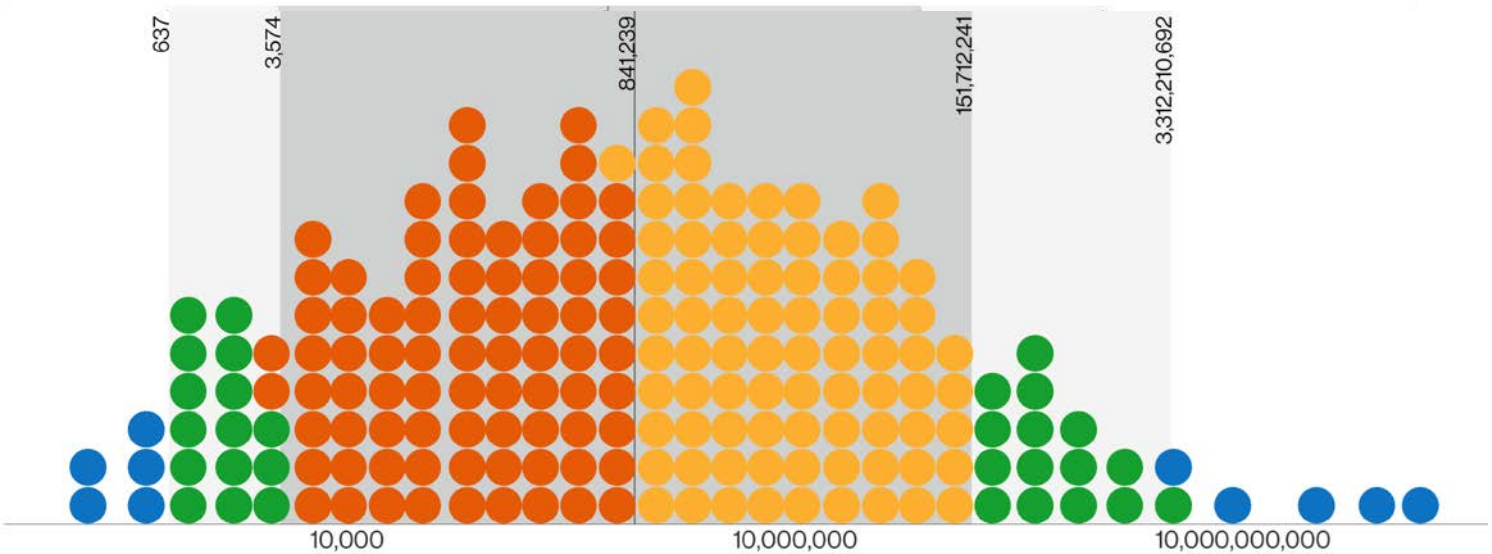
The Information industry overtook the Finance industry as the target of botnet attacks on customers this year.



Cloud in Basic Web Application Attacks breaches.
Each icon represents one breach.

Basic Web Application Attacks (cont'd)

Ninety-five percent of organizations suffering credential stuffing attacks had between 637 and 3.3 billion malicious login attempts through the year.



