2024 Data Breach Investigations Report

The authoritative source of cybersecurity breach information

Terrance Robinson, Eric Gentry, Bob Bratcher

June 2024

Safe harbor statement

NOTE: In this presentation we have made forward-looking statements. These statements are based on our estimates and assumptions and are subject to risks and uncertainties. Forward-looking statements include the information concerning our possible or assumed future results of operations. Forward-looking statements also include those preceded or followed by the words “anticipates,” “believes,” “estimates,” “expects,” “hopes” or similar expressions. For those statements, we claim the protection of the safe harbor for forward-looking statements contained in the Private Securities Litigation Reform Act of 1995. We undertake no obligation to revise or publicly release the results of any revision to these forward-looking statements, except as required by law. Given these risks and uncertainties, readers are cautioned not to place undue reliance on such forward-looking statements. The following important factors, along with those discussed in our filings with the Securities and Exchange Commission (the “SEC”), could affect future results and could cause those results to differ materially from those expressed in the forward-looking statements: adverse conditions in the U.S. and international economies; the effects of competition in the markets in which we operate; material changes in technology or technology substitution; disruption of our key suppliers’ provisioning of products or services; changes in the regulatory environment in which we operate, including any increase in restrictions on our ability to operate our networks; breaches of network or information technology security, natural disasters, terrorist attacks or acts of war or significant litigation and any resulting financial impact not covered by insurance; our high level of indebtedness; an adverse change in the ratings afforded our debt securities by nationally accredited ratings organizations or adverse conditions in the credit markets affecting the cost, including interest rates, and/or availability of further financing; material adverse changes in labor matters, including labor negotiations, and any resulting financial and/or operational impact; significant increases in benefit plan costs or lower investment returns on plan assets; changes in tax laws or treaties, or in their interpretation; changes in accounting assumptions that regulatory agencies, including the SEC, may require or that result from changes in the accounting rules or their application, which could result in an impact on earnings; the inability to implement our business strategies; and the inability to realize the expected benefits of strategic transactions.

As required by SEC rules, we have provided a reconciliation of the non-GAAP financial measures included in this presentation to the most directly comparable GAAP measures in materials on our website at www.verizon.com/about/investors

Disclaimer

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not be disseminated, distributed, or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

This document is for conceptual discussion only. It is not a formal offer from Verizon. Verizon reserves the right, in its sole discretion, to withdraw and/or modify any or all parts of this document. This material is confidential to Verizon. Further, Verizon shall have no obligation to provide all or any of the Services set forth or discussed in this presentation unless and until the parties execute a formal agreement and Verizon receives all required legal, regulatory, contract and/or FCC tariff approvals, if and as required. The terms and conditions of any such agreement may differ from the descriptions set forth in this document.

This document contains figures such as service goals, targets and the like that are aspirational and are subject to change without notice. These figures are included herein for reference only and Verizon does not provide any warranty or guarantee of any kind that Verizon will achieve or approximate any such goals, targets or the like.

The Verizon name and logos and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners.

Agenda

- **Introductions**
- **DBIR**
  - Summary of Key Findings
  - Incident Patterns Review
  - Industry-tailored Insights
  - Regions
- **VPS Solutions**

Eric Gentry
Managing Principal, VTRAC

Bob Bratcher
Sr.Manager Marketing, ATN Solutions

A comprehensive look at data security patterns

17
years

94
countries

30,458
incidents reviewed in our 2024 report

10,626
data breaches analyzed in our 2024 report

Learn how they're getting in.

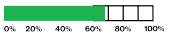
Our 2024 Data Breach Investigations Report analyzed a record high number of breaches. Here's what we learned.

Pathways to breaches

180%

Exploitation of vulnerabilities as an initial access step for a breach grew by 180% over last year.

68%

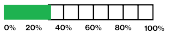


68% of all breaches involved a non-malicious human element.

15%

15% of breaches involved third parties, including data custodians or hosting partner infrastructures.

31%



31% of all breaches over the past 10 years have involved the Use of stolen credentials.

What it costs

$46,000 was the median loss associated with financially motivated incidents involving Ransomware or Extortion of some kind.[1]

$50,000 was the median loss attributed to Business Email Compromise in 2022 and 2023.[1]

Falling for scams is fast.

The median time for users to fall for phishing emails is < 60 seconds.

Response is slow.

It takes around 55 days for organizations to remediate 50% of critical vulnerabilities after patches are available.

1. According to the FBI's Internet Crime Complaint Center (IC3) ransomware complaint data.

Exploitation of vulnerabilities paints an unsustainable picture.

Even when considering only the Cybersecurity Infrastructure and Security Agency (CISA) Known Exploited Vulnerabilities (KEV) catalog, it takes organizations around 55 days to remediate 50% of those critical vulnerabilities after their patches are available.

On the flip side, the median time for detecting the first scan for a CISA KEV vulnerability is five days from publication in the Common Vulnerabilities and Exposures (CVE) database (not from the patch being available).

