

## RBN - The Good, Bad and the Ugly

An interesting story in Wired.com by Ryan Singel, based on email correspondence from a representative claiming to be from the Russian Business Network (RBN). As reported, the RBN's man said current reports about the organization "..... is subjective opinion based on guesswork." In keeping with this blog's "quantitative" format we make an attempt to shed some light on this.

Figure 1. Shows a representation of the RBN from the perspective of web infrastructure, it provides three levels of operation:

1. "Good" & "Bad" - RBN Autonomous System (AS) &ndash; backbone internet structure (see diagram 2)
2. "Bad" - RBN Global &ndash; Core server hosting operations, e.g. RU, UA, BR, DE (Denic.de, crew-gmbh.de), CH (rbnetwork.biz), IT, NL, Panama, UK (Too coin via &ndash; Ripe representation &ndash; sbttel), Seychelles.
3. "Ugly" - RBN Retail &ndash; Specific exploit, ID theft, MPack. e.g. iFrameCash, 76Service.

For the purpose of the Wired.com article there needs to be focus on the RBN Autonomous System &ndash; Figure 2.

The problem is the RBN's Autonomous System is integrated within the whole of the Russian , Eastern European, and Eastern Scandinavian internet system overall. For example three of the following:

- AS41181 RUSTELECOM, = AS4589 EASYNET, AS20597 ELTEL (general internet for Russia as a whole)
- AS34596 CONNECTCOM ConnectCom Ltd Autonomous System, &ndash; included within are # AS8426(CLARANET AS ClaraNET UK AS of European ISP)# AS20597(ELTEL AS ELTEL net Autonomous System) any # AS34596 & # AS24919(CUBIO AS Cubio Communications Ltd Helsinki Finland)
- AS39848 DELTASYS Delta Systems network &ndash; included within # AS20597(ELTEL AS ELTEL net Autonomous System) any AS39848, # AS24919(CUBIO AS Cubio Communications Ltd Helsinki Finland)

Although they are in the RBN Autonomous System they are within other Autonomous Systems. These should be discounted from the RBN "bad" or "ugly" groups.

Therefore, CONNECTCOM's spokesman to Wired.com is either:

(a) Another innocent caught in the bad and ugly RBN's maelstrom, they may actually own the RBN, but not the one we know.

(b) A RBN (bad or ugly) stooge trying to misdirect

As with earlier posts here, re; RBN hiding within US hosts, we have to recognize the RBN does the same in Russia and elsewhere. The requirement is to focus on the RBN "ugly" Retail Division. The specific source for website exploits, ID theft, etc.