Drops for Stuff: An Analysis of Reshipping Mule Scams

Shuang Hao* Kevin Borgolte* Nick Nikiforakis† Gianluca Stringhini◇
Manuel Egele‡ Michael Eubanks¶ [1] Brian Krebs▽ Giovanni Vigna*§
*University of California, Santa Barbara †Stony Brook University ◇University College London
‡Boston University ¶Federal Bureau of Investigation ▽KrebsOnSecurity.com §Lastline Inc.
{shuanghao,kevinbo,vigna}@cs.ucsb.edu nick@cs.stonybrook.edu g.stringhini@ucl.ac.uk
megele@bu.edu michael.eubanks@ic.fbi.gov krebsonsecurity@gmail.com

ABSTRACT

Credit card fraud has seen rampant increase in the past years, as customers use credit cards and similar financial instruments frequently. Both online and brick-and-mortar outfits repeatedly fall victim to cybercriminals who siphon off credit card information in bulk. Despite the many and creative ways that attackers use to steal and trade credit card information, the stolen information can rarely be used to withdraw money directly, due to protection mechanisms such as PINs and cash advance limits. As such, cybercriminals have had to devise more advanced monetization schemes to work around the current restrictions.

One monetization scheme that has been steadily gaining traction are reshipping scams. In such scams, cybercriminals purchase high-value or highly-demanded products from online merchants using stolen payment instruments, and then ship the items to a credulous citizen. This person, who has been recruited by the scammer under the guise of "work-from-home" opportunities, then forwards the received products to the cybercriminals, most of whom are located overseas. Once the goods reach the cybercriminals, they are then resold on the black market for an illicit profit. Due to the intricacies of this kind of scam, it is exceedingly difficult to trace, stop, and return shipments, which is why reshipping scams have become a common means for miscreants to turn stolen credit cards into cash.

In this paper, we report on the first large-scale analysis of reshipping scams, based on information that we obtained from multiple reshipping scam websites. We provide insights into the underground economy behind reshipping scams, such as the relationships among the various actors involved, the market size of this kind of scam, and the associated operational churn. We find that there exist prolific reshipping scam operations, with one having shipped nearly 6,000 packages in just 9 months of operation, exceeding 7.3 million US dollars in yearly revenue, contributing to an overall reshipping scam revenue of an estimated 1.8 billion US dollars per year. Finally, we propose possible approaches to intervene and disrupt reshipping scam services.

Categories and Subject Descriptors

K.4.1 [**Public Policy Issues**]: Abuse and crime involving computers; K.4.4 [**Electronic Commerce**]: Payment schemes, Security; J.4 [**Social and Behavioral Sciences**]: Economics.

Keywords

Security; Measurement; Underground Economy; Monetization.

CCS'15, October 12–16, 2015, Denver, Colorado, USA.

ACM 978-1-4503-3832-5/15/10 ...$15.00
DOI: http://dx.doi.org/10.1145/2810103.2813620.

1 Introduction

Due to their convenience, online banking and electronic commerce have grown significantly in the past years. With just a credit card and Internet access, one can buy a wide variety of goods and have them shipped to their residence, without the need of an in-person transaction.

At the same time, however, cybercriminals covet users' financial account information to profit off of them. Data breaches, phishing, and fraud continue to rise and affect millions of users each year. In 2012, the software company Adobe Systems was breached and information of nearly 152 million customers was stolen [1]. In late 2013, in a data breach against Target (the second largest discount retailer in the United States), attackers gained access to the credit card and personal information of up to 110 million customers [2]. In the very same spirit, in September 2014, the hardware store Home Depot discovered that their point-of-sale systems were infected with custom-built malware to exfiltrate credit card information, resulting in 56 million stolen credit cards from this incident alone [3]. Next to these high-profile cases, hundreds of smaller regional companies are breached, what appears to be, almost monthly.

In addition to online breaches of companies storing financial data, cybercriminals are now branching into the physical world by targeting the makers of Point-of-Sale (PoS) terminals and infecting them with malware, leading to the exfiltration of credit card data each time a customer swipes his credit card. For instance, in April 2015, Harbortouch, a PoS manufacturer, was attacked by cybercriminals who planted malware on their terminals which were then distributed to more than 4,200 businesses [4]. Finally, information stealing botnets and malware, such as Zeus or Torpig, remain important tools in the cybercriminal's arsenal to steal credit card information and account credentials [5].

Despite the criminals' seemingly inexhaustible stream of compromised credit card information, information theft is usually just the first stepping stone of a long series of transactions in the underground economy. More specifically, monetization of obtained credit card information is a difficult challenge that the cybercriminals face. Directly withdrawing money using stolen credit cards is usually limited to small amounts (the cash advance limit) and also bears the risk of exposing the cybercriminals' true identities and locations to law enforcement, credit card companies, and banks. Since criminals want to maximize their profit and avoid prosecution, they had to devise more elaborate monetization schemes. One class of particularly successful monetization schemes are so-called *reshipping scams*.

In a reshipping scam, the criminals purchase high-value products with stolen credit cards and recruit willing and unsuspecting people (*reshipping mules*) to receive and forward the packages on behalf of the criminals. Once the fraudsters receive the products, they then sell them on the black market for cash and thus profit at the cost of consumers, merchants, banks, and insurance companies. In the past

[1] Michael Eubanks is a Supervisory Special Agent in the Cyber Initiative and Resource Fusion Unit of the Federal Bureau of Investigation.

years, these reshipping scams have become one of the main approaches for attackers to monetize stolen credit cards.

Reshipping scams offer a variety of advantages to cybercriminals. First, domestic reshipping mules allow the criminals to sneak merchandise to countries that are not legitimate shipping destinations for a given product. Second, as the unwitting mules serve as relaying intermediaries who cloak the criminals' true identities, these schemes act as an additional level of indirection and obfuscate traces that the criminals might have left behind otherwise. Besides the advantages for criminals, reshipping scams can result in dire consequences for the mules. As an accomplice to fraud, the mules often end up with financial loss, sometimes suffer personal harm (PTSD, depression), and even enter the crosshair of both local and federal law enforcement [6, 7].

Disrupting the reshipping chains of these scams has the potential to cripple the underground economy by affecting a major income stream of cybercriminals. In this paper, we investigate the cornerstones of reshipping scams and identify vantage points to cause such disruption. Additionally, we present the first in-depth, large-scale study of reshipping scam operations. To characterize the operational logistics of reshipping scams and the relationships between the key actors, we analyze detailed log files from seven reshipping scams.

In summary, this paper makes the following contributions:

- We present the first in-depth, large-scale analysis of the operational logistics behind reshipping scams, based on log data collected from seven reshipping scams.
- We identify the key components in reshipping scams and provide insights about their operations, including volume of packages, estimated revenue, volume and churn of mules, and targeted merchants.
- We identify bottlenecks in the analyzed reshipping scams and propose intervention techniques that can be applied to attack and disrupt the reshipping chain. Such interference can reduce the criminals' profit, disincentivize reshipping scams as a monetization technique, and, in turn, prevent further unsuspecting users from falling victim to these scams.

2 Reshipping Scams

In this section, we first introduce the background and terminology used in reshipping scams, and then provide a detailed description of how criminals operate and manage such operations.

2.1 Terminology

In the reshipping scam ecosystem, criminals take on different roles depending on their involvement. Similarly, multiple victims are affected every time a single package is bought and shipped. We introduce the terminology (slang) used by the underground players and we define the individual roles of the entities involved in the scam.

Operator. The *operator* of a reshipping scam sets up and manages the reshipping scam's website, which is the central component of the entire operation, tying the various actors together. The website is typically well-designed and resembles sites of legitimate package handling and inventory companies to trick the mules into believing that the scam is indeed a legitimate operation. The responsibilities of the operator, however, do not end here: on a regular basis, he has to recruit mules who are willing to ship packages on behalf of a third party (i.e., the stuffers, see below). To this end, the operators resort to social engineering and promise the mules a commission or even a monthly salary for their work. Later on in the scam, once the operator recruited an initial set of mules, he "rents" out the recruited mules to other criminals who buy goods with stolen credit cards and pay the operator for what is effectively *reshipping as a service*.

Stuffer. The cybercriminals who rent mules from the reshipping scam sites' operators to move merchandise are referred to as *stuffers*. They purchase high-value products with stolen credit cards from merchants and have the merchants ship the items to the mules' addresses. Once the mules receive the packages, the stuffers provide them with prepaid shipping labels that the mules will use to ship the packages to the stuffers themselves. After they received the packages relayed by the mules, the stuffers sell the products on the black market (usually for cash) to make an illicit profit.

Drop. In underground forums, criminals refer to reshipping mules also as *drops*, a term derived from requests for mules which are often titled "drops for stuff." Most drops are people who are looking for a part-time or work-from-home job, but who are then deceived by the scam operators who pose as legitimate shipping companies [8]. Drops are the main labor force of the scam: their job is to receive packages for the stuffers, verify, photograph, repackage the contents, attach new shipping labels, and ship the packages to the stuffer (usually located in foreign countries). While they are often promised a commission per package or sometimes even a monthly salary by the scam operator, we discovered that drops are usually not paid, and, instead, they are abandoned by the operators after a short time (see Section 5.3). In this paper, we use the terms "drops" and "mules" interchangeably.

Cardholder. Next, there are *cardholders*, which is the term that the scam operators and stuffers use to refer to the owners of the stolen credit cards. Cardholders are one of the many groups of victims of the scam (alongside merchants, banks, insurers, and drops), because their credit cards are being used fraudulently by the criminals.

