Understanding Craigslist Rental Scams

Youngsam Park[1(✉)], Damon McCoy[2], and Elaine Shi[3]

[1] University of Maryland, College Park, USA
yspark@cs.umd.edu
[2] New York University, New York, USA
[3] Cornell University, Ithaca, USA

Abstract. Fraudulently posted online rental listings, rental scams, have been frequently reported by users. However, our understanding of the structure of rental scams is limited. In this paper, we conduct the first systematic empirical study of online rental scams on Craigslist. This study is enabled by a suite of techniques that allowed us to identify scam campaigns and our automated system that is able to collect additional information by conversing with scammers. Our measurement study sheds new light on the broad range of strategies different scam campaigns employ and the infrastructure they depend on to profit. We find that many of these strategies, such as credit report scams, are structurally different from the traditional advanced fee fraud found in previous studies. In addition, we find that Craigslist remove less than half of the suspicious listings we detected. Finally, we find that many of the larger-scale campaigns we detected depend on credit card payments, suggesting that a payment level intervention might effectively demonetize them.

1 Introduction

Today, many people use the Internet for at least part of their housing search [6]. This inevitably has led to profit-driven scammers posting fake rental listings, commonly known as "*rental scams*". Despite the ubiquitous presence of online rental scams, we currently lack a solid understanding of the online rental scam ecosystem and the different techniques rental scammers use to deceive and profit off their victims. While most efforts to mitigate this problem focus on filtering the posts, this is only the visible part of a well-honed set of scams and infrastructure established to extract money from their marks. An end-to-end understanding of a scam and its structural dependencies (message posting, email accounts, location of scammers, support companies, automated tools and payment methods) is often a crucial first step towards identifying potential weaknesses along the chain that can serve as effective choke-points for the defender [8,27]. In particular, this "understand, and then deter" trajectory has resulted in suggesting weak points for disrupting other domain-specific threats, such as payment processing in the counterfeit software and pharmacy spam domain [8,18,19].

In this paper, we conduct the first systematic empirical study of the online rental scams ecosystem as viewed through the lens of the Craigslist rental section.

J. Grossklags and B. Preneel (Eds.): FC 2016, LNCS 9603, pp. 3–21, 2017.
DOI: 10.1007/978-3-662-54970-4_1

Our in-depth analysis of these rental scam campaigns allows us to address questions geared at improving our understanding of the supporting infrastructure with the goal of exploring alternate points to undermine this ecosystem, such as: "What are the common underlying scams?", "Where are these scammers located and what tools do they use?", "How effective are current defences?", "What payment methods do they use?". We summarize our contributions and findings below.

By developing several effective detection techniques, we are able to identify several major rental scam campaigns on Craigslist. In addition, we extend Scambaiter automated conversation engine [21] to automatically contact suspected rental scammers, which enabled us to understand what support infrastructure they used and how they were monetizing their postings. In total we detected about 29 K scam listings over the 20 cities we monitored, within a period of 141 days.

We find a diverse set of methods utilized for monetizing the rental scam campaigns we identified. These include attempts to trick people into paying for credit reports and "bait-and-switch" rental listings. When we explored the payment method used, five of the seven major scam campaigns identified used credit cards. Many campaigns also depended on businesses registered in the USA to collect payments. We also find that Craigslist's filtering methods are currently removing less than half of the rental scam ads we detected.

Our results highlight the fact that scammers are highly customizing their monetization methods to the United States rental market. They also expose new scams and infrastructure that were not encountered in previous studies [7,15,21]. This difference highlights the need to understand a wider range of scam domain and suggests potential bottlenecks for many rental scam monetizing strategies at the regulatory and payment layers. For instance, United States regulatory agencies, such as the Federal Trade Commission (FTC) could investigate these companies and levy fines for their deceptive advertising practices. Another potential method of demonetizing these companies might be to alert credit card holder associations, such as Visa or MasterCard, to these merchants' deceptive billing and refund policies.

2 Data Sets

This paper focuses solely on *scams* and we consider spam, such as off-topic and aggressive repostings, as outside the scope of this paper. In this paper, we define a rental listing as a scam if (i) it is fraudulently advertising a property that is not available or not lawfully owned by the advertiser and (ii) it attempts to extract money from replies using either advanced fee fraud or "bait-and-switch" tactics.

The basis of our study relies upon repeated crawls of the rental section on Craigslist in different geographic locations to collect all listings posted in these regions and detect listings that are subsequently flagged. We then use a combination of manual searching for reported rental scams and human-generated regular expressions to map fraudulent listings into scam campaigns. For a small

subset of listings that are difficult to identify as scams or legitimate, we build an automated conversation engine that contacts the poster to determine the validity of the listing. Finally, we crawl five other popular rental listing sites to detect cloned listings that have been re-posted to Craigslist potentially by scammers.

2.1 Rental Listing Crawling

Our primary data set is based on listings collected from daily crawls of rental sections on Craigslist across 20 different cities and areas in the United States with the largest population [5]: New York, Los Angeles, Chicago, Houston, Philadelphia, San Antonio, San Diego, Dallas, San Francisco (Bay area), Austin, Jacksonville, Indianapolis, Columbus, Charlotte, Detroit, El Paso, Memphis, Boston and Seattle. Our crawler revisited each crawled ad three days after the first visit to detect if they have been flagged by Craigslist. The crawler performed a final recrawl of any unflagged listings 7 days after the first visit to determine if they have been flagged or expired. We also collected rental ads from five additional major rental listing websites, *Zillow*, *Trulia*, *Realtor.com*, *Yahoo! Homes* and *Homes.com*.

