Beyond Testing: What Really Matters

Andreas Marx
CEO, AV-TEST GmbH
AGENDA

About AV-TEST GmbH

Some Numbers and Statistics

Innovations and Presentations

Summary

Q&A
The AV-TEST Institute in Magdeburg/Germany – Hightech in historical ambience
We are a global acting and independent service provider in the field of IT security and antivirus research.

We have almost 20 years of experience in the field of malware and antivirus software.

We process more than 1.000 Terabyte testing data, including 120 million clean files and 150 million malware samples.

We feature more than 1 Petabyte storage space, with over 300 client and server systems.

We offer 30+ employees and several students a secure, variable and interesting position.
At AV-TEST, we're registering about 200,000 to 250,000 new unique malware samples a day.
And increasing number of them are related to the Android (mobile) platform.
Number of files vs. number of different exploits (CVE entries)
The story so far

AV-TEST was founded

2002 Porn Dialers

2002 Retrospective Testing

2003 Disinfection Disasters

2004 Outbreak Response Times

2005 Insecurity in Security Software

2007 'Dynamic Detection' Testing (Real World)

2007 The WildList is Dead

2009 Exploit Prevention Testing (Real World)

2009 'In-the-cloud' Scanning

2012 Android Security Product Testing

2013
Retrospective Testing - How Good Heuristics Really Work

VB Conference 2002

At the time of writing, this was a state-of-the-art single-feature test but such tests are now obsolete, as on-demand tests are outdated and you cannot “freeze” AV updates anymore and cloud access should not be limited, and not single features should be tested anymore.
(Porn) Dialers - Another Class of Malware?

VB Magazine 12/2002

At that time, dialers were a heavy problem to the Windows world, now the problem has shifted to mobile phones (especially in the Android space), calling expensive numbers or sending out text messages.
INNOVATIONS AND PRESENTATIONS

The Sober Effect: Disinfection Disasters

VB Magazine 12/2003

- Products had problems to effectively clean-up infected systems, e.g. due to the self-protection of malware (tasks cannot easily be killed)

- Fact: Repair is still one of the most challenging things these days

- Many more papers and presentations by us followed, still disinfection is often not tested at all or not tested properly
Antivirus Outbreak Response Testing and Impact

VB Conference 2004

• “How long does it take until signature updates are publicly available in cases of major worm outbreaks?”

• Still a valid question, but replace the word “outbreaks” with “background noise malware”, something around 200,000 unique samples per day

• Ideal protection is when the malware is blocked at the time it arrives at the system (it doesn’t matter if this is an hour or just a minute before, as long as the system is not compromised)
Insecurity in Security Software

VB Conference 2005

- The paradox: Security software is meant to secure the system, but nowadays it introduces new security holes. Every error could be security relevant when it happens in security software!

- Trustworthy computing development lifecycle:
  - Secure by design, Secure by default, Secure in deployment, Communications
The WildList is Dead, Long Live the WildList!

VB Conference 2007

- Problems at this time: The Changing Threat Landscape, Number of Malware Samples, Nobody Wants to Report, Outdated WildList
- Problems today: The Changing Threat Landscape, Number of Malware Samples, Nobody Wants to Report, Outdated WildList
- Quite a lot of suggestions have been made “to make it better”
- Main issue: WildLists tests are easy to pass (you know the test set in advance), they are good for marketing purposes, but doesn’t tell you anything about the real capabilities of AV programs
Testing of 'Dynamic Detection'

AVAR Conference 2007

- Historic: Static detection as part of the “traditional” way of AV testing
- Newly introduced: Dynamic detection -- and we demonstrated how to test it
- First full-feature “Real World” test description presented more than 6 years ago (the first “Real World” tests have started earlier in the year 2007)
- “Ideal setup”: real (not virtualized) hardware, base system with recent operating system and patch level, default settings of products under test, high volume and many different malware types, use the appropriate introduction vector (e.g. e-mail, web, download, P2P, USB key, network port), “Record the impact of the security software and compare the result to the actions of the malware on the clean base system”, check for detection, reporting and blocking
- With some minor changes, most parts of the setup are still valid
INNOVATIONS AND PRESENTATIONS

Why ‘In-the-cloud’ Scanning is not a Solution

VB Conference 2009

- ‘In-the-cloud’ scanning is helping the vendors to get their static detections rate up
- With reputation systems and further statistical analysis, those approaches can help even further in detecting malware
- But: ‘In-the-cloud’ scanning is still only a part of a whole security infrastructure (and not every product can access the cloud, e.g. in critical infrastructures)
- New (much better!) developments these days: reputation services instead of “pure” blacklisting and whitelisting
Testing Exploit-Prevention Mechanisms in Anti-Malware Products

CARO Workshop 2009

- Extension to the “Real World” testing methodology from 2007 to cover drive-by attacks etc.
- Testing needs to reflect these additional protection mechanisms: Whole product evaluation instead of only testing (possibly misleading) on-demand scanning capabilities
INNOVATIONS AND PRESENTATIONS

AV-TEST was founded

2002 Porn Dialers
2003 Disinfection Disasters
2005 Insecurity in Security Software
2007 'Dynamic Detection' Testing (Real World)
2009 Exploit Prevention Testing (Real World)
2013

2002 Retrospective Testing
2004 Outbreak Response Times
2007 The WildList is Dead
2009 'In-the-cloud' Scanning
2012 Android Security Product Testing

Android Security Product Testing

AVAR Conference 2012

- Wrong focus in past: Are malware detection and all the other technical features really the most important items?
- Problem: Results don’t help the user to choose the “right” product, according to his or her needs

What really matters: What happens when I lose my phone?
- Can I get it back?  →  Anti-Theft (Locate Device)
- Is my data safe?  →  Remote Wipe, Remote Lock, Encryption
- Can I get my data back?  →  Online Backup
- Is my privacy ensured?  →  Which apps spy on me and can security software tell me and protect me?
- Is malware or adware a problem for me?  →  Malware and PUA Detection rates
- I want to protect my child from inappropriate content on the phone.  →  Parental Control
A wide range of other security-related areas are covered, too, e.g.

- “Spam – More Dangerous than Ever Before”
- “Google vs. Bing: Search Engines Deliver Infected Websites as Their Top Results”
INNOVATIONS AND PRESENTATIONS

Find our research papers and conference presentations on www.av-test.org/en/publications
Thank you for your kind attention!
Are there any questions?