

RSAConference2022

San Francisco & Digital | June 6 – 9

SESSION ID: AFD-M03

BEC & Ransomware: Two Sides of the Same Cybercrime Coin

Crane Hassold

Director of Threat Intelligence
Abnormal Security
@CraneHassold

TRANSFORM



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

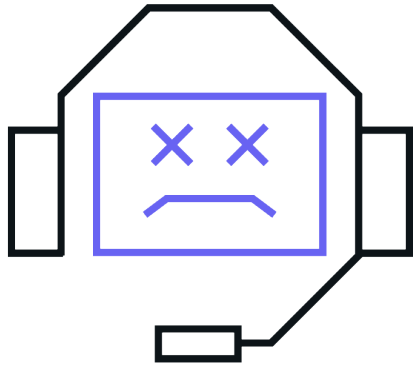


RSA®Conference2022

Ransomware: The Visible Menace



Three Primary Factors Driving Today's Ransomware Landscape



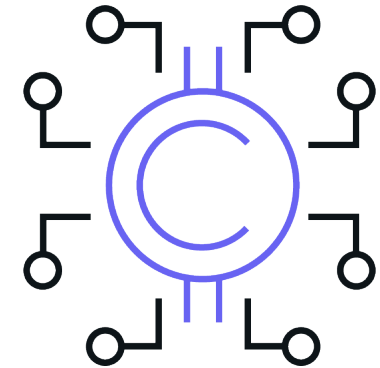
Ransomware-as-a-Service

(Access)



Extortion

(Incentive)

