Crypto-currency investigation

In 2018, as an investigations officer in one of the commercial banks In Kenya, I investigated a Bitcoin theft case.

Background

The suspects in the case were beneficiaries of fraudulently obtained crypto, that were wired to their accounts. The transactions were split in various bank accounts for ease of withdrawals, who would then withdraw and launder money to conceal the trace of theft.

Investigations

- We earmarked the accounts and froze, them. When funds were received, the suspects couldn't withdraw the funds. They brought themselves to the banks and were arrested.
- The culprits explained to us that, they were just beneficiaries of a long fraud chain where they received the money at a commission and remitted the same to beneficiaries. The fraud was facilitated through social engineering where attackers manipulate people into giving away private information or access. This could involve pretending to be customer support from an exchange or wallet provider.
- Others were done through phishing attacks or malware where they trick users into revealing their private keys or use malicious software, such as key loggers or Trojans, can be installed on a user's device to record keystrokes and steal login credentials or private keys.
- They were made to refund the funds and the case was taken over by the Directorate of Criminal Investigations- Banking Fraud unit for further processing and prosecutions.

Findings

- The crypto’s were obtained through hacking of the genuine owners accounts. Imposters take control of the genuine owners account either through hacking, social engineering, shoulder surfing etc
- Access to bitcoin platforms (Binance, local bitcoins .com)
- Initially Credential validations wasn’t good so any name could open and hold accounts
- Once fraudster have access to the genuine accounts, they would then start buying from genuine sellers-
- Loss of trace-So you end up going for the wrong culprit

Currently

The same is happening through impersonation and Identity theft