Merchant. Lastly, *merchants* are legitimate businesses, such as Verizon, Apple, or Amazon, who sell goods to the stuffers, not knowing that the credit card used to purchase the goods has been compromised. If they fail to identify the credit card as stolen in a timely manner, they ship the merchandise to the drop, and, in turn, often incur a significant loss through this scam. The loss is due to being robbed of the items, having paid for shipping, and having to return the funds to the cardholder (*chargeback*).

In the remainder of this paper, we adopt these terms to provide a holistic view of the underground economy of reshipping scams. In the following section, we describe in more detail how the different entities interact with each other and how the criminals operate the scam to realize an illicit profit by abusing and exploiting the cardholders, drops, and merchants.

2.2 Anatomy of a Scam Operation

All reshipping scams that we studied in this paper operate in the same way: *reshipping as a service*. A paid service that the stuffers subscribe to and pay for "on demand." The operators are paid for providing access to regularly-changing drops and charge a flat fee per shipment, or a percentage fee based on the value of the items shipped.

Figure 1 provides a slightly simplified view on how such a reshipping scam operates, and how the different entities interact with each other. First, the operator posts enticing but fake high-paying job advertisements, for work-at-home or part-time positions to various job portals, such as Craigslist (omitted from the figure). To apply for the job, applicants have to upload sensitive and personally-identifiable information, such as copies of their passport, their driver's license, or employment records, to the scammer's website (❶). Unknowingly, the applicant fell victim to the scam, even if they do not ship a single item. That is, besides becoming "drops for stuff," the victims provide sufficient information to become easy targets for identity theft where the scammers have access to all the necessary information to open bank accounts or credit cards in the victims' names. Once the scammers review the submitted application and documents, the applicant will be added to the list of drops. Note that drops are not necessarily made available to stuffers immediately. Instead, the operators might keep them unavailable in the

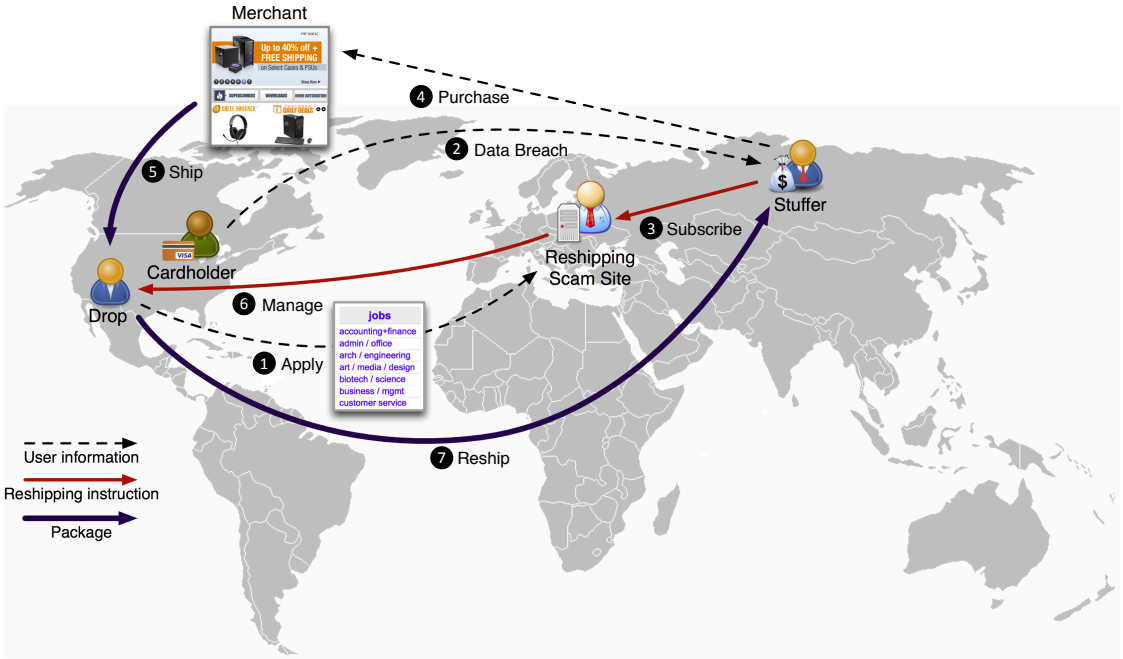


Figure 1: Operational steps of a standard reshipping scam. First, a drop applies for part-time job as a reshipper on a reshipping scam website (❶). Next, a stuffer obtains stolen credit cards (❷), e.g., through a data breach at a credit card processor or by buying them through an underground forum. To monetize these stolen credit cards, the stuffer signs up with the reshipping scam site to get access to drops (❸). The stuffer then purchases goods online, e.g., a computer, (❹), which the merchant ships to the drop (❺). The stuffer then provides a shipping label to the drop through the reshipping scam site (❻) that the drop uses to ship the goods to the stuffer (❼).

beginning to i) ensure a constant stream of drops later on, ii) to provide backup and exclusive drops for a premium, and iii) to strengthen their own reputation by advertising the size and provisions of their service. Once the operators have recruited an initial set of drops to start their operation, they advertise their services on various underground forums.

In the next step, a stuffer gains access to credit card information, possibly by breaching a credit card processor directly, or by buying the information on an underground forum (❷) [9]. For the purpose of this scam, it does not matter how the stuffer gains access to stolen credit cards. Without loss of generality and to simplify this example and Figure 1, we assume that the breach happens after the reshipping scam website has been created. To monetize the stolen credit card information the stuffer then subscribes to a reshipping scam site (❸). Stuffers can find such sites by a variety of means, such as advertisements of an operator or by actively posting requests for "drops for stuff" to an underground forum. Once a stuffer has subscribed to the reshipping service, he uses the stolen credit cards to purchase high-value or highly-demanded products (e.g., computers, cameras, lenses, or Apple products) from legitimate online retailers, such as Verizon, Apple, or Amazon. Instead of having the items shipped directly to himself, the stuffer requests a drop through the reshipping scam site and uses the drop's address as the delivery address for the package. However, instead of using the drop's name as the recipient, the stuffer provides the cardholder's name as the addressee. This serves the purpose of circumventing fraud detection systems employed at the cardholder's credit card issuer (❹).

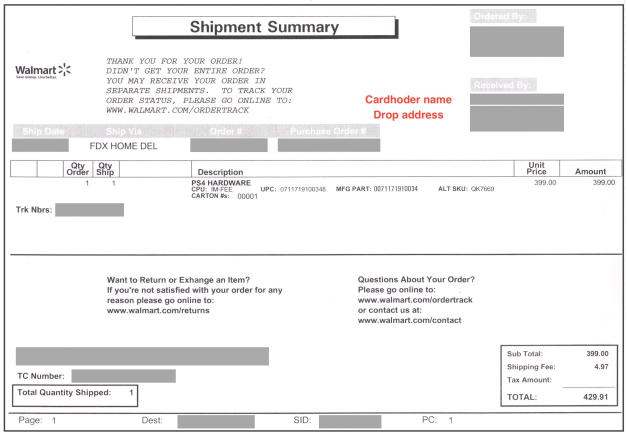
The stuffer then adds the order to the reshipping scam site, associates it with the drop, and informs the mule that a package will be arriving, addressed to the cardholder of the credit card used to buy the goods. Next, the merchant will ship the goods to the drop (❺). Upon arrival of the package, the mule is instructed to open it and repackage it. For some reshipping scam sites, the drop must also scan or take pictures of the invoice (Figure 2(a)) and of the goods that he has received for verification. The main reason this step is enforced by some operators is because they take a percentage commission based on the value of the item that the stuffer shipped through their service (see Section 5.1). Subsequently, the stuffer or operator, depending on how the site is operated, provides a prepaid shipping label to the drop (see Figure 2(b)) on which the sender field has a phony name and a bogus, but existing, address in the same city the drop resides in (❻). In our data, the destination address is with overwhelming majority in Moscow, Russia (see Section 5.4.3). Furthermore, we observe that the value disclosed on the customs form is merely a fraction of the actual value of the goods (circled red in Figure 2(b)). This allows stuffers to evade customs duty and import taxes. The drop then uses this prepaid label to ship the repackaged goods to the stuffer (❼).

Finally, the stuffer pays the scam operators, receives the packages, and resells the goods to realize their profit. For instance, in one case (see Figure 2), the stuffer bought a PlayStation 4 (with a stolen credit card) valued at 399 US dollars, which he can resell easily for 300 US dollars or more, resulting in a net profit for him of at least 100 US dollars (depending on the cost of the prepaid label and the cost of using the reshipping site; see Section 5.1).

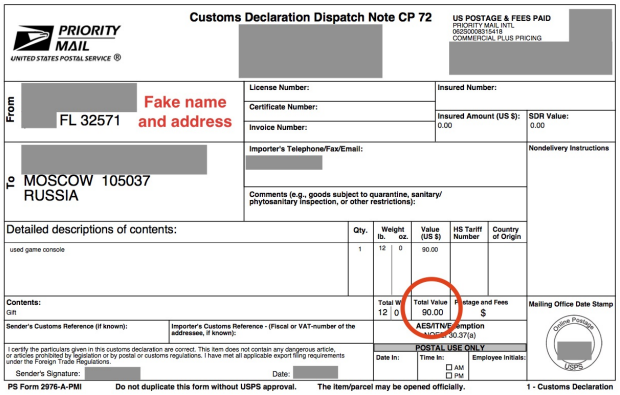
The drop remains active for about 30 days from the day of the first received package (see Section 5.3). Just as the drop should receive his first paycheck, the operator of the reshipping scam site suddenly ceases all communication with the drop and never makes the promised payment. Since the only communication channel between drop and operator was a messaging system that is tightly integrated into the reshipping website, all communication is cut by simply removing the drop's account. Eventually the drop realizes that he was scammed. In the worst case, the drop himself will be the victim of identity theft (since he uploaded identification documents during the application process) and perhaps even the subject of an investigation by local or federal law enforcement, because of his involvement in credit card fraud.

