Srovnávací testy antivirů

Igor Hák, viry.cz

VIRY.CZ
...když se havěť stává obětí !

Obsah

Historie srovnávacích testů

Současná situace

Metodika

Konkrétní příklady testů

Historie

- 1993-dnešek: Virus Bulletin (6 antivirů)
  Od 1998 ocenění VB100% Award
- 1994-99: University of Tampere
  (Marko Helenius)
- 1994-2004: University of Hamburg (VTC)
  (Klaus Brunnstein)

Současnost

- Virus Bulletin
- AV-test
- AV-comparatives
- Matousec
- PassMark
- Testy v časopisech
- Virus.gr

Současnost

- Výsledky jako argumentace pro obchod
- Perfektní materiál pro marketing. odd.
  - možnost "práce" s výsledky ☺

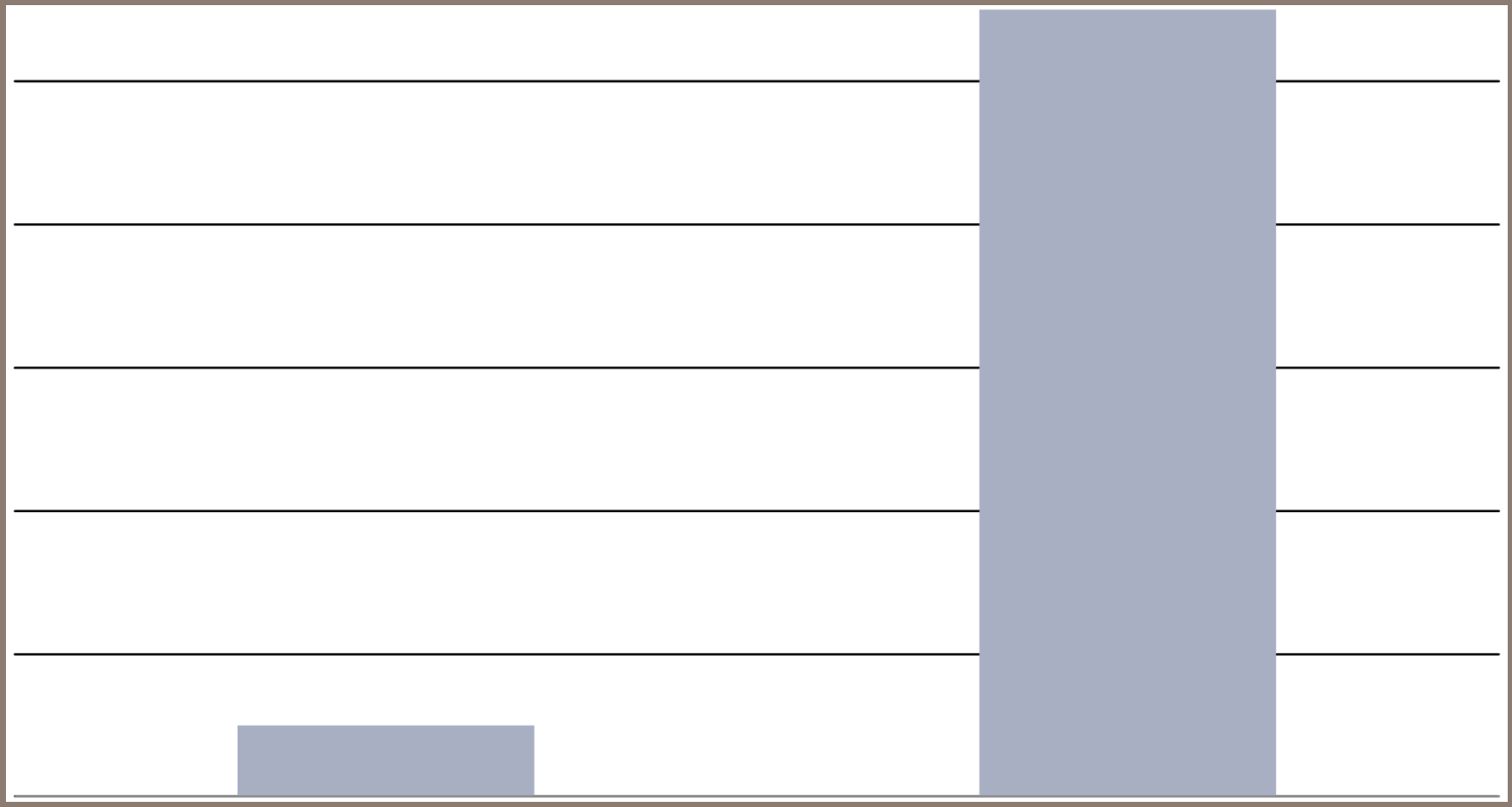
Současnost, marketing ☺

- Konstatování: *"V testu jsme druzí"*
- Marketing.odd.: *"Vyškrtneme prvního"*

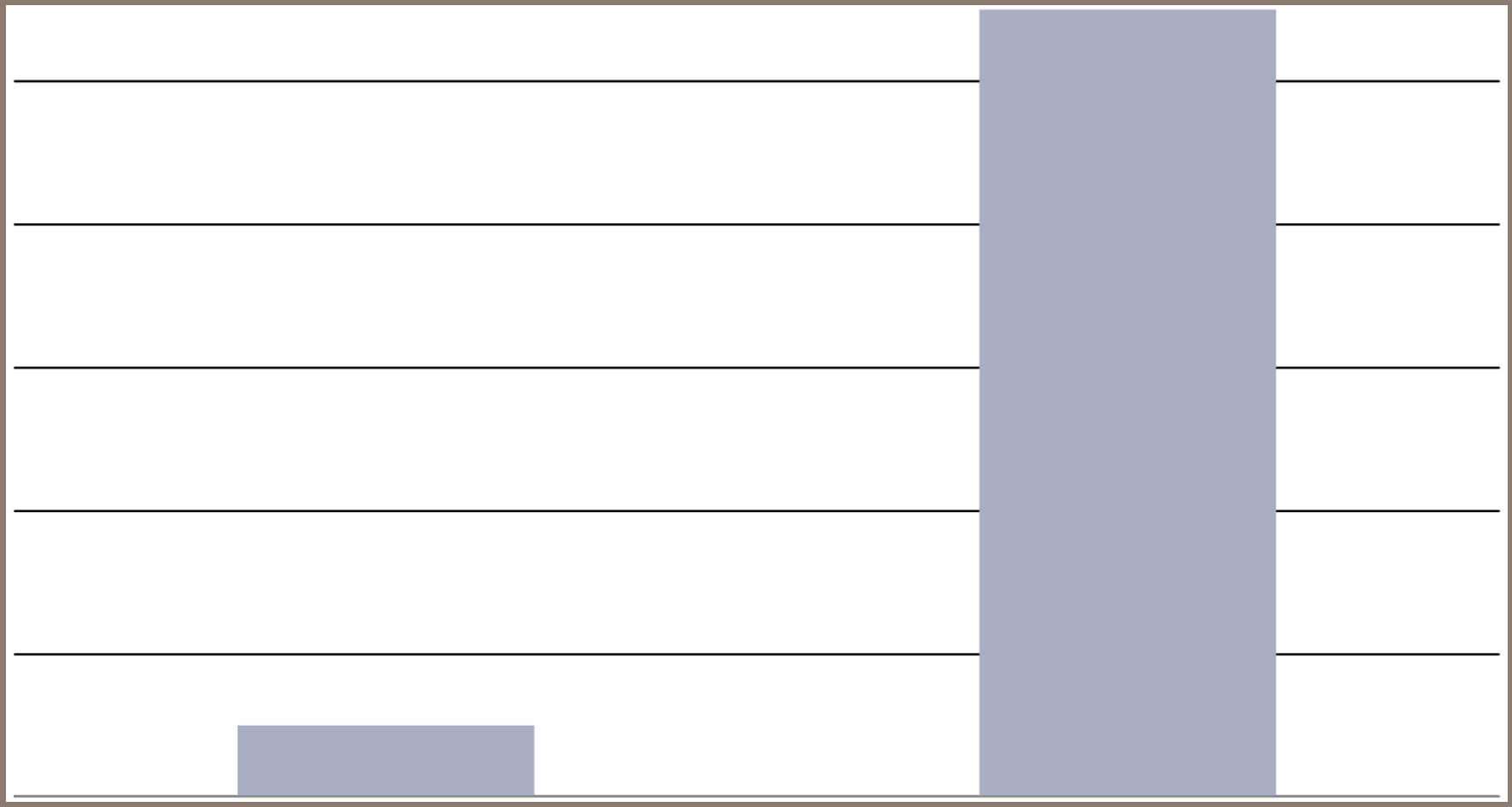
- *"Máme 100% detekci, ale poplachy"*
- *"Máme 100% detekci"*

