C-Suite Beware: You are the latest targets of cybercrime, warns Verizon 2019 Data Breach Investigations Report
Wednesday, May 08, 2019 04:01:00 AM (GMT)

- C-level executives increasingly and proactively targeted by social breaches – correlating to a rise of social-engineering attacks with financial motivation.
- Compromise of web-based email accounts using stolen credentials (98 percent) rising -seen in 60 percent of attacks involving hacking a web application.
- One quarter of all breaches still associated with espionage.
- Ransomware attacks still strong, accounting for 24 percent of the malware incidents analyzed and ranking #2 in most-used malware varieties.
- 12th edition of the DBIR includes data from 73 contributors, the highest number since launch.
- Analyzes 41,686 security incidents, and 2,013 confirmed breaches from 86 countries.

NEW YORK, May 08, 2019 (GLOBE NEWSWIRE) -- C-level executives – who have access to a company's most sensitive information, are now the major focus for social engineering attacks, alerts the Verizon 2019 Data Breach Investigations Report. Senior executives are 12x more likely to be the target of social incidents, and 9x more likely to be the target of social breaches than in previous years – and financial motivation remains the key driver. Financially-motivated social engineering attacks (12 percent of all data breaches analyzed) are a key topic in this year's report, highlighting the critical need to ensure ALL levels of employees are made aware of the potential impact of cybercrime.

"Enterprises are increasingly using edge-based applications to deliver credible insights and experience. Supply chain data, video, and other critical – often personal – data WILL be assembled and analyzed at eye-blink speed, changing how applications utilize secure network capabilities" comments George Fischer, president of Verizon Global Enterprise. "Security must remain front and center when implementing these new applications and architectures.

"Technical IT hygiene and network security are table stakes when it comes to reducing risk. It all begins with understanding your risk posture and the threat landscape, so you can develop and action a solid plan to protect your business against the reality of cybercrime. Knowledge is power, and Verizon's DBIR offers organizations large and small a comprehensive overview of the cyber threat landscape today so they can quickly develop effective defense strategies."

A successful pretexting attack on senior executives can reap large dividends as a result of their - often unchallenged - approval authority, and privileged access into critical systems. Typically time-starved and under pressure to deliver, senior executives quickly review and click on emails prior to moving on to the next (or have assistants managing email on their behalf), making suspicious emails more likely to get through. The increasing success of social attacks such as business email compromises (BECs -which represent 370 incidents or 248 confirmed breaches of those analyzed), can be linked to the unhealthy combination of a stressful business environment combined with a lack of focused education on the risks of cybercrime.

This year's findings also highlight how the growing trend to share and store information within cost-effective cloud based solutions is exposing companies to additional security risks. Analysis found that there was a substantial shift towards compromise of cloud-based email accounts via the use of stolen credentials. In addition, publishing errors in the cloud are increasing year-over-year. Misconfiguration ("Miscellaneous Errors") led to a number of massive, cloud-based file storage breaches, exposing at least 60 million records analyzed in the DBIR dataset. This accounts for 21 percent of breaches caused by errors.

Bryan Sartin, executive director of security professional services at Verizon comments, "As businesses embrace new digital ways of working, many are unaware of the new security risks to which they may be exposed. They really need access to cyber detection tools to gain access to a daily view of their security posture, supported with statistics on the latest cyber threats. Security needs to be seen as a flexible and smart strategic asset that constantly delivers to the businesses, and impacts the bottom line."

Major findings in summary

The DBIR continues to deliver comprehensive data-driven analysis of the cyber threat landscape. Major findings of the 2019 report include:

- **New analysis from FBI Internet Crime Complaint Center (IC3):** Provides insightful analysis of the impact of Business Email Compromises (BECs) and Computer Data Breaches (CDBs). The findings highlight how BECs can be remedied. When the IC3 Recovery Asset Team acts upon BECs, and works with the destination bank, half of all US-based business email compromises had 99 percent of the money recovered or frozen; and only 9 percent had nothing recovered.
- **Attacks on Human Resource personnel have decreased from last year**: Findings saw 6x fewer Human Resource personnel being impacted this year compared to last, correlating with W-2 tax form scams almost disappearing from the DBIR dataset.
- **Chip and Pin payment technology has started delivering security dividends:** The number of physical terminal compromises in payment card related breaches is decreasing compared to web application compromises.
- **Ransomware attacks are still going strong:** They account for nearly 24 percent of incidents where malware was used. Ransomware has become so commonplace that it is less frequently mentioned in the specialized media unless there is a high profile target.
- **Media-hyped crypto-mining attacks were hardly existent:** These types of attacks were not listed in the top 10 malware varieties, and only accounted for roughly 2 percent of incidents.
- **Outsider threats remain dominant:** External threat actors are still the primary force behind attacks (69 percent of breaches) with insiders accounting for 34 percent.

Putting business sectors under the microscope

Once again, this year's report highlights the biggest threats faced by individual industries, and also offers guidance on what companies can do to mitigate against these risks.

"Every year we analyze data and alert companies as to the latest cybercriminal trends in order for them to refocus their security strategies and proactively protect their businesses from cyber threats. However, even though we see specific targets and attack locations change, ultimately the tactics used by the criminals remain the same. There is an urgent need for businesses – large and small – to put the security of their business and protection of customer data first. Often even basic security practices and common sense deter cybercrime," comments Sartin.

Industry findings of note include:

- **Educational Services:** There was a noticeable shift towards financially motivated crime (80 percent). 35 percent of all breaches were due to human error and approximately a quarter of breaches arose from web application attacks, most of which were attributable to the use of stolen credentials used to access cloud-based email.
- **Healthcare:** This business sector continues to be the only industry to show a greater number of insider compared to external attacks (60 versus 42 percent respectively). Unsurprisingly, medical data is 18x more likely to be compromised in this industry, and when an internal actor is involved, is it 14x more likely to be a medical professional such as a doctor or nurse.
- **Manufacturing:** For the second year in a row, financially motivated attacks outnumber cyber-espionage as the main reason for breaches in manufacturing, and this year by a more significant percentage (68 percent).
- **Public Sector:** Cyber-espionage rose this year - however, nearly 47 percent of breaches were only discovered years after the initial attack.
- **Retail:** Since 2015, Point of Sale (PoS) breaches have decreased by a factor of 10, while Web Application breaches are now 13x more likely.

(More findings on all individual industries may be located in the full report.)

More data from highest number of contributors ever means deeper insights

"We are privileged to include data from more contributors this year than ever before, and had the pleasure of welcoming the FBI into our fold for the very first time," adds Sartin. "We are able to provide the valuable insights from our DBIR research as a result of the participation of our renowned contributors. We would like to thank them all for their continued support and welcome other organizations from around the world to join us in our forthcoming editions."

This is the 12th edition of the DBIR and boosts the highest number of global contributors so far - 73 contributors since its launch in 2008. It contains analysis of 41,686 security incidents, which includes 2,013 confirmed breaches. With this increase of contributors Verizon saw a substantial increase of data to be analyzed, totaling approximately 1.5 billion data points of non-incident data.

This year's report also debuts new metrics and reasoning which helps identify which services are seen as the most lucrative for attackers to both scan for and attack at scale. This analysis is based on honeypot and internet scan data.

The complete Verizon 2019 Data Breach Investigations Report as well as Executive summary is available on the DBIR resource page. Any organization wishing to become a DBIR contributor should contact dbir@verizon.com for further information.

About Verizon's security services and solutions
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, generated revenues of $130.9 billion in 2018. The company operates America's most reliable wireless network and the nation's premier all-fiber network, and delivers integrated solutions to businesses worldwide. With brands like Yahoo, TechCrunch and HuffPost, the company's media group helps consumers stay informed and entertained, communicate and transact, while creating new ways for advertisers and partners to connect. Verizon's corporate responsibility prioritizes the environmental, social and governance issues most relevant to its business and impact to society.

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 contact:
Clare Ward
+44 118 9053501
clare.ward@uk.verizon.com

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