Cyberespionage and ransomware attacks are on the increase warns the Verizon 2017 Data Breach Investigations Report
Thursday, April 27, 2017 04:01:00 AM (GMT)

Ransomware attacks gain greater popularity: now fifth most common specific malware variety

NEW YORK, April 27, 2017 /PRNewswire/ -- Cyberespionage is now the most common type of attack seen in manufacturing, the public sector and now education, warns the Verizon 2017 Data Breach Investigations Report. Much of this is due to the high proliferation of propriety research, prototypes and confidential personal data, which are hot-ticket items for cybercriminals. Nearly 2,000 breaches were analyzed in this year's report and more than 300 were espionage-related, many of which started life as phishing emails.

In addition, organized criminal groups escalated their use of ransomware to extort money from victims: this year's report sees a 50 percent increase in ransomware attacks compared to last year. Despite this increase and the related media coverage surrounding the use of ransomware, many organizations still rely on out-of-date security solutions and aren't investing in security precautions. In essence, they're opting to pay a ransom demand rather than to invest in security services that could mitigate against a cyberattack.

"Insights provided in the DBIR are leveling the cybersecurity playing field," said George Fischer, president of Verizon Enterprise Solutions. "Our data is giving governments and organizations the information they need to anticipate cyberattacks and more effectively mitigate cyber-risk. By analyzing data from our own security team and that of other leading security practitioners from around the world, we're able to offer valuable intelligence that can be used to transform an organization's risk profile."

This year's DBIR – the keystone report's 10th anniversary edition – combines up-to-date analysis of the biggest issues in cybersecurity with key industry-specific insights, putting security squarely on the business agenda. Major findings include:

- **Malware is big business**: Fifty-one (51) percent of data breaches analyzed involved malware. Ransomware rose to the fifth most common specific malware variety. Ransomware – using technology to extort money from victims - saw a 50 percent increase from last year's report, and a huge jump from the 2014 DBIR where it ranked 22 in the types of malware used.
- **Phishing is still a go-to technique**: In the 2016 DBIR, Verizon flagged the growing use of phishing techniques linked to software installation on a user's device. In this year's report, 95 percent of phishing attacks follow this process. Forty-three percent of data breaches utilized phishing, and the method is used in both cyber-espionage and financially motivated attacks.
- **Pretexting is on the rise**: Pretexting is another tactic on the increase, and the 2017 DBIR showed that it is predominantly targeted at financial department employees – the ones who hold the keys to money transfers. Email was the top communication vector, accounting for 88 percent of financial pretexting incidents, with phone communications in second place with just under 10 percent.
- **Smaller organizations are also a target:** Sixty-one (61) percent of victims analyzed were businesses with fewer than 1,000 employees.

"Cyber-attacks targeting the human factor are still a major issue," says Bryan Sartin, executive director, Global Security Services, Verizon Enterprise Solutions. "Cybercriminals concentrate on four key drivers of human behavior to encourage individuals to disclose information: eagerness, distraction, curiosity and uncertainty. And as our report shows, it is working, with a significant increase in both phishing and pretexting this year."

Business sector insights give real-life customer intelligence

This year's report provides tailored insights for key business sectors, revealing specific challenges faced by different verticals, and also answering the "who? what? why? and how?" for each. Key sector-specific findings include:

- The top three industries for data breaches are financial services (24 percent); healthcare (15 percent) and the public sector (12 percent).

- Companies in the manufacturing industry are the most common targets for email-based malware.
- Sixty-eight (68) percent of healthcare threat actors are internal to the organization.

"The cybercrime data for each industry varies dramatically," comments Sartin. "It is only by understanding the fundamental workings of each vertical that you can appreciate the cybersecurity challenges they face and recommend appropriate actions."

The most authoritative data-driven cybersecurity report around

Now in its tenth year, the "Verizon 2017 Data Breach Investigations Report" leverages the collective data from 65 organizations across the world. This year's report includes analysis on 42,068 incidents and 1,935 breaches from 84 countries. The DBIR series continues to be the most data-driven security publication with the largest amount of data sources combining towards a common goal – slicing through the fear, uncertainty and doubt around cybercrime.

"We started the DBIR series with one main contributor – ourselves," comments Sartin. "Our vision is to unite industries with the end goal of confronting cybercrime head-on– and we are achieving this. The success of the DBIR series is thanks to our contributors who support us year after year. Together we have broken down the barriers that used to surround cybercrime – developing trust and credibility. No organisation has to stand in silence against cybercrime – the knowledge is out there to be shared."

Get the basics in place

With 81 percent of hacking-related breaches leveraging either stolen passwords and/or weak or guessable passwords, getting the basics right is as important as ever before. Some recommendations for organizations and individuals alike include:

1. Stay vigilant - log files and change management systems can give you early warning of a breach.
2. Make people your first line of defense - train staff to spot the warning signs.
3. Keep data on a "need to know" basis - only employees that need access to systems to do their jobs should have it.
4. Patch promptly - this could guard against many attacks.
5. Encrypt sensitive data - make your data next to useless if it is stolen.
6. Use two-factor authentication - this can limit the damage that can be done with lost or stolen credentials.
7. Don't forget physical security - not all data theft happens online.

"Our report demonstrates that there is no such thing as an impenetrable system, but doing the basics well makes a real difference. Often, even a basic defense will deter cybercriminals who will move on to look for an easier target," concludes Sartin.

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, threat intel and response service 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

Verizon Communications Inc. (NYSE, Nasdaq: VZ), headquartered in New York City, has a diverse workforce of 161,000 and generated nearly $126 billion in 2016 revenues. Verizon operates America's most reliable wireless network, with 113.9 million retail connections nationwide. The company also provides communications and entertainment services over mobile broadband and the nation's premier all-fiber network, and delivers integrated business solutions to customers worldwide.

Media contacts:
Nil Pritam (APAC)
+65.6248.6599

nilesh.pritam@intl.verizon.com

Clare Ward (EMEA)
+44.118.905.3501
clare.ward@intl.verizon.com

Maria Montenegro (US)
312.894.2361
maria.montenegro@verizon.com

Related Links

http://www.verizon.com/
https://www.verizonwireless.com/
http://www.verizonenterprise.com/
http://www.verizon.com/about/

To view the original version on PR Newswire, visit: http://www.prnewswire.com/news-releases/cyberespionage-and-ransomware-attacks-are-on-the-increase-warns-the-verizon-2017-data-breach-investigations-report-300446807.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