Business Email Compromise (BEC)

PRESENTED BY: NIKKI ROBINSON, DSC

Introduction (Hi!)

- Over 12 years of experience in IT and Security
- Multiple industry certifications: CISSP, CEH/CNDA, MCITP, CCAA
- Doctorate of Science, Cybersecurity
- Dissertation: An Examination of Vulnerability Scoring Using Chained Vulnerability Attacks
- Focus: vulnerability and risk management, incident response, threat intelligence and hunting
- **All information is open-source

Agenda

- Phishing / Spear-phishing / BEC
- What is BEC?
- Types of BEC
- Attack Vectors
- How to Detect
- How to Prevent
- BEC Research

Phishing

- Can be done with email or text messages
- Noticed suspicious activity / log-in attempts
- Problem with payment / account
- Might have fake invoice
- Click link to make payment
- Eligible for government refund / IRS scams
- Coupon for free items

Reference: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Avoid Phishing

- Use Multi-factor Authentication!!!
- Protect mobile devices – updates / security software / encryption
- If suspicious – call Information Security team or Helpdesk
- Verify site's security – many tools available
- Consider white-listing, instead of blocking certain sites
- Keep systems patched

Reference: https://www.phishing.org/10-ways-to-avoid-phishing-scams

Spear-Phishing

- Phishing – broader term for ANY attempt
- Spear-Phishing – more thought / targeted
- Starts with potentially viewing social media profile to acquire target
- Use email address, friends, location, any related posts
- Messages include URGENT requests
- Take victims to spoofed website – ask for passwords, pins, account numbers, etc

Reference: https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing

Avoid Spear-Phishing

- Do NOT post personal information on social media sites
- Use different passwords on every account - try a password manager
- Always update software!!!
- Do NOT click on any links in an email – go directly to account in browser
- Be wary of friend requests or emails from “friends”
- Implement Data Protection Program = user education + best practices + Data Loss Prevention (DLP) software

Reference: https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing

What is BEC?

- Targets companies who conduct wire transfers / suppliers abroad
- Spoofing of corporate / publicly available emails of executives
- Compromise through keyloggers or initial phishing attack
- Fraudulent transfers from attackers
- Carefully research / monitor potential victims / organizations

Reference: https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

BEC Statistics! (From FBI IC3)

- Most costly cybercrime – comes from BEC scams
- 2013-2014 – 1,198 companies affected
- Between 2013-2018 – thieves took $12 billion
- 63% fraud losses are related to BEC
- Reported in all 50 states / 79 countries

Reference: https://krebsonsecurity.com/tag/business-email-compromise/

Private Industry

- May 2014
- Scam impersonated chief executive
- Policy is for computer and funds transfer fraud
- Covered up to $3 million
- Initial ask was for $480,000, then requested $18 million
- Transfer to Agricultural Bank of China
- Suing cyber insurance – refusing to cover $480,000 loss in BEC

Reference: https://krebsonsecurity.com/tag/business-email-compromise/

Non-Profit Organization

- Occurred in 2017
- $1 million cyber scam
- Connecticut-based nonprofit
- Compromised employee email, posed as employee, created false invoices
- Sent money to fraudulent person in Japan (we need solar panels!)
- Recouped most of losses with cyber insurance

Reference: https://www.bostonglobe.com/business/2018/12/12/hackers-fooled-save-children-into-sending-million-phony-account/KPnRi8xIbPGuhGZaFmlhRP/story.html

Fire Department

- 2 employees involved
- Gave $52,000 away in cyberattack
- Sent money to Turkish bank account
- Targeted Chief Executive / National Commander
- Employees did not follow spending / ordering rules

Reference: https://www.rnz.co.nz/news/national/292881/fire-service-scammed-out-of-$52,000

Types of BEC

- Bogus Invoice Scheme – foreign suppliers requesting payments
- CEO Fraud – Pose as CEO / executive requesting transfer
- Account Compromise – Executive account hacked
- Attorney Impersonation – Pretend to be from law firm (CRUCIAL or CONFIDENTIAL matters)
- Data Theft – HR / Payroll employees targeted – want PII or tax statements

