Verizon's 2016 Data Breach Investigations Report finds cybercriminals are exploiting human nature
Wednesday, April 27, 2016 07:00:00 AM (GMT)

NEW YORK, April 27, 2016 /PRNewswire/ -- Cybercriminals are continuing to exploit human nature as they rely on familiar attack patterns such as phishing, and increase their reliance on ransomware, where data is encrypted and a ransom is demanded, finds the Verizon 2016 Data Breach Investigations Report.

This year's report highlights repeating themes from prior year's findings and storylines that continue to play off of human nature, including:

- Eighty-nine (89) percent of all attacks involve financial or espionage motivations.
- Most attacks exploit known vulnerabilities that have never been patched despite patches being available for months, or even years. In fact, the top 10 known vulnerabilities accounted for 85 percent of successful exploits.
- Sixty-three (63) percent of confirmed data breaches involve using weak, default or stolen passwords.
- 95 percent of breaches and 86 percent of security incidents fall into nine patterns
- Ransomware attacks increased by 16 percent over 2015 findings.
- Basic defenses continue to be sorely lacking in many organizations.

"The Data Breach Investigations Report's increasing importance to businesses, law enforcement and governmental agencies demonstrates a strong desire to stay ahead of cybercrime," said Chris Formant, president of Verizon Enterprise Solutions. "Now more than ever, the collaboration and contributions evidenced in the DBIR from organizations across the globe are required to fully understand the threat landscape. And understanding is the first step toward addressing that threat."

Phishing tops the list of increasing concerns

One area that has picked up dramatically over the prior year is phishing i.e. where end users receive an email from a fraudulent source. Alarmingly, 30 percent of phishing messages were opened – up from 23 percent in the 2015 report – and 13 percent of those clicked to open the malicious attachment or nefarious link.

In prior years, phishing was only a leading attack pattern for cyber-espionage and has   now spread to seven of the nine incident patterns in the 2016 report. Its popularity has risen because it is an amazingly effective technique and offers attackers a number of advantages such as a very quick time to compromise and the ability to target specific individuals and organizations.

Adding to the list of human error are those caused by end users of an organization. 'Miscellaneous errors' take the No. 1 spot for security incidents in this year's report. These can include improper disposal of company information, misconfiguration of IT systems, and lost and stolen assets such as laptops and smartphones. In fact, 26 percent of these errors involve people mistakenly sending sensitive information to the wrong person.

"You might say our findings boil down to one common theme -- the human element," said Bryan Sartin, executive director of global security services, Verizon Enterprise Solutions. "Despite advances in information security research and cyber detection solutions and tools, we continue to see many of the same errors we've known about for more than a decade now. How do you reconcile that?"

Of increasing concern to Verizon's security researchers is the speed in which cybercrime is committed. In 93 percent of cases, it took attackers minutes or less to compromise systems and data exfiltration occurred within minutes in 28 percent of the cases.

As with the 2015 report, compromises of mobile and Internet of Things devices are not a significant factor in the 2016 DBIR. However, the report notes that proof of concept exploits are real and it's only a matter of time before a large scale breach impacts mobile and IoT devices, which means organizations should continue to be vigilant about protecting smartphones and IoT devices.

Also worth noting from the report is that Web application attacks climbed to the #1 spot for data breaches,

up 33 percent over prior year, and the vast majority (95 percent) were financially motivated.

The rise of the three-pronged attack

This year's report calls out the rise of a new three-pronged attack that is being repeated over and over again by cybercriminals. Many organizations are falling prey to this type of attack. The three-prongs are:

- Sending a phishing email with a link pointing to the malicious website, or a malicious attachment.
- Malware is downloaded onto an individual's PC that establishes the initial foothold, and additional malware can be used to look for secrets and internal information to steal (cyberespionage) or encrypt files for ransom. Many times the malware steals credentials to multiple applications through key logging.
- Use of the credentials for further attacks, for example, to log into third-party websites like banking or retail sites.

"The goal is to understand how the cybercriminals operate," said Sartin. "By knowing their patterns, we can best prevent, detect and respond to attacks."

2016 report reiterates the need for the basics

The researchers note that basic, well-executed measures continue to be more important than complex systems. Organizations should check to make sure they are taking care of these things:

- Know what attack patterns are most common for your industry.
- Utilize two-factor authentication for your systems and other applications, such as popular social networking sites.
- Patch promptly.
- Monitor all inputs: Review all logs to help identify malicious activity.
- Encrypt your data: If stolen devices are encrypted, it's much harder for attackers to access the data.
- Train your staff: Developing security awareness within your organization is critical especially with the rise in phishing attacks.
- Know your data and protect it accordingly. Also limit who has access to it.

"This year's report once again demonstrates that there is no such thing as an impenetrable system, but often times even a basic defense will deter cybercriminals who will move on to look for an easier target," added Sartin.

The Data Breach Investigations Report series Is based on actual caseloads

Now in its ninth year of publication, the "2016 Data Breach Investigations Report" analyzes more than 2,260 confirmed data breaches and more than 100,000 reported security incidents in this year's report – the highest since the report's inception in 2008. The report addresses more than 10,000 breaches and nearly 300,000 security incidents that have occurred over more than 11 years. The DBIR includes security incidents that don't result in breaches, in order to offer a better survey of the cybersecurity landscape. Verizon is among 67 global organizations that contributed data and analysis to this year's report.

Download the report

The full "2016 Data Breach Investigations Report," high-resolution charts and additional resources supporting the research are available on the DBIR Media 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, and 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 Communications Inc. (NYSE, Nasdaq: VZ), headquartered in New York City, generated nearly $132 billion in 2015 revenues. Verizon operates America's most reliable wireless network, with 112.6 million retail connections nationwide. The company also provides communications and entertainment services over America's most advanced fiber-optic network, and delivers integrated business solutions to customers worldwide.

VERIZON'S ONLINE NEWS CENTER: News releases, feature stories, executive biographies and media contacts are available at Verizon's online News Center at www.verizon.com/news/. News releases are also available through an RSS feed. To subscribe, visit www.verizon.com/about/rss-feeds/.

Verizon Enterprise Online News Room: News releases, blog posts, media contacts and other information are available at *Verizon Enterprise Solutions News & Insights* (news.verizonenterprise.com). News from Verizon Enterprise Solutions is also available through an RSS feed at http://www.verizonenterprise.com/rss-options/.

Media contacts:

Janet Brumfield
+1.614.582.9636
janet.brumfield@verizon.com
Twitter: janet_brumfield

Nilesh Pritam - APAC
+65.9277.9048
nilesh.pritam@intl.verizon.com
Twitter: @Nilesh_pritam

Clare Ward – EMEA
+44.118.905.3501
clare.ward@intl.verizon.com
Twitter: @ClareWSpeaks

To view the original version on PR Newswire, visit: http://www.prnewswire.com/news-releases/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-nature-300258134.html

SOURCE Verizon

Countries: United States
Industries: Telecommunications, Computer Electronics, Hardware & Software, High Tech Security
Languages: English
Primary Identifiers: VZ-US
Related Identifiers: VZ-US