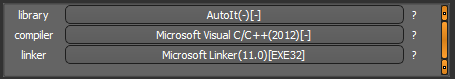
MALWARE ANALYSIS

Sample 1: Video related app with no icons, no user dialog, that captures your every move and connects to the internet, obviously.

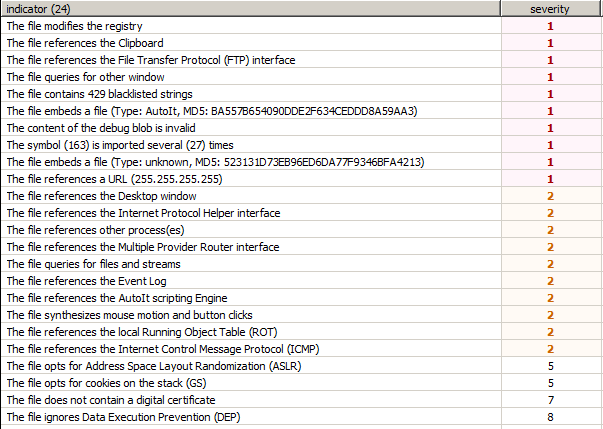
STATIC

MD5: <http://virusshare.com/hashes/VirusShare_00136.md5>

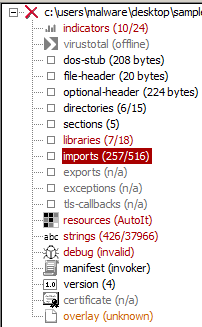
DIE :



PES :

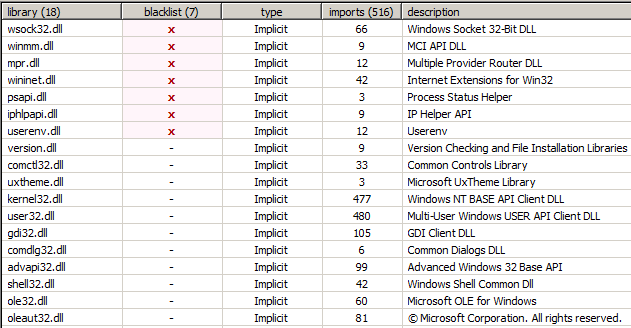


A lot of dodgy Network in addition to mouse replication.



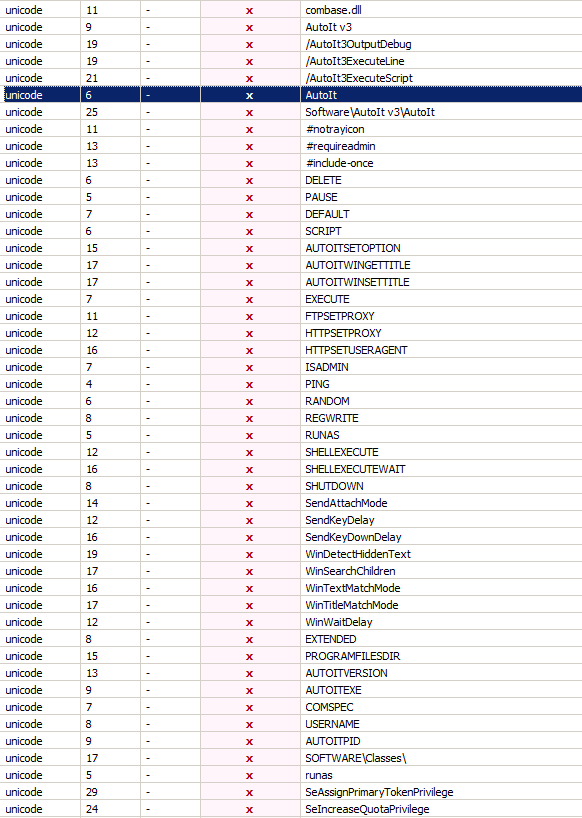
Library

Too many libraries for this type of program and very strange ones as well.

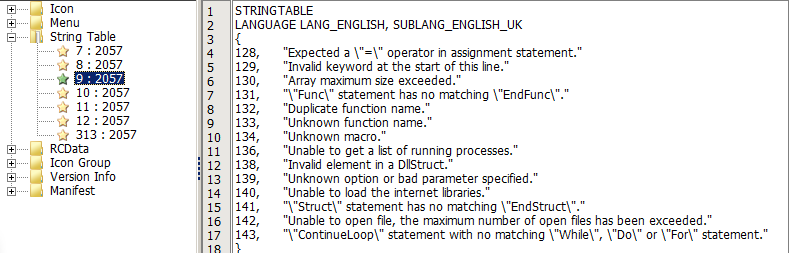


Strings :

The strings confirmed my suspicions about the dodgy libraries



RH :

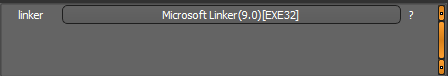


The String Table only contains Debug dialog.

