Money still makes the cyber-crime world go round - Verizon Business 2020 Data Breach Investigations Report is live
Tuesday, May 19, 2020 04:01:10 AM (GMT)

What you need to know:

- 86 percent of data breaches for financial gain - up from 71 percent in 2019
- Cloud-based data under attack – web application attacks double to 43 percent
- 67 percent of breaches caused by credential theft, errors and social attacks
- Clearly identified cyber-breach pathways enable a "Defender Advantage" in the fight against cyber-crime
- On-going patching successful - fewer than 1 in 20 breaches exploit vulnerabilities
- Report analyzes 32,002 security incidents and 3,950 confirmed breaches from 81 global contributors from 81 countries

NEW YORK, May 19, 2020 (GLOBE NEWSWIRE) -- The Verizon Business 2020 Data Breach Investigations Report (2020 DBIR) shows that financial gain remains the key driver for cybercrime with nearly nine in 10 (86 percent) breaches investigated financially-driven. The vast majority of breaches continue to be caused by external actors - 70 percent - with organized crime accounting for 55 percent of these. Credential theft and social attacks such as phishing and business email compromises cause the majority of breaches (over 67 percent), and specifically:

- 37 percent of credential theft breaches used stolen or weak credentials,
- 25 percent involved phishing
- Human error accounted for 22 percent as well.

The 2020 DBIR also highlighted a year-over-year two-fold increase in web application breaches, to 43 percent, and stolen credentials were used in over 80 percent of these cases - a worrying trend as business-critical workflows continue to move to the cloud. Ransomware also saw a slight increase, found in 27 percent of malware incidents (compared to 24 percent in 2019 DBIR); 18 percent of organizations reported blocking at least one piece of ransomware last year.

"As remote working surges in the face of the global pandemic, end-to-end security from the cloud to employee laptop becomes paramount," said Tami Erwin, CEO, Verizon Business. "In addition to protecting their systems from attack, we urge all businesses to continue employee education as phishing schemes become increasingly sophisticated and malicious."

Common patterns offer a Defender Advantage

The 2020 DBIR has re-emphasized the common patterns found within cyber-attack journeys, enabling organizations to determine the bad actors' destination while they are in progress. Linked to the order of threat actions (e.g. Error, Malware, Physical, Hacking), these breach pathways can help predict the eventual breach target, enabling attacks to be stopped in their tracks. Organizations are therefore able to gain a "Defender's Advantage" and better understand where to focus their security defenses.

Smaller businesses are not immune

The growing number of small and medium-sized businesses using cloud- and web-based applications and tools has made them prime targets for cyber-attackers. 2020 DBIR findings show that:

- Phishing is the biggest threat for small organizations, accounting for over 30 percent of breaches. This is followed by the use of stolen credentials (27 percent) and password dumpers (16 percent).
- Attackers targeted credentials, personal data and other internal business-related data such as medical records, internal secrets or payment information.
- Over 20 percent of attacks were against web applications, and involved the use of stolen credentials.

Industries under the cyber-spotlight

The 2020 DBIR now includes detailed analysis of 16 industries, and shows that, while security remains a

challenge across the board, there are significant differences across verticals. For example, in Manufacturing, 23 percent of malware incidents involved ransomware, compared to 61 percent in the Public Sector and 80 percent in educational services. Errors accounted for 33 percent of Public Sector breaches - but only 12 percent of Manufacturing. Further highlights include:

- **Manufacturing:** External actors leveraging malware, such as password dumpers, app data capturers and downloaders to obtain proprietary data for financial gain, account for 29 percent of Manufacturing breaches.
- **Retail:** 99 percent of incidents were financially-motivated, with payment data and personal credentials continuing to be prized. Web applications, rather than Point of Sale (POS) devices, are now the main cause of Retail breaches.
- **Financial and Insurance:** 30 percent of breaches here were caused by web application attacks, primarily driven by external actors using stolen credentials to get access to sensitive data stored in the cloud. The move to online services is a key factor.
- **Educational Services:** Ransomware attacks doubled this year, accounting for approximately 80 percent of malware attacks vs. last year's 45 percent, and social engineering accounted for 27 percent of incidents.
- **Healthcare:** Basic human error accounted for 31 percent of Healthcare breaches, with external breaches at 51 percent (up from 42 percent in the 2019 DBIR), slightly more common than insiders at 48 percent (59 percent last year). This vertical remains the industry with the highest number of internal bad actors, due to greater access to credentials.
- **Public Sector:** Ransomware accounted for 61 percent of malware-based incidents. 33 percent of breaches are accidents caused by insiders. However, organizations have got much better at identifying breaches: only 6 percent lay undiscovered for a year compared with 47 percent previously, linked to legislative reporting requirements.

Regional trends

The 81 contributors involved with the 2020 DBIR have provided the report with specific insights into regional cyber-trends highlighting key similarities and differences between them. For example, financially-motivated breaches in general accounted for 91 percent of cases in Northern America, compared to 70 percent in Europe, Middle East and Africa and 63 percent in Asia Pacific. Other key findings include:

- **Northern America:** The technique most commonly leveraged was stolen credentials, accounting for over 79 percent of hacking breaches; 33 percent of breaches were associated with either phishing or pretexting.
- **Europe, Middle East and Africa (EMEA):** Denial of Service (DoS) attacks accounted for over 80 percent of malware incidents; 40 percent of breaches targeted web applications, using a combination of hacking techniques that leverage either stolen credentials or known vulnerabilities. Finally, 14 percent of breaches were associated with cyber-espionage.
- **Asia Pacific (APAC)**: 63 percent of breaches were financially-motivated, and phishing attacks are also high, at over 28 percent.

Alex Pinto, Lead Author of the Verizon Business Data Breach Investigations Report, comments: "Security headlines often talk about spying, or grudge attacks, as a key driver for cyber-crime - our data shows that is not the case. Financial gain continues to drive organized crime to exploit system vulnerabilities or human error. The good news is that there is a lot that organizations can do to protect themselves, including the ability to track common patterns within cyber-attack journeys - a security game changer - that puts control back into the hands of organizations around the globe."

About the DBIR

The 2020 DBIR – its 13th edition - analyzed 32,002 security incidents, of which 3,950 were confirmed breaches; almost double the 2,013 breaches analyzed last year. These cases came from 81 global contributors from 81 countries, and the analysis also now covers 16 business sectors.

The complete 2020 Data Breach Investigations Report as well as Executive Summary is available on the DBIR resource page.

The DBIR team invites its readership to provide feedback on the findings and analysis within this year's report. Any organization wishing to do so, or become a DBIR contributor should contact

dbir@verizon.com for further information.

Verizon Communications Inc. (NYSE, Nasdaq: VZ) was formed on June 30, 2000 and is celebrating its 20th year as one of the world's leading providers of technology, communications, information and entertainment products and services. Headquartered in New York City and with a presence around the world, Verizon generated revenues of $131.9 billion in 2019. The company offers voice, data and video services and solutions on its award winning networks and platforms, delivering on customers' demand for mobility, reliable network connectivity, security and control.

VERIZON'S ONLINE MEDIA CENTER: News releases, stories, media contacts and other resources are available at www.verizon.com/about/news/. News releases are also available through an RSS feed. To subscribe, visit www.verizon.com/about/rss-feeds/.

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

Najuma Thorpe (US)
+1.732.427.2304
najuma.thorpe@verizon.com

Primary Identifiers: VZ-US
Related Identifiers: VZ-US
Subjects: Company Announcement