Drops for Stuff

An Analysis of Reshipping Mule Scams

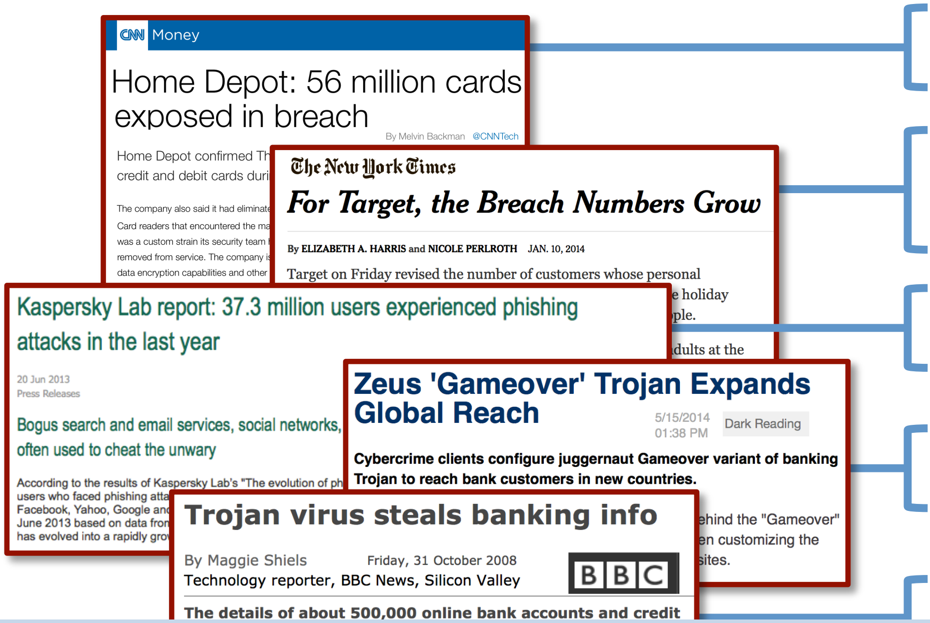
Giovanni Vigna

UC Santa Barbara
http://www.cs.ucsb.edu/~vigna

Lastline, Inc.
http://www.lastline.com

Overview

Prevalence of Data Breaches and Theft



CNN Money

Home Depot: 56 million cards exposed in breach

By Melvin Backman @CNNTech

Home Depot confirmed Th
credit and debit cards duri

The company also said it had eliminate
Card readers that encountered the ma
was a custom strain its security team
removed from service. The company is
data encryption capabilities and other

The New York Times

For Target, the Breach Numbers Grow

By ELIZABETH A. HARRIS and NICOLE PERLROTH JAN. 10, 2014

Target on Friday revised the number of customers whose personal
e holiday
ple.
dults at the

Kaspersky Lab report: 37.3 million users experienced phishing attacks in the last year

20 Jun 2013
Press Releases

Bogus search and email services, social networks, often used to cheat the unwary

According to the results of Kaspersky Lab's "The evolution of ph
users who faced phishing atta
Facebook, Yahoo, Google and
June 2013 based on data fron
has evolved into a rapidly grov

Zeus 'Gameover' Trojan Expands Global Reach

5/15/2014 01:38 PM Dark Reading

Cybercrime clients configure juggernaut Gameover variant of banking Trojan to reach bank customers in new countries.

ehind the "Gameover"
en customizing the
sites.

Trojan virus steals banking info

By Maggie Shiels Friday, 31 October 2008
Technology reporter, BBC News, Silicon Valley

BBC

The details of about 500,000 online bank accounts and credit

Home Depot breach (2014)
56 million cards

Target breach (2013)
40 million cards
70 million user info

Phishing (2013)
37 million users

Zeus Gameover (2014)
1 million PCs

Torpig botnet (2008)

Your Botnet is My Botnet: Analysis of a Botnet Takeover
Stone-Gross, Cova, Cavallaro, Gilbert, Szydlowski, Kemmerer, Kruegel, Vigna
ACM CCS, November 2009

Overview

How to Monetize?

