Empirically Characterizing Domain Abuse and the Revenue Impact of Blacklisting

Neha Chachra*, Damon McCoy, Stefan Savage, Geoffrey M. Voelker
About 65,600,000 results (0.37 seconds)

**Purchase Online - Viagra®**
Ad | www.viagraromedelivery.com/
Buy Real Viagra - Tips To Buy Online - Getting An Rx - Avoid Counterfeits

**Taking Viagra?**
Ad | www.helprx.info/
Save up to 75%. Get a free discount coupon by SMS, Email or Print!
How much can you save? - Find Your Rx Discount - Our Popular Discounts

**Canada pharmacy viagra - Arcadia Ales**
arcadiaales.com/canada-pharmacy-viagra
What is Canada pharmacy viagra? Beside canada pharmacy viagra mm274. Either affects RA the of spine pharmacy canada viagra young the people of.
You've visited this page 2 times. Last visit: 5/20/14

**Canadian Viagra Online Purchase Authentic FDA ...**
dcfencing.com/canadian-viagra-online/
Purchase Online and Save Money! Canadian Viagra Online. Purchase Authentic FDA-accredited Meds, at U.S. Online Drugstore. Get Pills Online. Purchase ...
You visited this page on 5/20/14.

**Online Canada Pharmacy - Canada drugs. Viagra online**
awccanadianpharmacy.com/
Viagra (Sildenafil) is an oral drug for male impotence, also known as erectile ...
Comparing with Viagra, Cialis ... more » buy now ..... Canadian Viagra is power!
Viagra - Female Viagra - Antibiotics - Men's Health
You visited this page on 5/20/14.

**Buy Viagra Online from Canada Drugs - Online Canadian ...**
https://www.canadadrugs.com/products/viagra
<table>
<thead>
<tr>
<th>Sender</th>
<th>Message</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextPaydayAdvance</td>
<td>Need Cash Quick? Get up to $1000 Now! - Need Cash Quick? Get up to $1</td>
<td>May 19</td>
</tr>
<tr>
<td>ADT Authorized Deal.</td>
<td>Sleep Better w/ ADT Monitoring for About $1/Day - Sleep Better w/ ADT M</td>
<td>May 18</td>
</tr>
<tr>
<td>Freescore360</td>
<td>View Your Complimentary Credit Score - View Your Latest Credit Score</td>
<td>May 18</td>
</tr>
<tr>
<td>Freescore360</td>
<td>View Your Complimentary Credit Score - View Your Latest Credit Score</td>
<td>May 18</td>
</tr>
<tr>
<td>Christian Dating</td>
<td>View Photos Of Christian Singles In Your Area &amp; Chat For FREE Tod;</td>
<td>May 18</td>
</tr>
<tr>
<td>Life Insurance Polic.</td>
<td>Fidelity Life: Up to $300,000 Coverage today! - Fidelity Life: Up to $300000</td>
<td>May 16</td>
</tr>
<tr>
<td>High Quality Replica Wat.</td>
<td>Get your favorite TopBrandName style without breaking the bank! - Sumr</td>
<td>May 12</td>
</tr>
<tr>
<td>Freescore360</td>
<td>View Your Complimentary Credit Score - View Your Latest Credit Score</td>
<td>May 10</td>
</tr>
<tr>
<td>Freescore360</td>
<td>View Your Complimentary Credit Score - View Your Latest Credit Score</td>
<td>May 10</td>
</tr>
<tr>
<td>Info</td>
<td>sensoriums - med store</td>
<td>May 10</td>
</tr>
<tr>
<td>Rolex</td>
<td>Swiss Replica Rolex Watches - Super Replicas - Luxury Watches, Bags, Jew</td>
<td>May 9</td>
</tr>
<tr>
<td>AT&amp;T Wireless</td>
<td>Free phones free delivery. It doesn't get any better.</td>
<td>May 7</td>
</tr>
<tr>
<td>AT&amp;T Wireless</td>
<td>Free phones, free delivery. It doesn't get any better.</td>
<td>May 7</td>
</tr>
<tr>
<td>Medicare Open Enroll.</td>
<td>Check Your 2014 Enrollment Plan - See Premiums. - Check Your 2014 En</td>
<td>May 2</td>
</tr>
<tr>
<td>Google Promotion</td>
<td>CONGRATULATIONS YOU ARE SELECTED - Google Corporation 1500 Amphitri</td>
<td>May 2</td>
</tr>
<tr>
<td>AT&amp;T Online Specials</td>
<td>Get a Free Phone from AT&amp;T - Online Only</td>
<td>May 2</td>
</tr>
<tr>
<td>AT&amp;T Online Specials</td>
<td>Get a Free Phone from AT&amp;T - Online Only</td>
<td>May 2</td>
</tr>
<tr>
<td>Perfect Luxury Watches</td>
<td>Get your favorite TopBrandName style without breaking the bank! - Repli</td>
<td>Apr 30</td>
</tr>
</tbody>
</table>
Spam was 70% of total email traffic in 2013
buydrugs.com
Canadianpharmacy.com
genericviagra.com
fmomail3.info
fmomail4.info
fooodexquisite.net
gingerbreadmanz.com
givespy.com
gnawstaxi.com
hathaywo.com

