RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: AFD-W09

Disrupting the BEC Kill Chain: Fighting BEC Attacks

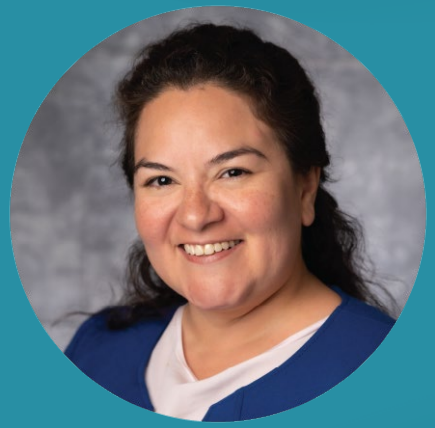
Patrick Peterson
Founder & CEO
Agari
@Peterson_Agari

Teresa Walsh
Global Head of Intelligence
FS-ISAC

RSAConference2020

Patrick Peterson

Founder & CEO
Agari



Teresa Walsh

Global Head of Intelligence
FS-ISAC

RSAConference2020

BEC: A Rapidly Growing Threat

BEC is a $~~1~~~~0~~~~0~~ million per month problem!

Source: 2019 FBI IC3 Report

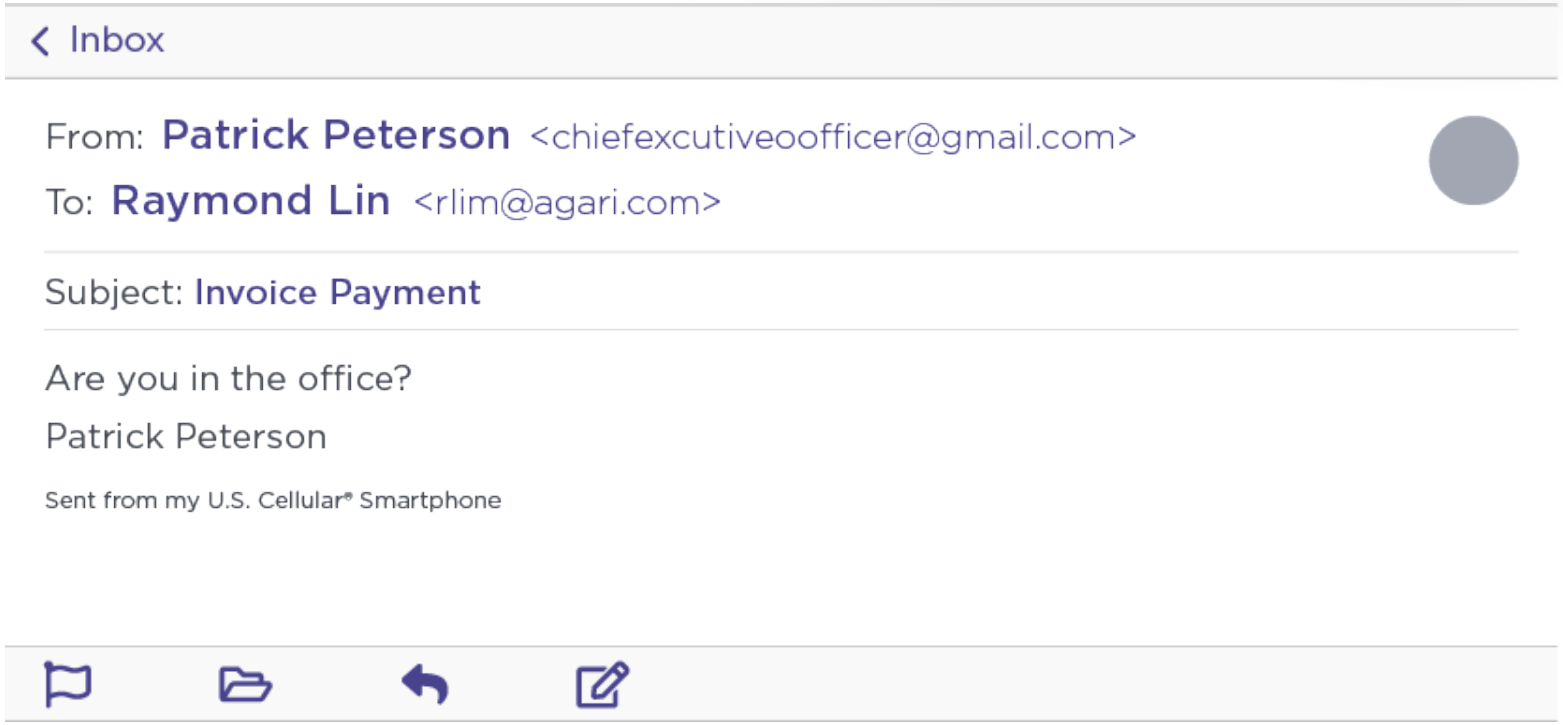
RSAConference2020

2020 Breaking News

BEC losses grew by 37%

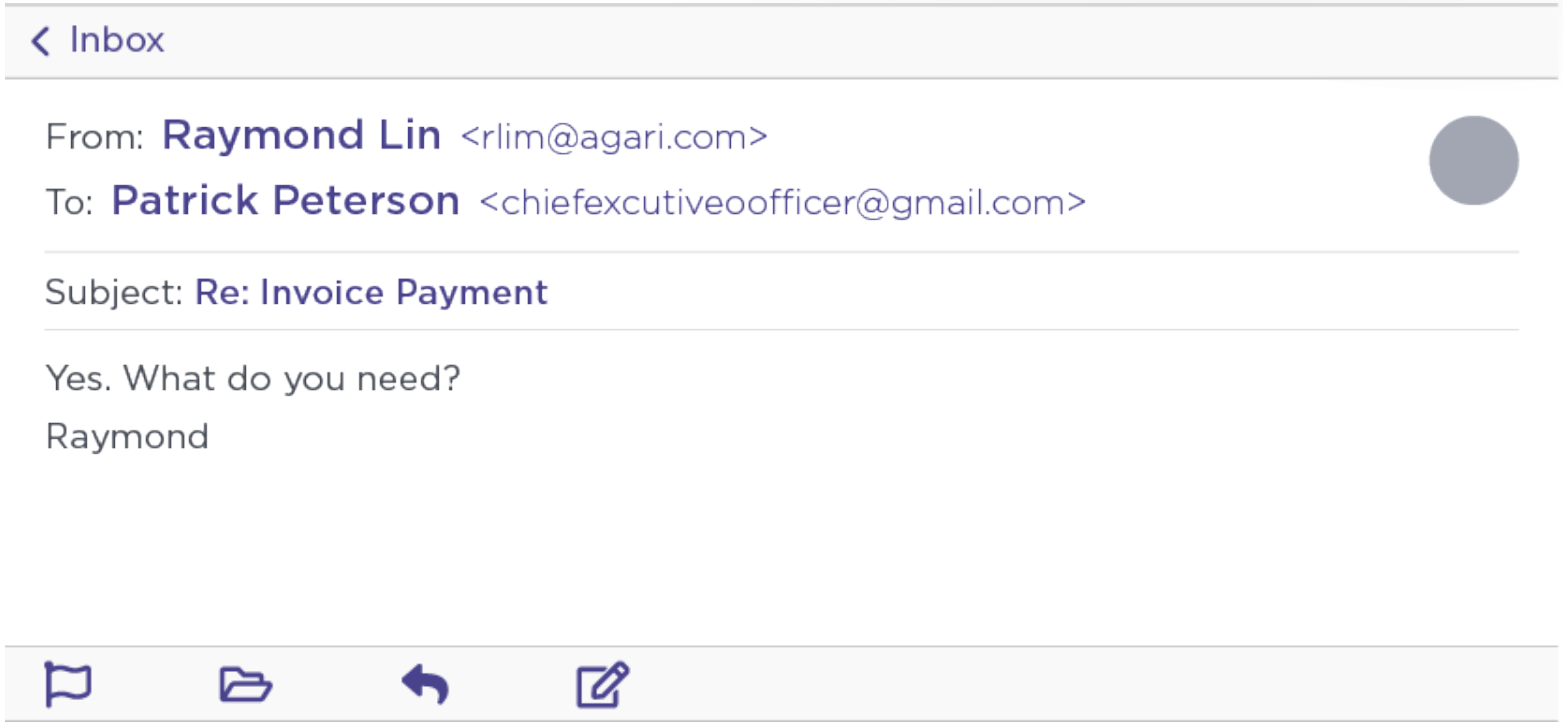
40% of all losses attributed to BEC

BEC Email to Agari



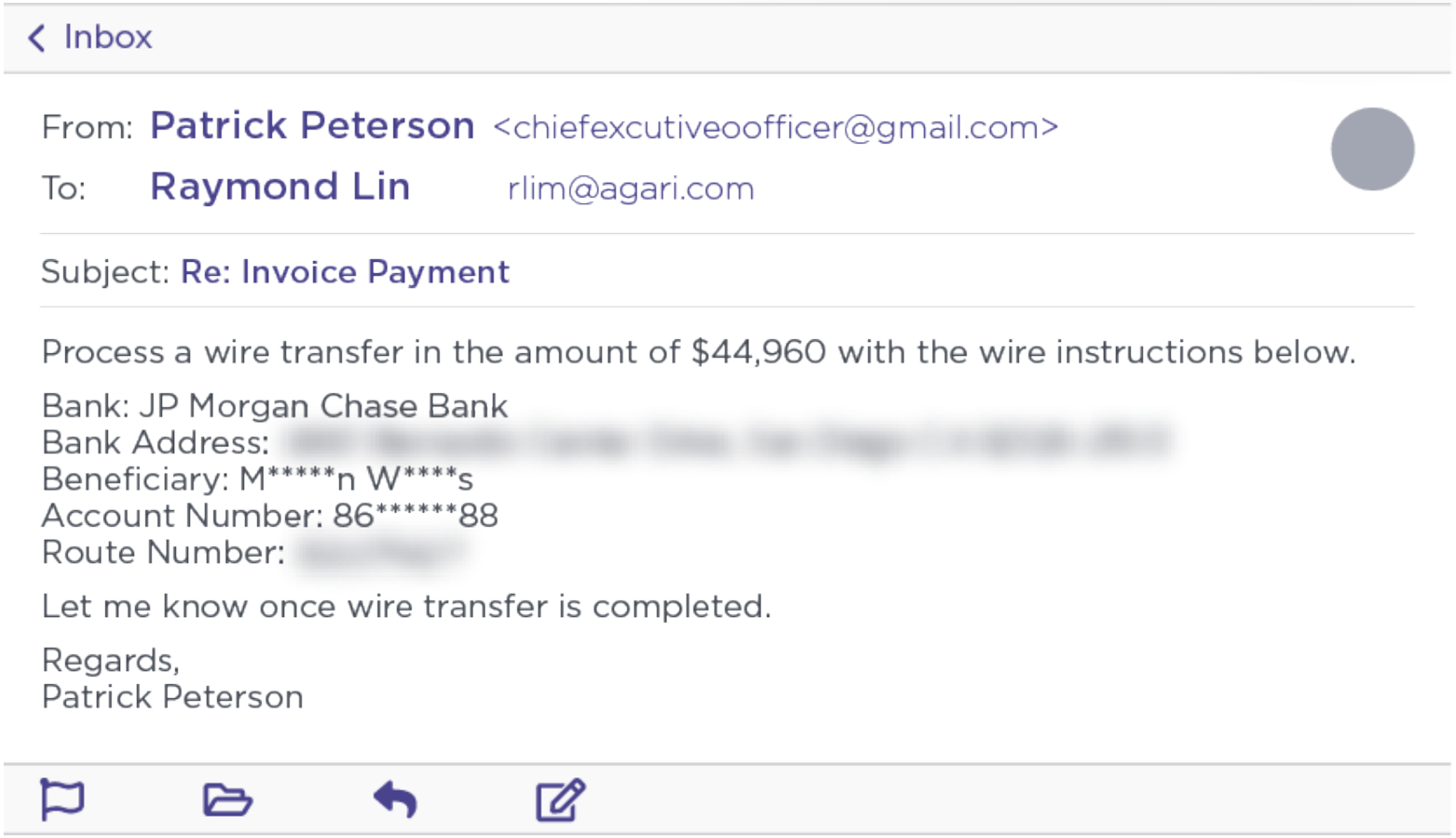
An “Incident” in our Parlance

BEC "Baiting" Response



Engaging the Fraudster

BEC Criminal Requests Wire, Reveals Valuable Asset



Inbox