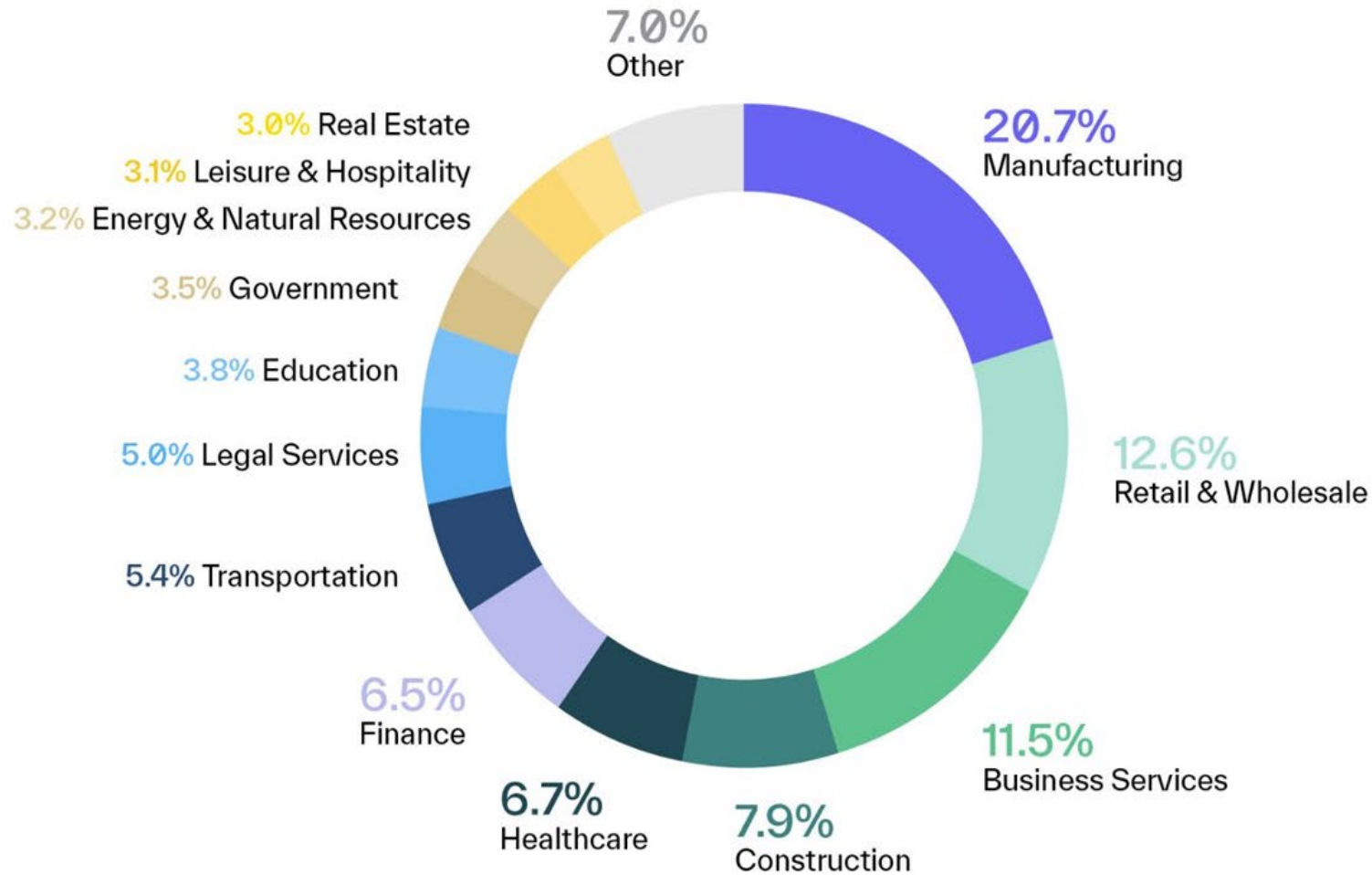


Cryptocurrency

(Scale)

Ransomware is Industry Agnostic

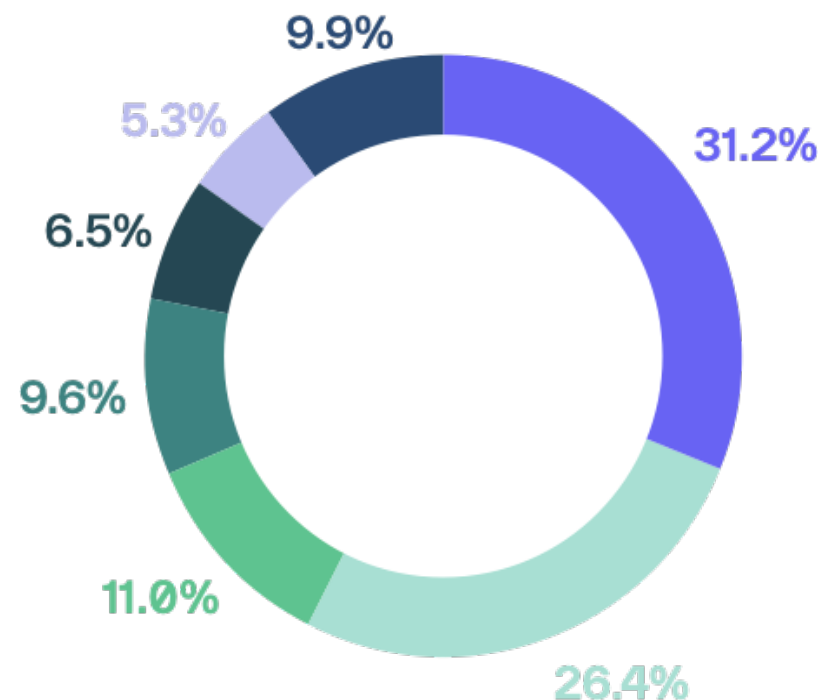
(But Some Industries Get More Attention Than Others)



The Myth of the Big Fish

Median Annual Revenue
of a Ransomware Victim:

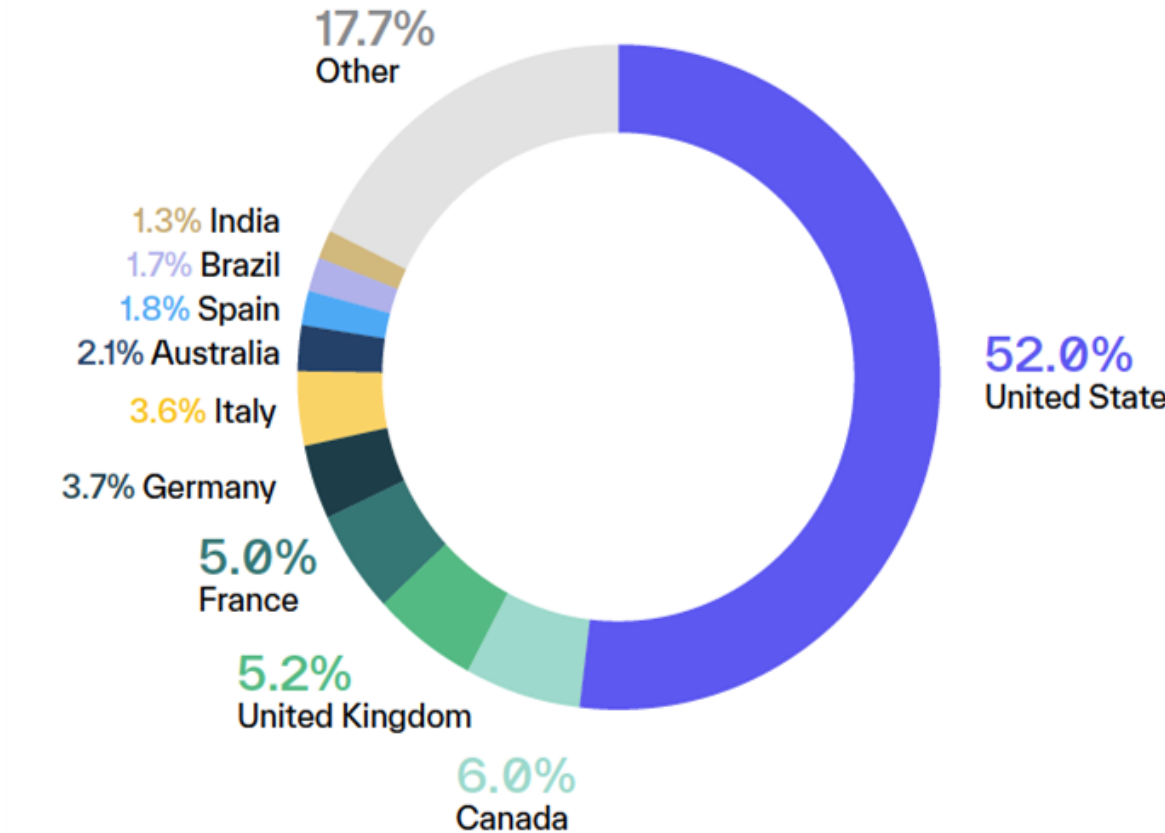
\$27 Million



Source: 2022 Abnormal Ransomware Victimology Report

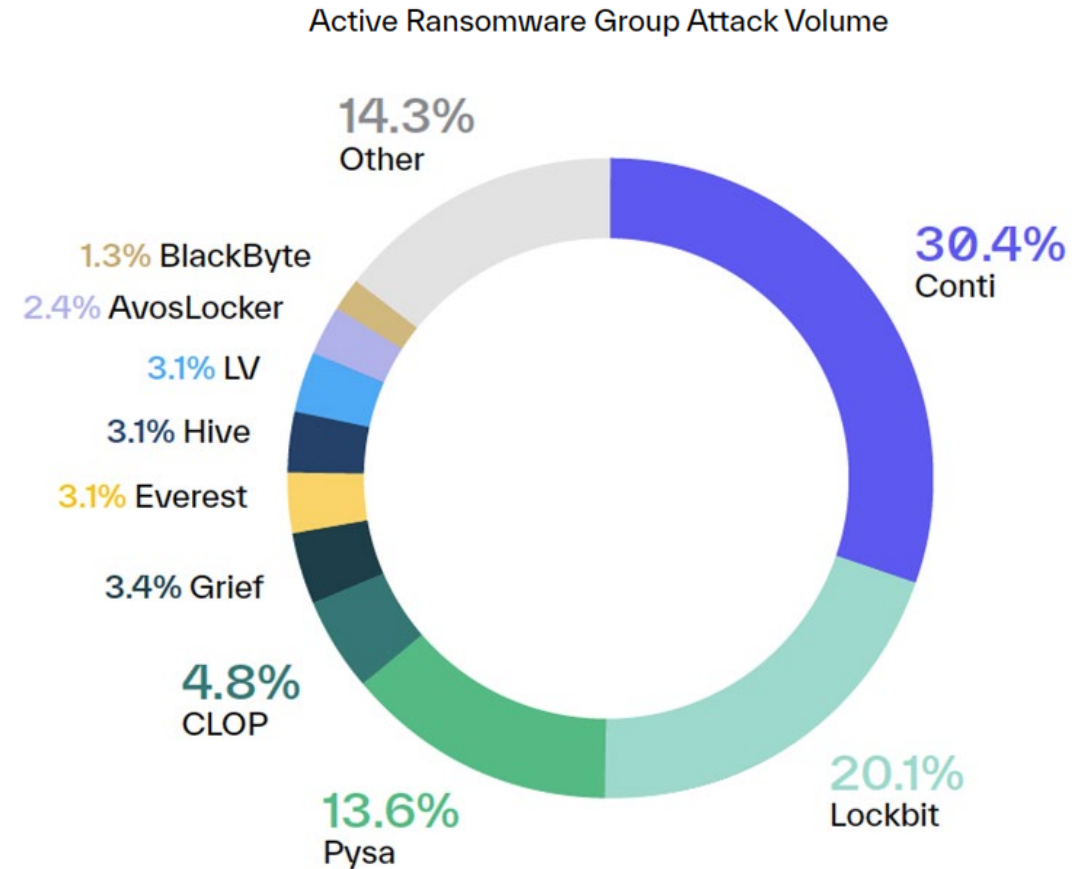
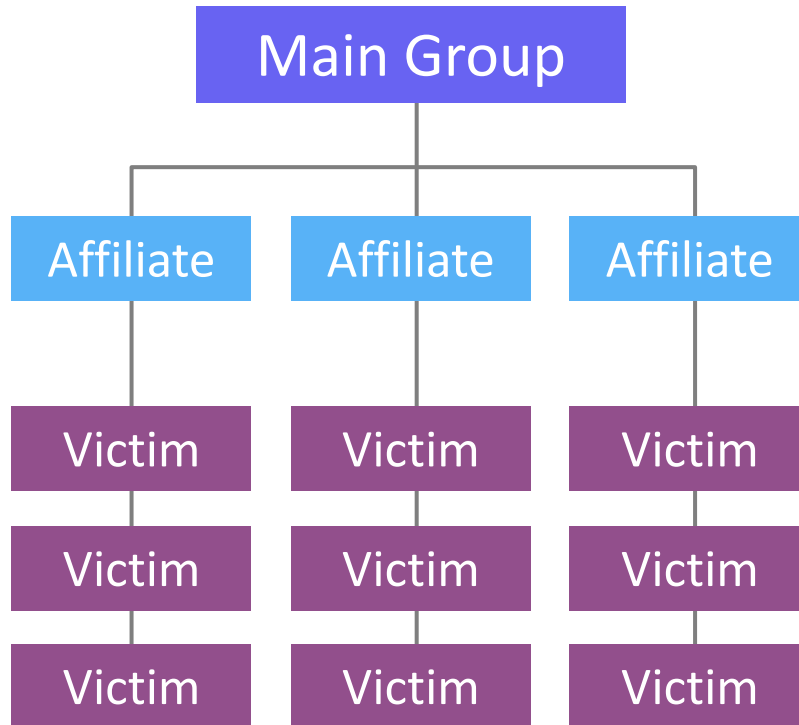
A Global Problem

