Disrupting the BEC Kill Chain: Fighting BEC Attacks

Patrick Peterson
Founder & CEO
Agari
@Peterson_Agari

Teresa Walsh
Global Head of Intelligence
FS-ISAC
Patrick Peterson
Founder & CEO
Agari

Teresa Walsh
Global Head of Intelligence
FS-ISAC
BEC: A Rapidly Growing Threat

BEC is a $139 million per month problem!

Source: 2019 FBI IC3 Alert
BEC losses grew by 37%

40% of all losses attributed to BEC
From: Patrick Peterson <chiefexecutiveofficer@gmail.com>
To: Raymond Lin <rlim@agari.com>

Subject: Invoice Payment

Are you in the office?
Patrick Peterson

Sent from my U.S. Cellular® Smartphone

An “Incident” in our Parlance
BEC “Baiting” Response

From: Raymond Lin <rlim@agari.com>
To: Patrick Peterson <chiefexecutiveofficer@gmail.com>

Subject: Re: Invoice Payment

Yes. What do you need?
Raymond

Engaging the Fraudster
BEC Criminal Requests Wire, Reveals Valuable Asset

From: Patrick Peterson <chiefexecutiveoofficer@gmail.com>
To: Raymond Lin rlim@agari.com

Subject: Re: Invoice Payment

Process a wire transfer in the amount of $44,960 with the wire instructions below.
Bank: JP Morgan Chase Bank
Bank Address:
Beneficiary: M****n W****s
Account Number: 86******88
Route Number:

Let me know once wire transfer is completed.
Regards,
Patrick Peterson

A Mule Account in our parlance
What is Business Email Compromise (BEC)

Financially motivated email-based identity deception
- BEC uses numerous cash out methods: Wire, SWIFT, Payroll, gift card
- Same techniques used for information theft

Email-based
- Email spoofing
  From: Patrick Peterson  <chiefexecutiveoofficer@gmail.com>
- Domain imitation
  From: Patrick Peterson  <ppeterson@aqari.com>
- Email compromise
  From: Patrick Peterson  <ppeterson@agari.com>

Email + Telephony based
Why is BEC Such a Problem?

- Traditional defenses focus on technical threats
- BEC has a higher ROI than other cyber attacks
- Social engineering is extremely effective
How Do We Fight BEC?

- By sharing fraud information, banks can stop future crime (to an extent)
  - Banks with mule accounts can investigate
  - Other banks can identify fraud transactions
  - Banks can use the fraud indicators to prevent future fraud transactions appropriately

- Effective but relies on confirmed fraud that’s already happened

- Targeting at BEC fraud before it happens currently
  - Education
  - Controls
  - Sharing

- Sliding further left of the Kill Chain, how do we fight BEC before it happens?
We know a lot about the BEC attack chain and the actors behind these attacks...

...and we can use this intelligence to defeat them!
A Look at the BEC Attack Chain

1. Target Generation
2. Lead Validation & Processing
3. Pre-Attack Testing
4. BEC Attack
How They select their targets

leadiQ

hunter

SalesRipe

Prospect.io

INTEL IUS
#RSAC

How BEC Groups Select Targets

<table>
<thead>
<tr>
<th>WORK EMAIL</th>
<th>EMAIL STATUS</th>
<th>NAME</th>
<th>TITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:hr2_chimulick@discovery.com">hr2_chimulick@discovery.com</a></td>
<td>Verified</td>
<td>Yitz Shenkowitz</td>
<td>CFO, Global Digital</td>
</tr>
<tr>
<td><a href="mailto:lfpop@osteocortex.co.uk">lfpop@osteocortex.co.uk</a></td>
<td>VerifiedLikely</td>
<td>Bill Covey</td>
<td>Group CFO</td>
</tr>
<tr>
<td>tom)<a href="mailto:davison@network-atm.co.uk">davison@network-atm.co.uk</a></td>
<td>NotVerified</td>
<td>Tom Davison</td>
<td>Interim CFO</td>
</tr>
<tr>
<td><a href="mailto:michael.evans@powerleague.com">michael.evans@powerleague.com</a></td>
<td>NotVerified</td>
<td>Michael Evans</td>
<td>CFO</td>
</tr>
<tr>
<td><a href="mailto:david.pippin@nfi.co.uk">david.pippin@nfi.co.uk</a></td>
<td>VerifiedLikely</td>
<td>David Pippin</td>
<td>CFO</td>
</tr>
<tr>
<td><a href="mailto:kevin.taylor@access.com">kevin.taylor@access.com</a></td>
<td>NotVerified</td>
<td>Kevin Taylor</td>
<td>CFO &amp; Treasurer</td>
</tr>
<tr>
<td><a href="mailto:cliff.roth@smartlink.co.uk">cliff.roth@smartlink.co.uk</a></td>
<td>Verified</td>
<td>Cliff Roth</td>
<td>CFO</td>
</tr>
<tr>
<td><a href="mailto:robinson@landwerfer.com">robinson@landwerfer.com</a></td>
<td>Verified</td>
<td>Matthew Robinson</td>
<td>CFO</td>
</tr>
<tr>
<td><a href="mailto:david.pipes@heen.com">david.pipes@heen.com</a></td>
<td>NotVerified</td>
<td>David Pipes</td>
<td>CFO</td>
</tr>
<tr>
<td><a href="mailto:kademon@soon.org">kademon@soon.org</a></td>
<td>Verified</td>
<td>Don Kademon</td>
<td>Sr. VP &amp; CFO</td>
</tr>
<tr>
<td><a href="mailto:jeff.humen@vertrac.com">jeff.humen@vertrac.com</a></td>
<td>Verified</td>
<td>Jeff Humen</td>
<td>CFO/Controller</td>
</tr>
<tr>
<td><a href="mailto:lor@cco.com">lor@cco.com</a></td>
<td>VerifiedLikely</td>
<td>Lori Vass</td>
<td>VP of Admin &amp; CFO</td>
</tr>
</tbody>
</table>
Validating Targets

