verizon

Read time: < 4 minutes

2016 Data Breach Investigations Report

Retail

Around 90% of all security incidents in the retail sector involved denial of service (DoS), point-of-sale (POS) or web app attacks. Attackers were often able to compromise systems in hours or less. But in 79% of cases it took retail organizations weeks or more to discover a breach had occurred.

This year's Data Breach Investigations Report (DBIR) is again based around the nine incident classification patterns identified in our 2014 report. Just three of these patterns – DoS attacks, POS instrusions and web app attacks – account for the vast majority (90%) of all security incidents experienced by retail organizations. When we look at breaches – with confirmed data disclosure – most of those (64%) involved POS intrusions.

To help you plan your defenses, we'll look in greater depth at the three patterns that account for most security incidents in the retail sector.

The Data Breach Investigations Report is the most comprehensive report of its kind. For the ninth time, it pulls together incident data from around the world, to reveal what's really happening in cybersecurity. The 2016 DBIR provides insights based on over 100,000 incidents from 82 countries, including 2,260 analyzed data breaches.

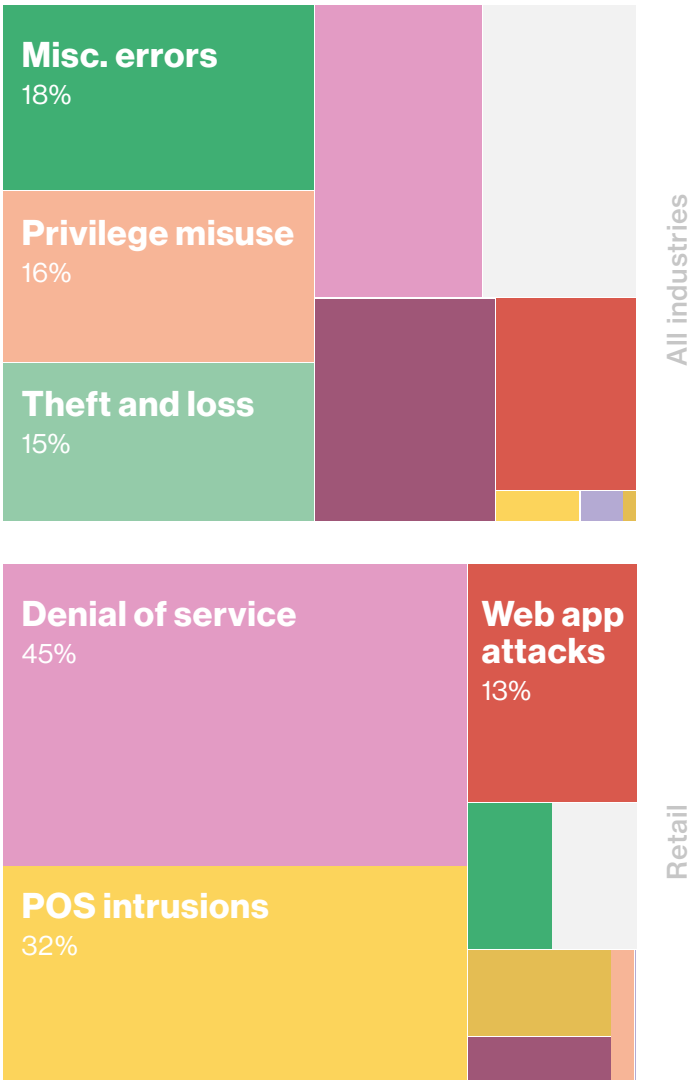


Figure 1: Incidents by pattern: All industries versus retail

Highlights of the 2016 DBIR

Prioritizing your defenses means understanding the threats you face. The 2016 DBIR enables you to do just that by providing insights based on over 100,000 incidents, including 2,260 analyzed data breaches.

