WINTER 2023 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss Business Email Compromise and financial loss in litigation settlements, relevant court cases, and best practices for prevention.

Business Email Compromise: Where Did Our Payment Go?

There's no end to the threats posed by email account compromise – data breaches and exfiltration, malicious payloads of malware or ransomware, exposure to liability, penalties and fines, loss of trust, and much more. When cybercriminals exploit organizations and individuals via their email accounts, their sophisticated tactics can go unnoticed until often significant amounts of money or data are stolen. Business Email Compromise (BEC) is especially insidious and was identified by a 2022 FBI report as "one of the fastest growing, most financially damaging internet-enabled crimes", and "a major threat to the global economy" (https://www.fbi.gov/file-repository/fy-2022-fbi-congressional-report-business-email-compromise-and-real-estate-wire-fraud-111422.pdf/view). In this article, we'll look at Business Email Compromise and the growing monetary damages on businesses.

While some of the first BEC crimes appeared around 2016, by the period of July 2019 through December 2021, financial losses due to BEC grew by 65% reaching $2.4 billion. This includes, of course, the peak of the COVID pandemic and the subsequent, rapid deployment of non-traditional business practices (ibid). That shift to conducting business virtually meant that many traditional gatekeeping precautions, like in-person account review, payment instruction and approvals, and invoicing happened entirely via email, presenting an increased opportunity for BEC fraud. There's no question that the motivation for BEC is money, with data exfiltration a close second. C-suite executives, because of their access to sensitive data and the authority they command, are desirable targets of BEC fraudsters.

CEO Impersonation is a form of social engineering attack in which the head of an organization loses control of their email via account takeover, spoofing with a forged email address, or impersonation of their email identity. Whaling, the attempt to target a specific "big fish" in the

organization, relies on either exploiting an executive directly or capitalizing on their authority to trick trusting employees into unknowingly executing fraudulent transfers. A sophisticated fraudster may successfully hack into an executive's email account and simply monitor conversations until such time as an opportunity presents itself. Then the criminal inserts himself into the conversation with an email directing a party to an ongoing communication to wire funds to a bank account set up by the criminal. The better the criminal, the more the email instructions appear genuine in terms of style, word choice, and even grammar and punctuation, to that of the executive. Unsurprisingly, the bank accounts into which the ill-gotten funds are transferred are rapidly cleared by subsequent wire payments, cash withdrawals, or with the help of "mules" who set up additional accounts into which funds can be deposited before being moved again. These accounts may be based on stolen identities. In addition to money, BEC scam artists also create fraudulent email requests for gift card purchases, personal information, payroll data, even investment information and cryptocurrency wallet details.

Vendor Email Compromise (VEC) is similar to CEO Impersonation except that the fraudulent emails are coming from a known vendor. VEC scams most frequently present a fake invoice or request immediate payment of a legitimate invoice to the fraudster's bank account. For VEC scams to work, one or both organizations need to have been infiltrated already. Often this is done through an elaborate phishing email scam that produces access to the accounts payable or receivable staff email accounts or to a small business' cloud-based accounting software application. Here again, the most sophisticated and successful of these scams require legitimate-looking invoices and a high degree of familiarity with the staff, products, services, and regular dealings between the organizations. To what extreme can VEC go? By accessing the banking details for Automated Clearing House (ACH) debit transfers, scammers can create fraudulent electronic fund transfers for themselves and cause the funds to be pulled directly from the victim's account. They can also create a set of fake wiring instructions though this is much harder to implement. Case in point, when a legal settlement payment was misdirected due to BEC, the court had little sympathy for the attorney who fell for the scam as the attorney had successfully transferred funds to the same recipient in the past (*Parmer v. UNITED BANK, INC.*, No. 20-0013. (W VA: Supreme Court of Appeals, 2020).

Business Email Compromise is a threat to organizations of all sizes. While organizations with strong sales and profits present a tempting target for thieves seeking a big payout, small businesses, firms, and non-profit organizations are often less able to devote personnel and resources to preventing, detecting, and remediating BEC, making them easier targets for small dollar heists. Irrespective of the size of the theft involved, BEC is a crime that threatens all organizations. Awareness of the magnitude, pervasiveness, and sophistication of BEC is the first step to protecting your email accounts from attacks.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

UF LAW's 10TH ANNUAL E-DISCOVERY CONFERENCE
Gainesville, FL: February 8-9, 2023

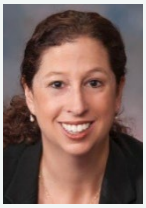
SOLID WEST 2023
San Francisco, CA: February 15, 2023

NETDILIGENCE CYBER RISK SUMMIT 2023
Ft. Lauderdale, FL: February 20-21, 2023

MASTER'S CONFERENCE FEBRUARY 2023
San Francisco, CA: February 22, 2023

ABA TECHSHOW 2023
Chicago, IL: March 1-4, 2023

Click here to see more upcoming events and links.



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: