Folex: An Analysis of an Herbal and Counterfeit Luxury Goods Affiliate Program

Mohammad Karami
George Mason University
Email: mkarami@gmu.edu

Shiva Ghaemi
George Mason University
Email: sghaemi@gmu.edu

Damon Mccoy
George Mason University
Email: dmccoy6@gmu.edu

***Abstract*—The profitability of the underground criminal business of counterfeit or unauthorized products is a major funding source that drives the illegal online advertisement industry. While it is clear that underground online affiliate-based programs are profitable for their owners, the precise business operations of such organizations are unknown to a large extent. In this study, we present the results of our analysis of a replica and herbal supplements affiliate program based on leaked ground truth data. The dataset covers a period of over two years and includes more than $6 million in sale records for an affiliate program known as *Tower of Power* (*TowPow*) focusing on the herbal supplements and counterfeit luxury goods market. In this paper we provide a detailed empirical analysis of the participating affiliates, sales dynamics, revenue sharing, domain usage patterns and conversion rates.**

I. Introduction

One of the principal funding sources for abusive advertising (e.g., e-mail spam) is the sale of counterfeit goods to consumers (e.g., pills, watches, handbags, etc.). The infrastructure for abusive advertising is realized by exploiting a broad range of different techniques including email spamming, supported by a large number of compromised hosts [6], blackhat search engine optimization (SEO) [7], [12], [23], [24], CAPTCHA solving services [17], and spamming on popular forums [19], [20] or online social networks [4], [5], [22]. However, few legitimate businesses wish to utilize these illegitimate advertising channels, thus they are often used to promote illegitimate online businesses, such as fake AV, counterfeit software, pharmaceuticals, herbal supplements, and replica luxury goods.

Understanding the economic structure of cyber criminal ecosystem is a significant challenge which has recently gained attention from research community [3], [8], [9], [12]. A precise understanding of the internal dynamics of online underground businesses forms a basis for identifying effective interventions for undermining such organizations [14], [15]. However, studies not based on ground truth data are susceptible to imprecise deductions. For instance, as pointed to in [16], in an attempt to estimate the turnover amount of leading online pharmacy programs, two different research studies using different methodologies [9], [12] arrived at significantly different estimations.

This paper provides an analysis based on ground truth affiliate and order data from the *Tower of Power* (abbreviated as *TowPow*) affiliate program that was affiliated with *ZedCash*[1] and is behind the infamous *ViaGrow* "banded" herbal male enhancement pills. By performing an analysis of hundreds of thousands of visitors, tens of thousands of sales, and the activity of over 100 affiliates we are able to provide detailed information on many key aspects of this market segment. This includes, conversion rates of visitors to customers, usage patterns of domains, ability of affiliates to drive sales, and revenue sharing between the affiliate-program and affiliates.

A few of our key new findings include: We find that herbal products are a growing segment of the spamvertised ecosystem, generating over $5 Million in revenue. Based on our analysis domains that are active for a week or less generate almost 50% of the total revenue. This highlights the difficulty of domain name based interventions. In addition, we confirm findings from other studies [8], [9], [16]

While the mechanics of underground affiliate-based programs have been outlined in previous works [13], [18], and ground truth data have been studied for specific segments, there is evidence that different market segments (pharmaceuticals [16] and fake anti-virus [21]) have different dynamics. Thus, one of the contributions of our analysis is to provide the first look at herbal supplements and replica products which are both relatively large market segments, collectively composing nearly 25% of the spam emails in a previous study [13][2]. We believe that the analysis in this paper provides unique insights and a significant addition to the growing body of research documenting the internal workings of underground affiliate programs.

II. Background

Due to competition in today's business environment, a level of productivity achieved only through specialization and strong business relationships with partners is demanded. The underground criminal business of counterfeit or unauthorized products is no exception in this regard. Over the last decade, vertically integrated underground organizations managing all aspects of their value chain have been largely replaced with

[1]ZedCash is an affiliate program that specializes in herbal products and replica designer goods [2]. It is open to affiliates by invitation only, but TowPow is a more open program that allows less established marketers access to market ZedCash products.

[2]Note that the herbal products were grouped into the pharmaceutical classification in this study.

organizations where some aspects of the value chain are outsourced to business partners. In particular, we have witnessed the rise of independent third party advertisers known as affiliates for promoting illegitimate businesses. The affiliates are paid on a commission basis for directing customer traffic using a wide range of often abusive spam-based techniques to storefronts provided by the sponsoring affiliate program. The affiliate programs turn a blind eye to the abusive-advertising techniques or in the case of *TowPow* offer services such as bullet proof shop hosting for their affiliates. This in turn, frees the affiliate to focus solely on the task of attracting customer traffic and the rest of tasks such as design of web storefronts, payment processing, order fulfillment, customer service, and etc are handled by sponsors. The affiliate-based model has been widely adopted within the underground ecosystem.