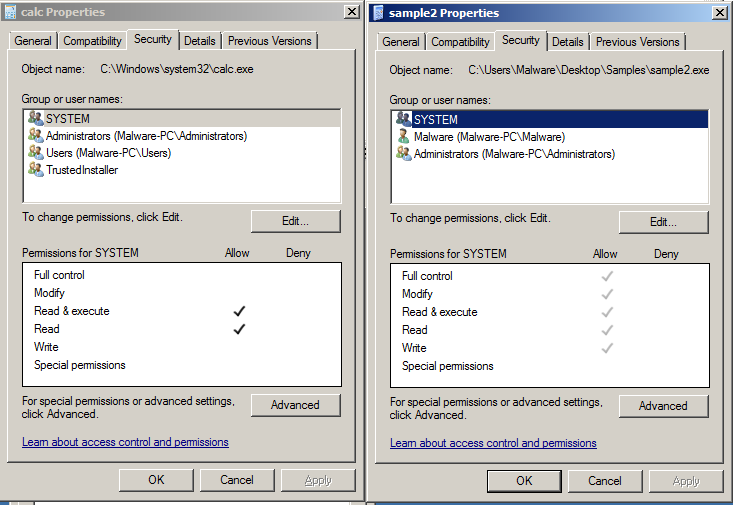
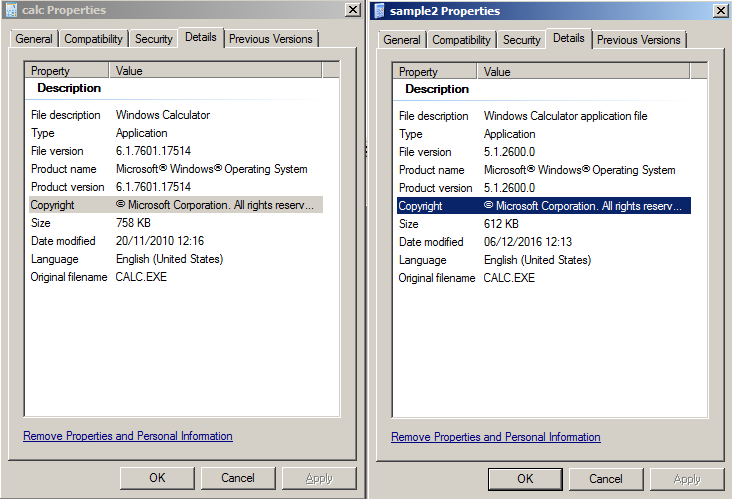
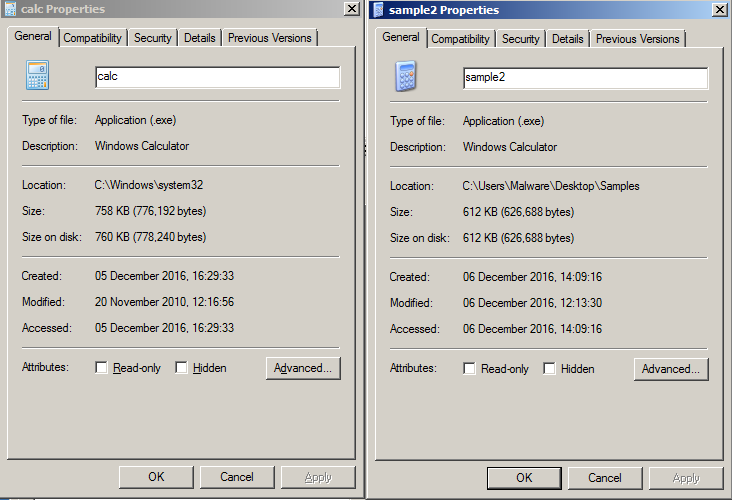
DYNAMIC

Sample 2: calc\_ng, just like the normal one but with candy hidden inside

DIE :

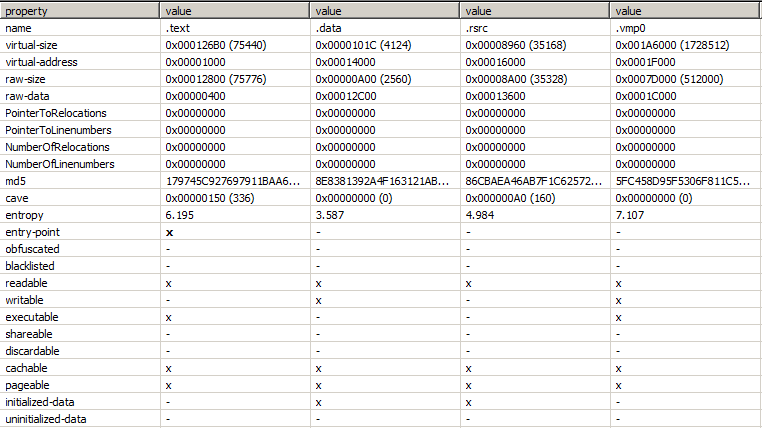
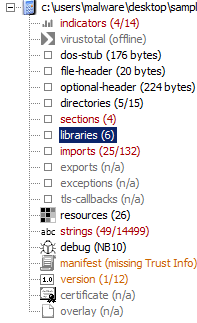


Comparison :



Real modified in 2010 -> version 6.1 | Sample2 modified 2016 -> version 5.1

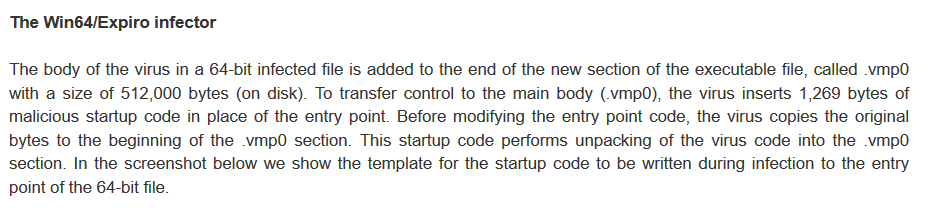
PES :



