proofpoint™

IMPOSTOR EMAIL THREATS

4 Business Email Compromise Techniques and How to Stop Them

INTRO DUCTION

The email was marked “urgent” and “strictly confidential.”[1]

“Glen, I have assigned you to manage file T521,” it began, addressing the accounting director of a Houston-based industrial manufacturer. “This is a strictly confidential financial operation, to which takes priority over other tasks.”

A follow-up call provided details: the manufacturer’s CEO needed $480,000 wired to an account in China as part of an upcoming deal. The director wired the money as instructed, heeding the email’s warning not to tell anyone about the transfer because of U.S. securities rules.

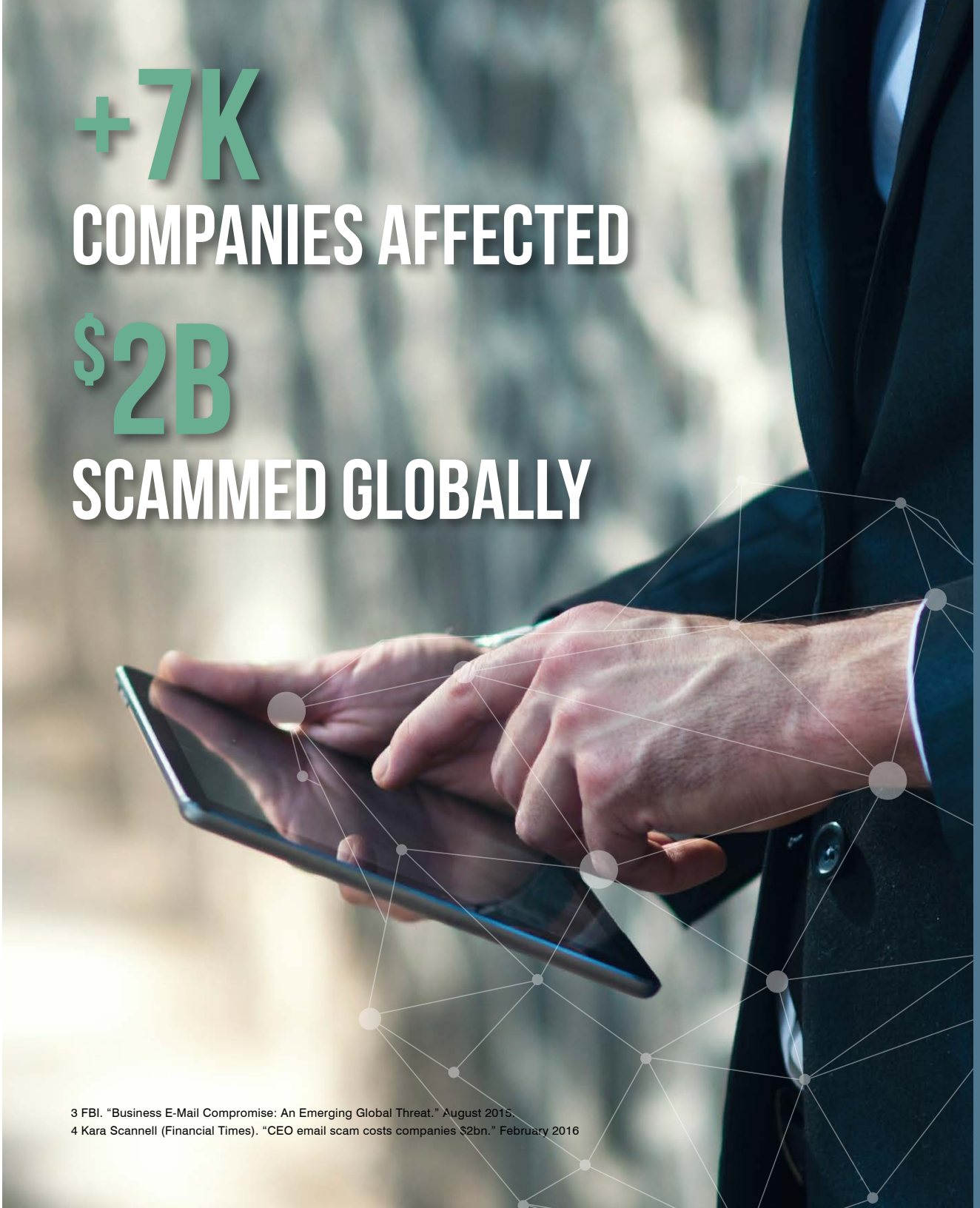
An email sent a week later confirmed the transfer—and asked for $1.8 million more. That’s when the director realized he had been scammed.