3 Data Description

We have collaborated closely with the Federal Bureau of Investigation (FBI) and the United States Postal Investigation Service (USPIS)



(a) Invoice of a Sony PlayStation 4 video game console that a stuffer purchased at Walmart and shipped through a drop.



(b) Prepaid reshipping label that the stuffer provided to the drop to ship the video game console to Moscow, Russia. Note that the customs declaration form states that it is a used game console and valued at 90 US dollars, while the original invoice states 399 US dollars.

Figure 2: Example invoice and reshipment prepaid shipping label from a purchase by a stuffer for which he utilized a reshipping scam site in our dataset (sensitive information masked).

over the course of this research effort. During this time we obtained a comprehensive and detailed dataset on seven reshipping scam websites and their operations, spanning from 2010 to 2015. We summarize the high-level statistics of our dataset in Table 1. While some reshipping scam websites have been taken down (SHIPPING-E, SHIPPING-F, and SHIPPING-G), others remain active at the time of submission and are of investigative interest to federal law enforcement. To avoid interference with any potential investigations, we use non-identifiable names to distinguish them instead of disclosing their actual names. Furthermore, disclosing the websites' names does not provide any additional insight into the scammers' operations. In the remainder of this paper, we therefore use the non-identifiable names exclusively. For each reshipping scam that we investigate, we have some or all of the following information, which we analyze in more detail in Section 5:

1) *Time Period*. The period indicates the time frame for each scam operation in our dataset. The longest running reshipping scam that we observed is SHIPPING-E, which was active for at least 12 months.
2) *Reshipping Logs*. The reshipping logs contain detailed information from the reshipping scam sites' databases, including: timestamps, corresponding stuffers, exploited cardholders, assigned drops, tracking numbers for the shipments by the merchants to the drops, and tracking numbers for the reshipped packages destined for the stuffer. The largest reshipping scam that we observed, SHIPPING-C, records 5,996 packages delivered within 9 months, i.e., over 20 packages per day have been shipped through it. Table 2 shows the breakdown of the recorded packages compared to other core elements of the reshipping logs, e.g., how many cardholders have been exploited, how many drops have been abused, and how many stuffers have profited in this specific operation. In the case of SHIPPING-C, each stuffer received 55.5 packages on average (i.e., used the reshipping service 55.5 times), 4,208 different cardholders were exploited, and each drop received nearly seven packages on average.
3) *Prepaid Labels*. Prepaid labels are the shipping labels that scammers purchase, and that are provided to the drops to ship the packages to the stuffer. All prepaid labels are PDF files, and most name the stuffer as the recipient, and provide a bogus sender address and information about the package's contents. While some information on the label is bogus (e.g., the sender address and the contents' value), the detailed description of the contents is commonly somewhat accurate. For instance, a package might contain a video game console, but instead of being used, it is actually brand new and significantly more valuable (see Figure 2(b)). We use optical character recognition (OCR) to automatically extract such information from the labels (PDF files) (see Section 5).
4) *Drop Details*. The drop details contain personally-identifiable information of drops, such as their home addresses, scans of their passports, drivers' licenses, prior employment records, and sometimes even their social security numbers. The scammers require the drops to submit this information to apply for the job in the first place. Providing this information to the scam operators bears an additional and significant risk for the drops: the operators can and are disclosing the information to stuffers if, for example, a drop is unreliable and does not reship some goods to the stuffers (see Section 5.1.1). This might be because the drop decided to keep the item or if the drop is caught by law enforcement before being able to ship the item. Disclosing this information to the stuffers is part of the agreement that the stuffer and the operator enter, and it provides the stuffer with a basic level of security because it allows them to identify the mules or abuse their information for other frauds, such as opening credit cards or bank accounts in their names.
5) *Messages*. The reshipping operations we studied feature an integrated messaging system. This messaging system is used by the scam operators to provide support to the stuffers and to the drops alike. For instance, in some cases providing the prepaid label to the drop (for the shipment to the stuffer) is part of the operator's overall service. In this case, the stuffer would request labels for shipments through the messaging system. In other cases, it is used to arrange payment by the stuffer to the operator. Similarly, a drop would report problems when trying to drop off a package at the postal office through the messaging system to the operator. Note that the integrated messaging system is the only communication channel that mules can use to contact the operator. Stuffers, however, are often provided with the information necessary to contact the operator through ICQ or Jabber for additional, time-sensitive support.
6) *Rules*. Finally, for some reshipping scam websites we have detailed information about operational policies and news updates that were posted on the websites. Additionally, this information contains the agreement that the stuffers enter into when using the service.

Note that the messages and rules provide anecdotal evidence that corroborates our hypotheses about the inner workings of reshipping scams.

To provide an in-depth analysis of the operational logistics of reshipping scams, we combine and link the separate datasets within a reshipping service. This allows us to gain novel insights on how the scam works in detail, and how the different parties interact with

Site	Time Period	Reshipping Logs	Prepaid Labels	Drop Details	Messages	Rules
SHIPPING-A	11 months in 2014 and 2015	1,960	846	88	1,889	✓
SHIPPING-B	9 months in 2013 and 2014	1,493	—	43	255	✓
SHIPPING-C	9 months in 2014 and 2015	5,996	—	106	—	—
SHIPPING-D	4 months in 2014	—	613	—	—	—
SHIPPING-E	12 months in 2010 and 2011	—	835	—	11,596	—
SHIPPING-F	2 months in 2011	991	—	—	—	—
SHIPPING-G	1 month in 2013	—	—	54	—	✓

Table 1: Summary of the site-specific data sets. Reshipping logs include detailed information about the package contents, their values, the corresponding stuffers, the receiving drops, tracking numbers, and timestamps. Prepaid labels contain information about the stuffers' locations, the cost of the labels, and the values of the items. Drop details include sensitive and personally-identifiable information, such as passports, drivers' licenses, or addresses. Messages contain interactions between stuffers and the website operators and messages between drops and the website operators. Rules contain information for stuffers on price changes for shipments, how and through what channels prepaid labels must be bought, information on refunds for lost shipments, or announcements that drops are unreliable.

Site	Time Period	Packages	Cardholders	Drops	Stuffers
SHIPPING-A	11 months in 2014 and 2015	1,960	1,184 (**1.7:1**)	82 (—)†	49 (**40.0:1**)
SHIPPING-B	9 months in 2013 and 2014	1,493	963 (**1.6:1**)	8 (—)†	71 (**21.0:1**)
SHIPPING-C	9 months in 2014 and 2015	5,996	4,208 (**1.4:1**)	881 (**6.8:1**)	108 (**55.5:1**)
SHIPPING-F	2 months in 2011	991	722 (**1.4:1**)	53 (**18.7:1**)	41 (**24.2:1**)

Table 2: Statistics on reshipping logs. The ratio in the parentheses indicates the ratio of the package counts to the counts of other elements. † Note that 75.41% packages of SHIPPING-A and 93.10% packages of SHIPPING-B have had no explicit assignment to any drop, possibly because the drop has been removed from the database. We investigate the churn of drop recruitment in detail in Section 5.3.

each other. For instance, if a reshipping log entry of SHIPPING-A indicates that stuffer *X* purchased goods with the stolen credit card of cardholder *Y* and assigned the reshipping task to drop *Z*, then we know that the credit card of victim *Y* was stolen and fraudulently charged, and that the merchant shipped a package to *Z*, whose address will appear in the drop details. From the associated prepaid label, we can then further identify the address and possibly the name of the stuffer. Continuing down this path, we can investigate the messages exchanged between *Z* and the scam operator, which might reveal that *Z* received specific reshipping instructions, e.g., to bundle two packages into one. Similarly, the interactions between the stuffer *X* and the scam operator can provide insightful information about the illegal business practices and the relationship between stuffers and operators. Due to the breadth and variety of the information available to us, we are able to provide highly-detailed insights into the operation of reshipping scams.

In addition to the site-specific data that we have analyzed, USPIS and the FBI have shared additional high-level information with us, including information on drops' addresses, label purchase services, and data on the scale of suspicious packages being shipped by drops. The provided information allowed us to expand our observations to a larger scale and to estimate the financial loss of victims (merchants, cardholders, and drops) of reshipping scams.

4 Ethics

The data that we analyze in this paper provokes various questions in respect to the ethical handling of it. First and foremost, the work that we present in this paper was conducted in full compliance with the approval of our institutional review board (IRB), as well as in close collaboration with federal law enforcement (FBI and USPIS). Furthermore, contrary to prior work, we are not trading or interacting with the operators of the scam, stuffers, or any middlemen. We are neither renting drops from the operator nor are we buying goods from the stuffers that they purchased with stolen credit cards. Over the course of this paper, we have not interacted with the victims or the scammers. Instead, we analyze information from their databases and operational logs exclusively.

