

Drops for Stuff

An Analysis of Reshipping Mule Scams

Shuang Hao¹ Kevin Borgolte¹ Nick Nikiforakis²
Gianluca Stringhini³ Manuel Egele⁴ Michael Eubanks⁵
Brian Krebs⁶ Giovanni Vigna^{1,7}

¹UC Santa Barbara ²Stony Brook University ³University College London

⁴Boston University ⁵Federal Bureau of Investigation

⁶KrebsOnSecurity.com ⁷Lastline Inc.

Prevalence of Data Breaches and Theft

CNN Money

Home Depot: 56 million cards exposed in breach

By Melvin Backman @CNNTech

Home Depot confirmed Thursday that it had exposed 56 million credit and debit cards during a data breach.

The company also said it had eliminated 100,000 card readers that encountered the malware. The company said it was a custom strain its security team removed from service. The company is testing new data encryption capabilities and other security measures.

Home Depot breach (2014)
56 million cards

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 information was exposed in a data breach that began last holiday season.

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

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 phishing attacks" report, users who faced phishing attacks in the last year used services such as Facebook, Yahoo, Google and Gmail. The report, released in June 2013 based on data from 2012, says that phishing has evolved into a rapidly growing threat.

Phishing (2013)
37 million users

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.

Behind the "Gameover" Trojan is a team of cybercriminals who are customizing the malware to reach bank customers in new countries.

Zeus Gameover (2014)
1 million PCs

Trojan virus steals banking info

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

The details of about 500,000 online bank accounts and credit and debit cards have been stolen by a virus described as "one of the most advanced pieces of crimeware ever created".

The Sinowal trojan has been tracked by RSA, which helps to secure networks in Fortune 500 companies.

Torpig botnet (2008)
0.5 million cards

How to Monetize?

- **Limitation** of previous monetization methods
 - Direct withdrawal
 - Risk of identity/location exposure
 - Money laundry (money mule)
 - Difficult to wire from credit cards to bank accounts
 - Direct purchase of high-value products for reselling
 - Usually no direct shipping to foreign countries

Reshipping Scam

- Recruit **mules** to receive and **reship** packages to cybercriminals overseas
- A major monetization scheme
 - Bypass embargo policies, and hide traces

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



JOB SCAM USED TO RESHIP MERCHANDISE TO RUSSIA

- **Goal:** Characterize key aspects of the underground economy behind reshipping scams

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

Roles in Reshipping Scam Ecosystem

- Crime organization
 - **Site operator:** Manage reshipping scam website
 - **Stuffer:** Purchase products with stolen cards, and rent mules for reshipping (“*Drops for stuff*”)
- Abused parties
 - **Drop:** Reshipping mule
 - **Cardholder:** Owner of the stolen card
 - **Merchant:** Online retail company

Reshipping Scam Operation



Data Summary

- Dataset of 7 reshipping scam sites (site A-G)
(Shared by concerned citizens anonymously)
 - Reshipping logs, prepaid labels, drop records, messages, rules and disclaimers
- Address information (city-level) of drops in U.S.
(Shared by the law enforcement)

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?

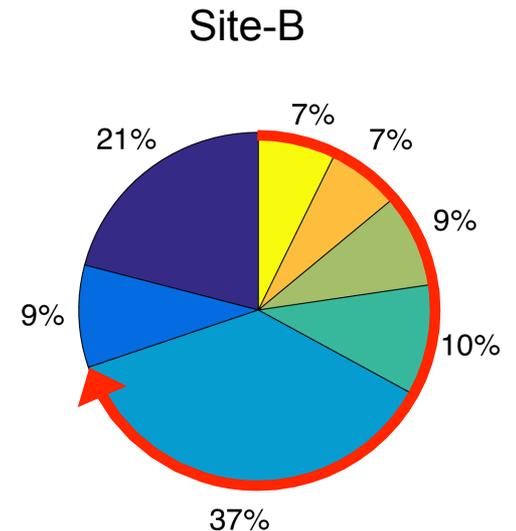
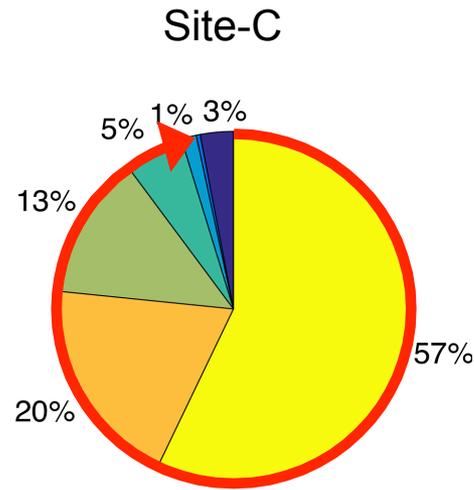
Agreement and Profit Split