The story is of cybercriminals motivated by money exploiting unforced errors:

- 89% of breaches had a financial or espionage motive.
- 63% of confirmed breaches involved leveraging weak, default or stolen passwords.
- 30% of phishing messages were opened in 2015; and 12% of targets clicked on the malicious attachment or link.
- 85% of successful exploit traffic was from the top 10 vulnerabilities. The other 15% covered 900 vulnerabilities.

This year's DBIR again focuses on the nine incident patterns we first identified in 2014, which cover over 85% of incidents. Understanding them will help you disrupt the dynamics of cybercrime and decrease the attackers' ROI.

Denial of service

Almost half (45%) of security incidents in the retail sector involved DoS attacks, intended to overwhelm organizations with malicious traffic and bring their normal business operations to a halt.

While the aim of DoS attacks is rarely to steal data, they can still be extremely damaging to your reputation and business operations. How would you cope if your key systems were taken out of action for an hour or, as is often the case, longer? Typical DoS attacks last for days and are difficult to mitigate with in-house resources. The costs associated with missed orders and the time spent on remediation can be enormous.

And it's worth bearing in mind that you don't have to be a high-profile company or engage in controversial activities to be a victim. Our data shows that DoS attacks affect all types of organizations.

What can you do?

- **Establish a mitigation plan:** Have a solid, comprehensive strategy that details what your organization should do in the event that your initial anti-DoS service fails**.**
- **Test your plan:** Test and update your plan regularly as your infrastructure and processes change, and as new DoS techniques emerge.
- **Segregate key servers:** Don't allow less sensitive systems to act as a gateway to more important ones. Separate critical infrastructure onto different network circuits.

Point-of-sale (POS) intrusions

Compromising the computers and servers that run POS applications is still proving fruitful for attackers seeking payment card data. These attacks are a significant threat in retail and accounted for 32% of all incidents and 64% of breaches, where data was stolen, in 2015.

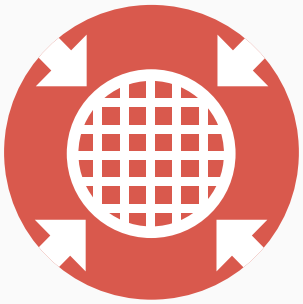
The vast majority of successful breaches leverage legitimate credentials to access the POS environment. Once attackers gain access to the POS devices, they install malware, usually a RAM scraper, to capture payment card data.

The following recommendations could help you prioritize your resources and minimize the risks.

What can you do?

- **Review your vendors' authentication:** If you aren't using two-factor authentication where you can, then you should. Also, because so many attacks come via vendors, you should seek partners that are using strong authentication too.
- **Monitor and separate:** Track who's using your POS systems – how and when – to make certain they're only being used by the right people. Separate the POS environment from the corporate LAN, so that it's not visible to the entire internet.
- **Use anti-virus software:** Basic though it seems, our research shows there are too many POS devices with no anti-virus protection at all. So install it on yours and keep it updated.

Web app attacks



Over one-in-ten (13%) of all security incidents and over a quarter (26%) of breaches in the retail sector involved attacks on web apps.

These attacks relate to the rising use of botnets – such as Dridex – to compromise customer devices. Key loggers are employed to steal passwords and then the stolen credentials are used for fraudulent transactions on the website.

Not all website compromises are targeted affairs. Across our all-industry dataset, we've seen incidents of websites that were used in distributed denial-of-service (DDoS) attacks or repurposed as phishing sites.

Incidents involving web apps are usually motivated by financial gain.

What can you do?

- **Patch promptly:** Establish a patch process for CMS platforms and third-party plugins.
- **Enable two-factor authentication:** Both phishing and malware lead to lost credentials. Using two-factor authentication can break the chain of attack.
- **Validate inputs:** Whether it's ensuring that the image upload functionality checks that it is actually an image and not a web shell, or that users can't pass commands to the database via the customer name field, many of the methods used to breach your data can be detected easily by establishing effective input validation.

