

Verizon '2015 Data Breach Investigations Report' Finds Cyberthreats Are Increasing in Sophistication; Yet Many Cyberattacks Use Decades-Old Techniques
Wednesday, April 15, 2015 08:01:00 AM (GMT)

For First Time, Report Estimates Cost of a Breach; Confirms 9 Basic Patterns Make Up Vast Majority of Security Incidents

NEW YORK, April 15, 2015 /PRNewswire/ -- Verizon's "[2015 Data Breach Investigations Report](#)," released today, reveals that cyberattacks are becoming increasingly sophisticated, but that many criminals still rely on decades-old techniques such as phishing and hacking.

According to this year's report, the bulk of the cyberattacks (70 percent) use a combination of these techniques and involve a secondary victim, adding complexity to a breach.

Another troubling area singled out in this year's report is that many existing vulnerabilities remain open, primarily because security patches that have long been available were never implemented. In fact, many of the vulnerabilities are traced to 2007 – a gap of almost eight years.

As in prior reports, this year's findings again pointed out what Verizon researchers call the "detection deficit" – the time that elapses between a breach occurring until it's discovered. Sadly, in 60 percent of breaches, attackers are able to compromise an organization within minutes.

Yet the report points out that many cyberattacks could be prevented through a more vigilant approach to cybersecurity.

"We continue to see sizable gaps in how organizations defend themselves," said Mike Denning, vice president of global security for Verizon Enterprise Solutions. "While there is no guarantee against being breached, organizations can greatly manage their risk by becoming more vigilant in covering their bases. This continues to be a main theme, based on more than 10 years of data from our 'Data Breach Investigations Report' series."

This year's comprehensive report offers an in-depth look at the cybersecurity landscape, including a first-time overview of mobile security, Internet of Things technologies and the financial impact of a breach.

The report indicates that, in general, mobile threats are overblown. In addition, the overall number of exploited security vulnerabilities across all mobile platforms is negligible.

While machine-to-machine security breaches were not covered in the 2014 report, the 2015 report examines incidents in which connected devices are used as an entry point to compromise other systems. The report also examines the co-opting of IoT devices into botnets -- a network of private computers infected with malicious software and controlled without the owners' knowledge -- for denial-of-service attacks.

This data reaffirms the need for organizations to make security a high priority when rolling out next-generation intelligent devices.

Verizon Develops New Model for Estimating the Cost of a Breach

Verizon security analysts used a new assessment model for gauging the financial impact of a security breach, based on the analysis of nearly 200 cyberliability insurance claims. The model accounts for the fact that the cost of each stolen record is directly affected by the type of data and total number of records compromised, and shows a high and low range for the cost of a lost record (i.e. credit card number, medical health record).

For example, the model predicts that the cost of a breach involving 10 million records will fall between \$2.1 million and \$5.2 million (95 percent of the time), and depending on circumstances could range up to as much as \$73.9 million. For breaches with 100 million records, the cost will fall between \$5 million and \$15.6 million (95 percent of the time), and could top out at \$199 million.

"We believe this new model for estimating the cost of a breach is groundbreaking, although there is definitely still room for refinement," said Denning. "We now know that it's rarely, if ever, less expensive to

suffer a breach than to put the proper defense in place."

Nine Basic Patterns Make Up 96 Percent of Security Incidents

Verizon security researchers explained that the bulk (96 percent) of the nearly 80,000 security incidents analyzed this year can be traced to nine basic attack patterns that vary from industry to industry. This finding, first presented in last year's report, is again central to Verizon's "2015 Data Breach Investigations Report." This approach can help enterprises effectively prioritize their security efforts and establish a more focused and effective approach to fighting cyberthreats.

As identified in the 2014 DBIR, the nine threat patterns are: miscellaneous errors, such as sending an email to the wrong person; crimeware (various malware aimed at gaining control of systems); insider/privilege misuse; physical theft/loss; Web app attacks; denial-of-service attacks, cyberespionage; point-of-sale intrusions; and payment card skimmers.

This year's report found that 83 percent of security incidents by industry involve the top three threat patterns, up from 76 percent in 2014.

