Scambaiter: Understanding Targeted Nigerian Scams on Craigslist

Youngsam Park¹, Jackie Jones², Damon McCoy², Elaine Shi¹ and Markus Jakobsson³

University of Maryland¹, George Mason University², ZapFraud³
Nigerian scam is so prevalent!

AusCERT 2013: Nigerian scam victim tells her story

Summary: Nigerian scam victim Jill explains how she was conned out of $300,000 over a four year period.

Woman out $400K to 'Nigerian scam' con artists

Victims lost $9.3 billion to 419 scammers in 2009

It's hard to believe that people are still falling for advance-fee fraud …
Targeted Nigerian scam variants

- **Fake payment**
  - “I sent a check (money order) with packaging fee. Please send your iPhone to my place ASAP!”

- **Rental scam**
  - “I’m out of country right now, so please send the rent and deposit via mail. Then I will send out the key!”

- **Dating scam**
  - “I’d love to meet you! Could you please help me buy a ticket to your state?”
Our research…

- **What’s the target?**
  - Targeted Nigerian scam with **fake PayPal payment** on Craigslist

- **What have we done?**
  - Bait scammers
  - Automated conversation with scammers
  - Analyze the large-scale scam data

- **What can we learn?**
  - Understand **how scammers work**
  - Look for the way to **deter the scams**
Methodology

- Magnetic honeypot advertisements
- Automated scam collection system
- Scammers’ IP collection
Magnetic honeypot advertisements

- Sell **over-priced** items
- **Attract** scammers but **repel** legitimate users

![Samsung Galaxy Note II GT-N7100 - $650](image)
Automated scam collection system

Automated data collection system

Database

Ad posting engine

Conversation engine

Proxy servers

Craigslist

Scammers

Automated conversation
Automated email conversation

Scammer’s first response
Chloe Morgan < @gmail.com >  Jun 3 (11 days ago) ☆
to me ☆☆
...what's your last price and hope in mint condition? hear from you asap as its urgent

@ gmail.com
Jun 10 (4 days ago) ☆
to Chloe  
The price is 320, firm.
The condition is almost perfect since it was not used frequently.
Please let me know if you need more information.

Our first reply
Scammer’s second response
Chloe Morgan  
Jun 11 (3 days ago) ☆
to me ☆☆
Hi....Regarding the laptop i am buying from you hope you still have it for sale? Please get back to me ASAP as i am really interested buying

@ gmail.com
Jun 11 (3 days ago) ☆
to Chloe  
Yes, it's still on sale. Please let me know if you need more information.

Our second reply
Scammer’s third response
Chloe Morgan  
Jun 11 (3 days ago) ☆
to me ☆☆
Yea i was sending to Virginia...You got a PayPal Account??

@ gmail.com
Jun 11 (3 days ago) ☆
to Chloe  
Sounds great. My paypal account is junhyosung02@gmail.com. Please let me know when the payment is done!!
Fake payment notification

service@int’l.paypal <postage_fund@in.com>
IP address collection

- Embed product images in reply emails
- Limitation
  - Only small part of scammers may access the embedded images
Experimental results

- Scammer group classification
- Scammer geolocation
- Level of scam process automation
### Dataset overview

#### Overview
- **Experiment duration**: 3 months
- **Cities/areas**: 20
- **Product category**: 4

#### Magnetic honeypot ads
- **Total number of ads**: 1,376

#### Emails
- **First scammer responses received**: 13,215 (9.6 per ad)
- **Fake PayPal payment emails**: 751
Scammer group classification

- **Conservative classification**
  - Same email address, shipping address or phone number
  - Email addresses with 90% identical prefix

<table>
<thead>
<tr>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:biglanre1@gmail.com">biglanre1@gmail.com</a></td>
</tr>
<tr>
<td><a href="mailto:biglanre10@gmail.com">biglanre10@gmail.com</a></td>
</tr>
<tr>
<td><a href="mailto:biglanre11@gmail.com">biglanre11@gmail.com</a></td>
</tr>
<tr>
<td><a href="mailto:biglanre12@gmail.com">biglanre12@gmail.com</a></td>
</tr>
<tr>
<td><a href="mailto:biglanre13@gmail.com">biglanre13@gmail.com</a></td>
</tr>
<tr>
<td><a href="mailto:biglanre14@gmail.com">biglanre14@gmail.com</a></td>
</tr>
</tbody>
</table>

- **Result**
  - Total number of groups: 1,234
  - Top 10 groups: 48%
Scammer group classification

- Aggressive classification
  - Conservative classification
  - IP addresses belong to a same class C subnet

- Result
  - Total number of groups: 1,172
  - Top 10 groups: 56.8%
## Scammer group classification

