The WildList is Dead,
Long Live the WildList!

Andreas Marx, Frank Dessmann
AV-Test GmbH, Magdeburg, Germany

http://www.av-test.org

Presented at the Virus Bulletin 2007 Conference in Vienna, Austria
http://www.virusbtn.com/conference/vb2007

Table of Contents

- Introduction
- The list of problems and concerns we have
  - The changing threat landscape
  - Increase in the number of malware samples
  - Nobody wants to report anything
  - The WildList is outdated when published
- Suggestions “to make it better”
- Q&A

Introduction (I)

- The WildList is the well-accepted standard for AV testing and certification…
  - But it’s not reflecting the “in the wild” situation properly
- Vesselin Bontchev already opened the discussion with a paper on the topic “The WildList – Still Useful?” at the 1999 Virus Bulletin Conference
  - The paper was so “controversial” that it was not printed in the conference proceedings
- We’re not alone with criticism, here are two examples from the VB 2007 proceedings…

Introduction (II)

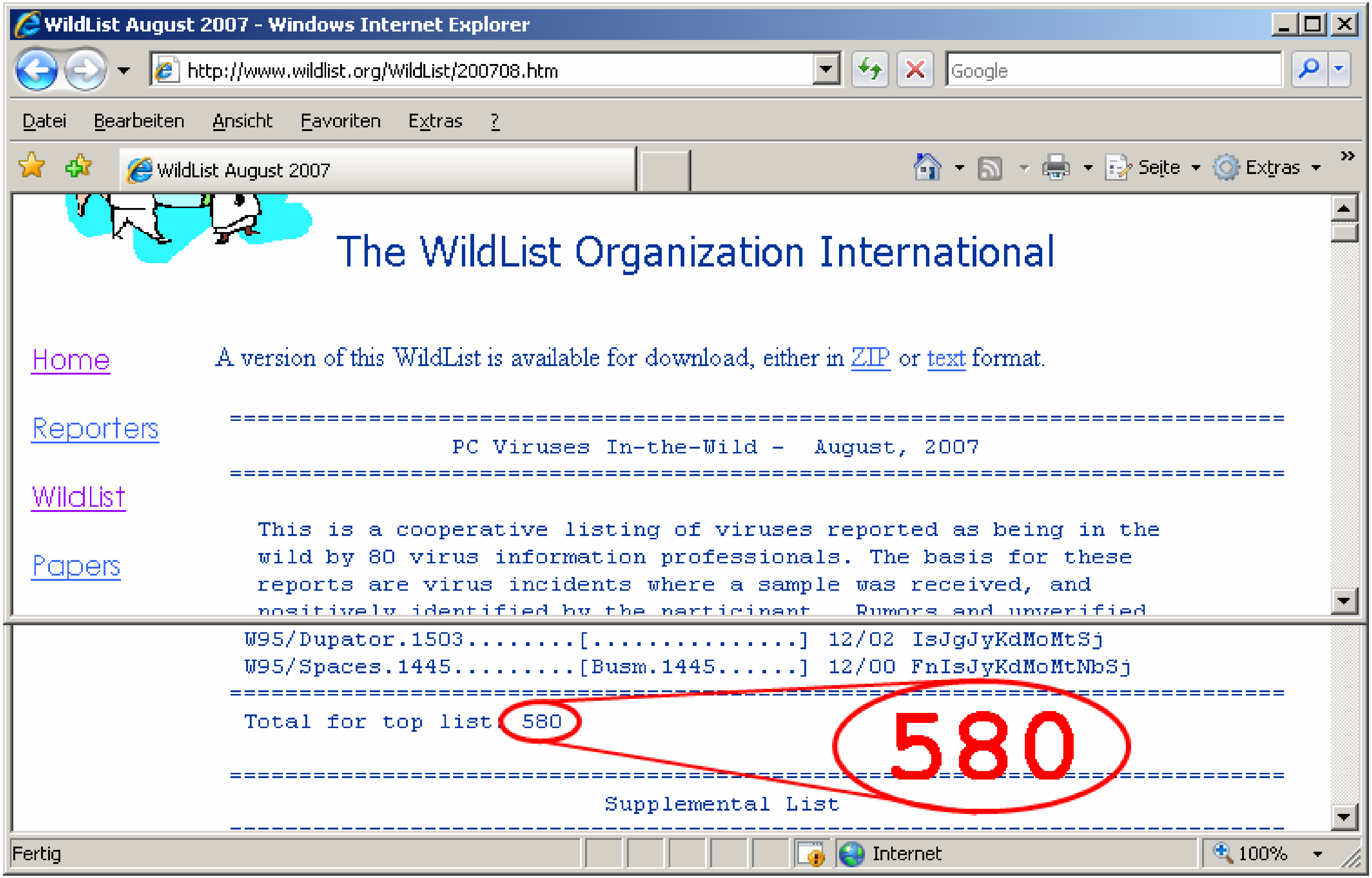
- Citing from McAfee’s VB 2007 paper

  “What a Waste – the Anti-Virus Industry DoS-ing Itself” [see page 134]:

  – “If we use the same criteria as the WildList (more than two reporters), and assume that the vast majority of malware these days is NOT zoo malware (zoo malware being that which is not seen in the wild), then **the WildList may be off by several more orders of magnitude** than even we have assumed.”

Introduction (III)

- Citing from the Fortinet’s VB 2007 paper “A Deeper Look at Malware – the Whole Story” [see page 205]:
  - “Since January 2005, based on Fortinet’s prevalence system […], there have been **20,000 malicious programs in the wild**. […] Each detection name may have hundreds or even thousands of variants associated with it (e.g. Tibs or Warezov with at least 6,000 variants and adware that has one name per ad company).”



WildList August 2007 - Windows Internet Explorer
http://www.wildlist.org/WildList/200708.htm
Google
Datei Bearbeiten Ansicht Favoriten Extras ?
WildList August 2007
Seite
Extras
Fertig
Internet
100%

The WildList Organization International

Home

Reporters

WildList

Papers

A version of this WildList is available for download, either in ZIP or text format.

```
==========================================================================
                  PC Viruses In-the-Wild -  August, 2007
==========================================================================

   This is a cooperative listing of viruses reported as being in the
   wild by 80 virus information professionals. The basis for these
   reports are virus incidents where a sample was received, and
   positively identified by the participant.  Rumors and unverified
```

```
  W95/Dupator.1503........[...............]  12/02 IsJgJyKdMoMtSj
  W95/Spaces.1445.........[Busm.1445......]  12/00 FnIsJyKdMoMtNbSj
==========================================================================
  Total for top list: 580

==========================================================================
                          Supplemental List
==========================================================================
```