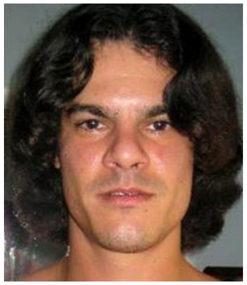


Photo of Albert Gonzalez by U.S. Secret Service

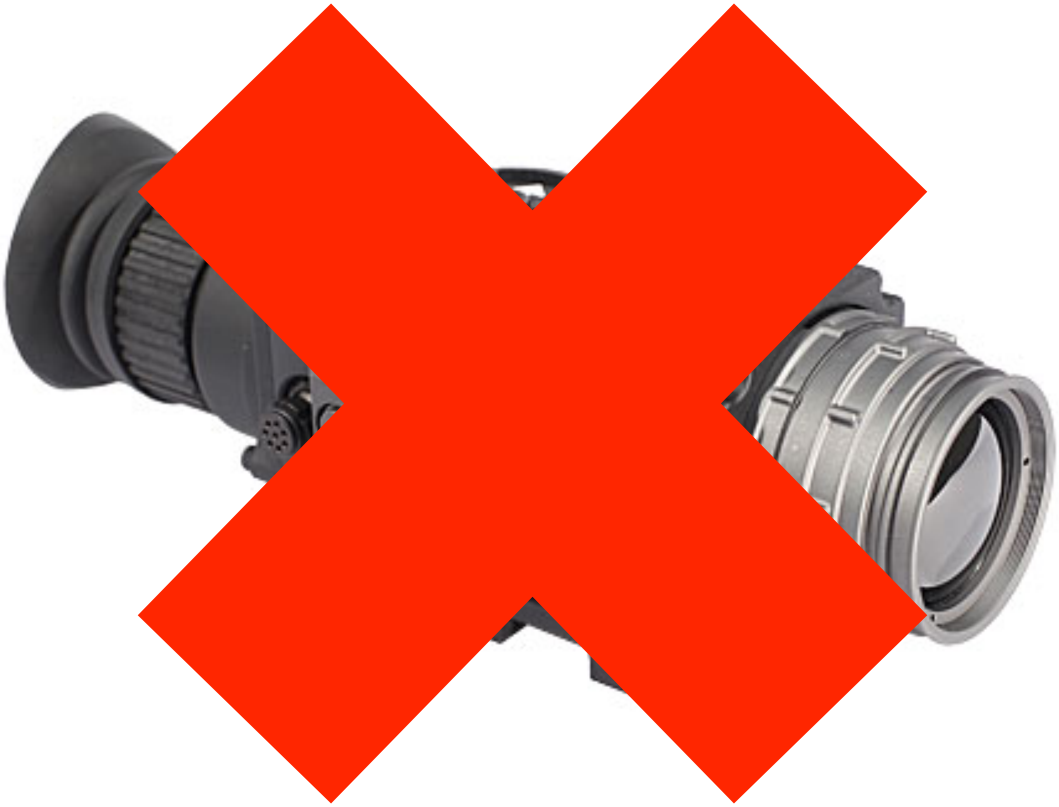
Criminal penalty 20 years federal prison
Criminal status serving sentence
Source: Wikipedia

Overview

How to Monetize?

Overview

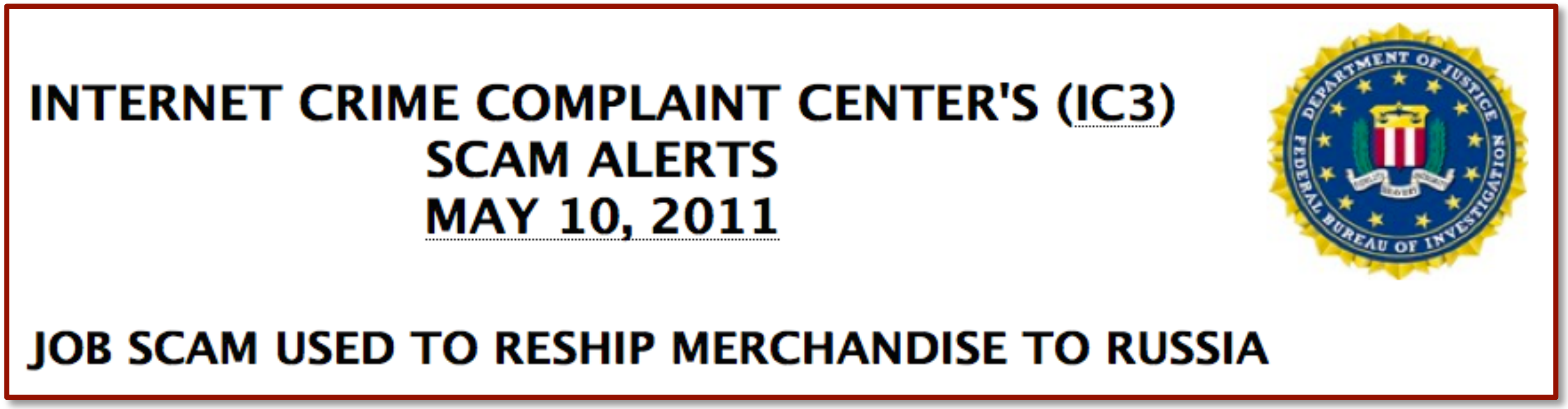
How to Monetize?