(With One Giant Void)



Source: 2022 Abnormal Ransomware Victimology Report

Ransomware is a Centralized Ecosystem



Source: 2022 Abnormal Ransomware Victimology Report

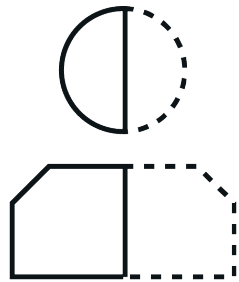
RSA®Conference2022

Business Email Compromise: The Silent Threat

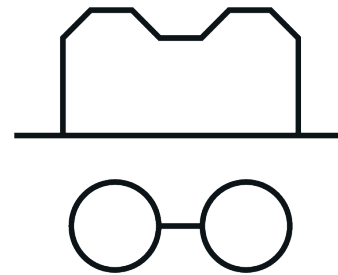


What is Business Email Compromise?

A spear phishing attack that involves the impersonation of a trusted individual to trick a person into making a financial transaction or sending sensitive materials.



Spoofing



Compromise

BEC: By the Numbers

\$43B+

lost since 2016

\$180,000+

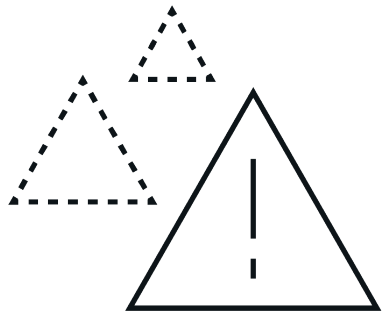
lost per attack

35%

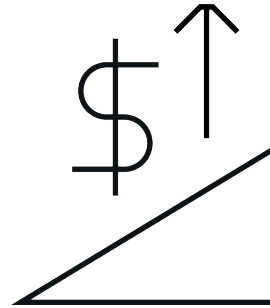
of all cybercrime losses

Source: FBI Internet Crime Complaint Center (IC3)

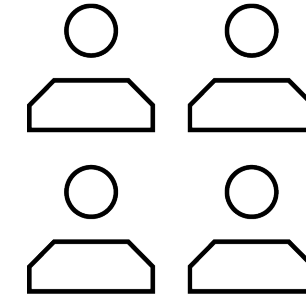
Why is BEC Such a Problem?



Traditional defenses focus on **technical threats**.

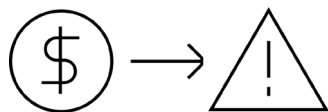


BEC has a **higher ROI** than other cyber attacks.



