RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: HT-R02

Business Email Compromise: Operation Wire Wire & New Attack Vectors

Anne Connell

Cybersecurity Engineer
CMU – SEI – CERT
@aconnell

Notices

This material is based upon work funded and supported by the Department of Justice under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM19-0222

Topics

- Introduction
- BEC Impact
- BEC Targets and TTPs
- Recon: How Attackers Collect Data on Targets
- Operation Wire Wire & New Attack Vectors
- Defending Against BEC
- Apply

What is BEC?

"Impersonation of executives or business contacts to obtain the transfer of funds or sensitive information"

Business Email Compromise (BEC) is:

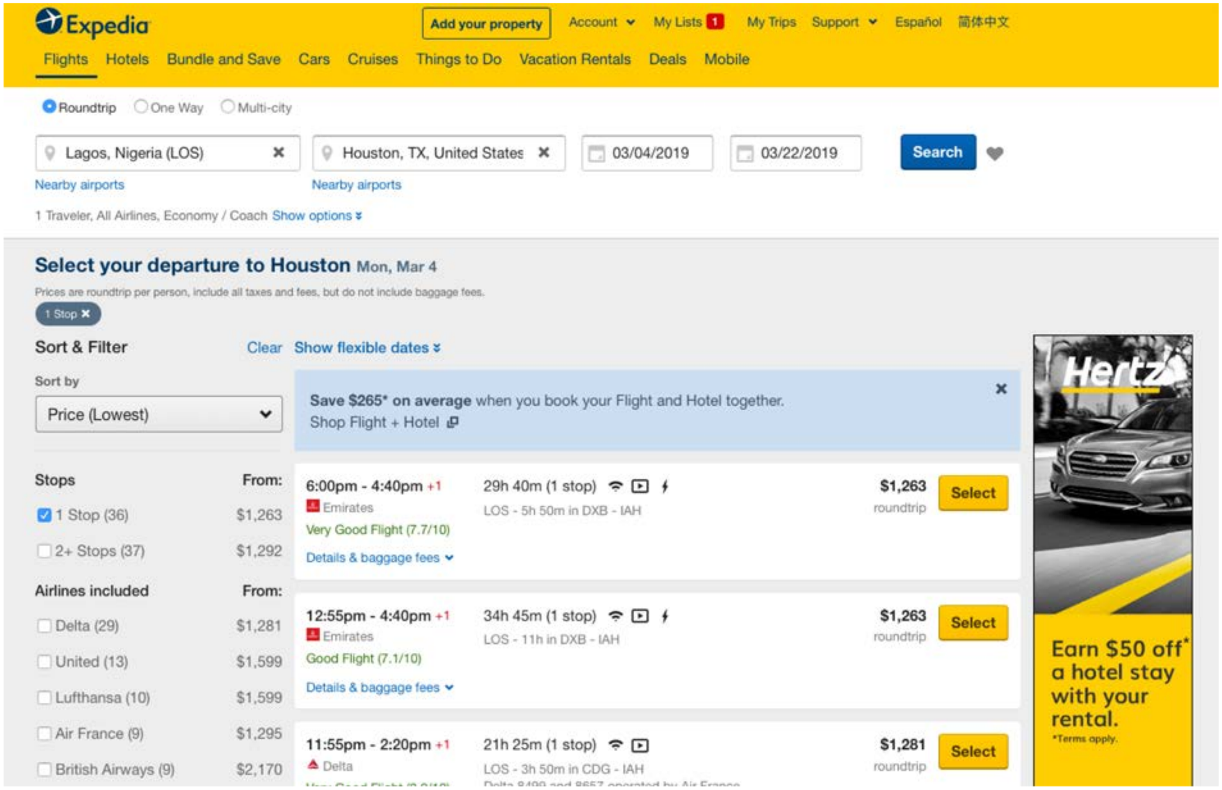
- Scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.
- Involves use of an email account compromise (EAC) component that targets individuals who perform wire transfer payments.
- Scam puts business email accounts, personally identifiable information (PII), and employee wage and tax information at risk.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

“Colvis”

Through the work he did in the Dallas area, he thieved $3.2 million using BEC scams.

Target Selection



● Roundtrip ○ One Way ○ Multi-city

Lagos, Nigeria (LOS) ✖ | Houston, TX, United States ✖ | 03/04/2019 | 03/22/2019 | Search

Nearby airports | Nearby airports

1 Traveler, All Airlines, Economy / Coach Show options

Select your departure to Houston Mon, Mar 4

Prices are roundtrip per person, include all taxes and fees, but do not include baggage fees.

1 Stop ✖

Sort & Filter | Clear | Show flexible dates

Sort by: Price (Lowest)

Stops	From:
☑ 1 Stop (36)	$1,263
□ 2+ Stops (37)	$1,292

Airlines included	From:
□ Delta (29)	$1,281
□ United (13)	$1,599
□ Lufthansa (10)	$1,599
□ Air France (9)	$1,295
□ British Airways (9)	$2,170

Save $265* on average when you book your Flight and Hotel together.
Shop Flight + Hotel

6:00pm - 4:40pm +1 | 29h 40m (1 stop) | $1,263 roundtrip | Select
Emirates | LOS - 5h 50m in DXB - IAH
Very Good Flight (7.7/10)
Details & baggage fees

12:55pm - 4:40pm +1 | 34h 45m (1 stop) | $1,263 roundtrip | Select
Emirates | LOS - 11h in DXB - IAH
Good Flight (7.1/10)
Details & baggage fees

11:55pm - 2:20pm +1 | 21h 25m (1 stop) | $1,281 roundtrip | Select
Delta | LOS - 3h 50m in CDG - IAH

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Scenario used for FBI CICP BEC Course

- Texas Energy Company Case coined the ‘BEC’ term
- This case is the scenario for FBI Cyber Investigator Certification Program (CICP) Training on the LEEP Portal

RSAConference2019

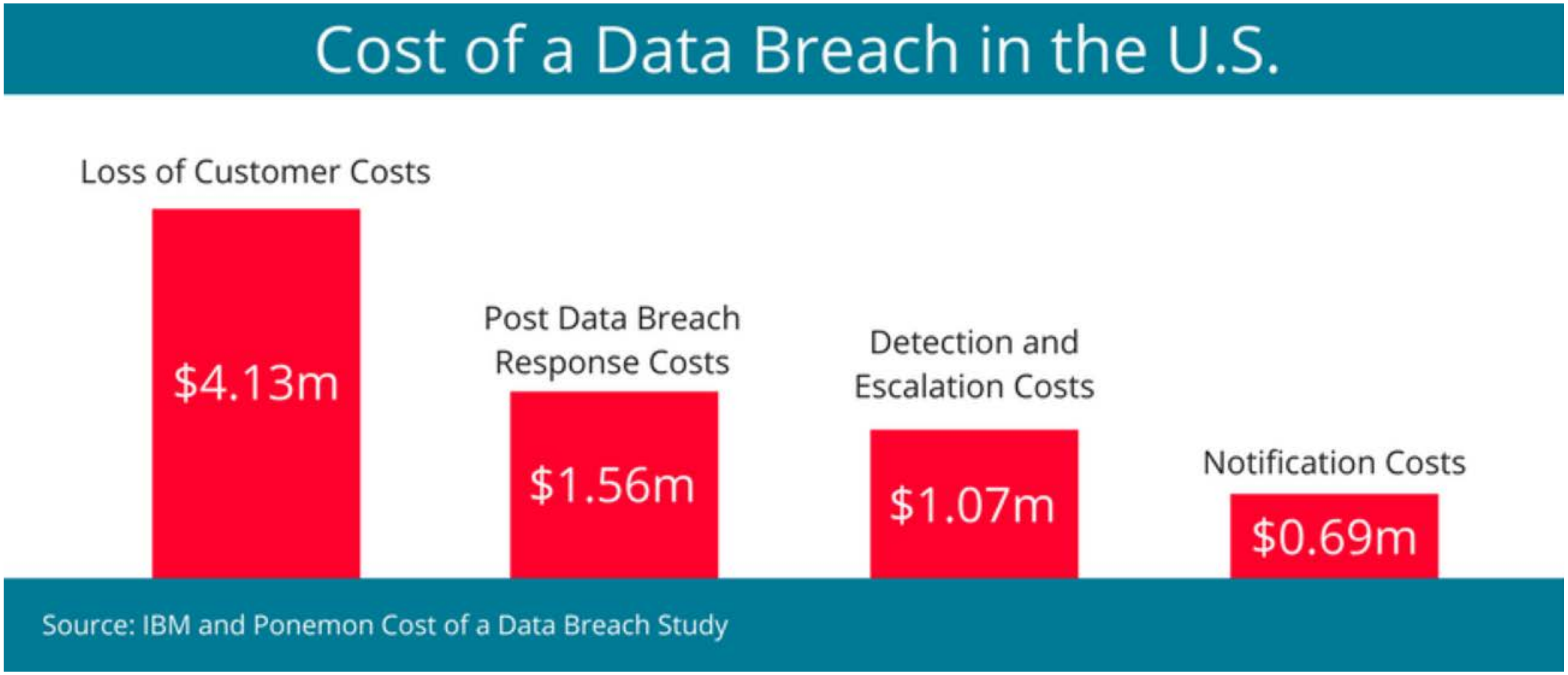
BEC Impact

International Business Email Compromise Schemes

BEC Numbers

- Business Email Compromise (BEC) attacks have increased by 136% from December 2016 to May 2018.
- It ranks #1 in the IC3's 2017 Internet Crime Report for the volume of victim losses, representing nearly half (48%) of the total losses of the top 10 Internet crimes.
- In 2017, IC3 received a total of **301,580 complaints** with reported losses exceeding **$1.4 Billion**.