Overview

Reshipping Scam

- Recruit mules to receive and reship packages to cybercriminals overseas



INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
MAY 10, 2011

JOB SCAM USED TO RESHIP MERCHANDISE TO RUSSIA

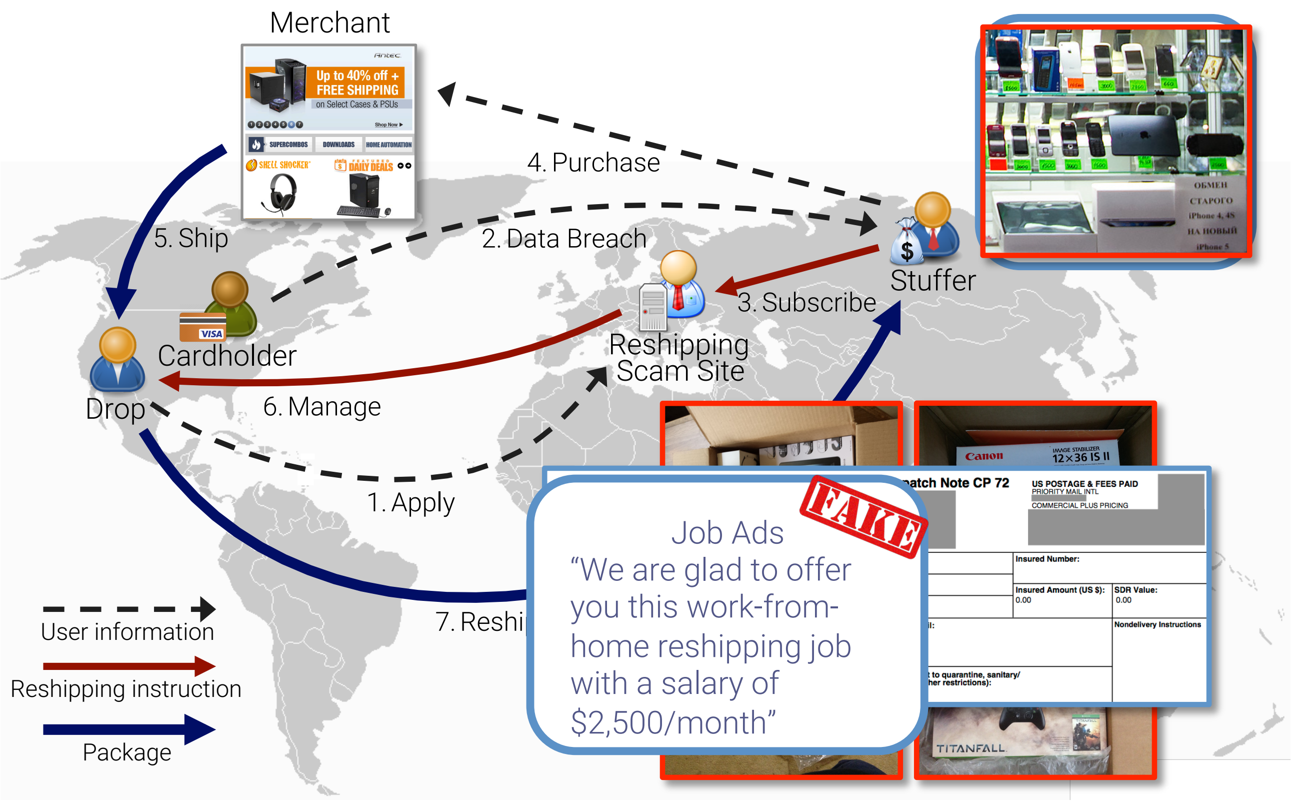
Our Work

- Analysis of log data from reshipping scams

- Characterization and measurement
  - Operation: business model, targeted products, label purchase
  - Negative effect: scam victims, financial loss
  - Mule: life cycle, geographical locations