Our crawler tracked all rental section ads on 20 cities/areas on Craigslist, for a total duration of 141 days, from 2/24/2014 to 7/15/2014. Table 1 shows the overall summary of this dataset. In whole, we collected over two million ads, among which 126, 898 have been flagged by Craigslist.

Table 1. Dataset summary. About 6% of rental ads are flagged for removal by Craigslist. Rental ads are considered to be expired 7 days after being posted.

Overview	Duration	141 days (2/24/14-7/15/14)
	Cities/areas	20
Rental ads	Total posted	2,085,663
	Flagged for removal	126,898 (6.1%)
	Deleted (by user)	338,362 (16.2%)
	Expired*	1,620,403 (77.7%)

2.2 Campaign Identification

Our crawling of Craigslist produced a large set of flagged and non-flagged ads that are potentially scam listings. We know that some of these ads are scams and that many of these are linked to a smaller number of distinct scam campaigns.

Due to the large number of ads in our data set a brute-force approach of manually analyzing a large set of ads would not be effective and would require a domain specific understanding of how scam ads differ from legitimate ads. In order to overcome these challenges, we bootstrap our knowledge of scam postings by finding a small number of suspicious ads in a semi-automated manner.

To this end, we manually surveyed a broad range of user submitted scam reports online [1,3,4] to gain some initial insights about rental scams. Based on these insights, we constructed the following heuristics to identify an initial set of suspicious rental listings:

- Detect suspicious cloned listings by correlating listings posted to Craigslist with other rental listing websites, in particular, cloned ads from other sites that exhibit a substantial price difference.
- Detect posts with similar contents across multiple cities, e.g., posts with the same phone number or email addresses.
- Focus on ads flagged by Craigslist, and manually identify suspicious scam listings. As we will report in detail later, not all flagged posts are scam listings; and conversely, not all scam posts were flagged by Craigslist
- Identify ads that are similar to user-reported scams.

2.3 Campaign Expansion Phase: Latitudinal

For some of the campaigns we identified and hand labelled a small number of initial scam posts. Based on these we would like to identify other similar listings that are part of the same campaigns using automated and semi-automated methods. To this end, we used an approach that uses human-generated scam signatures.

Human-Generated Scam Signatures. Our first approach is to manually inspect the handful of ads that we identified to be in the same campaign, and summarize a unique signature to identify this campaign. For example, one of the credit report scam campaigns have the following unique signatures: email accounts corresponding to the regular expression "[a–z]+[ ]@[ ]yahoo[ ](dot)[ ]com" and no other contact information is included.

We then applied our signatures to all of our crawled ads, to identify additional ads that belong to the same campaign. As detailed in later sections, we will rely on a combination of human and automated verification techniques to confirm that scam ads identified by these signatures are indeed scams.

2.4 Campaign Expansion Phase: Longitudinal

For the initial scam postings we identified above, and the suspicious listings we identified in the latitudinal campaign expansion phase (Sect. 2.3), we wanted to confirm whether these are indeed scam messages. To this end, we built an automated conversation engine to converse with the suspected scammer, to see if the conversation would lead to a phase where the scammer requested payment from us.

Automated Conversation Engine. We manually inspected the suspicious ads and found that some of them were clearly scams, e.g., the ads with a specific phone numbers that were reported as scams by many users. For others, while the ads appear highly suspicious, we were not sure whether they were scams as opposed to the more harmless spam posting from aggressive realtors or other service providers advertising their service/rentals.

We therefore relied on an automated conversation engine to (i) verify whether a suspicious ad is a scam and (ii) collect additional data. More specifically, we first selected a few suspicious ads and performed the email conversations manually. Then it was fairly straightforward to distinguish between legitimate users and malicious scammers during the email conversation. For example, clone ads scammers usually wanted to proceed with the rental process online since they were not in town for good purposes (e.g., serving in mission trip to Africa). From the preliminary conversations, we were able to generate a set of linguistic features (e.g., keywords such as "serving in mission" or rent application templates) and other types of features (e.g., embedded links to certain redirection servers) that distinguish rental scammers from other legitimate users.

We ran the automated conversation engine only for the emails selected based on a predefined set of features. During the email conversations, we were able to collect additional data such as email accounts, IP addresses, phone numbers, links and payment information from the scammers. As in [21], the automated conversation engine embedded an external image link into the emails. Once a scammer clicks or loads the link in any way, the link leads the scammer to our private web server that logs the visitor's IP address. In this way, we were able to collect the IP addresses of the scammers from two sources: email headers and access logs to the web server.

Ethics. The longitudinal automation phase is the only part of the data collection that involved human subjects. We took care to design our experiments to respect common ethical guidelines and received approval from our institution's IRB for this study. As mentioned above, sometimes we rely on automated conversations to confirm (or disconfirm) whether scams we identify are truly scams. To minimize the inconvenience brought on legitimate users, we abided by the following guidelines. First, we only sent automated emails to ads that we suspected to be scams. Detailed methods are explained in Sects. 3.1 and 3.2. Second, we kept the automated conversations to a low volume. In the entire data collection, we sent out 2,855 emails, from which we received 204 responses that were confirmed to be from scammers out of a total of 367 responses. From these initial results, we were able to improve our methods for detecting suspicious ads, which would further reduce the number of legitimate posters contacted. Finally, in some cases we called the phone number provided by the poster in order to collect additional information. These phone calls where all manually placed, restricted to low volumes and we only contacted suspected scam posters.