From: **Patrick Peterson** <chiefexcutiveoofficer@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: [redacted]
Beneficiary: M*****n W****s
Account Number: 86******88
Route Number: [redacted]

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

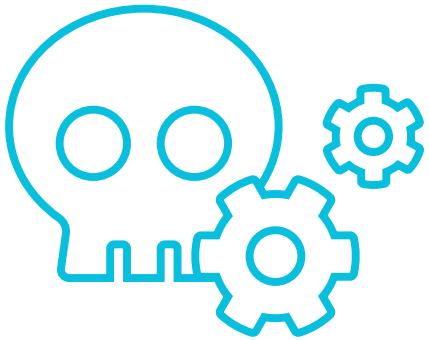
- BEC uses numerous cash out methods: Wire, SWIFT, Payroll, gift card
- Same techniques used for information theft

Email-based

- Email spoofing — From: Patrick Peterson <chiefexcutiveofficer@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?

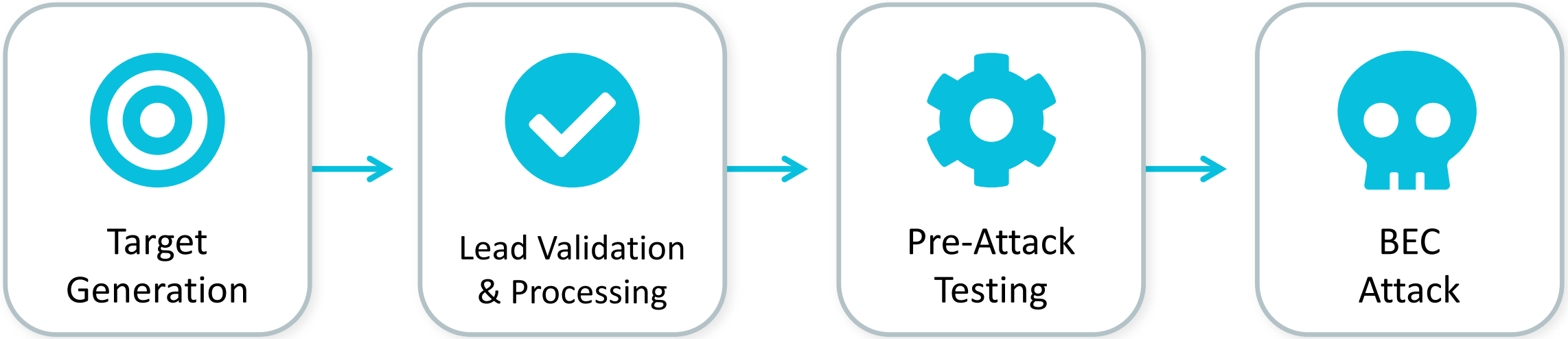
- By sharing fraud information, banks can stop future crime (to an extent)
  - Banks with mule accounts can investigate
  - Other banks can identify fraud transactions
  - Banks can use the fraud indicators to prevent future fraud transactions appropriately
- Effective but relies on confirmed fraud that's 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?

