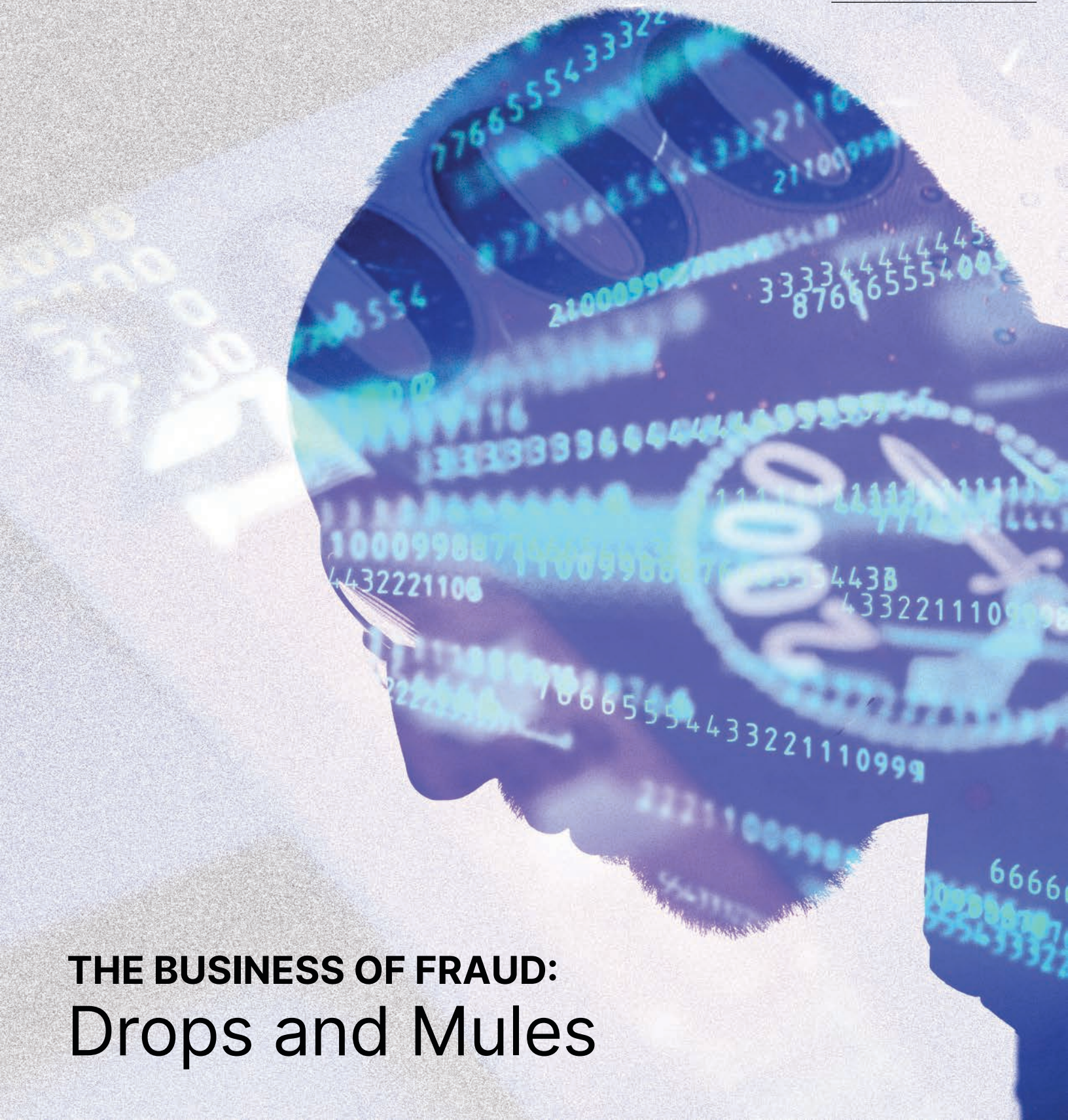
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

May 11, 2021



THE BUSINESS OF FRAUD:
Drops and Mules

Recorded Future®

Recorded Future analyzed current data from the Recorded Future® Platform, as well as dark web and open-source intelligence (OSINT) sources, to review bank drops and mules that facilitate nefarious activities by threat actors. This report expands upon findings addressed in "The Business of Fraud: An Overview of How Cybercrime Gets Monetized". It will be of most interest to anti-fraud and network defenders, security researchers, and executives charged with security and fraud risk management and mitigation.