- Intervention against reshipping scam services

Reshipping Scam Operation



Merchant

Stuffer

Reshipping Scam Site

Cardholder

Drop

1. Apply

2. Data Breach

3. Subscribe

4. Purchase

5. Ship

6. Manage

7. Reshi

Job Ads
“We are glad to offer you this work-from-home reshipping job with a salary of $2,500/month”

FAKE

User information

Reshipping instruction

Package

Data Summary

Site	***Time Period***	***Reshipping Logs***	***Prepaid Labels***	***Drop Records***
Site-A	11 months (2015)	1,960	846	88
Site-B	9 months (2014)	1,493	------	43
Site-C	9 months (2015)	5,996	------	106
Site-D	4 months (2014)	------	613	------
Site-E	12 months (2011)	------	835	------
Site-F	2 months (2011)	991	------	------
Site-G	1 month (2013)	------	------	54

Operation Policies

- How to split the illicit profit?
- What are the main targeted products?
- How to acquire prepaid shipping labels?

Agreement and Profit Split

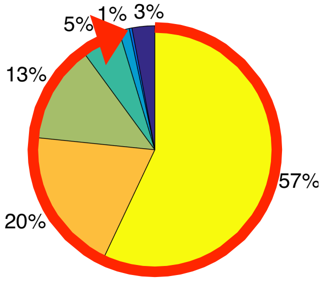
- Reshipping as a service
  - Percentage cut: up to 50% value (high-value products)
  - Flat rate: $50-$70 per package (lower-priced products)

- “Customer service” and compensation
  - Drop status (“active” or “problematic”)
  - 15% compensation for lost packages, or free shipping

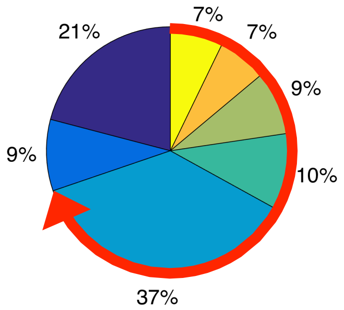
Products

		Product Category	Median Price (Site-C)
Electronics	🟨	Apple Products	$750
	🟧	Camera Related	$500
	🟩	Computer related	$1,030
	🟩	Other Electronics	$550
	🟦	Fashion and Apparel	$1,000
	🟦	Nutrition	$1,050
	🟪	Miscellaneous	$689