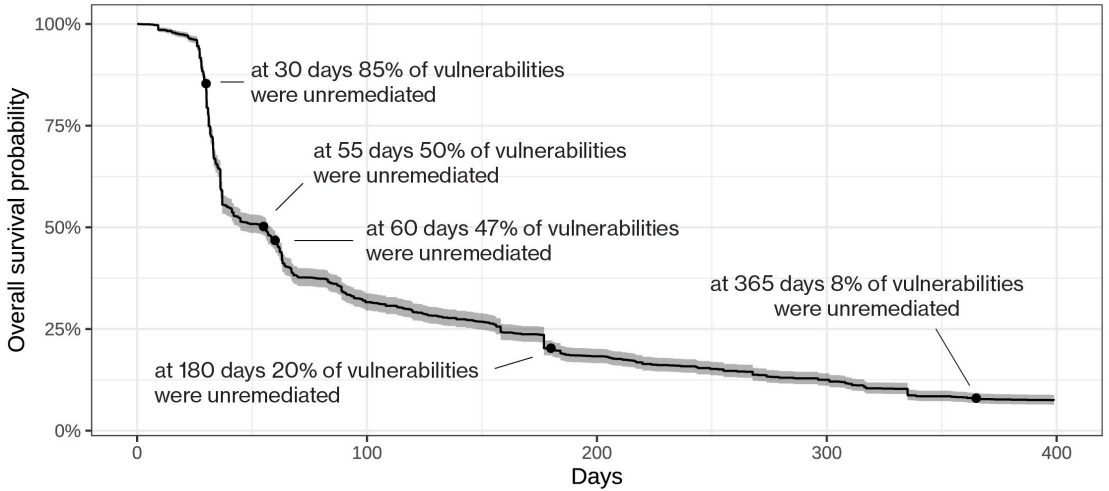


Figure 1. Survival analysis of CISA KEV vulnerability remediation data

Top data-driven and custom metric-related findings

More than two-thirds (68%) of breaches involved a non-malicious human element. These breaches were caused by a person who either fell victim to a Social Engineering attack or made some type of Error.

15% of breaches involved a third party, including data custodians or hosting partner infrastructures being breached, and direct or indirect software supply chain issues.

Our dataset saw a growth of breaches involving Errors, now at 28%, as we broadened our contributor base to include several new mandatory breach notification entities.

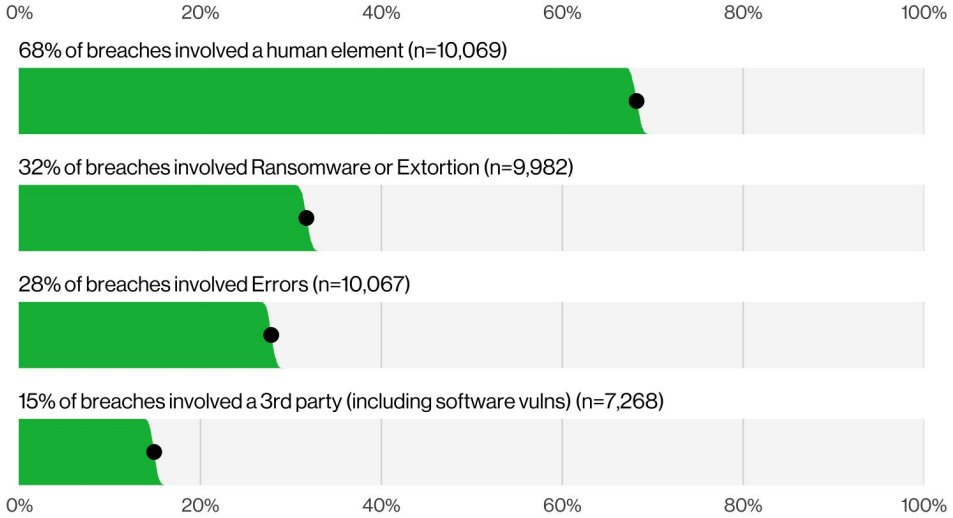


Figure 2. Select key enumerations in breaches

Ransomware

Roughly one-third of all breaches involved Ransomware or some other Extortion technique. Pure Extortion attacks have risen over the past year and are now a component of 9% of all breaches.

The shift of traditional ransomware actors toward these newer techniques resulted in a bit of a decline in Ransomware to 23%.

However, when combined, given that they share threat actors, they represent a strong growth to 32% of breaches. Ransomware was a top threat across 92% of industries.

Over the past three years, the combination of Ransomware and other Extortion breaches accounted for almost two-thirds (between 59% and 66%) of financially motivated attacks. The median loss in Ransomware and other Extortion breaches was $46,000 based on analysis of the FBI IC3 data set.

