Rise In Use of Cryptocurrency In Business Email Compromise Schemes

ic3.gov/Media/Y2021/PSA210413

April 13, 2021 (2021-04-13T14:35:00-04:00)

Alert Number

I-041321-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

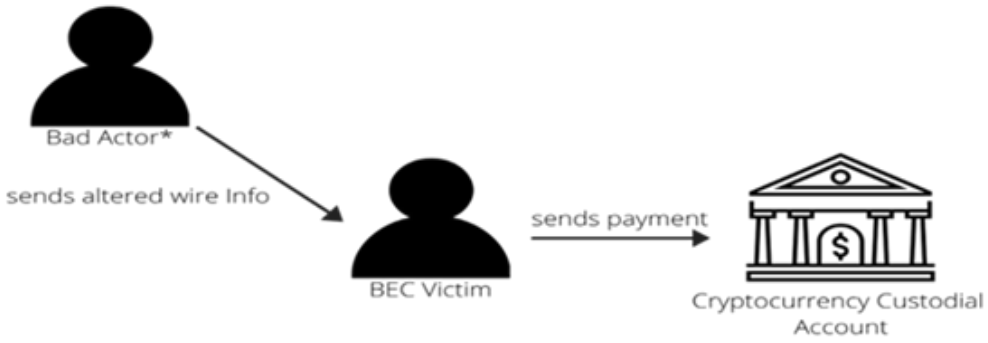
The IC3 has received an increased number of BEC complaints involving the use of cryptocurrency. Cryptocurrency is a form of virtual asset that uses cryptography (the use of coded messages to secure communications) to secure financial transactions and is popular among illicit actors due to the high degree of anonymity associated with it and the speed at which transactions occur.

Two iterations of BEC scenarios have been identified through IC3 complaint information: a direct transfer to a *cryptocurrency exchange* (CE) or a "second hop" transfer to a CE. In both situations, the victim is unaware that the funds are being sent to be converted to cryptocurrency.

A CE is an entity in the business of exchanging *fiat currency (government issued currency not backed by a commodity)* to cryptocurrency. CEs routinely hold custodial accounts with traditional financial institutions (FIs) that are used for easy trading/exchanging for customers.

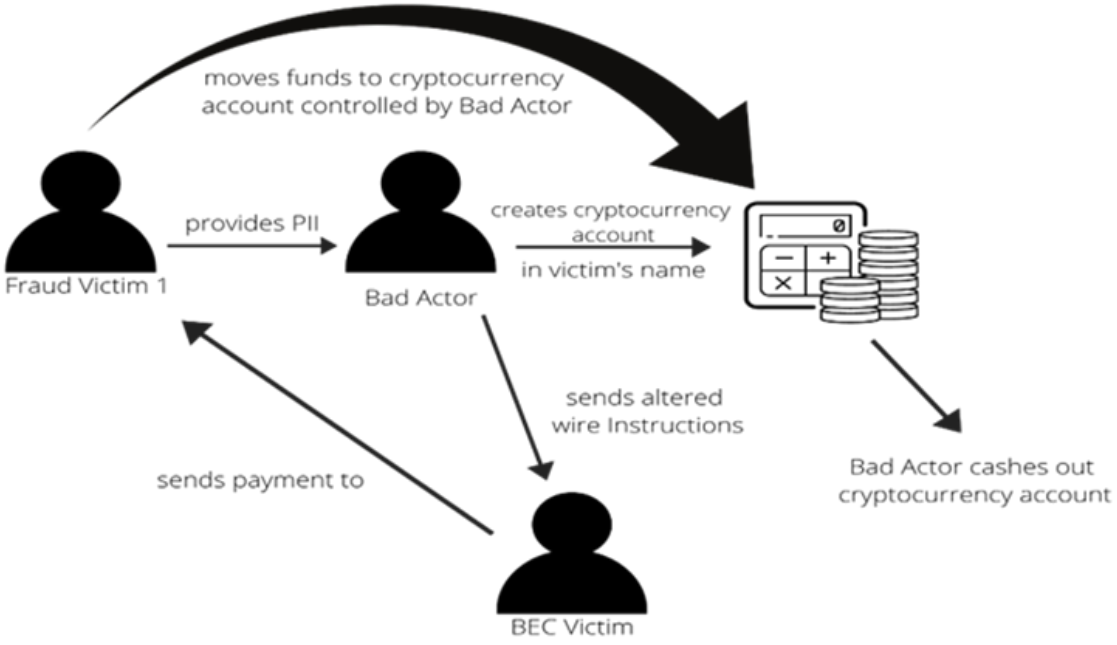
Direct Transfer

This iteration of the BEC/Cryptocurrency scam mirrors the traditional pattern of BEC incidents in the past. The victim entity will receive a spoofed or otherwise compromised email that contains doctored wire instructions provided by the bad actor; however, since the requested transfer is directed to a traditional financial institution (where the CE has a custodial account), it is not easily identified by the victim.