<table>
<thead>
<tr>
<th>Group</th>
<th># threads</th>
<th># source addresses</th>
<th># reply-to addresses</th>
<th>% source != reply-to</th>
<th># cities</th>
<th># product category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1096</td>
<td>178</td>
<td>23</td>
<td>100%</td>
<td>18</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>993</td>
<td>270</td>
<td>64</td>
<td>98.7%</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>885</td>
<td>313</td>
<td>48</td>
<td>95.8%</td>
<td>19</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>714</td>
<td>106</td>
<td>37</td>
<td>97.6%</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>700</td>
<td>52</td>
<td>11</td>
<td>98.6%</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>6</td>
<td>449</td>
<td>182</td>
<td>30</td>
<td>98.0%</td>
<td>17</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>441</td>
<td>60</td>
<td>17</td>
<td>97.5%</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>416</td>
<td>103</td>
<td>10</td>
<td>100%</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>9</td>
<td>330</td>
<td>19</td>
<td>8</td>
<td>94.8%</td>
<td>19</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>306</td>
<td>71</td>
<td>23</td>
<td>86.9%</td>
<td>20</td>
<td>4</td>
</tr>
</tbody>
</table>

### Top 10 groups summary
Scammer IP address analysis

Total number of IP addresses: 965
Shipping address/Phone number analysis

Shipping address:
- U.S.A.: 23%
- Nigeria: 70%
- Others: 7%

Phone number:
- U.S.A.: 91%
- Nigeria: 6%
- Other countries: 1%
- Unknown: 2%
Level of automation

- **Broken scripts** in email subject and content
- **Duplicate/template** email contents
- **Burst** of duplicate emails

**Broken Subject & Body**

[Subject:] <span class="i h data-id=0:00x0x_6FP1zGRnuHX> </span>

[Body:] Is your <span class="i h data-id=0:00x0x_6FP1zGRnuHX"></span> still available for sale??
i will reply right away. Thanks
Sent from Devon’s IPhone

[Subject:] <span class="i h data-id=3Fa3Le3I45Nd5I-c5Gcd624761cea879bf1558.jpg></span>

[Body:] <html><head><META http-equiv="Content-Type" content="text/html; charset=utf-8"></head>
<body>still for sale?; feel free to email me at darrenamos69@gmail.com</body></html>
Level of automation

- **Signs of manual labor**
  - **Curse/threat** emails
  - Scam emails peak during work hours of Nigeria
  - Wrong email address/name

### Belligerence/Threats

- [words omitted] Please respond to this mail before the penalty decision is taken against you. You are warned. We are waiting for your mail before we can credit your account and this is due to the large increase in the rate of the online scams recorded in the previous years. [words omitted]
- [words omitted] I think if I did not hear back from you within next 24hrs I will have to contact FBI about your actions on Craigslist.org. [words omitted]
- [words omitted] I will report you to PayPal and FBI. I give you 12hrs to get it ship [words omitted]
- Hey man what is going on I getting the FBI involve in this; is getting irritating [words omitted]
Level of automation

- Conclusion
  - Scam process is partially automated
  - Scammers may need to manually run automated tools
Summary

- Automated scam collection system
  - Magnetic honeypot ad posting
  - Automated email conversation

Findings

- A few large organizations
  - **Top 10 groups: 48%** of all collected scam trials

- Geolocation of scammers
  - **90%** from Nigeria and the United States

- Methods and tools of scammers
  - **Partially automated**
Future work

- Extending to other scam areas
  - Rental, dating scams
  - Fake payment scams on Ebay

- Filtering messages
  - Recurring themes, belligerent tones
  - Common linguistic features

- More precise tracking of scammer geolocation
  - GPS tracking
Thank you!

yspark@cs.umd.edu
Appendix

- Recurring theme
  - Present for family member and buyer overseas

- i want you to know you are also in safe hands and i want you to assure me that I won’t be disappointed with it *cos am getting it for my cousin* the issue is that am not around i would have come and see it

- i wanted to buy this for my Cousin; but the issue is am currently out of state on a Contract Project .The contract is strictly no call due to the lack of reception in the area.

- *im arranging it for my cousing birthday who live in OKLAHOMA USA.* im off shore and Right now the only way i can make the payment is via paypal as i don’t have access to my bank account online and theres no way i can issue out a check or something here
Military member unable to come view product
- because that is the only convenient means for me and due to my work frame i can not be able to get there and I promise everything will go smoothly. I really wish to be there to check out the item but i don’t have chance cause am very busy person (US MARINE). And am already back to camp but i will get home very soon

- i have no problem with the amount as am a US marine i work for the United State Marine Corps (USMC) but am currently hospitalized so am on a treatment in New york

- Am willing to buy and am a serious buyer but am not around now so i won’t be able to come to have a look because am in camp now I’m a Marine(US MARINE).
Recurring theme
  – Belligerence/Threats

- Please respond to this mail before the penalty decision is taken against you. You are warned. We are waiting for your mail before we can credit your account and this is due to the large increase in the rate of the online scams recorded in the previous years.

