THE PARTNERKA – WHAT IS IT, AND WHY SHOULD YOU CARE?

Dmitry Samosseiko
SophosLabs Canada, Sophos Inc., 580 Granville Street, Vancouver, BC, V6C 1W6 Canada

Email dmitry.samosseiko@sophos.com

ABSTRACT

Scareware, 'Canadian Pharmacy' spam, adult sites, comment spam on forums and blogs – we've seen these plaguing our web and email experience over the past few years. What links them together? What makes them grow in volume and complexity? Who is behind them? What business model drives their profits to millions of dollars annually?

The answer is hundreds of well-organized affiliate networks. They're known as 'partnerka' in Russia, where they form a booming business, yet exist in other places as well. Thousands of affiliates, each calling themselves a 'webmaster', work day and night to drive as much user traffic to their partners' stores as possible. The stores sell fake watches, fake anti-virus software, fake pills and fake love – the webmasters get their commission, making thousands of dollars per day.

This presentation will expose their economic model, as well as describe the most popular Russian 'partnerka' networks and their relation to spam and malware. It will reveal some 'insider' statistics and information, show the tools used for 'black SEO' (search engine optimizations), and explain its terminology and techniques.

We'll also discuss how traditional email spam has evolved into a complex web-based industry, creating new challenges for law enforcement, user education and for security labs.

INTRODUCTION

The first serious book about spam and spammers that I read was *Spam Kings* by Brian S. McWilliams (2004). The 'pioneers' of the email spam industry pictured in the book, like the ex-Nazi Davis Wolfgang Hawke, ran it as a small family business. Relying on nothing more than help from their relatives, they handled the entire process chain themselves: harvesting email addresses, authoring message content, sending bulk email, processing orders, rapidly switching their Internet service providers and, at a later stage, running from the FBI or being jailed.

Back in the early years there were a handful of 'spam kings' and they didn't have much to fear. Thanks to *The Spamhaus Project* we knew their names, addresses, what cars they drove and their relative position in the top spammers list.

Since then, many countries have established a variety of anti-spam laws governing the use of email communication and marketing, including the US, Europe, Australia and Canada. The legislation was not expected to eliminate spam and make the spammers extinct, but it did criminalize it, made it a punishable offence and as a result a much riskier endeavour.

So, the second generation spammers had to become a more organized and secretive group, forming professional spam outfits or collaborating online, where 'bot herders' could find their 'sponsors'.

But the peak of their evolution was the adoption of affiliate marketing methods in order to distribute responsibility for different spam tasks and to increase the army of 'advertisers'. Amongst the first spam gangs formed this way was the affiliate network Genbucks/SanCash, founded by the notorious spammer Shane Atkinson. It later ceased to exist but became a 'role model' for hundreds of new networks.

The affiliate marketing models work well for products with large profit margins. Generic drugs produced without a licence, pornography, pirated software, casinos, dating sites… the list goes on. These are the topics we commonly see in email and web spam, but not everyone knows that each theme is backed by numerous affiliate organizations with thousands of advertisers. Another fact, known to security industry researchers, is that the majority of the most powerful and controversial affiliate networks are based in Russia.

As an ethnic Russian and a security researcher, I didn't want to miss an opportunity to look into the not-so-well-hidden world of Russian affiliate partner networks, commonly referred to in slang as partnerka.

But let's first look at how the whole concept of spamming has changed.

'WEB IS THE NEW EMAIL'

Over the years anti-spam filters have become a de facto standard for any email service and are now providing efficient protection for almost every inbox. The filters continue to impact spammers' profits, forcing them to shift to new (yet still aggressive) advertisement techniques.

During the same time period, the emergence of Web 2.0 technologies – the blogosphere, social networks – has changed the way people communicate and find information online. It made the web a very attractive and powerful advertising platform, not only to legitimate businesses but also to those who sell generic drugs and counterfeit luxury items.

This isn't surprising, given that a person searching for cheap drugs online is a significantly more valuable target to shady online pharmacies than millions of email spam recipients who've never asked for it.

Another appeal factor is that web traffic today does not have a similar level of protection on the legal and the technological sides. There are no laws today that could be applied to spam on blogs or forums. And while various web filters do exist, they do not offer the same level of efficiency or adoption as their email counterparts. This is especially true for home users who are the main target.