This real-life account, detailed in legal filings this year, is just one example of impostor email threats. These threats, also known as business email compromise (BEC) and CEO fraud, slip past many email defenses. Rather than exploiting software flaws, weak security tools, or stolen credentials, impostor emails take advantage of human nature.

“BEC is a serious threat on a global scale,” said FBI Special Agent Maxwell Marker in a recent press release. “It’s a prime example of organized crime groups engaging in large-scale, computer-enabled fraud, and the losses are staggering.”[2]

1 Krebs on Security. “Firm Sues Cyber Insurer Over $480K Loss.” January 2016.

2 FBI. “Business E-Mail Compromise: An Emerging Global Threat.” August 2015.



+7K
COMPANIES AFFECTED

$2B
SCAMMED GLOBALLY

3 FBI. "Business E-Mail Compromise: An Emerging Global Threat." August 2015.
4 Kara Scannell (Financial Times). "CEO email scam costs companies $2bn." February 2016

THE COSTS OF IMPOSTOR EMAIL— AND WHY THEY WORK

Impostor email threats have hit more than **7,000 companies** since the FBI's Internet Crime Complaint Center (IC3) began tracking this type of scam in late 2013.[3] These attacks have collectively scammed victims out of more than **$2 billion globally.**[4]

Similar to the movie industry, these attacks take the "blockbuster" approach. Many messages will be quickly recognized by recipients as phishing and discarded. But the small few that succeed can yield millions of dollars in fraudulent transfers.

Unfortunately, these types of emails only rarely trigger security policy alerts. That's because they:

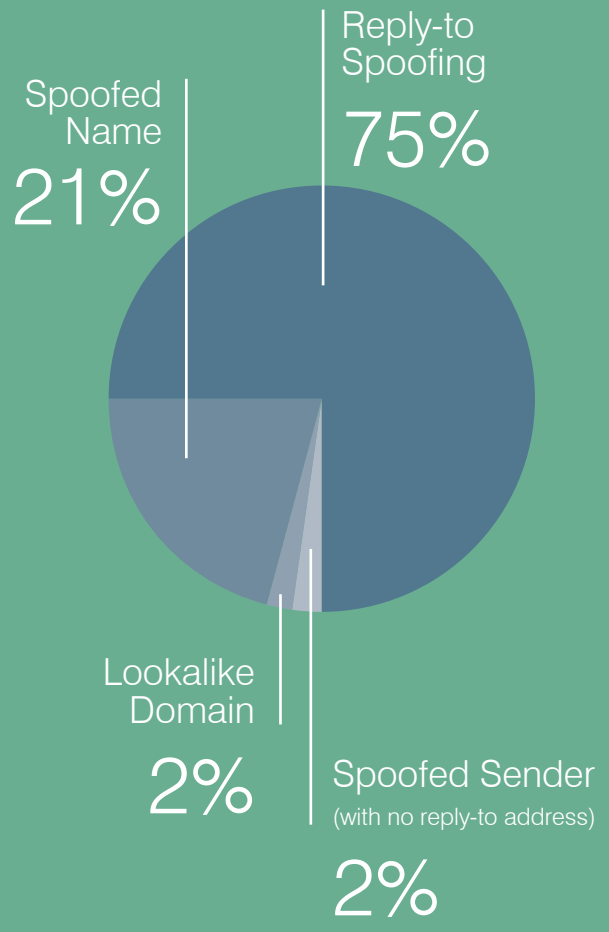
LOOK AND FEEL LEGITIMATE

DO NOT INCLUDE A MALICIOUS LINK OR MALWARE ATTACHMENT

DO NOT ARRIVE IN HIGH ENOUGH VOLUMES TO RAISE RED FLAGS

FOUR MESSAGE TYPES

As we explain in The Human Factor 2016 report, most impostor emails use one of four techniques to fool recipients:



REPLY-TO SPOOFING

In this technique, the “From” name and address is the real name and email address of the sender being impersonated (typically the CEO). The “Reply-to” name also uses the name of the executive. But the address—where any replies are actually sent—is the attacker’s. It often resembles something like ceo. executive@presidentmail.com.