However, because our data contains some personally-identifiable information (see Section 3), we must handle it properly and with extreme care. All our data is encrypted at rest (on the disk) as well as in motion (when transferred). Moreover, we use fictitious one-way pseudonyms to retain accountability but prevent disclosure of any personal information. Similarly, we abstracted addresses at a city level, which anonymizes the exact location and auxiliary information such as neighborhoods (e.g., high-income or low-income). Lastly, our work primarily presents aggregate statistics and results on the entire reshipping scam, and we are not reporting information on the victims (cardholders and drops) themselves.

Finally, the goal of this research is twofold. Primarily, we aim to provide a detailed exploration of the inner workings of reshipping scams to the research community. At the same time, this research is intended to provide law enforcement and policy makers with the most effective steps to disrupt this criminal activity and prevent more victims from being hurt by reshipping scams. We are certain that the benefits to the general public of our study strongly exceed any knowledge that the criminals might obtain from the high-level details that we present in our paper. We have worked closely with the FBI and USPIS in respect to not disclosing any information indicative of individual sites that might alert the operators.

5 Measurement and Analysis

In this section, we provide a detailed analysis of reshipping scams, calculate statistics on different aspects of them, and provide insights into the following issues: how do miscreants split the illicit profit, who are the victims, how much is the financial loss, and what is the life cycle of a drop. Furthermore, we identify potential bottlenecks in reshipping scam operations and propose intervention approaches.

5.1 Illicit Business Model

Miscreants use reshipping scams to gain an illicit profit, particularly to monetize stolen credit cards. The core component of the scam is the reshipping site, which provides "reshipping as a service" to other criminals (stuffers). A range of players participate in the scam, provide various services, and share the illicit income.

5.1.1 Agreement and Profit Split between Criminals

In exchange for renting drops out to stuffers, reshipping scam site operators charge a commission. The rule pages that we extracted

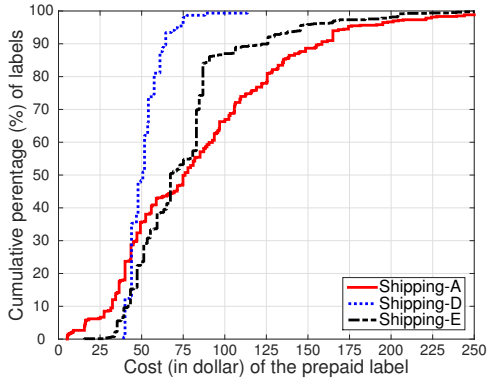


Figure 3: Distribution of prepaid label cost. The different reshipping scam sites specialize on different goods: SHIPPING-A focuses on luxury goods, SHIPPING-D targets reshipping of lower-priced items, and SHIPPING-E specializes on Apple Products. Note that SHIPPING-A includes prepaid labels to domestic addresses (within the US) to other reshipping services to further obscure the stuffers' final destination address. For SHIPPING-A, labels costing less than about 45 US dollars are almost exclusively domestic labels.

Product	Percentage	Average Price	Median Price
Apple Products	57.05%	$789	$750
iPhones	39.08%		
iPads	15.52%		
MacBooks	2.45%		
Camera Related	19.58%	$722	$500
Action Camcorder (GoPro)	14.59%		
Digital SLRs	4.57%		
Lenses	0.38%		
Flashes	0.04%		
Computer Related	13.29%	$1,030	$1,030
Laptops	8.53%		
Processors and Disks	4.19%		
Desktops	0.57%		
Other Electronics	5.40%	$611	$550
Fashion and Apparel	1.35%	$1,408	$1,000
Nutrition	0.36%	$1,020	$1,050
Miscellaneous	2.97%	$909	$689

Table 3: Product categories and prices for SHIPPING-C.

from reshipping sites expose two different business models: taking a *percentage cut* of the item's value, or charging a *flat rate* fee.

For instance, SHIPPING-A takes a percentage cut. Here, stuffers must pay a portion of the product's value to the site operator as the reshipping fee. Note that SHIPPING-A specializes on premium and high-value products, and requires a minimum value of any item shipped through it of 300 US dollars. Specifically, the operator charges up to 50% of the items' values and he maintains a detailed list of products that are eligible for reshipment. This list specifies the exact percentage cuts that the operator takes: e.g., 40–50% cut for Apple MacBooks, 35% for digital cameras and lenses, or 25% for baby strollers.

On the other hand, SHIPPING-B targets lower-priced products (e.g., clothing) and simply charges a flat-rate fee of 50 to 70 US dollars per package.

In both cases, reshipping scam site operators take a considerable portion of the profit. Stuffers are willing to pay the significant overhead because the operators play a key role in the scam: without the reshipping support, the stolen credit cards or accounts are worth little because they cannot be efficiently monetized.

In addition, reshipping sites provide a certain level of customer service for successful package delivery. If a drop who is not marked as problematic embezzles the package, reshipping sites offer free shipping for the next package or pay up to 15% of the item's value as compensation to stuffers (e.g., as compensation for "burning" the credit card or the already-paid reshipping label). Note that, in case the authorities identify the drop and intercept the package, the reshipping sites provide no compensation ("acts of God"). For a premium, stuffers can rent private drops that no other stuffers will have access to. Such private drops are presumably more reliable and are shielded from interference by other stuffers and, in turn, have a reduced risk to be discovered (hence, lower risk of losing packages).

Besides the actual drops, prepaid shipping labels are another critical resource. Historically, criminals simply created and used fake labels by modifying information and barcodes of existing labels. Once shipping companies started identifying such fraudulent labels, the miscreants started purchasing real labels but payed for them with stolen credit cards. Recently, shipping companies have become even more vigilant and started performing thorough checks on the validity of the credit cards that are used to purchase labels. This lead to successfully stopped shipments and discovered drops. Besides the shipping companies, drops became increasingly suspicious of the legitimacy of the reshipping company when the post office clerks asked where they received the label from. In response, reshipping scams prohibited the use of stolen credit cards to purchase labels and are actively imposing fines of up to 1,000 US dollars on the stuffer that violate this rule. Furthermore, such violators are threatened with public exposure if a post office declines a package because of a defective label (e.g., if the drop reports the incident to the operator). As a result, criminals moved toward "white label" shipping services [10], where the payment is made via a legitimate account (e.g., a bank account that was opened in the name of a drop with his personally identifiable information, see Section 3) or through companies. These labels are often considerably cheaper than those one would buy directly from a shipping company (due to large volume discounts). For example, criminals pay only 51.74 US dollars for a USPS Priority Mail Express label for a five-pound package to Russia, while the regular label costs 72.55 US dollars. Figure 3 provides more detail on the distribution of the costs of the prepaid shipping labels that the scammers use. In all cases, the majority of the labels costs less than 100 US dollars. Furthermore, the distribution of the label cost appears to be correlated with the value of items the scam operation targets: SHIPPING-A targets luxury goods and increases the slowest, with about 67% of all package labels costing 100 US dollars or less; SHIPPING-E focuses on Apple products, generally high-value, with nearly 90% of all prepaid labels costing 100 US dollars or less; on the other hand, SHIPPING-D specializes on lower-price items, and almost all of its labels (99%) cost 100 US dollars or less (all labels cost less than 125 US dollars). Note that the stuffers of SHIPPING-A reship to other reshipping services within the US (in Claymont, Delaware and Dover, Delaware; see Table 6), possibly to obscure their traces further. These domestic labels account for almost all labels costing less than 45 US dollars.[2]

Upon arrival of the packages at their destinations, criminals sell the goods on the black market, sometimes directly to wholesale retailers, who introduce the items into the regular and seemingly-legitimate delivery chain. Generally, in those foreign countries, the products can be sold for a 30-50% markup on top of the original purchase price, which allows scammers to increase their illicit income further. For instance, an Apple MacBook selling for 1,000 US dollars in the US, sells for 1,400 US dollars in Russia because the goods are often priced higher (custom duty, taxes, and other fees), or are difficult to acquire (sanctions, embargoes).

[2]Removing domestic labels from the cumulative percentage shifts SHIPPING-A's line to right, below SHIPPING-E.

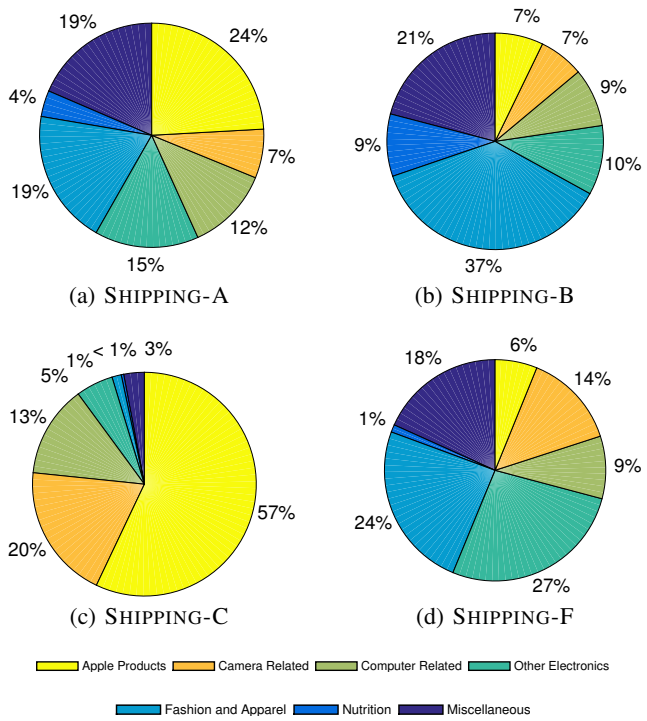


Figure 4: Proportion statistics of package content categories per reshipping scam. SHIPPING-A specializes on luxury-goods and charges a percentage cut per shipment, SHIPPING-B explicitly targets low-priced items and charges a flat fee per package, SHIPPING-C focuses on high-value electronics and charges a percentage cut, SHIPPING-F targets low to medium priced items.