2.5 Campaign Summaries

We present a high-level summary of the major scam categories and campaigns we identified in Table 2. For each campaign we assign it a name based on either the name of the company that is monetizing the scam when known or a feature used to identify the listings in the campaign. Applying our campaign identification methods from Sect. 3, we find seven distinct scam campaigns that account for 32 K individual ads. For each campaign the table lists the monetization category of the scam, the raw number of listings associated with that campaign, the percentage of ads that were flagged, the number of cities we found listings in out of the 20 total cities we monitored and the payment method used.

Table 2. Major rental scam campaigns. Rental scam campaigns of relatively large size in various rental scam types.

Scam category	Campaign	# Ads	% Flagged	City	Payment
Credit report	CreditReport_Yahoo	15,184	33.0%	20	Credit card
	CreditReport_Gmail	5,472	59.3%	9	Credit card
Rent	Clone scam campaigns	85	87.1%	17	Wire transfer
Realtor service	American Standard Online	3,240	62.4%	19	Credit card
	New Line Equity	3,230	43.3%	12	Credit card
	Search Rent To Own	1,664	77.5%	17	Credit card
Total		28,875	45.2%		

3 Analysis of Scam Campaigns

In this section, we will present our detailed findings for each campaign, including our insights on how the scams are organized, where they are geographically located and the degree of automation used by each campaign.

3.1 Credit Report Scams

In a typical credit report scam, a scammer posts a false rental ad for a property not owned by the scammer. When a victim user replies to the rental ad, the scammer asks the victim to obtain their credit score by clicking on a link included in the email. When the victim clicks the link, a scammer-operated redirection server redirects the victim to a credit score company and includes a referral ID. If the victim pays for the credit score service which accepts credit card payments, the scammer will be paid a commission by the credit score company through its affiliate program.[1]

[1] According to the affiliate program of *Rental Verified*, which is used by one of the credit report campaigns we found, it pays up to $18 per customer. https://rentalverified.com/affiliates.

Data Collection. We identified initial postings for each campaign by manually examining the Craigslist-flagged ads, and correlating contact information and unique substrings included in the postings with user reports found on scam report sites [1,3,4]. In this manner, we identified two major campaigns, henceforth referred to as *CreditReport_Yahoo* and *CreditReport_Gmail* respectively, due to their usage of signature Yahoo and Gmail email addresses.

From the few examples that we found manually, we latitudinally expanded the campaign dataset through human-generated signatures. Using the human generated signatures, we were able to identify additional scam ads from the same campaigns. Craigslist had failed to flag many of the scam ads we identified. Specifically, for CreditReport_Yahoo campaign, we found 15,184 scam ads of which 33.01% were flagged for removal by Craigslist. We also found 5,471 scam ads posted by CreditReport_Gmail of which 59.27% were flagged. More details are provided in Table 2.

Dataset Sanity Check. We verified the suspicious ads identified by the signatures are indeed scams in two ways. First, we performed a sanity check by manually investigating 400 randomly selected suspicious ads, 200 from each campaign. We considered a suspicious ad as a scam if (1) an ad contained no additional contact information such as name, phone number, street address or URL and (2) there existed same or similar ads with different email addresses in the same campaign. Through the manual inspection, we found only one false positive ad in CreditReport_Yahoo campaign and two in CreditReport_Gmail. The email addresses used in the false positive ads were also found in other suspicious ads, and we could also find out actual realtors who used those email addresses. Second, among a total number of 20,256 credit report scam ads we identified, we randomly selected 227 and 89 credit report scam ads from the CreditReport_Yahoo and CreditReport_Gmail campaigns respectively, and sent emails in response to the selected ads. Among the emails sent, we received 41 and 78 email responses and all of them were verified to be credit report scams.

In-depth Analysis. We present further analysis results of the two credit report scam campaigns. Both credit report scam campaigns appear to be located in the United States. In particular, the CreditReport_Gmail campaign appears to be located in New York city; while evidence described later (e.g., diverse IP addresses and short inter-arrival times within bursts) suggests that the CreditReport_Yahoo campaign appears to rely on a botnet for their operation. We now provide an in-depth analysis of the IP addresses and email accounts of both campaigns. Table 3 lists the overview of two credit report scam campaigns we found during the experimental period.

IP address analysis. For both campaigns, all the IP addresses observed are located in USA. However, two campaigns show completely different IP address usage patterns as shown in Table 3.

Table 3. Credit report scam campaigns.

	CreditReport_Yahoo	CreditReport_Gmail
Email account found	14,545 from 15,187 ads	1,133 from 5,472 ads
Affiliated websites	rentalverified.com, matchverification.com	freecreditnation.com, efreescore.com
IP addresses	69	30
IP addresses used once	65 (94.2%)	10 (33.3%)
Country	USA (100%)	USA (100%)
State	28 states	New York (100%)
ISP	Various	Verizon (100%)

For CreditReport_Yahoo, 69 IP addresses were found from 41 email conversations. The number of observed IP addresses are much larger than the number of corresponding email conversations since CreditReport_Yahoo uses mostly different IP addresses for each round of conversations. In addition, they rarely reuse any IP addresses across different email conversations. 94.64% are used only in a single email conversation, and every IP address is used in at most two email conversations. The IP addresses are distributed over 24 states in USA and mapped back to residential ISPs. These observations, combined with others described later (e.g., level of automation), suggest that this campaign is potentially using a botnet for operation.