BLACKLIST
Overview

Understand how domain blacklisting affects its monetizability

Answered using the ground truth data

- Amount, time of sale of drugs for every spammed domain
- Time and duration of blacklisting
Leaked Data Set

All transaction data for counterfeit pharmaceutical campaigns

Leaked publicly due to conflict
PharmaLeaks: Understanding the Business of Online Pharmaceutical Affiliate Programs

Damon McCoy* Andreas Pitsillidis* Grant Jordan* Nicholas Weaver† Christian Kreibich† Brian Krebs‡ Geoffrey M. Voelker* Stefan Savage* Kirill Levchenko*

*Department of Computer Science George Mason University
†Department of Computer Science and Engineering University of California, San Diego
‡International Computer Science Institute

Berkeley, CA

Abstract

Online sales of counterfeit or unauthorized products drive a robust underground advertising industry that includes email spam, “black hat” search engine optimization, forum abuse and so on. Virtually everyone has encountered enticements to purchase drugs, prescription-free, from an online “CanadaPharmacy.” However, even though such sites are clearly economically motivated, the shape of the underlying business enterprise is not well understood precisely because it is “underground.” In this paper we exploit a rare opportunity to view three such organizations—the GlavMed, SpamIt and RX-Promotion pharmaceutical affiliate programs—from the inside. Using “ground truth” data sets including four years of raw transaction logs covering over $185 million in sales, we provide an in-depth empirical analysis of worldwide consumer demand, the key role of independent third-party advertisers, and a detailed cost accounting of the overall business model.

1 Introduction

Much like the legitimate Internet economy, advertising is a major driver for the “underground” criminal economy. As it turns out, however, the culture and operations of the underground bear little resemblance to those found in the legitimate economy. Because of the absence of consumer transaction tracking and revenue reporting, the traditional metrics that drive sales in the legitimate economy (sales revenue, profit margin, cost of goods sold) are not available. Instead, metrics that are highly visible on the Internet but of little value for traditional business purposes are critical. For example, a measure of the volume of traffic that visits a site should be considered a key metric, but the value of actual sales is not.

Driven by competition between criminal organizations, a broad corpus of ground truth data has become available. In particular, in this paper we analyze the content and implications of low-level databases and transactional metadata describing years of activity at the GlavMed, SpamIt and RX-Promotion pharmaceutical affiliate programs. By examining hundreds of thousands of orders, comprising a settled revenue totaling over US$185M, we are able to provide comprehensive documentation on three key aspects of underground advertising activity:

Customers. We provide detailed analysis on the consumer demand for Internet-advertised counterfeit pharmaceuticals, covering customer demographics, product selection (including an examination of drug abuse as a driver), reorder rates and market saturation.

Advertisers. We quantitatively detail the role of third-party affiliate advertisers (both email/forum spammers and SEO-based advertisers), the dynamics of their labor market, their ability to drive revenue and the distribution of their commission income. This analysis includes the operators of many of the best-known botnets including MegaD, Grum, Rustock and Storm, and we document individual advertisers generating over $10M in sales.

Sponsors. We derive an empirical revenue and cost model that estimates that the GlavMed, SpamIt, and RX-Promotion pharmaceutical affiliate programs have generated over US$185M in sales revenue.
Leaked Data Set

SpamIt

GlavMed
### Leaked Data Set

Databases for SpamIt and GlavMed

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Created On</th>
<th>Affiliate</th>
</tr>
</thead>
<tbody>
<tr>
<td>placecanadianyule.com</td>
<td>2009-04-27 20:18:00</td>
<td>master666</td>
</tr>
</tbody>
</table>

~100 tables in each db

52K SpamIt domains

2K GlavMed domains
# Leaked Data Set

Led to over 3 years of sales

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Domain Name</th>
<th>Sale Time</th>
<th>Amount</th>
<th>Referrer</th>
</tr>
</thead>
<tbody>
<tr>
<td>placecanadianyule.com</td>
<td>2009-06-18 05:09:46</td>
<td>149.45</td>
<td><a href="http://groups.google.com/group/300x51242280263">http://groups.google.com/group/300x51242280263</a></td>
<td></td>
</tr>
</tbody>
</table>