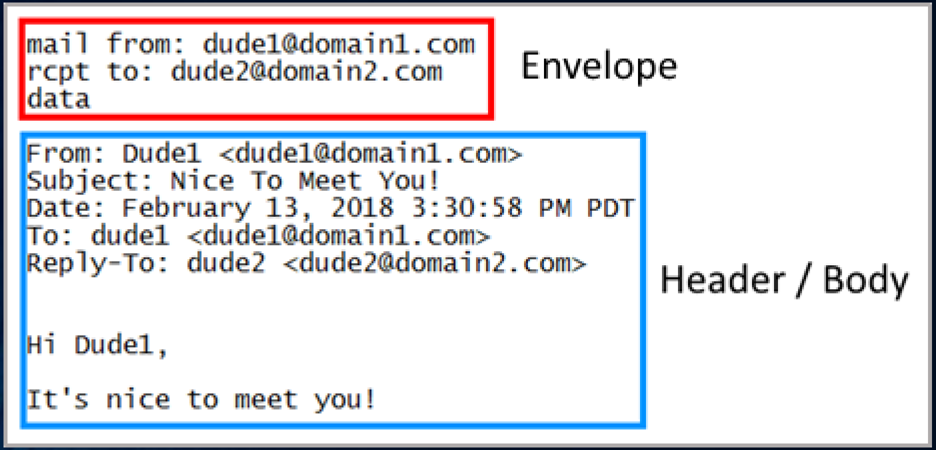
Reference: https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec)

Email Spoofing

- Email header forgery
- Message appears to originate from someone / somewhere else
- Popular in phishing / spam campaigns
- Hackers need an SMTP (Simple Mail Transfer Protocol) server and Outlook or Gmail
- Detection: Find originating IP address and trace back to sender
- Detection: Sender Policy Framework (SPF) – if soft-failed, something might be FISHY!

Reference: https://searchsecurity.techtarget.com/definition/email-spoofing

Email Spoofing Example



```
mail from: dude1@domain1.com
rcpt to: dude2@domain2.com
data
```

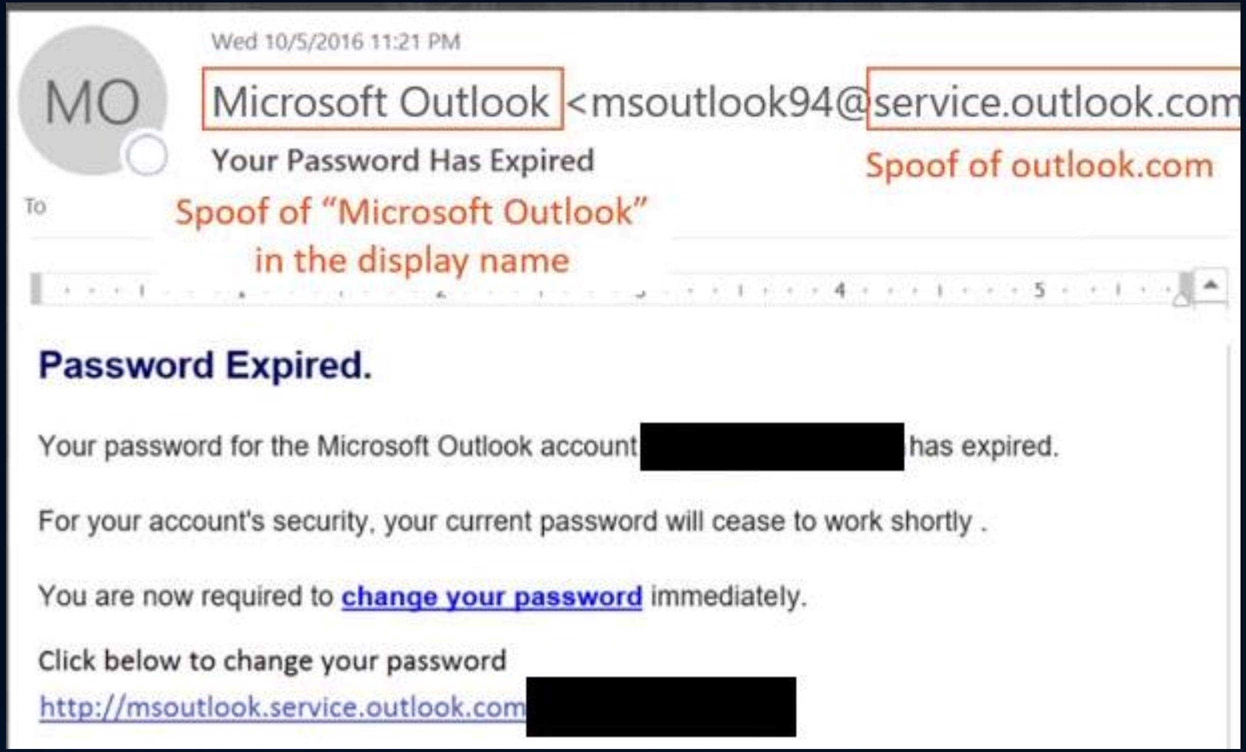
```
From: Dude1 <dude1@domain1.com>
Subject: Nice To Meet You!
Date: February 13, 2018 3:30:58 PM PDT
To: dude1 <dude1@domain1.com>
Reply-To: dude2 <dude2@domain2.com>


Hi Dude1,

It's nice to meet you!
```