While counterfeit pharmaceuticals represent a large portion of the goods promoted via spam advertisement channels, herbal supplements[3] and replica luxury goods were promoted by close to 25% of email spam messages in a previous study [13]. Selling herbal supplements, such as *ViaGrow*, has one key advantage over pharmaceuticals, namely it is more complicated to disrupt the payment processing for these goods. This stems from the fact that there are no intellectual property violations occurring, thus bondholder's complaints to card associations (Visa/Master Card) that have disrupted the pharmaceuticals and counterfeit software affiliate programs as documented in a previous study [15] will not be effective against herbal affiliate programs.

Due to the underground nature of cyber criminal ecosystem, most research studies have to rely on anecdotal data, inference or estimation techniques to draw conclusions [9], [12]. Certainly access to real world data and the knowledge derived from its analysis can be tremendously beneficial for the research community [16], [21]. Not only we can gain the privilege of perceiving how the underground cyber economy operates in the wild, we also gain a firm basis for evaluation and validation of research studies not based on ground truth data. For example, Kanich et al. used one method to estimate the conversion rate of visitors to orders for illicit pharmacy sites using HTTP logs from an image server and inference techniques to arrive at a conversion rate of 0.5% based on IP address [9]. However, Kanich et al. used a different technique in another study and at arrived at an estimate of a 2% conversion rate [8]. We are also unable to answer simple questions about the herbal and replica market, such as "how much is the average order size?" and "how well would inference techniques based on sequential order number allocation work at estimating revenue?"

In this paper we answer these questions for the herbal and replica market segments by focusing on the *TowPow* affiliate program. This program is affiliated with ZedCash, they actively recruited email spammers on underground forums[4] and dominate the herbal and replica segments [10].

[3]This segment is often group with pharmaceuticals, but as we will show herbal sales differs from the dynamics of the prescription free pharmaceuticals sales in some aspects.

III. Dataset

In this section we provide a brief overview of the dataset used in our analysis. The dataset was acquired as a SQL dump of the operational database of the Tower of Power (*TowPow*) affiliate program. The database dump only includes the definition of database tables and the corresponding data records. Thus, we are left with the challenging task of reverse engineering the semantic meaning of the database tables, and resolving inconsistencies and ambiguities in the data. Table I provides a summary of the data contained in this database.

The database includes a total of 35 tables; roughly half of these tables are related to the ticketing system of the affiliate program used for technical and administrative support of participating affiliates. Most of our analysis was performed using only five tables: *affiliatemaster* recording information about each affiliate, *affiliatesale* recording the details of each order, including the status of order, the order amount and the commission amount for the corresponding affiliate, *sitemaster* recording information on the products (15 products in total) being sold by the affiliate program, *domainmaster* recording information on the domain names used by each affiliate, and *clicks_subid* containing visit information for a limited number of domain names.

While this is an admissibly high quality dataset containing valuable data for understanding the internal operations of the underground affiliate program, some of the database tables are incomplete or contain inconsistent data. However, this imperfectness is not extensive and does not prevent us from conducting a reliable analysis to gain insight into the internal operations of the underground affiliate program. Where relevant, the data incompleteness will be noted while discussing data analysis.

A. Authenticity

Due to the fact that this is "leaked data" and we did not collect it ourselves, we will address the question of why we believe this data is genuine. While we cannot prove with absolute certainty that all or part of this data was not forged, there are several pieces of this data that we know are correct. For one, we joined *TowPow* as an affiliate [5] to access the effectiveness of a banking level intervention for a previous study [15] and we can observe our affiliate information in the dataset as expected. Secondly, we placed one purchase with *TowPow* and again we can find this purchase in the sales records as expected. While this evidence cannot prove that none of this data was altered or faked, we will proceed with our analysis under the assumption that this data is accurate.

[4]This is a quote from an underground posting advertising *TowPow*: "TowPow is not like any other affiliate system. Tow Pow offers not only quality landing pages, but they also offer FREE bullet proof domains and hosting for your spamming needs."

[5]TowPow is a relatively open affiliate program that only requires a brief online "interview" to establish that the applicant has a working knowledge of affiliate marketing techniques.

Period	Affiliates	Domains	Orders	Revenue
Oct 2009 - Dec 2011	119	3,730	59,695	USD $6.1M

TABLE I
SUMMARY OF *TowPow* AFFILIATE PROGRAM DATA USED IN THE ANALYSIS.

B. Ethics

The other concern is the ethics of dealing with "leaked data" that in all likelihood was obtained via illegal methods. This is not the first case of this type of data being used and in fact it has cropped up in a number of fields ranging from politics (Pentagon papers and State department cables), rogue pharmaceutical customer records and the study of stolen password datasets. This demonstrates a trend that using this type of data can be acceptable. We justify our choice to use this dataset by reasoning about harm.

The existence of this dataset has already been announced publicly and the association of this data to *TowPow* and *ZedCash* has also been widely publicized. Therefore, we cannot create any new harm by repeating these findings. To mitigate any additional harm to the different people involved, we created a number of protocols and controls that were put in place. First, there is no identifying information about customers in the database and we restrict our analysis of them to geo-locating the visitors to their country of origin and including this aggregate finding. We do not attempt any further investigation of the customer's location or identities. As for the operators of *TowPow* and their affiliates, we do not use their actual names even when we have become aware of this information from meta data or other sources. Our analysis is restricted to reporting results in aggregate or using their online handles when referring to major individual affiliates.