Enterprise Organizations Must Act Now

The longer it takes for an organization to discover a breach, the more time attackers have to penetrate its defenses and cause damage. In more than one quarter of all breaches, it takes the victim organization weeks, or even months, to contain the breaches.

This year's report is packed with detailed information and improvement recommendations based on seven common themes:

- The need for increased vigilance.
- Make people your first line of defense.
- Only keep data on a need-to-know basis.
- Patch promptly.
- Encrypt sensitive data.
- Use two-factor authentication.
- Don't forget physical security.

The Data Breach Investigations Report Series Is Based on Actual Caseloads

Now in its eighth year of publication, the "2015 Data Breach Investigation Report" analyzes more than 2,100 confirmed data breaches and approximately 80,000 reported security incidents in this year's report alone. The report addresses more than 8,000 breaches and nearly 195,000 security incidents that have occurred over more than 10 years. The DBIR also includes security incidents that don't result in breaches, in order to offer a better survey of the cybersecurity landscape. Verizon is among 70 global organizations that contributed data and analysis to this year's report.

Download the Report

The full "2015 Data Breach Investigations Report," high-resolution charts and additional resources supporting the research are available on the [DBIR Resource Center](#).

Verizon Delivers Unparalleled Managed Security Services

Verizon is a leader in delivering global managed security solutions to enterprises in the financial services, retail, government, technology, healthcare, manufacturing, energy and transportation sectors. Verizon combines powerful intelligence and analytics with an expansive breadth of professional and managed services, including customizable advanced security operations and managed threat protection services, next-generation commercial technology monitoring and analytics, rapid incident response and forensics investigations and identity management. Verizon brings the strength and expert knowledge of more than 550 consultants across the globe to proactively reduce security threats and lower information risks to organizations.

For more information, visit us at <http://www.verizonenterprise.com/solutions/security/>. For ongoing security insight and analysis from some of the world's most distinguished security researchers, read the [Verizon](#)

[Security Blog.](#)

Verizon Enterprise Solutions creates global connections that generate growth, drive business innovation and move society forward. With industry-specific solutions and a full range of global wholesale offerings provided over the company's secure mobility, cloud, strategic networking and advanced communications platforms, Verizon Enterprise Solutions helps open new opportunities around the world for innovation, investment and business transformation. Visit www.verizonenterprise.com to learn more.

Verizon Communications Inc. (NYSE, Nasdaq: VZ), headquartered in New York, is a global leader in delivering broadband and other wireless and wireline communications services to consumer, business, government and wholesale customers. Verizon Wireless operates America's most reliable wireless network, with more than 108 million retail connections nationwide. Verizon also provides converged communications, information and entertainment services over America's most advanced fiber-optic network, and delivers integrated business solutions to customers worldwide. A Dow 30 company with more than \$127 billion in 2014 revenues, Verizon employs a diverse workforce of 177,300. For more information, visit www.verizon.com/news/.

Verizon Enterprise Solutions Online News Center: News releases, blog posts, media contacts and other information are available in Verizon Enterprise Solutions' online News Center at <http://news.verizonenterprise.com>. News from Verizon Enterprise Solutions is also available through an RSS feed at <http://news.verizonenterprise.com/rss>.

To view the original version on PR Newswire, visit: <http://www.prnewswire.com/news-releases/verizon-2015-data-breach-investigations-report-finds-cyberthreats-are-increasing-in-sophistication-yet-many-cyberattacks-use-decades-old-techniques-300066005.html>

SOURCE Verizon

Contacts: Janet Brumfield, +1 614-560-2024, Janet.brumfield@verizon.com; Clare Ward, +44 118 905 3501, clare.ward@intl.verizon.com; Nilesh Pritam, +65 6248 6599, nilesh.pritam@intl.verizon.com

Countries: United States

Industries: Telecommunications, Computer Electronics, Hardware & Software, High Tech Security, Multimedia, Internet & Wireless Technology

Languages: English

Primary Identifiers: VZ-US

Related Identifiers: VZ-US