Curious Orca

- Verifying targets using bank probe emails sent during non-work hours
- Looking for an automated “bounce” message
  - No bounce = valid email
  - Bounce = invalid email
- For invalid addresses, scammer iterates through various username combinations
Visibility Into the BEC Attack Chain

- January 11, 2019 – targeting data for 500+ CA financial executives collected via LeadIQ
- January 13, 2019 – targeting data sent distributed for processing (validation, organization, augmentation)
- January 22, 2019 – processed leads sent back to primary actor
- January 28, 2019, 17:00 – pre-campaign test email sent from attack email account to test account
- January 28, 2019, 20:30 – attack email targeting Agari CFO intercepted

BEC Attack Cycle = 17 days
Vendor Email Compromise (VEC)

1. A criminal sends a targeted phishing email.
2. The recipient clicks on the link and is directed to a phishing website.
3. The recipient of the targeted email enters his or her credentials into the website.
4. The cybercriminal uses those credentials to set a forwarding rule to send copies of all emails to his own inbox.
5. The cybercriminal monitors the inbox to obtain information about invoices, payments, and other financial details.
6. When the opportunity arises, the cybercriminal uses his intel to send a fake invoice to the organization’s customer, informing the customer of new banking details.
7. Not realizing that the email is fake, the customer pays the invoice, depositing money directly into the cybercriminal’s bank account.
Active Defense Uses Low Impact Gray Zone

PASSIVE DEFENSE
Basic security controls, firewalls, antivirus, patch management, scanning and monitoring, etc.

EMAIL FILTERS TRAINING

ACTIVE DEFENSE: THE GRAY ZONE
BEC Automated Deception System
B54 Citadel

Requires Close Government Cooperation

Lower Impact/Risk
Higher Impact/Risk

OFFENSIVE CYBER
Hacking back/operations intended to disrupt or destroy external networks or information without authorizations, etc.

GENERALLY ILLEGAL

From: George Washington University Center for Cyber & Homeland Security “Into the Gray Zone: Active Defense by the Private Sector against Cyber Threats”
Scaling Active Defense For Intelligence Collection

- Automated BEC engagement and notification system
  - Crafts an email thread using only the attacker email and subject
  - 65% response rate
  - Financial Institutions and email providers notified in real-time

- Scales BEC intelligence collection
  - 6,000+ engagements since May 2019
  - 2,100+ mule accounts collected
BEC Fraud Intelligence Sharing Overview

1. "Incidents" reported to Agari ACID from multiple sources
2. ACID “baits” fraudster to extract mule accounts
3. Standardized incident and mule account intelligence CSV sent to FS-ISAC
4. FS-ISAC distributes intelligence to members
5. 7000+ FS-ISAC members + law enforcement agencies receive actionable intelligence

ACID = Agari Cyber Intelligence Division

Participating Institutions

BEC Email List

ACID

FS-ISAC

AGARI

EÚROPOL

Justice Department
Stopping Fraud **Before It Happens**

- Acting on “fresh” money mules helps stop fraud before the transfer happens
  - Contributes to analysis on recruiting trends and cashout methods
- Relying on the external sourcing from Agari helps overcome various challenges for banks
  - There are barriers to sharing today bank-to-bank
  - Measuring the success of this sharing against BEC can demonstrate the value mule sharing can bring
- FS-ISAC can help overcome those barriers to sharing, using value added intelligence to stop fraud and protect customers
BEC Group Matrix

London Blue
UK-Based Multinational Gang Runs BEC Scams Like a Modern Corporation

Scarlet Widow
Nigerian-Based BEC Scammer Group Targets Nonprofits and Schools; Launder Stolen Gift Cards

Silent Starling
The Emergence of Vendor Email Compromise and Its Impact on the Global Supply Chain

Exaggerated Lion
Leveraging G Suite and a Nationwide Check Mule Network to Build a Prolific BEC Operation
Stop by the Agari Booth
South Hall #1627  |  North Hall #6553

Get a Copy of the Exaggerated Lion Report
agari.com/exaggerated-lion

View Technical Demos

FS-ISAC
www.fsisac.com

Join Us! membership@fsisac.com
Members - leverage our BEC Fraud Intelligence!
Thank You
Patrick Peterson
CEO & Founder, Agari
acid@agari.com

Teresa Walsh
Global Head of Intel, FS-ISAC