



The Disconnect Between the WildList and Reality

New anti-malware certification scheme needed

Abstract

We all know that the information security scenario is changing rapidly. The ever growing number of malware samples received at our labs, the spread of thousands of variants of bots, trojans, rootkits, keyloggers, targeted attacks, etc. is leading to what we internally at Panda call a “silent epidemic”. In this scenario, users must count on products which effectively protect them against the more insidious threats currently “in the wild”. On the other hand, security certifications must attest to such effectiveness within the new malware environment. However, **the current criteria used to certify anti-virus products have become obsolete** and the certification seal is far from reflecting such effectiveness. End users purchase “anti-malware” solutions but product certifications are designed for “anti-virus” solutions, which can lead to confusion.

The WildList and “Anti-Virus” (AV) certifications

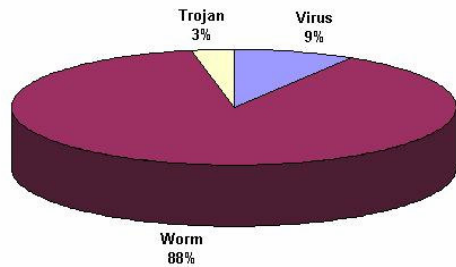
Information security certifications are useful mechanisms to improve confidence in computing, to increase IT users’ protection levels and to guarantee the use of appropriate security solutions. In order to be meaningful, security certifications must attest the effectiveness of products against a representative test bed of the threats that exist in the real world. The most recognized certifications today take **the WildList as their test bed of malware samples** to which the products must protect against. Detecting all the samples contained in the WildList is therefore required to obtain the certification.

The disconnect

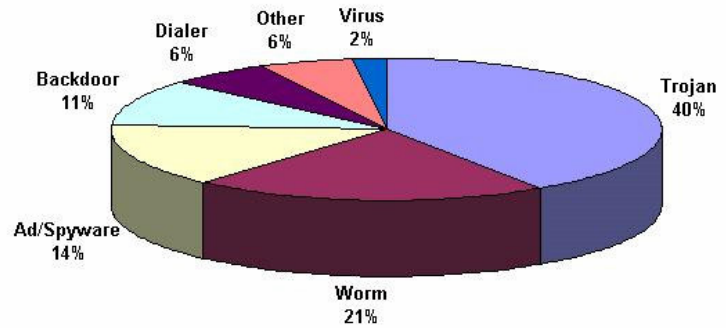
As the charts below show, and which all of us who work at anti-malware labs already know, currently the WildList is far from representing the malware situation in the real word. This is due to several factors:

- 1) **The WildList contains mostly samples of viruses, worms and very few trojans.** It does not contain other types of very common malware, such as dialers, rootkits, keyloggers, adware or spyware. As we know strict viruses have been in declining prevalence for quite some time now.
- 2) **The WildList contains a small number of samples,** perhaps due to the limitations of the current reporting criteria, the lack of automated processes to handle large amounts of samples, or perhaps even the low priority of this task during the course of normal activities at the lab (being a WildList reporter is entirely voluntary and no obligation exists to report any minimum number of samples). The result is that only a very small number of samples are included in the list.
- 3) **The WildList is always outdated,** in some cases by a few months (the current list is from November 2006). Publishing the WildList is manually intensive and very time consuming.

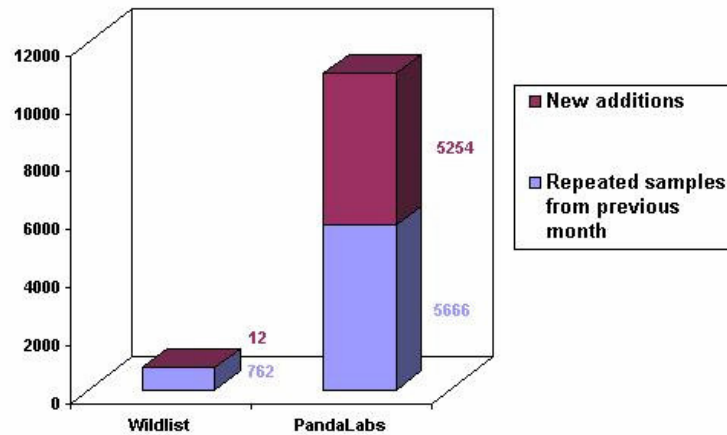
Most recent core WildList, Nov 06
Total samples: 774



PandaLabs, Nov 06
Total samples: 10,920



Samples included in the core WildList (data from WildList published on Nov, 06) in comparison to the circulating malware identified by PandaLabs on the same month (November, 2006).



New vs. repeated malware. Of the 774 samples included in the core WildList (Nov 06), only 12 of them are new additions. During the same period, PandaLabs received 5,254 new and unique samples of malware. These samples are submitted automatically from our customer base.

What is needed?

We need anti-malware certification criteria which reflect reality and guarantee the protection of users. As this is not an easy task, it could be undertaken in two phases, *one for correcting current problems in the short term and a second for implementing a broader solution to the problem*. Our recommendations are:

Phase 1: correct current problems of the WildList without changing the certification scheme

1. **Change the WildList reporting criteria to include all types of malware** (including ad/spyware, backdoors, rootkits, etc.). In other words, expand the WildList from a traditional (virus, trojans and worms) focus to a much broader malware perspective which represents the current threat environment.
2. **Encourage current members to report based on these new criteria** not only viruses, trojans and worms but also any malicious code that is actively infecting users. Alternatively, **expand the network of designated reporters** by incorporating new entities with high visibility on circulating security and malware threats, such as CERTs for example.
3. **Release the updated WildList more rapidly** so as to avoid two and sometime three month old lists which do not represent “current” threats.

By correcting these limitations we can make a significant and quantitative improvement in reflecting the reality of the threat environment with a more representative WildList, which will inevitably result in improved and valued certifications.

Phase 2: design a new certification scheme with extended participation

In a second phase a Task Force could be formed in charge of creating a more adequate certification scheme. This Task Force could join, for example, The WildList Organization, the Product Certification Organisations, the AVPD Consortium, and third party members such as CERTs.

This extended participation would therefore contribute to the credibility of the WildList and the certifications based on it, and to “raise the bar” for security vendors attempting to certify their products; in other words, to raise the baseline of commercial products in order to guarantee the protection of users.



For more information:

Pedro Bustamante, Senior Research Advisor
pbustamante@pandasoftware.com