C. Characterization

Affiliates. During the period (roughly two years) covered by the dataset, a total of 119 affiliates registered with *TowPow* and of these, 73 affiliates have actively participated in the affiliate program. An affiliate is considered to be an active participant if at least one order record is associated with that affiliate in the database. In our analysis, each affiliate is treated as a distinct individual. However, in a few cases there are evidences indicating the likelihood of one person registering under multiple affiliate accounts. For example, the same IP address is used to access two different accounts. In general, most of the affiliates did not provide an email address or other contact information when registering their accounts and therefore making it infeasible to perform a deduplication of the affiliate accounts.

Products. A total of 15 distinct products are promoted and sold by the *TowPow* affiliate program. We have categorized these products into four categories, Diet Supplements, Replica (Counterfeit luxury goods), Male Enhancement (including the *ViaGrow* "brand"), Ink Cartridges and Electronic Cigarette. Table II lists the items in each product category. We omit ink cartridge and electronic cigarettes from our analysis, since combined they represent an insignificant amount of revenue and orders[6].

Product Category	Items
Diet Supplement	PowerSlim, QuickSlim, TrimSpray, HCG, HCGSlim, RapidSlim, PremiumPower, HCGElite
Male Enhancement	ViagrowPro, Viagrow, ED Pills
Replica	SwissReplica, Couture
Electronic Cigarette	Electronic Cigarette
Ink Cartridges	E-Ink

TABLE II
PRODUCT CATEGORIES

Orders. Attempted purchases generated an order record that included a sequentially generated order ID number, the total amount of the sale, a time stamp of when the order was placed, what type of product was ordered, a status field indicating if the order was successfully billed, and the affiliate that generated the sale along with their commission amount. The dataset does not include any personal information about the customers such as name, address, or payment information. Because of this, we are unable do any analysis of reorders or customer demographics.

Domains and Visits. Beginning on November 19th 2010 the system started recording the domain that generated each sale, which allows us to perform our analysis of domain usage and sales patterns for this portion of the dataset. Subsequently, on September 2nd 2011 the system began recording visitor information for a limited subset of the active domains from which we can compute conversion rates and visitor location information.

IV. ANALYSIS

Using the dataset we provide an analysis of *TowPow* business from the perspective of the customers and affiliate marketers.

A. Customers

All money that flows into these abusively-advertised affiliate programs must come directly from customers. We will explore the questions of what pent-up demand for products is being fulfilled, since that is what ultimately sustains this entire abusive-advertising channel.

[6]Less then $3,320 and 54 total orders.

Product Category	Average Price
Diet Supplement	$97.82 ($117.77*)
Male Enhancement	$101.99 ($121.94*)
Replica	$188.10

TABLE IV
AVERAGE ORDER SIZE BY PRODUCT. (*INCLUDES SHIPPING FEES.)

Country	Percentage
United States	72%
Great Britain	5%
Canada	4%
Germany	3%
Others (123 countries)	16%

TABLE VI
VISITOR LOCATIONS BASED ON IP GEO-LOCATION

1) Product Selection: As we can see from Table III, the key niche that *TowPow* fills is demand for *HGC* herbal diet supplements and *ViaGrow* herbal male enhancement products which total 96% of their sales and 94% of their gross revenue respectively. In particular, their line of diet supplements was a key product area that was left untapped by many of the pharmaceutical affiliate programs, which focus their advertisements towards male enhancement products [16].

By doing an analysis of the order amounts and matching these up to the templates *TowPow* provided to affiliates shows that the order amounts do not include shipping fees of $19.95 charged on all herbal orders. If we include the $1.14M in shipping fees the total amount of gross revenue raises to $7.2M.[7]

Based on the sales records and our product categorization, we have calculated the average price of an item for each of the three product categories. Table IV shows that the average herbal order size is around $120 including shipping fees[8]. Looking at the actual herbal order sales amount and mapping them back to the quantity of bottles ordered, reveals that the smallest quantity of one bottle is the most popular. The average sales amount for replica goods is slightly higher than herbal sales and mapping purchase prices to sales amounts reveals that the low end ($124-$135) replica Rolex models make up 614 (30%) of the orders with the rest of the orders being more difficult to map back to products.

This demonstrates that even though discounts of up to 44% per a bottle are offered for larger herbal orders many customers are likely limiting their order to a smaller one to test out the effectiveness. In the case of replica luxury goods, it is clear that most of the advertising is directed towards counterfeit Rolex watches based on order amounts and the fact that these are featured on the shops' front pages. It is likely that customers are enticed by the steep discounts as compared to an authentic Rolex watch[9].

Finally, each order is assigned a sequentially increasing order number that matches the one given to customers in their order confirmation emails. Performing an analysis of these order number and order status field sheds light onto how accurate revenue estimation techniques would be for *TowPow*. To compute the error, we first determine that the range of order numbers is 80,428. Further, we find that 18,424 (24%) of the accepted orders were not billed successfully and 2,309 of the order numbers are missing from the database, indicating they were possibly filtered or deleted. This means that the gross revenue estimation technique used by Kanich et al. [9] would have an error of approximately 25% assuming that the exact average order amount is known.