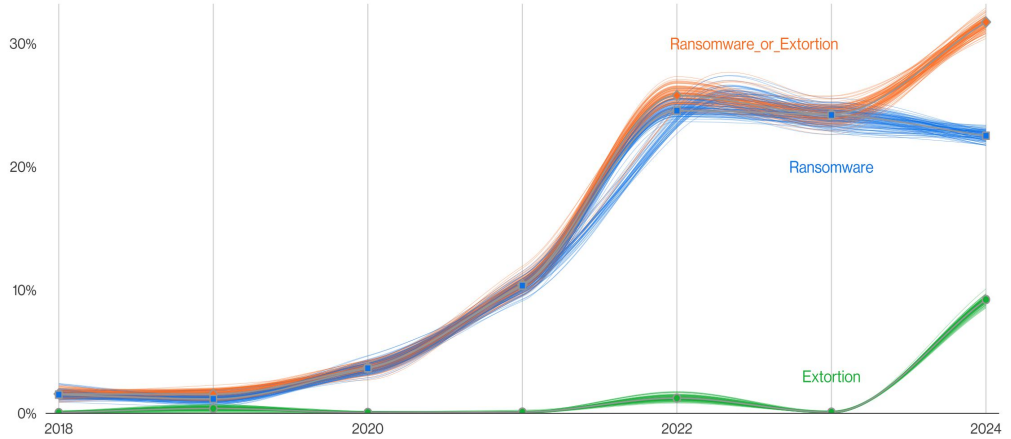
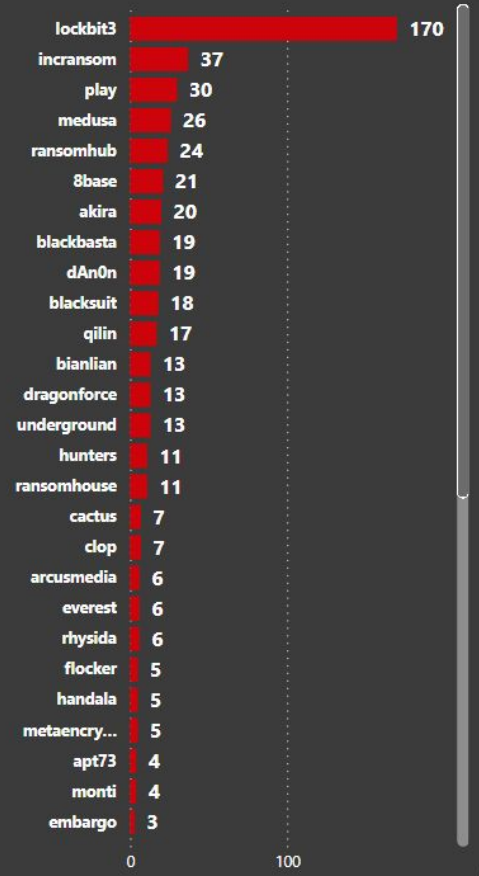