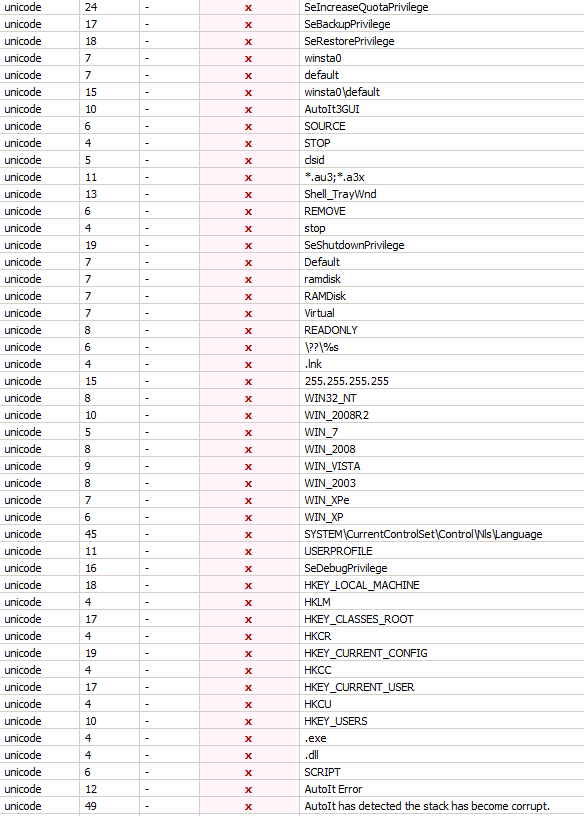
This last section seems odd, after research on vmp0 section -> It seems that our malware is Expiro. Will verify this with IDA and the dynamic analysis.

<https://blog.fortinet.com/2013/09/02/expiro-an-epo-file-infector>

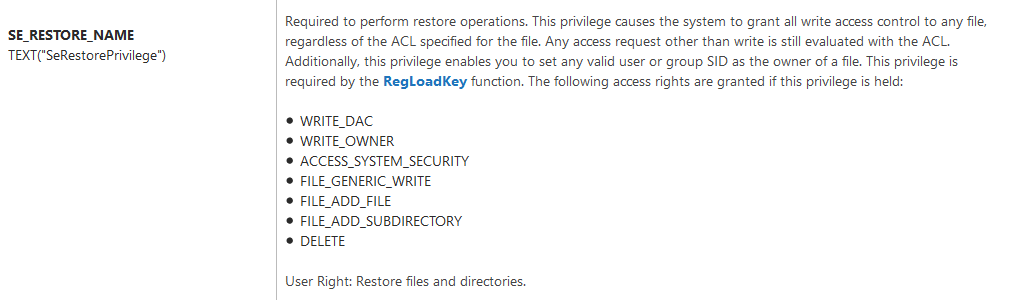
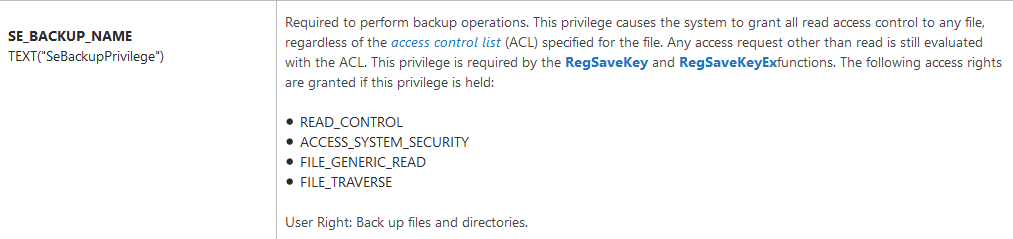
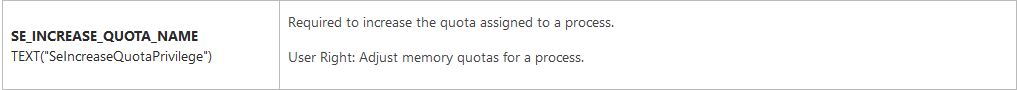
<https://artemonsecurity.blogspot.co.uk/2013/09/xpiro-64-bit-analysis.html>



Strings :

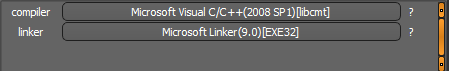
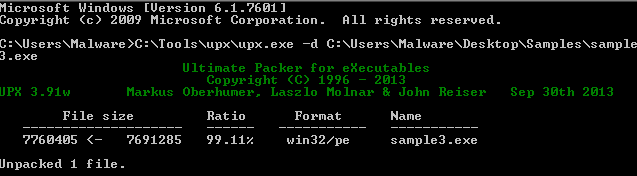
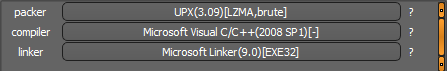