This explains why topical web traffic is becoming the main focus of affiliate networks of a certain kind. It gives them a safe legal framework to work within and benefits the most from the scalable model that affiliate marketing offers. Unlike email spam, web marketing has a significantly lower barrier to entry for a new member and offers an almost linear dependency between profits and the number of active 'partners'.

Just as Web 2.0 is about user-generated content, today's web and email spam (Spam 2.0?) is generated by a massive number of affiliates who direct traffic to a partner site to get their share of the revenue.

This explains why the number 1 position on the *Spamhaus* Top 10 spammers list, previously held by the notorious Russian

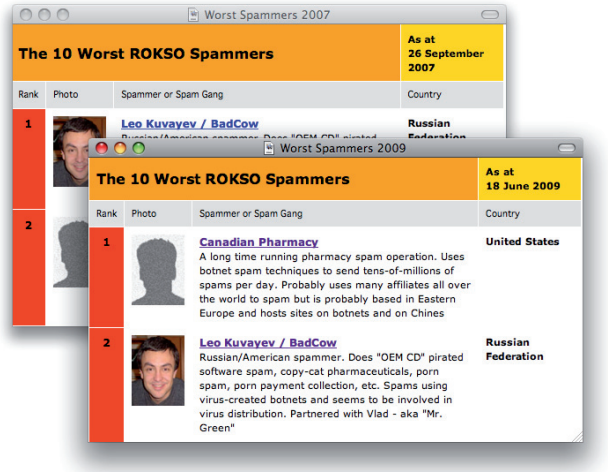

Figure 1: The 'Canadian Pharmacy' group now holds the number one position in the Spamhaus Top 10 spammers list.

spammer Leo Kuvayev, is now taken by the ambiguous 'Canadian Pharmacy' group.

It's important to mention, however, that there are literally hundreds of affiliate networks in Russia and around the world that promote legitimate products in relatively benign ways. The focus of this research is on the sites that push products that are deemed illegal in many jurisdictions and those that endorse unethical or straight-up criminal promotion techniques amongst their member base. But first, let's look at the taxonomy and common characteristics.

At the top level these shady businesses can be distinguished by the type of product or service they promote and sell. The most popular kinds include:

- Online pharmacies selling generic versions of popular drugs.
- Networks promoting 'scareware', a.k.a. 'rogue anti-virus' products.
- Counterfeit luxury products such as fake *Rolex* watches.
- Casinos.
- Adult sites.
- Dating services.
- Affiliate traffic generated via IFRAME insertions.

The majority of networks require an invitation from an existing member in order to join. This is often a good indicator of a business that supports unethical promotion practices. Among the most risky are those that openly allow spam traffic or sell rogue software. These partnerkas are usually closed to the general public (referred to as 'private') and require proof of traffic volumes and a certain reputation to be let in. Their websites often reveal nothing but a form to log in.

Another good sign of a dodgy affiliate business is a complete lack of transparency with respect to business ownership. The only contact information usually provided is a set of ICQ numbers. The portal administrators usually go by their nicknames and never reveal their real names on support forums. The banner ads that invite people to join the partnerships are usually placed on forums dedicated to spam, hacking, black SEO (search engine optimizations) and other unethical or illegal practices.

All partnerkas are in strong competition with each other. Allegiance is earned through more generous commission rates, shorter 'hold' periods, support for a wider range of payment methods (ePass, WebMoney, Fethard Finance, wire transfers), higher quality promotional material, better support, etc.

Many organize expensive parties for their members, send generous gifts for holidays, run lotteries where a top producer wins a luxury car, and the list goes on.

In some cases, the war between different partnerkas turns ugly, where one portal may get DDoS'ed by a competing gang.

TRAFFIC GENERATION TECHNIQUES

Affiliate marketing is all about driving quality traffic to your 'sponsor'. So, how does one go about generating it?

The 'white hat' Internet marketing involves running ads on quality websites or blogs which attract visitors by their useful content or functionality. This form of advertisement is rarely the case when we're talking about Russian pharma- or codec-affiliates.