Social engineering is extremely effective.

Executive Impersonation: The Classic BEC Attack



Wire Transfer

From: Reed Richards sgtrock@hvc.rr.com 5/9/22, 2:40PM
Subject: Re: Wire Payment
To: Sue Storm sue.storm@fantasticfour.org

Hi Sue,

I need you to process a wire transfer or an ACH payment to a consultant today. Are you available to take care of this now so I can send details?

Best Regards,

Reed



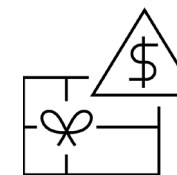
Payroll Diversion

From: Hank Pym <admin@mycompanymail.page> 5/17/22, 9:13AM
Subject: **Re: Direct Deposit Update**
To: Janet Van Dyne <jvdyne@pymtechnologies.com>

Hi Janet,

I need to change my direct deposit info on file before the next payroll is processed. Can you get it done for me?

Regards,
Hank

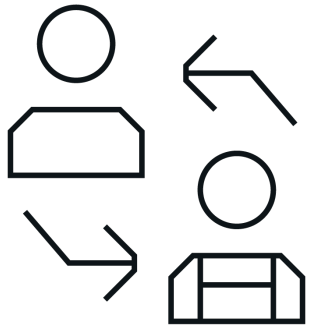


Gift Cards

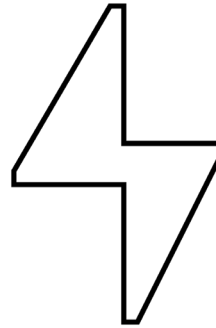
From: Jean Gray <personalmailbox667@gmail.com> 5/1/22, 6:21PM
Subject: **Re: Response**
To: Scott Summers <scott.summers@xavierinstitute.org>

Great, I'm having a busy day and I trust I can count on you to keep this as a surprise. I'm looking forward to surprising some of the staff with gift cards, And i want this to be between you and I pending when they receive it. Are you able to purchase on my behalf quickly and what local store do you think we have around to make this purchase? I'm considering a One Vanilla gift card, American Express gift card or an eBay gift card Since we have it almost everywhere.

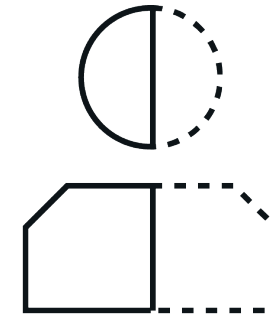
Financial Supply Chain Compromise: Today's Biggest BEC Threat