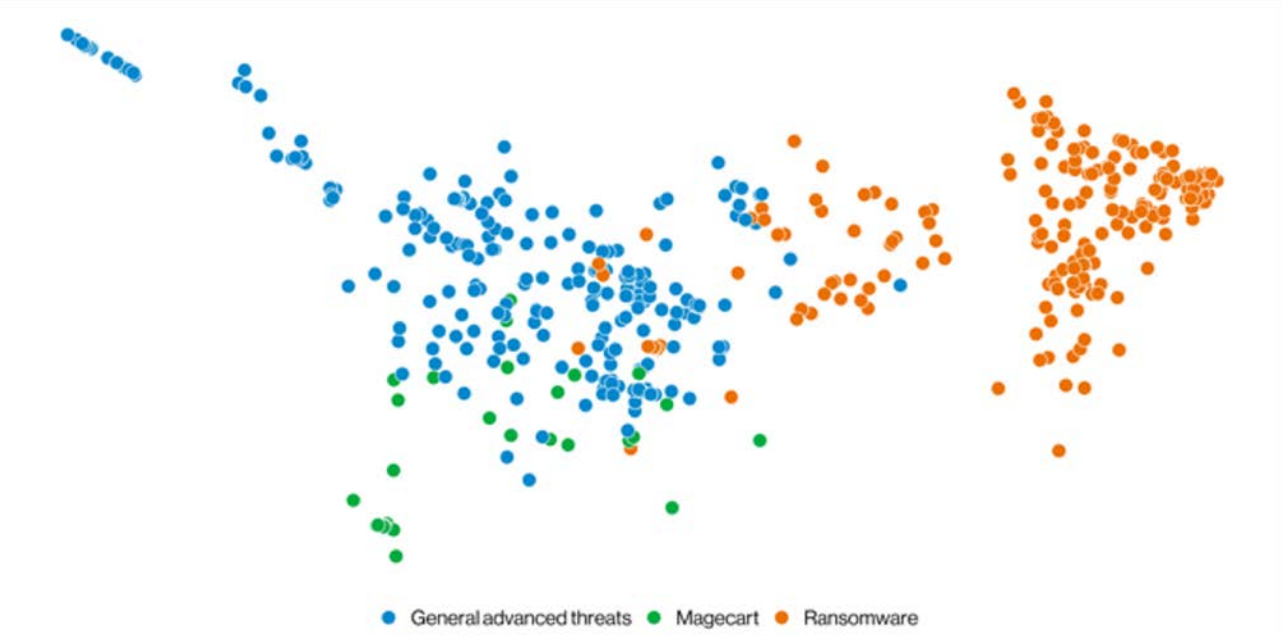
Number of credential stuffing attempts per organization
Credential stuffing attempts per organization, n=821
Each dot represents half of one percent of organizations.

System Intrusion

This new pattern consists of more complex attacks, typically involving numerous steps.

Over 70% of cases in this pattern involved malware and 40% involved hacking.

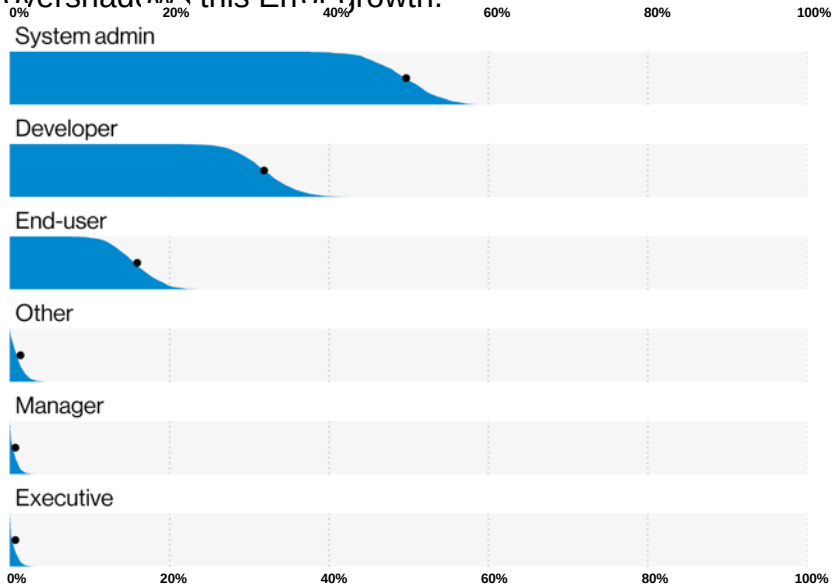
Ninety-nine percent of ransomware cases fell into this pattern.