Crossing the ethical boundary pays well. The most common methods of traffic generation for these sites include various forms of spam, black-hat SEO, malware and combinations of the above.

As noted above, email spam has become less popular amongst affiliates due to the high risk and steep entry barrier. This has been acknowledged by the affiliates themselves on SEO-related forums. But given that we see no shortage in the supply of 'Canadian Pharmacy' or 'fake Rolex' spam, it's not going to go away any time soon. It's just being carried out by a smaller 'elite' group of affiliates.

Another example of traffic-generating malware is a variety of so-called DNS Changer trojans that can place promoted sites at the top of web search results. This is achieved by redirecting DNS records for Google.com and other popular search engines to a lookalike site controlled by the affiliate. The replica site will proxy search results from the real one with the necessary modifications made to the search results.

Another example is the TDSS family which loads a variety of fake anti-virus software from partner sites. I suspect that the 'TDS' string seen in filenames (i.e. TDSServ.sys) of this malware means nothing more than 'Traffic Directing System' – a common term in the SEO world.

When it comes to 'pharma', adult or 'codec' partnerka, the techniques most commonly used are known as 'black-hat SEO'.

The main difference between white and black SEO is that the former implies only using the methods approved by search vendors, like editing content to increase its relevance to certain search keywords.

Black SEO, on the other hand, relies on techniques like spamdexing, 'doorway' pages and spam messages posted on blogs and forums.

The most popular is the creation of 'doorway' sites. These sites host content specifically created and optimized for a particular topic and search phrases. It would link to a

promoted site using a URL containing affiliate ID. When a search engine indexes a 'doorway' with a high density of related keywords it's likely to increase the page rank of the site referred to by the page, giving it a higher position in search results.

The common black SEO workflow involves:

1. Mining of *Google Trends* data for most popular search topics, whether it's 'britney spears' or 'death of david carradine'.
2. Generating content related to popular search phrases and linking it to a promotional site.
3. Uploading content as a blog or forum post, *Wikipedia* article or as a site on a 'throwaway' domain.

Most of the steps in this process can be automated by various SEO software tools.

For example, the program 'John22' will automatically generate HTML content for dozens of unique and meaningful content pages per second, will link them together, upload them via FTP and notify *Google* about the new site. The authors claim that even humans have difficulty recognizing that the content was generated automatically and that it's impossible for a search engine to tell the difference.

Other tools focus on automated parsing of search trend data, generation of unique content from *Wikipedia* articles and production of complete online forum sites with fictional user communities and conversations.

A special area of black SEO tools are the various spamware tools for blogs, forums and guestbooks, the most popular of which are A-Poster and Xrumer. Their functionality is similar to email spam-sending tools of the recent past, like SendSafe or DarkMailer.

A-Poster specializes in spamming guestbooks, while Xrumer works on forums. The latter provides support for automated forum registrations which often require a valid email address and a confirmation. The entire process is fully automated and includes CAPTCHA recognition to generate hundreds of free email accounts.

ZennoPoster is yet another suite of tools that is able to generate accounts on any webmail site, social networks, blogs, free web-hosting providers, etc. It can send SMS messages, parse search results, place spam on forums and guestbooks and perhaps brew a coffee, though this feature wasn't advertised. And all this treasure goes for a mere 289 euros.

If this all sounds too complex, the web traffic could simply be bought from a link exchange store and directed to your sponsor. The trick is to choose a partnerka with a high conversion rate to ensure that generated revenue will be greater than the cost of the traffic itself.

Now, let's look at some of the most prolific affiliate business types.

PHARMA-MASTERS

The online pharmacy is one of the most popular kinds of 'affiliate promotions'. The oldest and biggest partnerka in the Russian pharma-business is GlavMed, which can be translated as 'MedHeadquarters'.

Figure 2 shows how the GlavMed website illustrates the partnership model.

Figure 2: How GlavMed illustrates its partnership model.

Figure 3: GlavMed.

This partnerka is open to the public but requires an invitation from another network member. Its main brand is the notorious 'Canadian Pharmacy', which is all too familiar to everyone through massive email spam campaigns that seem never to end. This spam is tied to a sister entity of GlavMed, called SpamIt (spamit.com), which is a closed private network of email spam affiliates that has proven hard to infiltrate.