Reference ^: https://www.proofpoint.com/us/corporate-blog/post/how-does-email-spoofing-work-and-why-it-so-easy

Reference >: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-spoofing-protection



Wed 10/5/2016 11:21 PM

Microsoft Outlook <msoutlook94@service.outlook.com

Your Password Has Expired

Spoof of "Microsoft Outlook" in the display name

Spoof of outlook.com

Password Expired.

Your password for the Microsoft Outlook account [redacted] has expired.

For your account's security, your current password will cease to work shortly .

You are now required to change your password immediately.

Click below to change your password

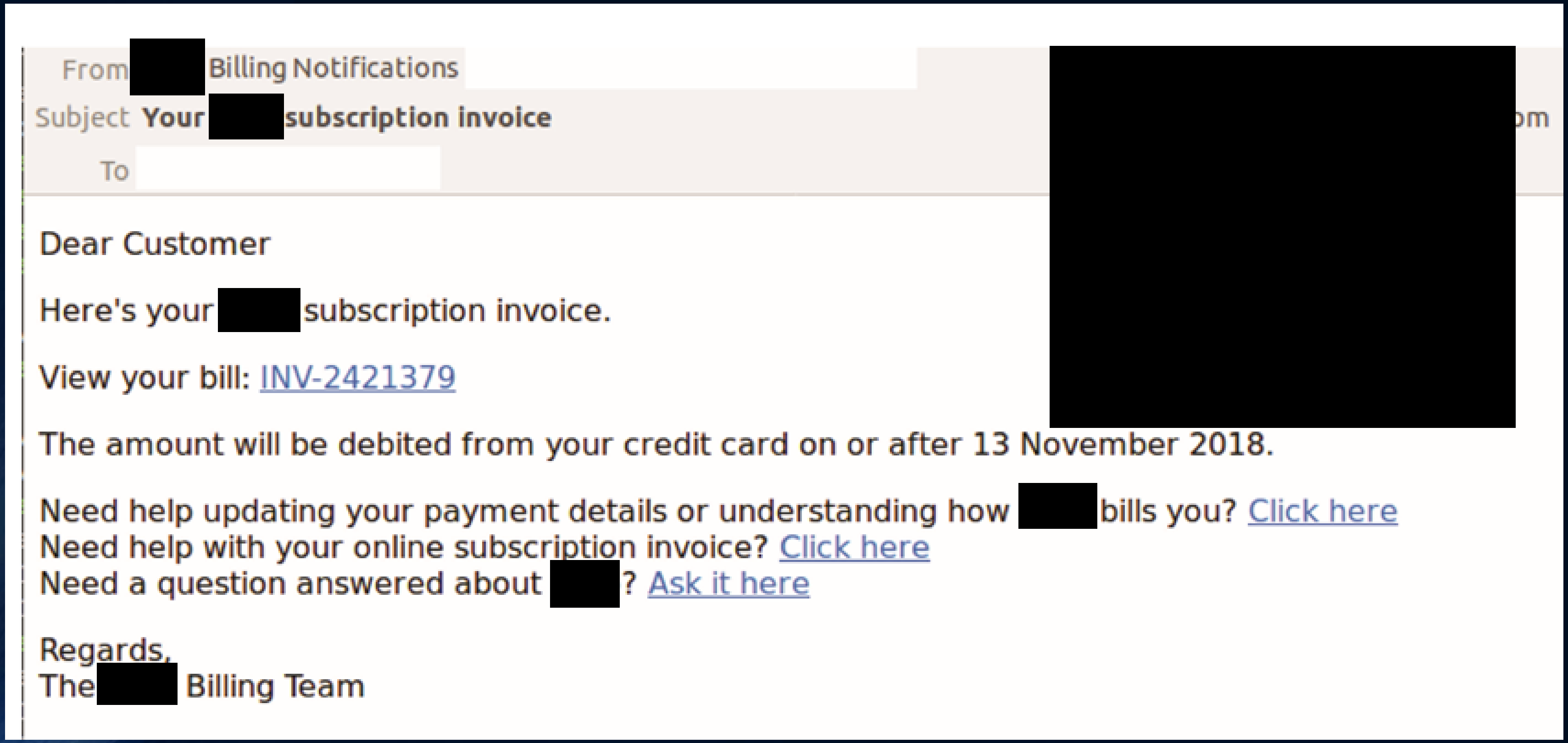
http://msoutlook.service.outlook.com [redacted]

