

## Russian Business Network - Faking its Demise

Although it is true the Russian Business Network (RBN) as AS40989 RBN AS RBusiness Network has relinquished its IP addresses (not the related &lsquo;peers&rsquo;), this blog has never shown this as the core centre of RBN activity or particularly relevant to its commercial activity. To simply test the hypothesis of the demise of the RBN as in recent headlines in the press using phrases as &ldquo;Mother of all cybercrime vanishes from the web&rdquo;, or &ldquo;RBN goes Poof&rdquo; is to simply review one of the RBN&rsquo;s major money earning retail activity.

HYPOTHESIS = Logically RBNs fake anti-spyware or rogue software should show major changes in serving and hosting over the last week or so, if the demise of the RBN is correct. Fortunately based on limited CYBERINT earlier we were able to show 57 well known &lsquo;fakes&rsquo; and 34 of the top 40 being RBN related, below can be seen the specifics.

RESULT = With the exception of the loss of replacement of AS40989 secondary name servers there has been little or no change to the core IP addresses.

(a) For example; Antivirgear shows a current Alexa Trend/Rank: #5,473 (out of an estimated 60 million web sites) improved over the last month. 397,296 U.S. visitors per month which is 10.7% of its traffic thus visitors worldwide = 3.7 million, this is just one of many &lsquo;fake&rsquo; web sites.

(b) It does assist in highlighting the role of Interpace AS 27595 (AKA; Atrivo (US), Inhoster - xbox.dedi.inhoster.com - Ukraine, and Estdomains) as a fundamental part of the RBN from 2004 (see fig 1).

For the results Figure 1 shows an overview of the RBN's / Atrivo share of the 'fakes' market. For completeness (click on the images to enlarge);

Figure 2 - shows the complete list of the 57 'fakes' in alphabetical order.

Figure 3 - shows the complete list of the 57 'fakes' ranked to specific hosts / servers.

N.B. - It should be noted the 6 'fakes' listed as offline, this are currently dormant, historically this has happened before and such domains often come back to use.

Click on Image to see detail

