2011 Was the Year of the 'Hacktivist,' According to the 'Verizon 2012 Data Breach Investigations Report'
Thursday, March 22, 2012 04:01:00 AM (GMT)

Attacks Are Increasingly Motivated by Political and Social Intent; Majority of Breaches Avoidable With Sound Security Measures

NEW YORK, March 22, 2012 /PRNewswire/ -- The "Verizon 2012 Data Breach Investigations Report" reveals the dramatic rise of "hacktivism" -- cyberhacking to advance political and social objectives.

In 2011, 58 percent of data stolen was attributed to hacktivism, according to the annual report released today from Verizon. The new trend contrasts sharply with the data-breach pattern of past several years, during which the majority of attacks were carried out by cybercriminals, whose primary motivation was financial gain.

Seventy-nine percent of attacks represented in the report were opportunistic. Of all attacks, 96 percent were not highly difficult, meaning they did not require advanced skills or extensive resources. Additionally, 97 percent of the attacks were avoidable, without the need for organizations to resort to difficult or expensive countermeasures. The report also contains recommendations that large and small organizations can implement to protect themselves.

Now in its fifth year of publication, the report spans 855 data breaches across 174 million stolen records – the second-highest data loss that the Verizon RISK (Research Investigations Solutions Knowledge) team has seen since it began collecting data in 2004. Verizon was joined by five partners that contributed data to this year's report: the United States Secret Service, the Dutch National High Tech Crime Unit, the Australian Federal Police, the Irish Reporting & Information Security Service and the Police Central e-Crime Unit of the London Metropolitan Police.

"With the participation of our law enforcement partners around the globe, the '2012 Data Breach Investigations Report' offers what we believe is the most comprehensive look ever into the state of cybersecurity," said Wade Baker, Verizon's director of risk intelligence. "Our goal 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."

The report findings reinforced the international nature of cybercrime. Breaches originated from 36 countries around the globe, an increase from 22 countries the year prior. Nearly 70 percent of breaches originated in Eastern Europe, with less than 25 percent originating in North America.

External attacks remain largely responsible for data breaches, with 98 percent of them attributable to outsiders. This group includes organized crime, activist groups, former employees, lone hackers and even organizations sponsored by foreign governments. With a rise in external attacks, the proportion of insider incidents declined again in this year's report, to 4 percent. Business partners were responsible for less than 1 percent of data breaches.

In terms of attack methods, hacking and malware have continued to increase. In fact, hacking was a factor in 81 percent of data breaches and in 99 percent of data lost. Malware also played a large part in data breaches; it appeared in 69 percent of breaches and 95 percent of compromised records. Hacking and malware are favored by external attackers, as these attack methods allow them to attack multiple victims at the same time from remote locations. Many hacking and malware tools are designed to be easy and simple for criminals to use.

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 (92 percent).

(NOTE: Additional resources supporting the "2012 Data Breach Investigations Report" are available, including high-resolution charts, B-roll available upon request.)

Key Findings of the 2012 Report

Data from the 2012 report also demonstrates that:

- **Industrial espionage revealed criminal interest in stealing trade secrets and gaining access to intellectual property.** This trend, while less frequent, has serious implications for the security of corporate data, especially if it accelerates.
- **External attacks increased**. Since hacktivism is a factor in more than half of the breaches, attacks are predominantly led by outsiders. Only 4 percent of attacks implicate internal employees.
- **Hacking and malware dominate**. The use of hacking and malware increased in conjunction with the rise in external attacks in 2011. Hacking appeared in 81 percent of breaches (compared with 50 percent in 2010), and malware appeared in 69 percent (compared with 49 percent in 2010). Hacking and malware offer outsiders an easy way to exploit security flaws and gain access to confidential data.
- **Personally identifiable information (PII) has become a jackpot for criminals** . PII, which can include a person's name, contact information and social security number, is increasingly becoming a choice target. In 2011, 95 percent of records lost included personal information, compared with only 1 percent in 2010.
- **Compliance does not equal security** . While compliance programs, such as the Payment Card Industry Data Security Standard, provide sound steps to increasing security, being PCI compliant does not make an organization immune from attacks.

"The report demonstrates that unfortunately, many organizations are still not getting the message about the steps they can take to prevent data breaches," said Baker. "This year, we have segmented our recommendations for enterprises and small businesses in the hope that this will make our suggestions more actionable. Additionally, we believe greater public awareness about cyberthreats and user education and training are vitally important in the fight against cybercrime."

Recommendations for Enterprises

1. **Eliminate unnecessary data.** Unless there is a compelling reason to store or transmit data, destroy it. Monitor all important data that must be kept.
2. **Establish essential security controls.** To effectively defend against a majority of data breaches, organizations must ensure fundamental and common sense security countermeasures are in place and that they are functioning correctly. Monitor security controls regularly.
3. **Place importance on event logs.** Monitor and mine event logs for suspicious activity – breaches are usually identified by analyzing event logs.
4. **Prioritize security strategy.** Enterprises should evaluate their threat landscape and use the findings to create a unique, prioritized security strategy.

Recommendations for Small Organizations

1. **Use a firewall.** Install and maintain a firewall on Internet-facing services to protect data. Hackers cannot steal what they cannot reach.
2. **Change default credentials**. Point-of-sale (POS) and other systems come with pre-set credentials. Change the credentials to prevent unauthorized access.
3. **Monitor third parties.** Third parties often manage firewalls and POS systems. Organizations should monitor these vendors to ensure they have implemented the above security recommendations, where applicable.

The DBIR can be downloaded in full at: *www.verizon.com/enterprise/2012dbir/us*

The Verizon 2012 DBIR will be available in seven languages. The initial report is in English, and translations will be available June 6 in French, German, Italian, Japanese, Spanish and Portuguese.

Verizon, through its Terremark subsidiary, helps organizations protect their core asset: data. The company does this through a robust suite of security 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. For more information, visit us at *verizonbusiness.com/products/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 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 108 million total 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 $111 billion in 2011 revenues, Verizon employs a diverse workforce of nearly 194,000. 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 News Center on the World Wide Web at *www.verizon.com/news*. To receive news releases by email, visit the News Center and register for customized automatic delivery of Verizon news releases.

SOURCE Verizon

Contacts: Brianna Carroll Boyle, +1-703-859-4251, brianna.boyle@verizon.com, Nilesh Pritam, +65-6248-6599, nilesh.pritam@sg.verizonbusiness.com, Clare Ward, +44-118-905-3501, clare.ward@uk.verizonbusiness.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