580

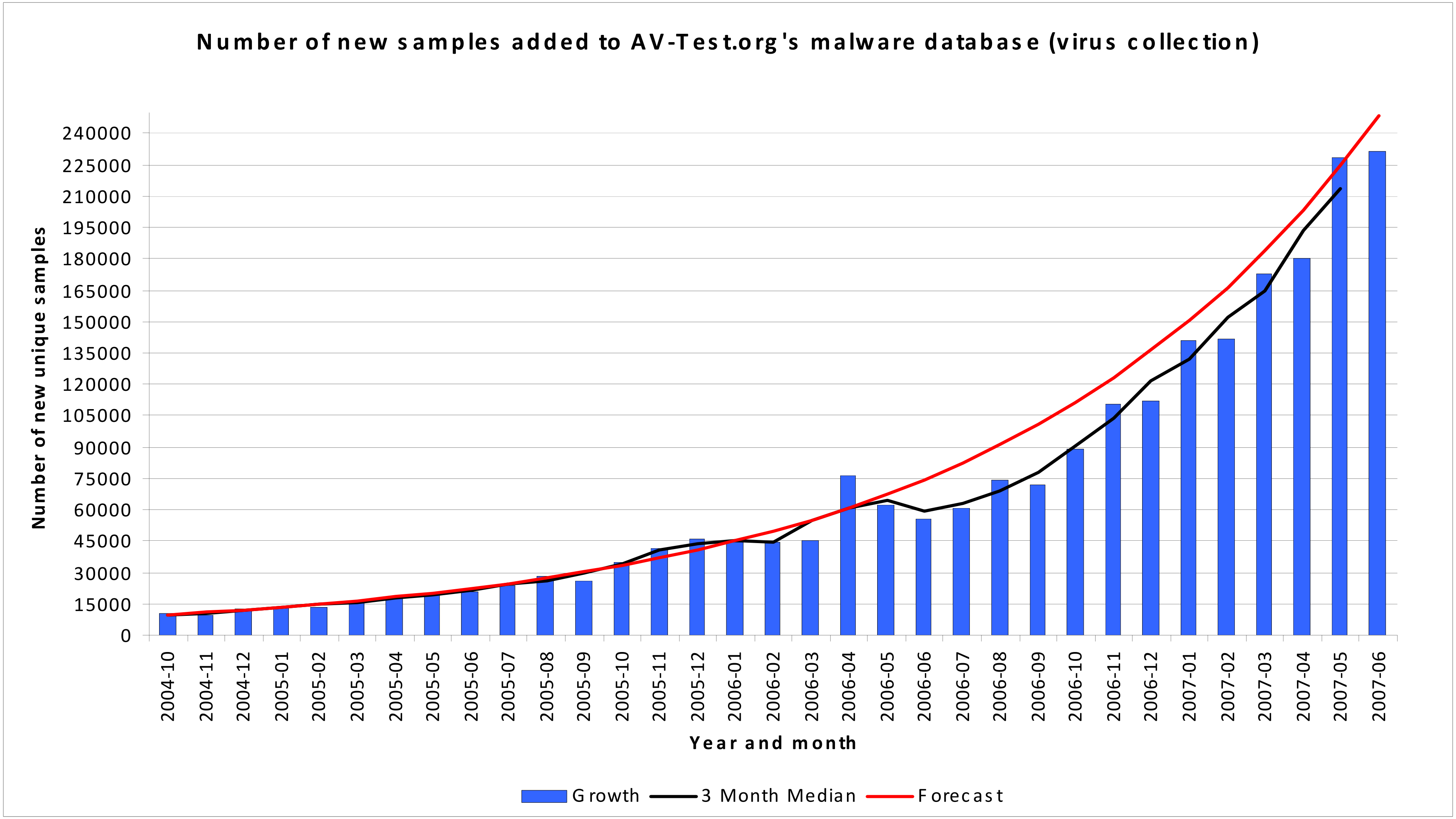
Problem 1: The Changing Threat Landscape

- The WildList only reflects viruses, worms and certain variants of bots running on Microsoft OS for PCs (e.g. Windows XP) which are able to replicate
- All other OS platforms like Unix, Linux, MacOS, Solaris as well as mobile platforms like Symbian or Windows CE are intentionally excluded
- All kind of Trojan Horses (e.g. password stealers and keyloggers), backdoors, exploits as well as ad- and spyware are intentionally excluded, too
- BUT this is the majority of today's malware!
  - Traditional viruses and worms died out, we're living in the world of a commercial malware industry

Problem 2: Number of Malware Samples (I)

- In 1996, we had an average of 8 viruses per month which were added to the WildList
- The maximum of newly added viruses was reached in 2005 with 36 samples per month
- In 2007 we have an average of only 20 samples which were added to the monthly WildList releases (with a minimum of 6 samples in March)
- BUT is this really a good reflection of today’s malware situation? Is the number of “in the wild” malware really that low?
- We have some different numbers from our lab…