2) Conversion Rate: Based on the visit information available for a limited number of domains and the order records associated with those domains we can calculate the conversion rates for this subset of domains. While the order records are available for 73 different affiliates, the clicks_subid table only records visit information of three affiliates covering nine different domains. Table V presents the conversion rate calculations for each domain. All of these domains sold herbal diet supplement, which comprise the bulk of gross revenue and sales. It shows that Penwire, the top earning affiliate, achieves a conversion rate of 2.7%, while the other two affiliates, Never and Fail, have conversion rates closer to 4%[10] This difference in conversion rate between affiliates highlights the fact that deriving techniques to estimate order volume and gross revenue based on the number of visitors is a challenging problem.

3) Visitor Location: As pointed to earlier, the dataset does not contain any information about the customers. However, it does contain the IP addresses for 430,095 visitors of the nine domains listed in Table V. To get an idea of where the visitors and potential customers are coming from, we used the GeoIP database from Maxmind[11] to identify the country locations for these visitors. As shown in Table VI, while there are visitors from 127 different countries, 72% of them are coming from United States and Great Britain and Canada have the second and third highest number of visitors, with 5% and 4% of visitors respectively[12]. The share of visitors and potential customers from United States is comparable with the measurement for online counterfeit pharmaceutical products [9]. It also confirms that money from western consumers is providing the monetary incentive for ceaseless exploitation of abusive-advertising channels by underground businesses.

B. Affiliates

The complexities of modern business environment have forced organizations to embrace specialization to sustain their

[7]Note that free shipping is offered for replica orders.

[8]These are in line with average sales amounts reported by similar studies of pharmacy orders [16].

[9]For example, the same Rolex Submariner Black Dial sells for $6,999 on amazon.com and for $135 on the *TowPow* sites, which is a discount of over 5000%.

[10]These conversion rates are in line with conversion rates reported by other studies of spam advertised products, such as fakeAV [21] and pharmaceuticals [8].

[11]http://www.maxmind.com/en/geolocation_landing

[12]We are assuming that the visitors are not using anonymizing services such as web proxy or VPN.

Product Category	Orders	Revenue
Diet Supplements	43,812 (73.40%)	$4.29M (70.45%)
Male Enhancement	13,746 (23.03%)	$1.40M (23.05%)
Replica	2,083 (3.49%)	$392K (6.44%)

TABLE III
BREAKDOWN OF PRODUCTS SOLD

Domain	Affiliate	Visitors	Orders	Conversion Rate
dropshcg.ru	Penwire	292	8	2.7%
hcg-ultra-drops.com	Penwire	50304	2515	5.0%
hcg-ultradrops.com	Penwire	49731	1522	3.1%
hcgultra-drops.com	Penwire	115125	3042	2.6%
hcg-drops-ultra.com	Penwire	77289	1514	1.9%
hcgultra24.com	Penwire	61091	1117	1.8%
hcglimited.com	Never	6273	272	4.3%
hcginfodiet.com	Never	13747	510	3.7%
hcgultrasale.com	Fail	56243	2084	3.7%
-	-	430095	12584	2.9%

TABLE V
CONVERSION RATES

competitiveness. In particular, third party advertisers are paid on a revenue sharing basis for directing visitors to sponsor's storefronts who eventually complete a transaction. Online businesses for selling replica and herbal supplement products are no exceptions, an affiliate program provides web storefronts, order fulfillment, customer service, etc and third party advertisers or affiliates are just responsible for promoting the program and directing traffic to storefronts. In the case of *TowPow*, many of their affiliates used abusive tactics such as botnet generated email spam, blackhat search engine optimization, comment spam, and etc. to promote *TowPow* products.

This section provides an analysis of the *TowPow* affiliates with an emphasis on their revenue generation and earnings.

1) Affiliate Registrations: There are a total of 119 affiliates registered with the program in a period of approximately two years, from October 2009 to November 2011. Fig 1 shows the monthly break down of the number of affiliates that joined *TowPow*. As can be observed, the majority of affiliates joined *TowPow* during the second half of the period. The number of monthly registrations reaches its peak in December 2010, which is potentially attributable to the holiday shopping season.

2) Affiliate Sales: We observe a four-month delay between the first affiliate registration date and the first sale date. This might indicate that *TowPow* did completely finish establishing their payment and fulfillment end of the business, which is shared with *ZedCash* based on past test purchases.