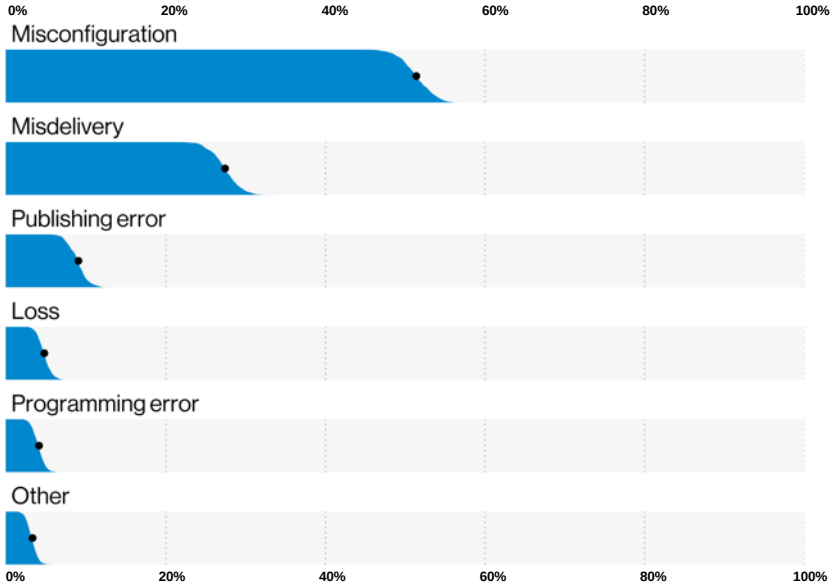
Principal component analysis of themes within System Intrusion pattern breaches

Miscellaneous Errors

Miscellaneous Errors decreased as a percentage of breaches. This was not due to a decrease in errors, however, but because of an increase in other types of breaches. The faster growth in Phishing and other Social-based attacks overshadows this Error growth.



Internal actor variety in Miscellaneous Error breaches, n=157

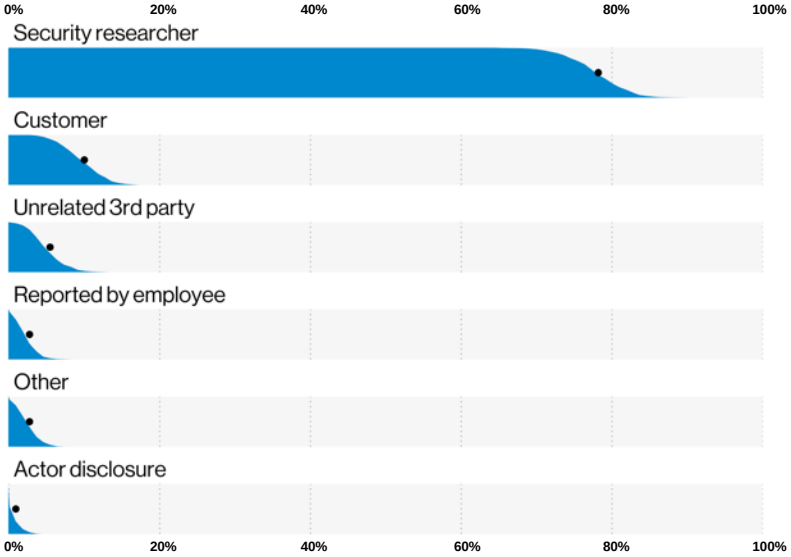


Top error varieties in Miscellaneous Errors breaches, n=609

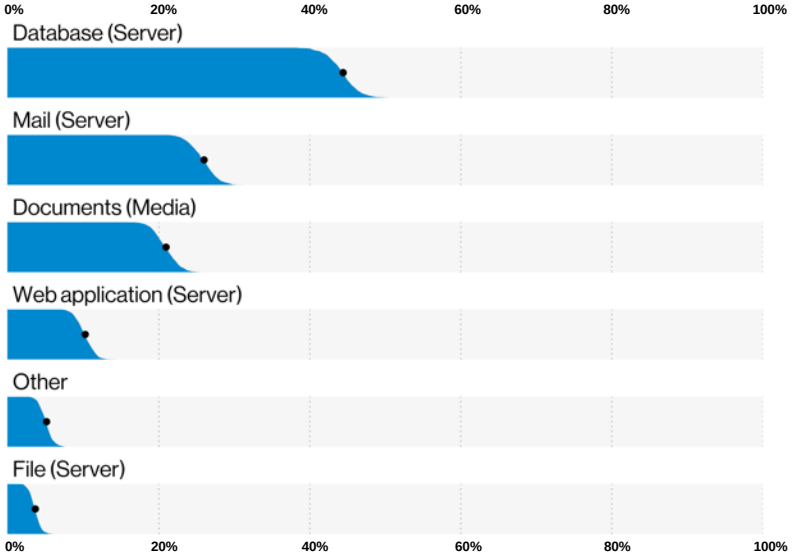
Miscellaneous Errors (cont'd)