**2M transactions for $170M over 3 years**
## Leaked Data Set

### Leaked database

<table>
<thead>
<tr>
<th>Sale Time</th>
<th>Domain</th>
<th>Amount</th>
<th>Referrer</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-06-18 05:09:46</td>
<td>placecanadianyule.com</td>
<td>149.45</td>
<td><a href="http://groups.google.com/group/300x51242280263">http://groups.google.com/group/300x51242280263</a></td>
</tr>
</tbody>
</table>

Sales
Example Referrers

http://bl111w.blu111.mail.live.com/mail/readmessagelight.aspx?action=markasnotjunk&folderid=...

http://mail.yahoo.com/mc/showFolder?fid=Inbox...

http://www.google.com/search?hl=en&amp;q=canadian+viagra&...

http://us.yhs.search.yahoo.com/avg/search?p=buy+prozac&...
98% of SpamIt revenue arose from emails

90% of GlavMed revenue arose from search
Example Referrers

http://bl111w.blu111.mail.live.com/mail/readmessagelight.aspx?action=markasnotjunk&folderid...

http://mail.yahoo.com/mc/showFolder?fid=Inbox...

http://www.google.com/search?hl=en&q=canadian+viagra&...

http://us.yhs.search.yahoo.com/avg/search?p=buy+prozac&...
20% of Hotmail sales, 40% of Yahoo mail sales are from junk folders

There is high demand for counterfeit drugs!
Affiliate Program Overview

Affiliate Program

Commission

Transaction Processing

Affiliate

Shop Site

Advertise

Purchase

Order fulfilment

Customer

Transaction Processing

Commission

Affiliate Program

Shop Site

Advertise

Purchase

Order fulfilment

Customer
Affiliate Program Overview

Affiliates advertise aggressively to get customers

Domain blacklisting disrupts advertising
Blacklist Data: URIBL

Popular email based blacklist

Used for classification of spammed domains

When and how long a domain was blacklisted

Study the effect on SpamIt domains
Attributes of a Good Blacklist

1. **Speed**: Identifies domains fast

2. **Coverage**: Identifies all or most domains

3. **Penalty**: Consequences of blacklisting

4. **Resource Choice**: Cost imposed due to replacing the resource
Speed

How fast is blacklisting?

Time to blacklist is an opportunity to monetize

Results:
- Most domains appeared within 48 hours
- Spammers earned $740K before domains were blacklisted ($21/domain)
Coverage

How many domains does blacklist identify?

Any missed domains will continue to monetize

Results:
- 88% of the 40,000 SpamIt domains blacklisted
- Remaining 12% earned 62% of total revenue ($1900/domain)
Penalty

Does blacklisting have consequences that force domain replacement?

Results:
Penalty

Domains continue to monetize after blacklisting

87% revenue after blacklisting ($147/domain)
Penalty

- Blacklisting used to classify emails into spam
- Due to demand, customers found emails from blacklisted domains continued to monetize
- Spammers replace domains after blacklisting
- Revenue peaks within 2 hours of blacklisting

![Graph showing revenue peaks within 2 hours of blacklisting and spammers replacing domains after blacklisting.](image-url)
Penalty

Revenue for block-access penalty

$21/domain in blocking regime
Resource Choice

What is the cost of replacing a domain?

Observations:
- Domains cost between $0.10 - $10
- Replacing domains can be automated
Summarizing Blacklisting Efficacy

Blacklists only affect the email vector

Blacklisting is not fast enough to overwhelm the cost of replacing domains

Penalty is too low (87% of the revenue after blacklisting)

Blacklists miss some domains that monetize heavily ($1900/domain)
Blacklist Evasion

Depends on how blacklist is constructed

Blacklists constructed using:
- Email honeypots
- Human identification for emails
Blacklist Evasion

3 ways to evade blacklists:

- Use a non-email vector
- Advertise solely to real humans
  - 96% of blacklisted domains, 0.5% non-blacklisted domains appear on honeypot feeds
  - 25% non-blacklisted domains appear in human identified spam
- Hide storefront domains behind redirections
Blacklist Evasion

Intermediate Domain
Identifying Intermediate Domains

Found variety of referrers

<table>
<thead>
<tr>
<th>Sale Time</th>
<th>Domain</th>
<th>Amount</th>
<th>Referrer</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009-06-18 05:09:46</td>
<td>placecanadianyule.com</td>
<td>149.45</td>
<td><a href="http://groups.google.com/group/300x51242280263">http://groups.google.com/group/300x51242280263</a></td>
</tr>
</tbody>
</table>
Identifying Intermediate Domains

Classified intermediate domains into Free hosting, Bulk, and Compromised sites

SpamIt abused cheap, third-party domains

GlavMed abused domains to increase search engine ranks and number of results
Free Hosting Domains
Viagra, Levitra, Cialis and More ED drugs

989 likes - I'm talking about this.

