**Ransomware still a top cybersecurity threat, warns Verizon 2018 Data Breach Investigations Report**
**Tuesday, April 10, 2018 04:01:00 AM (GMT)**

*Ransomware attacks double since 2017, and now target business critical systems*

- Ransomware is the more prevalent variety of malicious software, found in 39 percent of malware-related cases.
- Human factor continues to be a weakness: financial pretexting and phishing attacks now target Human Resource (HR) departments.
- 11th edition of the DBIR includes data from 67 contributing organizations, with analysis on over 53,000 incidents and 2,216 breaches from 65 countries.

NEW YORK, April 10, 2018 (GLOBE NEWSWIRE) -- Ransomware attacks are a key cybersecurity threat for global organizations, warns Verizon's 2018 Data Breach Investigations Report (DBIR). Ransomware is the most common type of malware, found in 39 percent of malware-related data breaches – double that of last year's DBIR – and accounts for over 700 incidents. What's more, Verizon's analysis show that attacks are now moving into business critical systems, which encrypt file servers or databases, inflicting more damage and commanding bigger ransom requests.

DBIR analysis also flags a shift in how social attacks, such as financial pretexting and phishing, are used. Attacks such as these, which continue to infiltrate organizations via employees, are now increasingly a departmental issue. Analysis shows that Human Resource (HR) departments across multiple verticals are now being targeted in a bid to extract employee wage and tax data, so criminals can commit tax fraud and divert tax rebates.

"Businesses find it difficult to keep abreast of the threat landscape, and continue to put themselves at risk by not adopting dynamic and proactive security strategies," says George Fischer, president of Verizon Enterprise Solutions. "Verizon gives businesses data-driven, real-life views on the cyber-threat landscape, not only through the DBIR series but also via our comprehensive range of intelligent security solutions and services. This 11th edition of the DBIR gives in-depth information and analysis on what's really going on in cybercrime, helping organizations to make intelligent decisions on how best to protect themselves."

## Major findings in summary

The 11th edition of the DBIR continues to deliver comprehensive data-driven analysis of the cyber threat landscape. Major findings of the 2018 report include:

- **Ransomware is the most prevalent variety of malicious software** : It was found in 39 percent of malware-related cases examined this year, moving up from fourth place in the 2017 DBIR (and 22nd in 2014). Most importantly, based on Verizon's dataset it has started to impact business critical systems rather than just desktops. This is leading to bigger ransom demands, making the life of a cybercriminal more profitable with less work.
- **The human factor continues to be a key weakness:** Employees are still falling victim to social attacks. Financial pretexting and phishing represent 98 percent of social incidents and 93 percent of all breaches investigated – with email continuing to be the main entry point (96 percent of cases). Companies are nearly three times more likely to get breached by social attacks than via actual vulnerabilities, emphasizing the need for ongoing employee cybersecurity education.
- **Financial pretexting targets HR:** Pretexting incidents have increased over five times since the 2017 DBIR, with 170 incidents analyzed this year (compared to just 61 incidents in the 2017 DBIR). Eighty eight of these incidents specifically targeted HR staff to obtain personal data for the filing of file fraudulent tax returns.
- **Phishing attacks cannot be ignored:** While on average 78 percent of people did not fail a phishing test last year, 4 percent of people do for any given phishing campaign. A cybercriminal only needs one victim to get access into an organization.
- **DDoS attacks are everywhere:** DDoS attacks can impact anyone and are often used as camouflage, often being started, stopped and restarted to hide other breaches in progress. They are powerful, but also manageable if the correct DDoS mitigation strategy is in place.

- **Most attackers are outsiders:** One breach can have multiple attackers and we found the following: 72 percent of attacks were perpetrated by outsiders, 27 percent involved internal actors, 2 percent involved partners and 2 percent feature multiple partners. Organized crime groups still account for 50 percent of the attacks analyzed**.**

"Ransomware remains a significant threat for companies of all sizes," says Bryan Sartin, executive director security professional services, Verizon. "It is now the most prevalent form of malware, and its use has increased significantly over recent years. What is interesting to us is that businesses are still not investing in appropriate security strategies to combat ransomware, meaning they end up with no option but to pay the ransom – the cybercriminal is the only winner here! As an industry, we have to help our customers take a more proactive approach to their security. Helping them to understand the threats they face is the first step to putting in place solutions to protect themselves."

Sartin continued: "Companies also need to continue to invest in employee education about cybercrime and the detrimental effect a breach can have on brand, reputation and the bottom line. Employees should be a business's first line of defense, rather than the weakest link in the security chain. Ongoing training and education programs are essential. It only takes one person to click on a phishing email to expose an entire organization."

**Biggest risks per industries analyzed**

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. Key industry findings include:

- **Education** – Social engineering targeting personal information is high, which is then used for identity fraud. Highly sensitive research is also at risk, with 20 percent of attacks motivated by espionage. Eleven percent of attacks also have "fun" as the motive rather than financial gain.
- **Financial and insurance** – Payment card skimmers installed on ATMs are still big business; however, we're also now seeing a rise in "ATM jackpotting," where fraudulently installed software or hardware instructs the ATMs to release large amounts of cash. DDoS attacks are also a threat.
- **Healthcare** – This is the only industry where insider threats are greater than threats from the outside. Human error remains a major contributor to healthcare risks.
- **Information**[1] – DDoS attacks account for over half (56 percent) of the incidents within this sector.
- **Public sector** – Cyber-espionage remains a major concern, with 43 percent of breaches being espionage motivated. However, it is not only state-secrets that are a target - personal data is also at risk.

Other industries examined within the report include accommodation and food services; professional, technical and scientific services; and manufacturing and retail.

_____

[1] Publishers, motion picture and sound recording companies

**The time to act is NOW**

Sixty-eight percent of breaches took months or longer to discover, even though 87 percent of the breaches examined had data compromised within minutes or less of the attack taking place. While safety cannot be guaranteed, proactive steps can be taken to help keep organizations from being victims. These are:

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.

**Still the most authoritative data-driven cybersecurity report around**

Now in its 11th year, the Verizon 2018 Data Breach Investigations Report leverages collective data from 67 organizations across the world. This year's report includes analysis on 53,000 incidents and 2,216 breaches from 65 countries. The DBIR series continues to be one of the most data-driven security publications on the globe, combining data from multiple sources towards a common goal – slicing through the fear, uncertainty and doubt around cybercrime.

Verizon will be showcasing its latest intelligent security solutions, including the recently launched Verizon Risk Report, at RSA 2018 in San Francisco, Moscone North Hall, booth #4121.

**About Verizon**
Verizon Communications Inc. (NYSE:VZ) (Nasdaq:VZ), headquartered in New York City, generated $126 billion in 2017 revenues. The company operates America's most reliable wireless network and the nation's premier all-fiber network, and delivers integrated solutions to businesses worldwide. Its Oath subsidiary reaches about one billion people around the world with a dynamic house of media and technology brands.

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/.


**Verizon global 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**

Jennifer Banks (US)
+1.908.208.8483
**jennifer.banks@verizon.com**


**Primary Identifiers:** VZ-US
**Related Identifiers:** VZ-US
**Subjects:** Calendar of Events, Product / Services Announcement