Large-Scale Financial Cybercrime, State-Affiliated Espionage Dominate Security Landscape, Finds 'Verizon 2013 Data Breach Investigations Report'
Tuesday, April 23, 2013 04:01:00 AM (GMT)

Report Offers New Insight Into Data Thieves and Their Motives; 'Understand Your Adversary' is Critical to Effective Defense and Response

NEW YORK, April 23, 2013 /PRNewswire/ -- The "Verizon 2013 Data Breach Investigations Report" reveals that large-scale financial cybercrime and state-affiliated espionage dominated the security landscape in 2012. Taking the top spot for all breaches in the 2013 report is financially motived cybercrime (75 percent), with state-affiliated espionage campaigns claiming the No. 2 spot (20 percent). Breaches in the No. 2 spot include cyberthreats aimed at stealing intellectual property -- such as classified information, trade secrets and technical resources -- to further national and economic interests.

The 2013 DBIR also found that the proportion of incidents involving hacktivists -- who act out of ideological motivations or even just for fun -- held steady; but the amount of data stolen decreased, as many hacktivists shifted to other methods such as distributed denial of service (DDoS) attacks. These attacks, aimed at paralyzing or disrupting systems, also have significant costs because they impair business and operations.

"The bottom line is that unfortunately, no organization is immune to a data breach in this day and age," said Wade Baker, principal author of the Data Breach Investigations Report series. "We have the tools today to combat cybercrime, but it's really all about selecting the right ones and using them in the right way.

"In other words, understand your adversary – know their motives and methods, and prepare your defenses accordingly and always keep your guard up," Baker said.

In 2012, victims represented a wide range of industries. Thirty-seven percent of breaches affected financial organizations, and 24 percent affected retailers and restaurants. Twenty percent of network intrusions involved the manufacturing, transportation and utilities industries, with the same percentage affecting information and professional services firms. Of all cyberattacks, 38 percent impacted larger organizations and represented 27 different countries.

"All in all, the large scale and diverse nature of data breaches and other network attacks took center stage for all to see in 2012," Baker said.

Now in its sixth year of publication, the 2013 data breach report includes 621 confirmed data breaches as well as more than 47,000 reported security incidents. Over the entire nine-year range of this study, that tally now exceeds 2,500 data breaches and 1.2 billion compromised records. Verizon is joined by 18 organizations from around the world that contributed data and analysis to this year's report.

"With more than a three-fold increase in data contributors this year, the '2013 Data Breach Investigations Report' offers what we believe is the most comprehensive look ever into the state of cybersecurity," said David Small, chief platform officer for Verizon Enterprise Solutions. "As always, our goal in producing the report is to increase the awareness of global cybercrime in an effort to improve the security industry's ability to fight it, while helping government agencies and private sector organizations develop their own tailored security plans."

Other Key Findings in the 2013 Data Breach Investigations Report

External attacks remain largely responsible for data breaches, with 92 percent of them attributable to outsiders and 14 percent committed by insiders. This category includes organized crime, activist groups, former employees, lone hackers and even organizations sponsored by foreign governments. As in the prior year's report, business partners were responsible for about 1 percent of data breaches.

In terms of attack methods, hacking is the No. 1 way breaches occur. In fact, hacking was a factor in 52 percent of data breaches. Seventy-six percent of network intrusions exploited weak or stolen credentials (user name/password); 40 percent incorporated malware (malicious software, script or code used to compromise information); 35 percent involved physical attacks (such as ATM skimming); and 29 percent

leveraged social tactics (such as phishing).

The proportion of breaches incorporating social tactics such as phishing was four times higher in 2012, which, according to the breach report, is directly related to the tactic's widespread use in targeted espionage campaigns.

Additionally, the compromise-to-discovery timeline continues to be measured in months and even years, as opposed to hours and days. Finally, third parties continue to detect the majority of breaches (69 percent).

(NOTE: Additional resources supporting the "2013 Data Breach Investigations Report" are available, including high-resolution charts. B-roll available upon request.)

The report can be downloaded in full at: *http://www.verizonenterprise.com/DBIR/2013/*. As in years past, the 2013 report includes recommendations that large and small organizations can implement to help safeguard their business.

Verizon Offers Comprehensive Security Solutions to Help Protect Enterprises

Verizon helps organizations protect their core asset: data. The company does this through a robust suite of managed security services and security consulting services -- including governance, risk and compliance solutions; identity and access management solutions; investigative response; data protection services; threat management services; and vulnerability management services -- delivered in the cloud or on premises in more than 50 countries. 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 at *securityblog.verizonbusiness.com*.

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 nearly 99 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 in more than 150 countries, including all of the Fortune 500. A Dow 30 company with nearly $116 billion in 2012 revenues, Verizon employs a diverse workforce of 181,900. For more information, visit *www.verizon.com*.

VERIZON'S ONLINE NEWS CENTER: Verizon news releases, executive speeches and biographies, media contacts, high-quality video and images, and other information are available at Verizon's online News Center at *newscenter.verizon.com*. The news releases are available through an RSS feed. To subscribe, visit *newscenter.verizon.com/corporate/feeds*.

SOURCE Verizon

Contacts: Janet Brumfield, 614-723-1060, janet.brumfield@verizon.com, Nilesh Pritam, +65 6248 6599, nilesh.pritam@intl.verizon.com, Clare Ward, +44 118 905 3501, clare.ward@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