In the case of the CreditReport_Gmail campaign, 30 IP addresses were found from 78 email conversations. Of the 30 IP addresses, about 66.7% were reused in more than one email conversations and the maximum number of email threads that share the same IP address is 7. All the observed IP addresses of the CreditReport_Gmail campaign are located in New York City, and map back to a single ISP, *Verizon Online LLC*.

Level of automation. We observed many signs of scam process automation, including extremely short inter-arrival time in a burst of emails and duplicate or templated email messages. Table 4 lists example email bursts received from CreditReport_Yahoo campaign. Many email bursts consisting of up to 7 emails were observed and an average inter-arrival time between two emails ranges between 4.5 s and 24.7 s. Within each burst, emails were always sent from different IP addresses and therefore, usually sent from different cities. This observation also supports the use of the widely-deployed botnet. We also observed many duplicate or templated emails from both campaigns, which are also strong signs of automation. Example email message frequently observed during the whole experiment is shown in Fig. 4 in Appendix B.

On the other hand, we also observed signs of manual labor. One example is a distribution of time of day that we received email messages from scammers. In the case of CreditReport_Yahoo, we never received any email response between 7 PM

Table 4. Example inter-arrival time for burst email responses of CreditReport_Yahoo. Emails in the same burst have different content, although they contain a similar embedded link to a direction server.

# Emails in burst	Burst duration (sec)	Mean inter-arrival time (sec)	# Cities	# IP locations
7	62	10.3	5	7
4	67	22.3	3	4
4	74	24.7	3	4
3	9	4.5	3	3
3	11	5.5	3	3

and 9 AM EST (Eastern Standard Time) and in case of CreditReport_Gmail, there was no response between 8 PM and 7 AM EST.

3.2 Clone Scam

In clone scams, typically a scammer copies another legitimate rental ad from a different rental website, e.g., *realtor.com*. The cloned ad typically has the same street address and sometimes has the same description as the original ad. However, often the scammer lowers the rental price. This scam is typically monetized by the scammer requesting a money wire transfer or bank transfer for first months rent and a deposit.

Data Collection. To detect clone scams, our crawler tracked rental posts on Craigslist and 5 other major rental websites. We compared these ads and identified Craigslist rental ads cloned from other websites.

Overall, we identified 22,852 cloned ads spanning all 20 cities on Craigslist – however, not all of these are necessarily scam ads. The majority of these appear to be legitimate users advertising their rentals on multiple websites. We then focused on the subset of 2,675 cloned ads with a price difference of at least $300. These ads are deemed to be suspicious, but we still cannot be sure whether they are truly scam ads. To verify whether the identified suspicious ads are truly scams, we sent 2, 517 emails to suspicious ads using our automated conversation engines. From the emails we sent, we received 237 responses among which 85 are verified to be scams.

In-depth Analysis of Confirmed Scams. We now report statistics on the 85 confirmed clone scams. Our major insight is that most of these scams originate from Nigeria, and are likely operated by a small number of scam factories. To reach this conclusion, we performed a detailed analysis of the IP addresses, email addresses, wire transfer requests and bank account information contained in the scam attempts. We then performed a clustering algorithm based on identifying information.

IP address analysis. Excluding IPs from well-known web mail provider, such as Gmail and Microsoft, we observed a total of 89 unique IP addresses located in 7 countries. We used DB-IP database [2] to geolocate each IP address offline in order to prevent the leakage of the scammer's IP address information that would result from using an online service. 66.29% of the collected IP addresses are from Nigeria and 15.73% were from the U.S. The result shows fairly similar trend compared to the result of the previous study by Park et al. [21] which shows 50.3% and 37.6% of IP addresses of Nigerian sales scammers were from Nigeria and the U.S. Even though we consider the possibility of proxies or anonymous networks, the consistent results from two studies strongly imply that the major number of the scammers were actually located in Nigeria.

Payment Request Analysis. From our conversations with clone ad posters, we collected a total of 12 unique payment requests and 8 duplicated requests for the same name or bank account. Interestingly, the proportion of payment request geolocation is significantly different from that of IP geolocation. 41.67% of requests are located in the US while 25% are located in Nigeria. For a money transfer via Western Union or MoneyGram, a sender needs to specify the receiver's location information including street address, city and country. However, due to the small sample size of payment requests it is unclear if there is any bias in the subset of conversations that resulted in a payment request versus those for which we were able to collect an IP address.

Phone number analysis. We collected a total of 22 distinct phone numbers from 24 email threads. 64% of the phone numbers are registered in the USA, but half of these are identified as VoIP numbers. The rest (36%) were registered in Nigeria.

Clustering. In order to better understand how scammers are organized, we clustered the emails messages into groups based on similarities of their attributes. We used a conservative clustering strategy. Any two email threads are classified into a same group only if they shared one of the following: exactly the same email accounts, phone numbers, bank accounts, IP addresses or rent application templates. Since those attributes provide us with fairly explicit clues for clustering, we are highly confident of our clustering result. The result suggests that these clone scammers are likely to originate from *a small number of scam factories*.

Table 5. Top 3 clone scam groups.

Group	Ads (%)	Email accounts	Bank accounts	Phone numbers
1	31 (36%)	21	4	9
2	16 (19%)	16	2	3
3	6 (7%)	6	0	2
Others	32 (38%)	29	5	8
Total	85	70	11	22

Through the clustering, we found a total of 15 scammer groups. Among them the top 3 groups account for 72% of all observed email threads. More detailed information of the top 3 groups are illustrated in Table 5. While IP addresses of the second and third groups are largely located in Nigeria, those of the first group are spread over Nigeria, the US, Malaysia and Egypt.