Site-C



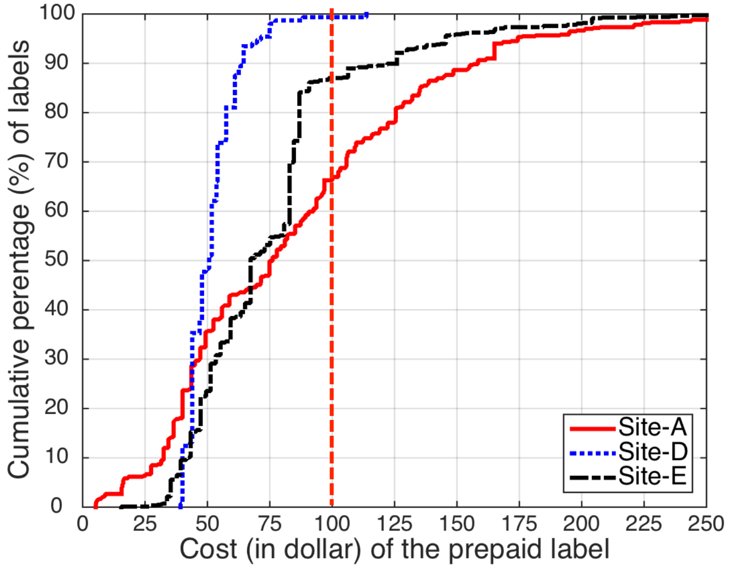
Site-B



Above 70% of the products are electronics and luxury clothing

Operation

Label Purchase



The “white labels” have relatively cheap prices, less than $100 per package

Victims & Loss

Negative Effect

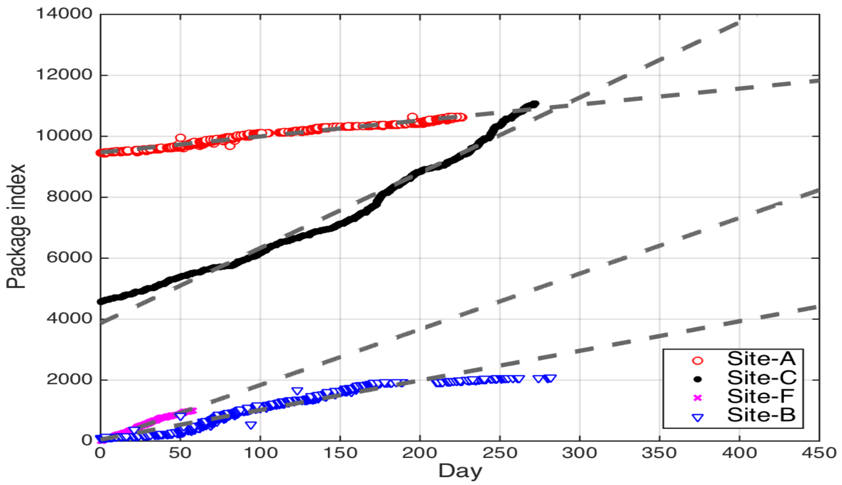
Victims

- Main victims
  - Merchant: Liability to reimburse cardholders, loss of products, chargeback (up to $100)
  - Drop: Fake job with no payment, identity fraud

- Other victims
  - Cardholder
  - Card issuer
  - Destination country

Victims & Loss

From Package to Revenue



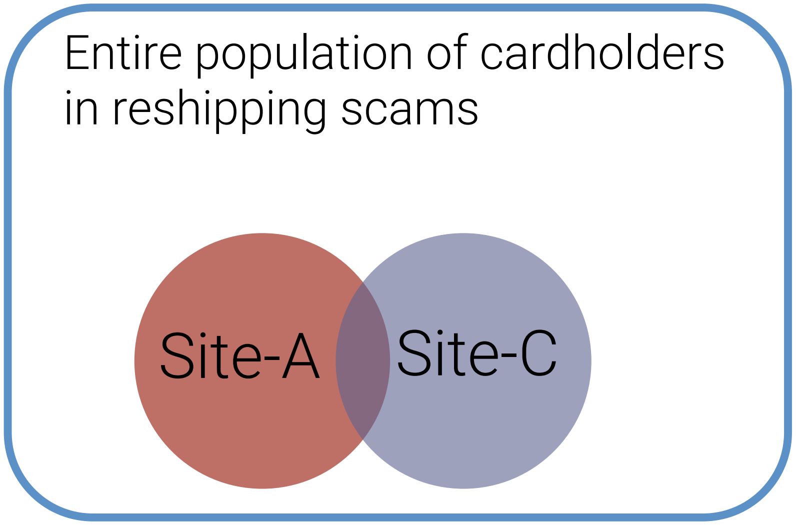
Estimated package number per year

Site-C	9,009
Site-F	6,673
Site-B	3,541
Site-A	1,911

Revenue = # packages x average product price

Site-specific revenue is up to $7.3 million per year

Overall Revenue Estimate



Population estimate

$$= \frac{|A| \times |C|}{|A \cap C|}$$

≈ 1.6 million victim cardholders per year

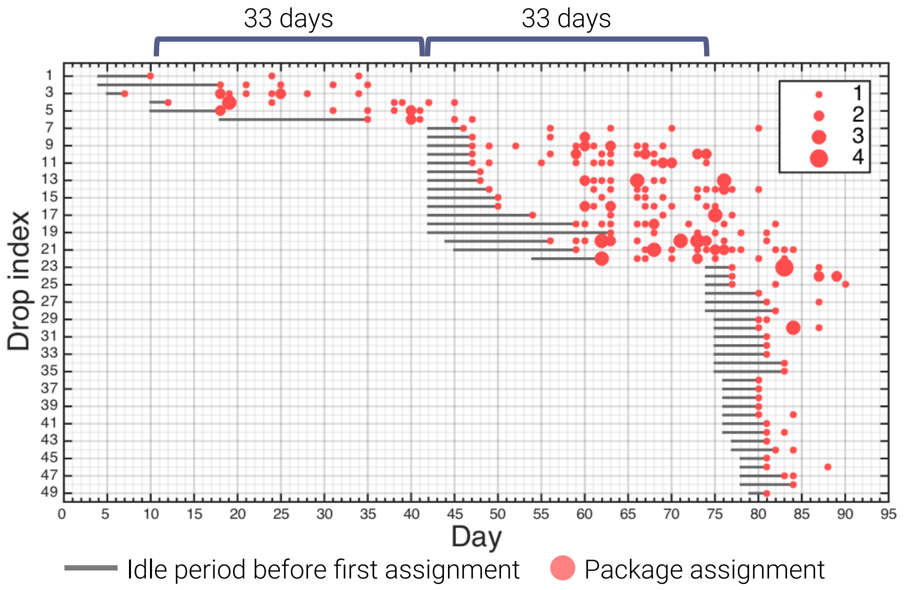
Overall estimated revenue is $1.8 billion per year