5.1.2 Product Categories and Targeted Merchants

Reshipping scams tend to ship high-value and highly-demanded products to foreign countries, which can, in turn, yield a higher profit than lower-priced items. In the following, we examine the core products that cybercriminals purchase for these reshipping scams. Our findings can help retailers to avoid fraud and assist postal services to identify suspicious packages because they allow to focus attention on the products that the criminals desire. We group the products into seven categories (see Table 3): *Apple Products* (iPhones, iPads, and MacBooks), *Camera Related* (action camcorders, digital SLRs, and lenses), *Computer Related* (desktops, laptops, and parts like processors and disks), *Other Electronics* (referring to other electronic items besides the ones listed in the previous three categories, like GPS, or TVs), *Fashion and Apparel* (e.g., clothes, watches, and handbags), *Nutrition* (e.g., vitamins and sport supplements), and *Miscellaneous* (products not included in the other categories, such as power tools and baby strollers).

Figure 4 illustrates the proportions of the product categories observed for four reshipping scam operations (compare Table 2), whose logs contain detailed descriptions of the products that the stuffers purchased. For SHIPPING-C, cybercriminals heavily targeted the *Apple Products* and *Camera Related* categories (see Figure 4(c)) and, for SHIPPING-B, *Fashion and Apparel* (see Figure 4(b)). Generally, electronic products, such as iPhones and cameras, have high unit prices but are inexpensive to ship because of their limited weight and small size. Luxury and brand-name fashion and accessories are often in high-demand in foreign markets and are also less likely to be damaged in transit.

In the case of SHIPPING-C, our data also includes the purchase prices of the products that the stuffers shipped. Table 3 shows the product categories, the average prices, and the median prices of the products for each category. Scammers mainly target expensive products that are worth hundreds or even thousands of dollars. Based on the recorded unit prices, we later investigate the financial loss caused by reshipping scams in Section 5.2.2.

Rank	Store (.com)	Pct.	Rank	Store (.com)	Pct.
1	shop	26.23%	11	t-mobile	1.60%
2	verizon	14.86%	12	amazon	1.35%
3	att	13.20%	13	groupon	1.27%
4	gopro	6.18%	14	abt	0.90%
5	newegg	4.52%	15	hp	0.88%
6	sprint	3.78%	16	lenovo	0.75%
7	ebay	3.60%	17	academy	0.70%
8	apple	3.47%	18	tigerdirect	0.67%
9	bestbuy	2.78%	19	macmall	0.48%
10	walmart	1.98%	20	staples	0.43%

Table 4: Online stores targeted by stuffers who use SHIPPING-C. Top 20 of the online stores targeted by stuffers who use SHIPPING-C for reshipping, accounting for 89.63% of all packages. Note that `shop.com` works as a proxy: it handles credit card processing for merchants (e.g., Best Buy), who ship the item once the order was processed by `shop.com`.

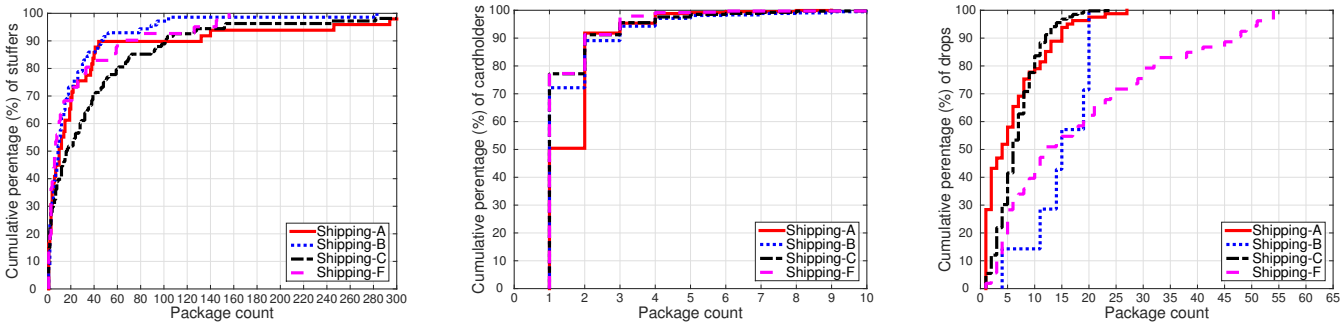
Interestingly, the log data from SHIPPING-C also specifies from which online store the items were purchased. Cybercriminals target a variety of online stores, and the stuffers using SHIPPING-C for reshipping defrauded 233 unique online stores alone. Table 4 lists the top 20 websites with the most purchases, which account for 89.63% of the packages. The store site with most illicit purchases, `shop.com`, is a large shopping comparison and marketing company, where customers can shop from many retailers and manufactures. `shop.com`, however, only sells products through their OneCart program, which works similar to Amazon Marketplace. That is, `shop.com` handles payment processing and informs the merchant to ship the product, who, in turn, ships the goods. Multiple reasons might exist why criminals prefer to use `shop.com` by such a large margin: i) fraudulent use of credit cards might not be detected as quickly as by the merchants themselves, or ii) the delay to notify the merchant when `shop.com` receives a chargeback or is alerted about a fraudulent credit card might be long enough for the items to have arrived at the drop and might have been already reshipped. This increases the response time of the merchants and payment processor which is advantageous for the cybercriminals.

5.1.3 Allocation of Drops to Stuffers

Reshipping scam operators act as service providers, renting their drops out to stuffers. As such, they have control of how many drops the stuffers can use at the same time. Subsequently, stuffers choose their drops from the candidate pool and assign reshipping tasks to them. Our data contains a snapshot of an assignment between 47 drops and 38 stuffers from SHIPPING-A. In Figure 6, the white circles on the bottom are drops, and the black circles are stuffers. A black dot on the grids means that the corresponding drop reships packages for the corresponding stuffer. Drops are ordered from left to right in the number of the associated stuffers. Stuffers are ordered from bottom to top in the number of the allocated drops. The red cross indicates the average number of drops and stuffers respectively. For instance, drops on the right side of the vertical red line have more stuffer assignments than the average drop. Note that the assignment is not exclusive, a drop can forward packages for multiple stuffers, and a stuffer can have multiple drops to distribute the reshipping tasks to. The eight left most drops (gray shade), however, are exclusive drops and serve only one stuffer.

5.2 Negative Impact and Financial Loss

Although it might appear that the prey of reshipping scams are fundamentally the users whose financial and personally-identifiable information is stolen (like credit cards and store accounts), there are several other actors who are negatively affected by the scam. Here-



(a) Package count per stuffer. (b) Package count per cardholder. (c) Package count per drop.

Figure 5: Distribution of package appointments.

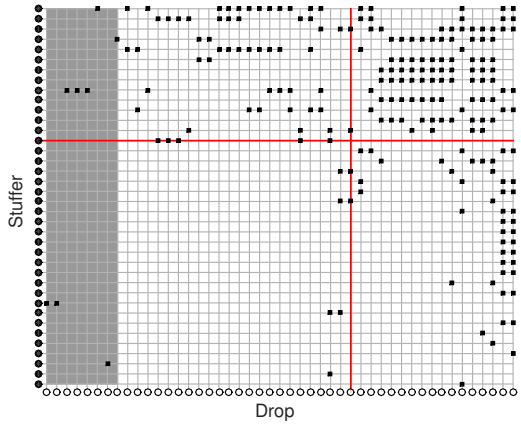


Figure 6: Mapping between drops and stuffers for SHIPPING-A**.** The white circles on the bottom indicate drops, and the black circles on the left represent stuffers. The elements on one dimension is ordered by the numbers of the associated elements on the other dimension (left to right and bottom to top). The red lines in the middle indicate the averages. The eight left most drops are exclusive (gray shade).

inafter, we identify the victims in reshipping scams, and we quantify their financial loss.

5.2.1 Victims

First, investigations by federal law enforcement confirmed that the cardholders in reshipping scams were the victims from data breaches or information theft. The problem is twofold. On the one hand, credit cards are generally insured and the cardholder rarely suffers financial loss. On the other hand, if cybercriminals steal a debit card (which, in the US, uses the same payment processing techniques as a credit card, and can often be used interchangeably) then the cardholder is not necessarily insured and often unable to dispute the transaction, leaving him alone with the financial loss the criminals incurred. In case of a compromised credit card, then the loss is distributed over different parties. First, the cardholder needs to spend time and effort to fight the fraudulent transaction. Second, the bank needs to issue and send a new credit card to the cardholder. Third, the merchant has to cover the loss of the merchandise and an additional chargeback, which can range up to 100 US dollars. Additionally, due to consumer protection against credit card fraud, retailers are usually held liable for the illicit purchases and have to reimburse the cardholder for all incurred charges. At this point, it is often too late for the retailer to retrieve the merchandise because it has been shipped out to the drop and might have already been reshipped. Furthermore, besides the chargeback fee, retailers have paid (directly or indirectly through the chargeback) for shipping to the drop. In the case that stolen credit cards are used to buy prepaid cards (which are then used to buy the actual goods), then the prepaid card issuer will face financial loss. While most cardholders appeared only once or twice, others are used for five or more times (see Figure 5(b)), increasing the damage done and the cybercriminals' profit before they need to compromise more credentials.