Playing with register, network interfaces, and privilege constants



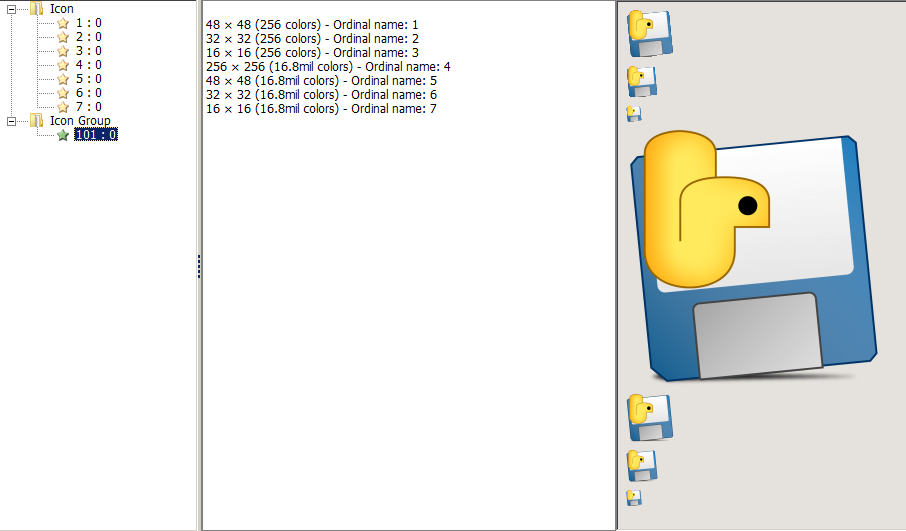
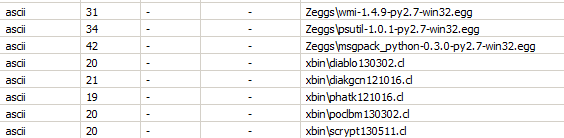
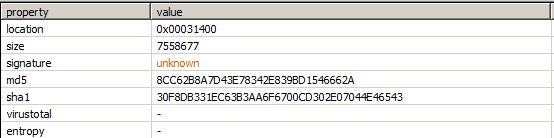
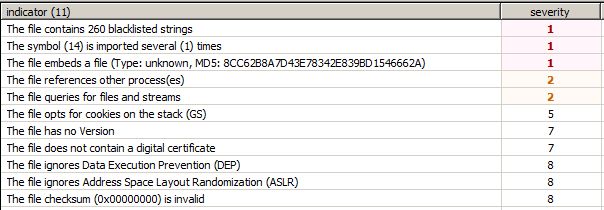
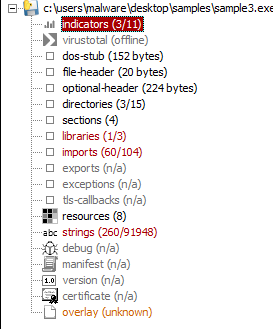
Sample 3: half python, because who needs full python

DIE :



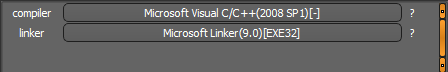
Upx is already suspicious

PES :

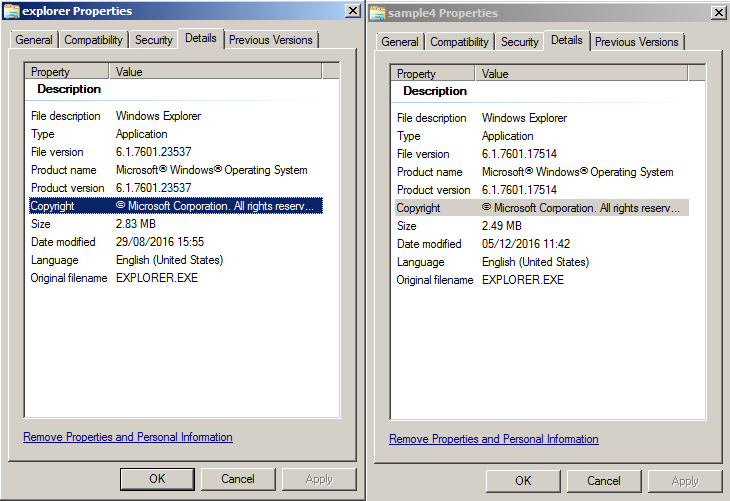
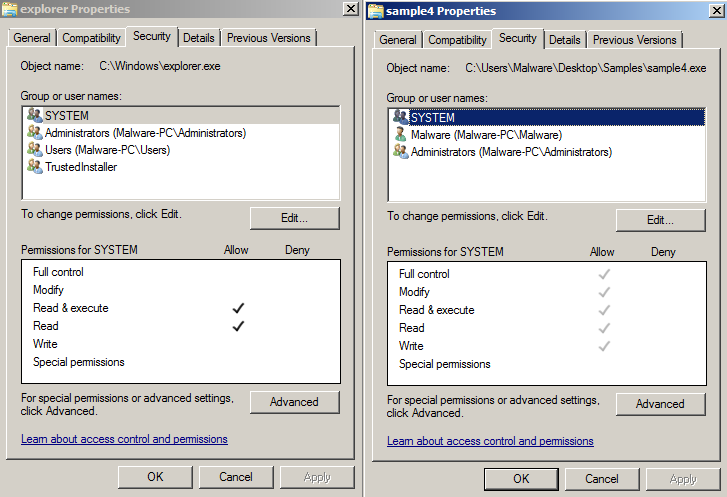
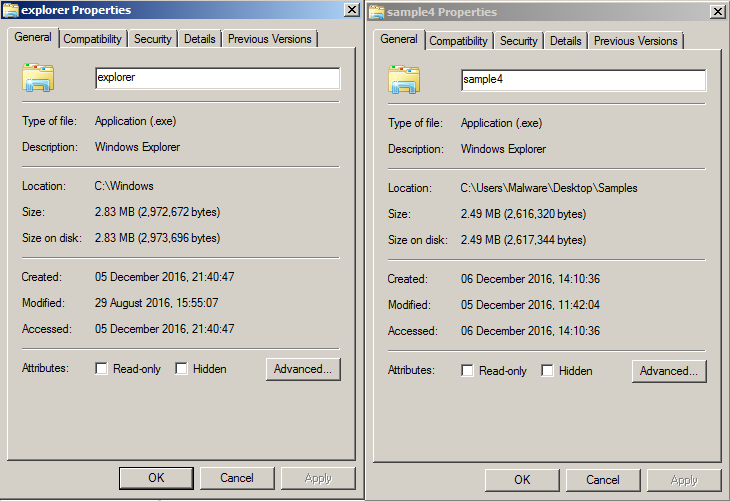