Executive Summary

"Mules", individuals who transfer money or other goods on behalf of others, are a crucial component to the success of financial crimes, particularly money laundering for capital earned through illegal means such as drugs, fraud, or human trafficking. Typically, the threat actor will make contact with the victim or advertise their operations through social media platforms, job or dating websites, and underground forums. The criminal will entice the victim with a lucrative weekly salary such as a percentage of the money that passes through their personal account. These various platforms are also a way in which complicit mules who are familiar with the business can advertise their services for potential jobs. We have identified threat actors targeting potential money mule victims through a multitude of scams on English, Russian, Spanish, and Portuguese forums and channels.

Mules are usually supported by a network of "drop" services, which have infrastructure in place such as warehouses, vehicles, fake IDs, and more to coordinate the logistics of handling the dirty money or fraudulent goods that mules transfer. These services are essential for further obfuscating the origin and destination of the money and goods.

Key Judgments

- Mules are used, knowingly or unknowingly, to launder money for various forms of criminal operations.
- The use of money mules has grown and is expected to grow substantially. In 2020 US law enforcement agencies took action against over 2,300 money mules, far surpassing 2019's efforts, which acted against around 600 money mules.
- Though advantageous for criminals, reshipping and money laundering scams can result in serious consequences for the mules. As accomplices to fraud, the mules often end up losing money, sometimes suffer personal harm, and can even be pursued by federal and local law enforcement.
- Demand has grown for mules, in particular money mules, in Latin America. Recorded Future has identified Portuguese- and Spanish-speaking threat actors consistently advertising the need for bank drop associates.

Threat Analysis

A money mule is a person who transfers fraudulent money on behalf of someone else. Online threat actors recruit money mules to move money, either physically or electronically through various bank accounts, or through a multitude of other methods. Typically, the mule is paid for services with a small percentage of the money transferred. Money mules are often recruited online for what they think is legitimate employment or provide assistance because they believe they have a trusting or romantic relationship with the individual who is asking for help moving money, not aware that the money they are transferring is dirty. Once received, the mule will wire the money into a third-party bank account and withdraw the money received, possibly via several cashier's checks, convert the money into a virtual currency or a prepaid debit card, send the money through a money service business, or some combination of these. Criminals can then receive the laundered cash, which was usually originally stolen from victim accounts that were usually obtained by some form of account takeover.

More than 90% of money mule transactions identified are linked to cybercrime. The illegal money often comes from criminal activities like phishing, malware attacks, online auction fraud, e-commerce fraud, business e-mail compromise (BEC) and CEO fraud, romance scams, holiday fraud (booking fraud), and many others.

Typically, upon receiving fraud training through different forums, cybercriminals identify drops and mules services for their operations. Some fraud tutorials and courses are specifically focused on recruiting drops and mules.

Drop services, unlike other cybercrime services, require a physical human presence to successfully carry out the carding operations. Each developed carding enterprise has a team of people who will intercept stolen packages, verify purchases, and handle the situation when someone is needed to act as the impersonated account owner. Drop services already have teams on the ground with an established infrastructure of fake identities, IDs, warehouses, and vehicles. These teams can be used for other aspects of the operation, such as placement of banners, flyers, cold calling, recruiting others, and cashing out at banks and ATMs.

- The drops and money mules ecosystem starts with a recruitment process that allows cybercriminals to involve local personas in their criminal enterprise. These are individuals who are used as recipients of stolen funds, as those who cash out stolen payment cards at ATMs, or as individuals who use their accounts to launder funds between various accounts. Money mules who have accounts with a history of legitimate transactions or those with a good credit history are often prized because transactions involving their accounts are less likely to be flagged. Some money mules know they have been recruited to assist criminal activity, but others become money mules without realizing their activity is benefiting fraudsters. These criminal elements usually use several methods to recruit victims:
- Work-From-Home Scams: A job posting offers easy money for reshipping packages, buying gift cards or postal money orders, or transferring money, which can be done at home.
- Confidence Scams: A person or business you don't know offers you a commission if you transfer money for them. Many of these scammers are active on social media sites.
- Lottery Scams: A person informs you that you need to transfer or accept money in order to collect a prize or winnings.
- Romance Scams: A person you've met online or on an app, who says they're romantically interested in you, asks you to transfer money or packages.

