

## RBN - Fake Codecs

With the ongoing tracking of "fake" software websites related to the Russian Business Network (RBN) and their associates it is

important to note the growth of the fake codec websites. A codec is a small program that's allows an operating system or a program to properly play audio or video in a particular format, e.g. MP3, WAV, Xvid, MPEG, Indeo and Cinepak.

Figure 1. Sample "fake" codec site - Gamecodec.com

This article is cumulative snapshot report based upon current and historical community reporting from; Zlob Watch (peki.blogspot), Sunbelt, and the excellent earlier work of Jahewi's Fake Codec Information (unfortunately last updated Jan 20th 07). The key issues are:

\* Currently shown here (see fig. 2 below) 53 active, with the 60 earlier reported mostly dormant domains (see fig. 3 below) provides for a total of at least 113 "fake" codec web sites operational over an 18 month period. It would appear many of the active domains alternate on a regular basis from being non resolvable (apparently offline) to online.

\* The prime exploits from these sites are (a) Zlob - shows fake error messages and silently installs fake anti-spyware products. (b) DNSChanger silently adds rogue DNS name servers to your PC or Mac. These name servers will resolve non-existing domains (typo-squatting) to IP addresses associated with the authors to generate revenue and could potentially re-routes traffic from legitimate web sites to other suspicious web sites. Ref peki.blogspot

Note: We should clarify that the Mac fake codecs are only for the DNS changing trojans and that not all the sites listed will spawn Mac stuff.

\* These exploits are designed for Mac and Windows users; with the attack vector similar to the "fake" anti-spywares however the technique is varied by constantly emerging new domains but mostly to a singular web landing page interface.

\* Most importantly all 113 domains are or were registered with Estdomains, similarly all of the active 53 domains in fig. 2 are hosted by AS27595 by Atrivo; AKA - InterCage, Inhoster, Cernal, etc. Also added should be AS 36445 a newer Autonomous Server apparently used by Cernal. For blocking purposes the following IP ranges should be incorporated:

64.28.176.0/20 AS27595 INTERCAGE

85.255.118.0/20 AS27595 INTERCAGE

85.255.112.0/20 AS36445 CERNE

Figure 4 - Sample IP Map - Zerocodec