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