- I think if I did not hear back from you within next 24hrs I will have to contact FBI about your actions on Craigslist.org

- I will report you to PayPal an FBI I give you 12h to get it ship

- Hey man what is going on I getting the FBI involve in this; is getting irritating
Scammer email accounts analysis

<table>
<thead>
<tr>
<th>First responses</th>
<th>13,125</th>
</tr>
</thead>
<tbody>
<tr>
<td>First responses with different source and reply-to addresses</td>
<td>10,826 (81.9%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Second responses</th>
<th>1,626</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second responses with different source and reply-to addresses</td>
<td>316 (19.4%)</td>
</tr>
</tbody>
</table>
Scammer group classification

Emails per day – top 10 groups
Scammer pattern analysis

![Graph showing the number of effective ads posted and the number of 1st scam responses over time. The graph highlights a peak in activity between 12PM and 6PM WAT.]

![Another graph illustrating the percentage of scam responses over time, with a focus on the response time distribution for 1st and 2nd scam responses.]
## Scammer IP address analysis

<table>
<thead>
<tr>
<th>IP address</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not in black/graylist</td>
<td>43.9%</td>
</tr>
<tr>
<td>Blacklisted</td>
<td>40.4%</td>
</tr>
<tr>
<td>Graylisted</td>
<td>14.0%</td>
</tr>
<tr>
<td>Web crawler</td>
<td>1.7%</td>
</tr>
</tbody>
</table>

### IP addresses blacklisted by Project Honey Pot

<table>
<thead>
<tr>
<th>IP address</th>
<th>Country</th>
<th># times observed</th>
<th>Blacklisted?</th>
</tr>
</thead>
<tbody>
<tr>
<td>41.211.193.X</td>
<td>Nigeria</td>
<td>298</td>
<td>-</td>
</tr>
<tr>
<td>41.203.67.X</td>
<td>Nigeria</td>
<td>241</td>
<td>Yes</td>
</tr>
<tr>
<td>41.203.67.X</td>
<td>Nigeria</td>
<td>204</td>
<td>Yes</td>
</tr>
<tr>
<td>41.203.67.X</td>
<td>Nigeria</td>
<td>160</td>
<td>Yes</td>
</tr>
<tr>
<td>41.211.198.X</td>
<td>Nigeria</td>
<td>93</td>
<td>-</td>
</tr>
<tr>
<td>41.206.15.X</td>
<td>Nigeria</td>
<td>89</td>
<td>Yes</td>
</tr>
<tr>
<td>41.184.21.X</td>
<td>Nigeria</td>
<td>89</td>
<td>Graylisted</td>
</tr>
<tr>
<td>41.206.15.X</td>
<td>Nigeria</td>
<td>88</td>
<td>Yes</td>
</tr>
<tr>
<td>41.211.201.X</td>
<td>Nigeria</td>
<td>85</td>
<td>-</td>
</tr>
<tr>
<td>41.206.15.X</td>
<td>Nigeria</td>
<td>79</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Top 10 IP addresses by the number of times observed**
Scammer IP address analysis
Top 10 groups

- **Email account reuse**
  - 97% of emails received from top 10 groups have different source and reply-to addresses
### Scammer email accounts analysis

<table>
<thead>
<tr>
<th>Email Provider</th>
<th>Percentage</th>
<th>Relative market share estimation</th>
<th>IMAP/SMTP</th>
<th>Hide sender IP?</th>
<th>Price for 1000 PVAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gmail</td>
<td>65.0%</td>
<td>25.0%</td>
<td>Yes</td>
<td>Yes</td>
<td>$90</td>
</tr>
<tr>
<td>Microsoft</td>
<td>10.0%</td>
<td>20.3%</td>
<td>No (POP3/SMTP)</td>
<td>Yes</td>
<td>$5</td>
</tr>
<tr>
<td>AOL</td>
<td>4.9%</td>
<td>11.9%</td>
<td>Yes</td>
<td>No</td>
<td>$50</td>
</tr>
<tr>
<td>Yahoo</td>
<td>3.5%</td>
<td>42.8%</td>
<td>Yes ($20)</td>
<td>No</td>
<td>$15</td>
</tr>
<tr>
<td>Others</td>
<td>16.6%</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

* PVA (Phone Verified Accounts)
### Level of automation

<table>
<thead>
<tr>
<th>Stage</th>
<th>Signs of automation</th>
<th>Signs of manual labor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading in Craigslist ads</td>
<td>Short inter-arrival time of first response, Broken scripts in email subject, Duplicate/template email contents</td>
<td>Received emails peak during work hours</td>
</tr>
<tr>
<td>First scam response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Second and later scam responses</td>
<td>Short inter-arrival time of second responses, Duplicate/template responses</td>
<td>Scammers’ curse emails, Received emails peak during work hours</td>
</tr>
<tr>
<td>Fake payment notification</td>
<td>Duplicate/template responses</td>
<td>Wrong email address/name in the notification</td>
</tr>
</tbody>
</table>

**Conclusion**
- Both first and second responses are **partially automated**
- Scammers may need to **manually run or attend to automated tools**