The members of SpamIt are allegedly the group behind the Storm, Waledec and potentially Conficker botnets, responsible for email distribution and fast-flux hosting of the spam websites.

GlavMed, on the other hand, proclaims a strong anti-spam policy focusing on 'legal' SEO traffic generation. Searching for GlavMed's support phone number (+1 (210) 888 9089) reveals over 120,000 online pharmacy sites selling generic drugs (Figure 4).

We discovered, however, that the PHP-based e-commerce backend (SE2) available for download from GlavMed's user

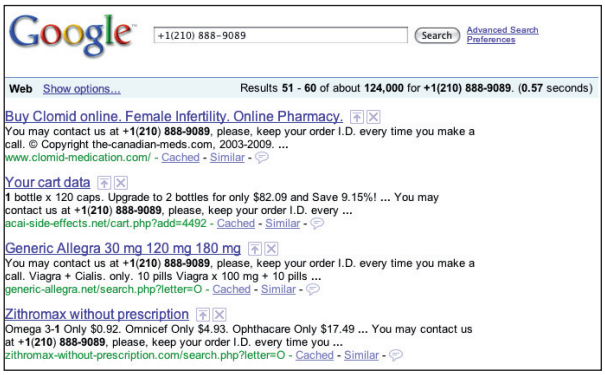

Figure 4: Searching for GlavMed's support number reveals over 120,000 online pharmacy sites.

area is exactly what powers the 'Canadian Pharmacy' sites advertised in spam.

Just like any other partnerka, GlavMed starts with a public portal, the main part of which is the members' area with statistics on store visits, purchases and commission earned. Many webmasters claim to be addicted to these stats pages, watching intently how the traffic they generate converts to payments.

Every affiliate has an option to download two versions of GlavMed's e-commerce software to deploy on their own domains or simply to direct traffic to a set list of domains owned by GlavMed. The former provides more flexibility for customization and SEO optimizations.

Each store deployment contains a backdoor interface that allows GlavMed's order processing system to collect hit statistics and purchase orders.

Another core feature of the main site is the forum where affiliates discuss issues, share ideas and get attentive and high quality support from the partnerka owners.

GlavMed advertises a 40% commission fee on each sale. Assuming the cost of an average purchase is around $200, even a couple of purchases per day become a good source of income.

During our research we came across a log file of purchases made on 'Canadian Pharmacy' websites advertised in email spam. This data revealed over 20 drug purchases per day per spam campaign, which can add up to $1,600 paid in commission fees per day. **Correction:** *there were in fact 200 purchases per day average (not 20), which could lead up to $16,000 in payments (not $1,600).*

While GlavMed is one of the oldest and clearly the most popular pharma businesses, there are legion others. Stimul-cash.com, Rx-partners, Rxcash.biz, Evapharmacy, Rx-Signup.com and DrugRevenue names just a few.

Most of them focus exclusively on web promotion methods, while a small portion still unofficially support traffic generated through email spam. According to messages posted on relevant forums, GlavMed and Evapharmacy are the most spam-friendly sponsors in the world of 'pharma'.

CODEC- AND SOFT-PARTNERKA

Over the last two to three years we've witnessed an emergence of a new Internet threat called scareware, which quickly became one of the most prevalent kinds of malware.

This threat exploits the increasing fear among users of computer malware and relies on various social engineering tricks or software exploits to install a fake security product. The rogue software is both annoying and hard to get rid of, unless you're willing to pay $30–$50 for the fake product or a similar amount of money to buy real defence. This shouldn't be big news to anyone these days, even though some people still fall victim to it.

What is not common knowledge, though, is that this Internet threat is predominantly driven by Russian partnerka networks.

These 'sponsors' are often called 'pay-per-install-', 'soft-' or 'codec-' partnerka. The latter is related to the most commonly used social engineering technique that fools people into installing a video codec or a *Flash* player update to watch video content. The commission paid to affiliates is usually based on the number of 'loads' (installations) achieved.

For the soft-partnerka networks, also known as antispyware-partnerka, the revenue sharing is based on actual sales of fake software.