Recruitment Process

Threat actors create fake companies, use hacked accounts of legitimate companies, or post job vacancies on popular job search engines for what appears to be legitimate jobs for job seekers. Once the threat actor has hired the applicant, the individual is given access to a web panel where they can fulfill their weekly duties and requests. Once the threat actor has hired the mule, the individual is carrying out the nefarious activities of the threat actor — sometimes knowingly, and sometimes unknowingly. This factor is significant in running the drop, so when drops are discussed on forums, they are always identified as "witting" or "unwitting" drops. Witting drops are typically recruited through word of mouth.

Each type has its advantages and disadvantages. Individuals who know they are involved in illegal activity are frequently easier to deal with because the drop handler can discuss the various contingencies with them ahead of time. However, these drops or money mules will need to set up new accounts and sometimes have to take the time to age the accounts so that activity in the accounts looks less suspicious. Using witting mules also presents more risk to the employer because individuals who know they are involved in illegal activity are more likely to keep the money, knowing that the handlers have little legal recourse against the drop.

Unwitting drops or money mules have the advantage of using their own legitimate accounts, which typically have a history of legitimate transactions and are less likely to be flagged for suspicious activity. However, if issues do come up, the unwitting individual is less likely to know how to resolve them and the handler frequently has a harder time convincing them to create the false narrative necessary to overcome suspicion. In some cases, unwitting drops will simply send the money or product back if they get nervous.

Money Mules Examples

In finding money mules, threat actors typically look for individuals who are seeking to make quick profits and can transmit goods across a border or checkpoint of some kind, whether physical or digital. A parallel that illustrates this is the use of mules for trafficking narcotics. Just as drug mules are often paid to move narcotics across a border, money mules are used to move money (usually generated from the sale of drugs, fraud, human trafficking, or arms trafficking) across financial borders or through the banking system. Money mules are typically granted a percent of the cash if they allow their banking accounts to be used to launder criminal proceeds. Banking credentials, online passwords, and sometimes even bank cards and personal identification numbers are fully surrendered. While most money mules will get paid, there are instances where they receive nothing, while their banking details are used to steal from them and other victims with their accounts eventually being closed by the financial institution.

In most scenarios, a threat actor will advertise a job on dark web and clearnet forums, shops, social media, and messaging platforms. From an international law enforcement perspective, if one is caught money muling, they can be arrested, their house can be searched, and can receive a lengthy prison sentence if convicted.

Some examples of threat actors who either shared bank drop strategies, were recruiting mules, or advertised their drop services in 2020:

- December 2020: "Pangea", a member of Club2CRD Forum, posted an advertisement requesting UK drop services for well-known banks in the region
- November 2020: "bl4cksun_drops", a threat actor on Boveda Forum, sought a money mule for Banorte, one of the largest banking and financial service companies in Mexico.
- July 2020: "buckballad", a member of now-defunct Torum Forum, developed his own PDF book ("Ballads Guide") to share with other cybercriminals on how to develop a successful drops and mules operation.

Another example that could be found on Verified Forum was an advertisement posted by "silicis18", a member of multiple underground communities, where they offer a wide variety of ready-to-go bank accounts for money laundering purposes.

"Verta", another member of the forum Verified, was advertising a money mule service that they launched in November 2020. According to the threat actor, they can take money of any origin and assist with fund transfers and money laundering. Verta claimed to provide their service for $4,500 and higher amounts for a 50% commission fee. The threat actor noted that they employ money mules who use their personal banking accounts. According to Verta, their customers can order a specific number of accounts in the banks of their choice, and opt to exchange funds into Bitcoin.