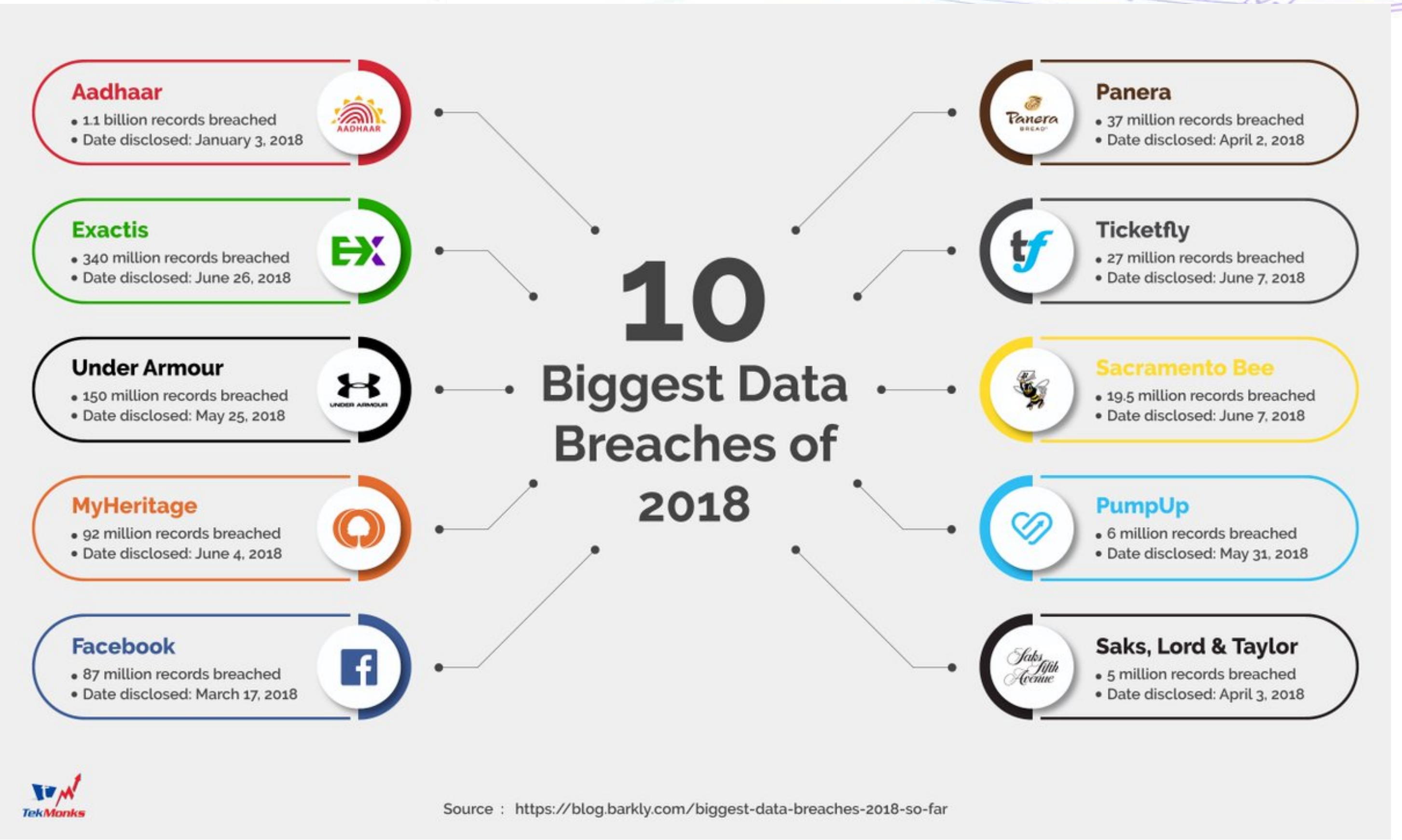
Source: "2017 Internet Crime Report" https://pdf.ic3.gov/2017_IC3Report.pdf



Cost of a Data Breach in the U.S.

Source: IBM and Ponemon Cost of a Data Breach Study

https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf



10 Biggest Data Breaches of 2018

Aadhaar
- 1.1 billion records breached
- Date disclosed: January 3, 2018

Exactis
- 340 million records breached
- Date disclosed: June 26, 2018

Under Armour
- 150 million records breached
- Date disclosed: May 25, 2018

MyHeritage
- 92 million records breached
- Date disclosed: June 4, 2018

Facebook
- 87 million records breached
- Date disclosed: March 17, 2018

Panera
- 37 million records breached
- Date disclosed: April 2, 2018

Ticketfly
- 27 million records breached
- Date disclosed: June 7, 2018

Sacramento Bee
- 19.5 million records breached
- Date disclosed: June 7, 2018

PumpUp
- 6 million records breached
- Date disclosed: May 31, 2018

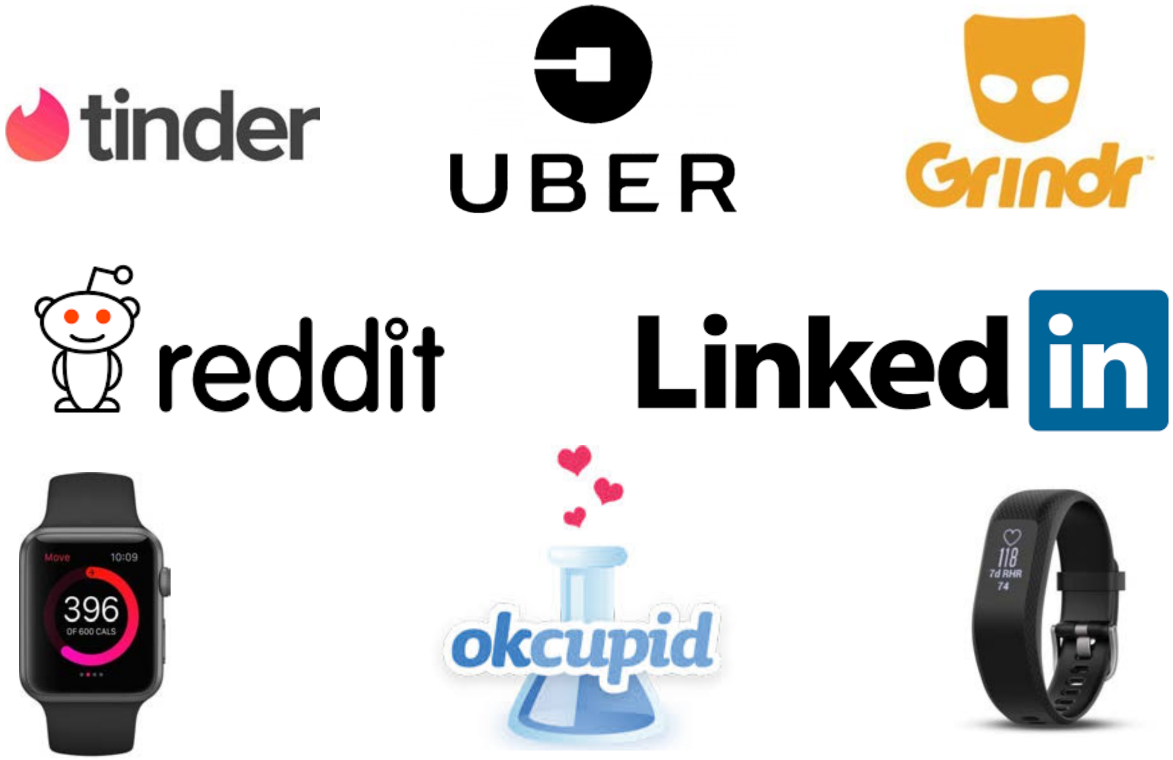
Saks, Lord & Taylor
- 5 million records breached
- Date disclosed: April 3, 2018

TekMonks

Source : https://blog.barkly.com/biggest-data-breaches-2018-so-far

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Social Media Mining



- Names
- Gender
- Social security numbers
- Birthdays
- Addresses
- Driver's license #
- Zip Code

BEC Attack Examples

- Google/Facebook $100M Partner Invoice Scam
  - Evaldas Rimašauskas $100 million to BEC attacks impersonating their server hardware supplier Quanta even from Google and Facebook
- MacEwan University $11.8M Wire Transfer Fraud
  - Defrauded of $11.8 million in a BEC attack impersonating a vendor of the university.
- New York Judge Loses Over $1.5M in Real Estate Scam
  - A NY State Supreme Court judge lost over $1.5 million in a BEC attack that impersonated her lawyer,

- Source: Symantec Attack Trends Report, 2018.

