Mat Kresz, Esq.

Mat Kresz, Attorney
312-967-5900 (Office)
312-986-9600 (Cell)
MBK@KreszLaw.com

- Mat Kresz is a Cybersecurity & Data Privacy, Technology, Intellectual Property, and Business attorney in Chicago.
- Notably, Mat's practice is informed and enhanced by his background in business as a business leader and as a former Chief Information Officer (CIO) at a mid-size enterprise that served Fortune 500 clients.
- Through the business and technology experience he gained in those roles, Mat is equipped to identify opportunities, solve problems, and mitigate risk with business requirements in mind.

© 2023 ISBA Mutual Insurance Company 1

Today's Agenda

I. Common Terms
II. BEC & Wire Fraud Case Studies and recent developments regarding BEC
III. What you can do to prevent a BEC and Wire Fraud
IV. What to do if you're a victim
V. Ethical (and legal) responsibilities

© 2023 ISBA Mutual Insurance Company 2

I. Common Terms

- **Phishing**
  Practice of sending fraudulent emails that purport to be authentic to induce recipient to take actions that leads to fraud.
- **Spear Phishing**
  Phishing that targets specific individuals.
- **BEC**
  "Business Email Compromise." Incidents where an email account becomes compromised –whether a "business" email account, or otherwise.
- **SPAM** (in Contrast to Phishing)
  Junk email. Unwanted, unsolicited, and sent in bulk, but not necessarily malicious.
- **ESP**
  Email Service Provider, such as Office 365, G Suite for Business, ZOHO, etc.
- **Tenant** (Also Email Tenant or Tenant Account)
  A company account within an ESP that contains one or more email boxes. The account that is designated to be the "Admin" account usually provides access and visibility to all email boxes and their configuration within the Tenant Account.
- **Mailbox Rules**
  Email handling rules that perform one or more actions on an email message when a certain condition is met. Example: A mailbox rule could be established to forward any email that contains "wire" or "money" to fraudster@aol.com.
- **MFA or 2FA**
  "Multi-Factor Authentication" or "Two Factor Authentication." Commonly, it is an access code that is generated by the service provider (such as an ESP) and texted to the user that the user must enter in addition to their user name and password to access the subject service.
- **Session Cookie**
  A small file saved to a computer that a website uses to confirm that the user has previously authenticated (successfully logged-in), so that the website need not request the user's credentials to re-authenticate him/her when the user clicks a link while in that session. Note: this is not the "remember me" feature, but can function like it.
- **Threat Actor**
  The bad guy. Usually part of a gang that specializes in certain types of cyber crime.

© 2023 ISBA Mutual Insurance Company 3

II. BEC & Wire Fraud Case Studies

- A) Law Firm that Practiced Family Law Experienced a BEC; Notified Client/s
- B) BEC in a Real Estate Transaction Resulted in $380,000 Loss
- C) Law Firm Wired $63,000 Settlement Payment to Fraudster; Client Sued

© 2023 ISBA Mutual Insurance Company 4

II. A) Law Firm with Family Law Practice Experienced a BEC; Notified Client/s

- **Facts**
  - Family law firm of about 5 attorneys handled Wills, Trusts, Estates.
  - The attorney responsible primarily for Estates work observed mailbox rules that she did not set. The on-staff IT person (who was also the receptionist) suspected that a BEC occurred.
- **Investigation**
  - Counsel for the Firm retained a Cyber Forensics Firm.
  - Cyber Forensics investigation determined that three of five email accounts within the tenant were compromised; and that
  - The threat actor likely gained access to at least one account by way of "credential stuffing." (Credential stuffing is the practice of using password credentials that were leaked through an unrelated service's data breach.)
  - The Firm certified that one compromised account could have contained Personally Identifiable Information and Financial Account information, but that there was substantially no likelihood that the other compromised accounts contained the same.
- **Conclusion**
  - Firm notified the client whose personal and account information could have been compromised that a data incident occurred; and
  - Firm provided client with credit monitoring service.

© 2023 ISBA Mutual Insurance Company 5

B) BEC in a Real Estate Transaction Results in $380,000 Loss

- **Facts**
  - Buyers wired to sellers a substantial down payment on a home, approximately $380,000.
  - Practically just before closing, the parties discovered that the payment was made to a fraudulent bank account.
- **Investigation**
  - A forensic investigation was substantially inconclusive.
  - It was not clear whether the buyer's, seller's or attorneys' email accounts were compromised, or whether more than one parties' email accounts were compromised because all email correspondences appeared to be "true."
  - (My theory: access to a domain registrar where the subject domains were registered was compromised, and that enabled the threat actor to set up a second ESP that sent "true" emails through the true domains.)
- **Conclusion**
  - Claim was made to at least one party's Cyber Liability carrier.
  - Carrier attempted to settle – but the matter carried on…

