AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

Malware Removal – Beyond Content and Context Scanning

Tom Brosch, Maik Morgenstern
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

Copyright © 2007 AV-Test GmbH

Table of Contents

Copyright © 2007 AV-Test GmbH

Malware Removal

- Why...
  - … is **Malware Removal** necessary?
  - … is comprehensive **Malware Removal** necessary?
  - … is **Malware Removal** a lot of work and a problem?

Copyright © 2007 AV-Test GmbH

Why is Malware Removal necessary?

- Systems still get infected for different reasons
  - Users install an Anti-Malware software when it is too late …
  - Users update an Anti-Malware software when it is too late …
  - Anti-Malware vendors react when it is too late …
- These systems have to be cleaned

Copyright © 2007 AV-Test GmbH

Why is Comprehensive Malware Removal Necessary?

- Comprehensive Malware Removal?
  - Malicious processes should be terminated and the related executables be removed
  - What about Run keys in the Registry?
  - What about settings changed by the malware?
  - What about other components, like image files or configuration files used by the malware?
- Why care?
  - Because the user cares
  - They are looking for a “really clean” system, since that’s what they pay for
  - Risk of reinfection when missing components or system changes
  - Another security product might “detect” the leftover components and leave the user in an uncertain state
  - Rogue Anti-Spyware products are producing false positives at the moment, they might happily switch to the leftover components

Copyright © 2007 AV-Test GmbH

Why is Malware Removal a Lot of Work and a Problem?

- To have proper removal routines in place, a lot of analysis work by the Anti-Malware vendor is required
  - Different behavior of malware on different systems
  - Behavior of malware may change over time (downloaded components)
  - Threats are way more complex today
- The increasing amount of malware is not going to make it better
- Bad removal routines indicate a bad analysis, which doesn't increase the trust of users in the software