RSAConference2019

BEC Targets and TTPs

Techniques, Tactics, and Procedures (TTPs)

International Business Email Compromise Schemes

BEC Common Targets

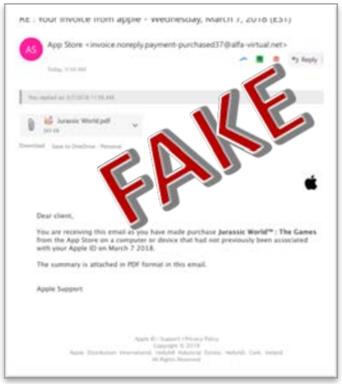
- Real Estate
- Legal Services
- B2B Commerce
- Database and W2 Theft

PII and W-2 Information Targets

- The US Internal Revenue Service (IRS) Stopped 6+ million suspicious returns in 2017
- These efforts prevented payment of $11 billion in suspicious returns
- The IRS still paid out approximately $5.1 billion in Stolen Identity Return Fraud (SIRF) in 2017

BEC Types

“Email Hacked”, “Credentials Stolen”



RE : Your invoice from apple - Wednesday, March 7, 2018 (EST)

AS App Store <invoice.noreply.payment-purchased37@alfa-virtual.net>

Today, 11:56 AM

You replied on 3/7/2018 11:56 AM.

Jurassic World.pdf

Download · Save to OneDrive - Personal

Dear client,

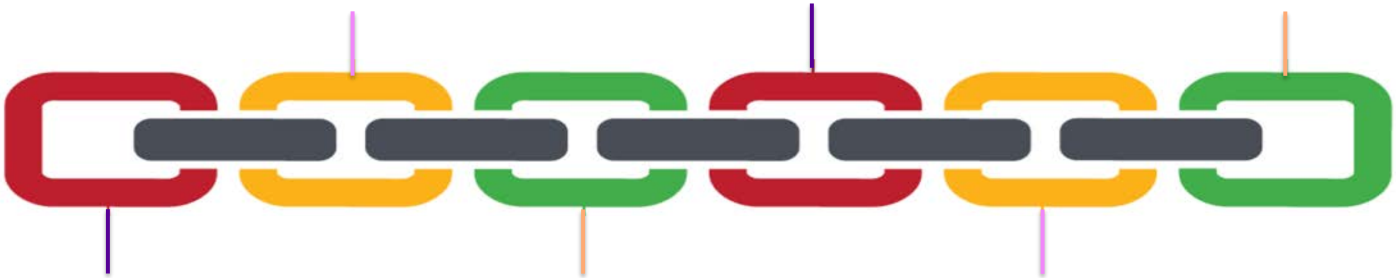
You are receiving this email as you have made purchase **Jurassic World™ : The Games** from the App Store on a computer or device that had not previously been associated with your Apple ID on March 7 2018.

The summary is attached in PDF format in this email.

Apple Support

Apple ID | Support | Privacy Policy
Copyright © 2018
Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland
All Rights Reserved

BEC Attack Timeline



1. HIT LIST
Attacker does recon and generates lists compromising the name of a sender and the name and email of recipient. Typically in batches of 50/100

2. LAUNCH
Attacker launches attack by transmitting initial requests to the users on the hit list

3. REQUEST
As victims respond, the criminal engages in a small number of exchanges, after which he makes a request to perform a wire transfer to a 'supposed' vendor

4. EXFILTRATION
Wire transfers are not made to accounts belonging to criminal, but to mules

5. EXTRACT
Criminals always want receipts for transfers as a way to prove the money was transferred or to verify its worth the effort to attempt to extract the funds