- 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

- Category prices and proportions

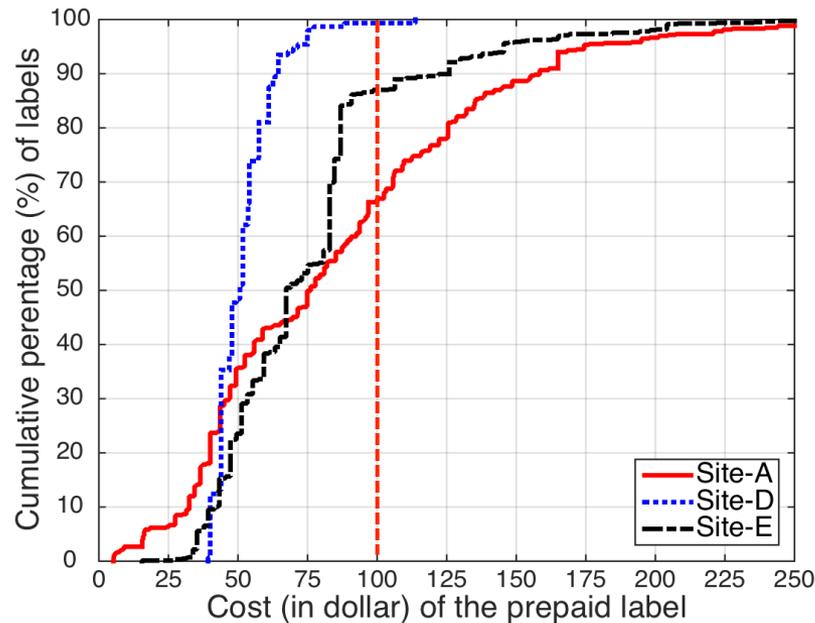
		Product Category	Median Price (Site-C)
Electronics		Apple Products	\$750
		Camera Related	\$500
		Computer related	\$1,030
		Other Electronics	\$550
		Fashion and Apparel	\$1,000
		Nutrition	\$1,050
		Miscellaneous	\$689



Above 70% of the products are electronics and luxury clothing

Label Purchase

- Move from fraudulent labels towards “white labels”
 - Paid with cybercrime-funded bank accounts



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

Negative Effect

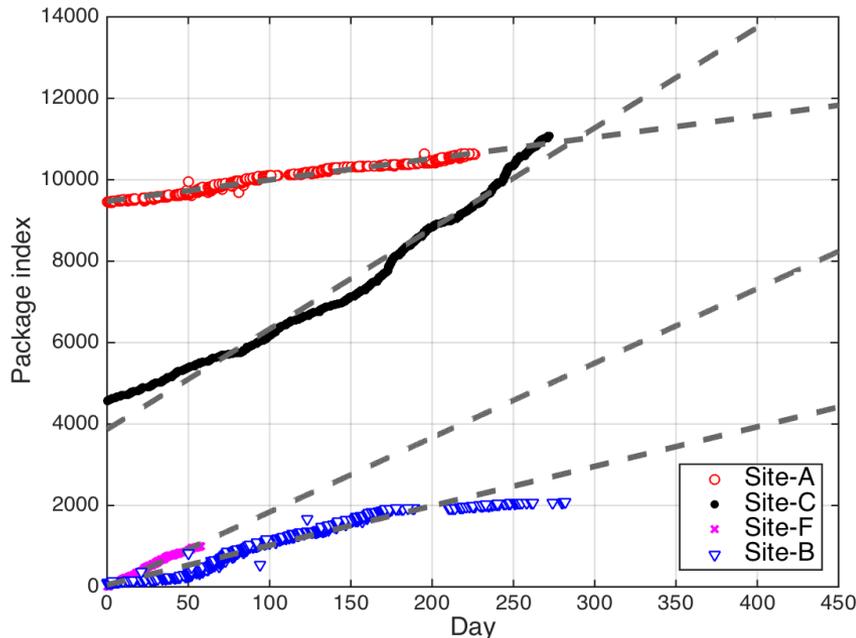
- Who are negatively affected?
- How much is the financial loss?

