McAfee®

Protect what you value.

Rebuilding Anti-Malware Testing for the Future

Dr. Igor Muttik, James Vignoles | McAfee | Avert Labs®

In the beginning, God created the Bit and the Byte. And from those he created the Word.

In the beginning, God created the Bit and the Byte. And from those he created the Word.

And there were two Bytes in the Word; and nothing else existed. And God separated the One from the Zero; and he saw it was good.

In the beginning, God created the Bit and the Byte. And from those he created the Word.

And there were two Bytes in the Word; and nothing else existed. And God separated the One from the Zero; and he saw it was good.

And God said - Let the Data be; And so it happened. And God said - Let the Data go to their proper places.

In the beginning, God created the Bit and the Byte. And from those he created the Word.

And there were two Bytes in the Word; and nothing else existed. And God separated the One from the Zero; and he saw it was good.

And God said - Let the Data be; And so it happened. And God said - Let the Data go to their proper places.

And God said - Let the computers be to process the Data. Thus God created computers and called them hardware.

In the beginning, God created the Bit and the Byte. And from those he created the Word.

And there were two Bytes in the Word; and nothing else existed. And God separated the One from the Zero; and he saw it was good.

And God said - Let the Data be; And so it happened. And God said - Let the Data go to their proper places.

And God said - Let the computers be to process the Data. Thus God created computers and called them hardware.

And there was no Software yet. But God created programs; good and bad... And told them - Go and multiply yourselves and fill all the Memory.

In the beginning, God created the Bit and the Byte. And from those he created the Word.

And there were two Bytes in the Word; and nothing else existed. And God separated the One from the Zero; and he saw it was good.

And God said - Let the Data be; And so it happened. And God said - Let the Data go to their proper places.

And God said - Let the computers be to process the Data. Thus God created computers and called them hardware.

And there was no Software yet. But God created programs; good and bad... And told them - Go and multiply yourselves and fill all the Memory.

And God said - I will create the AV Software; And the AV Software will check programs and govern over the computers and programs and Data.

In the beginning, God created the Bit and the Byte. And from those he created the Word.

And there were two Bytes in the Word; and nothing else existed. And God separated the One from the Zero; and he saw it was good.

And God said - Let the Data be; And so it happened. And God said - Let the Data go to their proper places.

And God said - Let the computers be to process the Data. Thus God created computers and called them hardware.

And there was no Software yet. But God created programs; good and bad... And told them - Go and multiply yourselves and fill all the Memory.

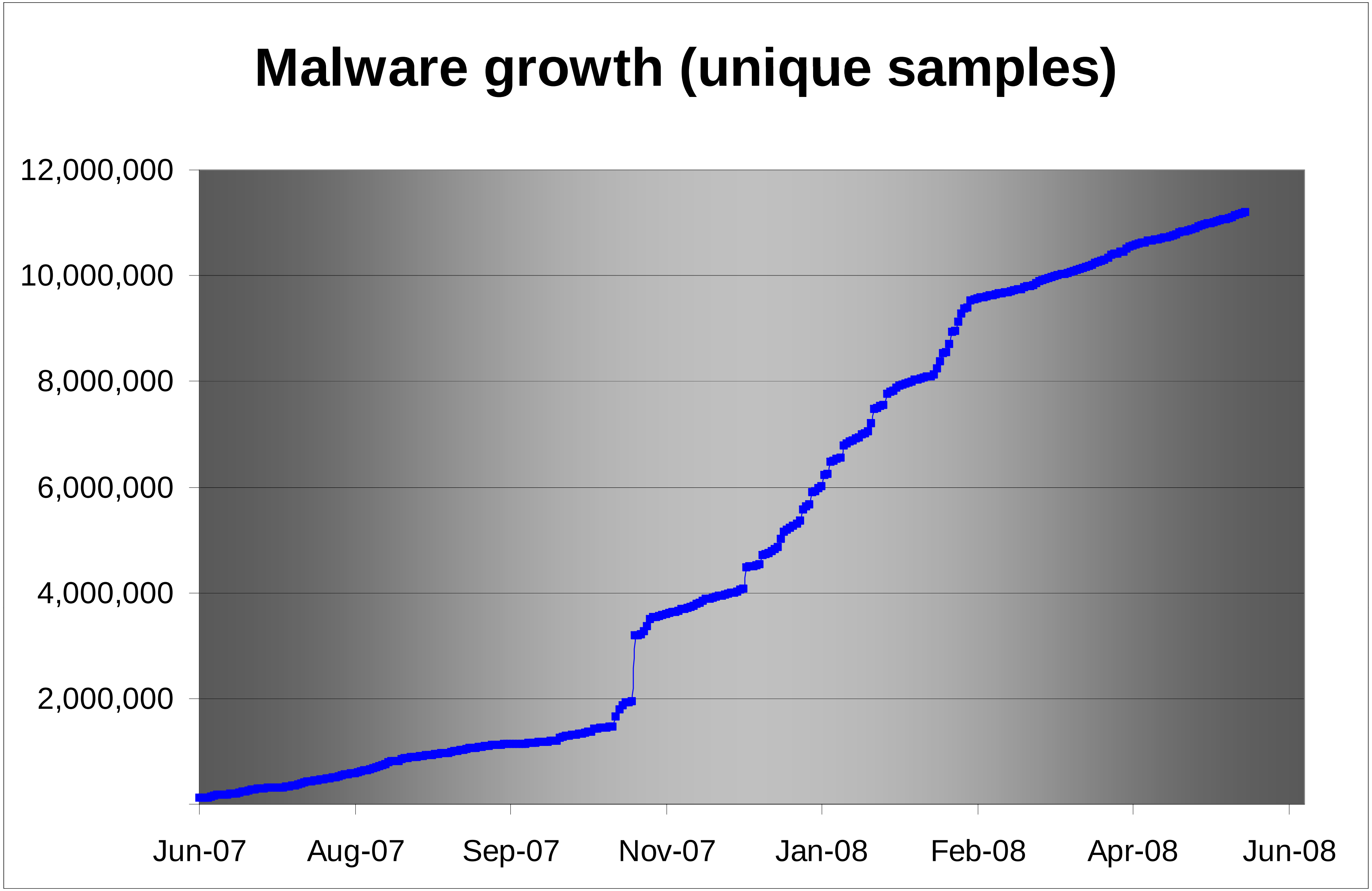
And God said - I will create the AV Software; And the AV Software will check programs and govern over the computers and programs and Data.