Email Header Forgery

Reference: https://www.howtogeek.com/121532/htg-explains-how-scammers-forge-email-addresses-and-how-you-can-tell/

```
Delivered-To: [MY EMAIL ADDRESS]
Received: by 10.182.3.66 with SMTP id a2csp104490oba;
Sat, 11 Aug 2012 15:32:15 -0700 (PDT)
Received: by 10.14.212.72 with SMTP id x48mr8232338eeo.40.1344724334578;
Sat, 11 Aug 2012 15:32:14 -0700 (PDT)
Return-Path: <e.vwidxus@yahoo.com>
Received: from 72-255-12-30.client.stsn.net (72-255-12-30.client.stsn.net. [72.255.12.30])
by mx.google.com with ESMTP id c41si1698069eem.38.2012.08.11.15.32.13;
Sat, 11 Aug 2012 15:32:14 -0700 (PDT)
Received-SPF: neutral (google.com: 72.255.12.30 is neither permitted nor denied by best guess record for domain of
e.vwidxus@yahoo.com) client-ip=72.255.12.30;
Authentication-Results: mx.google.com; spf=neutral (google.com: 72.255.12.30 is neither permitted nor denied by best
guess record for domain of e.vwidxus@yahoo.com) smtp.mail=e.vwidxus@yahoo.com
Received: by vwidxus.net id hnt67m0ce87b for <[MY EMAIL ADDRESS]>; Sun, 12 Aug 2012 10:01:06 -0500
(envelope-from <e.vwidxus@yahoo.com>)
Received: from vwidxus.net by web.vwidxus.net with local (Mailing Server 4.69)
id 34597139-886586-27/./PV3Xa/WiSKhnO+7kCTI+xNiKJsH/rC/
for root@vwidxus.net; Sun, 12 Aug 2012 10:01:06 –0500
…
From: “Canadian Pharmacy” e.vwidxus@yahoo.com
```

Invoice Scams (1 of 2)



From [redacted] Billing Notifications

Subject **Your [redacted] subscription invoice**

To

[redacted]

Dear Customer

Here's your [redacted] subscription invoice.