Copyright © 2007 AV-Test GmbH

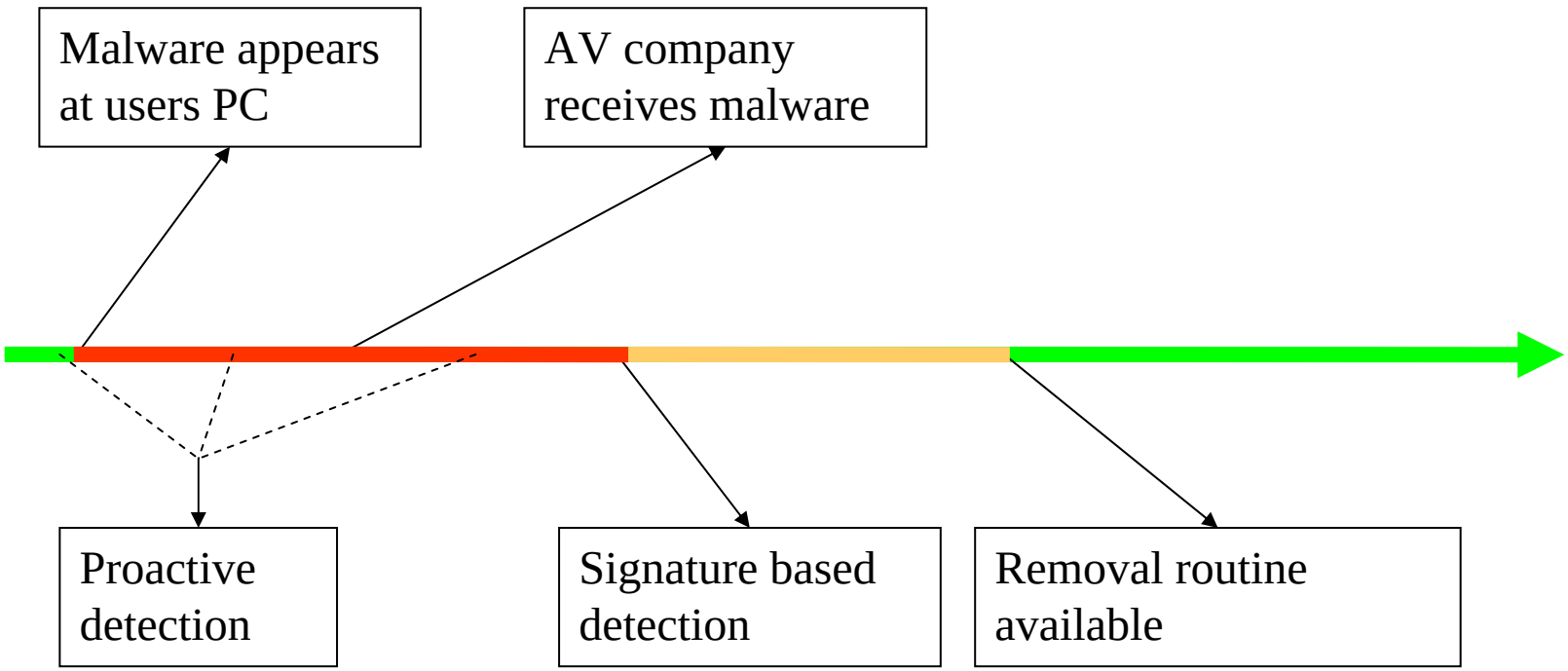
Content and Context Scanning

- Content scanning uses signatures to identify malicious components
- Context scanning uses context rules to identify linked malicious components
- A combination of both is required to cope with today's complex threats
- Both approaches require an analysis
- Several issues have to be considered: random file names, rootkits, anti-removal techniques, shared components, pre-infection settings, changing behavior of malware
- Simple fixes and workarounds are available for most problems

Copyright © 2007 AV-Test GmbH

Content and Context Scanning

- Response times



Copyright © 2007 AV-Test GmbH

Malware Removal – Test Results

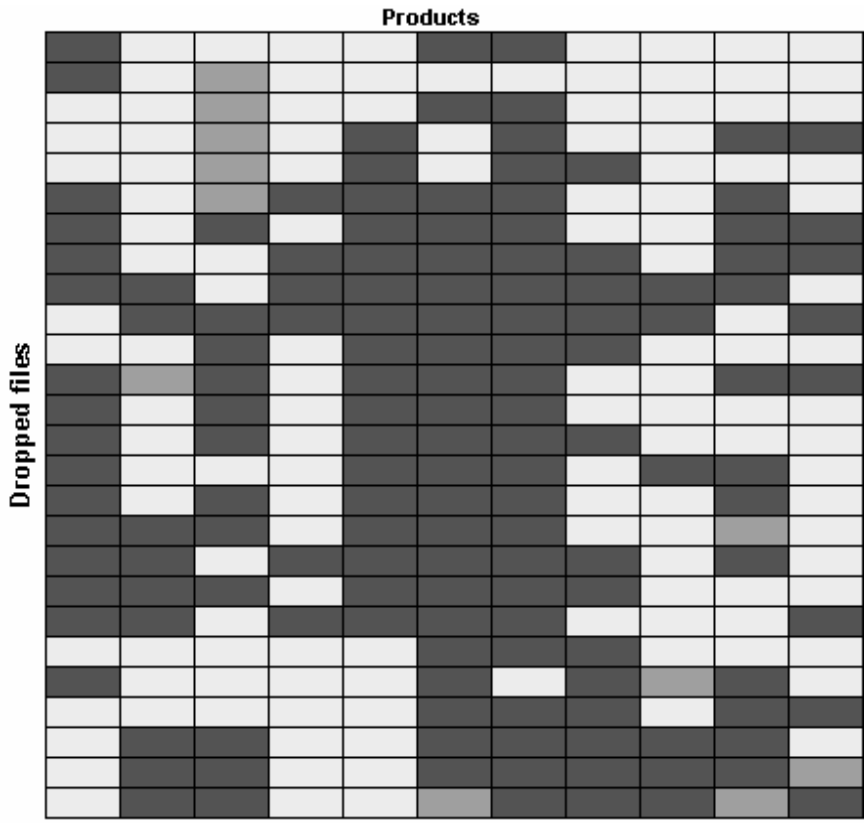
- Response Times and proactive detection