3.3 Realtor Service Scam

Realtor service scams involve a special type of realtor service, such as *pre-foreclosure rental* or *rent-to-own rental*. This type of rental is attractive to renters, since they may be able to own the property while paying monthly rent similar to the usual monthly rent of the same area. Realtor service scam campaigns usually request a victim to sign up for a private realtor service to get a list of rent-to-own rentals or pre-foreclosure rentals. To sign up for the service, the victim needs to pay up to $200 initial fee and/or $40 monthly fee.

While these businesses actually provide their customers with a list of homes, their rental ads are still considered scams since the ads are typically fake with unreasonably low rent prices, and/or for properties they do not own. Moreover, many user scam reports claim that in most cases, the properties in the provided list are not even for rent or sale at all. In addition, the refund process is extremely difficult but this is not explained clearly before the customer signs up for their services.

Data Collection. As listed in Table 2, we found a total of 8,134 realtor service scam ads over all 20 cities of Craigslist, and about 57% of the ads were flagged by Craigslist. Through the manual inspection on the crawled Craigslist rental ads, we found several phone numbers and URLs observed frequently across multiple cities on Craigslist. We then extended the initial sets of phone numbers and URLs by correlating them with various user scam reports [1,3,4]. Based on the human generated signatures of phone numbers and URLs, we identified three large realtor services with advance fee campaigns: *American Standard Online*, *New Line Equity* and *Search Rent To Own*.

Among the three campaigns we found, two were identified by sets of phone numbers and the other campaign was identified by a set of URLs. For the soundness of the collected phone numbers, we manually called each number and confirmed a set of numbers actually belong to a same campaign. We confirmed that all phone numbers of a single campaign leaded us to the same automatic response system. Then we conversed with a representative over the phone and confirmed the business name of each campaign. Table 6 lists three large realtor services scam campaigns.

American Standard Online. American Standard Online (ASO) was identified based on a total of 20 phone numbers. We gathered the set of phone numbers from our suspicious phone number detection method and many other sources such as *800notes.com*. Using the set of phone numbers, we found 3,240 rental ads posted by ASO over 19 cities on Craigslist. Among them, 62.34% were flagged

Table 6. Realtor service with advance fee campaigns.*: BBB rating of the sibling websites.

	American Standard Online	New Line Equity	Search Rent To Own
Scam signatures	20 phone numbers	22 phone numbers	5 URLs
Payment	Initial fee ($199)	Initial fee ($9.95), Monthly fee ($40.95)	Initial fee ($109.95), Monthly fee ($39.95)
BBB rating	F	Not found	Not found (C/F*)

for removal. Their ads offer rentals with much lower rent prices than other ads in the same area. However, a user is not able to get the information of the property from ASO representatives on the phone.

Because ASO is a registered company in the USA, we could find their record from *Better Business Bureau (BBB)*. BBB website shows that the company ASO has a total of 302 customer complaints and its rating is at the lowest 'F'. The record obviously tells us that doing business with ASO could be highly risky. This also means that the Federal Trade Commission (FTC) could potentially investigate this company and enforce fines or criminal penalties that would demonetize this campaign.

According to many user scam reports, the scam process of ASO is as follows. If a victim calls the number to ask about the rental ad, ASO never answers the questions about the rental ads. Instead, ASO requests a payment of $199 for an initial fee to get an access to their pre-foreclosure (or rent-to-own) property database. Once the victim signs up for the service, ASO provides the victim with a property list. Due to the nature of the term "pre-foreclosure", it is usually uncertain that the properties in the list are actually in the status of pre-foreclosure, and most of them turns out to be not for rent or sale.

At the time of contract, ASO lures victims by guaranteeing 100% refund after 90 days from the contract in case ASO does not satisfy their customers. However, their actual refund policy requires a wait of at least 90 days from the contract and at least 3 denial letters from the owners of the properties in the provided list. It is obvious that getting the multiple denial letters is extremely difficult.

New Line Equity. New Line Equity (NLE) is another campaign which provides a special type of realtor service. We identified NLE based on 22 phone numbers observed over 12 cities. Based on the set of phone numbers, a total of 3,230 NLE rental scam ads were identified, and 43.34% of them were flagged.

Many user reports claim that the scam process of NLE is quite similar to that of ASO. A victim calls the number found in a Craigslist rental ads, and NLE requests an initial fee $9.95 and monthly fee $40.95. Once the victim makes a payment, NLE provides him with a list of pre-foreclosure properties. In many

cases, however, it turns out that most of the listed properties are not for rent or sale. We could not find a record of NLE from BBB, but there exists a record with a similar business name, *New Line of Equity* which has a BBB rating of 'D'. Many user reports complain about the difficulties in terminating the monthly fee payment.

Search Rent To Own. We identified Search Rent To Own (SRO) based on five URLs frequently observed over 17 cities on Craigslist. Among the five URLs, one was used as the main URL and the rest were redirection links to the main URL. Based on the set of URLs, we identified 1,664 SRO rental scam ads of which 77.46% of them were flagged. Similarly to the other two campaigns, SRO posts false rental ads on Craigslist and ask the victims to sign up their services with initial and monthly fees. The BBB record of this campaign did not exist but we found the records of two sibling websites listed in SRO website. BBB rating of those two sibling websites were 'F' and 'C', which are poor ratings for legitimate businesses.