6. REPEAT
Whether the criminal manages to receive the funds or not, he is likely to try requesting again

RSAConference2019

Recon: How Attackers Collect Data on Targets

International Business Email Compromise Schemes

Multiple Ways of Obtaining Information

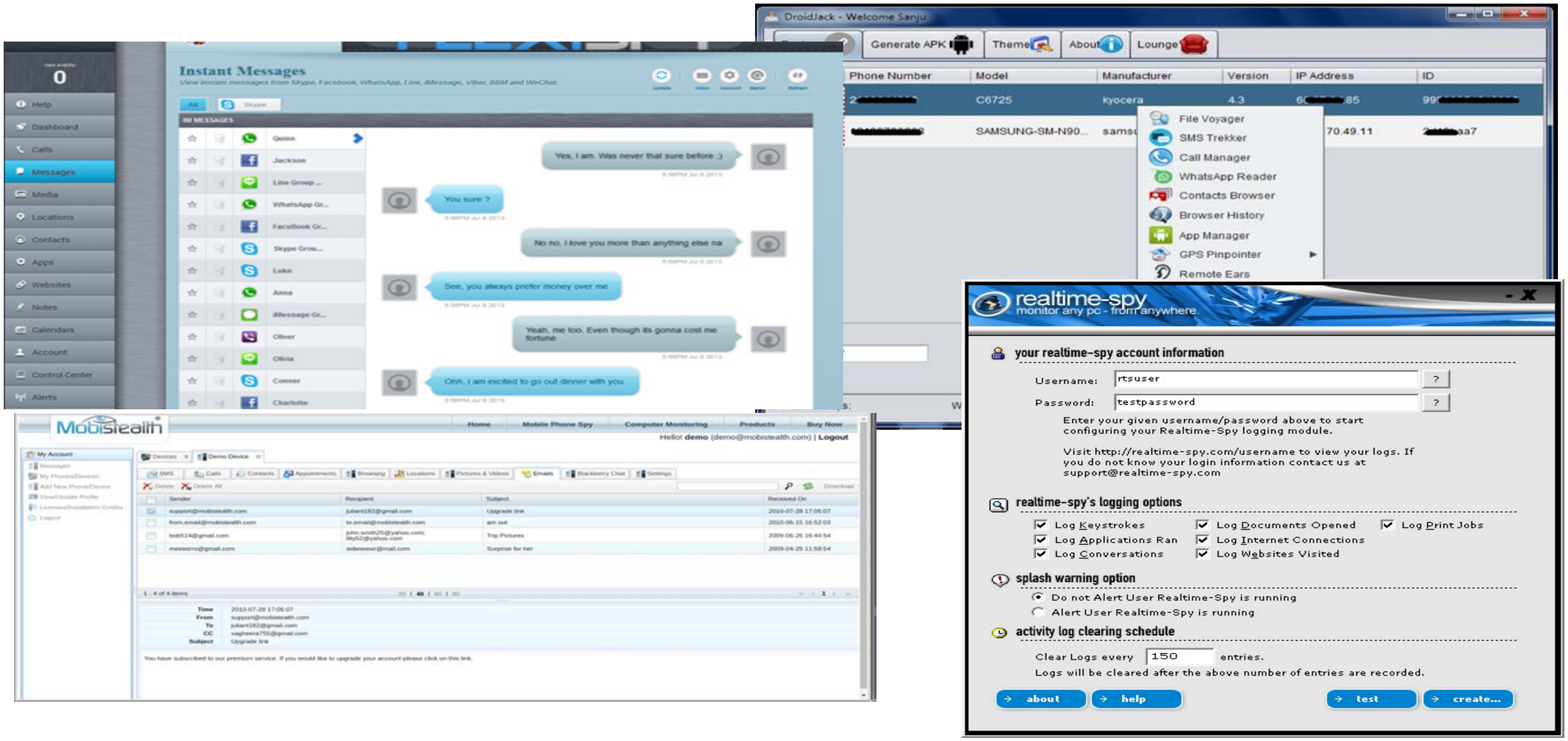
- Professional cybercrime rings
- Malware
- Web compromise
- Access Control
- Open Source Intel Collection (OSIT)
- Social Engineering
- Social Media Mining
- Dark Web Mining

Source: ISACA State of Cyber Security 2017

Social Engineering

- “From” field spoofing
  - From field appears to come from someone known, but actual sender address is different
- “Reply-To” field spoofing
  - Reply-To address field contains different email address (web mail)
- Sender spoofing
  - Address and From fields are faked, reply not expected - single phrase attack
- Visual domain spoofing
  - Homograph attack

Dark Web Mining



Instant Messages

View instant messages from Skype, Facebook, WhatsApp, Line, iMessage, Viber, BBM and WeChat.

Quinn · Jackson · Line Group ... · WhatsApp Gr... · FaceBook Gr... · Skype Grou... · Luke · Anna · iMessage Gr... · Oliver · Olivia · Conner · Charlotte

Yes, I am. Was never that sure before ;)

You sure ?

No no, I love you more than anything else na

See, you always prefer money over me

Yeah, me too. Even though its gonna cost me fortune

Ohh, I am excited to go out dinner with you.

DroidJack - Welcome Sanju

Phone Number	Model	Manufacturer	Version	IP Address	ID
2[redacted]	C6725	kyocera	4.3	6[redacted].85	99[redacted]
[redacted]	SAMSUNG-SM-N90...	samsu		70.49.11	2[redacted]aa7

Mobistealth

Hello! demo (demo@mobistealth.com) | Logout

	Sender	Recipient	Subject	Received On
☑	support@mobistealth.com	juliant182@gmail.com	Upgrade link	2010-07-28 17:05:07
□	from.email@mobistealth.com	to.email@mobistealth.com	am out	2010-06-15 16:52:03
□	bob514@gmail.com	john.smith25@yahoo.com; kitty52@yahoo.com	Trip Pictures	2009-06-26 16:44:54
□	meeeerrs@gmail.com	sidewwwr@mail.com	Surprise for her	2009-04-29 11:58:54

1 - 4 of 4 items

Time 2010-07-28 17:05:07
From support@mobistealth.com
To juliant182@gmail.com
CC vagheera755@gmail.com
Subject Upgrade link

You have subscribed to our premium service. If you would like to upgrade your account please click on this link.

realtime-spy
monitor any pc - from anywhere.

your realtime-spy account information

Username: rtsuser

Password: testpassword

Enter your given username/password above to start configuring your Realtime-Spy logging module.

Visit http://realtime-spy.com/username to view your logs. If you do not know your login information contact us at support@realtime-spy.com

realtime-spy's logging options

☑ Log Keystrokes ☑ Log Documents Opened ☑ Log Print Jobs
☑ Log Applications Ran ☑ Log Internet Connections
☑ Log Conversations ☑ Log Websites Visited