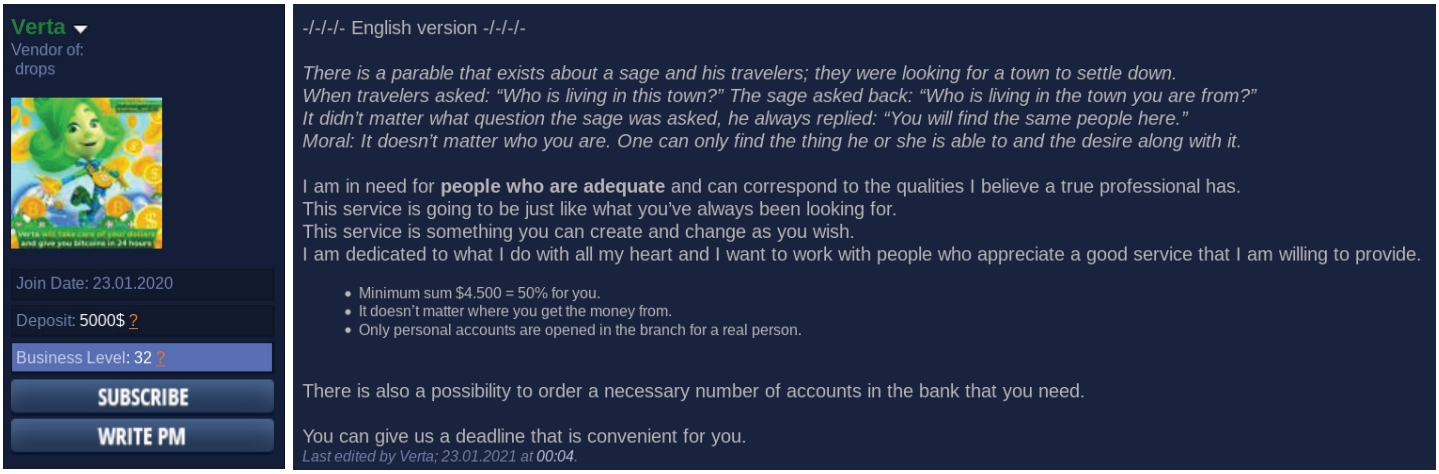


Figure 1: An advertisement by Verta's services (Source: Verified Forum)