Based on the available sales records, out of 119 affiliates who have registered with the program, only 73 have actually generated at least one sale and only 67 have produced a sale that was successfully billed. The number of successfully billed sales generated by an affiliate ranges from one to 10,944 for the most successful affiliate. With the exception of Replicas, the share of the product categories from the sales records, matches with the number of affiliates involved in selling products in those categories. Table VII summarizes the number

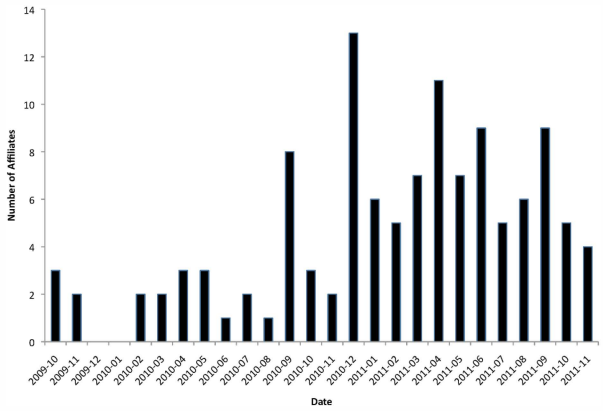

Fig. 1. Monthly registrations of affiliates

Product Category	# of affiliates
Diet Supplement	54
Male Enhancement	29
Replica	33

TABLE VII
NUMBER OF AFFILIATES MARKETING EACH CATEGORY OF PRODUCTS.

of active affiliates for each of the three product categories, note that some affiliates were promoting more than one category of products and most affiliates that promoted *ViaGrow* male enhancement products also promoted *HGC* diet supplements.

3) Affiliate Commissions: For each generated order, the dataset includes the commission amount paid to the corresponding affiliate. Analysis of the commissions shows that *TowPow* paid out 35% of the total sales amount not including shipping fees as a commission to their affiliates[13].

The total amount of sales for all affiliates and all products

[13]This commission structure is slightly lower than that of the pharmaceutical market, were top earning affiliates negotiate commission of 40-45% [16].

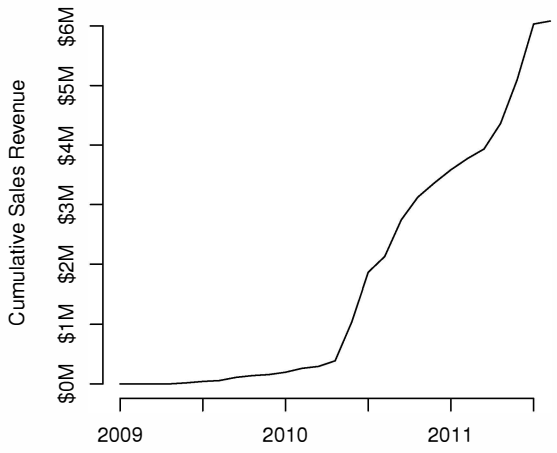

Fig. 2. Cumulative sales amount

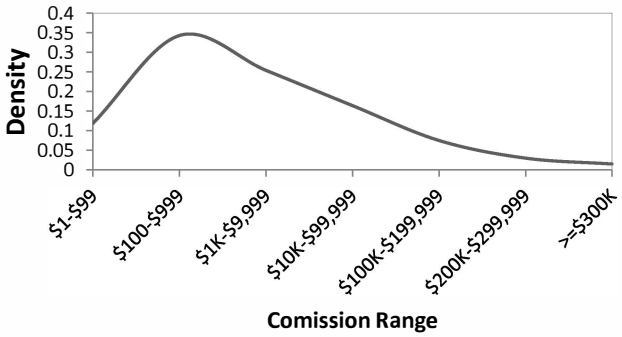

Fig. 3. Distribution of commission among affiliates

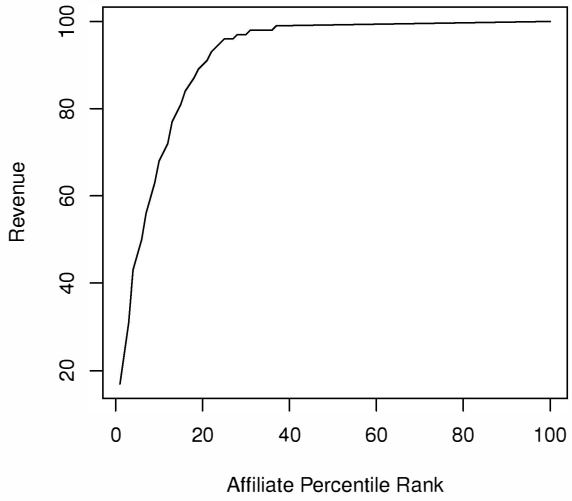

Fig. 4. Distribution of affiliate contributions to total *TowPow* revenue

is more than $6 million in gross revenue (over $7 million if estimated shipping fees are included). Figure 2 shows the cumulative amount of sales over time. As it can be observed, there are no sales for the first four months and only 10% of the total gross revenue was generated in the first year. This shows the latent demand for herbal products that *TowPow* and their affiliates fulfilled and indicates that this market segment of the underground economy is not yet saturated as 90% of gross revenue was generated in the second year. Much of this sales growth can be linked to four key affiliates that joined close to the end of the first year and generated close to half of the revenue in the second year.