Misconfiguration was by far the most common form of error (approximately 52%) and the vast majority of the time, when known, security researchers (80%) were responsible for discovery.

Personal data was the most commonly exposed data type in this pattern.



Discovery method varieties in Miscellaneous Error breaches, n=110

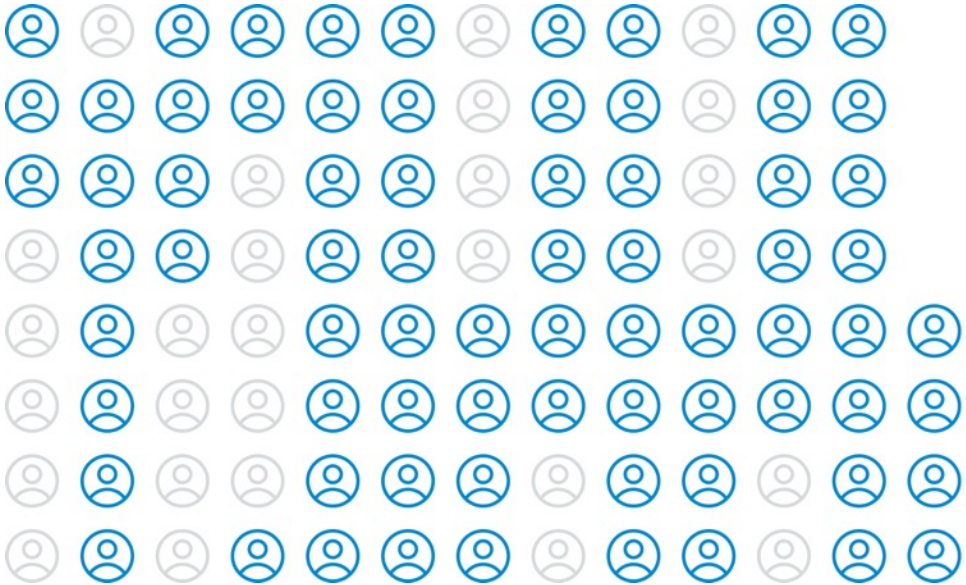


Top asset varieties in Miscellaneous Errors breaches, n=635

Privilege Misuse

Privilege Misuse continues to decrease as a percentage of breaches, thus underscoring the lower incidence of malicious insider threats compared to the top patterns.

Seventy percent of breaches in this pattern were due to privilege abuse.



Seventy percent of breaches in this pattern were due to privilege abuse.
Each icon represents 10 breaches.

Privilege Misuse (cont'd)

Over 30% of incidents take months or years to discover.

