WHITE PAPER

AFFILIATE PROGRAMS: LEGITIMATE BUSINESS OR FUELING CYBERCRIME?

INTRODUCTION

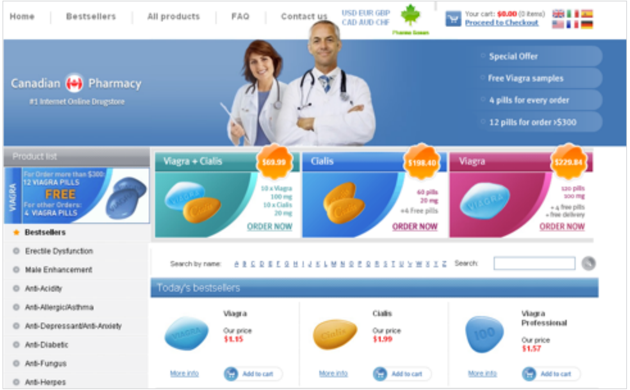
We have all seen the progress that security vendors and law enforcement have made in the fight against spammers and cybercrime. Action such as a Botnet take-down, either technically or the physical arrest of a Botnet operator which had the same overall effect, or the arrest of a cybercrime gang. All this has been progress but you can help but think that we are targeting the foot soldiers, the cannon fodder of cybercrime where as it might be more successful to go after some bigger fish or a more common denominator.

Affiliate programs are the financial middle men between vendors looking to market their products and marketing companies looking to advertise and market products. Legitimate affiliate programs do exist, such as those offered by companies like Amazon and then there are illegitimate affiliate programs offered by companies such as SpamIt. Wikipedia defines affiliate programs as:

> “Affiliate marketing is a marketing practice in which a business *rewards one or more affiliates for each visitor or customer brought about by the affiliate’s own marketing efforts. Examples include rewards sites, where users are rewarded with cash or gifts for the completion of an offer, and the referral of others to the site. The industry has four core players: the merchant (also known as ‘retailer’ or ‘brand’), the network, the publisher (also known as ‘the affiliate’), and the customer.”*

AN EXAMPLE OF AN AFFILIATE PROGRAM

A perfect example of an affiliate program is how botnet operators typically get paid for the spam they send. First, you have the merchant who wants to sell their products; a company like Canadian Pharmacy is an example. Then you have the publisher or spammer in this example. The network connecting these two parties is the affiliate program. In the not too distant past, it was thought to be an organization called SpamIt, and then you had the customers, or spam victims in this case.



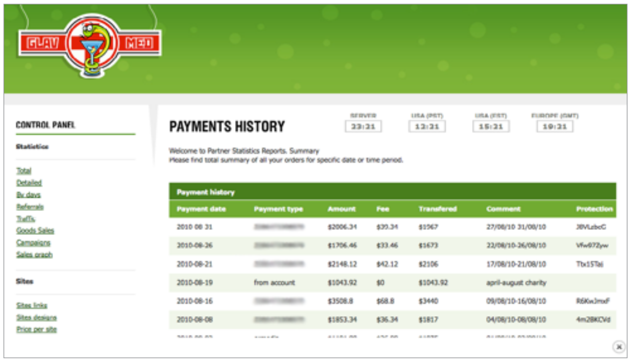
Canadian Pharmacy Website

So when Canadian Pharmacy wants to sell their products, they contact an affiliate program, SpamIt. They provide Spamit with email templates of what they would like marketed. SpamIt then provides these templates to some spammers they do business with, often also including the lists of email addresses to be spammed. Each spammer is also allocated a referral code to insert into the URL link in their spam message. When a spam victim, or customer clicks on a URL link in the spam message and purchases a product from the Merchant, Canadian Pharmacy knows which spammer to credit the sale to. The merchants typically pay a percentage of the sale to the affiliate program to pass onto the spammer, with the affiliate program of course taking a cut from this payment.

HOW MUCH MONEY DO THEY MAKE?

In the affiliate program described above, over US $150 million in sales were generated between May 2007 and June 2010 according to data provided by Krebs on Security: http://krebsonsecurity.com/2011/02/spamit-glavmed-pharmacy-networks-exposed/

The spammers could expect to earn up to 40% on any sales they made through their spam, which would add up to anywhere between US $5,000 to US $50,000 per month.



CONTROL PANEL

Statistics

- Total
- Detailed
- By days
- Referrals
- Traffic
- Goods Sales
- Campaigns
- Sales graph

Sites

- Sites links
- Sites designs
- Price per site

PAYMENTS HISTORY

SERVER	USA (PST)	USA (EST)	EUROPE (GMT)
23:21	13:21	15:21	19:21

Welcome to Partner Statistics Reports. Summary
Please find total summary of all your orders for specific date or time period.

Payment history

Payment date	Payment type	Amount	Fee	Transfered	Comment	Protection
2010 08 31	[redacted]	$2006.34	$39.34	$1967	27/08/10 31/08/10	JBVLzbcG
2010-08-26	[redacted]	$1706.46	$33.46	$1673	22/08/10-26/08/10	Vfw072yw
2010-08-21	[redacted]	$2148.12	$42.12	$2106	17/08/10-21/08/10	Tbx15Tai
2010-08-19	from account	$1043.92	$0	$1043.92	april-august charity	
2010-08-16	[redacted]	$3508.8	$68.8	$3440	09/08/10-16/08/10	R6KwJmxF
2010-08-08	[redacted]	$1853.34	$36.34	$1817	04/08/10-08/08/10	4m2BKCVd

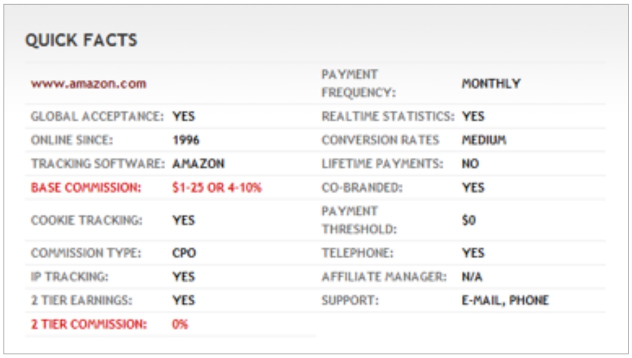
Publisher Account Information from a Glavmed Spammer Partner
Courtesy of Krebs on Security http://krebsonsecurity.com/2011/02/spamit-glavmed-pharmacy-networks-exposed/

Another example of shady affiliate programs are Pay-per-Install programs. In this scenario, a publisher is paid by the number of successful installations of whatever software is distributed. The common choice in PPI payouts are the fake anti-virus applications. Yabucks was a well-known affiliate program specializing in PPI campaigns. Below you can see what a publisher could expect to earn based by the location of the infected machine:

Country	Rate per 1,000 installs $US
USA	170
Canada	120
United Kingdom	110
Australia, Europe	50

Yabucks PPI Payments by Location of Infected Machine

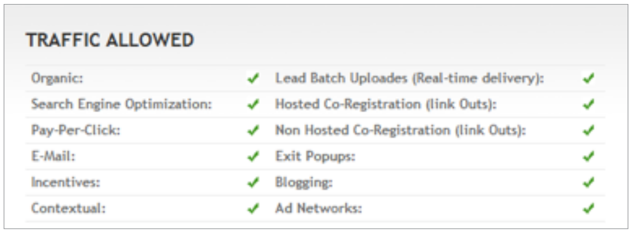
From a legitimate viewpoint, below are the details from the Amazon Books affiliate program:



QUICK FACTS

www.amazon.com		PAYMENT FREQUENCY:	MONTHLY
GLOBAL ACCEPTANCE:	YES	REALTIME STATISTICS:	YES
ONLINE SINCE:	1996	CONVERSION RATES	MEDIUM
TRACKING SOFTWARE:	AMAZON	LIFETIME PAYMENTS:	NO
BASE COMMISSION:	$1-25 OR 4-10%	CO-BRANDED:	YES
COOKIE TRACKING:	YES	PAYMENT THRESHOLD:	$0
COMMISSION TYPE:	CPO	TELEPHONE:	YES
IP TRACKING:	YES	AFFILIATE MANAGER:	N/A
2 TIER EARNINGS:	YES	SUPPORT:	E-MAIL, PHONE
2 TIER COMMISSION:	0%		

Table continues next column

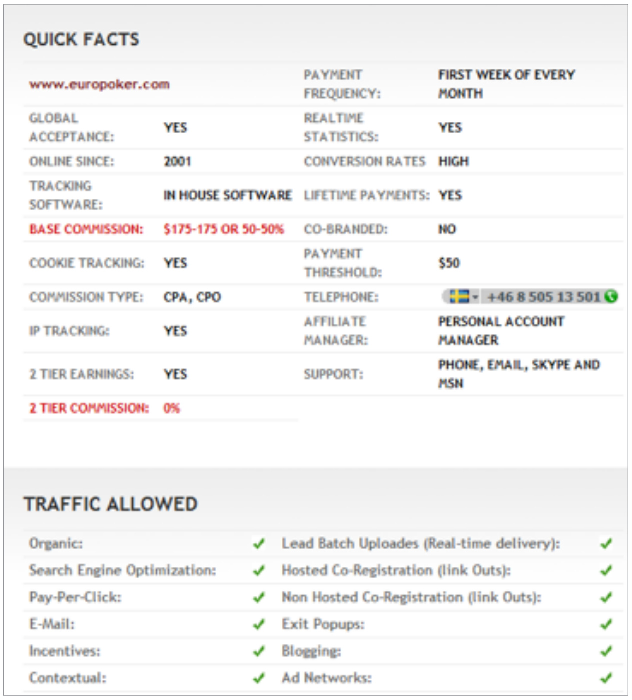


TRAFFIC ALLOWED

Organic:	✓	Lead Batch Uploades (Real-time delivery):	✓
Search Engine Optimization:	✓	Hosted Co-Registration (link Outs):	✓
Pay-Per-Click:	✓	Non Hosted Co-Registration (link Outs):	✓
E-Mail:	✓	Exit Popups:	✓
Incentives:	✓	Blogging:	✓
Contextual:	✓	Ad Networks:	✓

Note the type of commission, CPO or Cost-per-Order meaning the publisher or company doing the actual marketing gets paid by how many orders they help to generate—in this case up to $25 or 10% of the order.

Another very common category of legitimate affiliate programs are gambling sites. One example is Europoker:



QUICK FACTS

www.europoker.com		PAYMENT FREQUENCY:	FIRST WEEK OF EVERY MONTH
GLOBAL ACCEPTANCE:	YES	REALTIME STATISTICS:	YES
ONLINE SINCE:	2001	CONVERSION RATES	HIGH
TRACKING SOFTWARE:	IN HOUSE SOFTWARE	LIFETIME PAYMENTS:	YES
BASE COMMISSION:	$175-175 OR 50-50%	CO-BRANDED:	NO
COOKIE TRACKING:	YES	PAYMENT THRESHOLD:	$50
COMMISSION TYPE:	CPA, CPO	TELEPHONE:	+46 8 505 13 501
IP TRACKING:	YES	AFFILIATE MANAGER:	PERSONAL ACCOUNT MANAGER
2 TIER EARNINGS:	YES	SUPPORT:	PHONE, EMAIL, SKYPE AND MSN
2 TIER COMMISSION:	0%		

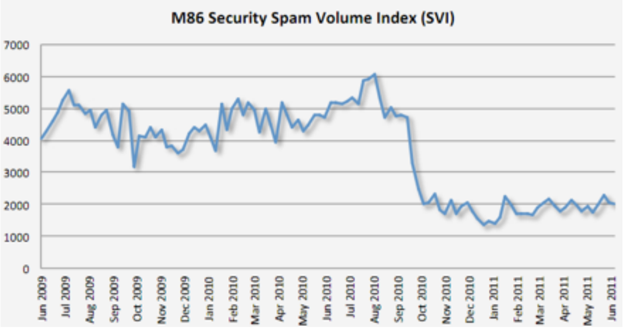
TRAFFIC ALLOWED

Organic:	✓	Lead Batch Uploades (Real-time delivery):	✓
Search Engine Optimization:	✓	Hosted Co-Registration (link Outs):	✓
Pay-Per-Click:	✓	Non Hosted Co-Registration (link Outs):	✓
E-Mail:	✓	Exit Popups:	✓
Incentives:	✓	Blogging:	✓
Contextual:	✓	Ad Networks:	✓

Note the two types of commissions: Cost-per-Order and Cost-per-Action. CPA refers to payment made to the publisher when a user takes some action on a site such as signing up for an account or adding funds to an existing account.

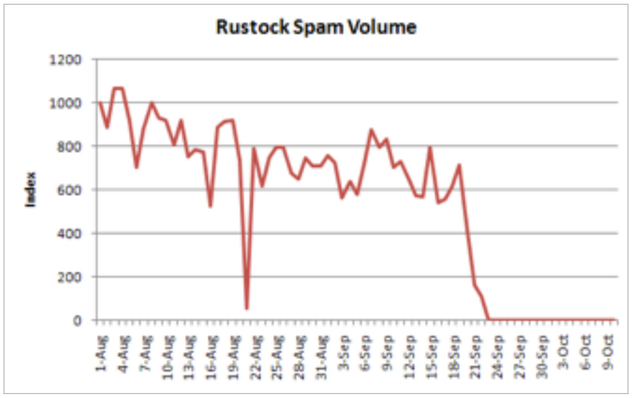
THE EFFECT OF ADDRESSING THE AFFILIATE PROGRAMS

Any action in the fight against cybercrime is worthwhile, but we always have to be mindful of how effective each action is. Is there a way of being more efficient? What we are suggesting here is going after the money, in this case, the affiliate programs. The best example of how successful this could be would be looking at the drop in spam volume when SpamIt unexpectedly closed down their business. In the graph below, you can see this drop in spam volume occurred overnight.



Spam Volume Index 2009–2011

As we know, the vast majority of spam today is sent by botnets. One of the most prolific spambots has been Rustock. We can see this drop in spam activity to an even greater degree by looking closely at Rustock spam volume:

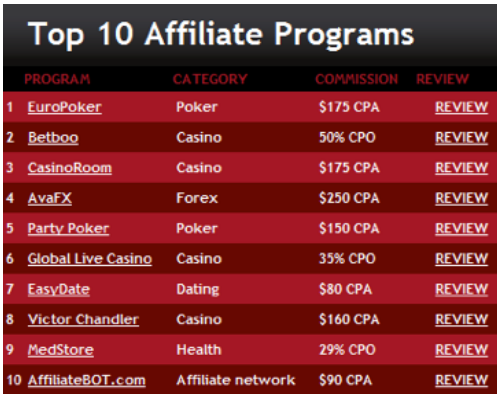


Drop in Spam from Rustock Botnet After Spamit Closure

Previously, we have seen temporary impacts to overall spam volume when individual botnets were taken down. These botnets would recover slowly or another botnet would rise up to take its place. Until now, this has not happened with Spam volumes still at two-thirds what they were prior to SpamIt closing. Since our records began the SpamIt closure has had the biggest and longest lasting effect on Spam volumes.

DETERMINING THE DIFFERENCE BETWEEN LEGITIMATE AND ILLEGITIMATE AFFILIATE PROGRAMS

This is can be pretty difficult; it typically comes down to the products or services being offered. For example, these are the top 10 affiliate programs from affiliatetips.com:



Top 10 Affiliate Programs

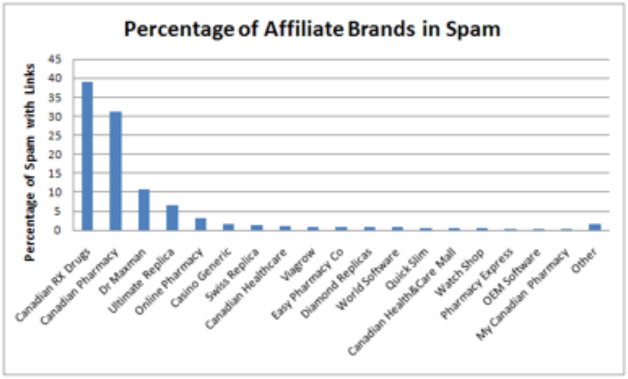
	PROGRAM	CATEGORY	COMMISSION	REVIEW
1	EuroPoker	Poker	$175 CPA	REVIEW
2	Betboo	Casino	50% CPO	REVIEW
3	CasinoRoom	Casino	$175 CPA	REVIEW
4	AvaFX	Forex	$250 CPA	REVIEW
5	Party Poker	Poker	$150 CPA	REVIEW
6	Global Live Casino	Casino	35% CPO	REVIEW
7	EasyDate	Dating	$80 CPA	REVIEW
8	Victor Chandler	Casino	$160 CPA	REVIEW
9	MedStore	Health	29% CPO	REVIEW
10	AffiliateBOT.com	Affiliate network	$90 CPA	REVIEW

All of these affiliate categories meaning Casino, Dating etc., and not the actual companies) have also been marketed through spam. But with the case of rogue anti-virus applications that might be a little easier to recognize, replica goods such as watches and handbags, deals too good to be true should invite suspicion.

The next step would be to investigate the method of payments, from where are they coming and using which method? SpamIt used Webmoney, a virtual currency popular in Russia that is similar to PayPal, except that transactions are largely irreversible. Other affiliate programs used ePassporte, a virtual currency that closed its doors in September 2010 amid allegations of fraud and misappropriation of funds.

The final step would be to investigate the company themselves, how long in business, reputation, geographic location and so on.

Below is a graph of Affiliate programs we have identified in spam messages from research completed in May 2010:



As you can see, all of this is pretty subjective, but successfully identifying illegitimate affiliate programs is important because closing these down can have a much bigger and longer lasting impact on Cybercrime and spam levels, than individual Botnet take-downs.

VERSION 07.13.11

HOW TO GO AFTER THE AFFILIATE PROGRAMS

This is the crucial piece. When we have identified and confirmed that a particular affiliate program is illegitimate, what can you really do about it? Lessons can be learned here from the SpamIt closure; there has been much conjecture about what caused them to suddenly close their doors, literally overnight, but a big part is thought to be down to embarrassment. M86 Security and other organizations were naming and shaming them in regular blog posts. The Krebs on Security blog as well as several publications also named them on a regular basis. Perhaps the constant attention became to much?

This same method can also be used with the business partners an affiliate program has to use, like banks and other financial organizations that they use, advertising networks, the merchants that are their customers, etc. Even if these organizations are illegitimate as well; turning up the heat on the affiliate program they use will undoubtedly make them reconsider this arrangement.

Of course, we should not forget about the actions that security researchers and law enforcement can take. We have to do our part by remaining vigilant and gathering the facts and statistics, and passing them onto the proper parties that might be able to do something about it.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations.
Simply contact us or visit:
www.m86security.com/downloads.

ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 25,000 customers and 26 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Irvine, California with international headquarters in London and development centers in California, Israel, and New Zealand. For more information about M86 Security, please visit: **www.m86security.com**.

M86 SECURITY®

Corporate Headquarters
8845 Irvine Center Drive
Irvine, CA 92618
United States

Phone: +1 (949) 932-1000
Fax: +1 (949) 932-1086

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom

Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Suite 3, Level 7 100 Walker St.
North Sydney NSW 2060
Australia

Phone: +61 (0)2 9466 5800
Fax: +61 (0)2 9466 5899