And God said – it is not good for AV Software to be alone. He took a bit from the AV Software's body and created a creature that would look up at the AV Software; and admire the AV Software; and love the things the AV Software does; and God called the creature: the AV Software Tester.

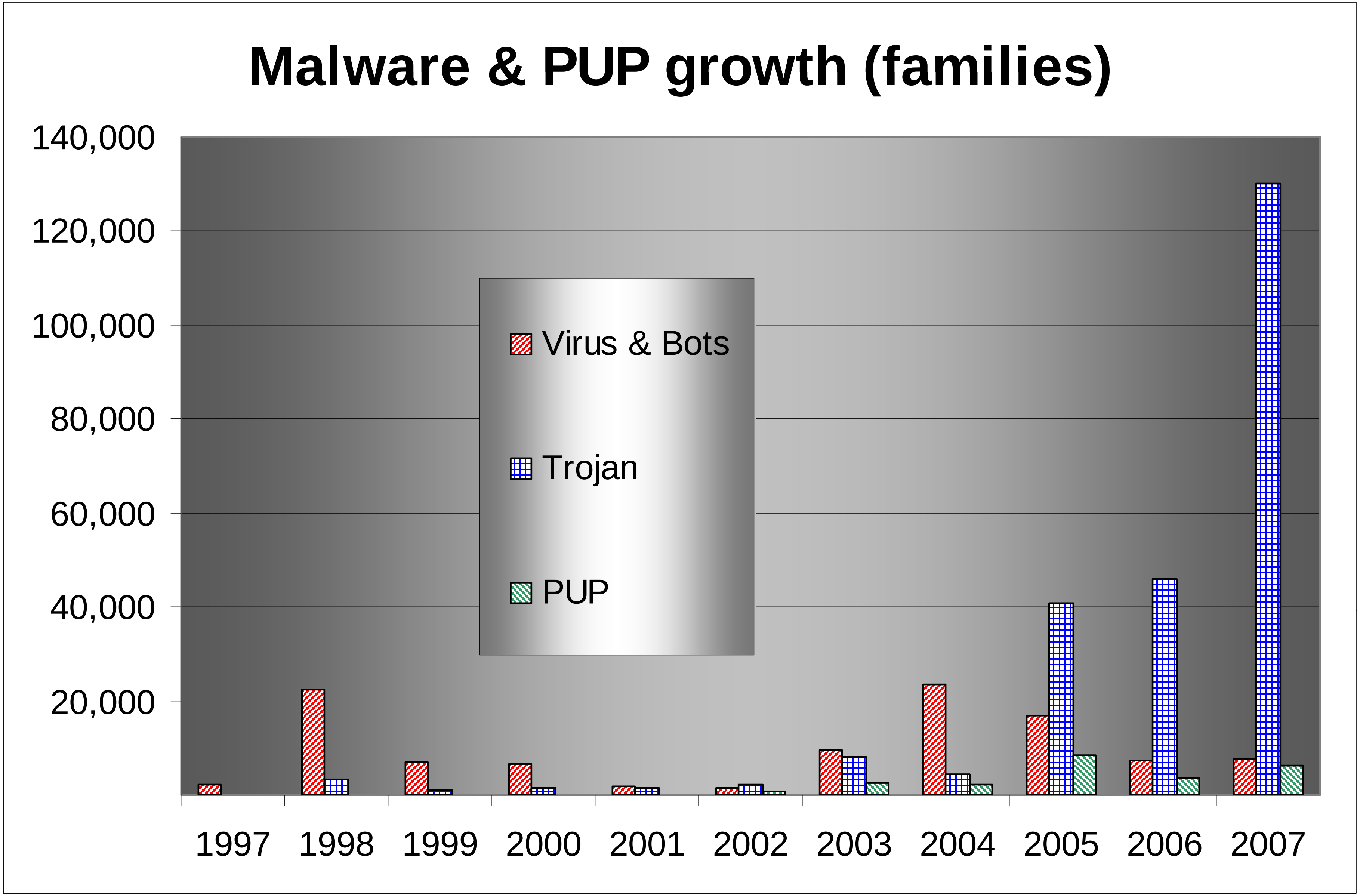
Agenda

- The evolution
  - Evolution of malware
  - Evolution of protection
  - Products become multi-dimensional
  - “Everything in, nothing out”
- Defining the test set
  - Reducing the test set
  - Importance of meta-data
- Suggestions for the future
  - AMTSO
  - Sharing meta-data
  - User and environmental profiles
  - Distributed testing
- Conclusion
- Questions