Figure 3. Ransomware and Extortion breaches over time

verizon

May 2024 in Review



548

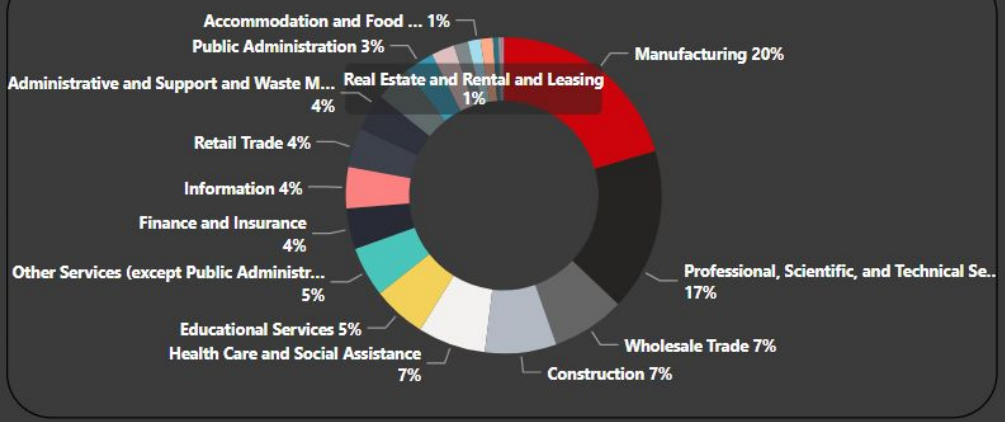
Total # of Known Victims in May 2024

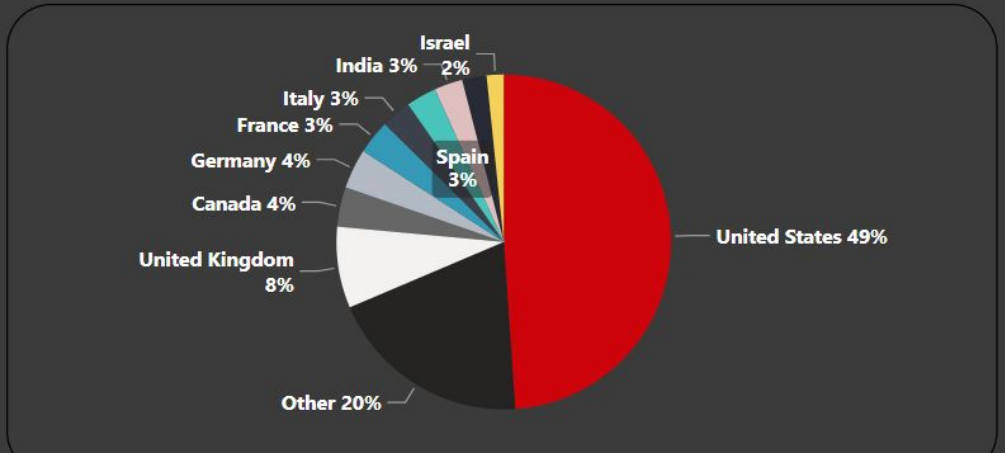
46

Active Ransomware Groups

2024

Victims Year to Date





Incident patterns review

Breach patterns

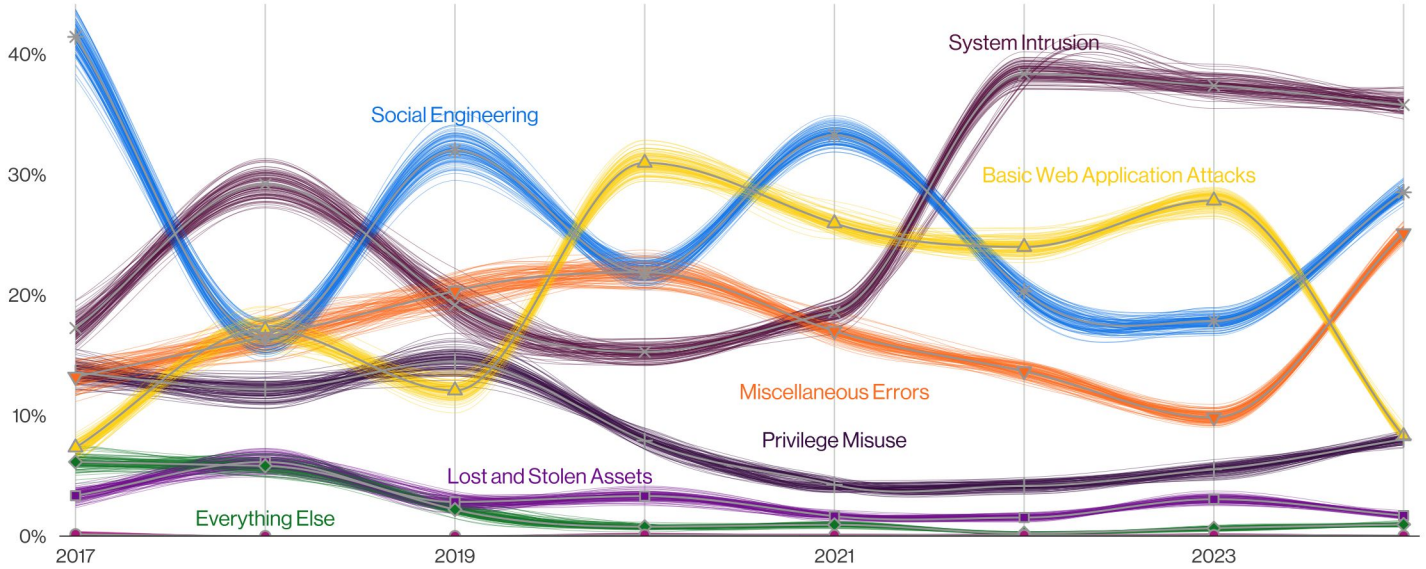


Figure 4. Patterns over time in breaches

System Intrusion

For the third year in a row, System Intrusion leads with 35% of breaches.

70% of System Intrusion incidents involved Ransomware as attackers continued to leverage a bevy of different techniques to compromise an organization and monetize its access.

92% of our industries have Ransomware (or some type of Extortion) as one of their top three actions. Education was the most impacted by MOVEit-related breaches (> 50%).

The median loss associated with Ransomware/Extortion breaches ranged between $3 (three dollars) and $1,141,467 for 95% of the cases. Only 4% of complaints had registered any adjusted loss in FBI IC3 complaints.

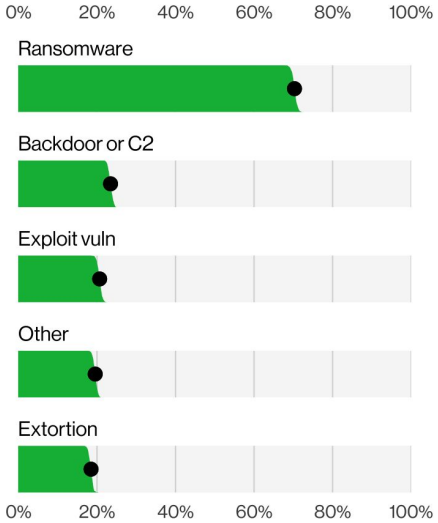


Figure 5. Top Action varieties in System Intrusion incidents

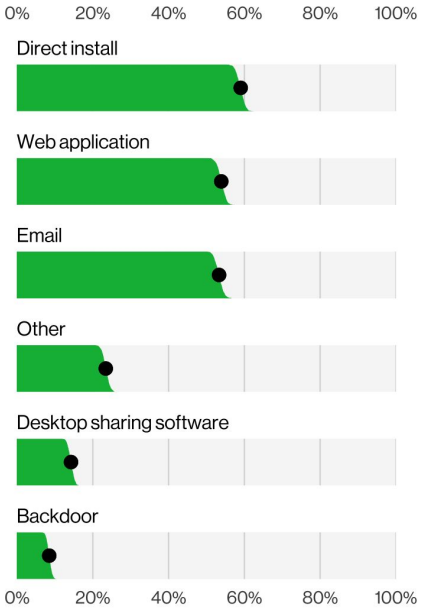


Figure 6. Top Action vectors for System Intrusion incidents (n=1,789)

Social Engineering

We have not seen a dramatic rise in Pretexting like we did last year. However, it is also true that it hasn't decreased. More than 40% of incidents involved Pretexting and 31% involved Phishing.