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

Revenue Estimate

- From packages to revenue



- Estimated package number per year

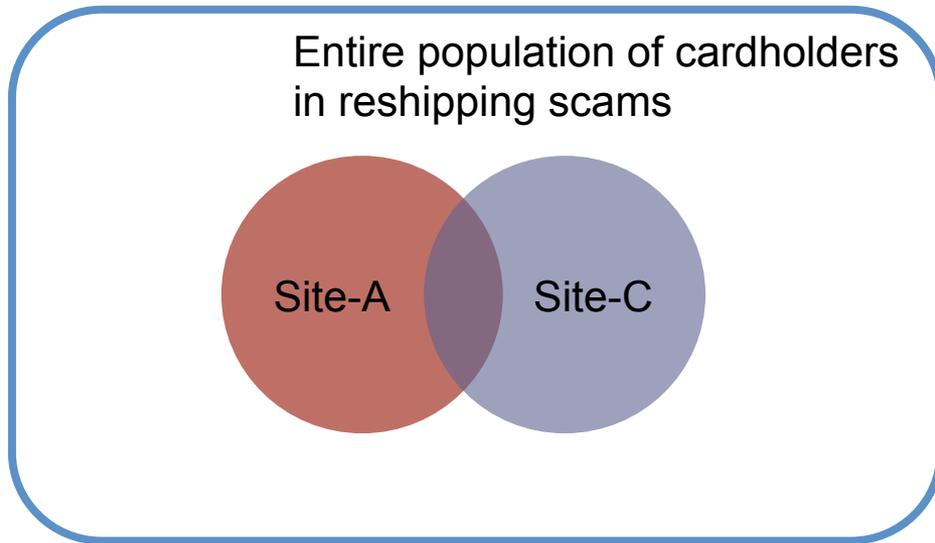
Site-C	9,009
Site-F	6,673
Site-B	3,541
Site-A	1,911

- Revenue = # packages x average product price

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

Overall Revenue Estimate

- Capture-recapture to infer the number of total cardholders



- Population estimate
$$= \frac{|A| \times |C|}{|A \cap C|}$$

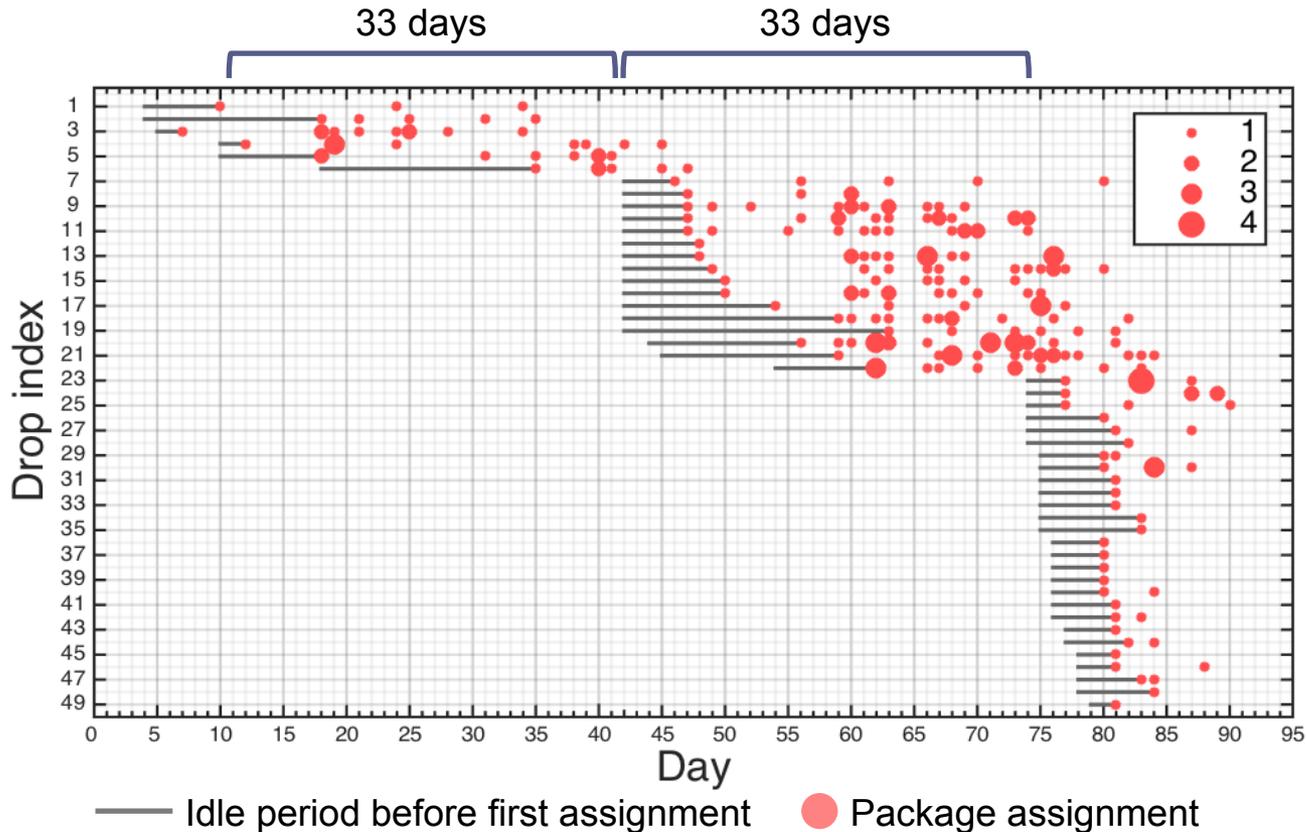
 ≈ 1.6 million
victim cardholders
per year