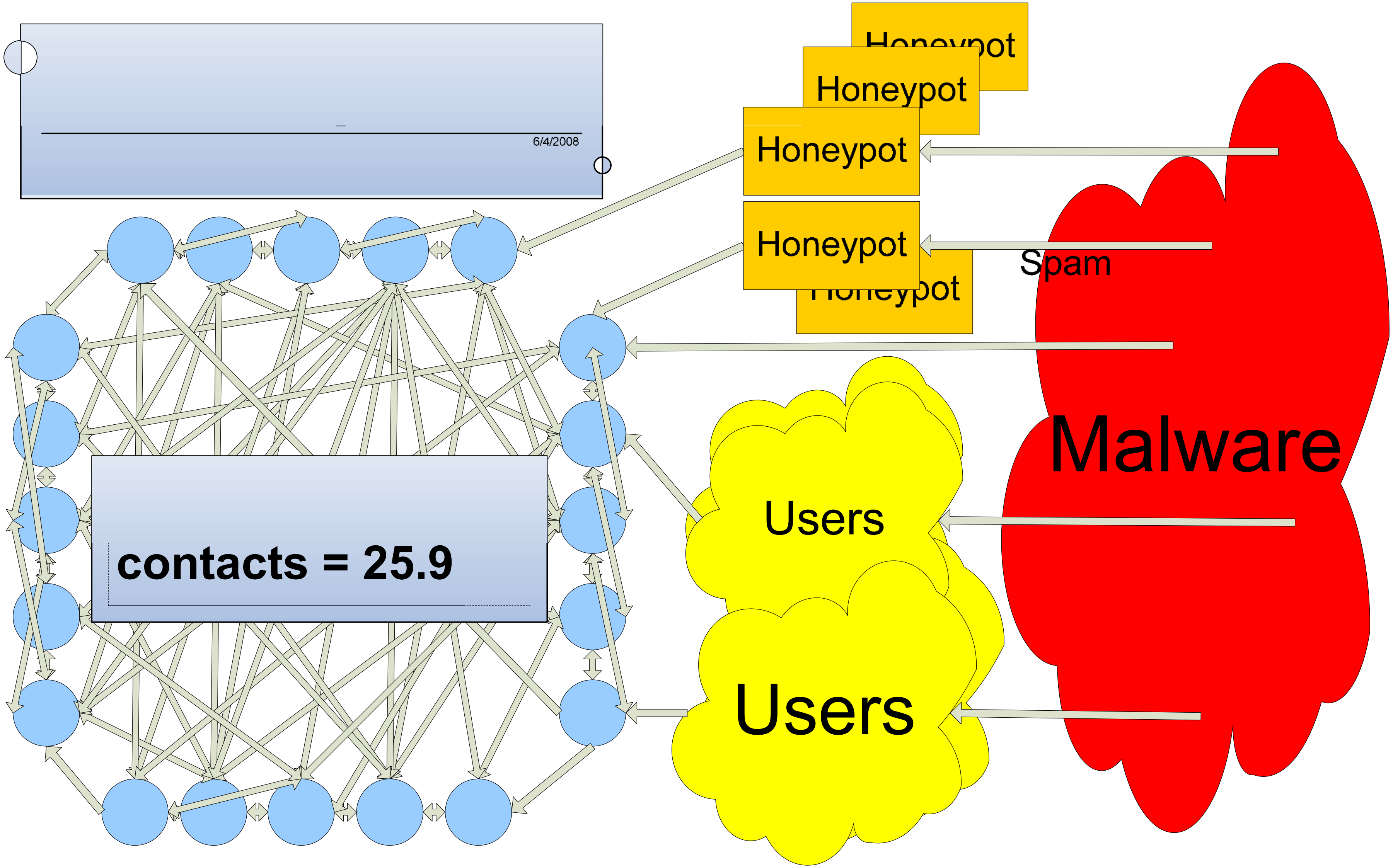
The Evolution



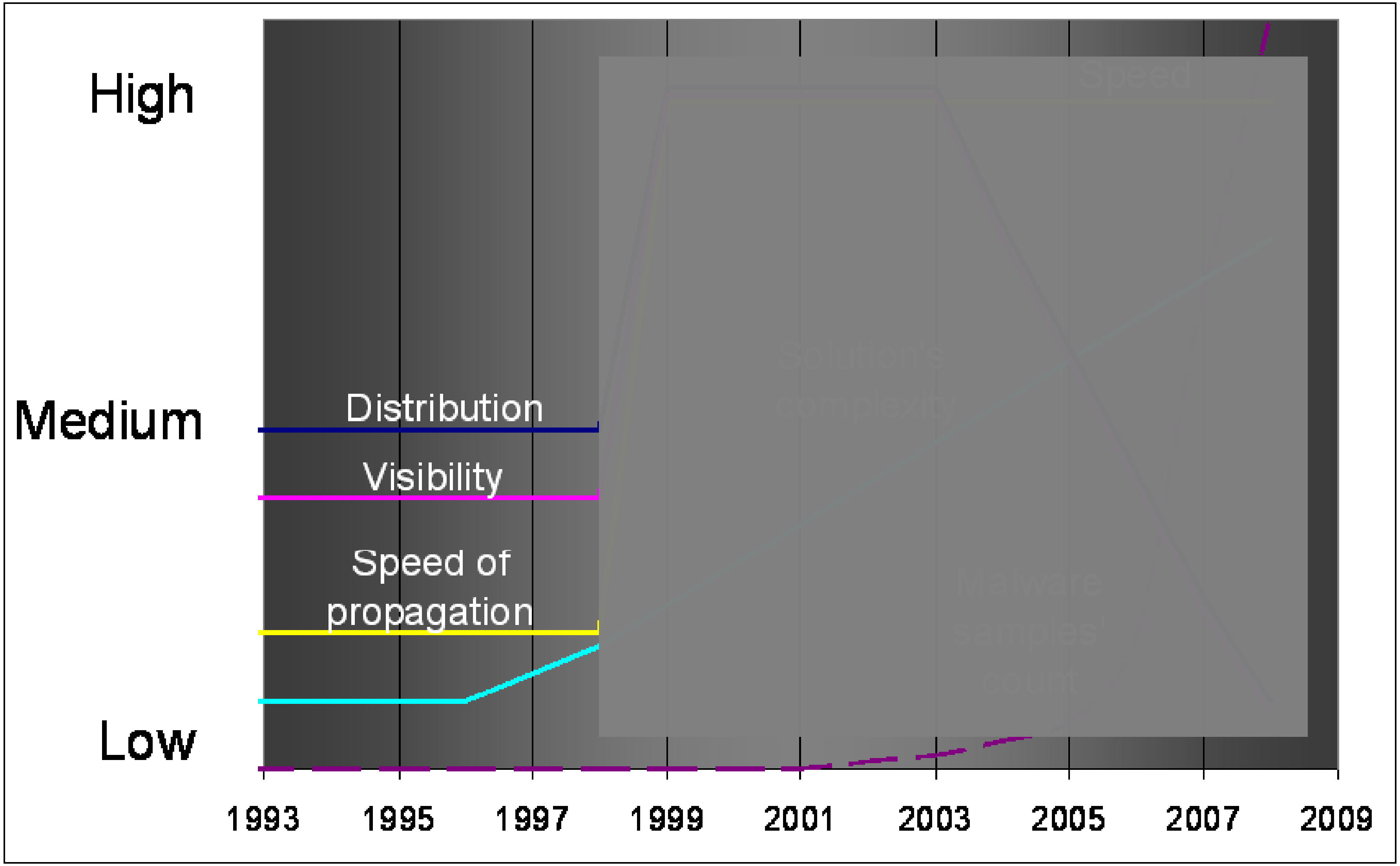
Source: McAfee Avert Labs


Malware & PUP growth (families)
140,000
120,000
100,000
80,000
60,000
40,000
20,000
Virus & Bots
Trojan
PUP
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007