splash warning option

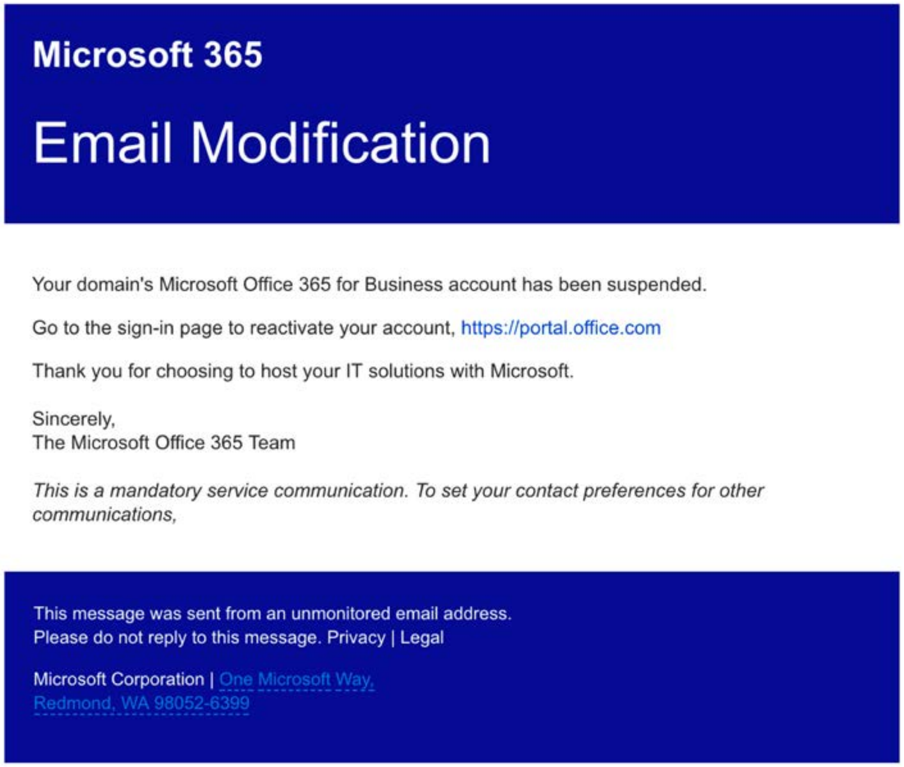
● Do not Alert User Realtime-Spy is running
○ Alert User Realtime-Spy is running

activity log clearing schedule

Clear Logs every 150 entries.
Logs will be cleared after the above number of entries are recorded.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Office 365



Microsoft 365

Email Modification

Your domain's Microsoft Office 365 for Business account has been suspended.

Go to the sign-in page to reactivate your account, https://portal.office.com

Thank you for choosing to host your IT solutions with Microsoft.

Sincerely,
The Microsoft Office 365 Team

This is a mandatory service communication. To set your contact preferences for other communications,

This message was sent from an unmonitored email address.
Please do not reply to this message. Privacy | Legal

Microsoft Corporation | One Microsoft Way,
Redmond, WA 98052-6399

RSAConference2019

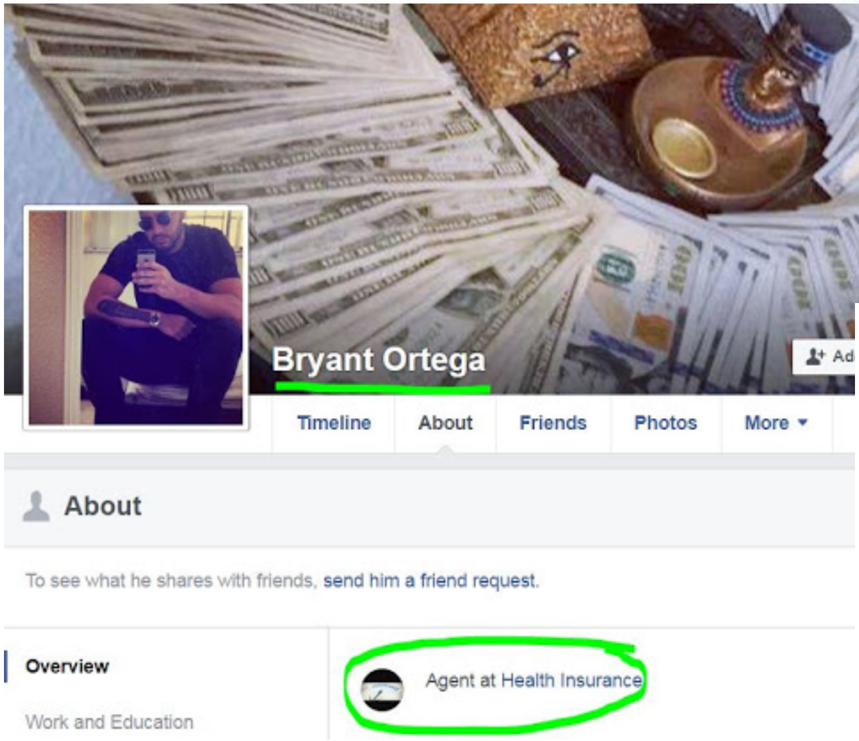
Operation Wire Wire & New Attack Vectors

International Business Email Compromise Schemes

Wire Wire Scam

- "BEC Hit List"
- Biggest losses compared to any other attack vector
- Billions of dollars lost
- 'Slimwaco' – CFO list of 200+ companies and 1000s of individuals targeted
- Global teams coordinating
- Over $600 million lost in BEC attacks

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.



Bryant Ortega

Timeline | About | Friends | Photos | More ▾

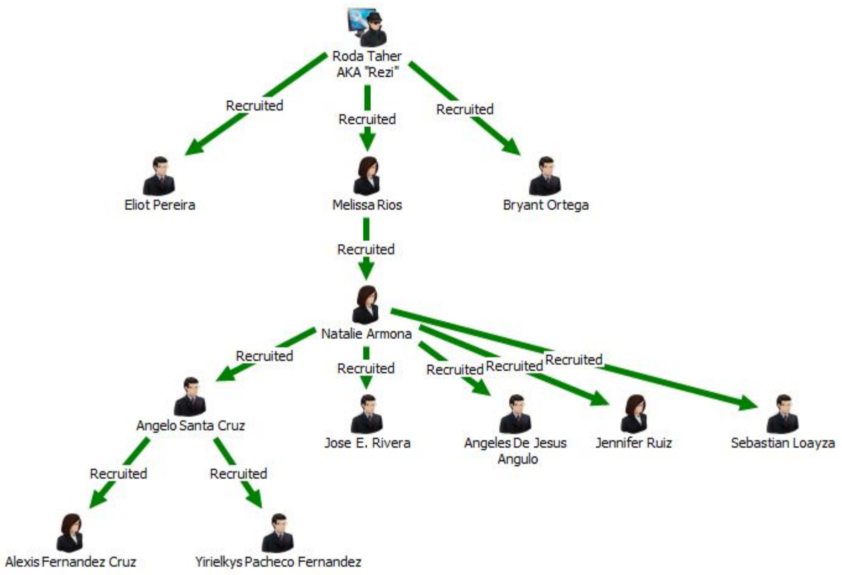
About

To see what he shares with friends, send him a friend request.