The unwitting drops are victims too. The miscreants often do not pay the promised salary or commission and they abuse the drops' personal information in other frauds and open bank accounts in the victims' names (see Section 5.3). While being victims of the scam, the drops also face the risk of becoming a target in lawsuits for assisting in fraud. Finally, the destination countries for the goods lose tax income and customs duty as the packages are not properly declared by the criminals.

5.2.2 Loss Estimate and Damages

Site-Specific Revenue Estimate. First, we investigate the number of illicit purchases and measure the financial loss incurred by single reshipping scam operations. The log data from four reshipping scams (see Table 2) includes the timestamps of purchases and the accumulated indexes of the packages (except for SHIPPING-F, whose index starts at 1). Figure 7 shows in more detail how the reshipping scams evolve over time. The x-axis indicates the relative time starting at the beginning of our observation periods, and the y-axis shows the package indices. We fit the package counts via least squares linear regression. Furthermore, when we project the dates back to when the package index was 0 for site SHIPPING-A and SHIPPING-C, these inferred dates match the domain registration dates of the sites, which supports the correctness of our model. The number of packages that are shipped in a specific time period through each reshipping scam appears to not increase for SHIPPING-A and SHIPPING-F (linear regression fits all recordings well). However, for SHIPPING-C, the operation appears to gain momentum as the rate of shipped packages toward the end of our dataset significantly outperforms the linear regression. In contrast, SHIPPING-B, seems to have reached its end of life at slightly over a total of 2,000 packages.

We use this model to estimate how many illicit purchases are being made by cybercriminals for a given period. Thus, in a one year period we estimate 1,911 packages being shipped through SHIPPING-A, 3,541 through SHIPPING-B, 9,009 through SHIPPING-C, and 6,673 through SHIPPING-F respectively. The annual package number from a reshipping scam site is typically in the magnitude of 1,000–10,000, while other highly-productive reshipping operations reportedly manage close to 50,000 packages in a single year. Note that, the majority of stuffers, around 80%–90%, have shipped less than 60 packages during our observation. However, a small number of stuffers ordered up to 300 packages (see Figure 5(a)).

If we further correlate the product ratios (see Figure 4) and the average prices of each category (see Table 3) with the estimated number of

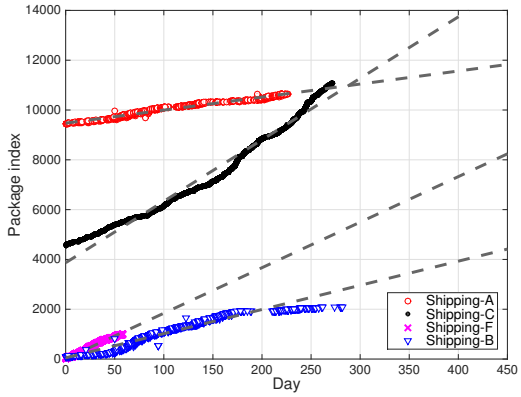


Figure 7: Linear regression of number of package (based on database index) increase over time. The day (x-axis) is relative to our first observation.

purchases, then we can estimate the annual illicit revenue of a single reshipping scam site to range from 1.8 million US dollars (SHIPPING-A) to over 7.3 million US dollars (SHIPPING-C). Note that, for simplicity and to be conservative, we do not include the potential product markup (see Section 5.1.1) in foreign countries in our revenue calculation.

Overall Financial Loss. In addition to the per-site revenue, we estimate the overall financial loss incurred by reshipping mule scams by estimating the number of cardholder victims and the damage per cardholder. For an accurate estimate, we first infer the number of cardholder victims for all reshipping scams by using a mark and recapture (capture-recapture) approach, which is a technique used to estimate a population's size in ecology and epidemiology [11]. Following, we use the Lincoln index [12]. The idea of a capture-recapture analysis is to repeatedly sample from the population to estimate its size. First, we take a sample S_1, mark, and then release it back into the population. We then take a second sample S_2 and examine the marked members of S_2, which is the intersection of S_1 and S_2. We then estimate the population $P = \frac{|S_1| \times |S_2|}{|S_1 \cap S_2|}$. For a perfectly accurate capture-recapture model some assumptions are crucial, e.g., the population is homogeneous and closed (i.e., no new entries are allowed). Some of the assumptions do not necessarily hold for our analysis, however, they have likely only negligible impact because of the significant time-wise overlap (see Table 2) and the way that credit card information is stolen (see Section 1). For example, in our case, new cardholders might be defrauded and involved in the scam, possibly reducing accuracy of the estimate slightly. However, we aim to only use the estimate for an initial approximation of the population size of the abused cardholders.

For our population estimate we consider two fraud cases as referring to the same credit card or account if the owners' names are identical and the purchases from different reshipping scam sites occur close in time. In our analysis, we use a threshold of one month since it is very likely that the fraud is detected within one month, either through automatic means or by verifying the account statement. If the time difference between two cases exceeds one month, it is likely that separate cardholder victims have the same name, or that the same victim has had his replacement credit card compromised once again. We use the two sites in our data set with most defrauded cardholders: SHIPPING-A and SHIPPING-C. They overlap for seven months, during which 761 cardholders were defrauded by stuffers using SHIPPING-A and 3,569 were defrauded by stuffers using SHIPPING-C. Three cardholders appear on both sites during the overlap period. Therefore, the estimated number of overall cardholders who are victims of reshipping mule scams per year is $\frac{761 \times 3{,}569}{3} \times \frac{12}{7} \approx 1,552,005$. Note that, while these numbers serve as an estimate, the number of stolen credit card information and potential victims is multiple magnitudes larger and our estimate is likely on the conservative side (see Section 1).

We calculate the average damage per cardholder based on exact data from SHIPPING-C's reshipping logs. Overall, we see a total of 5,505 packages with a legitimate item value (we remove 491 packages from the data for which the item's value is not provided or for which an obviously fake value is given; we only exclude items with item value less or equal to 1 US dollar). For these 5,505 packages, a total of 3,926 cardholders were defrauded with the sum of all values being 4,542,104.53 US dollars. In turn, this results in an average damage per cardholder of $\frac{4{,}542{,}104.53}{3{,}926} = 1,156.93$ US dollars.

Finally, by multiplying the average loss per cardholder with the estimated overall number of cardholders, we can estimate that the overall reshipping scam revenue is around 1.8 billion US dollars per year.

5.3 Drop Recruitment

Drops are the main labor force in the reshipping scam as they receive and reship goods for the cybercriminals. In this section, we investigate the characteristics of drops and the timing patterns when they sign up and relay packages, and where the drops are located.

5.3.1 Drop Churn / Life Cycle

First, to better understand how and when the criminals utilize the drops (i.e., to analyze their life cycle), we investigate the signup time of drops and when they are first associated with packages. Figure 8 shows the life cycles of drops in more detail. The x-axis indicates the relative days, and the y-axis presents the indices of drops observed from SHIPPING-A. A red circle indicate an assignment event where a stuffer assigns a reshipping task to a drop, with the size of the circle being proportional to the number of packages assigned on any given date. A black line indicates the idle period between the day when a drop has successfully signed up at the reshipping scam site and the day of his first assignment.

A drop receives packages shortly after he has signed up, usually after a few days. We observe a clear churn pattern in the drops' life cycles: Cybercriminals stop using the drops after around 30 days and start to employ a new batch of drops. The hypothesis is that the reshipping sites abandon the drops before the first expected paycheck dates. We examined the message exchanges between the reshipping site operators and the drops to verify this hypothesis. As a concrete example, on day two after the drop signed up, the drop sent an email to confirm when he will receive his first paycheck (*"I know the pay is only once a month so when will I receive my first check!? "*). In the weeks after, the drop and the site operator had frequent contact about issues regarding packages and labels. On day 30, the drop asked again: *"Exactly what time will my check be deposited into my account Monday!?"*, to which the site operator replied that he would receive it: *"by the end of Monday"*. The drop then continued to reship packages. On day 35, the drop inquired again about his payment date (*"What time will I be paid!?"*). The site operator then instructed the drop to ship all packages to receive the check, likely to make sure all merchandise has been shipped. On day 36, we observe that the drop asked again about his payment (*"When will my check be deposited!?"*), to which the operator never replied. We have found multiple other instances in which drops complained about not receiving compensation and none of the messages in our data set showed any proof that drops successfully received payments. Our findings strongly suggest that the cybercriminals intentionally make no payment to the drops, which results in fast drop turnover and requires regular recruitment. Without actually paying mules, the scammers save money while being able to advertise high salaries and compensation, which, in turn, attracts more drops. For example, SHIPPING-A promised drops a monthly salary of 2,500 US dollars.

Overall, the criminals utilize an average drop to reship between five (SHIPPING-A) and fifteen (SHIPPING-F) packages, with some outliers reshipping over 50 packages during their 30-day lifetime (SHIPPING-F). Figure 5(c) shows the distribution of the counts of packages delivered to the drops. Interestingly, different sites exhibit differ-

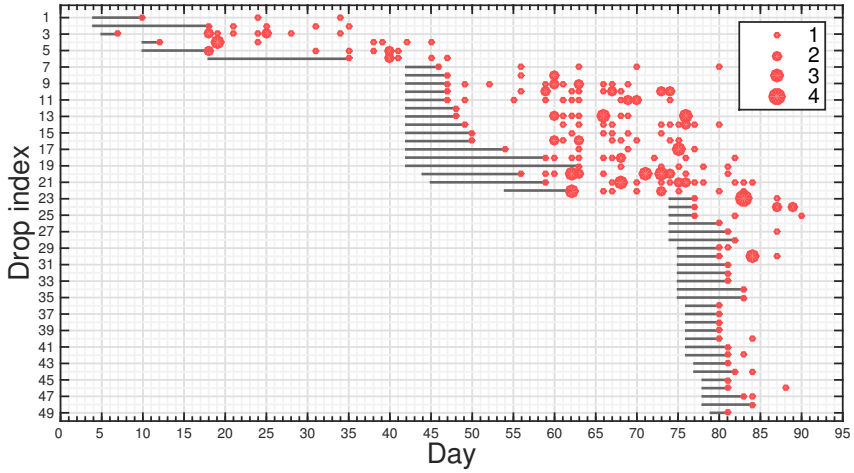


Figure 8: Life cycle of drops for SHIPPING-A**.** The red circles represent assigned package counts. The black horizontal lines indicate the periods from drop signups to the first packages.