According to the user reports, SRO first lures a customer by offering 3-day free trial service. However, SRO does not fully explain that a $39.95 monthly fee will be charged automatically after the free trial. We found many customer complains indicating that they were not notified upfront about the fact that monthly fee would be charged automatically after the free trial.

4 Flagged Ads Analysis

Currently, Craigslist relies on a flagging mechanism to filter out scam and spam ads. Our measurement study reveals that Craigslist currently flags only about 47% of all the scam ads that we identified. Further, for a subset of the scams (specifically, clone scams) that we closely monitored, the median time till flagging (for the ads that do get flagged) is about 13 h – see Fig. 1. The figure also shows that roughly 60% of clone scam ads remain active for more than 10 h and 40% remain active for more than 20 h.

For other scam categories, our data collection method did not allow us to obtain the time of flagging due to limitations of our measurement study: First, monitoring all ads on a per-hour basis would generate too much traffic, and our experiments were designed to keep our crawler's traffic volume low. Second, detecting these unknown scams required some manual effort. Hence, for some scam categories, we did not identify the scam ads soon enough to allow us to monitor them on a per-hour basis.

Even though revisiting all ads on a per-hour basis is too aggressive, we were able to revisit all ads we crawled twice after three and seven days to determine whether they have been flagged. Table 7 presents a summary of the composition of the Craigslist-flagged ads. Of 126,898 Craigslist-flagged ads, we found about 10.2% are *Scams* where we found concrete proof of scams via automated email conversation. On the other hand, about 70.3% are classified as *Spams* which consists of local ads that are found usually within a single cities and a few renown

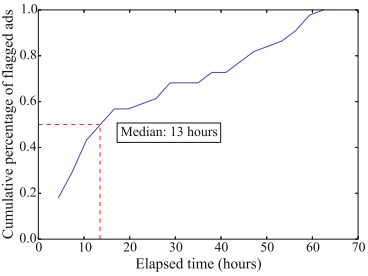

Fig. 1. Time taken to flag scam clone ads. Our system monitored 85 clone scam ads and found that among the flagged ads, only 40% were flagged within 10 h from ad posting time. In addition, about 60% were flagged within a day.

Table 7. Flagged ads categorization. 10.17% of flagged ads are identified as scams while 70.30% are identified as spams.

Category	Campaigns	# Ads (%)
Scams	Credit report scam	8,255 (6.51%)
	Clone scam	74 (0.06%)
	Realtor service scam	4,572 (3.60%)
Spams	Local ads	76,752 (60.48%)
	Credit repair ads	2,234 (1.76%)
	Legitimate rental ads	10,224 (8.06%)
Unidentified		24,787 (19.53%)
Total		126,898 (−%)

legitimate real estate companies. This leaves 24,787 (19.5%) ads as *Unidentified* where we were not able to ascertain if the ads were benign or malicious. Some of these could be clone ads or other lower volume Rent scams, but they are unlikely to be part of a higher volume template-based campaign based on the diversity of their content.

5 Discussion

This section will serve to provide a higher level view of our analysis to put into context the value of this study and potential limitations.

Potential Detection and Conversation Limitations. The heuristics we used to detect and validate scam posting were highly accurate based on our analysis. However, it still leaves the question of how many scam listings we did not detect. Without ground truth we cannot provide an estimate for this question. A fair set of assumptions is that our heuristics performed well at detecting the majority of listings associated with larger templated campaigns and worse on the cloned and manually generated rent scam listings, due to the fact that it is difficult to detect these based on the contents of the listing. In spite of this, we do detect some cloned ads and are able to gain an understanding of the structure of their scams from our conversations with these scammers.

Similarities and Differences with Other Study. Park et al. [21] focused on understanding the structure of scammers posing as buyers on Craigslist. The study found that 70% of scammers provided physical shipping addresses located in Nigeria. Furthermore, the study found evidence of a largely manual work force that would respond to scams within 1–2 days during peak work hours in Nigeria.

In this study, we find a diversity of scams that depend on different sets of infrastructure as well as rent scammers that are structured similarly to those that were encountered in their study. The credit report scams depend on credit report companies in the United States that operate affiliate programs and payout commissions for generating sales. The "bait-and-switch" campaigns depend on rental service businesses that are often incorporated in the United States and accept credit card payments with deceptive refund and re-billing policies.

6 Related Works

Advanced Fee Fraud. There have been a number of previous studies that have looked at the structure by Smith [23], Buchanan and Grant [7] and estimated losses from advance fee fraud by Dyrud [9]. Whitty and Buchaman [29] and Rege [22] have investigated the dynamics of online dating scams. More closely related to our domain, Johnson [15] explored the offline methods of real estate scammers. More broadly, Stajano and Wilson [24] created a taxonomy of the different types of psychology motivations used by scammers. Garg and Nilizadeh [11] investigated whether economic, structural and cultural characteristics of a community affects the scams on Craigslist. Tive [28] introduced in his study various techniques of advance fee fraud. Herley [12] has argued that Nigerian scammers deliberately craft their messages to be unbelievable as a method of reducing the number of replies from people that are unlikely to fall victim to these scams. In contrast, our study aimed to be more focused on collecting empirical data to enable a data-driven analysis of rental scams that does not rely on self reported statistics.