View your bill: INV-2421379

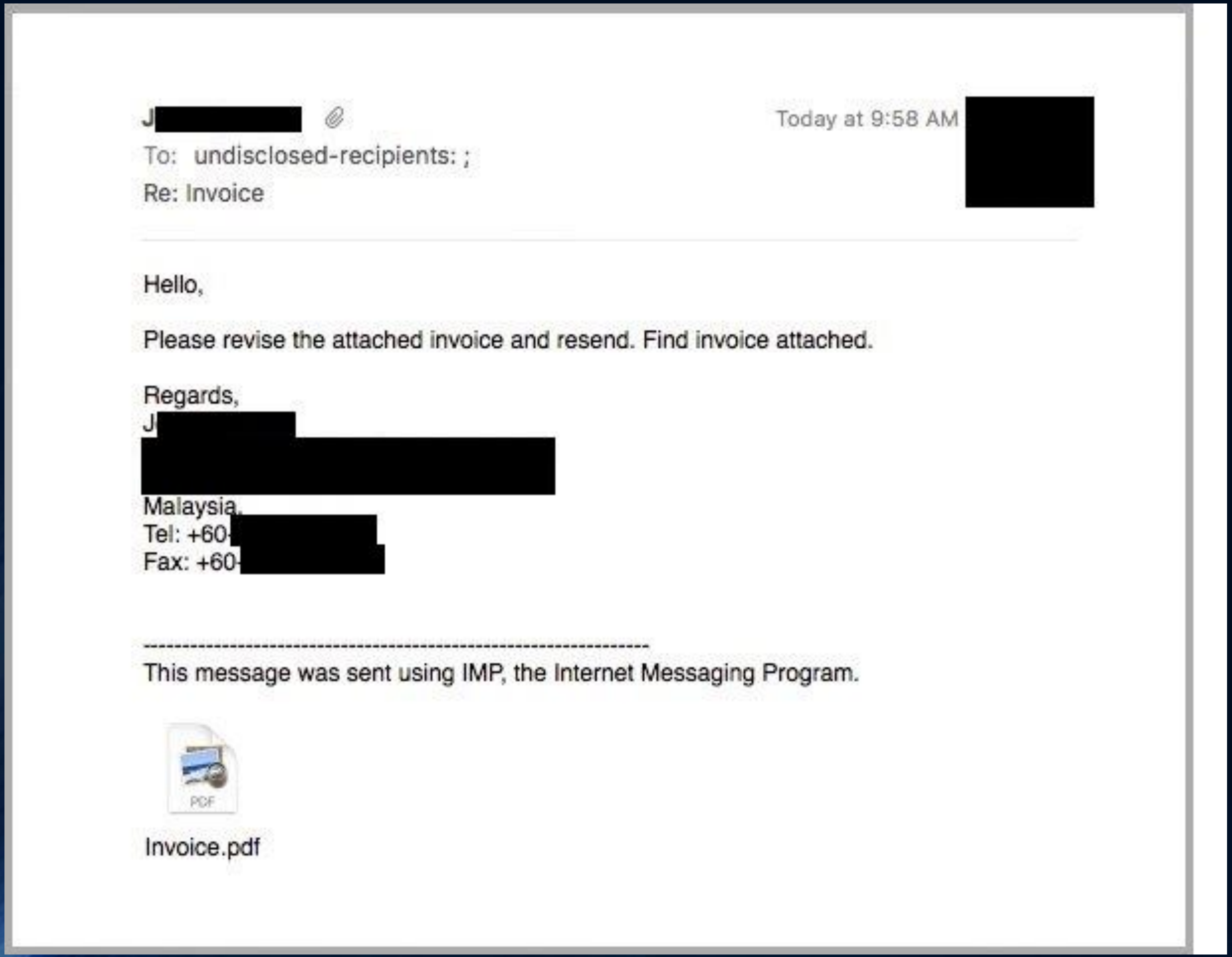
The amount will be debited from your credit card on or after 13 November 2018.

Need help updating your payment details or understanding how [redacted] bills you? Click here
Need help with your online subscription invoice? Click here
Need a question answered about [redacted]? Ask it here

Regards,
The [redacted] Billing Team

Reference: https://www.mailguard.com.au/blog/beware-invoice-email-scam-brandjacking-xero

Invoice Scams (2 of 2)



J[redacted]

Today at 9:58 AM [redacted]

To: undisclosed-recipients: ;

Re: Invoice

Hello,

Please revise the attached invoice and resend. Find invoice attached.