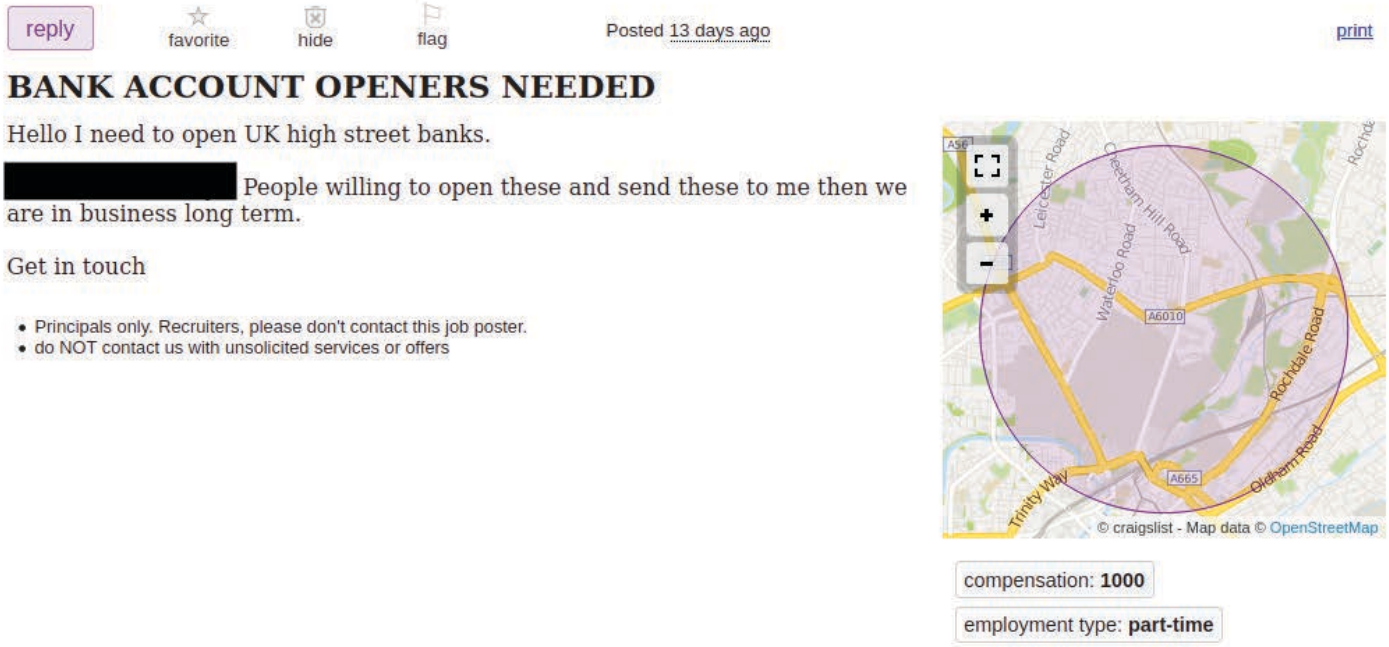


Figure 2: Recruitment advertisement on Craigslist for bank drops (Source: Craigslist UK and Ireland)

Shipment Drops

A mail-forwarding company is a logistics company that delivers goods from one country to another and is often used as a front company by threat actors. Mail-forwarding companies are commonly used to fulfill international deliveries when the shop does not offer international delivery itself.

Reshipping or shipment drops scams are typically offered as an at-home job that involves repackaging stolen goods and forwarding them, often outside the US. To apply for the job, applicants have to upload sensitive and personally identifiable information (PII), such as copies of their passport, driver's license, or employment records to the scammer's website. After uploading these sensitive documents, an applicant has not only fallen victim to partaking in the scam but has also provided the threat actor their PII to steal their identity by opening a bank account, credit cards, or other accounts to facilitate their criminal activities. Once the scammers review the submitted application and documents, the applicant will be added to the list of drops. Scammers ask victims to pay their own shipping charges and pay reimbursement and compensation with a fake check. In addition to seeing their paychecks bounce, those who fall for reshipping scams may be liable for shipping charges and even the cost of goods purchased online with stolen credit cards.

Figure 3: Banners for shipping drop advertisements (Source: WWH Club Forum)

[Translation of top image: DON'T WORRY BE HAPPY
RESHIPPING
ONLY QUALITY DROPS IN THE USA FOR STUFF]

In April 2021, "primum_leo", a member of the forum Verified, was advertising a reshipping mules and drops service called "Carders Brotherhood". According to the threat actor, they created the service for their own payment card fraud needs but with enough experience and underground demand decided to open it up for a larger audience in 2019.

Currently, primum_leo manages 80 mules and drops based in the US, who receive packages to their addresses or pick up packages at small branches of delivery services companies in the 20-mile radius from their location. The threat actor claims that their mules and drops can receive and pick up packages under their names or cardholders' names, likely using fake identification documents.

The threat actor noted that the "Carders Brotherhood" service provides their customers with access to an automated panel allowing for easy management of mules and drops under their control. According to primum_leo, they employ witting mules and drops, whose average term of service is 1 month.

Longstanding cybercriminals such as primum_leo use their own software, often called a "panel", to manage mules and drops they employ. A panel allows for easy and automated control over human drops by both service operators and their customers. Usually, this software is developed and maintained for a specific mules and drops vendor, also known as drop-herder, who will update it with information about individuals they employ. For example, primum_leo will populate the panel with information about their 80 drops in the US (as of April 2021), and primum_leo's customers will select individuals based on their geographical location, prices, and availability. Access to the panel is given to vetted customers, usually engaged in carding (payment fraud) operations.

A typical panel allows for an easy selection and deployment of available mules and drops. With simple point-and-click navigation, cybercriminals can choose either witting or unwitting drops, based on the state where they need to receive or reship stolen items. Sometimes a panel will include additional details about mules and drops, such as the individual's age and "life expectancy", or just "live" — slang terms cybercriminals use to explain how long a particular mule or drop has been in operation.