RSAConference2020

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



How They select their targets

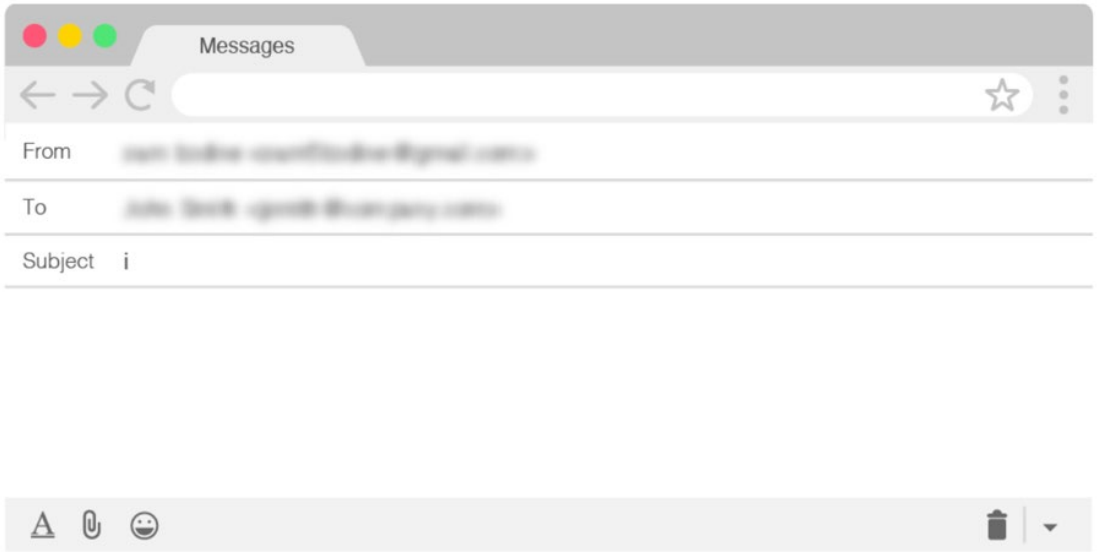
How BEC Groups Select Targets

WORK EMAIL	EMAIL STATUS	NAME	TITLE
[redacted]	Verified	[redacted]	CFO, Global Digital
[redacted]	VerifiedLikely	[redacted]	Group CFO
[redacted]	NotVerified	[redacted]	Interim CFO
[redacted]	NotVerified	[redacted]	CFO
[redacted]	VerifiedLikely	[redacted]	CFO
[redacted]	NotVerified	[redacted]	CFO & Treasurer
[redacted]	Verified	[redacted]	CFO
[redacted]	Verified	[redacted]	CFO
[redacted]	NotVerified	[redacted]	CFO
[redacted]	Verified	[redacted]	Sr. VP & CFO
[redacted]	Verified	[redacted]	CFO/Controller
[redacted]	VerifiedLikely	[redacted]	VP of Admin & CFO

