Drops for Stuff
An Analysis of Reshipping Mule Scams

Shuang Hao¹ Kevin Borgolte¹ Nick Nikiforakis² Gianluca Stringhini³ Manuel Egele⁴ Michael Eubanks⁵ Brian Krebs⁶ Giovanni Vigna¹,⁷

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

Prevalence of Data Breaches and Theft

- 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) 0.5 million cards
Overview

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

**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

1. Apply
2. Data Breach
3. Subscribe
4. Purchase
5. Ship
6. Manage
7. Reship

User information
Reshipping instruction
Package

Checkout
Name: Cardholder
Address: Drop’s
Order summary: 

Merchant

Reshipping Scam Site

Stuffer

Drop

Cardholder
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)*

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

<table>
<thead>
<tr>
<th>Product Category</th>
<th>Median Price (Site-C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple Products</td>
<td>$750</td>
</tr>
<tr>
<td>Camera Related</td>
<td>$500</td>
</tr>
<tr>
<td>Computer related</td>
<td>$1,030</td>
</tr>
<tr>
<td>Other Electronics</td>
<td>$550</td>
</tr>
<tr>
<td>Fashion and Apparel</td>
<td>$1,000</td>
</tr>
<tr>
<td>Nutrition</td>
<td>$1,050</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>$689</td>
</tr>
</tbody>
</table>

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

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

$$\approx 1.6 \text{ million victim cardholders per year}$$

Overall estimated revenue is $1.8 \text{ billion per year}$
Drop Recruitment

• How long do drops remain active?

• Where are the drops?
Life Cycle of Drops

Drops are abandoned without getting paid after about 30 days.

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!?

33 days

Idle period before first assignment

Package assignment
Locations of Drops

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

<table>
<thead>
<tr>
<th>State</th>
<th>Drop likelihood</th>
<th>Diff to US 2014 US Annual Unemployment Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Georgia</td>
<td>0.01099%</td>
<td>▲ +1.0%</td>
</tr>
<tr>
<td>Nevada</td>
<td>0.01011%</td>
<td>▲ +1.6%</td>
</tr>
<tr>
<td>Delaware</td>
<td>0.00951%</td>
<td>▼ –0.5%</td>
</tr>
<tr>
<td>Florida</td>
<td>0.00919%</td>
<td>▲ +0.1%</td>
</tr>
<tr>
<td>Maryland</td>
<td>0.00868%</td>
<td>▼ –0.4%</td>
</tr>
<tr>
<td>North Carolina</td>
<td>0.00710%</td>
<td>▼ –0.1%</td>
</tr>
<tr>
<td>Mississippi</td>
<td>0.00674%</td>
<td>▲ +1.6%</td>
</tr>
<tr>
<td>Arizona</td>
<td>0.00667%</td>
<td>▲ +0.7%</td>
</tr>
<tr>
<td>Illinois</td>
<td>0.00608%</td>
<td>▲ +0.9%</td>
</tr>
<tr>
<td>Virginia</td>
<td>0.00599%</td>
<td>▼ –1.0%</td>
</tr>
</tbody>
</table>

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

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

* 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

http://www.cs.ucsb.edu/~shuanghao