Figure 3 shows the distribution of revenue earned by affiliates. Collectively, the affiliates earned over $2 million in commissions. However, this amount is not evenly distributed over all of the affiliates. In fact, as shown in Figure 4, just 4% (3 in total) of the affiliates earned 40% of all commissions paid to affiliates. The minimum amount earned by an affiliate is $20.98 and the highest amount earned is $368,370. While the average commission for a *TowPow* affiliate was around $32K, most affiliates earned far less and it was only a few successful affiliates that were responsible for generating the bulk of the revenue. This points to the fact that disrupting these few successful affiliates would heavily reduce the amount of revenue injected into the underground economy by *TowPow*.

4) Actual Payments to Affiliates: The database includes a table for recording the history of payments to affiliates. While there are 73 affiliates with at least one successfully billed order, the payment history records only contain payouts for 61 affiliates. Webmoney is used as the primary means for financial settlement with affiliates. We noticed that there are no payment records for affiliates with a total commissions amount of less than $100. This suggests that the affiliate program has a threshold of $100 as the minimum commission amount that must be earned by an affiliate before they receive a payout. We were able to identify eight affiliates with a total commission amount of less than $100 having no records in the payment history table. Based on the information in the payment history table, the total amount of payments to affiliates is $1,933,329. This is close to the total commission amount owed to affiliates based on the sales records.

C. Domains

Many past interventions of abusive-advertising channels have been focused at the registrar and domain name level [11], [14]. This section provides some insight into the usage patterns of domains by affiliates. This includes the average active lifetime of domains and the revenue generated by domains over their lifetime.

1) Affiliate domain name usage: The dataset contains 3,730 distinct domain names assigned to 41 affiliates. Breaking down the domain names based on their Top Level Domains (TLDs), 93% of them are *.ru*, 6% are *.com* and 1% belong to other

Affiliate	Domain Name	Average Visitors
Penwire	hcg-ultra-drops.com	7186
Penwire	hcg-ultradrops.com	5525
Penwire	hcgultra24.com	2776
Fail	hcgultrasale.com	2163
Penwire	hcg-drops-ultra.com	2088
Penwire	hcgultra-drops.com	1984
Never	hcginfodiet.com	1249
Never	hcglimited.com	1045

TABLE VIII
AVERAGE NUMBER OF DAILY VISITORS

TLDs such as *.info* or *.org*.

The allocation of domain names to affiliates is highly variable ranging from more than a thousand domain names assigned to a single affiliate to an affiliate using a single domain name. However, no direct relationship was observed between the number of domains assigned to an affiliate and their profitability. In fact, the most successful affiliate was allocated only 8 domain names. Our hypothesis for this domain name behavior is that affiliates utilize different abusive-advertising vectors, such as email spam or blackhat search engine optimization techniques. Unfortunately, we do not have ground truth data, such as HTTP referer information to support this conclusion. However, an analysis of the *uribl* domain blacklist [1] reveals that a large number of the *.ru* domains are present, suggesting that they were used in email spam campaigns at some point. Furthermore, web searches for some of the most successful domain names leads to redirection sources such as fake blogs that include links to these domains. This is an indication for the usage of blackhat search engine optimization techniques for directing visitors to these sites.

2) Average number of daily visitors: Table VIII summarizes the average number of visitors per day for domains that have at least an average of 1000 daily visitors[14]. As can be observed, most of the domains listed in Table VIII belong to Penwire, the most successful affiliate that likely utilized blackhat search engine optimization techniques to attract potential customers.

As the domains associated with orders were not initially recorded in the database, we can only identify 685 distinct domains used for generating sales. Furthermore, due to cross-table data inconsistencies, we are only able to infer the domain names for 96 of these domains. This includes 50 *.com* domains, 39 *.ru* domains and 7 domains with *.info/.biz/.org* TLDs. We used the service provided by *domaintools.com* to gather the historic whois data for these domains. All the *.ru* were registered through NAUNET-REG-RIPN registrar and the Center of Ukrainian Internet Names was the registrar for 90% of the *.com* domains. However, past analysis of domain register level interventions show that they do not have a significant and lasting economic impact on affiliate programs [14].

[14]Please note that the dataset only contains the visitor information for nine domains