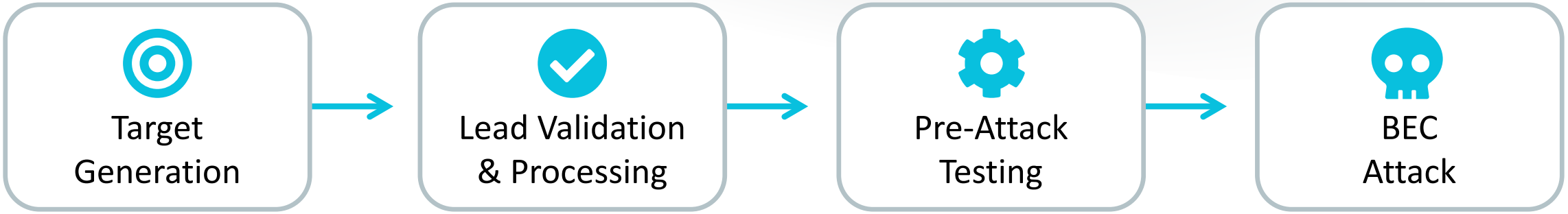
Validating Targets

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

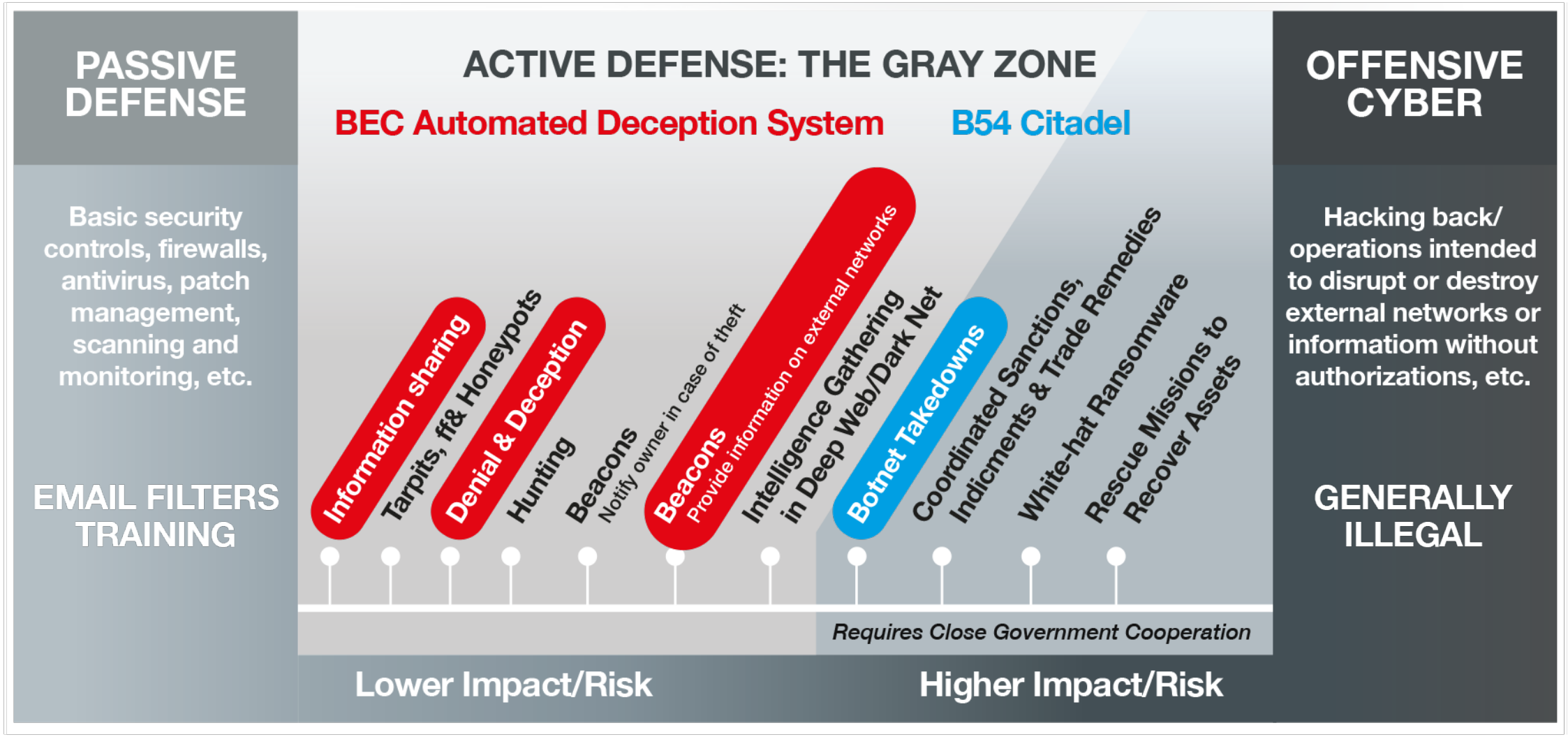


- January 11, 2019 – targeting data for 500+ CA financial executives collected via LeadIQ
- January 13, 2019 – targeting data sent distributed for processing (validation, organization, augmentation)
- January 22, 2019 – processed leads sent back to primary actor
- January 28, 2019, 17:00 – pre-campaign 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)