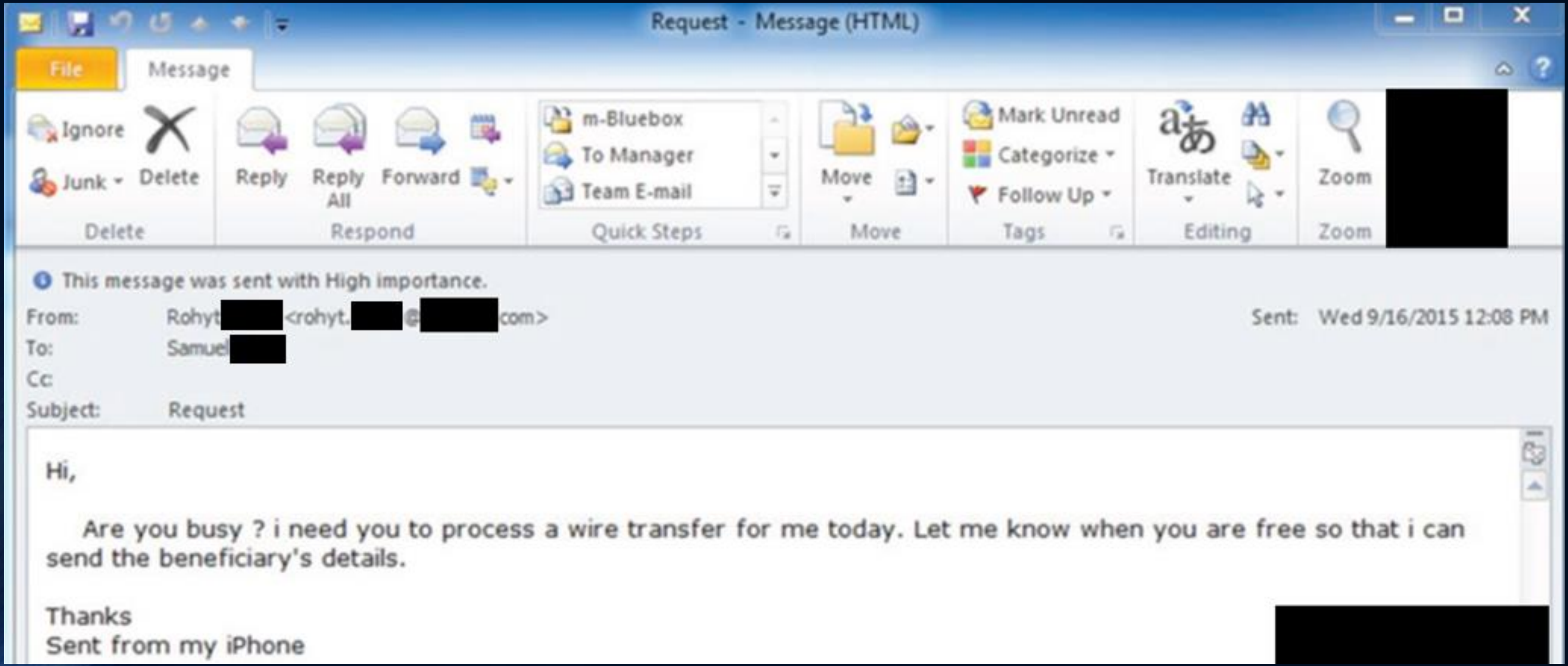
Regards,
J[redacted]
[redacted]
Malaysia.
Tel: +60-[redacted]
Fax: +60-[redacted]

This message was sent using IMP, the Internet Messaging Program.

Invoice.pdf

Reference: https://www.mailguard.com.au/blog/fraudulent-invoice-email-carries-an-adobe-id-phishing-pdf-attachment

CEO / Executive Fraud



[redacted]

This message was sent with High importance.

From: Rohyt[redacted] <rohyt.[redacted]@[redacted]com>
Sent: Wed 9/16/2015 12:08 PM
To: Samuel[redacted]
Cc:
Subject: Request

Hi,

Are you busy ? i need you to process a wire transfer for me today. Let me know when you are free so that i can send the beneficiary's details.

Thanks
Sent from my iPhone

[redacted]

Reference: https://cofense.com/10-ways-defend-business-email-compromise-ceo-email-fraud-scams/