© 2023 ISBA Mutual Insurance Company 6

C) Law Firm Wired $63,000 Settlement Payment to Fraudster; Client Sued

- **Facts**
  - In the case of Bile v. RREMC, LLC, Civil Action No. 3:15cv051, 2016 U.S. Dist. LEXIS 113874 (E.D. Va. Aug. 24, 2016), a settlement between Bile and RREMC was reached, wherein Bile was to receive $65,000 from RREMC to settle a claim. RREMC was to pay $2,000 by check, and $63,000 by wire.
  - Bile's Counsel experienced a BEC, unknown to him at the time.
  - RREMC's Counsel received an email from the fraudster posing as Bile's Counsel that issued instructions to wire $63,000 to a certain Barclay's account in Bile's name. RREMC initiated the wire and wired $63,000 to the fraudster, unknowingly.
  - Bile's Counsel inquired to RREMC's Counsel re. status of payment – and this is when the parties discovered that Wire Fraud occurred.
- **Claim**
  - Bile sued RREMC for specific performance (that it wire another $63,000 to Bile).

© 2023 ISBA Mutual Insurance Company 7

C) Law Firm Wired $63,000 Settlement Payment to Fraudster; Client Sued

- **Findings**
  - Bile's Counsel (BC) received an email from Bile sent through _____@aoi.com. (Bile's true email address was _____@aol.com). The email directed BC to have the settlement funds be wired to a Barclay's account in Bile's name in London. BC asked Bile if he issued such direction, and Bile said "no." BC determined that this email was fraudulent, deleted it, but did not notify RREMC's Counsel (RC) of the incident.
  - Bile became impatient with the receipt of his settlement and began "hounding" RC to accelerate payment, and threatened to take actions forbidden by the settlement agreement. RC agreed to initiate payment to Bile in part on fear that Bile might rescind the settlement agreement.
  - RC received an email from BC's true email account (but sent by the fraudster) requesting that the consideration be wired to a Barclay's account. RC didn't question it because: it used BC's typical salutation and contained BC's typical typographical errors; reiterated urgent payment; email was consistent with a prior phone call that the parties would confirm wire instructions by email; the parties communicated by phone and email throughout the case.
  - RC initiated the wire according to the instructions set forth in the BC email, to the fraudster's account.

© 2023 ISBA Mutual Insurance Company

C) Law Firm Wired $63,000 Settlement Payment to Fraudster; Client Sued

- **Outcome**
  - The Court found that Bile's Counsel (BC) failed to exercise ordinary care when it had actual knowledge of a fraudster's attempt to meddle with the transaction but failed to warn RREMC's Counsel (RC) that the transaction was apparently targeted by a fraudster.
  - The Court also found that RC did not fail to exercise ordinary care because it had no indication that the transaction was targeted, and opined that since RC followed its procedures closely, RC would not have initiated the wire had it known that the transaction was being targeted by a fraudster.
  - Therefore, RC was found to have performed when it paid out the first $63,000 by wire – and is not liable to pay a second $63,000 to plaintiff Bile.

© 2023 ISBA Mutual Insurance Company

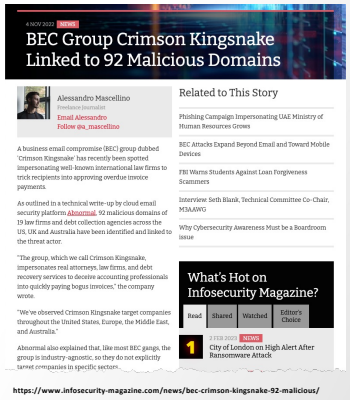
© 2023 ISBA Mutual Insurance Company

Which Party Shoulders the Loss?

- In Arrow Truck Sales, Inc. v. Top Quality Truck & Equipment, Inc., No. 8:14-cv-2052-T-30TGW, 2015 U.S. Dist. LEXIS 108823 (M.D. Fla. Aug. 18, 2015), a truck seller's (Top) and truck buyer's (Arrow) email accounts were both compromised, and furthermore, the fraudster established phony email accounts for both parties that visually appeared to be true.
- The fraudster's actions led to Arrow paying $570,000 to the fraudster, and not to Top for 12 trucks.
- The Court recognized that "[u]nder the 'imposter rule,' the party who was in the best position to prevent the forgery by exercising reasonable care suffers the loss. See, e.g. UCC § 3-404(d); State Sec. Check Cashing, Inc. v. Am. Gen. Fin. Servs., 409 Md. 81, 972 A.2d 882 (Md. App. 2009)." Arrow Truck Sales, Inc. v. Top Quality Truck & Equip., Inc., No. 8:14-cv-2052-T-30TGW, 2015 U.S. Dist. LEXIS 108823, at *15 (M.D. Fla. Aug. 18, 2015).
- And ruled that **the party that was in the best position to prevent the fraud but failed to attempt to verify the wire instructions failed to exercise reasonable care, and would be liable.**