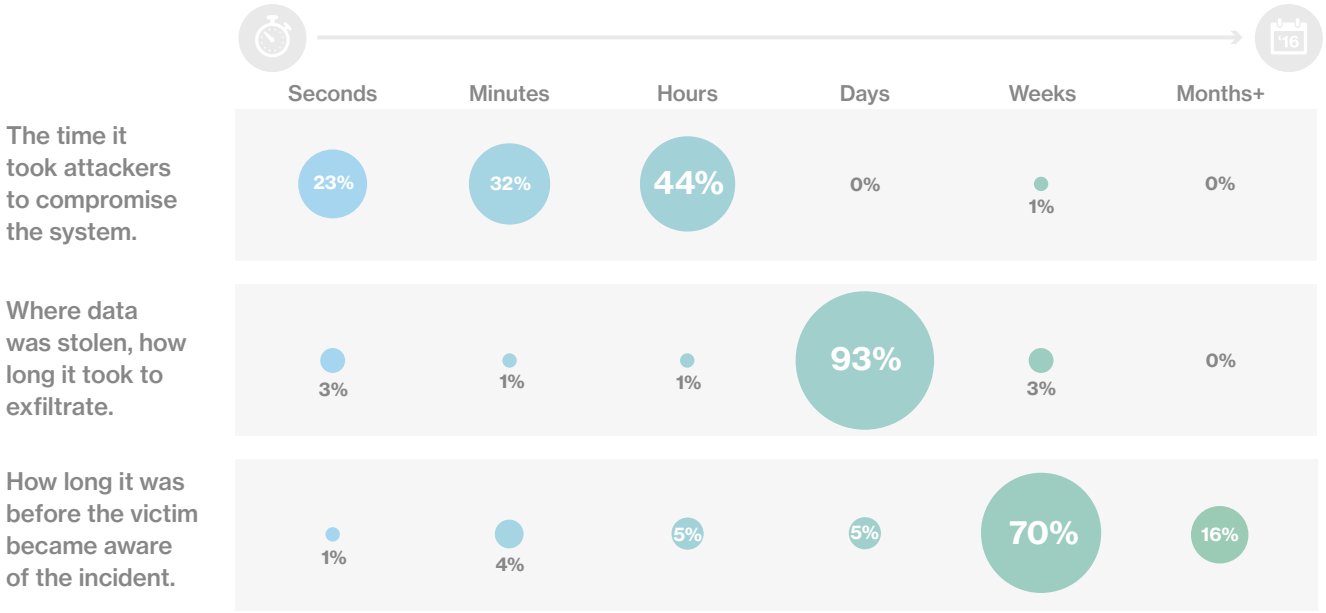


Figure 2: Incident timeline for retail

Time to discover an incident

Systems were compromised in hours or less in the retail sector in 99% of cases. Exfiltration was also fast – in over 98% of incidents data was taken in days or less. But organizations typically took weeks or longer to discover there had been an incident. And in 16% of cases, discovery took months or more.

You have to know what you're really up against. Only then can you get the right data security solutions for your organization. Build your defences on the DBIR. Get the vital insights you need today.

Read the report now ›

How can we help?

Our Managed Security Services (MSS) platform processed over 61 billion events in 2015. And we operate nine security operations centers on four continents. We were positioned as a leader in the 2015 Gartner Magic Quadrant for Managed Security Services, Worldwide.

We put our unique security insight to work every day in the solutions we provide – to help you guard against the threats you face.

Our cloud-based distributed denial of service (DDoS) protection platform, DDoS Shield, can filter large volumes of DDoS traffic – regardless of carrier.

Our PCI Compliance consultants have a deep understanding of risk and how to manage it. They can help you identify, assess and close the security holes that could damage you the most, and implement consistent processes to help protect your POS environment.

Our Unified Security Services are comprehensive, managed services that help protect the network edge where data flows in and out of your organization. That's ideal for retail businesses with a large number of physical locations.

VerizonEnterprise.com

© 2016 Verizon. All Rights Reserved. The Verizon name and logo 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. WP16714 04/16