Product/Service:
All about Viagra, Levitra, Cialis and More ED drugs
https://best-online-ed-store.com/?wm=2010480&sid=8030

About - Suggest an Edit

Highlights

Post
Photo / Video
Write something on this Page...

Viagra, Levitra, Cialis and More ED drugs
August 5, 2013

Hot offer for you Viagra, Cialis, Levitra discount up to 60%...

Invite Your Friends to Like This Page
Type a friend's name...

Recent Posts by Others

Joseph Bodon
Buy viagra and cialis online without a prescription; from a leading online pharmacy...

Like, +1, Share, Comment

Neha
Home

Create Page
Free Hosting Domains

Domains which allow anyone to host content

Features:
- Free
- Often not blacklisted at all

Represent 86% of SpamIt revenue from intermediate domains
Bulk Domains

Cheap domains purchased for redirection

Features:
- Inexpensive
- Easily blacklisted
- Useful for SEO

13% of SpamIt revenue, 46% of GlavMed revenue
Ordering Viagra Online --- Price Comparison On A Single ...


Buy VIAGRA at EXTRA LOW PRICES. Wide variety of generic and brand VIAGRA packages. BEST quality generic VIAGRA with 100% satisfaction guaranteed!

Viagra RX Store Online. Purchase Viagra, generic Cialis ...

toodco.ru/hoodco/?goto=http://www.viagrarxstore.com/

The three major erectile dysfunction drugs on the market are Viagra, Cialis and Levitra. Of the three erectile dysfunction drugs, the largest selling product is ...

Generic Viagra


Generic Viagra is used to treat male impotence also known as Erectile Dysfunction. Also, it has been approved by US FDA for treating pulmonary arterial ...

Erectile dysfunction

addurlsite.ru/jump.php?29563

Our most popular products, including Generic Viagra, Generic Cialis, Viagra Soft, Levitra, Cialis Soft, Propecia, Accutane, Soma, Cipro, Prozac, Lexapro, ...

Viagra - Family Practice Notebook

liter.lib.ru/cgi-bin/redirect.cgi?url=www.fpnotobook.com/Urology/...
Compromised Domains

Sites hacked for hosting links to storefronts

Features:
- Useful for SEO
- Takedown is slower

26% of GlavMed revenue
Canadian Online Pharmacy
infosuite.welch.jhmi.edu/WelchCenter/aggregator/sources/3
Canadian Pharmacy - get free pills buying viagra and cialis - get more with us without prescription.

Canadian Pharmacy Cialis : Lowest Prices - Thompson Center
thompsoncenter.missouri.edu/...msoe.p... University of Missouri-Columbia
Generic Pharmacy. We Always Have The Cheapest Offers In Our Online-Drugstore. Canadian Pharmacy Cialis. The Best Pharmacy Online-Offers! Pharmacy ...

Canadian Pharmacy Verification : Lowest Prices
thompsoncenter.missouri.edu/...msoe.p... University of Missouri-Columbia
Generic Pharmacy. High quality pills are only in our drugstore. Canadian Pharmacy Verification. Lowest Price Guaranteed! Our drugshop has everything you...

Canadian Pharmacy Lexapro : Lowest Prices
thompsoncenter.missouri.edu/...msoe.p... University of Missouri-Columbia
Generic Pharmacy. Best Prices On The Web! Canadian Pharmacy Lexapro. High quality pills are only in our drugstore. Best Online Drugstore.

Cialis Canada Pharmacy - Generic Drugs Online
www.osher.ucsf.edu/cialis-c... UCSF Osher Center for Integrative Medicine
Cialis canada pharmacy. Discount Prescription Drugs. Free consultation and discrete overnight shipping is available. Online Pharmacy: 24h online support.

Levitra online canadian pharmacy - The New Paltz Oracle
oracle.newpaltz.edu/levitra-on... State University of New York at New Paltz
Levitra online canadian pharmacy. 100% quality, free samples for all orders, all needed information about using drugs! 24/7 free consultations.

Star Drugstore: Canadian pharmacy cialis paypal best ...
www.tulane.edu/.../home.php?... Canadian pharmacy cialis paypal. Viagra is a popular erectile dysfunction treatment pills, be sure buying only quality pills with us.
Intermediate Domain Abuse

Spammers abuse wide variety of domains to:

- Evade detection and blacklisting
- Increase traffic at minimal cost

Spammers are flexible at switching strategies
Temporal Domain Abuse

Spammers switch from free hosting to bulk domain abuse
Temporal Domain Abuse

GlavMed

Revenue ($) vs. Date (2008-2010)

- Paid traffic
- Search
- Other
- Compromised
- Free hosting
- Bulk
Summary

Blacklisting currently unable to undermine spamming enterprise

Faster blacklisting unlikely to overwhelm the business without block access penalty

Coverage is important to improve but difficult

- Agile spammers
- Many evasion techniques exist