© 2023 ISBA Mutual Insurance Company

Trending Now: "Crimson Kingsnake" Impersonates Law Firms in BEC



Nov. 04, 2022

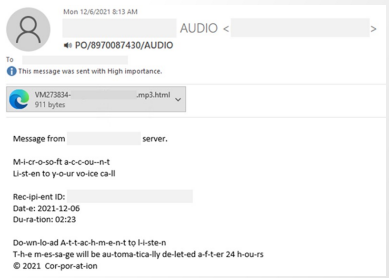
- The "Crimson Kingsnake" gang impersonates law firms and debt collectors across the US, UK, and Australia to collect on "unpaid invoices."

  https://www.infosecurity-magazine.com/news/bec-crimson-kingsnake-92-malicious/

© 2023 ISBA Mutual Insurance Company

Trending Now: AiTM Phishing Scheme Used to Bypass MFA

Email with Purported Voicemail Attached (below):


Mon 12/6/2021 8:13 AM

AUDIO <

PO/8970087430/AUDIO

To

This message was sent with High importance.

VM273834- .mp3.html
911 bytes

Message from server.

M-i-cr-o-so-ft a-c-c-ou--n-t
Li-st-en to y-o-ur vo-ice ca-ll

Rec-ipi-ent ID:
Dat-e: 2021-12-06
Du-ra-tion: 02:23

Do-wn-lo-ad A-t-t-ac-h-m-e-n-t to l-i-ste-n
T-h-e m-es-sa-ge will be au-toma-tica-lly de-let-ed a-f-t-er 24 h-ou-rs
© 2021 Cor-por-at-ion

https://www.microsoft.com/en-us/security/blog/2022/07/12/from-cookie-theft-to-bec-attackers-use-aitm-phishing-sites-as-entry-point-to-further-financial-fraud/

July 12, 2022

- Fraudsters can overcome 2FA by stealing the session cookie.
- Fraudster causes a user to access a legitimate website (such as Office 365) through the Fraudster's Proxy. When the user logs in to the legit website, the Fraudster is able to intercept the session cookie, and return to the legitimate website to access the user's account without logging in (because he has the session cookie that tells the site that authentication has occurred).
- One way that a fraudster redirects users through his proxy is by sending phishing emails with a "voicemail attached" that requires login to retrieve.

© 2023 ISBA Mutual Insurance Company

III. What you can do to prevent a BEC and Wire Fraud

- Conduct Security Awareness Training. Security awareness keeps security issues "top of mind" and lowers "email fatigue."
- Stay out of financial transactions if you can. Let the payor and payee work directly to work out remittance plans. Then, confirm with the parties that the transaction was made.
- Verify wire instructions by phone if you have to be involved in the transaction, even if the wire instructions by email appear to be true.
- If you suspect that the transaction is being "targeted," immediately warn the other party by phone, not email. Remember: your emails might be seen and intercepted by a bad actor.
- Use a strong password that you only use for your email account. Don't use the same password across multiple services.
- Use a commercial ESP that caters to businesses. Business accounts will have additional tools that can be used to detect or prevent intrusions and prevent fraud. They often have better support, too.
- Implement 2FA / MFA. It's included in many services.
- Contact your IT professional about features that you might already have that could be enabled to help you recognize fraud. (Example: [EXTERNAL] banner. "You don't normally receive email from… " banner.)
- Also: buy insurance that covers wire fraud.

© 2023 ISBA Mutual Insurance Company

© 2023 ISBA Mutual Insurance Company

IV. What to do if you're a victim

- Engage Cyber / Data Privacy Counsel to assist you.
- Initiate a claim to your cyber liability carrier.
- Immediately provide notice to the other party to prevent further fraudulent transactions.
- Immediately contact the financial institutions involved. They may be able to retrieve some of the mal-wired funds, or freeze what funds might be in the fraudster's account. Move quickly!
- Contact local law enforcement and make a police report. (Local law enforcement might refer you to another agency.)
- Contact the FBI's Internet Crime Center to report the incident.
- Assess your ethical responsibilities post-incident.

© 2023 ISBA Mutual Insurance Company 14

V. Ethical Responsibilities

- **ABA's Formal Opinion 483.** "[T]he American Bar Association Standing Committee on Ethics and Professional Responsibility reaffirm[ed] that lawyers have a duty to notify clients of a data breach…."
- **Notify Opposing Counsel.** "[A]ttorneys have 'an obligation to contact opposing counsel when and if they receive suspicious emails instructing them to wire settlement funds to a foreign country where such [a] request has never been made during the course of performance of the parties." Bile v. RREMC, LLC, Civil Action No. 3:15cv051, 2016 U.S. Dist. LEXIS 113874, at *34 (E.D. Va. Aug. 24, 2016).
- **Data Privacy Laws & Contractual Obligations.** State and federal data privacy laws may also apply that require that a data incident that involved personal information. Furthermore, notice may be required pursuant to a contract.

© 2023 ISBA Mutual Insurance Company 15

© 2023 ISBA Mutual Insurance Company