Social Engineering accounts for 29% of breaches and 12% of incidents. Extortion-based attacks were also classified here, giving this pattern a big bump.

Based on FBI IC3 data, the median amount stolen in a BEC has remained stable at around $50,000. The FBI's response team was able to recoup just under 80% of the lost money for more than 50% of the cases.

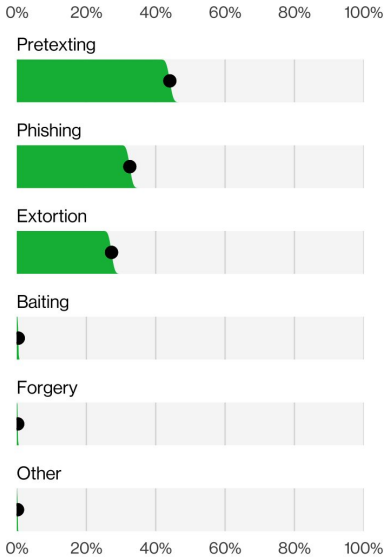


Figure 7. Top Action varieties in Social Engineering incidents (n=3,647)

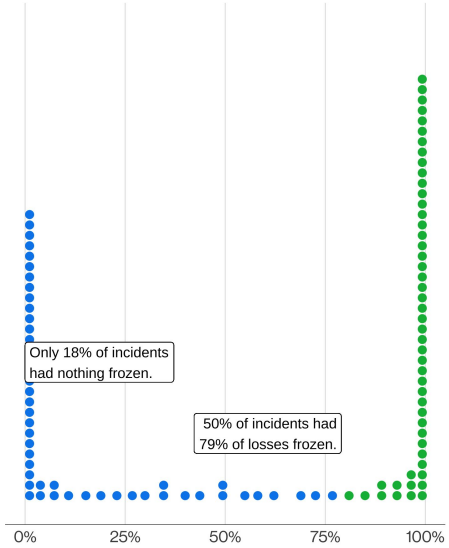


Figure 8. Percentage of adjusted losses distribution for BECs (n=2,041). Based on FBI IC3 complaints in which a transaction occurred.

Miscellaneous Errors

This pattern is significantly up – 25% as opposed to 9% last year. The growth is due in large part to mandatory reporting entities, suggesting that that Errors are a more prevalent cause of breaches.

End-users accounted for 87% of errors as opposed to 20% in last year's report; while System administrators dropped to only 11% (from 46% last year). This drop is in large part the result of the corresponding rise in Misdelivery.

Data compromised included Personal (94%), Internal (34%) and Bank (14%).

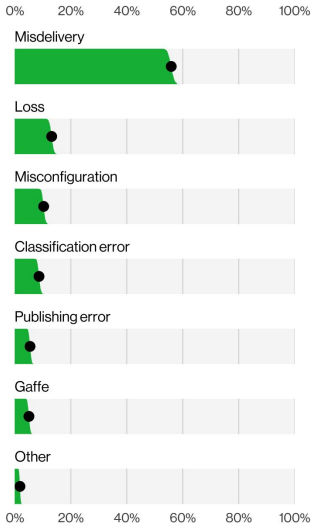


Figure 9. Top Action varieties in Miscellaneous Errors breaches (n=2,586)

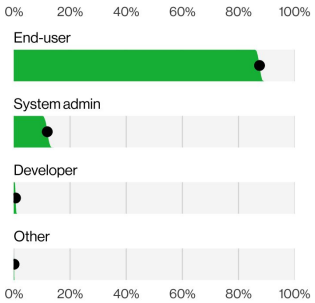


Figure 10. Top Actor varieties in Miscellaneous Errors breaches (n=2,260)

Basic Web Application Attacks

Basic Web Application Attacks breaches and incidents tend to be largely driven by attacks against Credentials, which are then leveraged to access a variety of resources. They represented 8% of the dataset.

77% of Basic Web Application Attacks breaches involve the Use of stolen credentials.

13% of breaches in this pattern involve the Exploit vuln action.

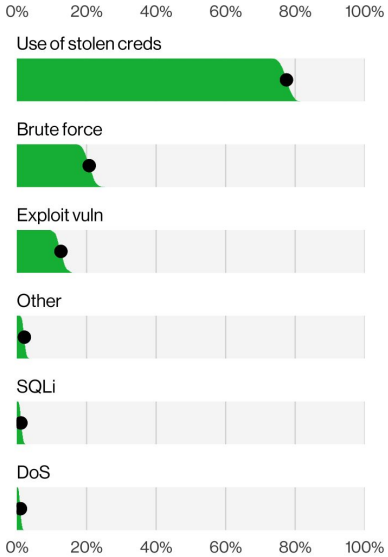


Figure 11. Top Hacking actions in Basic Web Application Attacks breaches (n=713)

Denial of Service

Denial of Service was responsible for 55% of incidents analyzed this year.

