proofpoint

March 23, 2017

Business Email Compromise (BEC) Attacks Increase 45 Percent, 2/3 Use Spoofed Email Domains to Trick Victims

Cybersecurity leader Proofpoint enhances its comprehensive multi-layer BEC protection with integrated Email Fraud Defense authentication

SUNNYVALE, Calif., March 23, 2017 (GLOBE NEWSWIRE) -- Proofpoint, Inc., (NASDAQ:PFPT), a leading next-generation security and compliance company, today released new research into business email compromise (BEC) attacks which indicates an acceleration in their sophistication and velocity. Overall BEC attacks increased by 45 percent in the last three months of 2016 compared to prior months based on Proofpoint's extensive research into attack attempts across more than 5,000 enterprise customers. To help organizations combat BEC threats, Proofpoint recently enhanced its comprehensive BEC protection with Proofpoint Email Fraud Defense to ensure organizations can authenticate their email, as well as Proofpoint Digital Risk Defense's Web Discover module to proactively identify lookalike domains.

BEC attacks, which have cost organizations billions of dollars [(1)], put every email-based relationship at risk. During an attack, cybercriminals pretend to be a company executive and send highly-targeted emails to employees to trick recipients into wiring money or sending sensitive information. Proofpoint is the only company that provides the multi-layered approach needed to protect organizations from all forms of BEC attacks.

"Seventy-five percent of our customers were hit with at least one attempted BEC attack in the last three months of 2016—and it only takes one to cause significant damage," said Ryan Kalember, senior vice president of Cybersecurity Strategy for Proofpoint. "Our research shows static policies cannot keep up as attackers are constantly changing their socially-engineered messages. Organizations need detection, authentication, visibility, and data loss prevention to ensure they don't fall victim."

Proofpoint's extensive research into BEC attack attempts across more than 5,000 enterprise customers between July-December 2016 (including U.S., Canadian, UK, German, French, and Australian organizations) confirms cybercriminals are using social engineering to target and exploit victims. Below are key Proofpoint findings:

- **BEC attacks increased by 45 percent in the last three months of 2016 vs. the prior three months. 2/3 of all BEC attacks spoofed their email address domain** so that their fraudulent emails displayed the same domain as that of the company targeted in the attack.
- **Companies of all sizes are prone to BEC attacks.** Proofpoint data indicates no correlation between the size of the company and BEC attack volume. Larger companies make for attractive targets because they have more funds to draw on and greater organizational complexity to hide behind, even if they tend to have stricter financial controls. And while smaller companies may not yield the same returns, the relative absence of financial controls makes them more vulnerable.
- **Manufacturing, retail and technology organizations are generally more targeted with BEC attacks.** Hit repeatedly every month, cybercriminals look to take advantage of more complex supply chains and SaaS infrastructures which often accompany these industries.
- **While CEO impersonation continues in BEC attacks, cybercriminals are increasingly targeting victims deeper within organizations.** There is a shift beyond simple fraudulent CEO-to-CFO BEC attacks to CEO-to-different employee groups. For example, to accounts payable for wire transfer fraud attempts, to human resources for confidential tax information and identities—and engineering for intellectual property theft.
- **More than 70 percent of the most common BEC subject line families feature the words "Urgent" "Payment" and "Request."** The top seven subject line families include: payment (30 percent), request (21 percent), urgent (21 percent), greeting (12 percent), blank (nine percent), FYI (five percent), and, where are you? (two percent).

Proofpoint's Email Fraud Defense solution protects organizations from attacks spoofing trusted domains by using the power of email authentication. Featuring a DMARC (Domain-based Message Authentication Reporting & Conformance) reporting interface combined with the guidance of a world class team of authentication experts, Email Fraud Defense helps

organizations identify, authorize, configure and authenticate all legitimate email traffic, so that security teams can implement policies to block abuse of their domains.

Email Fraud Defense is also part of Proofpoint's comprehensive multi-layer BEC protection solution, which includes policy and dynamic classification through Proofpoint Email Protection, data loss prevention with Proofpoint Email DLP, and proactive lookalike domain detection via Proofpoint Digital Risk Defense.

For more information on Proofpoint BEC protection, please visit www.proofpoint.com/bec. And for more information about Proofpoint Email Fraud Defense, please visit https://www.proofpoint.com/us/products/email-fraud-defense.

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+

(1) FBI. "Business Email Compromise: The 3.1 Billion Dollar Scam." June 2016.

Media Contact:

Kristy Campbell

Proofpoint, Inc.

(408) 517-4710

kcampbell@proofpoint.com

Primary Logo

Source: Proofpoint, Inc.

News Provided by Acquire Media