Active Defense Uses Low Impact Gray Zone

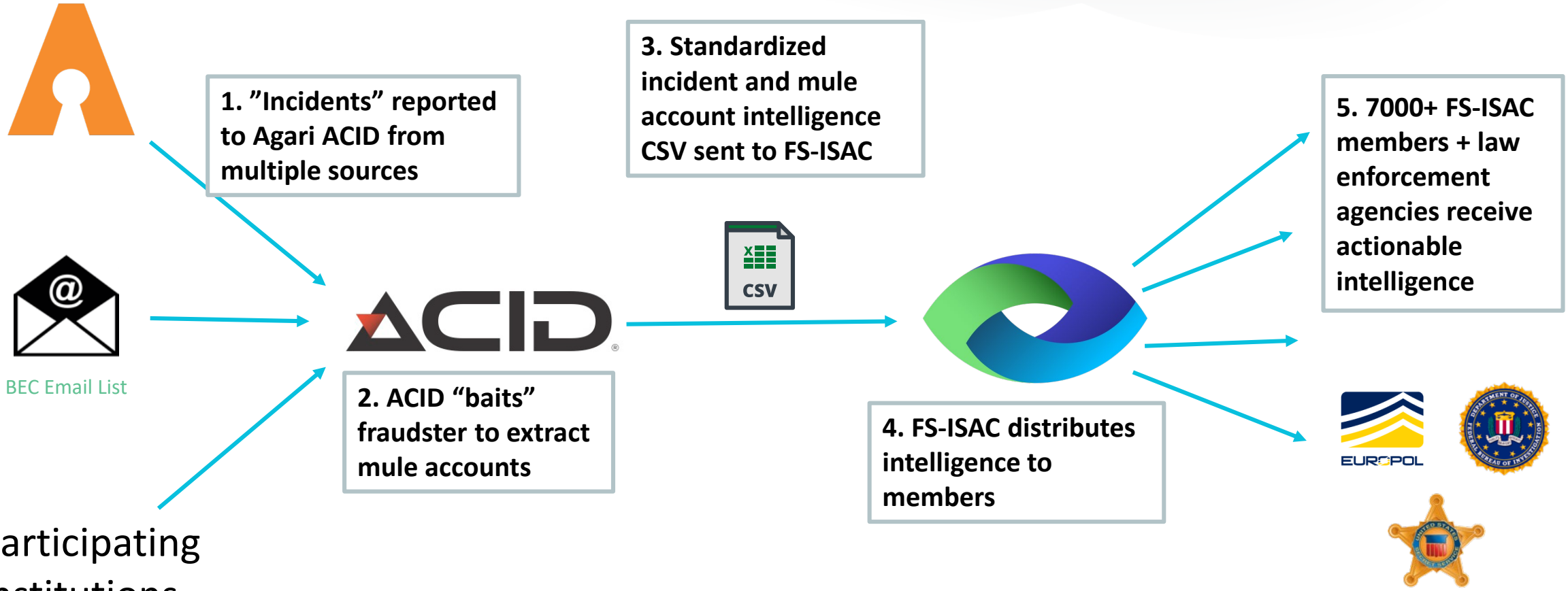


From: George Washington University Center for Cyber & Homeland Security "Into the Gray Zone: Active Defense by the Private Sector against Cyber Threats"