Content delivery network (CDN)–monitored, web application–focused Denial of Service attacks show a median attack size of 1.6 gigabits per second (Gbps), with the 97.5th percentile of those attacks increasing to 170 Gbps from the previous high of 124 Gbps. Those attacks are usually short duration, with large volumes – 50% of those attacks are less than five minutes long.

Attacks on ISP-level defenses, including individuals, are significantly smaller in size and duration, with a median time of nine minutes.

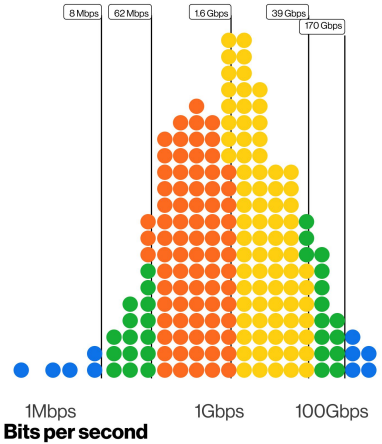


Figure 12. Bits per second in CDN distributed DoS (DDoS) incidents (n=10,713, log scale)

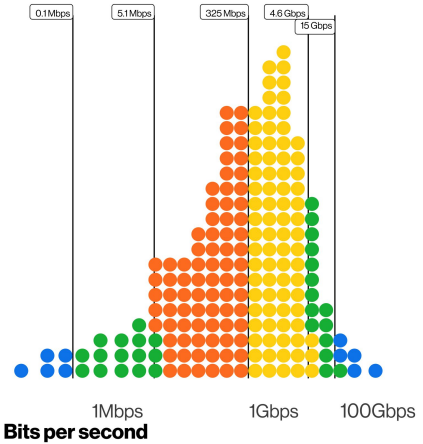
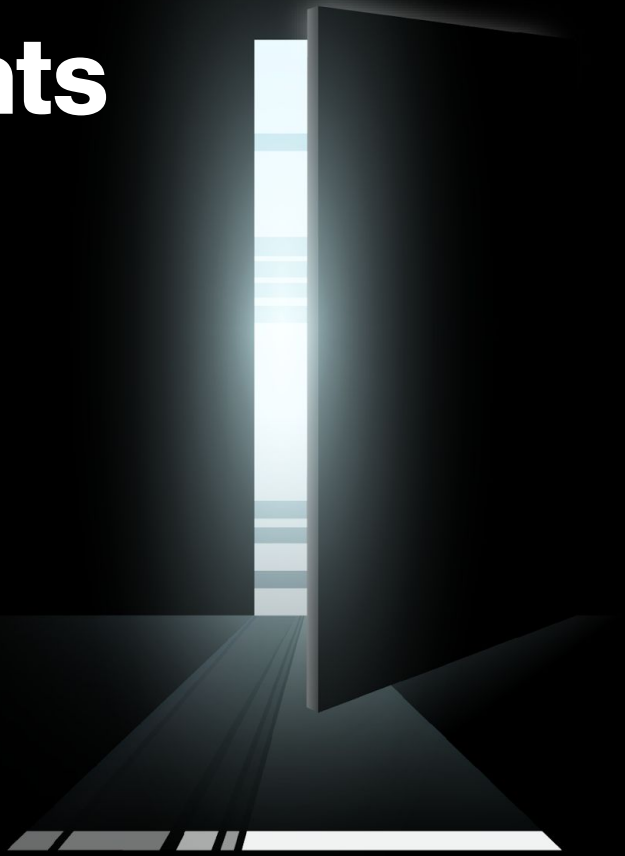


Figure 13. Bits per second in ISP-level DDoS incidents (n=800,155, log scale)