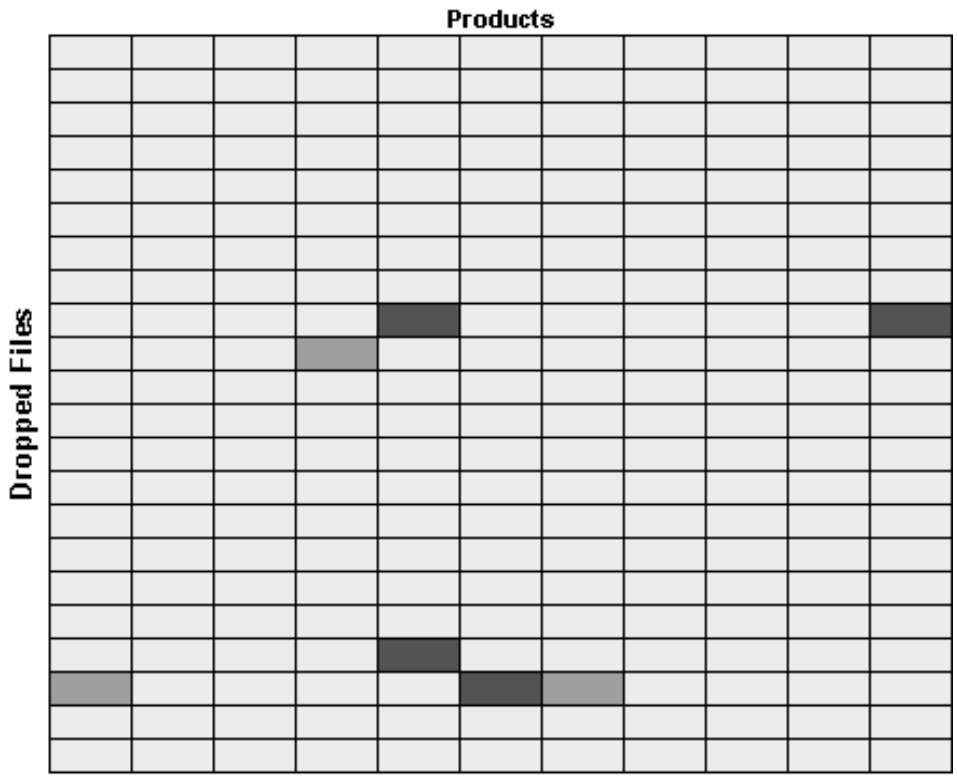
Vendor / Product	Average response time range, including proactive detections	Proactive detection (based on different tests)
Avira AntiVir	2 to 4 hours	20 to 50%
Alwil Avast	6 to 8 hours	5 to 35%
Grisoft AVG	6 to 8 hours	5 to 35%
BitDefender	2 to 4 hours	25 to 60%
F-Secure	less than 2 hours	20 to 50%
Kaspersky	less than 2 hours	20 to 50%
McAfee	14 to 16 hours	25 to 45%
Microsoft	38 to 40 hours	5 to 15%
Eset Nod32	4 to 6 hours	30 to 70%
Panda	4 to 6 hours	20 to 50%
Symantec Norton	6 to 8 hours	15 to 50%
Trend Micro	6 to 8 hours	15 to 45%

Copyright © 2007 AV-Test GmbH

Malware Removal – Test Results

- Detection of dropped components
- Ad- and Spyware vs. WildList Malware





Copyright © 2007 AV-Test GmbH

Malware Removal – Test Results

- Removal Results

	Files created	**Registry keys created**
AdWare.Hotbar	183	789
	Files removed	**Registry keys removed**
Product A (AV)	16	0
Product B (AV)	25	0
Product C (AV)	26	43
Product D (AS)	182	778

Copyright © 2007 AV-Test GmbH

Malware Removal – Conclusion

- Certain threats are handled very well (e.g. WildList malware)
- Other threat categories could need some more attention
- Proactive detection is far from 100%
- Response times still go up to several days
- It takes some time until removal routines are in place and no product is 100% perfect

Copyright © 2007 AV-Test GmbH

Generic Malware Removal

- Overview
  - What is needed?
    - Reduce the response time where no sufficient disinfection routine is available
    - Disinfection without a dedicated analysis done by the vendors
  - Alternative times for an analysis
    - When the malware is first run on the users pc
    - When the malware is detected by the antivirus product

Copyright © 2007 AV-Test GmbH

Generic Malware Removal

- Overview
  - How to analyze on detection time?
    - Run the malware again and monitor the changes it makes to the system
    - Run the malware without damaging the system
  - Sandbox-based disinfection
    - What is it?
    - How does it work?
    - How well does it work and what are the problems?