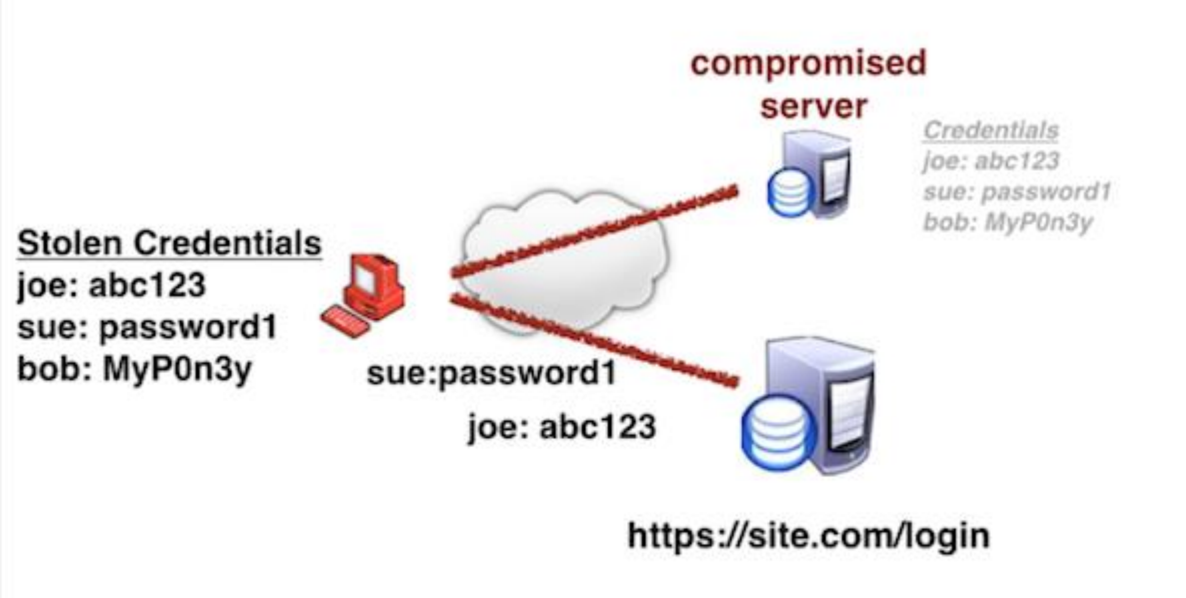
Attorney Impersonation

- Many methods to BEC, but two most common scenarios are CEO fraud and Attorney impersonation
- Attacker contacts employee directly
- Fake attorney is included in important case (NO TIME!!!!)
- Transfer funds to attorney or gain sensitive proprietary data
- Could be a great example for a phishing exercise!

Reference: https://resources.infosecinstitute.com/bec-attacks-attorney-impersonation-works/#gref

Credential Stuffing

1. Attacker acquires usernames / pw from a website breach / pw dump site
2. Uses account checker to test stolen creds against website (ex: social media)
3. Successful logins allow attacker to take over account
4. Drains stolen accounts (PII, stored values, etc)
5. Use account info going forward (send spam / create transactions)



Reference: https://www.owasp.org/index.php/Credential_stuffing

Reference (image): http://michael-coates.blogspot.be/2013/11/how-third-party-password-breaches-put.html

How to Detect?

- Email received from Executive team or leadership – must process payment now!
- Message is brief, urgent, bypass normal processes
- Sender may say they are traveling – from mobile device (as shown in our example!)
- Email is from Gmail / Hotmail instead of business account
- Someone asks you to open bank account to send / receive money
- And if you can't tell, call your Helpdesk or Security team!

Reference: https://www.aarp.org/money/scams-fraud/info-2019/business-email-compromise.html

BEC Research

- Trend Micro Report (2018) – Malware in BEC has decreased / attackers prefer more simple phishing attacks
- David Zweighaft (2017) – Determined financial institutions need to be proactive / create culture of skepticism / more training
- Asaf Cidon et al. (2019) – Worked on tool with Barracuda Networks to prevent BEC attacks using supervised learning

Reference: https://documents.trendmicro.com/assets/TrackingTrendsinBusinessEmailCompromise.pdf

Reference: https://www.emerald.com/insight/content/doi/10.1108/JOIC-02-2017-0001/full/html

Reference: https://www.usenix.org/conference/usenixsecurity19/presentation/cidon

How to Prevent (1 of 2)

- Intrusion Detection System (IDS) Rules (xy-business vs xy_business)
- Email rules (reply is different from the “from” email)
- Color coding (internal accounts (ex: blue) / external (ex: purple)
- Payment verification (require two-factor authentication!!!)
- Confirmation request (maybe add phone verification? Directory vs external numbers)
- Scrutiny – tell your employees to report suspicious fund requests!

Reference: https://www.barracuda.com/glossary/business-email-compromise

How to Prevent (2 of 2)

- DMARC record on your company domain name – spoofed emails will not get delivered
- Training!!!
  - Provide examples of BEC
  - Show how easy it is to spoof emails
  - Training should be tailored to specific teams – they may see different threats
  - Security is everyone’s responsibility!

Reference: https://www.barracuda.com/glossary/business-email-compromise

Cyber Insurance

- Prepare for the worst!
- Cyber risk insurance or Cyber Liability Insurance Coverage (CLIC)
- Transfer risk to someone else!
- By 2020, premiums at $7.5 billion
- 1/3 companies have some type of cyber insurance
- Covers first AND third parties

Reference: https://www.cio.com/article/3065655/what-is-cyber-insurance-and-why-you-need-it.html

Comments / Questions?!