Cooley

2016 Verizon Data Breach Investigations Report

May 4, 2016

On April 26, 2016, Verizon published its ninth annual Data Breach Investigations Report ("DBIR"), which looks at breach trends, common vulnerabilities, and categories of security incidents that affected organizations in 82 countries last year. The 2016 DBIR analyzes over 64,000 security incidents (events that compromised information's integrity, confidentiality or availability) and 2,260 data breaches (incidents that resulted in confirmed disclosure of data).

In 2015, more than 90% of incidents and data breaches fell into one of nine categories. Most commonly, security incidents were caused by miscellaneous errors, such as sending emails or paper documents to the wrong recipients (11,347 incidents); insider and privilege misuse, such as an employee using unapproved hardware like a USB drive to store sensitive information (10,490 incidents); and physical theft or loss of laptops and paper documents (9,701 incidents). The most serious incidents—those resulting in the most confirmed data breaches—however, were web app attacks, including hacking using stolen credentials and installing malware (908 confirmed breaches) and point of sale or "POS" attacks against environments where debit and credit card retail transactions are conducted (525 confirmed breaches).

2015 found attackers are getting faster at compromising their victims. For example, the time to compromise was almost always on the order of days or minutes. One particularly fast method of accessing sensitive data is phishing, which accounted for 9,576 security incidents and 916 confirmed data breaches in 2015. Phishing (a form of social engineering) involves sending an email message containing a malicious attachment or link to a victim with the intent of tricking him or her into opening the attachment or clicking on the link. In the majority of phishing cases, that click allows the attacker to install persistent malware on the victim's computer.

The DBIR analyzes several million results of phishing tests conducted by various information security vendors. Their findings show that we may be getting worse, not better, at recognizing phishing messages; the number of targets who opened the test phishing message rose by 7%, from 23% in 2014 to 30% last year, and about 12% of those who opened the message went further and clicked on the malicious attachment. The median time between sending a phishing message and the first click on its attachment? Under four minutes. In fairness to those who clicked, however, the DBIR notes that the main perpetrators of phishing attacks are sophisticated, with significant time and resources to craft believable "bait": in 2015, 89% of phishing attacks were perpetrated by organized crime syndicates and 9% were perpetrated by state-affiliated actors.

Insider and privilege misuse was also very common, with insiders most frequently motivated by financial gain, followed closely by espionage. The 2016 DBIR looked at how insiders' motivations have changed since 2009, and while incidents motivated by espionage have risen, incidents motivated by the prospect of financial gain have fallen. Other inside actors are motivated by grudges, ideology, and even just plain fun. Even more concerning, actions by insiders are some of the hardest for organizations and law enforcement to detect. In fact, 70% of these incidents are taking months or even years to discover.

The 2016 DBIR also shows that payment card data remains a popular target for attackers. POS intrusions accounted for 534 security incidents, almost all of which resulted in confirmed data breaches, last year. Businesses in the accommodation, food service and retail industries experienced most of these attacks, oftentimes after the attackers first compromised their POS vendors' security. Almost all (97%) of data breaches involving stolen credentials leveraged legitimate partner access to get to customer data.

Attackers also used physical devices to steal payment card information. Skimming devices physically implanted in magnetic payment card readers—for example, a pinhole camera installed on an ATM to surveil individuals entering debit card PINs—caused 102 security incidents in 2015. Of those, 86 resulted in confirmed data breaches. The vast majority (94%) of breaches involving payment card skimmers were related to ATMs, but attackers also targeted gas pump terminals (5% of breaches) and PIN entry devices (1%). In 2015, 70% of payment card skimming incidents were the work of criminal organizations.

Additional findings from this year's DBIR include:

- Industries hardest hit by data breaches include the finance, accommodation, information and retail industries, as well as the public sector;
- 63% of confirmed data breaches involved stolen, weak or default passwords;
- The vast majority of breaches perpetrated by hackers targeted well-known software bugs—the top 10 vulnerabilities accounted for 85% of successful exploit traffic; and
- 89% of breaches were motivated by the potential for financial gain or espionage.

If you would like to discuss Verizon's findings from the 2016 DBIR in greater detail or have any other cybersecurity or privacy questions, please don't hesitate to contact our Privacy & Data Protection practice group. We can provide you with additional information or insights, tailored to your or your organization's needs.

Key Contacts

Matthew D. Brown **San Francisco**	**brownmd@cooley.com** **+1 415 693 2188**
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090