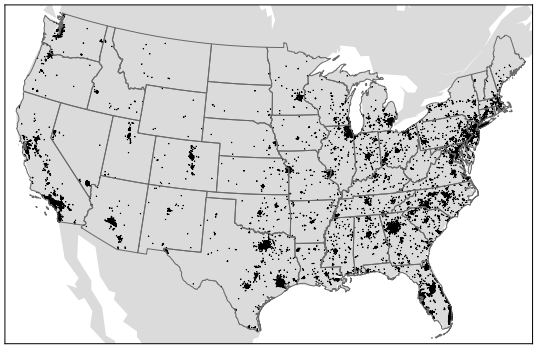


Figure 9: Locations of the drops.

Rank	State	Drop likelihood	Difference to US 2014 Annual Unemployment Rate
1	Georgia	0.01099%	▲ + 1.0%
2	Nevada	0.01011%	▲ + 1.6%
3	Delaware	0.00951%	▽ – 0.5%
4	Florida	0.00919%	▲ + 0.1%
5	Maryland	0.00868%	▽ – 0.4%
6	North Carolina	0.00710%	▽ – 0.1%
7	Mississippi	0.00674%	▲ + 1.6%
8	Arizona	0.00667%	▲ + 0.7%
9	Illinois	0.00608%	▲ + 0.9%
10	Virginia	0.00599%	▽ – 1.0%

Table 5: Drop states. States are ordered decreasing in the drop likelihood (number of drops in a state / population of state) and the difference of the state unemployment rates to the average unemployment rate in the US in 2014 (above (▲) or below (▽) the average).

ent trends: SHIPPING-C replaces drops significantly more quickly than SHIPPING-F, while both have about the same number of packages reshipped in the same time frame (see Figure 7). For SHIPPING-B, drops ship at least four packages and half of them ship 14 packages or more.

5.3.2 Geography

Figure 9 shows the distribution of city-level addresses of drops. In the US, five states, California, Florida, Texas, Georgia, and New York, account for 44.33% of the drops. However, only in one of those states, namely Georgia, the likelihood to encounter a mule at random among the state population exceeds 0.01%. To measure the likelihood that a resident of a state is recruited as a mule, henceforth called *drop likelihood*, we divide the number of drops in a state (observed in our data) by the entire population of that state [13]. We summarize our findings in Table 5, which shows the rankings of the top 10 states in terms of drop likelihood (in decreasing order).

Finally, we compare the annual unemployment rates of these states in 2014 [14] to the federal average. The last column in Table 5 lists the differences of the state unemployment rates compared to the federal unemployment rate, where ▲ indicates a higher unemployment rate in that state and ▽ indicates a lower rate. Most states, except Virginia (rank 10), have unemployment rates close to or above the US average rate, which could indicate that cybercriminals target unemployed or underemployed groups to recruit mules.

5.4 Intervention Analysis

All parties who are actively losing money through shipping scams (see Section 5.2) have a strong incentive to prevent these fraudulent transactions. In this spirit, many merchants stopped shipping to high-risk countries, such as Russia, and have been shipping goods exclusively within the US for some time. This, in turn, prompted cybercriminals to adopt the reshipping mule scheme that we analyze in this paper.

In this section, we outline promising ways in which shipping service companies can aid in combating this monetization technique and help to reduce the damage done to the businesses involved, by identifying suspicious packages before they leave the country. While we discuss these measures separately, the individual approaches can be combined to pinpoint high-risk packages, which can be inspected by law enforcement.

A successful identification of a reshipping-scam-originating package can soften the blow on victim merchants (the merchandise can be returned), and stop criminals from profiting since they do not receive the goods that they were planning on selling on the black market. We argue that the cost of this selective increased screening of suspicious packages can be covered by the most victimized vendors, since the cost is likely to be many times smaller than the cost of stolen merchandise.

5.4.1 Access Patterns

One way to detect suspicious packages is by analyzing how, when, and from where tracking information of possibly-suspicious packages is accessed at the shipping provider's or a third-party's package tracking website. This information can include data points such as the browsers' user-agent of the visitors, their source IP addresses, their timezones, or their languages. For instance, tracking information for a package from Walmart to a person living in California will (in most cases) not be tracked exclusively by someone in Russia. As such, if a website visitor from a different country is tracking a package more actively than the actual recipient or sender, then this can be a strong indicator that the package might be suspicious.

Site	Destination	Label Percentage
SHIPPING-A	*Moscow Area, Russia*	*85.89%*
	Moscow, Russia	80.66%
	Balashiha, Russia	3.65%
	Sverdlovskiy, Russia	0.97%
	Gorodok, Russia	0.61%
	Claymont, DE, US	6.08%
	Dover, DE, US	2.43%
	Other Cities	5.60%
SHIPPING-D	*Moscow Area, Russia*	*89.07%*
	Zheleznodorozhnyj, Russia	63.13%
	Balashiha, Russia	25.77%
	Moscow, Russia	0.17%
	Kiev, Ukraine	10.11%
	Nikolaev, Ukraine	0.49%
	Other Cities	0.33%
SHIPPING-E	*Moscow, Russia*	*91.14%*
	Krasnodar, Russia	4.36%
	Stavropol, Russia	1.45%
	Other Cities	3.05%

Table 6: Destinations of the reshipped packages. Moscow and its suburbs account for a clear majority of the packages final destination regardless of the reshipping site and the items it targets. At least 85% of all packages are being reshipped to Moscow.

5.4.2 Label Purchases

Similar to analyzing access patterns to identify suspicious packages, one can track who purchases package labels and through which channels. The prepaid labels are being used when the drops mail the package to the stuffer (see Figure 1, ❼) and, therefore, the corresponding shipments constitute the last chance to intervene before the merchandise reaches the stuffer and the damage is irreversible. For instance, to identify a suspicious package, one can analyze the buyer of a package label, the extent to which a single account pays for multiple different labels (e.g., "white label" services), or if packages always go to the same destination but are being shipped by different senders, e.g., by identifying if a label provider acts as a hub in the scheme. Based on this information, a risk score can be assigned to each label service who sold the label and for each individual purchased label. This risk score then captures how likely it is that the package contains goods paid for through illicit means, allowing to selectively delay it, and aiding in discovery and recovery.

5.4.3 Reshipping Destinations

The final destinations of the packages that are reshipped are usually overseas (e.g., in Russia). A stuffer is more likely to use addresses within a small area for his packages that is under his control so that he can retrieve it without any issues. Although it is often impossible to apprehend criminals who are abroad, the patterns of reshipping destinations can help to intercept the international shipping packages before they leave the country, e.g., at an USPS International Service Center.

To better understand the distribution of the final destinations, we use OCR techniques to extract the recipient addresses in the "To" fields from the electronic shipping labels (see Figure 2(b)). Table 6 breaks down the destination cities of the packages. We see a clear trend that the stuffers ship to Moscow and its suburbs (including Zheleznodorozhnyj and Balashiha) and we notice that scammers tend to send the packages to a limited number of addresses and cities, presumably to collect the packages easily. Focusing inspection efforts on the packages destined to the stuffers' prime destination cities can increase the success of intercepting items from reshipping scams.

6 Related Work

This paper is the first large-scale, in-depth study of reshipping scams. In this section we first analyze previous research on related topics, such as "money mules" (for money laundering) and mule recruiting in general. Then we briefly describe previous research that studied other parts of criminal operations.

6.1 Mule Studies

A first report on reshipping scams was published by the US Postal Service in 2004 [8]. The report describes a scheme in which people were recruited online to receive packages containing goods purchased with stolen credit cards at their homes and sending them to a postal box where the cybercriminal could collect them. The analysis performed in this paper shows that this scheme has considerably evolved over the last years, and that it is now controlled by well-organized criminal groups.

A wealth of research studied the means of cybercriminals to recruit mules, and analyzed their demographics. Goett examined the recruitment of money mules via online job boards [15] by collecting 126 email alerts from two job aggregators, and discovering 177 mule posts on 80 different job boards during seven weeks. Goett's main findings include that scammers tend to post jobs under multiple company names, use a chain of mules to launder money, and prefer mules that respond quickly to requests. Florencio et al. showed that participating in money laundering made mules liable according to the US consumer protections against fraud [16], and resulted in mules losing money. The study also suggested that the mule recruitment is the bottleneck in online fraud. In this paper, we shed light on various components of reshipping scams, providing the research community with useful insights on this increasingly popular monetization method for compromised payment instruments.

