proofpoint.

BUSINESS EMAIL COMPROMISE THREAT UPDATE Q1 2017

KEY TAKEAWAYS

- **BEC is a massive problem.** Nearly 85% of organizations were targeted in the first quarter of 2017.
- **All companies are at risk of BEC attacks.** These attacks target companies of every size across all industry verticals. We found no correlation between the size of the organization and how often they received BEC emails.
- **Cyber criminals are becoming more sophisticated.** Attackers are targeting different assets—not just money. At the same time, they are finding new ways to hide from security systems and persuade victims to send money and sensitive information.

Business email compromise (BEC) is one of today's greatest cyber threats. These attacks—which involve fraudsters posing as an executive or colleague to trick companies into sending money or sensitive information—have cost victims $5.3 billion since the FBI began tracking it in 2013.

Unlike most cyber attacks, BEC doesn't exploit technical vulnerabilities or use malware. Instead, it targets people directly, preying on human trust to hurt employees, business partners, and customers around the world.

To understand the scope and impact of this growing challenge, Proofpoint examined BEC attacks across customers in the first quarter of 2017.

BEC IS ON THE RISE, AND ALL ORGANIZATIONS ARE POTENTIAL TARGETS

The number of BEC threats continues to grow. In the first quarter of 2017, 84.8% of organizations were targeted with at least one malicious message. That's an increase of nearly 10% over the previous quarter. These threats have consistently targeted companies of all sizes and in all geographies.

While all industry verticals are at risk, some are more frequent targets. Industries that rely more heavily on software-as-a-service apps (such as technology companies) and those with more complex supply chains (such as manufacturing), saw more than 40 BEC attempts per organization on average.

ATTACKERS CONSTANTLY SHIFT THEIR APPROACH

BEC attacks are always changing—both what attackers want and how they get it.

Shifting aims

Wire fraud continues to be the most common form of BEC. Among BEC emails sent, 27% of subject lines referenced the need for a payment of some sort to be made.

So-called W2 scams, in which attackers request employee tax information to steal victims' identities, still account for a small percentage of total BEC attacks. But we saw a 3,408% spike in W2 attacks vs. the previous quarter as the U.S. tax-filing deadline approached.

Evolving techniques

While many impostor emails use bland subject lines to hide from security tools, others try to convey urgency so that recipients will react quickly—before they have a chance to question the request. And to add an extra sheen of credibility, 8% of BEC emails included a fabricated conversation history leading up to the attacker's request.

OVER HALF OF ALL BEC ATTACKS USE DOMAIN-SPOOFING TECHNIQUES

Among all BEC attacks, 54% spoofed the domain of the organization they were seeking to exploit. This technique make the impostor BEC email look as if it is coming from within the organization.

Display-name spoofing, in which the attacker uses "header from" name of someone within the organization, appeared in 45% of BEC emails. We also saw lookalike domain spoofing. In this approach, the attacker uses a domain that can be confused with the organization's real domain at first glance. It may use the numeral 1 in place of a lowercase "l," for instance, or transpose letters of the real domain. We also saw more business-partner spoofing techniques, where criminals impersonate partners and other trusted third parties.

Many BEC attackers use consumer webmail services because they're free, fast, and anonymous. Gmail was the most popular email service, appearing as the "Reply-to" and "From" address domain in about a third BEC attacks. AOL was close behind at 30%, and mail.com was third at 16%.

BEC BY SUBJECT HEADER CATEGORY

Subject category	2016-Q3	2016-Q4	2017-Q1
Payment	28.63%	25.08%	27.36%
Request	21.24%	17.40%	19.98%
Urgent	16.28%	19.03%	16.81%
Greeting	9.98%	10.65%	7.34%
Blank	4.55%	7.26%	7.28%
W2	0.20%	0.12%	4.21%
FYI	2.42%	5.07%	2.43%
Where are you?	1.77%	2.14%	1.65%
Document	0.38%	1.45%	1.08%
Date	1.73%	1.23%	0.61%
Legal	0.06%	0.02%	0.26%
Confidential	0.20%	0.13%	0.13%
Tax	0.01%	0.02%	0.11%
Other	12.56%	10.42%	10.75%

CYBERCRIMINALS ARE GROWING MORE SOPHISTICATED IN TARGETING PEOPLE

BEC has traditionally targeted company CFOs by posing as the CEO. But attackers are widening their nets, targeting and posing as other types of workers. Cyber criminals are spoofing more executives with authority and targeting employees deeper in the organization and across more departments.

Of the organizations targeted in Q1, 72% saw more than one person's identity spoofed. Attackers spoofed four people per organization on average. At the same time, the average number of people targeted has risen 50% over the past six months to 12.

CONCLUSION AND RECOMMENDATIONS

BEC attacks are more pervasive and sophisticated than ever. Cyber criminals are adapting their tactics to circumvent outdated technologies and exploit vulnerable processes and people.
To stop these attacks before they reach their targets, security strategies must fundamentally change. Organizations need a multi-layered solution that includes:

- Domain Message Authentication Reporting & Conformance (DMARC) email authentication. This framework blocks all BEC attacks that spoof your trusted domains and target employees and business partners.
- Dynamic classification. This capability stops display-name and lookalike-domain spoofing at the email gateway.
- Data loss prevention. This capability prevents sensitive information, such as W2s, from leaving the organization.

To learn how Proofpoint can help you stop BEC attacks, visit proofpoint.com/bec

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organizations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organizations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.

©Proofpoint, Inc. Proofpoint is a trademark of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are property of their respective owners.