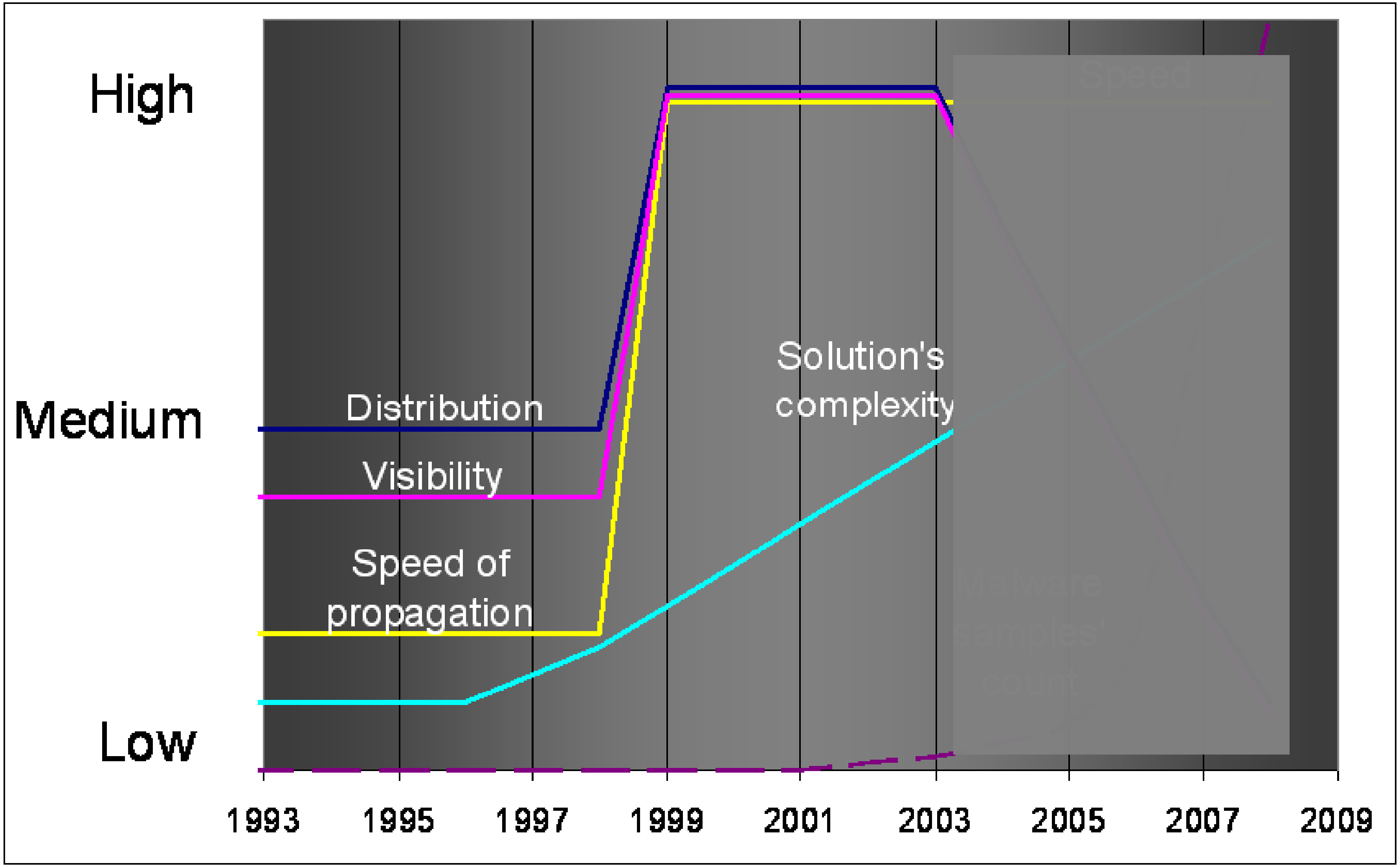
Distribution of samples



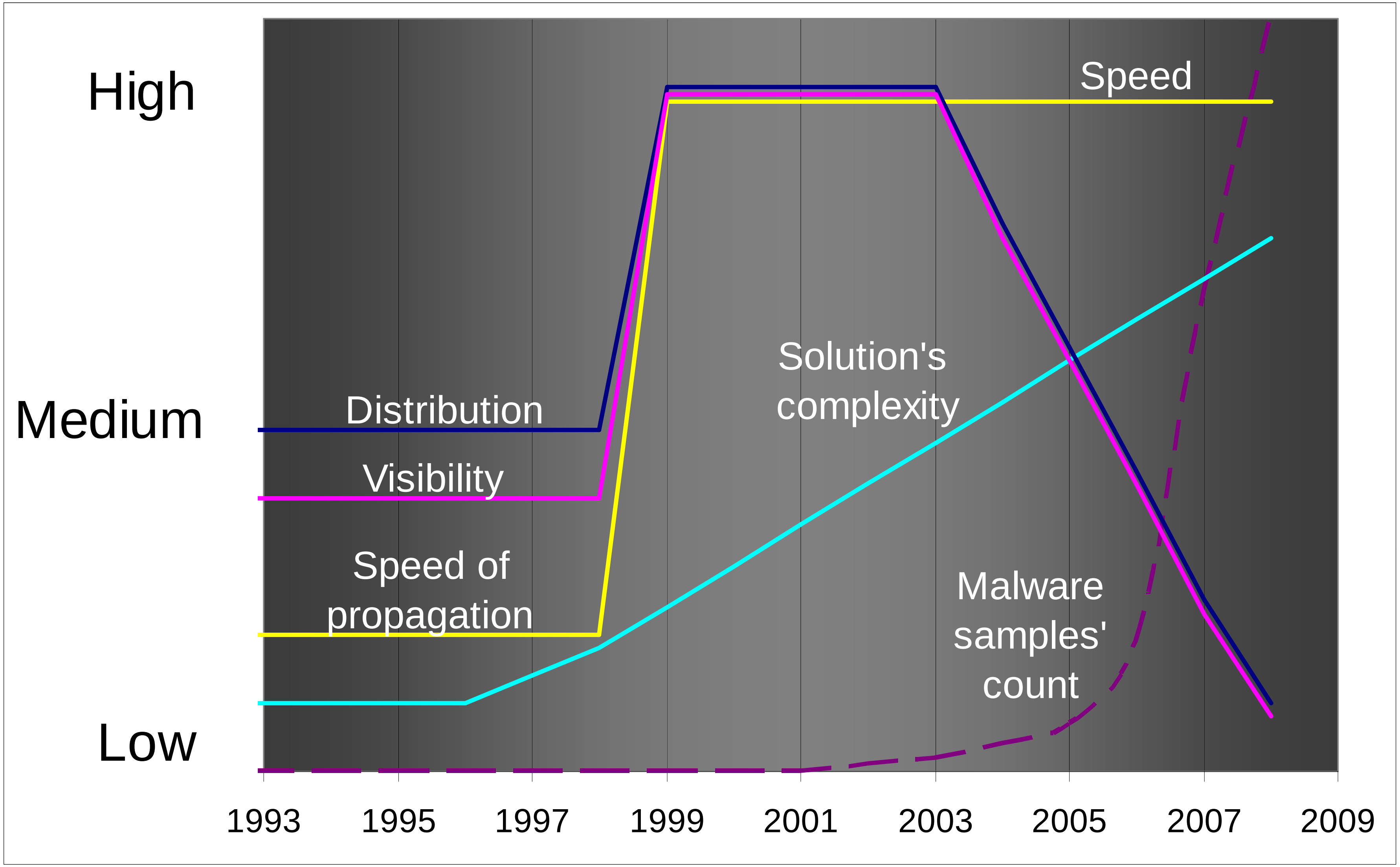
Evolution of malware



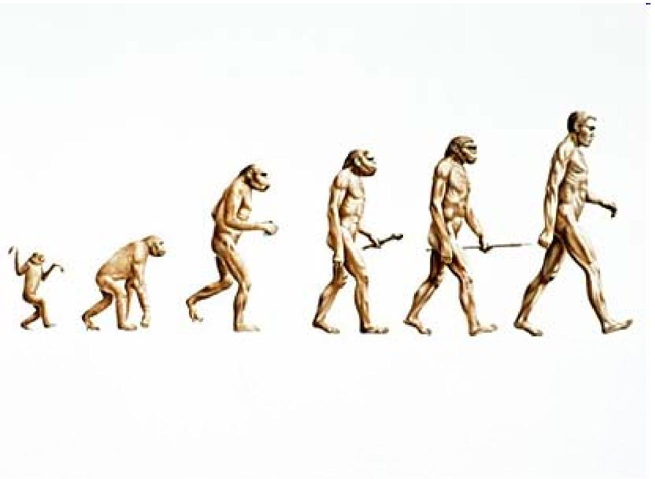
Evolution of malware



Evolution of malware

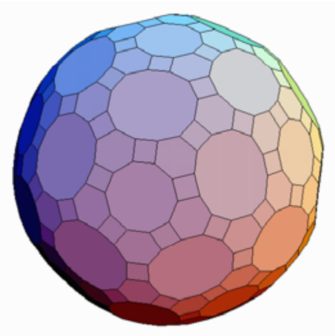


Evolution of protection



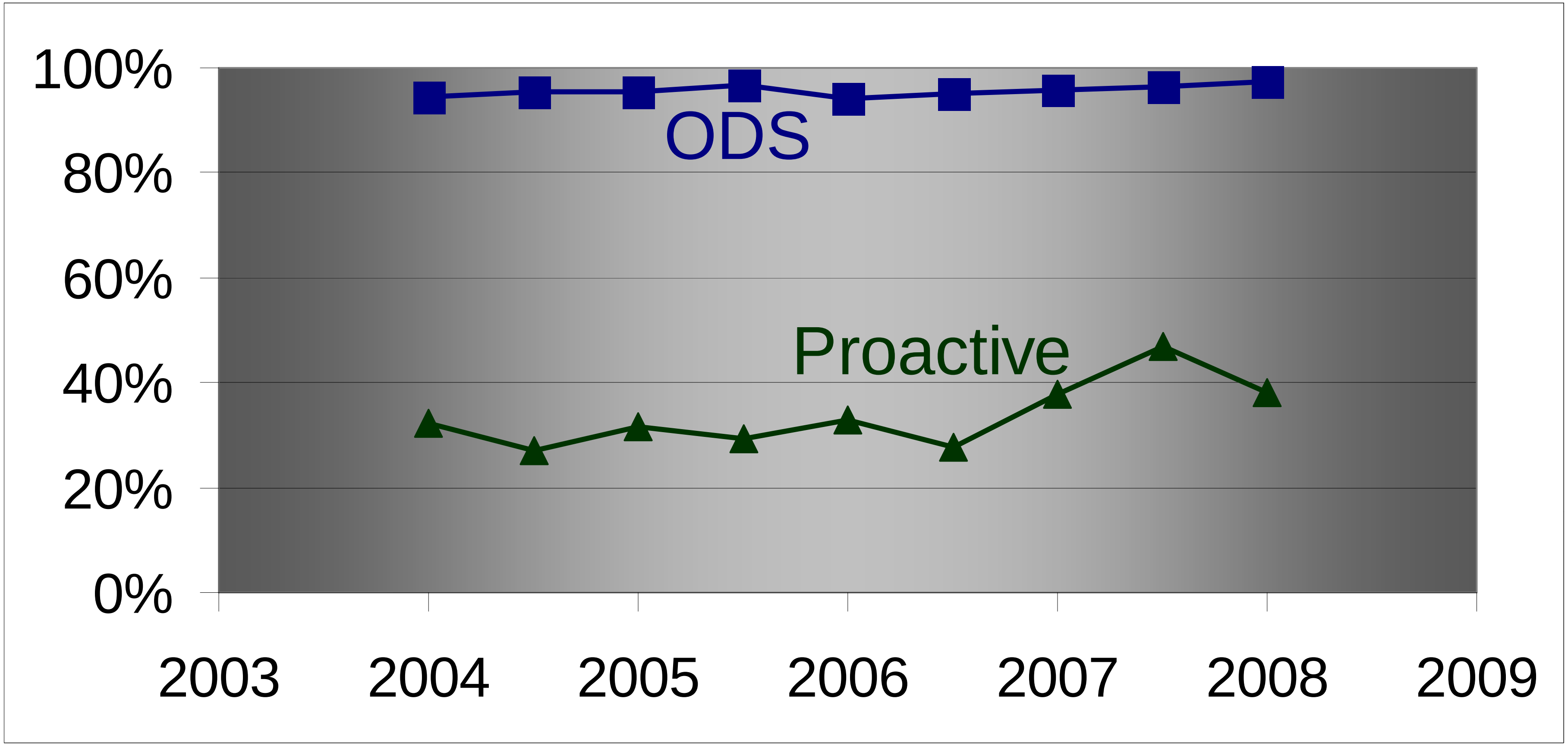
- Scanning was born in 1980-90s
  - Testing ODS over sample collection
  - Then it reflected user experience well
- Assumption was that every piece of malware will be re-used
  - Getting less and less true
  - If not re-used – why detect by a scanner?
  - That means the meta-data (commonality, age) is very important
- Measuring the quality by scanning past threats is getting progressively less relevant