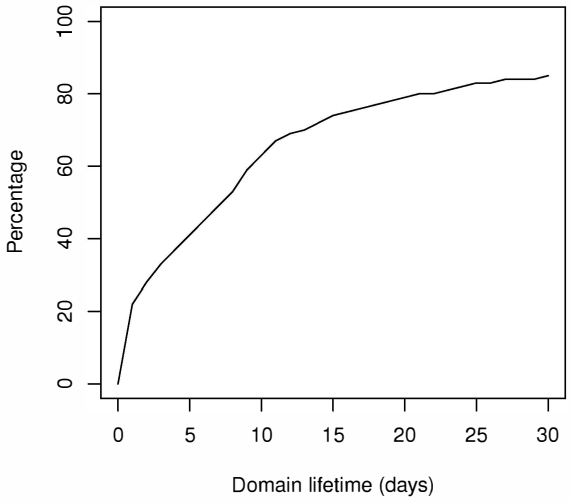

Fig. 5. CDF of domain lifetimes based on first and last sale generated

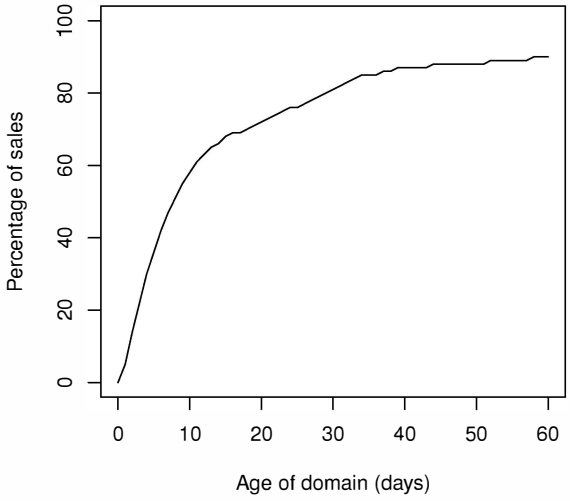

Fig. 6. Cumulative percentage of sales for the entire *TowPow* program based on the age of the domain

3) Lifetime of domain names: Figure 5 shows the lifetime for all 685 domains that generated a sale based on the first sale generated as the initial use of the domain and last sale generated as the end of that domain's usage. This shows that most domains are fairly short lived. For instance, half of the domains have a lifetime less than one week and a quarter of the domains only generate sales for less than three days.

Figure 6 shows the cumulative amount of total revenue contributed to *TowPow* as domains age. For example, this shows that domains that were active for a week or less

generated close to half of the total revenue for the affiliate program. This indicates that any intervention at the registrar and domain level must be highly reactive, since a large amount of the value is extracted from a domain within the first few days it is active.

V. Discussion

One of the main contributions of our analysis is to point out difference in the herbal and replica market dynamics as compared to other heavily studied market segments, such as pharmaceuticals and fake AV. In this section we put our analysis in context and point out how it differs and is similar to other underground market segments from the perspective of conversion rates, order dynamics, and affiliate commissions.

Domain Usage. We find that domain names are a short lived and quickly monetized resource. This indicates that domain name level interventions might not have a significant economic impact. Ours is the first study of this dynamic, so it is not clear if this is the case for other market segments.

Order size. The average order size of successful herbal sales was between $118-$122, which is closely related to the average order size of $115-$135 found in the illicit pharmaceutical affiliate programs [16]. However, our findings reveal that the average order size for replica is $188 which is an increase of over 25%. These are all larger then those found in a study of fake AV that reported average order size ranged from $60-$83 [21]. Thus, illustrating the similar and different dynamics of each market segment.

Affiliate commissions. Our study and prior studies [16], [21] have pointed out the fact that most affiliates are not that successful and that underground affiliate programs rely on a few key affiliates to generate most of their sales. Also, all of the studies agree that around 30-45% of sales amounts are paid out to these affiliates and that Webmoney is often used as the electronic currency for payments to affiliates. This paints a clear picture that a few successful affiliates are responsible for much of the abusive advertising.

Successful billing rates. We find a higher incidence of orders that were not successfully billed in our study 24% compared to only 8-12% found in the study of pharmaceutical affiliate programs [16]. This might be explained by pharmacy affiliates filtering more attempted purchases (20%) before they are recorded in their order database as opposed to less than 3% of the orders in our analysis.

Conversion rate. The conversion of 2.9% is close to that of 2% that has been reported by other studies of fake AV [21] and pharmaceutical spam [8]. However, it differs from another study by Kanich et al. that estimated a conversion rate of 0.5% for a pharmaceutical affiliate program. [9] Our more fine gained analysis of three affiliate's conversion rates show a range between 2.7%-4%, this indicates that depending on the affiliates promoting a program the conversion rate can vary by at least a few percent.

VI. Conclusion

In this paper we presented an empirical analysis of, *TowPow*, an herbal and replica focused affiliate program. As we showed in our analysis, this is a growing sector of the abusive-advertising market that funds the larger underground cyber crime ecosystem. Affiliates play a critical role in the success of any online counterfeit business by employing a variety of illegitimate advertising methods, such as "black hat" search engine optimization, large scale botnet-supported spamming, and forum abuse. Our analysis reveals the dependence of the affiliate program on a handful of highly successful affiliates that are responsible for generating a major share of the revenue stream. To maximize the effectiveness of an affiliate-level intervention effort, these high earning affiliates should be identified and disrupted.

While the survival of the affiliate program over many months implies the profitability of the program, we did not have enough data at our disposal to calculate the net revenue of the program. However, we do provide numbers on the gross revenue, order dynamics and commissions paid to affiliate marketers. We also present an analysis of domain usage that highlights some of the challenges of domain registrar interventions. This provides a rare detailed view into the inner works of an herbal and replica program. Increasing our understanding of a broader segment of underground affiliate program's underlining business models will allow us to isolate intervention points that are effective across a broad class of spamvertised goods.

References

[1] Uribl.com - realtime uri blacklist. www.uribl.com/.

[2] Zed-cash - spamwiki. http://spamtrackers.eu/wiki/index.php/Zed-Cash.

[3] J. Caballero, C. Grier, C. Kreibich, and V. Paxson. Measuring pay-per-install: the commoditization of malware distribution. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, pages 13–13, Berkeley, CA, USA, 2011. USENIX Association.