Figure 4: Carders Brotherhood advertisement (Source: Telegram)

[Translation of top image: CARDERS BROTHERHOOD
IT'S TIME TO EARN MORE
Your trusted and verified reshipping service in USA
Price for package reshipping:
Test drops — free of charge
Package delivered to the drop's address — $50
Pickup from a branch under the drop's name — $80
Pickup from a branch under the cardholder's name — $150]

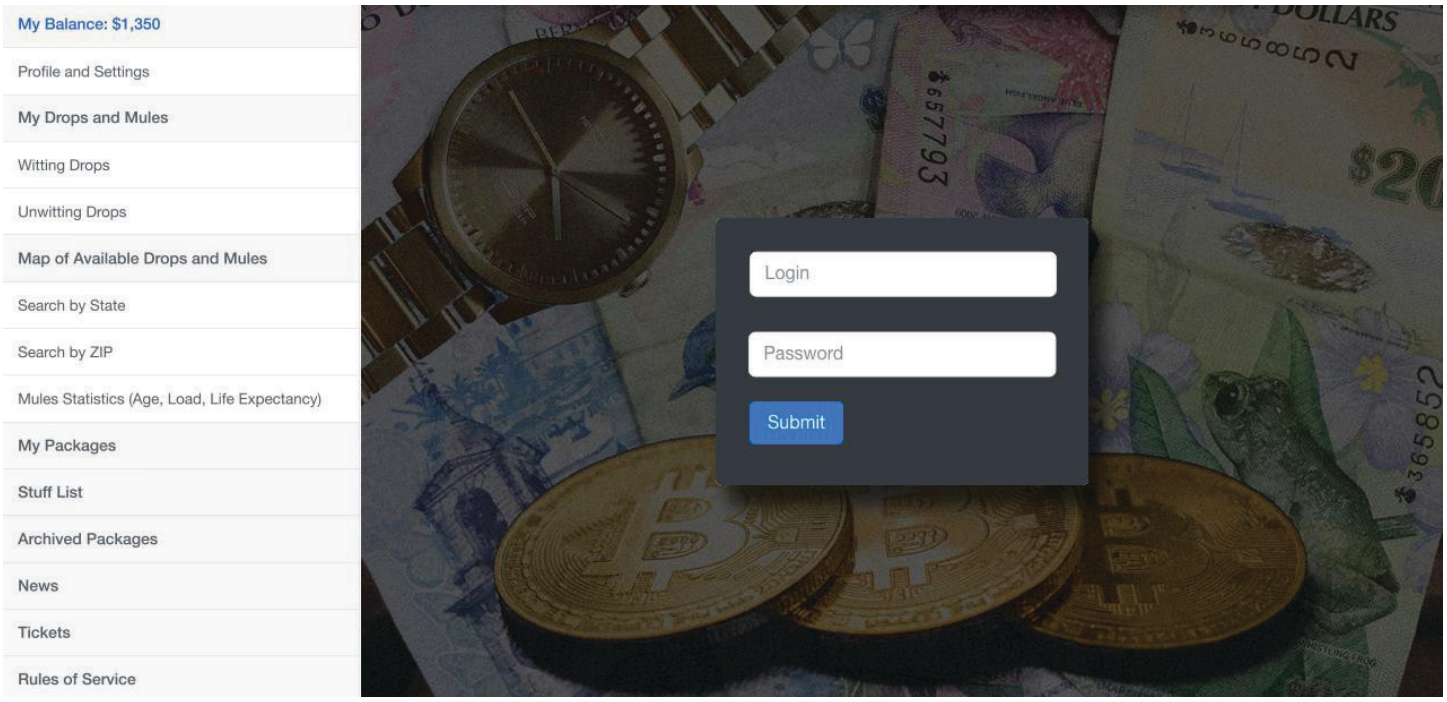


Figure 5: Sample panel for managing human mules and drops (Source: Recorded Future)

Most threat actors select mules and drops who have been "live" or in operation for a longer time, as well as prefer to use witting mules who have experience, are less likely to contact law enforcement, or be uncontrollable by drop-herders.

The average "life expectancy" of witting drops is 2 to 3 months, and unlike unwitting drops, they are selected more often to receive and reship expensive items. Witting drops are usually double the price of unwitting drops, as they are aware of the risks they are taking and are less likely to lose a package or disappear from the drop-herder's radar.