Overview

Work and Education

Agent at Health Insurance



Roda Taher AKA "Rezi"

Recruited → Eliot Pereira

Recruited → Melissa Rios

Recruited → Bryant Ortega

Melissa Rios Recruited → Natalie Armona

Natalie Armona Recruited → Angelo Santa Cruz

Natalie Armona Recruited → Jose E. Rivera

Natalie Armona Recruited → Angeles De Jesus Angulo

Natalie Armona Recruited → Jennifer Ruiz

Natalie Armona Recruited → Sebastian Loayza

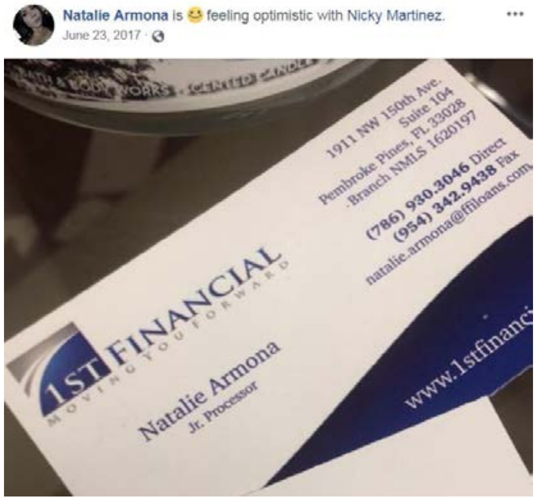
Angelo Santa Cruz Recruited → Alexis Fernandez Cruz

Angelo Santa Cruz Recruited → Yirielkys Pacheco Fernandez

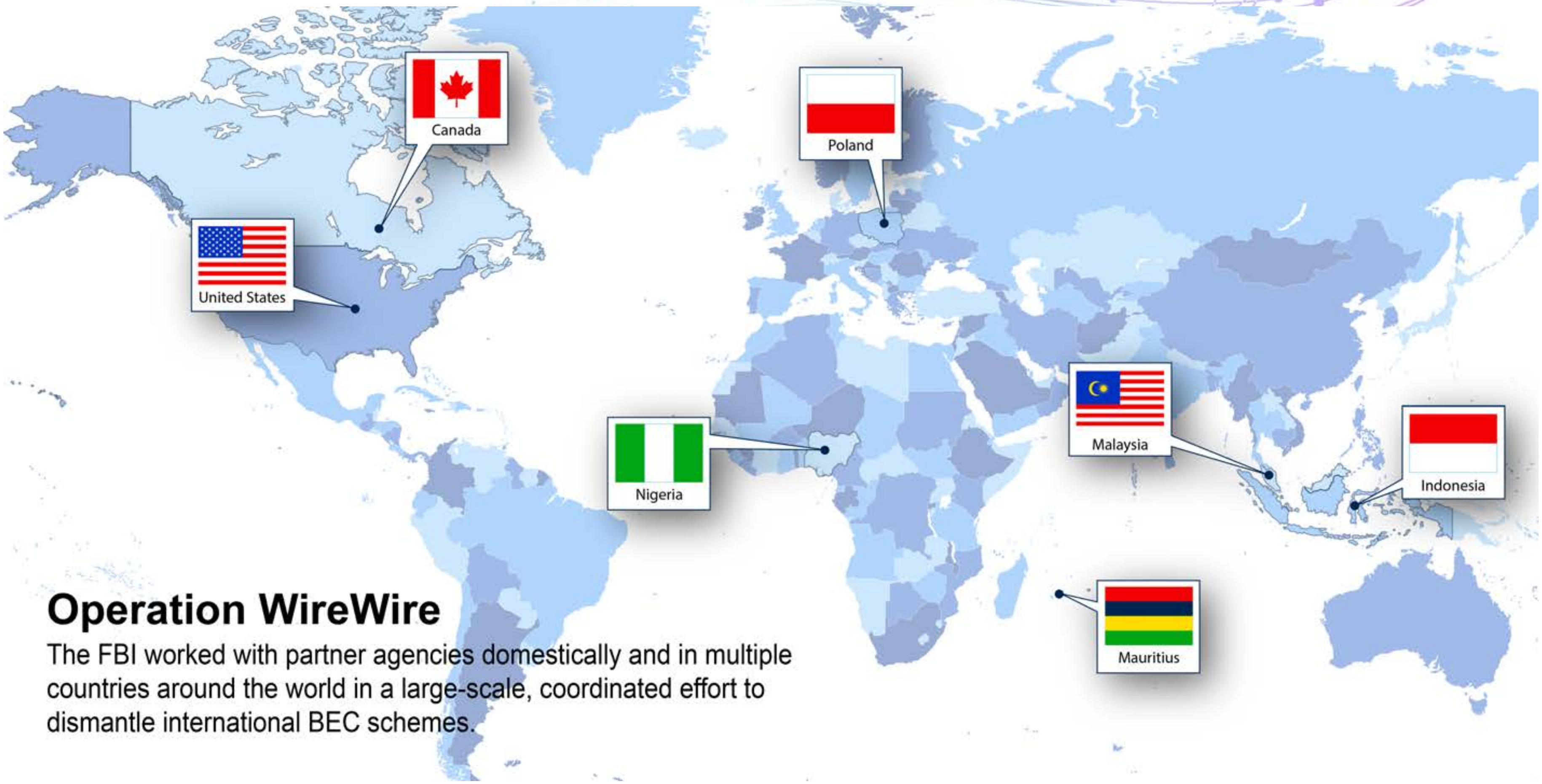
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Wire Wire Scam