Industry-tailored insights



Breaches by Industry

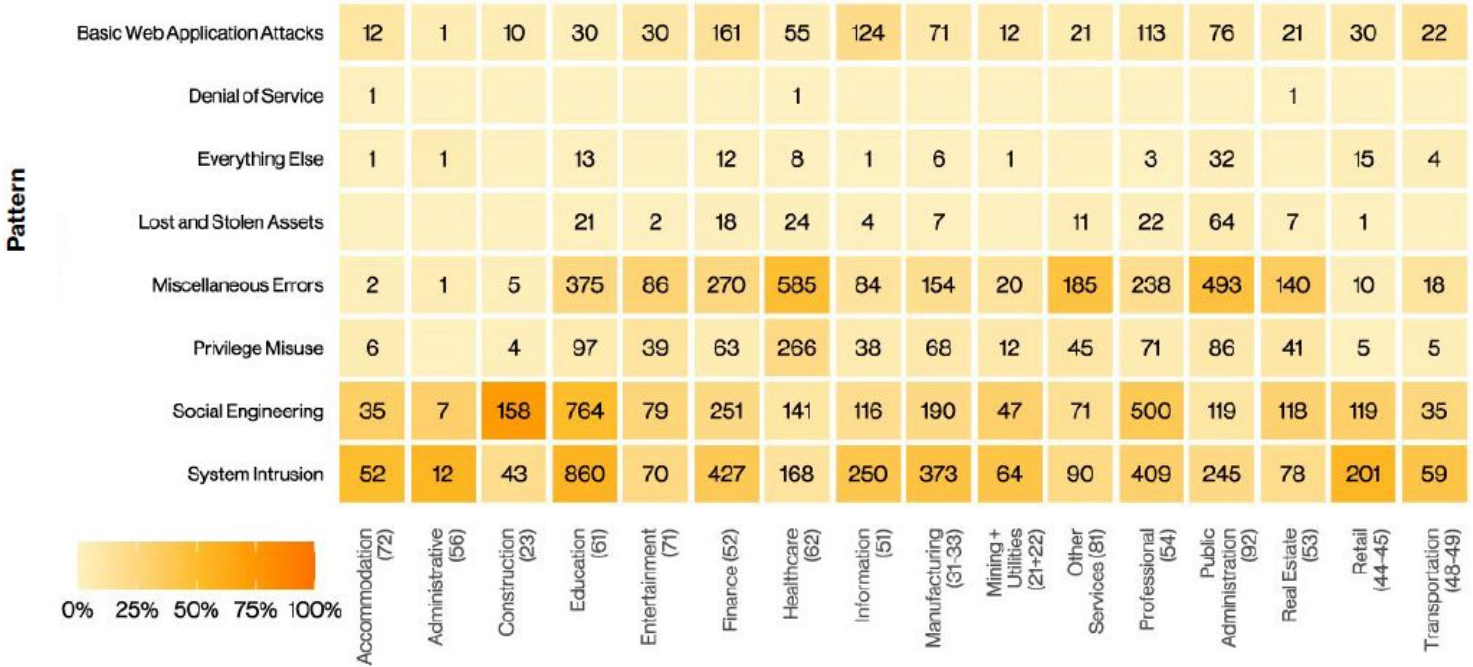
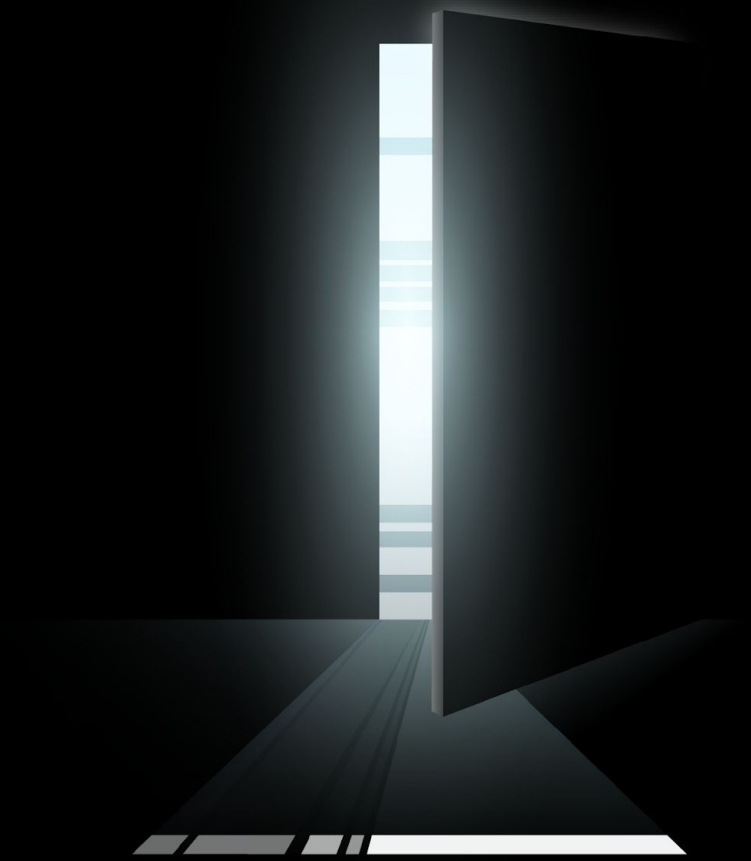


Figure 14. Breaches by industry

Regions



Regions – Northern America

The System Intrusion pattern remains among the top for all regions. The two main action types are hacking via the Use of stolen credentials and malware in the form of Ransomware.

Social Engineering has increased from 29% to 45% when viewed as a whole (mostly driven by Northern America).

Extortion was the greatest driver of this growth in NA as it was present in 46%
of its breaches. Our other Social Engineering favorites had a more timid showing in Northern America breaches: 13% for Phishing and 4% for Pretexting.

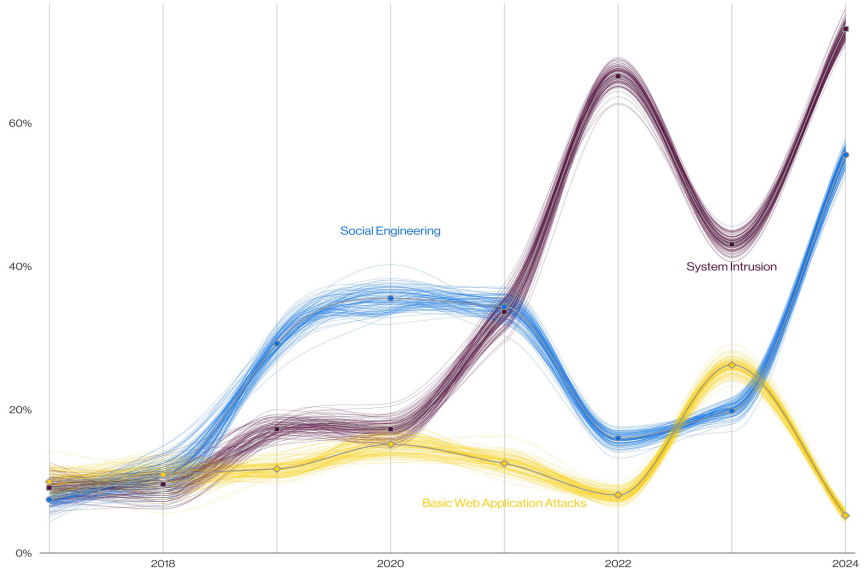


Figure 15. Top patterns in Northern America breaches over time

Regions – APAC and EMEA

With regard to actors, the majority of cybercrime continues to be carried out by financially motivated external parties.

