THE MALWARE NAMING CHAOS

Ferenc Leitold, fleitold@veszprog.hu
University of Veszprém

WildList is the most authentic source of information on which viruses are spreading In the Wild. The lists of widespread viruses are based on reports of researchers around the world. These lists are very good information source for experts. They always know which listed virus is which. Unfortunately the average user is unable to identify the listed viruses. There is a great help about it: in the virus descriptions menu point there is some info about the listed viruses, but there are some problems about it:

- The latest available description list is not actual.
- The information is based on only F-Secure database. So it is related to the F-Secure naming convention.
- There are some missing list elements where there is no information.
- There are some viruses where the information of the variants link to the same place.

It means that it is impossible to correctly identify the listed viruses.

In this situation the good solution would be the publication of exact comparable names that can be used for identification as well.

Real-time AV testing project may be the solution for this purpose. It can provide virus naming information for In-The-Wild viruses. It means that every virus sample should be checked using almost all updates published by AV developers. This system is able to do this automatically. So if a new upgrade of an AV published it can detect it and the test is executed in some minutes the update process executed. After update procedures executed the whole image of the operating system and the updated AV saved. If a new virus appeared in the wild then it has to be checked by all AV software. But not only the actual ones used, the previous 15-20 versions has to be checked as well. Using this method it can be checked which is the first version of AV that is able to identify the new virus.

This Real time AV tests can provide exact information for virus identification including AV product name, version, build number, virus database version, ... It is possible to search for earlier information as well. It is possible to identify if an AV vendor changes the name of a virus.