Sample 4: explorer\_ng, actually explorer

DIE :

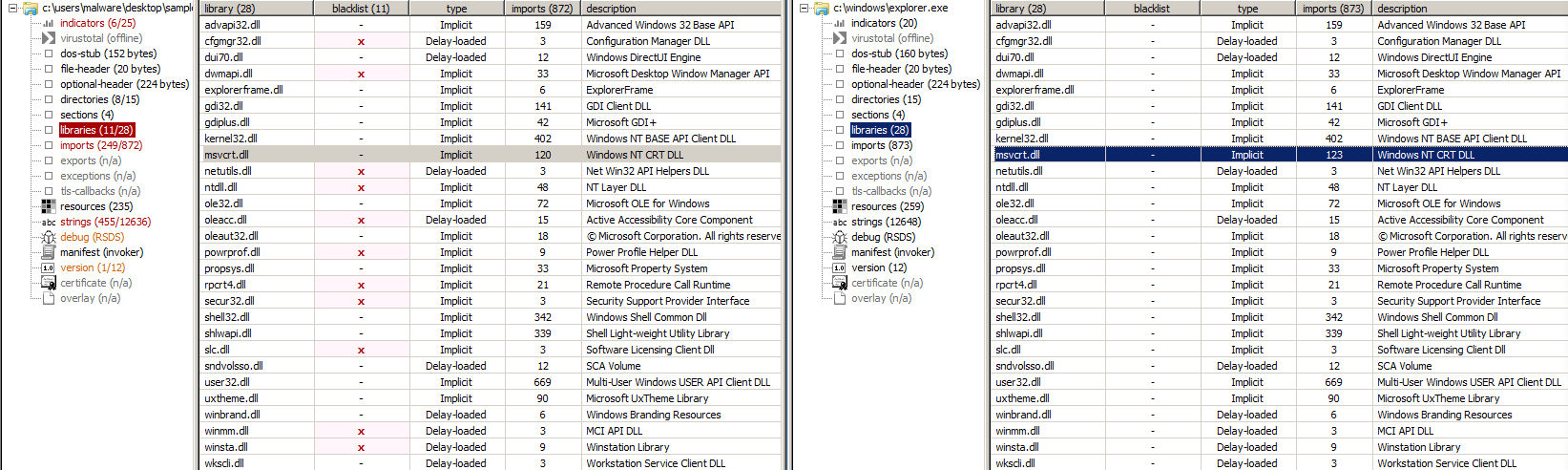


Comparisons :



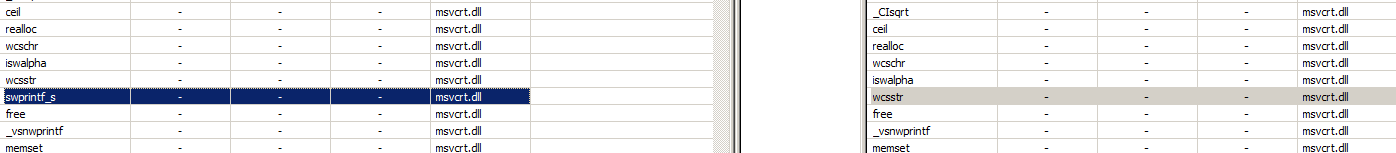
The only thing odd here is the difference in size and version.

PES Comparison :



Almost the same values, but with some really small changes in the ressources and strings. 1 thing to check in IDA and DW is these differences in number of imports.

DW and imports comparison, swprintf\_s is missing in the sample

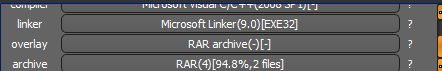


NON-suspicious

Sample 5: mutorrent\_ng, Trojan.exe is our new torrent client

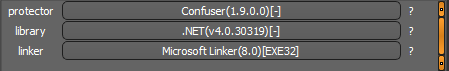
DIE :



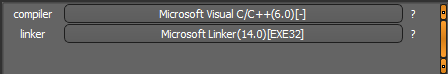
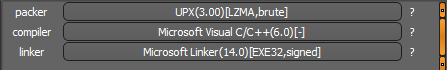


Unrar -> Crack + uTorrent

DIE Crack :