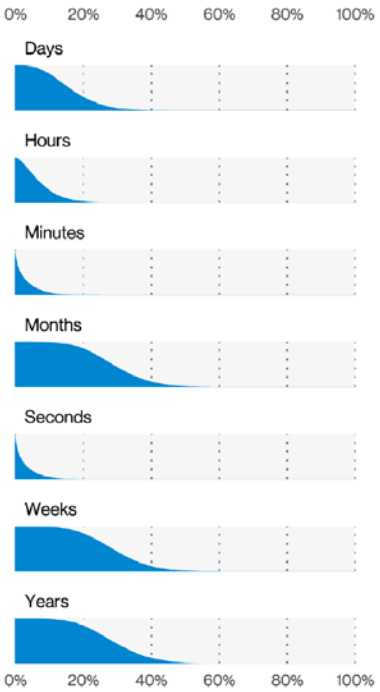
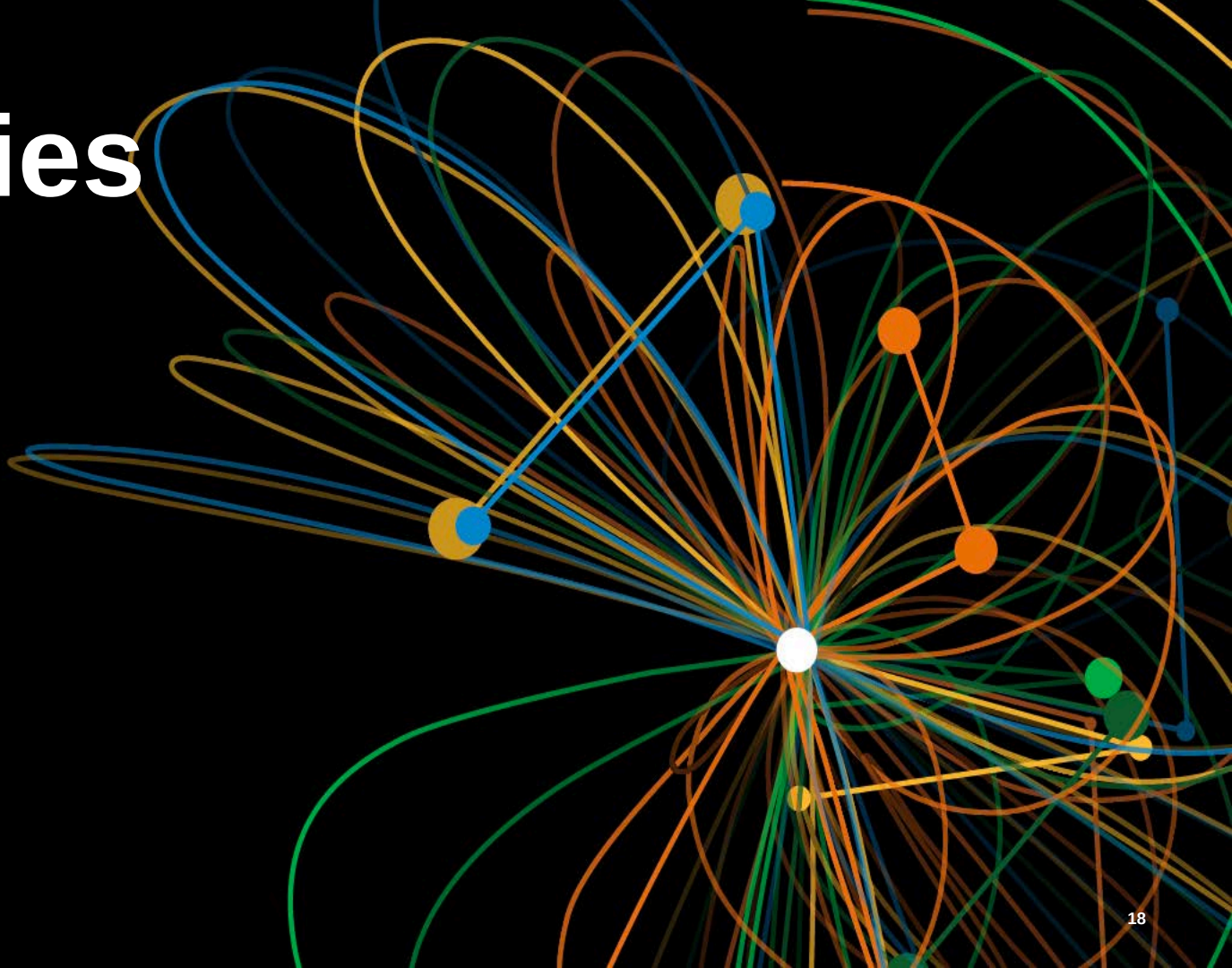


Figure 71. Discovery timeline in Privilege Misuse breaches (n=22)

