2014 Data Breach Investigations Report

RETAIL

This year’s Verizon Data Breach Investigations Report (DBIR) is based around nine incident classification patterns: common signatures that describe the vast majority of security incidents.

Just three of these nine patterns cover almost three-quarters (74%) of the security incidents experienced by retail companies. Improving your defenses against these three threats could make your organization much more secure.

DENIAL OF SERVICE

The top threat affecting your operations is not what you might expect: in fact, it’s rarely to do with stealing data at all. 33% of the incidents from retail organizations in our dataset are denial of service (DOS) attacks.

DOS attacks involve the use of armies of “botnets” to overwhelm an organization's systems and applications with malicious traffic, causing normal business to grind to a halt, sometimes until the victim pays a ransom.

The scale of DOS attacks has gone up 115% since 2011, as attackers have refined their methods. In the past malware was often used to co-opt the PCs of unwitting home users into the criminal’s botnet. Now, attackers are targeting servers. These are more powerful and have high-bandwidth connections, allowing the attacker to mount a much bigger attack.

While DOS attacks are rarely connected to attempts to steal data, they can still be extremely damaging to your reputation and business operations.

Imagine if a DOS attack took your ecommerce site down in one of your busiest periods. Or if it paralyzed your ERP applications. The costs of lost productivity and time spent on remediation can be enormous.

And 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 kinds of companies.

What you can do:

• **Segregate key assets.** Keep your most important systems on a separate network circuit so they won’t be compromised by an attack targeting other servers.

• **Test your anti-DOS service.** This isn’t an install-and-forget type of service.

• **Have a plan.** Key operations teams need to know how to react if there is an attack. You should also have a backup plan in case your primary anti-DOS service doesn’t work.

Data breaches can be extremely costly. The Verizon DBIR has, for years, been the best source of insight about the threat landscape. This year’s report covers over 63,000 security incidents from 95 countries.

This year’s DBIR uses statistical methods to identify ‘clusters’ of similar incidents and breaches. Just nine patterns cover 92% of the security incidents that we’ve analyzed over the last ten years.

![Security incidents by pattern, retail companies versus all industries, 2011–2013](image_url)
POS INTRUSIONS
The second most popular type of attack is much more what you’d expect in the retail sector: intrusions against point of sale (POS) systems. Nearly a third of incidents involved POS intrusion, and that’s without including attacks that involved tampering directly with devices to skim card data.

POS attacks get a lot of media coverage, but from a frequency standpoint, this largely remains an issue for small and medium-size businesses — and in reality, overall the number of POS attacks in 2012 and 2013 is substantially lower than the number recorded in 2010 and 2011 (despite having ten times more contributors in the latter years). But the fact is that even the largest retailers may often have very decentralized structures, which can leave individual stores vulnerable to attack.

Most POS attacks follow a clear pattern. A financially motivated attacker, often an organized criminal group operating from Eastern Europe, compromises a POS device, installs malware to gather card data as it’s being processed, and then uses that card data to access funds.

These attackers are experienced at exploiting a wide range of known POS flaws quickly.

What you can do:
• Restrict remote access. Limit remote access into your POS systems by third-party companies — such access can be misused.
• Enforce strong password policies. Our PCI Compliance Report found that over 25% of companies still use factory defaults.
• Reserve POS systems for POS activities. Don’t allow staff to use them to browse the web, check email or play games.
• Use two-factor authentication. Two-factor authentication helps prevent stolen credentials being used to gain access to systems.

31%
OF INCIDENTS WERE ATTRIBUTABLE TO POS INTRUSIONS.

WEB APP ATTACKS
One in ten incidents in our retail dataset involved attacks on web applications. Retail today is a web-heavy industry — and not just because of ecommerce. As a result, attackers can use a wide variety of techniques to target your critical systems.

While most other attacks against retailers are financially motivated, web app attacks are primarily ideological. In our whole 2013 dataset, almost two-thirds of web app attacks were attributable to activist groups. With retailers’ corporate social responsibility practices often in the news, ranging from staff welfare to environmental damage, it’s unsurprising that some bad press would translate into action.

What you can do:
• Use two-factor authentication. Prevent stolen passwords from being used to break into your web apps.
• Consider switching to a static content management system. Instead of executing code to generate the content for every request, pre-generate pages to reduce the opportunity for exploits.
• Enforce lockout policies. Locking accounts after repeated failed login attempts will help to thwart brute-force attacks.

10%
OF INCIDENTS WERE WEB APP ATTACKS.

How can we help?
We put our unique security insight to work every day in the solutions we provide. Our products and services can help you guard against the threats you face.

• Our DoS Defense Detection and Mitigation service analyzes your traffic at the network level and looks for anomalies. As well as alerting you, it can automatically mitigate an attack, helping prevent malicious traffic from reaching your network. Our scale means that we can deal with even the largest attacks.
• Our PCI Compliance consultants have a wealth of industry knowledge, so they can appreciate your challenges and make recommendations about both IT and business process transformation, to help protect your POS environment.
• Our Application Vulnerability Scanning services are a software-as-a-service (SaaS) offering that enables you to identify vulnerabilities in web applications, before they’re exploited.

Download the full report, infographic, and other DBIR resources from verizonenterprise.com/DBIR/2014

verizonenterprise.com

© 2014 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. MC15934 4/14