

# INSIDE OF AVP4

vx-underground.org archive // z0mbie



Did you know that there is some secret stuff inside of AVP4 files?

Yep, this is a list of some internal messages and resources, author names, plugin descriptions, comments, CLSID's, and other shit.

Secret stuff has a fixed header of 0x0E bytes length, 'KLsw\x00\x00KLsw\x04\x00\x00\x00', and right after these bytes the compressed and then encrypted stuff is placed. The decrypted (just unXOR'ed -- did you prayed to XOR today?) stuff begins with a header of 0x1E bytes length, including some CRC inside, and then some data, compressed with the same method as .AVC bases. Decompressed data contains a header, then list of resources itself, and terminates with another CRC (probably CRC32, but who cares).

```
Secret stuff format:
<----0x0E----> <----0x1E----> <----- ? ----->
KLsw00KLsw4000 [hhhhhhhhhhhhcrc [hhhhxxxxxxxcrc]]
\fixed header/                                \--compressed--/
                                         \-----stupidly XOR'ed-----/
```

Internal format of the resource list is the following:

Length	Description
0x13	Useless Header
4	Type (int, string, etc)
n	Data (Length depends on Type, may be zero)
4	Type
n	Data
...	....
4	CRC

So, the following objects are containing this stuff:

Plugin Files	Program Files\Kaspersky Lab\*.PPL (.rsrc/ovr)
Configuration files	Program Files\Kaspersky Lab\*.KLR (plain)
Some libraries	Program Files\KAV Shared Files\*.DLL (.rsrc)
Registry settings	System Registry, in binary form (HKLM\Software\KasperskyLab\Components\101\Standalone\OptionsPagesState)

Well, right after we understood what the injustice kaspersky is going to do, we spent some hours and wrote a little program, called AVP4 Secret Resources Unpacker (AVP4SRU), and unpacked all the found secret stuff just for fun. And now, all the unpacked files have .SRU extension, and are available to download [here](#).

greetz to **Krukov** - brief and to the p