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



ACID = Agari Cyber Intelligence Division

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

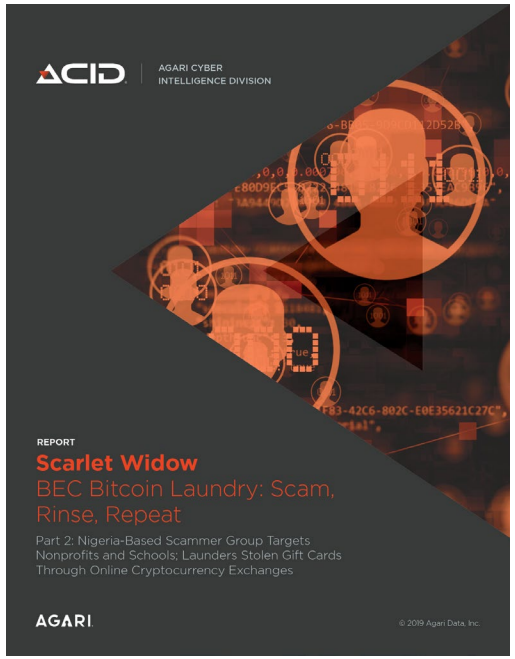
BEC Group Matrix

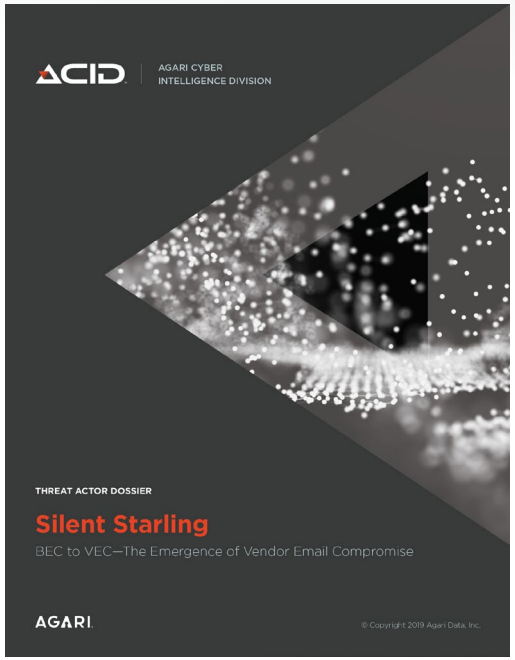
London Blue

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

Scarlet Widow

Nigerian-Based BEC Scammer Group Targets Nonprofits and Schools; Launders Stolen Gift Cards



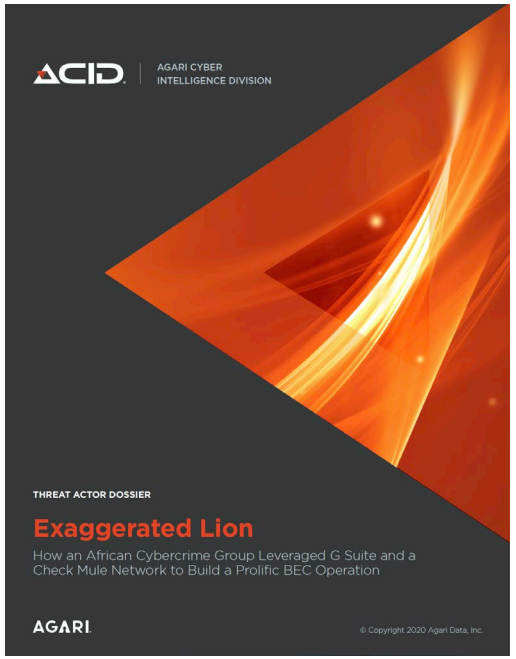


Silent Starling

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



RSAConference2020

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!

AGARI | FS-ISAC

RSAConference2020

Thank You

Patrick Peterson
CEO & Founder, Agari
acid@agari.com

Teresa Walsh
Global Head of Intel, FS-ISAC