- This case shows the increase in BEC target refinement
- “Huge Elite Limited" in Shanghai, China was the recipient of ill-gotten gains from Bryant Ortega.
- Natalie Armona was recruited having job as a Junior Processor at a lending firm



Natalie Armona is 😆 feeling optimistic with Nicky Martinez.
June 23, 2017 ·



Operation WireWire

The FBI worked with partner agencies domestically and in multiple countries around the world in a large-scale, coordinated effort to dismantle international BEC schemes.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Coordinated Takedown

- Several U.S. federal authorities and police from other countries were involved
- Six-month investigation that lead to arrests of suspected scammers in the U.S. and overseas.
- 74 arrests in all:
  - 42 arrested were located in the U.S.
  - 29 in Nigeria and
  - 3 in Canada, Mauritius, and Poland.
- $2.4 million seized
- $14 million recovered

The Wire Wire Scam

- The Operation
  - Not a sophisticated technological attack
  - Increased effort and workflow of actors
  - Robust social connections between these actors
- The Takedown
  - Global cooperation
  - BEC awareness
  - Reporting will increase

Wire Wire Targets

- Target Lists:
- Experian.com/small-business/mail-lists
- InfoUSA.com
- DatabaseUSA.com
- ReferYes.com
- Dark Web Marketplaces
- eGrabber.com

“Capture leads & prospects from any webpage, find & add any missing field (email/phone/...), update, de-dupe, merge & segment any prospect list”

Wire Wire Victim Profile

- Title companies
- Consulting firms
- IT Providers
- Legal Services
- Banks
- Transportation

Wire Wire Scenarios: Romance & Employment

- “Romance scams,” which lull victims to believe that their online paramour needs funds for an international business transaction, a U.S. visit or some other purpose
- “Employment opportunities scams,” which recruits prospective employees for work-from-home employment opportunities where employees are required to provide their PII as new “hires”
- Are significantly overpaid by check whereby the employees wire the overpayment to the employers’ bank

RSA®Conference2019

Defending Against BEC

International Business Email Compromise Schemes

Why is this a problem?

- Traditional security solutions rely on the following:
  - Anti-malware, Link Detection, Reputation, Content Analysis
- Messages are usually hand crafted
  - Little to detect
  - High reward warrants the additional effort

Security & Training Awareness is Flawed

- Should users be your first AND last line of defense?
- How diligent are your users?
- Training time = lost productivity?
- Ongoing training costs

Defending Against Scams

Awareness is key:

- Carefully scrutinize all emails
- Educate and train employees
- Verify vendors
- Know your customers
- Confirm requests
- Report it to the Internet Criminal Complaint Center (IC3) at: https://www.ic3.gov/default.aspx

Prevent Users Becoming Victims

- Identify similar domain names (abc_company.com != abc-company.com)
- Flag different 'Reply-To' address
- Color-code *internal* from *external* email
- Use 'known approved' details only
- Authenticate requests by phone
- Create 'two step' approval process for changes, much like 2fa

Technology Solutions

- Separate analysis of sender email(s), First part(s), Domain(s)
- Email message headers dynamic matching and scoring
- Implement SPF, DKIM, and DMARC at your organization
- Monitor VIP names most likely to be impersonated
- Visual spoofing detection engine,
  - e.g. apple != aqqle, Charm -> Charrn

Protect Accounts and Data

- Create intrusion detection system (IDS) rules that flag e-mails similar to company e-mail (*abc_company.com* would flag *abc-company.com)*
- Create e-mail rules to flag e-mail where the "reply" e-mail address differs from the "from" e-mail address
- Color code virtual correspondence (internal vs. external accounts)
- Verify changes in vendor payment location by adding 2fa
- Confirm requests for transfers of funds by using phone verification as part of a 2fa using only previously known numbers
- Carefully scrutinize all e-mail requests for transfer of funds

RSAConference2019

Apply

International Business Email Compromise Schemes

Key Indicators of BEC

- Large wire or funds transfer to a recipient the company has never dealt with in the past.
- Transfers initiated near the end of day (or cut-off windows) and/or before weekends or holidays.
- Receiving account does not have a history of receiving large funds transfers in the past.
- Receiving account is a personal account, whereas the company typically only sends wires to other businesses.

Strategies to Apply

- BEC attack awareness training for internal staff (Account Managers, BSA, Fraud, Wire Room, etc.)
- **Implement SPF, DKIM, and DMARC at your organization**
- Create a list of known good domains used by your organization and business partners, and use a domain name permutation algorithm to create a list of similar domain names
- Create a network or email policy to block recently registered domains

Summary

- Traditional BEC methods (still successfully used)
  - Bogus Invoice
  - CEO Fraud
  - Social Engineering
  - Account Compromise
  - Attorney Impersonation
- BEC workflow and attack vectors are improving and expanding:
  - Large quantities of data exposure leaves people vulnerable
  - Actors are leveraging the data exposure, combining it with multiple sources, and are able to both refine and expand target lists
  - BEC is easy to execute and on the rise

If You Want to Know More

- https://www.fbi.gov/news/stories/business-e-mail-compromise
- https://www.IC3.gov
- https://www.ic3.gov/media/2016/160614.aspx
- https://www.cisecurity.org/press-release/national-isacs-fbi-uss-and-symantec-collaborate-to-fight-business-email-compromise/

RSAConference2019

Thank you!
Questions?

Anne Connell

aconnell@cert.org