Severity:
HIGH

CTM360®
Powered by EDX LABS
Subsidiaries: PENTEST360 | DMARC360 | MG360

FROM UNEMPLOYED TO A MONEY MULE DURING THE COVID-19 CRISIS

BY KAWTHAR ABDULLA

Date: 17th September 2020
Category: Money Mule

THREAT TARGETS:	POSSIBLE IMPACTS:	TARGET AUDIENCE FOR CIRCULATION:
• Financial Institutions • Banking customers	• Unauthorized transactions • Financial, reputational and data loss	• C-Level Executives • IT security team • General public

Cybercriminals are taking advantage of the COVID-19 pandemic, to lure laid-off individuals seeking jobs or working remotely. These cyber crooks have been targeting this specific class of people to work for them as money mules.

Money mules are used for money laundering which is the common terminology used to describe individuals that transfer illegal money on behalf of the criminals via various means, such as a courier service, electronic transfer, or even physically delivering the money to an address or individual. They are often recruited via online job websites, dating websites, spam emails or social platforms. Scammers may also compromise employers' websites to search millions of resumes and determine the targets.

Money mules can be categorized into three main groups:

- **Unwitting:** Individuals who are unaware of being a part of the scam
- **Witting:** Individuals who did not pay attention to the red flags and choose to continue the process of transferring money
- **Complicit:** Individuals who have full awareness of being money mules

Many times unaware people also fall prey to such scammers who lure the target individual against a fee to open an account and later operate that account on the target's behalf using his/her online banking credentials.

In the cycle of Money laundering, money mules play three roles. Firstly, placement which is the process of transferring funds to money mule's bank account. Secondly, layering is the process of moving money into different bank accounts among money mules and criminals. There is a possibility during this phase the money being split into multiple transactions to avoid being traced. Lastly, integration, in this stage funds are reintroduced into the legitimate economy, appearing to have originated from a legitimate source and then the funds transferred back to the financial system of the scammers.

The detection process (KYC-Know your customer) for money mules in banks is becoming complicated nowadays due to the rapid growth of Fintech. Since opening accounts and registration processes are made easier by machine learning and biometric solutions, it is challenging to deploy systems that can assess and analyze suspicious behavior as opposed to a trained human who would have better reasoning.

The focus must shift from waiting until the funds have left a suspicious account to focusing on funds entering accounts to detect mule accounts. Individual banks internally need to focus on capturing mule accounts, but sadly it is not taken seriously by many.

There are various points in the transaction cycle where controls may be added to minimize the probability of any fraudulent transaction to pass through. Firstly, an acknowledgement statement to be added in the transaction request that the individual is not performing the transfer on behalf of someone else as that may lead him to be criminally charged. Also, to put controls at an early stage when the money comes into an account.

By being pre-emptive in action, banks can detect mule schemes at an early stage. Most of the time, money mule accounts are identified only when it is too late. It is best to monitor all cash flow and money transfers holistically to create a better understanding of the money mule tactics and overall behavior.

Recommendations for Banking sector:

- Monitor bank accounts for any suspicious transactions.
- Banks should heed to countries of origin of the money in question
- Compliance officers can identify money mules by witnessing where the money is sent
- Monitor wealth clients, as Criminal networks may convince an individual with an account in a bank to create shell companies and trusts as part of their “legal” job.
- Staying up to date on client activity and identifying account owners and legal beneficiaries before the establishment of a business relationship. Doing so will help reduce banks' risk of exposure to money mules.

Signs to spot a money mule email (For individuals):

- The specific job duties are not described properly.
- The job requires the transfer of money and goods.
- The company location is in a foreign or unknown country with bogus contact information.
- No education or prior experience is required.
- The job only requires online interaction and transaction of funds
- The job offers unreasonably large commission & salary with minimum efforts.
- The writing includes poorly written grammar and awkward sentences.
- The e-mail address used to contact a potential mule is registered on a web-based service (Gmail, Yahoo!, Windows Live, Hotmail, etc.) rather than the organization-based domain.

Protect yourself from committing fraud (For individuals):

- Ignore any emails that request your bank details in any job/opportunity abroad.
- Always confirm the authenticity of the company/institution before handing out such personal information.
- Avoid any form of income coming in from unknown persons.
- Use protected forms of transactions and monitor all transactions in and out of your account.
- Background check on the person or company that has contacted you before putting your complete trust in them.
- Call appropriate authorities such as your bank if you suspect any suspicious activity.

References:

https://www.fbi.gov/file-repository/money-mule-awareness-booklet.pdf

https://calert.info/details.php?id=1239

https://www.icicibank.com/online-safe-banking/money-mule.page

https://www.us-cert.gov/sites/default/files/publications/money_mules.pdf

http://www.bbc.com/news/uk-42132802

For more information:
Email: monitor@ctm360.com Tel: (+973) 77 360 360