Copyright © 2007 AV-Test GmbH

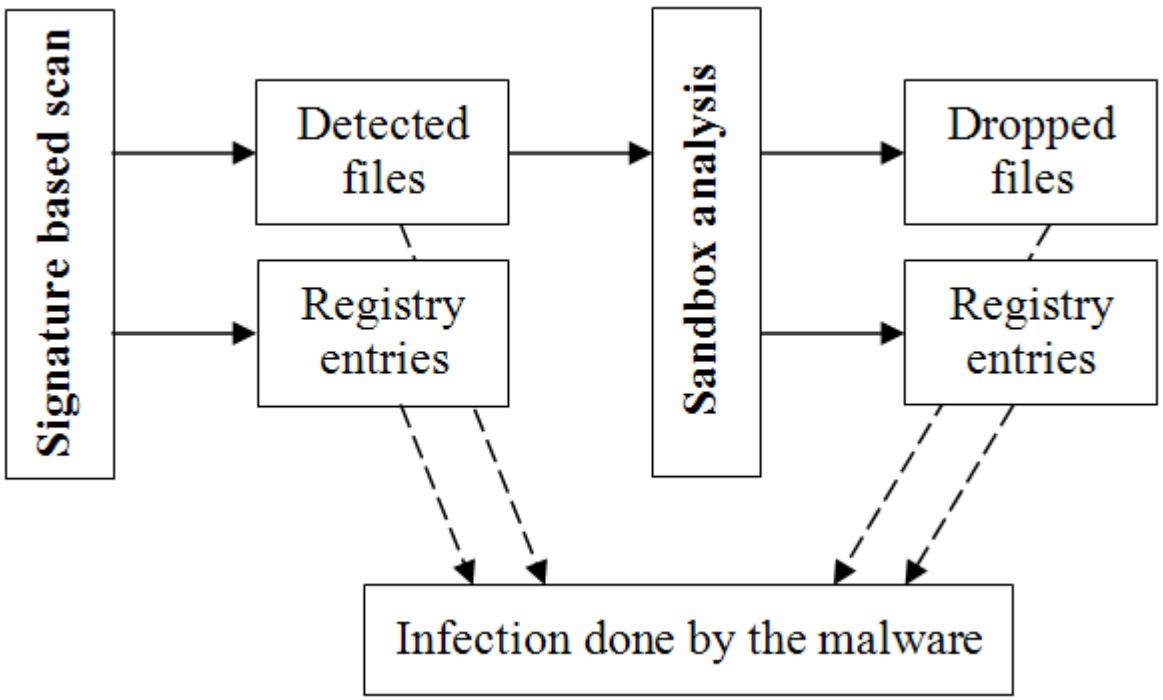
Generic Malware Removal

- Sandbox based Removal
  - The Idea
    - Emulate the malware and report all system changes
    - Perform a removal based on this report
  - What is a sandbox?
    - Virtual environment separated from the system
    - Executable files can be testdriven to analyse their behaviour

Copyright © 2007 AV-Test GmbH

Generic Malware Removal

- Sandbox based Removal
  - Single-stage approach



Copyright © 2007 AV-Test GmbH

Generic Malware Removal

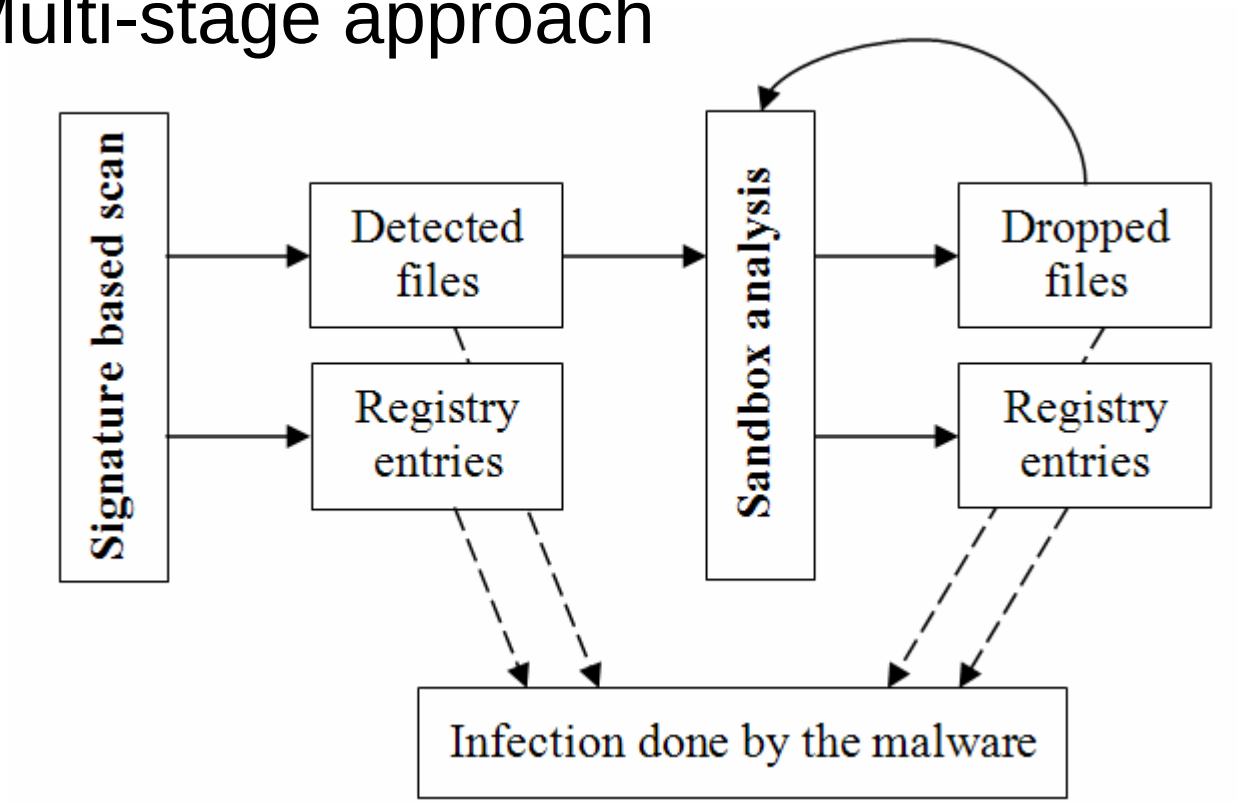
- Sandbox based Removal
  - Test results
    - Comparison of manual analysis with the sandbox analysis
    - Only few files and registry entries found
      - Example: Admedia
      - 24 of 48 files found
      - 6 of 178 Registry entries found