Access to a drop-herder's panel and service usually costs between $50 and $200 per package or sometimes is percentage based, which can be as high as 55% (and as low as 15%) of the stolen item's actual price. Additionally, some panels keep drop statistics, such as the total number of packages received and sent by an individual, how many packages are assigned presently (which helps threat actors understand a particular drop's workload), the individual's name and address, as well as their availability to receive a package in their own name or by using counterfeit identification documents.

Portuguese- and Spanish-Language Mules

Mule recruitment and bank drop advertisements are listed across multiple languages on dark web forums. We have identified that discussions around the recruitment of mules and bank drop participants have increased among speakers of 2 languages in particular over the last year: Spanish and Portuguese. An examination of our source collections over the last year for threat actors using dark web sources in Portuguese and Spanish identified the following events and patterns:

- Threat actors are sharing tutorials on what drops are and best practice strategies with their counterparts on well-established dark web forums and shops, which include well-known Spanish and Portuguese forums such as ChkNet Carding Forum, Boveda Forum, Foro Liberator, Raid Forums, and Nulled Forum.
- These sources included the following types of advertisements for mule recruitment and drops: advertisements for drops of compromised credit cards, requests looking for drop associates and partners, and cybercriminals advertising their drop services.
- The most common type of drop advertising identified among Portuguese- and Spanish-speaking threat actors pertained to the recruitment of mules for bank drops and cashout opportunities within the Latin America (LATAM) region as well as in other countries.