Goa et al. [10] investigates the use of ontology-based knowledge engineering for Nigerian scam email text mining. Isacenkova et al. [14] analyzed public scam email datasets mostly aggregated from numerous user reports. They identified over 1,000 different scam campaigns largely based on phone numbers. Huang et al. [13] measured romance scammer techniques on dating websites. Most recently, Park et al. [21] created Scambaiter, a measurement infrastructure that can automatically converse with scammers that reply to sales listings and performed an analysis of the methods and structure of these groups of scammers. Our work builds on this, but focuses on scammers that are posting fraudulent rental lists targeting people seeking housing on Craigslist. Unlike previous studies, our investigation we have focused on (1) understanding in-depth the modi operandi and infrastructure leveraged by rental scammers operating on Craigslist, and (2) identifying methods to detect larger-scale scam campaigns and scammers that are engaged in posting fraudulent rental lists.

Underground Studies. Another large body of recent work has set about conducting empirical measurements to understand the dynamics and economic underpinnings of different types of cybercrime. Much of this work has been focused on spam email [16,25], illicit online pharmacies [20], and mapping out scam hosting infrastructure [17,26]. Our work builds on this, but focuses deeply on fraudulent rental lists in particular. We have conducted, to our knowledge,

the first large scale empirical measurement study of fraudulent rental lists. It provides us with insights into how these scams are monetized and how they might be better detected in the future.

7 Conclusion and Future Work

Rental scams on Craigslist are a real threat encountered by many people searching for housing online; we found about 29 K rental scam postings on Craigslist across 20 major cities in 141 days. These fraudulent postings are designed to attract people interested in locating housing and target them with scams tailored to the rental domain. Based on our analysis of these scams we have identified a few potential chokepoints in rental scams that merit further investigation. We also note that analysis of online rental markets in other countries would be beneficial to improving our understanding of rental scams in other locations.

Craigslist's Detection Methods. Based on our analysis Craigslist removed 87% of the cloned ad postings we detected, after an average delay of around 10 h. Their flagging rate for the larger templated campaign postings was far lower at 50%. As future work, we plan to investigate automated detection approaches to improve filtering.

Regulatory and Payment Follow Up. As future work, we plan to contact the Federal Trade Commission (FTC) and card holder associations, such as Visa and MasterCard to inform them of our findings. We also, plan to perform test purchases from merchants to understand which banks they are contracting with to process credit card transactions.

Expanding to Other Countries. Many of these scams were specific to the United States. We plan to expand our studies to other countries in order to understand how scammers adapt their methods to other regions.

Conclusion. In this paper, we presented a systematic empirical measurement study of rental scams observed on Craigslist. As part of this study we present techniques that are effective at identifying rental scam postings and classifying them into larger scam campaigns. In parallel, we contacted a subset of these scammers to gain detailed information about the infrastructure required for them to profit. In total we identify seven major rental scam campaigns of which five depend on credit card payments for deceptively advertised services and businesses that are often registered in the United States. Finally, we find that filtering efforts by Craigslist remove less than half of the listings we detected. We believe that our techniques for identifying scam campaigns and understanding of their infrastructure could provide more effective methods for disrupting rental scams.

Acknowledgements. We thank Markus Jakobsson and the anonymous reviewers for their valuable feedback. This work was supported by the National Science Foundation grant CNS-1619620. This work was funded in part by NSF grants CNS-1314857, CNS-1453634, CNS-1518765, CNS-1514261, a Packard Fellowship, a Sloan Fellowship, two Google Faculty Research Awards, a VMWare Research Award, and an NSA Lablet grant.

A Example Scam Ads

(See Figs. 2 and 3)

```
*Come See this stunning 2 bedroom 2.5 bathroom home*
*Come See this quiet 3 bedroom 2 bathroom rental property* 2014 Deal
*Come See this lovely 1 bed / 1.5 bath rental* Discount for 2014
*Come Lay your eyes upon this wonderful 2 bedroom 1.5 bathroom property*
*Come Lay your eyes upon this gorgeous 1 bed 1 bath place*
*Come Lay your eyes upon this gorgeous 1 bed / 1.5 bath rental*
```

Fig. 2. Example ad titles with sophisticated templates used by CreditReport_Yahoo campaign.

B Example Scam Emails

```
Thanks for emailing me regarding the house is still available, but
presently I'm on business trip to Kuala Lumpur,Malaysia.
...
PLEASE TELL US ABOUT YOURSELF
Full Name_____________________________
Home Phone ( )_____________________________
Cell Phone ( ) ____________________
Date of Birth_____________________
Current Address_____________________
City____________State______ Zip______
Reasons for Leaving_____________Rent $________
Are you married_____________________________
How many people will be living in the house___________
Do you smoke_____________
Do you have a pet_____________
Do you have a car_____________
Move In Date_____________
```

Fig. 3. Example rent application template. Clone scam campaigns usually request a victim to fill out their rent application form.

```
Hello,
I hope you are having a wonderful day. Here's some good news: the
apartment's still available!
...
When you're ready for a personal appointment, then please go to the link
below and grab your free credit score. We recommend this site because
all of our tenants used it and never had any problems. Just fill out the
form and indicate that you want the score. What is in the report isn't
important to us, it's more of a formality to have it on file, to make
sure there are no previous property related issues. You can get your
free credit score at CLICK HERE
Remember, we only need to see the page about the rental history. That's
all we need to see at the showing. We typically waive the security
deposit with a score of 560+.
...
```

Fig. 4. Credit report scam email.