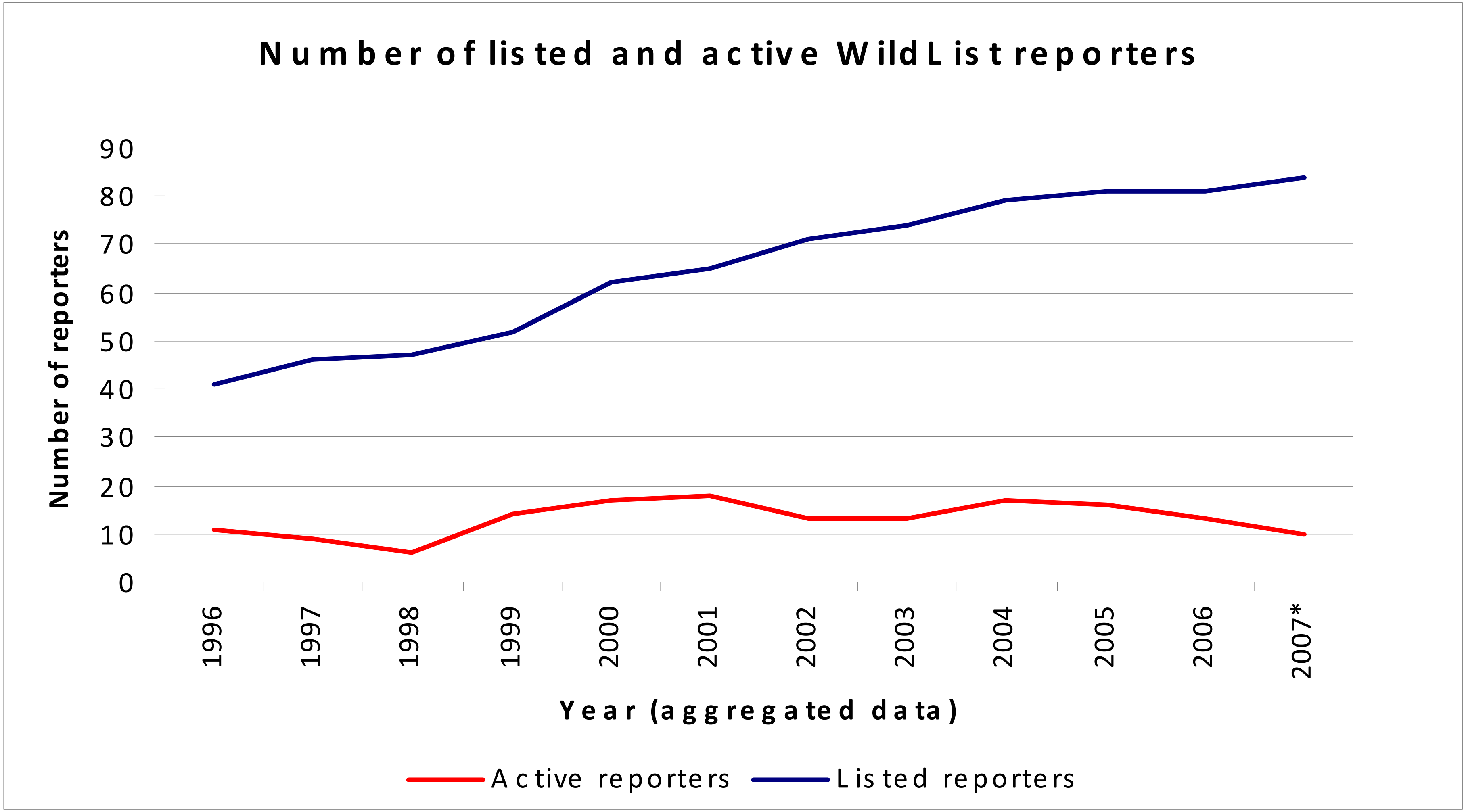
Problem 2: Number of Malware Samples (II)



Problem 3: Nobody Wants to Report (I)