    ⇒ Single-stage approach not suitable for real malware

Copyright © 2007 AV-Test GmbH

Generic Malware Removal

- Sandbox based Removal
  - Multi-stage approach



Copyright © 2007 AV-Test GmbH

Generic Malware Removal

- Sandbox based Removal
  - Test results
    - More files and registry entries found
      - Example: Win32/Admedia
      - Increase from 24 to 32 of 48 files found
      - Increase from 6 to 10 of 178 Registry entries found
    - Multi-stage approach better but far from good

Copyright © 2007 AV-Test GmbH

Generic Malware Removal

- Problems and solutions
  - Related to the sandbox (same for many malware samples)
    - The native API
    - Different behaviour in virtual environments
  - Related to the malware (can not be solved by improvements of the sandbox)
    - User interaction
    - Downloaded files from the internet during infection
    - Scheduled tasks, infection after reboot, etc.

Copyright © 2007 AV-Test GmbH

Generic Malware Removal

- Problems and solutions
  - Related to the malware
    - Different behavior on an infected system
    - Random filenames
    - Pre-infection settings
  - Some worst case scenario
    - Inactive sample triggers the removal routine
    - The malware breaks out of the sandbox (exploiting some vulnerability) during emulation
    - Infection instead of disinfection

Copyright © 2007 AV-Test GmbH

Further Concepts – Supervision

- Log the system changes done by a certain application
- As soon as it is known that this application is malicious, all the changes can easily be reverted
- Solves the problem of pre-infection settings or different behavior in sandbox and real pc
- There are other problems coming up:
  - Which applications should be supervised?
  - Which system changes are malicious and should be reverted?
  - Applications might evade the supervision

Copyright © 2007 AV-Test GmbH

Further Concepts – Supervision

- Similar concepts are already used in current software:
  - Guards which monitor system areas and block all changes or ask the user whether to allow or block
  - Behavior based detection/prevention/blocking, which is a far better approach, because it takes the whole behavior and not only single actions into account and can, in the best case, decide by itself

Copyright © 2007 AV-Test GmbH

Conclusion

	Content and Context Scanning (Manual Analysis)	Sandbox based approach	Supervision approach
Availability (Response time)	- (minutes to days)	+ (instantly)	+ (instantly)
Different behavior in sandboxes	+ (depends on the quality of the analysis)	- (obviously a problem)	+ (no problem)
Performance impact	+ (none)	+ (nearly none)	- (rather much)
Handling of pre-infection settings	- (resetting default values in the best case)	- (resetting default values in the best case)	+ (no problem)
Decision whether changes are malicious or not	+ (depends on the quality of the analysis)	- (hard to do)	- (hard to do)
Catch all (relevant) changes	+ (depends on the quality of the analysis)	- (problematic, as seen)	- (can be a problem)

Copyright © 2007 AV-Test GmbH

Questions & Answers

- ???

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

Copyright © 2007 AV-Test GmbH