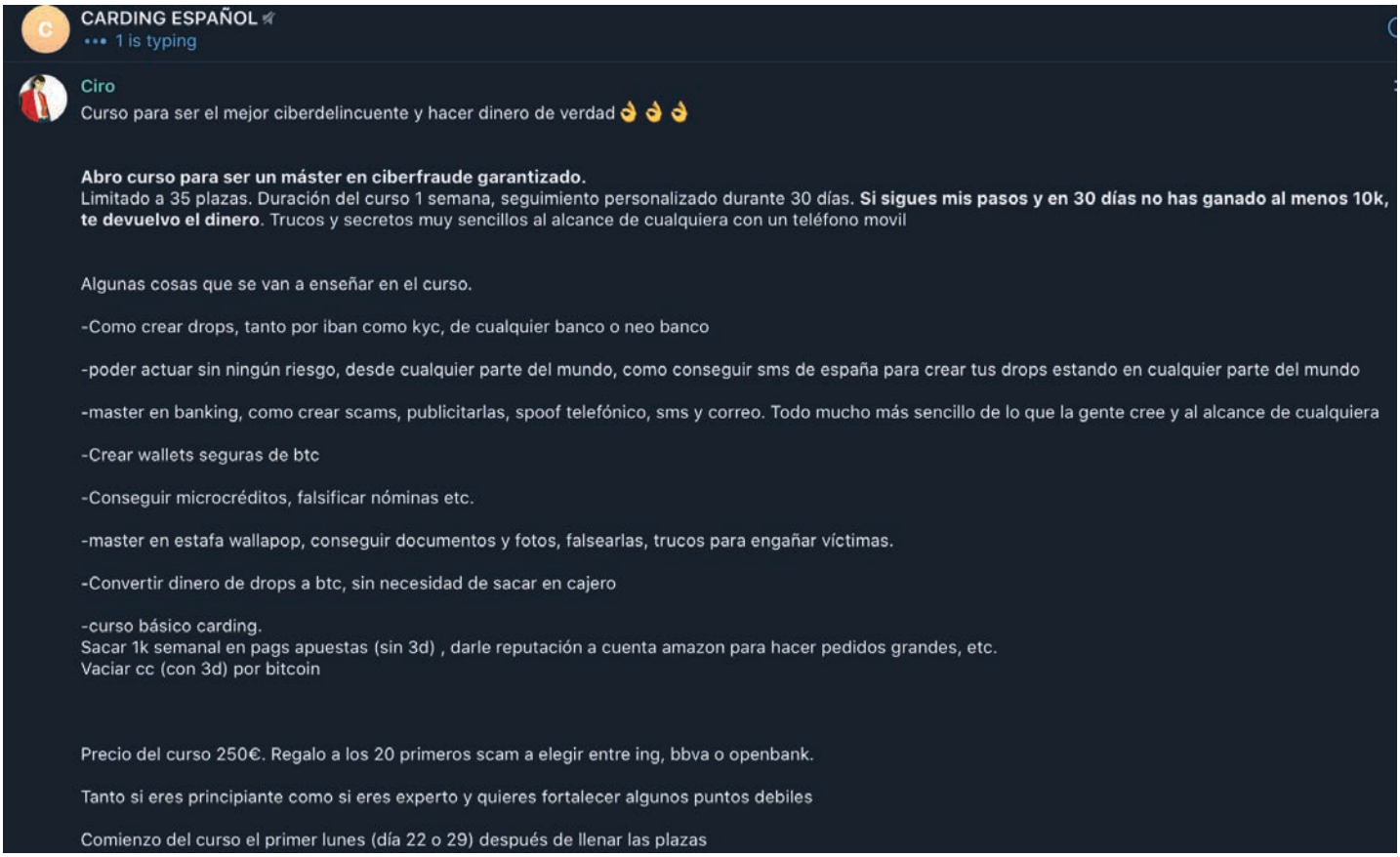


Figure 6: Ciro advertising a fraud tutorials course which includes bank drops (Source: Telegram)

[Translation of top image: CARDING ESPAÑOL
A course to be the best cybercriminal and make real money
A one week course limited to only 35 spots and a guarantee that after 30 days if the student has not made at least $10,000 USD I will return the student's money. Simple tricks and secrets within reach of any mobile phone

A few things that we will learn in the course:
How to create drops, like KYC, from whatever bank or financial institution
How to act without any risk whatsoever, from any part of the world, how to get SMS messages from Spain to create your drops in any part of the world
Create secure bitcoin wallets
How to get microcredits, falsify payroll etc.
How to be a master in swindling, and how to get access to documents, photos, falsify them, and strategies to trick victims
How to convert drop money to bitcoin without having to go to an ATM
Basic carding course
Price of the course is 250 euros. The first 20 people to join the course will receive a scamming opportunity against ING, BBVA, or Openbank
The beginning of the course will be on Monday (22 to 29) after the open student slots fill

Figure 7: Ciro advertising a fraud tutorials course which includes bank drops (Source: Telegram)

As an example of a typical post, on Boveda Forum in July 2020, the Spanish-speaking threat actor "Milagros2213" was looking for a drop associate in the US who was willing to split the proceeds 50/50. The threat actor left their email address and ICQ number as points of contact. Based on responses in the thread, other threat actors were also interested. Similarly, in early January 2021 on ChkNet Carding Forum, the threat actor "samukaos111" discussed the basics of bank and product drops and how to best use the PII of victims to successfully carry out a job.

Telegram

Underground communities in the LATAM region are mostly found on mobile chat platforms, such as Telegram, WhatsApp, and Discord (gaming).

Latin American online forums are an environment for learning how to become a hacker and the sharing of information and tools. In the region, forums have acted as a source for entry-level hackers ("script kiddies") since their inception. While the majority of forums serve as a source for learning, there are products and services for sale. Mobile forums, in particular Telegram channels, have become the preferred environment to advertise bank drops and mule associates.

Outlook

As the number of internet users grows each year, the potential to be a mule victim does as well. Cybercriminals will continue to seek and take advantage of internet users who are in financial distress and looking to earn fast money. Bank drop associates will continue to be in high demand, specifically in Latin America as a result of economic insecurity in the region. Additionally, cyber threat actors who have experience in mule operations are likely to modernize their tactics, techniques, and procedures in order to evade detection from law enforcement authorities as well as to improve their overall schemes and illicit businesses.

If a job advertisement appears too good to be true, it most likely is. Recorded Future suggests that individuals and companies alike watch out for warning signs, and do research on that particular company prior to business being officially conducted between the two parties. If you believe that you are participating in a money mule scheme, stop transferring money and merchandise immediately and notify local enforcement authorities. These authorities may include your bank, the service you used to conduct the transaction, and law enforcement.

Recorded Future recommends that organizations and individuals conduct the following general measures to defend against becoming a potential mule:

- Investigate the person or company before doing business with them.
- When transferring money, use a method that protects the transaction. For example, many banks, credit cards, and services such as PayPal may offer fraud protection.
- Monitor the transactions, including checking for withdrawals from your bank account and tracking an order.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.