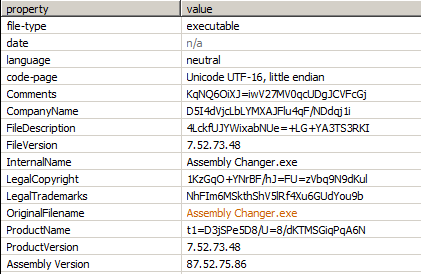
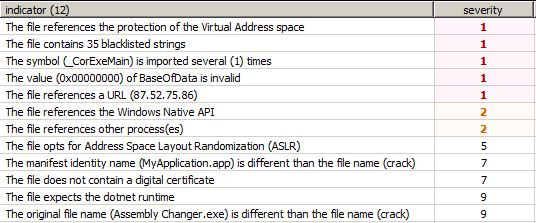
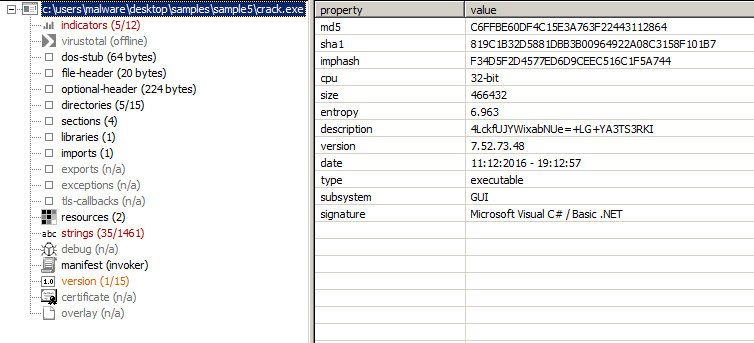
DIE uTorrent :



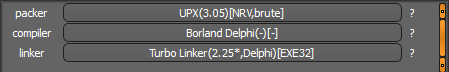
I decided to check everything

PES original :

PES crack :



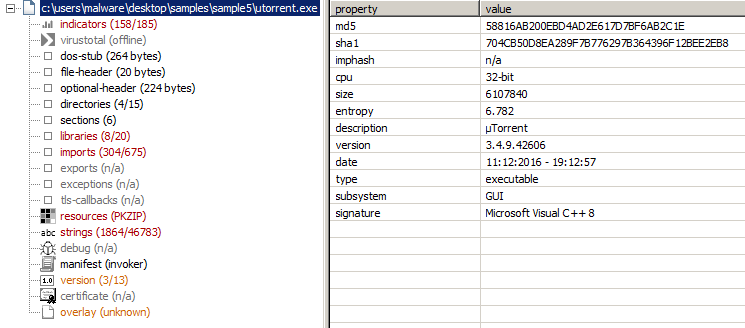
MD5 : <https://www.virustotal.com/en/file/cbcd579a3bd0455a7034fb70d0ffcc52fb1a44428a6306d88cd784c55b349019/analysis/>



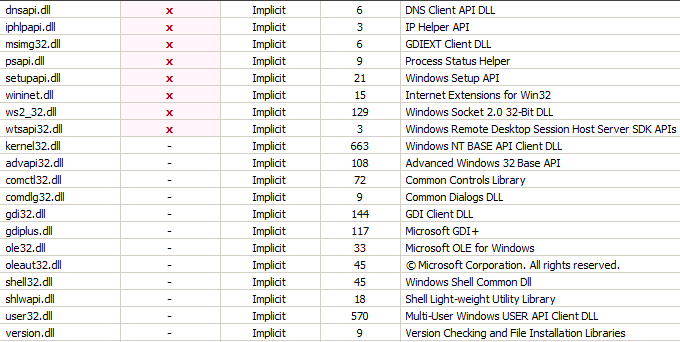
Assembly Changer.exe redirects to a Trojan DB and the IP addresses found in the versions as well (87.52.75.86 (Danemark), 7.52.73.48 (USA)

PES UPX:

PES uTorrent :



We can see that the ressources seem to hide a zip package inside. Probably malicious code wrapped for more obfuscation.



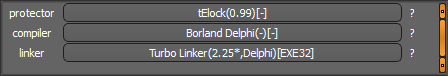
Some of these links make sense because utorrent is a torrent client, but some or very dodgy :

The md5 : <https://www.virustotal.com/en/file/30eebb89987c78eb2679f81739bb7a0f95cb8162c555ad0c39c34e02ea6757cd/analysis/1478209777/> and further research -> <https://en.wikipedia.org/wiki/OpenCandy>

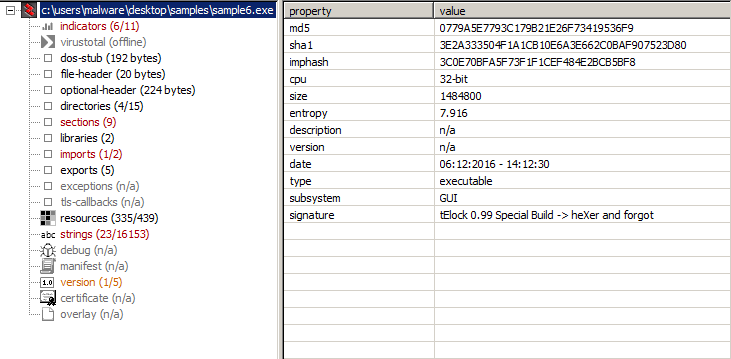
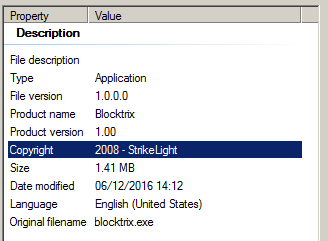
We’ll check in IDA and dynamic analysis for confirmation.