[4] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao. Detecting and characterizing social spam campaigns. In *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, IMC '10, pages 35–47, New York, NY, USA, 2010. ACM.

[5] C. Grier, K. Thomas, V. Paxson, and M. Zhang. @spam: the underground on 140 characters or less. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pages 27–37, New York, NY, USA, 2010. ACM.

[6] J. P. John, A. Moshchuk, S. D. Gribble, and A. Krishnamurthy. Studying spamming botnets using botlab. In *Proceedings of the 6th USENIX symposium on Networked systems design and implementation*, NSDI'09, pages 291–306, Berkeley, CA, USA, 2009. USENIX Association.

[7] J. P. John, F. Yu, Y. Xie, A. Krishnamurthy, and M. Abadi. deseo: combating search-result poisoning. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, pages 20–20, Berkeley, CA, USA, 2011. USENIX Association.

[8] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage. Spamalytics: an empirical analysis of spam marketing conversion. In *Proceedings of the 15th ACM conference on Computer and communications security*, CCS '08, pages 3–14, New York, NY, USA, 2008. ACM.

[9] C. Kanich, N. Weaver, D. McCoy, T. Halvorson, C. Kreibich, K. Levchenko, V. Paxson, G. M. Voelker, and S. Savage. Show Me the Money: Characterizing Spam-advertised Revenue. In *Proceedings of the USENIX Security Symposium*, San Francisco, CA, August 2011.

[10] B. Krebs. Inside the gozi bulletproof hosting facility. http://krebsonsecurity.com/2013/01/inside-the-gozi-bulletproof-hosting-facility/, 2013.

[11] LegitScript and KnujOn. Rogues and registrars. are some domain name registrars safe havens for internet drug rings? http://www.legitscript.com/download/Rogues-and-Registrars-Report.pdf, 2010.

[12] N. Leontiadis, T. Moore, and N. Christin. Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, pages 19–19, Berkeley, CA, USA, 2011. USENIX Association.

[13] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Félegyházi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, D. McCoy, N. Weaver, V. Paxson, G. M. Voelker, and S. Savage. Click trajectories: End-to-end analysis of the spam value chain. In *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, SP '11, pages 431–446, Washington, DC, USA, 2011. IEEE Computer Society.

[14] H. Liu, K. Levchenko, M. Félegyházi, C. Kreibich, G. Maier, G. M. Voelker, and S. Savage. On the effects of registrar-level intervention. In *Proceedings of the USENIX Workshop on Large-scale Exploits and Emergent Threats (LEET)*, Boston, MA, March 2011.

[15] D. McCoy, H. Dharmdasani, C. Kreibich, G. M. Voelker, and S. Savage. Priceless: the role of payments in abuse-advertised goods. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 845–856, New York, NY, USA, 2012. ACM.

[16] D. McCoy, A. Pitsillidis, G. Jordan, N. Weaver, C. Kreibich, B. Krebs, G. M. Voelker, S. Savage, and K. Levchenko. Pharmaleaks: understanding the business of online pharmaceutical affiliate programs. In *Proceedings of the 21st USENIX conference on Security symposium*, Security'12, pages 1–1, Berkeley, CA, USA, 2012. USENIX Association.

[17] M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage. Re: Captchas: understanding captcha-solving services in an economic context. In *Proceedings of the 19th USENIX conference on Security*, USENIX Security'10, pages 28–28, Berkeley, CA, USA, 2010. USENIX Association.

[18] D. Samosseiko. The Partnerka — What is it, and why should you care? In *Proc. of Virus Bulletin Conference*, Sept. 2009.

[19] Y. Shin, M. Gupta, and S. Myers. The nuts and bolts of a forum spam automator. In *Proceedings of the 4th USENIX conference on Large-scale exploits and emergent threats*, LEET'11, pages 3–3, Berkeley, CA, USA, 2011. USENIX Association.

[20] Y. Shin, M. Gupta, and S. A. Myers. Prevalence and mitigation of forum spamming. In *INFOCOM 2011. 30th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 10-15 April 2011, Shanghai, China*, pages 2309–2317. IEEE, 2011.

[21] B. Stone-Gross, R. Abman, R. Kemmerer, C. Kruegel, D. Steigerwald, and G. Vigna. The Underground Economy of Fake Antivirus Software. In *Proceedings of the Workshop on Economics of Information Security (WEIS)*, 2011.

[22] K. Thomas, C. Grier, D. Song, and V. Paxson. Suspended accounts in retrospect: an analysis of twitter spam. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*, IMC '11, pages 243–258, New York, NY, USA, 2011. ACM.

[23] D. Wang, S. Savage, and G. M. Voelker. Cloak and dagger: Dynamics of web search cloaking. In *Proceedings of the ACM Cloud Computing Security Workshop*, Chicago, IL, October 2011 2011.

[24] D. Wang, S. Savage, and G. M. Voelker. Juice: A longitudinal study of an seo campaign. In *Proceedings of the Network and Distributed System Security Symposium*, NDSS'13, 2013.