Multi-dimensional products = multi-dimensional testing



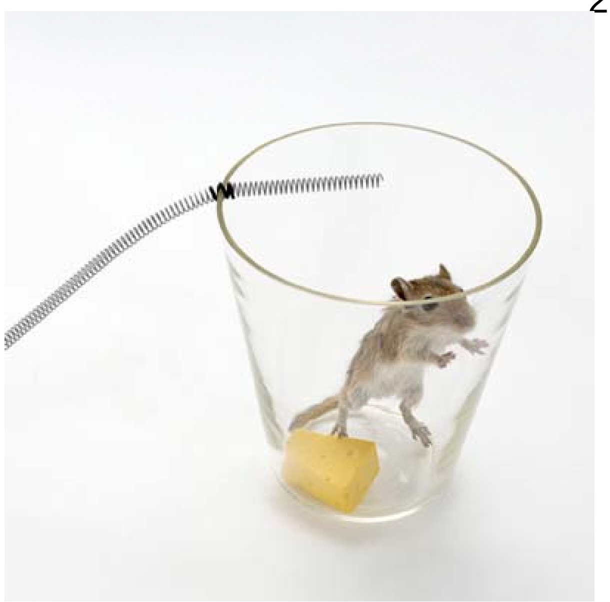
- Extreme growth in malware count is due to how successful AV products are
- Scanners are “testable” by the bad guys
- Solution - proactive multi-dimensional security products
  - Behavioral
  - Herd intelligence and field telemetry
  - Instant updating
  - Web filtering/reputation
  - Anti-spam
  - Access-protection rules (e.g. - no PEs in %TEMP%)
  - White-listing, black-listing (files, URLs, IPs, etc.)
- So testing also have to change

Industry average detection rates



Based on data from AV-Comparatives.org

Everything in, nothing out



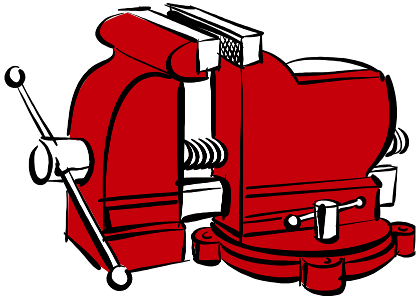
- Test sets rarely shrink
  - Dropped DOS viruses
  - Dropped Word6 macros
- Today viruses are out-numbered by short-lived trojans
- What mechanisms are available to track threats’ commonality and ageing?
  - Sample counts, telemetry in AV products
  - Virtually none available to the testers
- Anti-Spam model
- Concerted effort to retire threats

Accuracy and reproducibility

- “Freezing” the solutions tested
  - — Repeatability
  - — Verifiability
  - — Controlled changes
- Some solutions cannot be “frozen”
  - — If they rely on dynamic online database
    - Protection in-the-cloud
    - Managed services
  - — If security software modifies itself
    - For example – old threats are “aged out”
    - Or if there is artificial intelligence (self-modifiable database of detection or behavioral rules)
  - — Comprehensive logging
    - Verifiable but not repeatable

Defining the test set

Reducing the test set



- Can we test against all samples? Yes.
- Do we need to test against all samples? No.
- Need info about what can be removed
  - Meta-data about age and commonality
  - Verify sample’s viability
  - Periodically verify samples again
- Weeding the test set is a not a one-off exercise
  - Malware also uses “in-the cloud” technology
  - Malware test set cannot be frozen either!

Do no harm

- Sample testing requires execution
- Leaks from the laboratories
  - Isolated networks
  - Simulated Internet
  - Risks of DDoS, spam, data leakage
- Solutions
  - Filtering firewalls (automatic and interactive)
  - Logging and playback of network traffic

Example – many HTML samples

- Encrypted/encoded HTML

```
<Script Language='Javascript'>
<!--
document.write(unescape('%3C%41%20%68%72%65%66%3D%68%74%74%70%3A%2F%2F
%77%77%77%2E%62%61%64%2E%62%69%7A%3E%3C%69%6D%67%20%73%72%63%3D%68%74
%74%70%3A%2F%2F%77%77%77%2E%62%61%64%2E%62%69%7A%2F%6D%61%6C%77%61%72
%65%2E%65%78%65%20%77%69%64%74%68%3D%31%20%68%65%69%67%68%74%3D%31%3E%0A'));
//-->
</Script>
```

- Contains a script
- With only a link inside
- Link is frequently inactive
- Is this a valid malware sample?
- Are spammed downloaders?