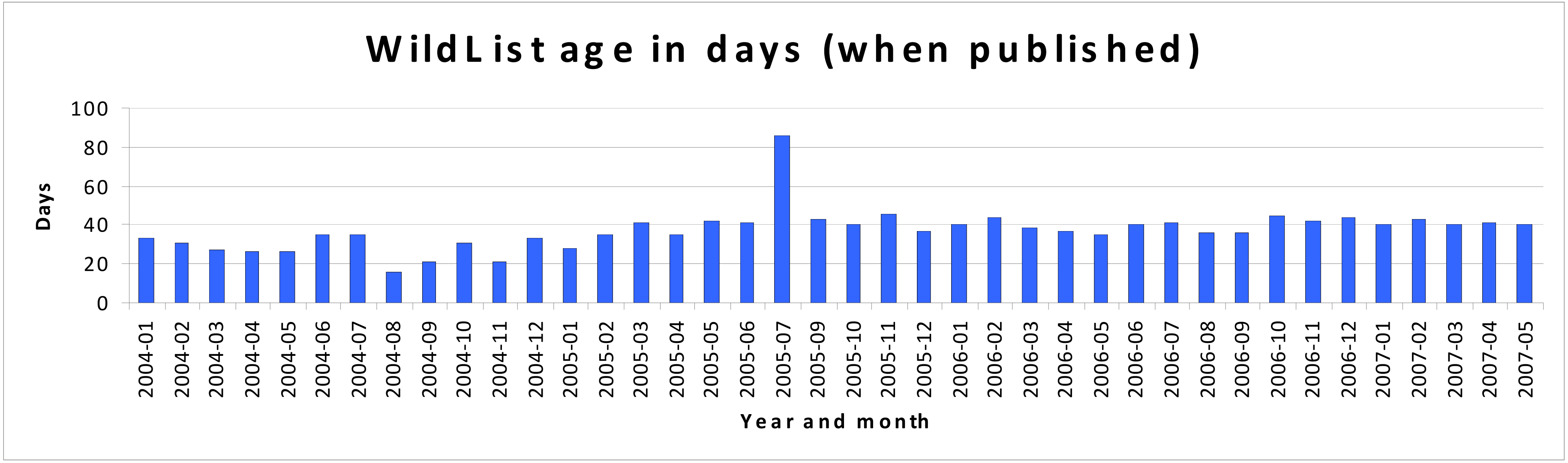
- The reporting process is too bureaucratic
  - Only individual, not corporate reporters are allowed
  - Reporters need to wait for a report form
  - When the report form arrives, there is just a small amount of time left to actually report something
  - All samples and related data are exchanged by e-mail in an unstructured format which can’t be handled by a machine, but by a human only
  - There is no confirmation of any report, so entries might or might not be added, updated or deleted
- Most reporters are working for AV companies
  - Is there really no conflict of interests?
- The number of active reporters is too low!

Problem 3: Nobody Wants to Report (II)



Problem 4: Outdated WildList

- New WildLists are usually published around 40 days after the end of the reporting period
- Statistics and samples are getting available to AV companies, testers and interested parties with this delay
- BUT is this really "up to date", is this "current" malware?



Suggestions “to Make it Better” (I)

- Change the definition of the WildList and extend it to non-selfreplicating malware and other platforms
  - Different WildList sections can be used for certain classes of malware as well as ad- and spyware
- Make it easier for reporters to report
  - Add “automatic reporting” features (where no or less human input is required), e.g. to include honeypots
  - Support more input systems than just e-mail
  - Extend the reporters to include more AV users, CERTs and other groups which are dealing with malware
  - Switch from individual to corporate reporting
  - Offer benefits for the best reports of active reporters (we’re speaking about quality, not quantity!)

Suggestions “to Make it Better” (II)

- More automatic processing is required
  - Use as many automatic systems as possible to process more samples in a timely manner
  - Only problematic or complex samples are left for manual handling (until further system improvements)
  - Don’t try to develop such tools at your own, but use commercial and open source software which is already available at the market and put everything together
- The WildList must be published more frequently (e.g. weekly instead of monthly) and a lot earlier
  - It requires a lot of work, of course… but…
  - With a good support of automation it’s possible to do it!

Conclusion

- Currently, the WildList has a lot of problems
  - Many of them are known for many years already, but they have never been addressed
  - Tests based on the WildList are still seen as “state of the art”, but are getting more and more meaningless
    - They are too easy to pass, good for marketing purposes, but doesn’t say anything about the real capabilities of AV programs
- Different AV companies are already offering better statistics of the current “in the wild” situation at their own websites (e.g. world virus maps)
- Important changes have to be implemented ASAP
  - Quite some time has passed by already…
  - So we have to act now, before it’s finally too late!

Questions & Answers

- ???

- Note: Many testing papers can be found at:
  http://www.av-test.org → Publications → Papers