Drop Recruitment

- How long do drops remain active?

- Where are the drops?

Life Cycle of Drops



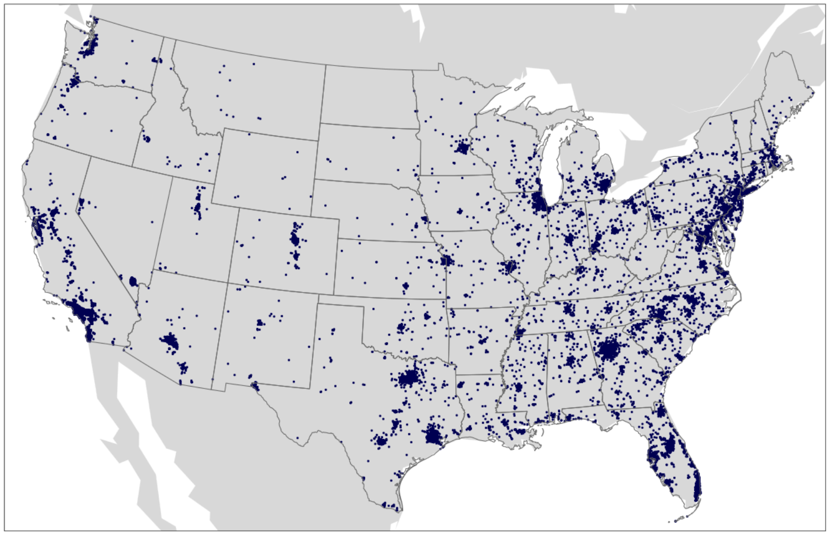
I know the pay is only once a month so when will I receive my first check!?

What time will I be paid!?

When will my check be deposited!?