EHLOhacker.com
MAIL FROM: <evildude@hacker.com>
RCPT TO: <fred.finance@acmecorp.com>

Reply-To: evildude@hacker.com

Fred,

I need you to make a wire transfer ASAP..

Messages

Transfer

Bob Bossman

Sent: Wednesday, October 2, 2015 at 5:17 PM

To:

Fred,

I need you to make a wire transfer ASAP..

SPOOFED NAME

In this approach, the impostor email uses the name of the spoofed executive in the “From” field. But the email address comes from an outside service such as Gmail that belongs to the attacker.

EHLOhacker.com
MAIL FROM: <evildude@hacker.com>
RCPT TO: <fred.finance@acmecorp.com>

From: Bob Bossman<bob.bossman@gmail.com>
Reply-To: evildude@hacker.com
Subject: Transfer

Fred,

I need you to make a wire transfer ASAP..

Messages

Transfer

Bob Bossman

Sent: Wednesday, October 2, 2015 at 5:17 PM

To:

Fred,

I need you to make a wire transfer ASAP..

SPOOFED SENDER
(WITH NO REPLY-TO ADDRESS)

In this approach, the impostor email uses the name and email address of the spoofed executive. But the email does not contain a “Reply-to address.” Because the lack of a “Reply-to” address makes two-way conversations impossible, the message includes complete wire-transfer instructions to make follow-up messages unnecessary.

EHLOhacker.com
MAIL FROM: <evildude@hacker.com>
RCPT TO: <fred.finance@acmecorp.com>

From: Bob Bossman<bob.bossman@legtcompany.com>
Reply-To:
Subject: Transfer

Fred,

I need you to make a wire transfer ASAP...

Messages

Transfer

Bob Bossman

Sent: Wednesday, October 2, 2015 at 5:17 PM

To:

Fred,

I need you to make a wire transfer ASAP...

LOOKALIKE DOMAIN

In this approach, the attacker's "From" address is close enough in appearance to the impersonated executive's to fool a rushed employee eager to please the boss. In one case we saw, the attacker created an email address that was just one letter different from the customer domain. Imagine a spoofed email from the CEO of "legitcompany.com" that is rendered "legtcompany.com" (note the missing "i").

EHLOhacker.com
MAIL FROM: <evildude@hacker.com>
RCPT TO: <fred.finance@acmecorp.com>

From: Bob Boss<bob.boss@legtcompany.com>
Reply To: evildude@hacker.com
Subject: Transfer

Fred,

I need you to make a wire transfer ASAP..

Messages

Transfer

Bob Boss

Sent: Wednesday, October 2, 2015 at 5:17 PM

To:

Fred,

I need you to make a wire transfer ASAP..

RECOMMENDATIONS

Stopping this threat requires the right technology solutions and procedural controls. Here are a few ways you can mitigate the risks of impostor email threats.

- **Deploy an email gateway that supports advanced configuration options** for flagging suspicious messages based on attributes (such as direction and Subject line) and email authentication techniques.

- **Adopt advanced threat solutions to identify and block targeted attacks** that travel over email, the No. 1 threat vector. These solutions must take into account the increasing sophistication of emerging threats and socially engineered attacks. Speak to your security vendor about system settings to identify and block impostor email threats.

- **Put internal finance and purchasing controls in plac**e to authenticate legitimate requests. These controls should include a secondary, out-of-band, in-person, or phone approval by another person in the organization.

- **Make users aware of the latest social engineering and phishing schemes** through regular training. Done right, “phishing” your own employees can also be a useful test of how effective your user-awareness efforts are. This approach also helps address the “human factor” of attacks.

To learn more about how Proofpoint can help your organization combat impostor email threats,

READ OUR WHITE PAPER "IMPOSTOR IN THE MACHINE"

ABOUT PROOFPOINT

Proofpoint Inc. (NASDAQ:PFPT) is a leading next-generation security and compliance company that provides cloud-based solutions for comprehensive threat protection, incident response, secure communications, social media security, compliance, archiving and governance. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system. Proofpoint protects against phishing, malware and spam, while safeguarding privacy, encrypting sensitive information, and archiving and governing messages and critical enterprise information.

More information is available at www.proofpoint.com

© Proofpoint, Inc., 2016. 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.