Moore et al. analyzed websites used to recruit mules on the Internet and discovered that such sites show the tendency of staying online for long periods of time even after they have been reported to Internet Service Providers and law enforcement [17]. Aston et al. examined the age, gender, and ZIP code of 660 confirmed money mule cases during 2007, gathered by a major Australian financial institution [18]. Their results showed that mule recruitment trended toward males between ages 25–34. Jones et al. conducted a 75-day analysis about the monetization methods used by Nigerian scammers by creating 56 honeypot Craigslist ads [19] and interacting with the scammers that contacted them. The authors find that victimized sellers can, among others, become money mules, by caching fake checks sent to them as compensation for their sold products, and wiring a portion of the money to scammers.

6.2 Cybercrime Studies

The reshipping scam schemes exposed in this paper are a popular method used by cybercriminals to monetize stolen credit cards and are therefore often used in conjunction with other fraud and information-stealing schemes. In 2009, Stone-Gross et al. hijacked Torpig, an information stealing botnet, and performed a detailed study of the stolen data type and bot population [5]. Among other types of data, the Torpig botnet specialized in stealing credit card information from infected computers. Reshipping scams could potentially have been employed by the cybercriminals to monetize the stolen credit cards.

A wealth of work has been conducted on analyzing cybercriminal operations involving email spam and the underground economy surrounding it. Levchenko et al. [20] analyzed the monetization of spamming botnets, and, in particular, studied the spam-advertised pharmaceutical, software, and replica affiliate programs. Other studies analyzed the coordination of spamming botnets and estimated the illicit profit of cybercriminals [21–25]. Stringhini et al. developed a methodology to track the different actors involved in spam operations, and analyzed the relationships between these actors [26]. Kanich et al. infiltrated the Storm botnet and measured the conversion rate of spam [21]. McCoy et al. analyzed customer demand and operation overheads of spam campaigns

by using transaction logs of pharmaceutical affiliate programs [27]. Our work complements previous research by providing insights in a monetization scheme that had, so far, evaded the attention of researchers.

Other research has examined how cybercriminals recruit workers for various illicit operations [28, 29]. Meiklejohn et al. studied the anonymity of bitcoin users [30]. Bitcoin and other digital currencies are another method that cybercriminals use to launder the money , which can be used instead of the reshipping schemes described in this paper. Note, however, that attackers cannot account for the unpredictability of the value of digital currencies thus, we argue that, monetization through reshipping scams is more profitable for attackers and thus, more likely to be chosen over alternative monetization schemes.

7 Conclusion

In this paper, we presented the first in-depth and large-scale study of *reshipping as a service*, a prominent way that cybercriminals use to monetize stolen credit cards and other financial instruments. We have shown that criminals operate reshipping scams in different ways, target different goods to be shipped through them, provide different levels of service and guarantees, charge different fees, and split profits differently. Yet, our results also highlight similarities between different reshipping scams when it comes to drop recruiting, management, and churn. That is, the scam operators advertise work-from-home and part-time jobs for recruitment and abandon mules by ceasing all communications shortly before the mules should be paid.

Furthermore, we have shown that a single criminal-operated reshipping service (SHIPPING-C) can earn a yearly revenue of over 7.3 million US dollars, most of which is profit. Additionally, based on our analysis, we can estimate that nearly 1.6 million stolen credit cards are fraudulently charged as part of reshipping scams each year. These stolen credit cards, in turn, result in an estimated overall revenue for criminal-operated reshipping scams of 1.8 billion US dollars, and are possibly responsible for damages up to the same amount to merchants, credit card holders, banks, and insurers. Finally, we proposed various techniques that can be leveraged to disrupt the operation of reshipping scams by identifying, and selectively delaying or stopping packages containing repackaged merchandise that was purchased with stolen credit cards.

8 Acknowledgments

We thank the reviewers for helpful feedback and suggestions to improve the paper. We also thank Jamie Portell and Jonathan Todd Bame of the United States Postal Inspection Service (USPIS) for their valuable insights and the many thought-provoking discussions.

This work was supported by the Office of Naval Research (ONR) under grant N00014-12-1-0165, the Army Research Office (ARO) under grant W911NF-09-1-0553, the Department of Homeland Security (DHS) under grant 2009-ST-061-CI0001, the Cyber Research Institute, and the National Science Foundation (NSF) under grant CNS-1408632.

References

[1] K. Zetter. Hackers Breached Adobe Server in Order to Sign Their Malware. WIRED, Sep. 2012. http://www.wired.com/2012/09/adobe-digital-cert-hacked/.

[2] The New York Times. For Target, the Breach Numbers Grow. Apr. 2014. http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html.

[3] R. Sidel. Home Depot's 56 Million Card Breach Bigger Than Target's. Wall Street Journal, Sep. 2014. http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

[4] B. Krebs. Harbortouch is Latest POS Vendor Breach. Krebs On Security, May 2015. http://krebsonsecurity.com/2015/05/harbortouch-is-latest-pos-vendor-breach/.

[5] B. Stone-Gross, M. Cova, L. Cavallaro, B. Gilbert, M. Szydlowski, R. Kemmerer, C. Kruegel, and G. Vigna. Your Botnet is My Botnet: Analysis of a Botnet Takeover. In *ACM Conference on Computer and Communications Security (CCS)*, Nov. 2009.

[6] KTVB News. New Boise Scam Entices Victims to Ship Stolen Goods. Jul. 2014. http://www.ktvb.com/story/news/local/2014/07/15/12701471/.

[7] WAFF News. Re-shipping Scam Can Turn Job Seekers into Unwitting Criminals. Mar. 2014. http://www.waff.com/story/25034260/re-shipping-scam-can-turn-job-seekers-into-unwitting-criminals.

[8] USPIS, Delivering Justice Work @ Home Scams: They Just Don't Pay!, 2004.

[9] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker. An Analysis of Underground Forums. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference (IMC)*, Nov. 2011.

[10] B. Krebs. 'White Label' Money Laundering Services. Krebs On Security, Aug. 2014. http://krebsonsecurity.com/2014/08/white-label-money-laundering-services/.

[11] G. Arthur and F. Seber, The Estimation of Animal Abundance and Related Parameters., Jan. 1973.

[12] F. Lincoln. Calculating Waterfowl Abundance on the Basis of Banding Returns. Ser. Circular (United States. Dept. of Agriculture). U.S. Department of Agriculture, 1930. https://books.google.com/books?id=w4n_MQEACAAJ.

[13] U.S. Census Bureau. Annual Estimates of the Resident Population: 2014 Population Estimates. Dec. 2014. http://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=PEP_2014_PEPANNRES.

[14] Bureau of Labor Statistics. Regional and State Unemployment – 2014 Annual Averages. Mar. 2015. http://www.bls.gov/news.release/srgune.htm.

[15] J. Goett. Measuring the Presence of Money Mule Recruitment in Online Job Boards. UC Berkeley, Tech. Rep., May 2012.

[16] D. Florencio and C. Herley. Phishing and Money Mules. In *Proc. IEEE Workshop on Information Forensics and Security*, Dec. 2010.

[17] T. Moore and R. Clayton. The Impact of Incentives on Notice and Take-down. In *Proc. IEEE Workshop on Information Forensics and Security*, Jun. 2008.

[18] M. Aston, S. McCombie, B. Reardon, and P. Watters. A Preliminary Profiling of Internet Money Mules: An Australian Perspective. In *Proc. Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*, Jul. 2009.

[19] J. Jones and D. McCoy. The Check is in the Mail: Monetization of Craigslist Buyer Scams. In *Proc. 9th Symposium on Electronic Crime Research*, Sep. 2014.

[20] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, D. McCoy, N. Weaver, V. Paxson, G. M. Voelker, and S. Savage. Click Trajectories: End-to-End Analysis of the Spam Value Chain. In *IEEE Symposium on Security and Privacy*, May 2011.

[21] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, V. Paxson, G. M. Voelker, and S. Savage. Spamalytics: An Empirical Analysis of Spam Marketing Conversion. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, Oct. 2008.

[22] C. Kanich, N. Weaver, D. McCoy, T. Halvorson, C. Kreibich, K. Levchenko, V. Paxson, G. Voelker, and S. Savage, Show Me the Money: Characterizing Spam-advertised Revenue. *USENIX Security Symposium*, Aug. 2011.

[23] B. Stone-Gross, T. Holz, G. Stringhini, and G. Vigna. The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, Mar. 2011.

[24] J. Iedemska, G. Stringhini, R. Kemmerer, C. Kruegel, and G. Vigna. The Tricks of the Trade: What Makes Spam Campaigns Successful?, in *International Workshop on Cyber Crime*, May 2014.

[25] C. Kreibich, C. Kanich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage. Spamcraft: An Inside Look at Spam Campaign Orchestration. In *USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, Apr. 2009.

[26] G. Stringhini, O. Hohlfeld, C. Kruegel, and G. Vigna. The Harvester, the Botmaster, and the Spammer: On the Relations Between the Different Actors in the Spam Landscape. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Jun. 2014.

[27] D. McCoy, P. A., G. Jordan, N. Weaver, C. Kreibich, B. Krebs, J. Voelker, S. Savage, and K. Levchenko. PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs. In *USENIX Security Symposium*, Aug. 2012.

[28] M. Motoyama, D. McCoy, K. Levchenko, S. Savage, and G. M. Voelker. Dirty Jobs: The Role of Freelance Labor in Web Service Abuse. In *USENIX Security Symposium*, Aug. 2011.

[29] Y. Park, J. Jones, D. McCoy, E. Shi, and M. Jakobsson. Scambaiter: Understanding Targeted Nigerian Scams on Craigslist. In *Network and Distributed System Security Symposium (NDSS)*, Feb. 2014.

[30] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In *ACM SIGCOMM Conference on Internet Measurement Conference (IMC)*, Oct. 2013.