Sample 6 : Blocktrix renamed Hupigon for the 2016 version

Die :



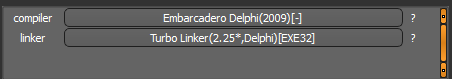
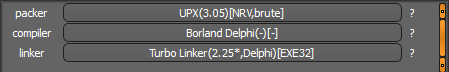
Properties



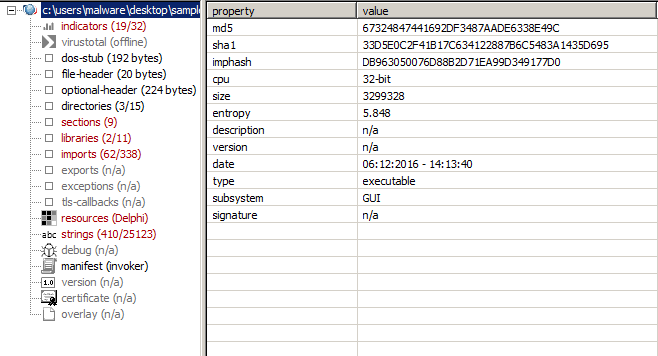
MD5 : <https://www.f-secure.com/v-descs/backdoor_w32_hupigon.shtml>

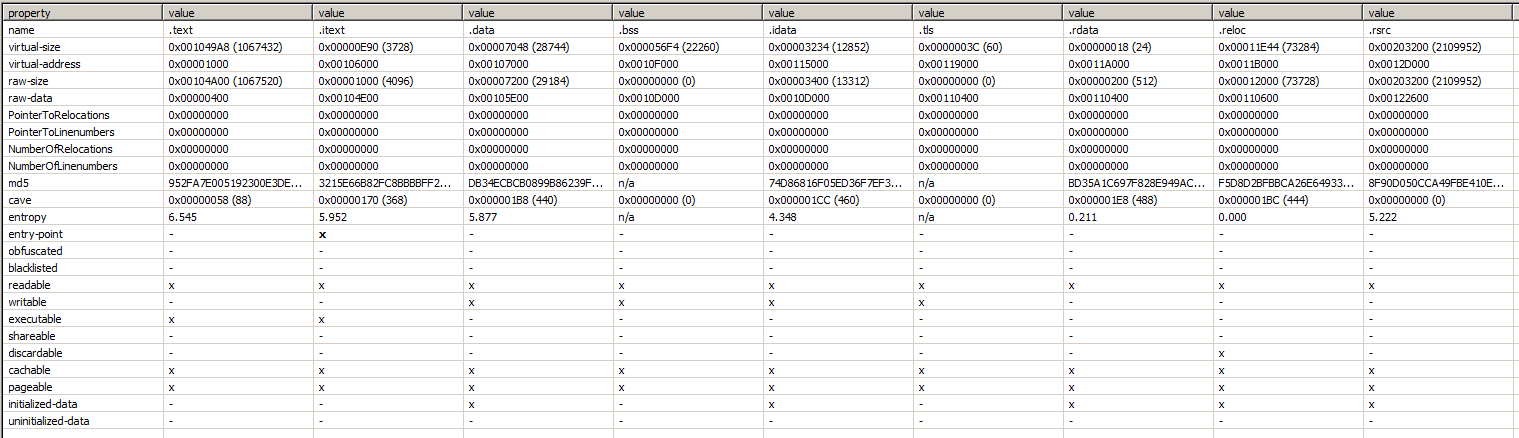
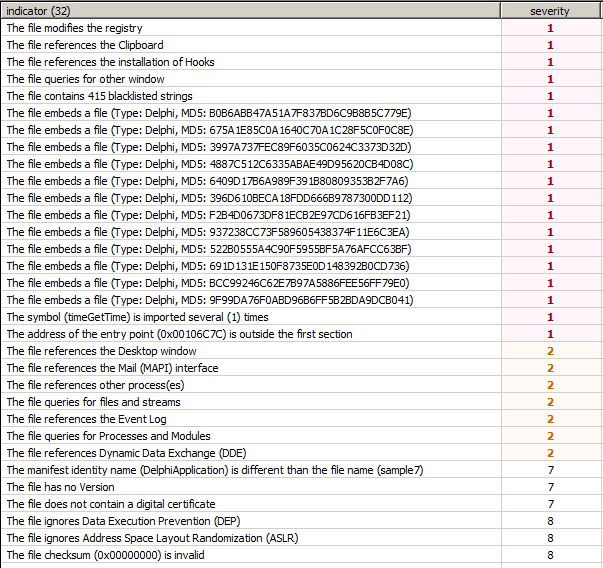
Sample 7 : Security essentials don't like it when you try to open your taskmng

DIE :



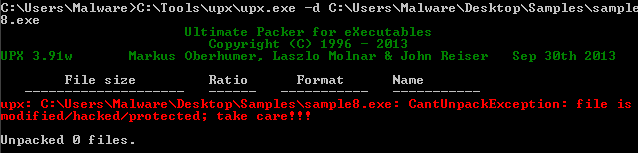
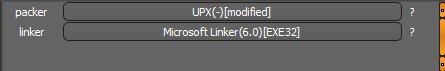
PES :