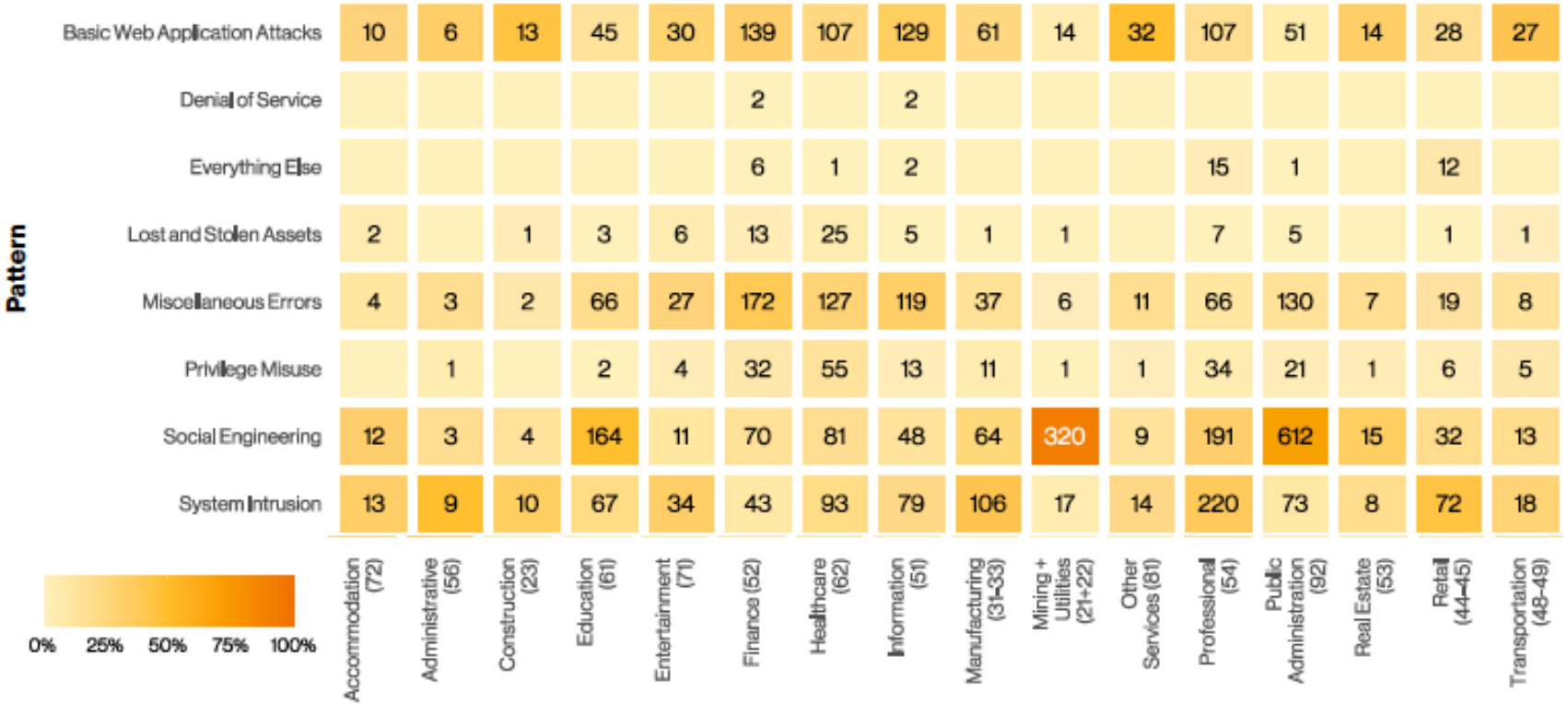
Figure 72. Discovery timeline in 2021 breaches (n=195)

Industries



verizon

Industry Overview (Breaches)



Healthcare NAICS 62

Summary

Basic human error continues to beset this industry as it has for the past several years. The most common Error continues to be Misdelivery (36%), whether electronic or of paper documents. Malicious Internal actions, however, have dropped from the top three for the second year in a row. Financially motivated organized criminal groups continue to target this sector, with the deployment of Ransomware being a favored tactic.

