REPORT

proofpoint®

EMAIL FRAUD THREAT REPORT

Q3 2017

proofpoint.com

EMAIL FRAUD THREAT REPORT Q3 2017

Email fraud—also known as business email compromise (BEC)—is one of today's largest cyber threats. These socially engineered attacks seek to exploit people rather than technology. They impersonate people in authority. By preying on human nature, and workers' eagerness to please, they steal money and valuable information from employees, customers, and partners.

According to the FBI, email fraud is costing victims billions of dollars.[1]

To better understand this ever-evolving threat, Proofpoint analyzes email fraud attacks against thousands of organizations around the globe. Here are our findings for Q3 2017.

ORGANIZATIONS ARE UNDER ATTACK MORE THAN EVER

Email Fraud continues to be growing problem and targets organizations of all shapes and sizes

The number of email fraud threats rose in the third quarter of 2017. More of these malicious emails being sent, and organizations are being targeted more frequently. The average number of targeted attempts per organization increased 12% over the previous quarter. And 49% of companies were targeted with more than 10 email fraud messages.

Attackers target companies of all size and in all geographies. That was still the case in Q3. We found no statistical correlation between the size of a company and how frequently it is targeted by email fraud.

All industries are at risk. But organizations with more complex supply chains (such as manufacturing) and those that rely more heavily on software as a service (such as tech) are targeted more often.

ATTACKERS ARE GROWING MORE SOPHISTICATED

Email fraud is always changing, but some aspects have proven remarkably constant. Subject categories on fraudulent email change little from one quarter to the next, for example. Likewise, wire fraud endures as the most frequent form of email fraud. Nearly one in every three (29%) email fraud message includes some variation of "payment" in the subject line.

Still, attackers' approach continuously evolves. That's because attackers are finding new ways to deceive security technology and the people who rely on it.

This quarter, subject lines that included "request" rose 43% over the previous quarter. Subject lines with "urgent" fell by 21% in the same period. The change suggests that attackers are trying to appeal a range of personality types. This approach is consistent with the highly-targeted nature of these threats.

Another clever tactic that we have seen in recent quarters is to end the email with a fake email history, a fabricated chain of back-and-forth replies. This fictional backstory gives the email a veneer of authenticity and spurs the victim to act. In Q3, about 9.5% of all email fraud messages included a fake email chain in Q3, which is consistent with the previous quarter.

BEC BY SUBJECT HEADER CATEGORY

Subject category	2016-Q4	2017-Q1	2017-Q3
Payment	25.08%	27.36%	28.75%
Request	17.40%	19.98%	21.50%
Urgent	19.03%	16.81%	15.52%
Greeting	10.65%	7.34%	7.66%
Blank	7.26%	7.28%	10.02%
W2	0.12%	4.21%	0.06%
FYI	5.07%	2.43%	1.26%
Where are you?	2.14%	1.65%	2.46%
Document	1.45%	1.08%	0.48%
Date	1.23%	0.61%	0.42%
Legal	0.02%	0.26%	0.16%
Confidential	0.13%	0.13%	0.18%
Tax	0.02%	0.11%	0.02%
Other	10.42%	10.75%	11.52%

1 FBI. "Business E-Mail Compromise/E-Mail Account Compromise: The 5 Billion Dollar Scam." May 2017.

ATTACKERS ARE EXPANDING THEIR REACH WITHIN TARGETED ORGANIZATIONS

The number of people spoofed within each targeted organization leveled off at about five. Just over half of companies saw between two and five spoofed identities. This consistently low number makes sense; only so many people within an organization have the authority to request wire transfers and sensitive information.

Still, the number of people targeted within each organization continues to rise. One-to-one "whaling" attacks are common (such as someone spoofing the CEO in a fraudulent message to the CFO). But cyber criminals are expanding their reach and targeting more people within organizations.

About 73% of organizations had multiple identities spoofed and more than one employee targeted. (We call these "some-to-many" attacks.)

The average number of people targeted per organization grew 28%. And most attacks targeted multiple people within an organization. Only 15% of companies saw just one person targeted by email fraud in Q3. That's down from 17% in the previous quarter.