Vendor Email
Compromise

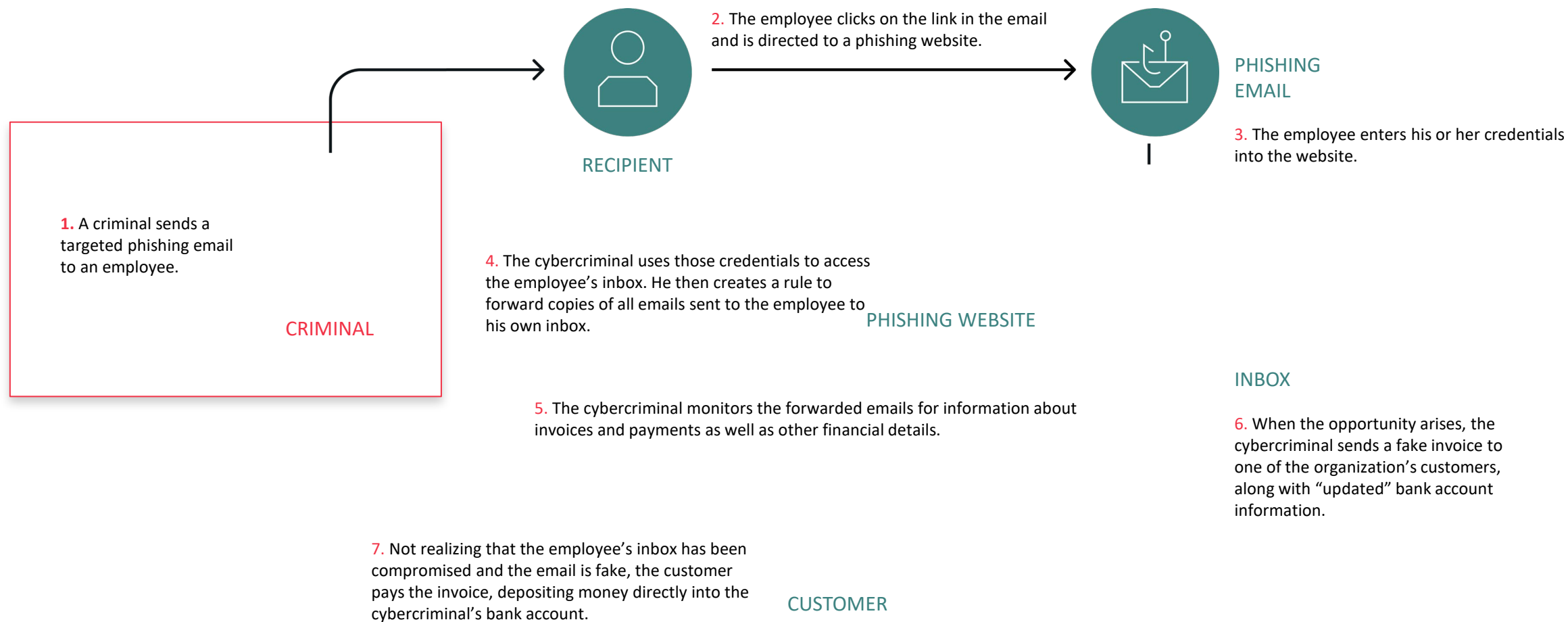


Aging Report
Attacks



Third-Party
Impersonation

Vendor Email Compromise: Today's Biggest BEC Threat



Aging Report Attacks: VEC (Without the Compromise)

#RSAC

From: Pepper Potts <fakeceo@gmail.com> 4/22/22, 8:45AM
Subject: **Re: AR REPORT**
To: Tony Stark <tony.stark@starkindustries.com>

Tony,

I need you to email me the aging report from A/R (Due within the next 30 days and a month overdue), and also include customer payable contact email on this report.

Regards,
Pepper

From: Tony Stark <tony.stark@starkindustries.com> 5/2/22, 9:22AM
Subject: **Follow up – ACME Corporation USD \$86,801.80**
To: Steve Rogers <steve.rogers@acme.com>

Hi Steve,

Natasha, our CFO asked me to follow up with you on our payment status. Please let us know if you have any payment to remit to us.

Kindly note that our office has recently made changes to our remittance information and we advise all our payments to be remitted to our banking information via ACH, direct deposit or wire transfer only moving forward. We would provide you with our revised remittance information for proper update and payment processing.

I await your soonest response.

Thanks,

Tony

Vendor	Current	1-30 Days	31-60 Days	60-90 Days	Outstanding Balance	POC	Email
ACME Corporation	\$86,801.80	-	-	-	\$86,801.80	Steve Rogers	steve.rogers@acme.com
Advanced Idea Mechanics	\$94,843.70	\$133,089.90	\$85,728.85	\$83,091.35	\$396,753.80	Baron von Strucker	bvstrucker@aim.com
Hammer Industries	\$42,701.50	-	-	-	\$42,701.50	Justin Hammer	justin.hammer@hammer.com
Oscorp Industries	\$76,385.20	\$41,013.10	-	-	\$213,670.45	Norman Osborn	nosborn@oscorp.com
Pym Technologies	\$51,494.50	\$50,257.20	\$122,667.70	-	\$224,419.40	Hank Pym	hank.pym@pymtech.com
Daily Bugle	\$132,171.25	\$104,176.00	-	-	\$236,347.25	Jonah Jameson	jjjameson@dailybugle.com
TOTAL OUTSTANDING	\$484,397.95	\$328,536.20	\$208,396.55	\$83,091.35	\$1,200,694.20		

Third-Party Impersonation

From: Norman Osborn <nosborn@lookalikedomain.com> 5/6/22, 9:42AM
Subject: **OSCORP PO # A482281 for DAILY BUGLE**
To: J. Jonah Jameson <jjj@dailybugle.com>

Hi Jonah,

Going forward with your order, Before we can continue proceeding with your order. Be informed we have moved into the advanced age of billings. We are only set up to receive payments electronically via ACH/Wire Transfers. Do not use the previous information for remittance. it is now outdated.