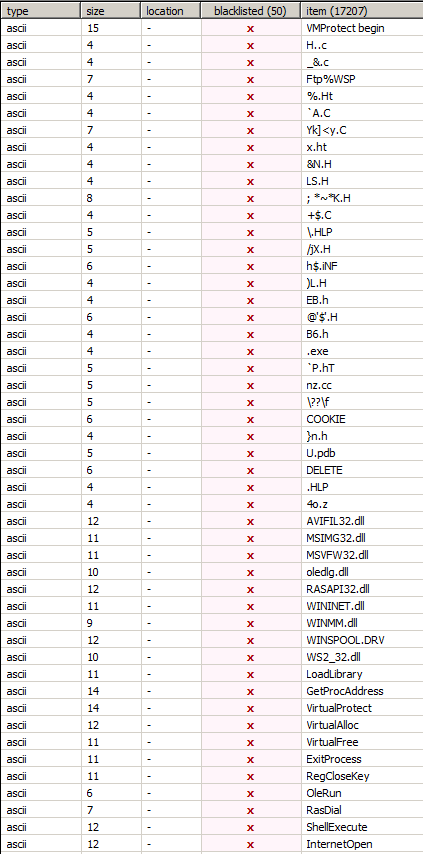
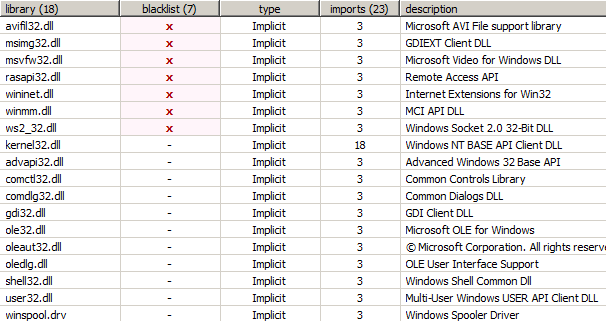
Sample 8 : Automatic on-hook software, great simple chinese tutorial

DIE :



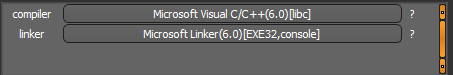
Protected against upx decompression, pretty skechy plus the libraries used

PES :

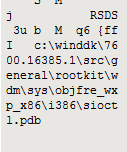
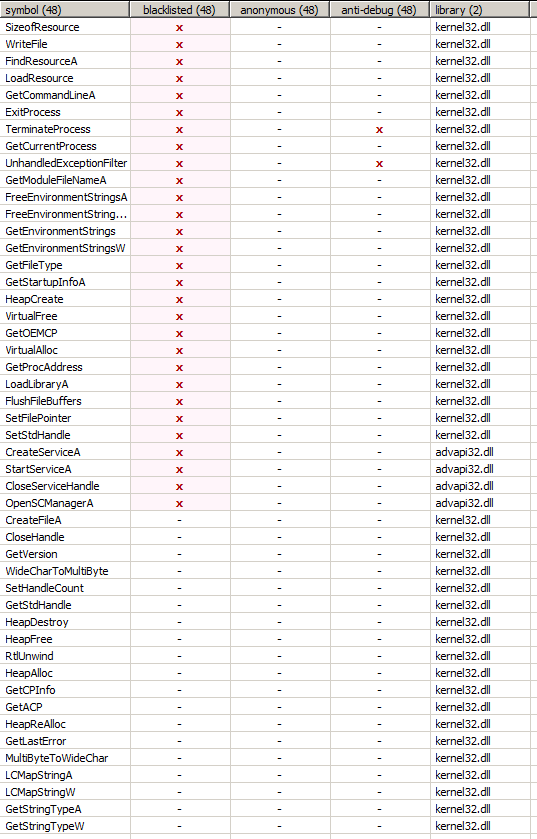


Sample 9: Powerfull driver that we hide with a rootkit to keep the other drivers from getting jealous

DIE :

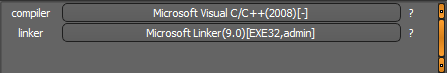


PES :

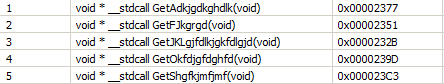
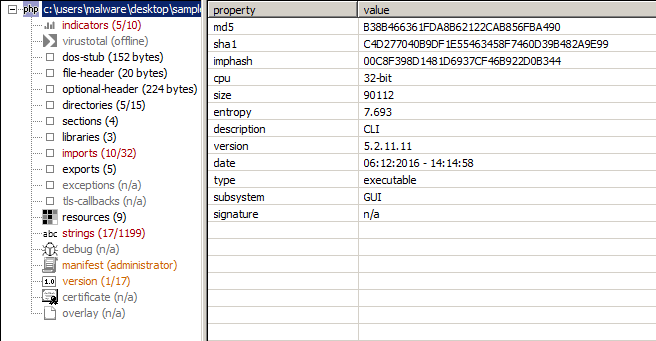


Sample 10: PHP trojan not liked by the AVs but has a rootkit friend to protect him

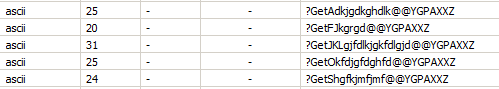
DIE :



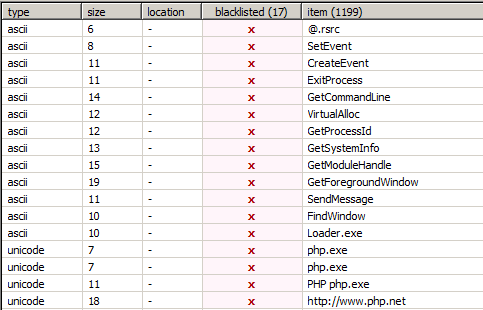
PES :



This looks like functions renamed to remain hidden. To check with IDA



Here we can see the arguments passed ?





<https://www.virustotal.com/en/file/187538470ce16260cb47c2fe47789525bbbb2a8bc8f67bdd5c7abc69bd5206da/analysis/1305684161/>

<https://totalhash.cymru.com/analysis/?f169459dcb24103d1a9a8ff7aabd00947ed906b0>