References

1. 800notes. http://800notes.com/
2. DB-IP. http://db-ip.com/
3. Report craigslist Scams. http://reportcraigslistscams.com/
4. Ripoff Report. http://www.ripoffreport.com/
5. United States Census Bureau. http://www.census.gov/
6. National association of realtors - field guide to quick real estate statistics. http://www.realtor.org/field-guides/field-guide-to-quick-real-estate-statistics (2013)
7. Buchanan, J., Grant, A.J.: Investigating and prosecuting Nigerian fraud. U. S. Attorneys' Bull. **49**(6), 39–47 (2001)
8. Clayton, R., Moore, T., Christin, N.: Concentrating correctly on cybercrime concentration. In: Proceedings of the Fourteenth Workshop on the Economics of Information Security (WEIS), Delft, Netherlands, June 2015
9. Dyrud, M.A.: I brought you a good news: an analysis of Nigerian 419 letters. In: Proceedings of the 2005 Association for Business Communication Annual Convention (2005)
10. Gao, Y., Zhao, G.: Knowledge-based information extraction: a case study of recognizing emails of Nigerian frauds. In: Montoyo, A., Muńoz, R., Métais, E. (eds.) NLDB 2005. LNCS, vol. 3513, pp. 161–172. Springer, Heidelberg (2005). doi:10.1007/11428817_15
11. Garg, V., Nilizadeh, S.: Craigslist scams and community composition: investigating online fraud victimization. In: International Workshop on Cyber Crime, IEEE (2013)
12. Herley, C.: Why do Nigerian Scammers say they are from Nigeria? In: WEIS (2012)
13. Huang, J.M., Stringhini, G., Yong, P.: Quit playing games with my heart: understanding online dating scams. In: Almgren, M., Gulisano, V., Maggi, F. (eds.) DIMVA 2015. LNCS, vol. 9148, pp. 216–236. Springer, Cham (2015). doi:10.1007/978-3-319-20550-2_12

14. Isacenkova, J., Thonnard, O., Costin, A., Balzarotti, D., Francillon, A.: Inside the scam jungle: a closer look at 419 scam email operations. In: Security and Privacy Workshops (SPW), 2013 IEEE, pp. 143–150. IEEE (2013)
15. Johnson, C.: Fakers, breachers, slackers, and deceivers: Opportunistic actors during the foreclosure crisis deserve criminal sanctions. Cap. Univ. Law Rev. **40**(4), 853 (2012)
16. Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G.M., Paxson, V., Savage, S.: Spamalytics: an empirical analysis of spam marketing conversion. In: Proceedings of the 15th ACM Conference on CCS. ACM (2008)
17. Konte, M., Feamster, N., Jung, J.: Dynamics of online scam hosting infrastructure. In: Moon, S.B., Teixeira, R., Uhlig, S. (eds.) PAM 2009. LNCS, vol. 5448, pp. 219–228. Springer, Heidelberg (2009). doi:10.1007/978-3-642-00975-4_22
18. Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Félegyházi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., McCoy, D., Weaver, N., Paxson, V., Voelker, G.M., Savage, S.: Click trajectories: end-to-end analysis of the spam value chain. In: IEEE Symposium on Security and Privacy (2011)
19. McCoy, D., Dharmdasani, H., Kreibich, C., Voelker, G.M., Savage, S.: Priceless: the role of payments in abuse-advertised goods. In: Proceedings of the 2012 ACM Conference on CCS, CCS 2012 (2012)
20. McCoy, D., Pitsillidis, A., Jordan, G., Weaver, N., Kreibich, C., Krebs, B., Voelker, G.M., Savage, S., Levchenko, K.: Pharmaleaks: Understanding the business of online pharmaceutical affiliate programs. In: USENIX Security Symposium (2012)
21. Park, Y., Jones, J., McCoy, D., Shi, E., Jakobsson, M.: Scambaiter: understanding targeted nigerian scams on craigslist. In: NDSS (2014)
22. Rege, A.: What's love got to do with it? Exploring online dating scams and identity fraud. Int. J. Cyber Criminol. **3**(2), 494–512 (2009)
23. Smith, A.: Nigerian scam e-mails and the charms of capital. Cult. Stud. **23**(1), 27–47 (2009)
24. Stajano, F., Wilson, P.: Understanding scam victims: seven principles for systems security. Commun. ACM **54**, 70–75 (2011)
25. Stone-Gross, B., Holz, T., Stringhini, G., Vigna, G.: The underground economy of spam: a botmaster's perspective of coordinating large-scale spam campaigns. In: Proceedings of the 4th USENIX Conference on Large-Scale Exploits and Emergent Threats, LEET 2011, p. 4. USENIX Association, Berkeley (2011)
26. Stone-Gross, B., Moser, A., Kruegel, C., Kirda, E., Almeroth, K.: FIRE: FInding Rogue nEtworks. In: Proceedings of the Annual Computer Security Applications Conference (ACSAC), Honolulu, HI, December 2009
27. Thomas, K., Huang, D., Wang, D., Bursztein, E., Grier, C., Holt, T., Kruegel, C., McCoy, D., Savage, S., Vigna, G.: Framing dependencies introduced by underground commoditization. In: Proceedings of the Fourteenth Workshop on the Economics of Information Security (WEIS), Delft, Netherlands, June 2015
28. Tive, C.: 419 scam: Exploits of the Nigerian con man. iUniverse (2006)
29. Whitty, M.T., Buchanan, T.: The online romance scam: a serious cybercrime. CyberPsychol. Behav. Soc. Netw. **15**(3), 181–183 (2012)