Accounts deceivable: Email scam costliest type of cybercrime

April 9 2022, by Alan Suderman

Sherry Williams, executive director of One Treasure Island, poses for a photo at her office on Tuesday, April 5, 2022, in San Francisco. Business Email Compromise scams are a type of crime where criminals hack into email accounts, pretend to be someone they're not and fool victims into sending money to places they aren't supposed to. In the case of Williams, the San Francisco nonprofit director, thieves hacked the email account of the nonprofit's bookkeeper then inserted themselves into a long email thread, sent messages asking to change the wire payment instructions for a grant recipient, and made

off with $650,000. Credit: AP Photo/Eric Risberg

It's a crime that siphons untold billions from the economy—but many people have never heard of it.

Business Email Compromise scams involve criminals hacking into email accounts, pretending to be someone they're not and fooling victims into sending money where it doesn't belong.

Although they get far less attention than the massive ransomware attacks that have triggered a powerful government response, BEC scams have been by far the costliest type of cybercrime in the U.S. for years, according to the FBI.

The huge payoffs and low risks associated with BEC scams have attracted criminals worldwide. Some flaunt their ill-gotten riches on social media, posing in pictures next to Ferraris, Bentleys, and stacks of cash.

Almost every enterprise is vulnerable to BEC scams, from Fortune 500 companies to small towns. Even the U.S. State Department got duped into sending BEC scammers more than $200,000 in grant funds meant to help Tunisian farmers, court records show.

"The scammers are extremely well organized and law enforcement is not," said Sherry Williams, a director of a San Francisco nonprofit that recently fell victim to a BEC scam.

Losses in the U.S. due to BEC scams in 2021 were nearly $2.4 billion, according to a new report by the FBI. That's a 33% increase from 2020 and more than a tenfold increase from just seven years ago.

And experts say many victims never come forward and the FBI's numbers only show a small fraction of just how much money is stolen each year.

BEC scammers use a variety of techniques to hack into legitimate business email accounts and trick employees to send wire payments or make purchases they shouldn't. Targeted phishing emails are a common type of attack, but experts say the scammers have been quick to adopt new technologies, like "deep fake" audio generated by artificial intelligence to pretend to be executives at a company and fool subordinates into sending money.

In the case of Williams, the San Francisco nonprofit director, thieves hacked the email account of the nonprofit's bookkeeper, then inserted themselves into a long email thread, sent messages asking to change the wire payment instructions for a grant recipient, and made off with $650,000.

After she discovered what happened, Williams said, her calls to law enforcement went nowhere.

The FBI told her the local U.S. attorney's office won't take her case. She flew to Odessa, Texas, where the bank that initially received the stolen money was located. The money by then was long gone and the local detective was powerless to help. Williams asked her U.S. senators for help and later learned the Secret Service was investigating, but she said it hasn't given her any updates.

Crane Hassold, an expert on BEC scams and former cyber analyst with the FBI, has heard of federal prosecutors declining to take BEC cases unless several million dollars were stolen, a minimum threshold that speaks to how out of control the problem is.

"There's so many of them they can't possibly work them all," said Hassold, now director of threat intelligence at Abnormal Security.

The Justice Department has launched months-long operations in recent years that have netted hundreds of arrests worldwide.

"Our message to criminals involved in these types of BEC schemes will remain clear: The FBI's memory and reach is long and wide-ranging, we will relentlessly pursue you no matter where you may be located," said Brian Turner, executive assistant director of the FBI's Criminal, Cyber, Response, and Services Branch.

But security experts say the wave of arrests has had little impact, and the FBI's own numbers show that BEC scams continue to grow at a rapid clip.

Sophisticated BEC scams targeting businesses and other organizations started taking off in the mid-2010s. It was also around that time when ransomware attacks—in which hackers break into networks and encrypt data—started to grow in frequency and severity.

For years both BEC scams and ransomware attacks were treated largely as a law enforcement problem. That's still true for BEC attacks, but ransomware is now a key national security concern after a series of disruptive attacks on critical infrastructure like the one last year against the biggest fuels pipeline in the U.S. that led to gas shortages along the East Coast.

The National Security Agency's hackers have taken action to disrupt ransomware operators' networks. The Justice Department set up a special ransomware task force to better organize the law enforcement response. And U.S. President Joe Biden has pressed the issue directly with President Vladimir Putin of Russia, where many ransomware operators

are located.

Nothing close to those efforts has been deployed against BEC fraud despite the huge financial losses.

If the U.S. were to launch a whole-of-government response to BEC fraud, it almost certainly would focus heavily on Nigeria. Nowhere are BEC fraudsters more active than in Africa's most populous nation, where scammers have able to operate almost unchecked for decades.

Ramon Abbas, a well-known Nigerian social media influencer who went by Hushpuppi, had more than 2 million followers on Instagram before he was arrested in Dubai. Abbas' social media posts showed him living a life of total luxury, complete with private jets, ultra-expensive cars and high-end clothes and watches.

"I hope someday I will be inspiring more young people to join me on this path," read one Instagram post by Abbas, who pleaded guilty in the U.S. to international money laundering related to BEC and other cybercrimes last year. His sentencing is currently set for July.