Kindly let me know which you prefer in the above so we can proceed further with your PO.
Would so much appreciate your earliest confirmation

Regards,

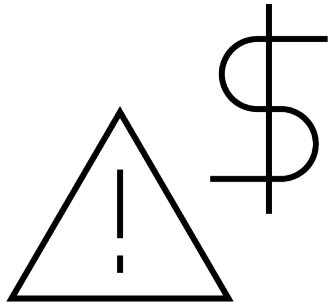
From: Carol Danvers<cdanvers@lookalikedomain.com> 5/15/22, 11:12AM
Subject: **RE: Kree Systems:Unpaid Invoice**
To: Monica Rambeau <monica.rambeau@sword.org>

Hello,

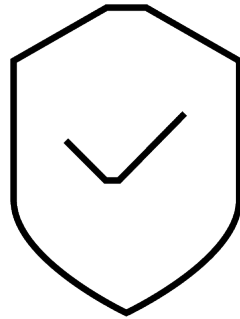
Can you please confirm with your accounting department if there's any due/unpaid invoices owed to our company, as we are currently switching to a new accounting software and a couple of invoices are missing? We apologize for the inconvenience, kindly attach any due/unpaid invoices with this email. I'll appreciate it if all concerned people treat this as urgent. Thanks.

Regards,
Carol Danvers
Chief Executive Officer

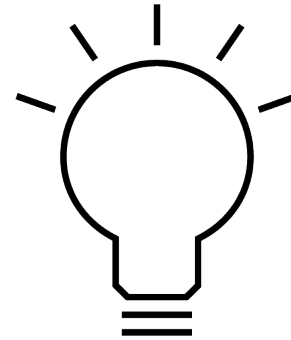
Why are Financial Supply Chain Compromise Attacks Such a Threat?



