The Rise of Business Email Compromise (BEC)

Why BEC now?
Social Media and social engineering has added to the success rate for spoofing attacks. Attackers are not just randomly choosing their targets.

These attackers are extremely sophisticated and will follow targets for months, on social media, news sites, and other social platforms.

Business Email Compromise
US $5.3 billion stolen between October 2013 and December 2016.

Ransomware
US $1 billion stolen in 2016

Each dollar graphic represents $1K USD.

How it works
Adversaries create targeted messages and add unique details about either the person they are posing as, and/or the person they are attacking, to add legitimacy to the request.

BEC Campaign
Adversary sends an email

Urgent Message
Compels recipient to send money

Criminal Accounts
Money ends in foreign and domestic bank accounts

Who’s at risk?
Large organizations with mature threat defenses can fall victim to BEC. Both Facebook and Google have been victims of BECs and wire fraud.

$100M
Amount stolen from Facebook and Google

Educate Your Users
Encourage users to think twice about emails that demand unusual requests

Consider Threat Tools
Sender policy framework (SPF) can block emails with spoofed addresses

Safeguard your Organization

Learn more about protecting your business from email-based threats with the:
Cisco Email Security buyer’s guide

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the USA and other countries. A listing of Cisco’s trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.