In addition to actual software, each 'sponsor' also provides promo material, which is usually a set of HTML designs and scripts that entice users to click and install. The most popular was the different variations of 'PornTube' – a youtube.com lookalike offering adult videos for free.

Due to the openly criminal nature of these affiliate groups, the codec-partnerkas do not last very long. Most of them are exclusively private and require affiliates to have a certain reputation in the SEO world before they can be admitted as members. But there are some, like Buckster.ru, that are more relaxed about new registrations.

Buckster advertises itself as a partnerka for 'garbage' traffic. Its two core 'brands' are WinXdefender and VirusDoctor – both perfect examples of rogue AV software.

Once registered, you can log into an admin interface, showing you the URLs to advertise and your current statistics. As you can see in the screenshot in Figure 5, the author of this paper, though tempted, did not generate any traffic for his financial gain.

Having this sort of access can often expose useful information to a security researcher. The main benefits are the fresh links to promotional sites and the software binary itself. Both could be used to maintain a high level of detection for this threat and can drive development of a broader protection layer. In this particular example, the DNS network hosting the TDS domain (Traffic Direct System) contains a number of other fake AV-related websites that could be blocked as soon as they get registered.

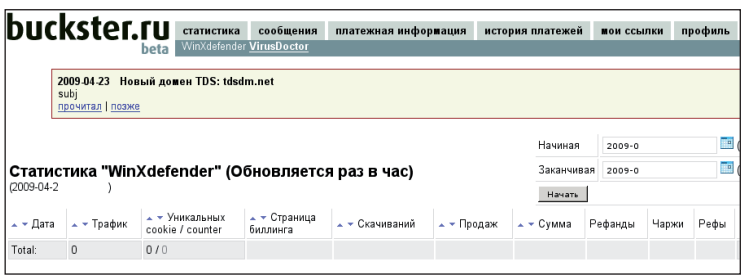

Figure 5: Buckster admin interface.

Search Results for IP: **91.210.57.135**

Nameservers matching query:

Nameserver	IP	First Seen	Last Modified
ns2.rapidantivir09.com	91.210.57.135	2009-04-24 06:15:08	2009-04-24 06:15:08
ns1.rapidantivir09.com	91.210.57.135	2009-04-24 06:14:21	2009-04-24 06:14:21
ns2.tdsdm.net	91.210.57.135	2009-04-24 01:16:42	2009-04-24 01:16:42
ns1.tdsdm.net	91.210.57.135	2009-04-24 01:16:10	2009-04-24 01:16:10
ns2.eccprocessing.net	91.210.57.135	2009-04-10 01:10:21	2009-04-10 01:10:21
ns1.eccprocessing.net	91.210.57.135	2009-04-10 01:03:38	2009-04-10 01:10:11
ns2.multifeeddomain.com	91.210.57.135	2009-03-24 06:00:29	2009-03-24 06:00:29
ns1.multifeeddomain.com	91.210.57.135	2009-03-24 05:48:50	2009-03-24 05:59:02
ns2.softcollector.com	91.210.57.135	2009-03-13 05:41:42	2009-03-13 05:41:42
ns2.vistaantivirus2009.com	91.210.57.135	2009-03-06 05:49:47	2009-03-07 05:38:56
ns1.vistaantivirus2009.com	91.210.57.135	2009-03-06 05:48:24	2009-03-07 05:37:52
ns2.test112233.com	91.210.57.135	2009-03-05 05:51:58	2009-03-05 05:51:58
ns1.test112233.com	91.210.57.135	2009-03-05 05:50:32	2009-03-05 05:50:32
ns2.xsoftstore.com	91.210.57.135	2008-12-25 04:30:19	2009-02-26 05:36:16
ns2.isoftmart.com	91.210.57.135	2008-12-25 04:29:17	2009-02-26 05:35:51
ns1.xsoftstore.com	91.210.57.135	2008-12-25 04:28:18	2009-02-26 05:35:32
ns1.isoftmart.com	91.210.57.135	2008-12-25 03:30:12	2009-02-26 05:34:58
ns2.nordelica.com	91.210.57.135	2008-09-25 05:48:29	2009-03-05 05:51:40
ns2.n-softstore.com	91.210.57.135	2008-09-25 05:48:27	2009-02-26 05:35:57
ns1.nordelica.com	91.210.57.135	2008-09-25 05:44:20	2009-03-05 05:49:52
ns1.n-softstore.com	91.210.57.135	2008-09-25 05:42:31	2009-02-26 05:35:13

Figure 6: The DNS network hosting the TDS domain contains a number of other fake AV-related websites.