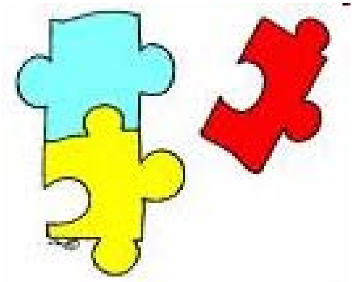
Example – many HTML samples

- Encrypted/encoded HTML

```
<A href=http://www.bad.biz><img src=http://www.bad.biz/exploit.jpg
width=1 height=1>
```

- Contains a script
- With only a link inside
- Link is frequently inactive
- Is this a valid malware sample?
- Are spammed downloaders?

Test sets



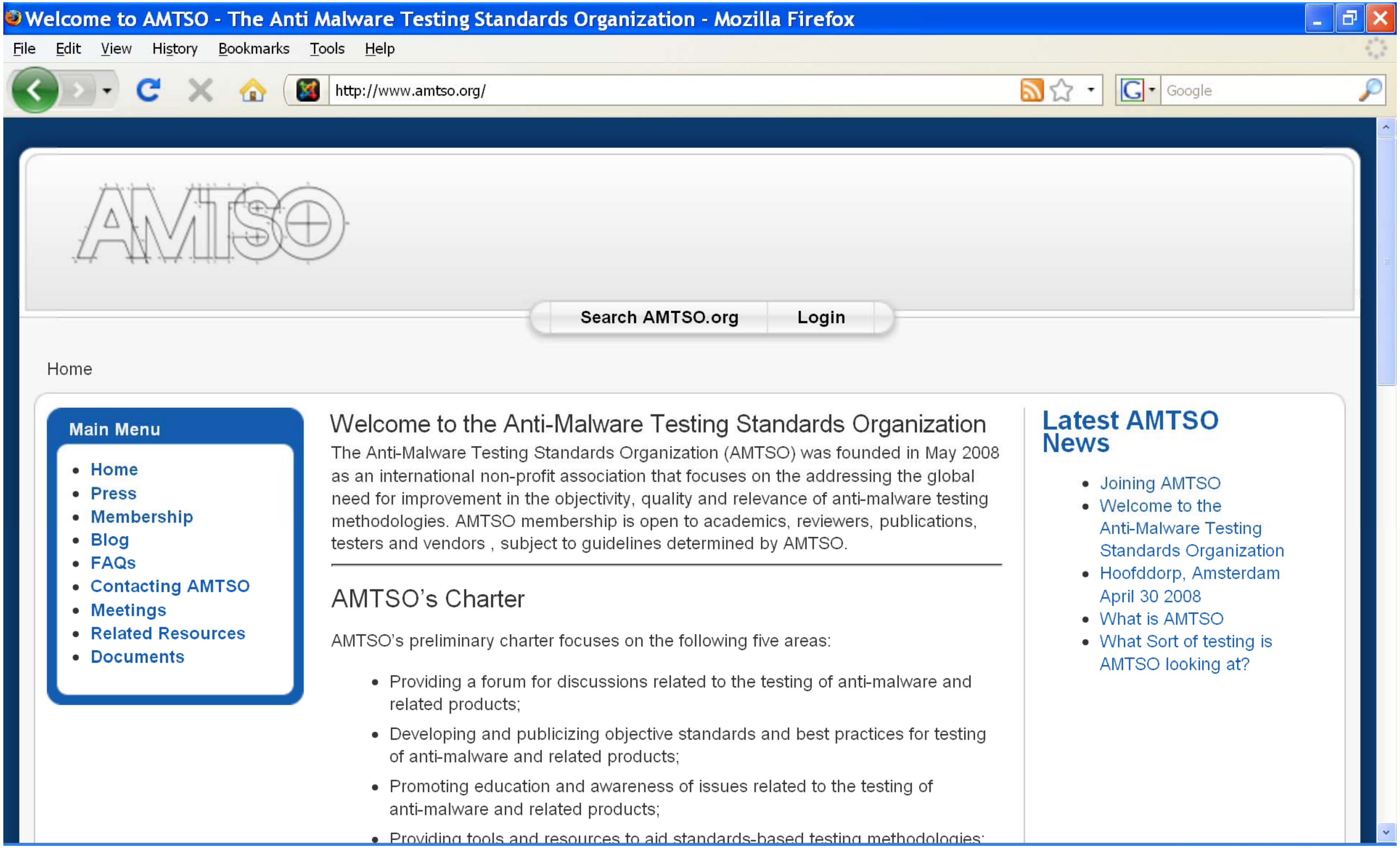
- Weeding and sorting
- Reducing the size but keeping relevant
  - Small set will produce random results
  - Ranking threats using field telemetry
  - Removing short-lived and inactive threats
  - Excluding most HTMLs
  - Grouping threats (“attack groups”)
  - “Chopping the tail”
- Meta-data needed
  - Sharing meta-data
  - Standard for meta-data is needed
- Same applies to clean set – commonality & age

Suggestions for the future

“Hard core” collections

- Test what is not commonly known
- Identify samples detected by the majority
- Exclude these samples – test the rest
- No bias in favour of products used for selection
- Recognizing and resolving the bias
  - Geographical
  - Timing

AMTSO – www.amtso.org



Welcome to the Anti-Malware Testing Standards Organization

The Anti-Malware Testing Standards Organization (AMTSO) was founded in May 2008 as an international non-profit association that focuses on the addressing the global need for improvement in the objectivity, quality and relevance of anti-malware testing methodologies. AMTSO membership is open to academics, reviewers, publications, testers and vendors , subject to guidelines determined by AMTSO.