DOMAIN SPOOFING ATTACKS EXPAND THEIR FOOTPRINT

Domain spoofing, where an attacker hijacks a trusted email domain to commit email fraud, accounts for many email fraud attacks. These can be stopped cold by deploying DMARC (Domain Message Authentication Reporting & Conformance) email authentication. Still, the number of domain spoofing attacks grew 5%. About 89% of organizations were targeted by at least one of these malicious emails in the quarter. That's up from 87% in the previous quarter.

U.S. AGENCIES FALLING FAR SHORT OF FEDERAL MANDATES

Shortly after the end of the quarter, the U.S. Department of Homeland Security directed all civilian federal agencies to implement SPF (Sender Policy Framework) and DMARC (Domain-based Message Authentication, Reporting & Conformance) authentication in 2018. The rules are part of Binding Operational Directive 18-01.

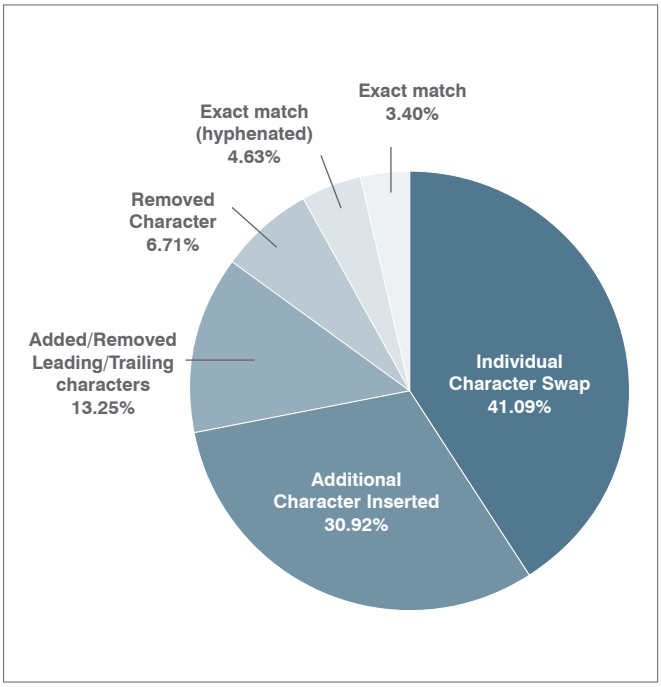
Authentication is crucial. Nearly 1 in every 8 emails sent from a federal agency is fraudulent. But only 17% of the agency's domains have deployed both SPF and DMARC. Of the 133 agencies identified as part of the DHS mandate, 100 do not have any DMARC policies published yet.

CHARACTER SWAPPING LEADS LOOKALIKE DOMAIN TECHNIQUES

Lookalike domains— in which attackers register a domain that's confusingly similar to the real one—is another leading spoofing technique. This tactic is also known as typosquatting.

Swapping characters is the most common technique, at about 41% of all lookalike domains. Among these, switching an "I" for a lowercase "L" was the most popular form, occurring more than 19% of the time. Exchanging a "U" for a "V" appeared next most frequently at 9.5% of the time. Changing an "O" with the numeral "0" followed at nearly 9% of the time.

Inserting an additional character occurred in almost 31% of lookalike domains. An "I" is inserted as an additional character most frequently for these types of lookalike domains, occurring 26% of the time. Other common characters inserted into a domain included: "L" (nearly 18%), "R" (13%), "S" (nearly 11%), and "E" (nearly 7%). "I" is commonly inserted in front of other characters, while "S" typically appears after the other characters.



CONCLUSION AND RECOMMENDATIONS

Despite large commitments to security, email fraud is on the rise. Cyber criminals are becoming more advanced. They are successfully evading traditional security solutions, leaving your people as the last line of defense. Email fraud tactics and approaches are always changing. That's why you need a multi-layered defense that includes:

- DMARC email authentication. Block all impostor email attacks that spoof trusted domains.
- Dynamic classification. Analyze the content and context of the email and stop display-name and lookalike domain spoofing at the email gateway.
- Data loss prevention. Prevents sensitive information, such as W2s, from leaving your environment.
- Lookalike domain discovery. Identify and flag potential risky domains outside of your control.

To learn more about the Proofpoint Email Fraud solution visit proofpoint.com/us/solutions/email-fraud