Another very popular – but a bit more private – codec-partnerka is RefreshStats. Despite its efforts to stay private we were able to take a peek at its admin interface. One of the affiliates was careless enough to upload a screenshot of their desktop to one of his 'PornTube' sites (Figure 7). The screenshot offers a picture of the admin portal with this affiliate's earnings and hit statistics ($6,456 for the month of August 2008).

Mac users are not immune to the scareware threat. In fact, there are 'codec-partnerka' dedicated to the sale and promotion of fake Mac software. One of the recent examples is Mac-codec.com. At the time of writing this article, the site is no longer available, but just a few months ago it was offering $0.43 for each install and offered various promo materials in the form of MacOS 'video players'.

Often enough, some interesting information can be obtained directly from the partnerka home pages, without needing to register.

http://refreshstats.com/stats.php

02-08-2008	23855	21475	504	1:43	$158.13	$0	$158.13
03-08-2008	25474	22360	425	1:53	$123.7	$0	$123.7
04-08-2008	59883	50612	937	1:54	$280.84	$0	$280.84
05-08-2008	40602	36039	771	1:47	$245.3	$0	$245.3
06-08-2008	156	130	10	1:13	$2.62	$0	$2.62
07-08-2008	22218	18582	343	1:54	$88.16	$0	$88.16
08-08-2008	57061	48085	1027	1:47	$318.21	$0	$318.21
09-08-2008	49897	43686	975	1:45	$308.94	$0	$308.94
10-08-2008	41313	38096	860	1:44	$287.31	$0	$287.31
11-08-2008	34476	31833	778	1:41	$275.3	$0	$275.3
12-08-2008	33568	31282	735	1:43	$255.66	$0	$255.66
13-08-2008	36092	33202	756	1:44	$249.03	$0	$249.03
14-08-2008	39282	35610	584	1:61	$194.94	$0	$194.94
15-08-2008	36032	33324	763	1:44	$251.41	$0	$251.41
16-08-2008	42017	37371	809	1:46	$260.15	$0	$260.15
17-08-2008	63588	51187	993	1:52	$283.1	$0	$283.1
18-08-2008	46827	40118	853	1:47	$255.98	$0	$255.98
19-08-2008	46566	38893	709	1:49	$256.56	$0	$256.56
20-08-2008	40531	32552	658	1:49	$211.56	$0	$211.56
21-08-2008	50791	40264	840	1:48	$261.41	$0	$261.41
22-08-2008	52599	42578	891	1:48	$276.99	$0	$276.99
23-08-2008	51627	41067	853	1:48	$283.71	$0	$283.71
24-08-2008	63865	48372	952	1:51	$298.34	$0	$298.34
25-08-2008	27687	22768	474	1:48	$151.57	$0	$151.57
26-08-2008	44395	37768	795	1:48	$268.65	$0	$268.65
27-08-2008	52943	43614	859	1:51	$276.11	$0	$276.11
28-08-2008	17022	13545	267	1:51	$100.04	$0	$100.04
Total	1138509	969697	20281	1:48	$6456.93	$0	$6456.93

Figure 7: One affiliate's earnings and hit statistics displayed in the RefeshStats admin portal.

Figure 8: MacCodec.com.

For example, yet another scareware vendor, Topsale2.ru, states on its front page that only traffic from the USA, Canada and Australia is being accepted and that the commission rate is up to $25 per sale. Its promo materials include 'web scanners' (a dynamic HTML page that deceives users into believing that their PCs have been scanned and that viruses were found), codecs (pages with fake video players that require an 'update') and three different variants of EXEs (the actual payload). They do not shy away from saying that one of the executables advertised was made specifically for loading into a botnet.