Frequency	655 incidents, 472 with confirmed data disclosure
Top Patterns	Miscellaneous Errors, Basic Web Application Attacks and System Intrusion represent 86% of breaches
Threat Actors	External (61%), Internal (39%) (breaches)
Actor Motives	Financial (91%), Fun (5%), Espionage (4%), Grudge (1%) (breaches)
Data Compromised	Personal (66%), Medical (55%), Credentials (32%), Other (20%), (breaches)
Top IG1 Protective Controls	Security Awareness and Skills Training (14), Secure Configuration of Enterprise Assets and Software (4), Access Control Management (6)

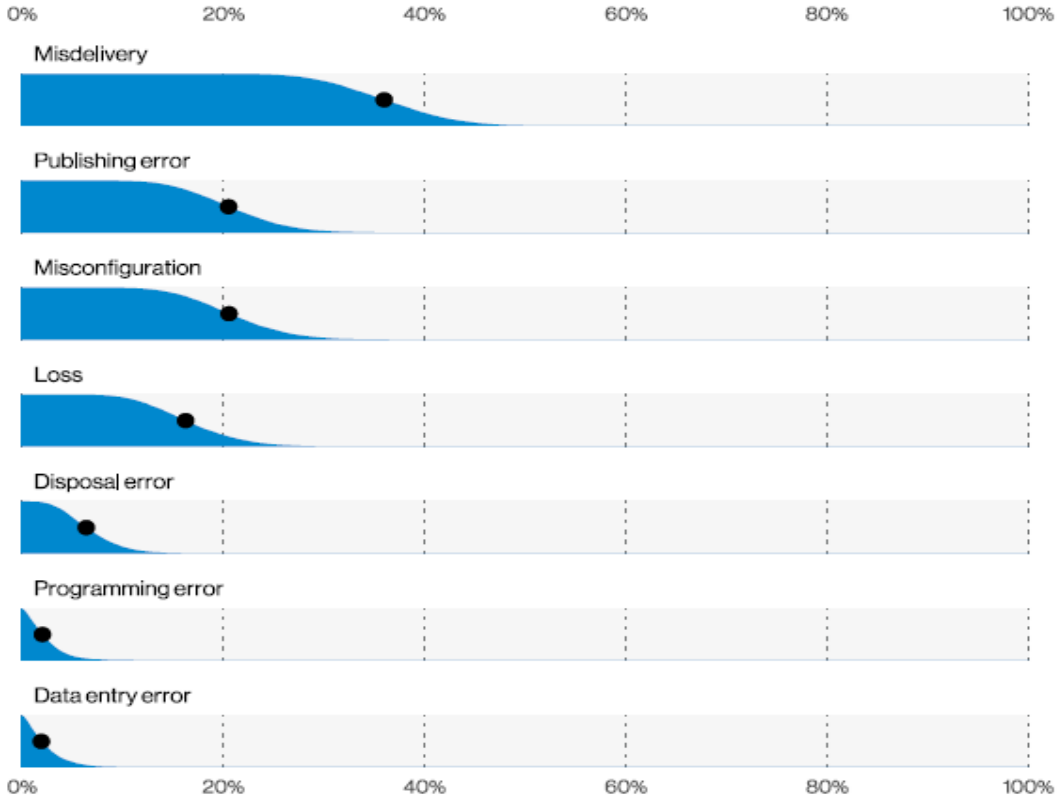
