proofpoint.

June 6, 2017

Proofpoint's Annual Human Factor Cybersecurity Report Details Ransomware, BEC, Phishing, and Mobile Threat Trends

Highly personalized, targeted cyberattacks focus on exploiting people, not just their technology

SUNNYVALE, Calif., June 06, 2017 (GLOBE NEWSWIRE) -- Proofpoint, Inc., (NASDAQ:PFPT), a leading next-generation security and compliance company, today announced its annual Human Factor report findings, which detail that cyberattackers are relying more than ever on exploiting people instead of software flaws to install malware, steal credentials/confidential information, and transfer funds. The report, based on analysis of attack attempts across more than 5,000 worldwide enterprise customers throughout 2016, provides a deep dive into attack trends across email, mobile, and social media communication channels to help organizations and users stay safe.

"Accelerating a shift that began in 2015, cybercriminals are aggressively using attacks that depend on clicks by humans rather than vulnerable software exploits—tricking victims into carrying out the attack themselves," said Kevin Epstein, vice president of Proofpoint's Threat Operations Center. "It's critical that organizations deploy advanced protection that stops attackers before they have a chance to reach potential victims. The earlier in the attack chain you can detect malicious content, the easier it is to block, contain, and resolve."

Proofpoint's Human Factor key findings include:

- **Business email compromise (BEC) attack message volume rose from 1% in 2015 to 42% by the end of 2016 relative to emails bearing banking Trojans.** BEC attacks, which have cost organizations more than $5 billion worldwide, use malware-free messages to trick recipients into sending confidential information or funds to cybercriminals. BEC is the fastest growing category of email-based attacks.

- **Someone will always click—and fast.** Nearly 90% of clicks on malicious URLs occur within the first 24 hours of delivery with 25% of those occurring in just ten minutes, and nearly 50% of clicks occur within an hour. The median time-to-click (the time between arrival and click) is shortest during business hours from 8 a.m. to 3 p.m. EDT in the U.S. and Canada, a pattern that generally holds for the U.K. and Europe as well.

- **More than 90% of malicious email messages that featured nefarious URLs led users to credential phishing pages.** And a full 99% of email-based financial fraud attacks relied on human clicks rather than automated exploits to install malware. Phishing messages designed to steal Apple IDs were the most sent, but Google Drive phishing links were the most clicked.

- **Half of the clicks on malicious URLs occur on devices that are outside the purview of enterprise desktop management.** Forty-two percent of clicks on malicious URLs were made from mobile devices, double the long-running rate of 20%. And 8% of clicks occur on potentially vulnerable versions of Windows for which security patches are no longer available.

- **Social media fraudulent support account phishing increased 150% in 2016.** During these attacks cybercriminals create a lookalike social media account posing as the customer service account of a trusted brand. When someone tweets to a company looking for help, the attacker swoops in.

- **Watch your inbox closely on Thursdays.** Malicious email attachment message volume spikes more than 38% on Thursdays over the average weekday volume. Ransomware attackers in particular favor sending malicious messages Tuesday through Thursday. On the other hand, Wednesday is the peak day for banking Trojans. Point-of-sale (POS) campaigns are sent almost exclusively on Thursday and Friday, while keyloggers and backdoors favor Mondays.

- **Attackers understand email habits and send most email messages in the 4-5 hours after the start of the business day, peaking around lunchtime.** Users in the U.S., Canada, and Australia tend to do most of their clicking during this time period, while French clicking peaks around 1 p.m. Swiss and German users don't wait for lunch to click; their clicks peak in the first hours of the working day. U.K. workers pace their clicking evenly over the course of the day, with a clear drop in activity after 2 p.m.

To download Proofpoint's Human Factor report, please visit www.proofpoint.com/humanfactor.

An infographic accompanying this release is available at http://www.globenewswire.com/NewsRoom/AttachmentNg/497f1cc0-a7b0-418d-9f0e-ba1eaa216a80

About Proofpoint, Inc.
Proofpoint Inc. (NASDAQ:PFPT) is a leading next-generation security and compliance company that provides cloud-based solutions to protect the way people work today. Proofpoint solutions enable organizations to protect their users from advanced attacks delivered via email, social media and mobile apps, protect the information their users create from advanced attacks and compliance risks, and respond quickly when incidents occur. More information is available at www.proofpoint.com.

Connect with Proofpoint: Twitter | LinkedIn | Facebook | YouTube | Google+

MEDIA CONTACT:

Patricia Hogan

Proofpoint, Inc.

(408) 763-3863

phogan@proofpoint.com

Primary Logo

Source: Proofpoint, Inc.

News Provided by Acquire Media