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!?

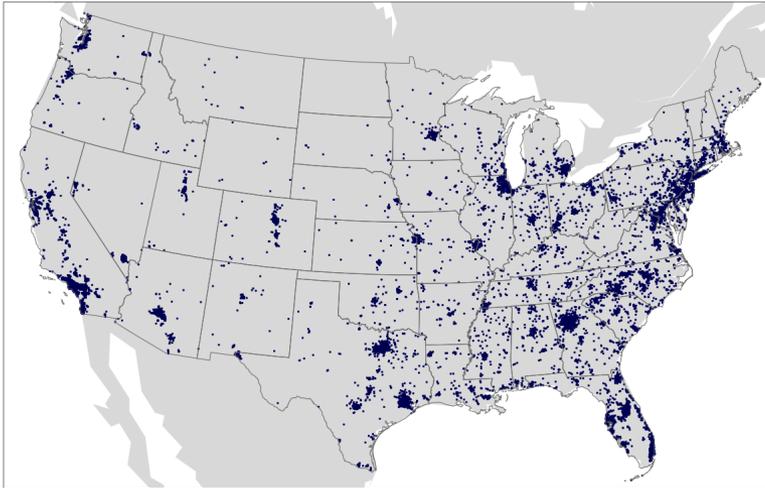
What time will I be paid!?

When will my check be deposited!?

Drops are abandoned without getting paid after about 30 days

Locations of Drops

- Drop likelihood = # drops in state / population of state



	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

- Vantage points at shipping service companies
 - Patterns in package tracking
 - Accounts of label purchases
 - Shipping destinations

Reshipping Destinations

- Top destination cities from reshipping scam sites

<i>Site</i>	<i>Destination</i>	<i>Label Percentage</i>
Site-A	Moscow area, Russia*	85.89%
	Claymont, DE, US	6.08%
	Dover, DE, US	2.43%
Site-D	Moscow area, Russia*	89.07%
	Kiev, Ukraine	10.11%
	Nikolaev, Ukraine	0.49%
Site-E	Moscow, Russia	91.14%
	Krasnodar, Russia	4.36%
	Stavropol, Russia	1.45%

* Including Moscow, Balashiha, and Zheleznodorozhnyj

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

Conclusion

- Reshipping scam is prolific: Yearly revenue up to \$7.3 million of a single site, and overall estimated \$1.8 billion
- We provided detailed analysis on operation policies, targeted products, “white labels”, and drop recruitment
- We proposed approaches to intercept reshipping packages