Drops are abandoned without getting paid after about 30 days

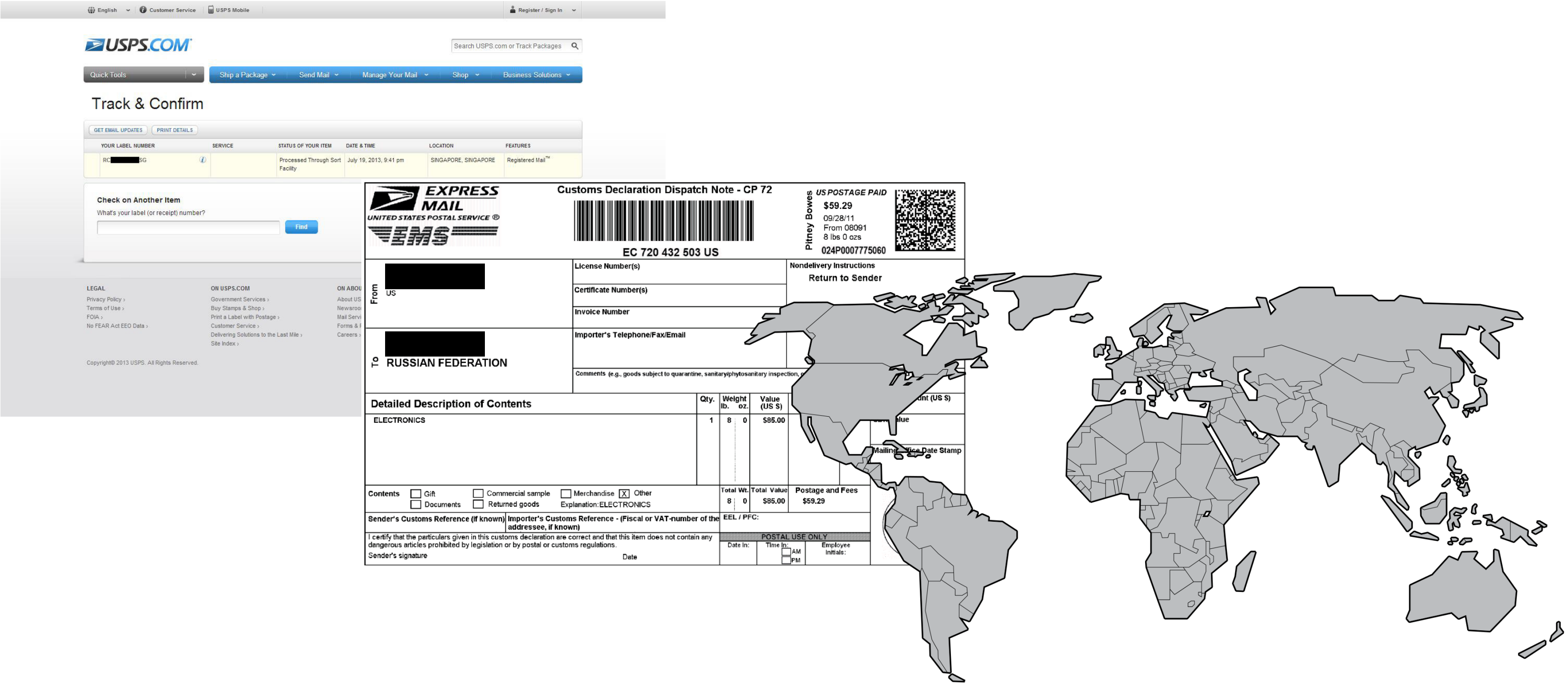
Locations of Drops



	State	*Drop likelihood*	*Diff to US 2014 US 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%

Scammers target unemployed or underemployed groups to recruit drops

Intervention Approaches



Track & Confirm

YOUR LABEL NUMBER	SERVICE	STATUS OF YOUR ITEM	DATE & TIME	LOCATION	FEATURES
RC[redacted]SG		Processed Through Sort Facility	July 19, 2013, 9:41 pm	SINGAPORE, SINGAPORE	Registered Mail™

Check on Another Item

What's your label (or receipt) number?

Copyright© 2013 USPS. All Rights Reserved.

EXPRESS MAIL
UNITED STATES POSTAL SERVICE ®
EMS

Customs Declaration Dispatch Note - CP 72

EC 720 432 503 US

Pitney Bowes
US POSTAGE PAID
$59.29
09/28/11
From 08091
8 lbs 0 ozs
024P0007775060

From [redacted]
US

To [redacted]
RUSSIAN FEDERATION

License Number(s)

Certificate Number(s)

Invoice Number

Importer's Telephone/Fax/Email

Comments (e.g., goods subject to quarantine, sanitary/phytosanitary inspection,

Nondelivery Instructions
Return to Sender

Detailed Description of Contents	Qty.	Weight lb.	oz.	Value (US $)
ELECTRONICS	1	8	0	$85.00

unt (US $)

lue

Mailing ffice Date Stamp

Contents ☐ Gift ☐ Documents ☐ Commercial sample ☐ Returned goods ☐ Merchandise ☒ Other
Explanation: ELECTRONICS

Total Wt.		Total Value	Postage and Fees
8	0	$85.00	$59.29

Sender's Customs Reference (If known)

Importer's Customs Reference - (Fiscal or VAT-number of the addressee, if known)

EEL / PFC:

I certify that the particulars given in this customs declaration are correct and that this item does not contain any dangerous articles prohibited by legislation or by postal or customs regulations.

Sender's signature   Date

POSTAL USE ONLY
Date In: Time In: ☐ AM ☐ PM   Employee Initials:

Reshipping Destinations

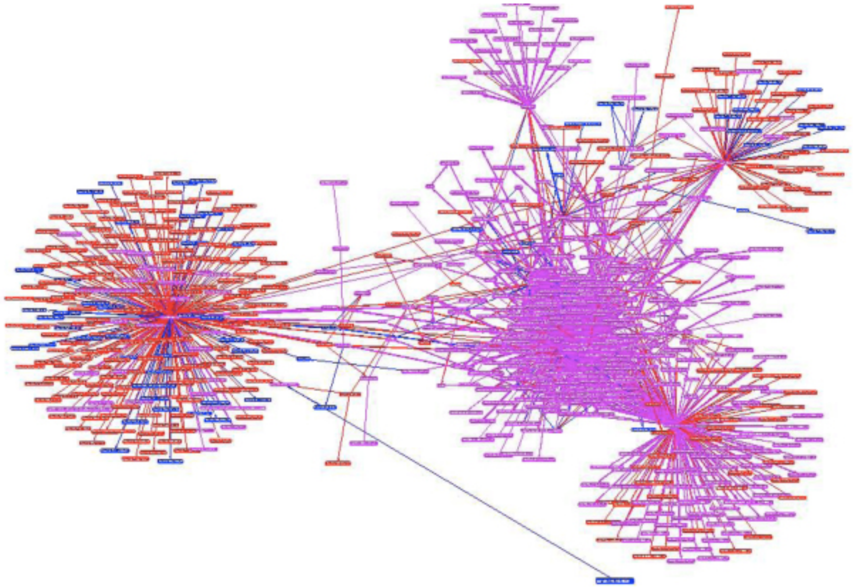
Site	***Destination***	***Label Percentage***
Site-A	Moscow area, Russia*	85.89%
	Claymont, DE, US	6.08%
	Dover, DE, US	2.43%
Site-D	[illegible]	7%
	Kiev, Ukraine	10.11%
	Nikolaev, Ukraine	0.49%
Site-E	Moscow, Russia	91.14%
	Krasnodar, Russia	4.36%
	Stavropol, Russia	1.45%

At least 85% packages are shipped to Moscow and its suburbs

* Including Moscow, Balashiha, and Zheleznodorozhnyj

Conclusions

Criminals use various come-ons to trick you into what Postal Inspectors call "reshipping fraud."



Authors

Shuang Hao[1] Kevin Borgolte[1] Nick Nikiforakis[2]
Gianluca Stringhini[3] Manuel Egele[4] Michael Eubanks[5]
Brian Krebs[6] Giovanni Vigna[1,7]

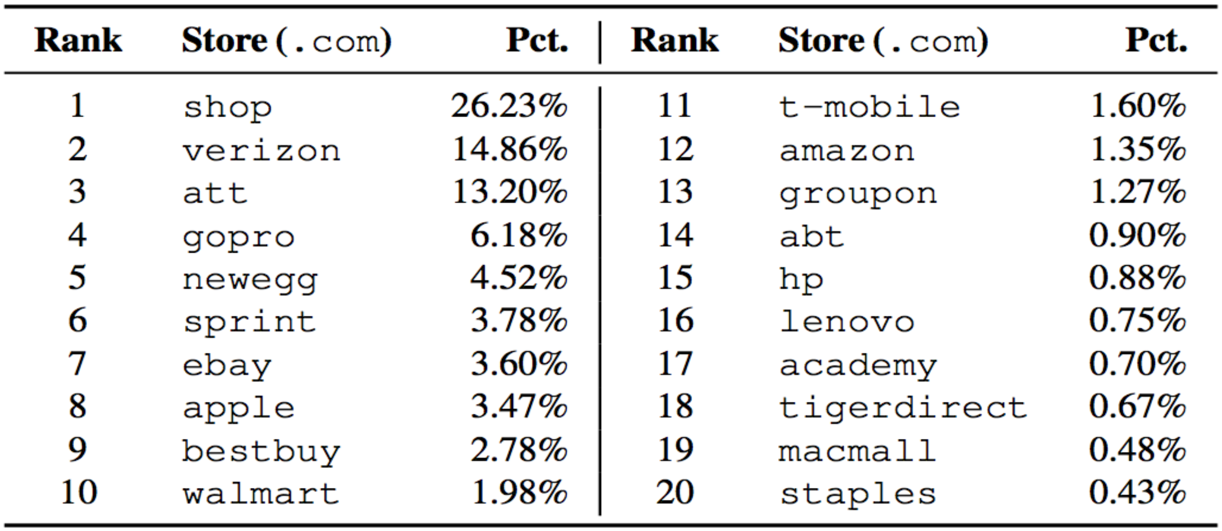
[1] UC Santa Barbara [2] Stony Brook University [3] University College London
[4] Boston University [5] Federal Bureau of Investigation
[6] KrebsOnSecurity.com [7] Lastline Inc.

?

Backup

Victim & Loss

Targeted Stores



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%