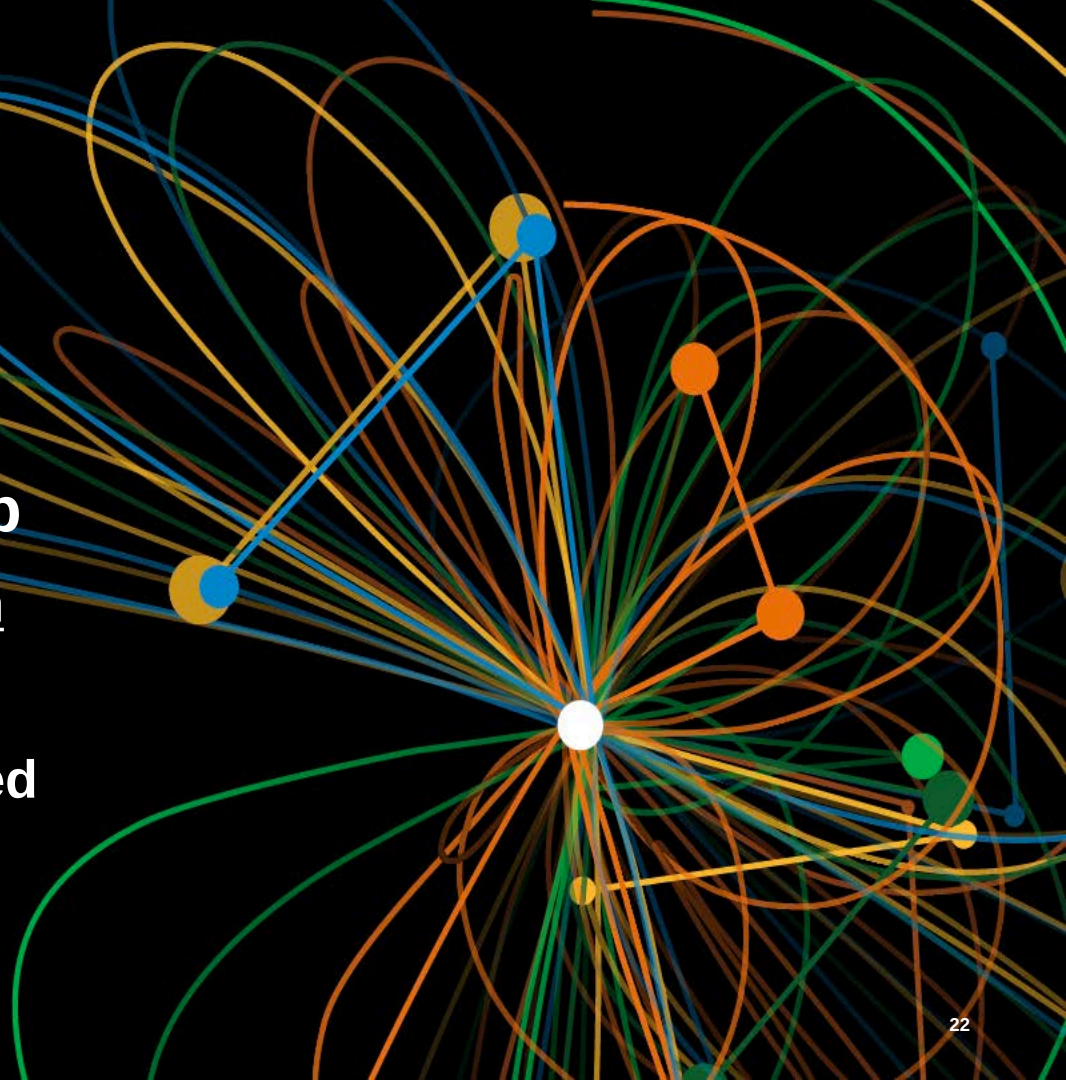


Figure 108. Error varieties in Healthcare breaches (n=70)

More Information

Download the DBIR	**verizon.com/dbir**
Grab the DBIR Graphics	**https://github.com/vz-risk/dbir/tree/gh-pages/2021**
Learn about VERIS	**www.veriscommunity.net and**
	http://github.com/vz-risk/veris
Explore the VERIS Community Database	**http://www.vcdb.org and https://github.com/vz-risk/VCDB/issues**
Ask a Question	**DBIR@verizon.com**
Follow Us	**@vzdbir and hashtag #dbir**

Thank you!



Twitter: @SuzanneWidup

suzanne.widup@verizon.com

and

@VERISDB for data breach feed

verizon