AMTSO's Charter

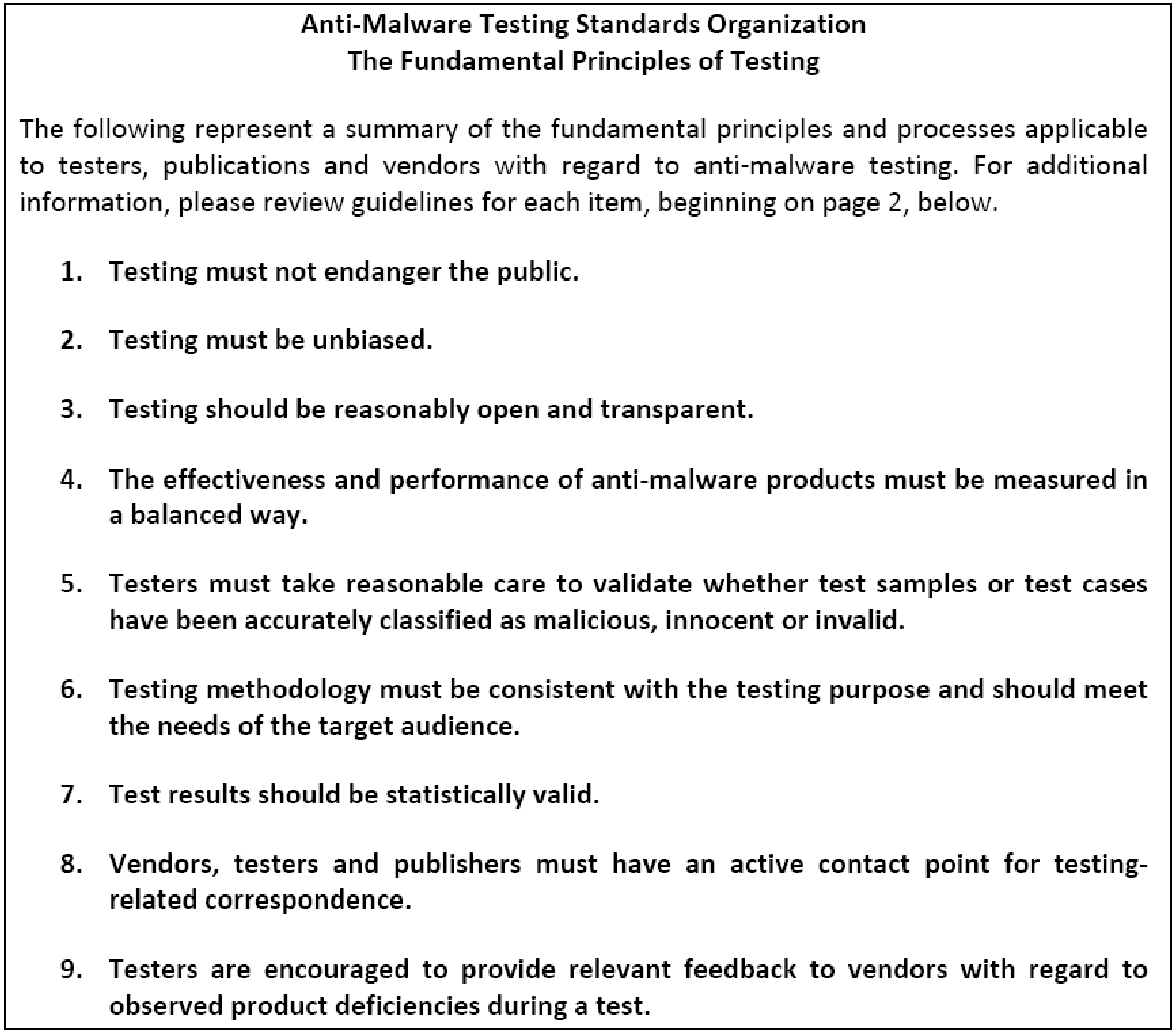
AMTSO's preliminary charter focuses on the following five areas:

- Providing a forum for discussions related to the testing of anti-malware and related products;
- Developing and publicizing objective standards and best practices for testing of anti-malware and related products;
- Promoting education and awareness of issues related to the testing of anti-malware and related products;
- Providing tools and resources to aid standards-based testing methodologies;

Latest AMTSO News

- Joining AMTSO
- Welcome to the Anti-Malware Testing Standards Organization
- Hoofddorp, Amsterdam April 30 2008
- What is AMTSO
- What Sort of testing is AMTSO looking at?

AMTSO principles



Anti-Malware Testing Standards Organization
The Fundamental Principles of Testing

The following represent a summary of the fundamental principles and processes applicable to testers, publications and vendors with regard to anti-malware testing. For additional information, please review guidelines for each item, beginning on page 2, below.

1. **Testing must not endanger the public.**
2. **Testing must be unbiased.**
3. **Testing should be reasonably open and transparent.**
4. **The effectiveness and performance of anti-malware products must be measured in a balanced way.**
5. **Testers must take reasonable care to validate whether test samples or test cases have been accurately classified as malicious, innocent or invalid.**
6. **Testing methodology must be consistent with the testing purpose and should meet the needs of the target audience.**
7. **Test results should be statistically valid.**
8. **Vendors, testers and publishers must have an active contact point for testing-related correspondence.**
9. **Testers are encouraged to provide relevant feedback to vendors with regard to observed product deficiencies during a test.**

For better testing

- Follow AMTSO principles (www.amtso.org)
- Testing “whole solution” is always better
  - Protection at the point of delivery (SMTP / HTTP / POP3 / IM / P2P scanner)
  - Threat class – for example:
    - Rootkits
    - Parasitic viruses
    - Malware that does data exfiltration
  - Cleaning
- The user and the environment profile
  - A script simulating specific user behavior (“GUI monkey”)
    - Internet surfer
    - P2P or IM user, etc.

Distributed live testing

- Common AV testing plug-in
  - Installs alongside AV
  - Tracks security responses and submit logs
  - “Retrospective telemetry”
  - Like SETI@Home
  - Allows for retrospective analysis of product efficacy
  - Can be open-source
- Collect user feedback
- Combining objective and subjective measurements

Conclusions

- Testing is no longer a simple task
- Great synergy in the industry - AMTSO
- Collect and standardize telemetry meta-data
- Share it and use it – for dev and testing
- We are optimistic

Questions, please

mig@mcafee.com