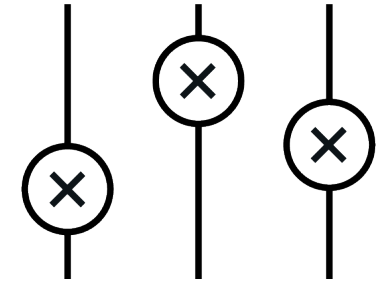
Higher loss
amounts



Use of trusted
identities



Crafted using
real intelligence





No control over
initial compromise

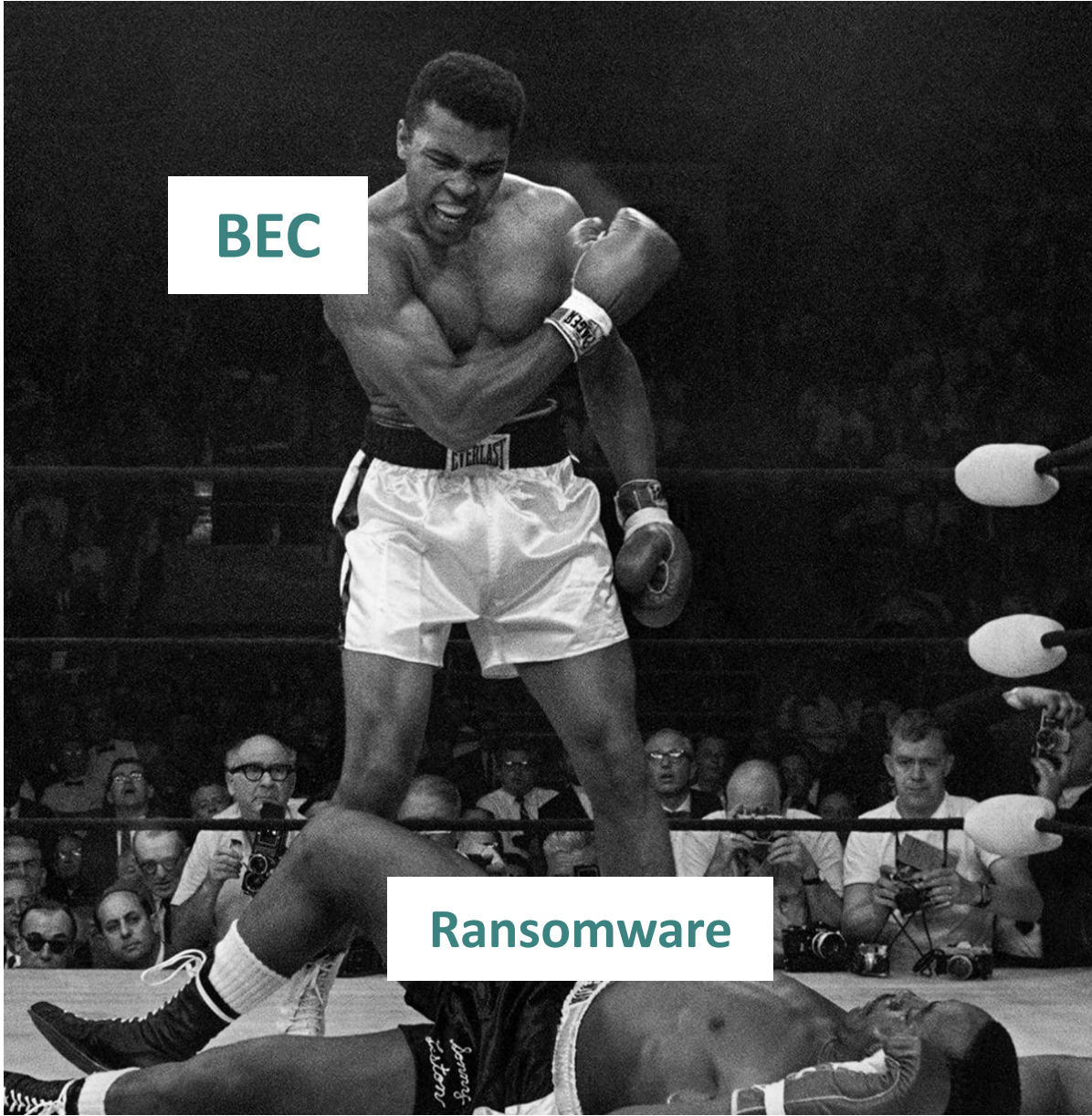
RSA®Conference2022

Ransomware vs. BEC: Tale of the Tape



BEC vs. Ransomware: Tale of the Tape

 BEC	 Ransomware
Financially-motivated	Usually financially-motivated
Delivered via email	Indirect email delivery
Frequently bypasses legacy email defenses	Usually detected by legacy email defenses
Usually not public	Sometimes highly visible
Highly decentralized actors (Nigeria/Western Africa)	Highly centralized actors (Russia/Eastern Europe)
19,900+ reported attacks (2021)	3,700+ reported attacks (2021)
\$2.4 billion in losses (2021)	\$49 million in losses (2021)



BEC

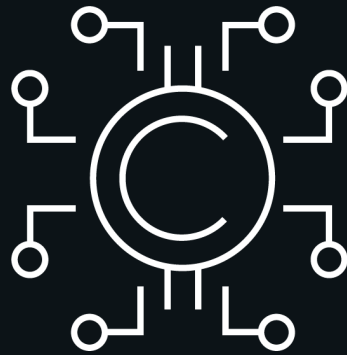
Ransomware

RSAConference2022

So What's Next?



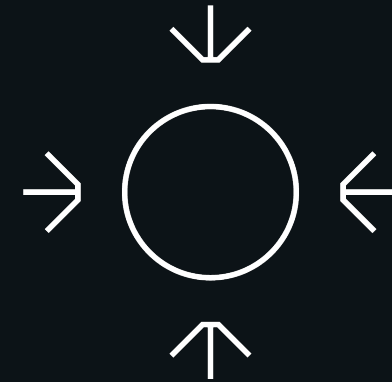
What Happens When the Ransomware Landscape is Disrupted?



Cryptocurrency
Regulation



Geopolitical
Conflict



Law Enforcement
Pressure

What Happens If Two Major Cyber Threats Collide?



Scale and Sophistication of
Ransomware

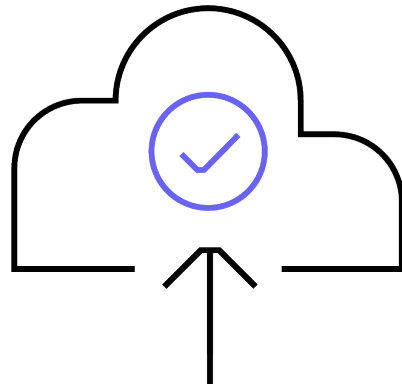
+

Financial Impact and Money
Mule Networks of BEC

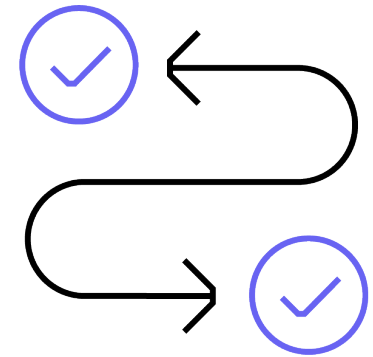
How Do We Combat These Future Threats?



Focus on
Identity



Cloud-First
Approach



Understand Your
Supply Chain

Apply What You've Learned Today

- Is my organization prepared to defend against the more advanced social engineering threats that bypass the secure email gateway?
- Do I have effective internal processes developed to prevent unauthorized wire transfers and direct deposit changes?
- How would my organization respond if it was hit with a successful ransomware attack?
- Are my employees aware of the various email-based threats targeting them today?

RSAC[®]Conference2022

Thank You

Crane Hassold

Director of Threat Intelligence, Abnormal Security

chassold@abnormalsecurity.com

[@CraneHassold](https://twitter.com/CraneHassold)