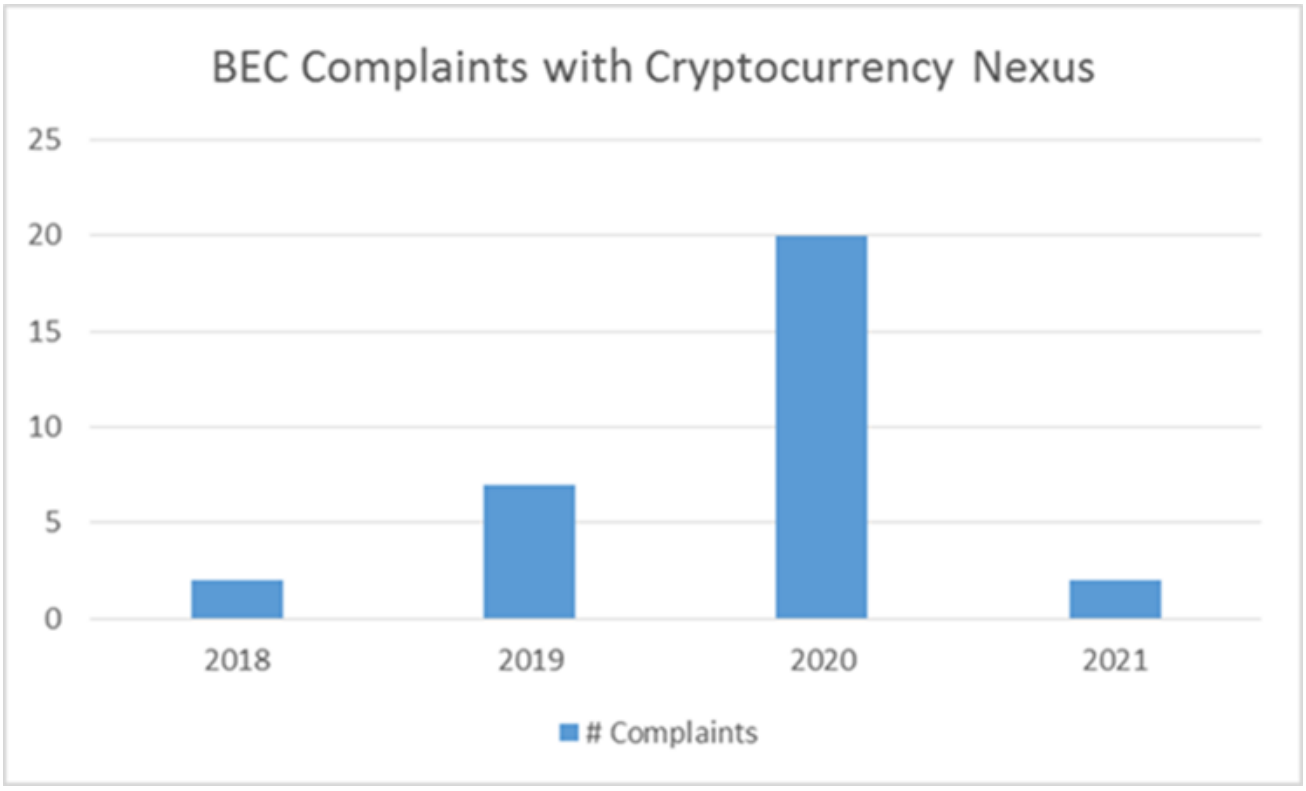


Second Hop Transfer

This iteration of the BEC/Cryptocurrency scam uses victims of other cyber-enabled scams such as Extortion, Tech Support, and Romance Scams. Often, these individuals provided copies of identifying documents such as driver's licenses, passports, etc., that are used to open cryptocurrency wallets in their names. Once received by the scammer, the victim's bank account can be used to receive BEC funds that are then instructed to transfer to a CE custodial account or even directly to the exchange itself.



While the use of cryptocurrency is regularly reported in other crime types seen at the IC3 (e.g., tech support, ransomware, employment), it was not identified in BEC-specific crimes until 2018, and even then, at minimal numbers. By 2019, reports had increased, culminating in the highest numbers to-date in 2020. Based on the data received, the IC3 expects this trend to continue into 2021.



Similar to the classic BEC scams that IC3 has been tracking since 2013, the average dollar loss associated with these incidents is much higher than other forms of fraud reported to the IC3; however, smaller transactions are not immune to the scheme. The annual reported loss associated with these incidents has climbed steadily since the first reported in 2018, topping $10M in 2020.

Suggestions For Protection

- Use secondary channels or two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business/individual it claims to be from.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Refrain from supplying login credentials or PII of any sort via email. Be aware that many emails requesting your personal information may appear to be legitimate.
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's address appears to match who it is coming from.
- Ensure the settings in employees' computers are enabled to allow full email extensions to be viewed.
- Monitor your personal financial accounts on a regular basis for irregularities, such as missing deposits.

If you discover you are the victim of a fraud incident, immediately contact your financial institution to request a recall of funds. Regardless of the amount lost, file a complaint with www.ic3.gov or, for BEC/EAC victims, BEC.ic3.gov, as soon as possible.