The site claims the average traffic conversion rate is $100–$250 per 1K loads, which with $25 commission rate implies that up to 10 of every 1,000 users infected with a fake AV threat end up actually paying for it.

To further convince potential affiliates to sign up the home page links to sample statistics for an average member ($4916 commission paid in 11 days), as shown in Figure 9.

Again, we can see how a successful webmaster can make over $180,000 per year on this network alone from traffic averaging 10K visits per day. Assuming that most webmasters direct their traffic to more than one sponsor at a time, it is no surprise that affiliate marketing and black SEO are extremely appealing career paths for a computer savvy person in Eastern Europe.

In 2008 we observed a record number of codec partners' sites – CodecCash, SmileCash, OXOCash, Go-Go-Cash, IframeVip, Bucks Loads, Ruler-Cash, 3XLCash, SpicyCodec, VIP Codec, K2Cash, VIPSoftCash, Topsale.us, RulerCash, CashPanic, Traffic-Converter.biz and SoftwareProfit, to name just a few. With each maintaining its own set of software and promo material, there is little wonder that the volume of rogue anti-virus applications and codec doorway sites has risen to unprecedented levels in recent years.

The majority of the aforementioned sites appear to have gone away for a variety of reasons. Some of them blame their

User stats for period 2009-03-01 - 2009-03-15 :

Date	Visits	Buy page	Loads	Sales	Ratio (Uniq/Sales)	Ratio (Loads/Sales)	Ch-backs	Refunds	Referals	Sales	Money
2009-03-01	15817	492	7980	37	1:427	1:215	0	1	0.00	1078.92	1078.92
2009-03-02	14013	409	5925	28	1:500	1:211	0	2	0.00	779.22	779.22
2009-03-03	9949	252	2832	21	1:473	1:134	0	2	0.00	569.43	569.43
2009-03-04	11765	298	3482	12	1:980	1:290	0	0	0.00	359.64	359.64
2009-03-05	7504	173	3064	2	1:3752	1:1532	0	0	0.00	59.94	59.94
2009-03-06	3023	106	3801	8	1:377	1:475	0	1	0.00	209.79	209.79
2009-03-07	2370	113	6416	9	1:263	1:712	0	1	0.00	239.76	239.76
2009-03-08	8841	278	6388	24	1:368	1:266	0	1	0.00	689.31	689.31
2009-03-09	10936	358	5234	6	1:1822	1:872	0	4	0.00	59.94	59.94
2009-03-10	12331	379	6862	24	1:513	1:285	7	2	0.00	482.05	482.05
2009-03-11	5384	194	833	13	1:414	1:64	0	0	0.00	388.31	388.31
Total:	**101933**	**3052**	**52817**	**184**	**1:553**	**1:287**	**7**	**14**	**0**	**4916.31**	**4916.31**

Figure 9: Topsale's sample statistics for an average member.

billing systems which turn accounts down as soon as they recognize that they are related to scareware sales. Others were exposed by Brian Krebs in his *Security Fix* blog in the *Washington Post*, and by other security researchers. These articles often initiate a take-down effort similar to what happened to McColo, EstDomains and 3FN.

But there is a new trend emerging. Here is an excerpt from a blog post made on 6 June 2009 by the CashPanic team:

'... this business is no longer as attractive as before due to high costs and risks which no longer get compensated by the declining profits ...'

We can only hope that this trend is affecting all of the fake anti-virus vendors and that we will soon witness an end to it.

CONCLUSION

Affiliate web marketing attracts thousands of people motivated by the high earning potential and the flexibility of self-employment. The examples mentioned in this article are merely the tip of the iceberg. The affiliate networks focused on the promotion of illegal products are part of a growing multi-million dollar 'industry'. Affiliate web marketing also became the main driving force behind the recent explosion in malware, website infections, email spam and general web pollution.

At the same time we see some hopeful signs. Security researchers are working closely with law enforcement to orchestrate rogue network take-downs. Billing and hosting companies are becoming more responsive to abuse reports and do stop providing support to rogue businesses. The most dangerous sides of the affiliate business such as scareware are being forced to close or go underground, which impacts their operational costs.

All this good news will not completely eliminate unethical and illegal Internet practices, but the effects may reduce the impact to a manageable level.