One notable exception is that of APAC, where instead of more than 90% of attacks being financially motivated, we see that the Espionage motive is greater than it is elsewhere and accounts for 25% of breaches (as opposed to between 4% and 6% in the other regions).

Due to the nature of our new contributing agencies in EMEA, we have seen a substantial rise in the Miscellaneous Errors pattern.

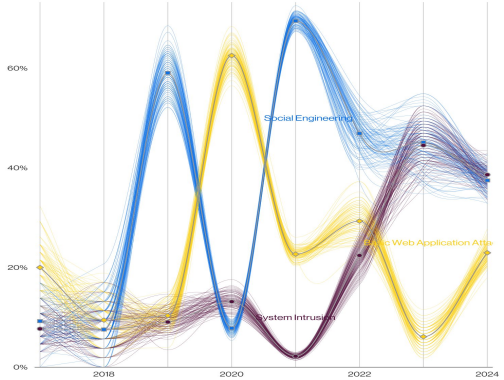


Figure 16. Top patterns in APAC breaches over time

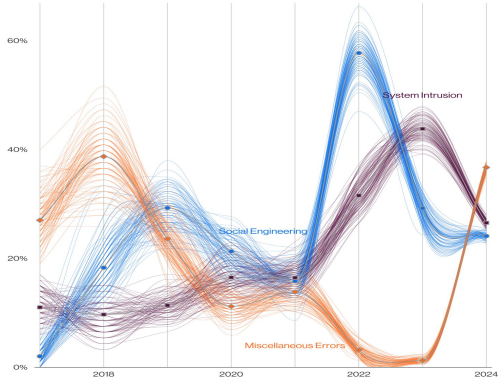
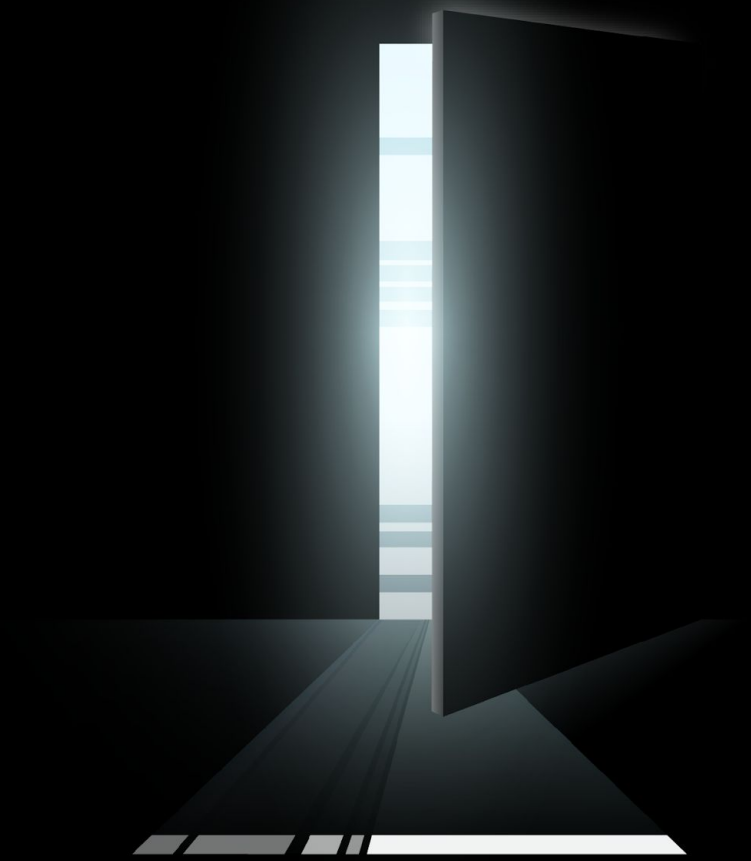


Figure 17. Top patterns in EMEA breaches over time

VPS Solutions



VPS Solutions

- **Network Detection and Response***
- **DDoS Shield for Internet Dedicated Services***
- **Verizon Business Internet Security***
- DDoS Shield
- Penetration Testing
- PCI-DSS
- Rapid Response Retainer
- Executive Breach Simulation
- Ransomware Attack Simulation
- Security Risk Assessment
- Red Team Operations

*Available for both Sell To/Sell Thru

Questions?

DBIR: verizon.com/dbir
Email: dbir@verizon.com

If you are interested in becoming a contributor to the annual Verizon DBIR (and we hope you are), the process is very easy and straightforward. Please email us at .