- *"V lednu a březnu jsme neuspěli"*
- *"Počítáme to až od května"*

Současnost, marketing ☺



Současnost, marketing ☺



Metodika

Přesně daný postup při realizaci testování
Špatná metodika = špatný test

"Dělá" rozdíl mezi realitou a testem

Metodika, on-demand skener

Testování AV, kde je ručně spuštěna kontrola (disku, adresáře…)

Tester **vědomě** nakopíruje tisíce **infikovaných** souborů.
Pak instaluje antivirus a spustí kontrolu.

- ***Kdy to nastane v reálu?***

Metodika, on-access skener

Test "rezidentního štítu"

Tester kopíruje infikované soubory z adresáře do adresáře.

- ***Já se při kopírování ještě nezaviroval!***

Metodika, on-access skener

- Ignoruje technologie typu HIPS
- Neřeší reálný způsob šíření dané havěti
- Ignoruje rozdílné nastavení filtrů

Metodika, vytvoření sbírky havěti

Větší sbírka (ZOO) – ideální pro tiskoviny:

- jasný vítěz (větší rozdíly v %)
- lidi "žerou" obrovské testy

Menší sbírka:

- žádný jasný vítěz, žádná "bomba" (obvykle všichni 100%)

Metodika, vytvoření sbírky havěti

Větší sbírka, hlavní problémy:

- s 99% havěti se nesetkáme
- od každé havěti jen jeden soubor

Dokáže antivirus detekovat i jinou kopii shodné havěti?

Potvrzena "honba" AV společností za lepšími výsledky!

VIRY.CZ
...když se havěť stává obětí !

Metodika, hodnocení výsledků

Nutno hodnotit i "druhou stranu mince"

- Úspěšnost detekce (%)
- **Úroveň falešných poplachů**
  (FP, false positives)
- Rychlost skenování

Virus Bulletin (virusbtn.com)

Od 1998 “VB100% Award” ocenění

- 100% detekce ITW virů OD skenerem
- 100% detekce ITW virů OA skenerem
- bez falešných poplachů

- ITW je kamenem úrazu…

VIRY.CZ
...když se havěť stává obětí !

Virus Bulletin (virusbtn.com)

ITW = In the Wild

- seznam PC **Viruses** In the Wild
- www.wildlist.org

Viry jsou před vymřením

- stabilní "platforma" po několik let
- 100% detekce je tak téměř jistá!

W32/Slenfbot!ITW#25.....[..............] 11/08 PaTl
W32/Slenfbot!ITW#26.....[..............] 11/08 MtPaTl
W32/Slenfbot!ITW#27.....[..............] 11/08 PaTl
W32/Slenping!ITW#3......[..............] 11/08 PaTl
W32/Small!ITW#6.........[..............] 10/08 PaTl
W32/Small!ITW#7.........[..............] 11/08 AoPa
W32/Small!ITW#8.........[..............] 11/08 StTl
W32/Sohanad!ITW#135.....[..............] 11/08 StTl
W32/Spybot!ITW#283......[..............] 11/08 AoSt
W32/Vaklik!ITW#15.......[..............] 7/08 PaTl
W32/Vaklik!ITW#22.......[..............] 7/08 PaTl
W32/Vaklik!ITW#24.......[..............] 7/08 PaTl
W32/Vaklik!ITW#45.......[..............] 8/08 AoTl
W32/Vaklik!ITW#49.......[..............] 8/08 AoTl
W32/Vaklik!ITW#54.......[..............] 8/08 PaTl
W32/Vaklik!ITW#55.......[..............] 8/08 PaTl
W32/Vaklik!ITW#62.......[..............] 10/08 PaTl
W32/Vaklik!ITW#63.......[..............] 11/08 PaTl
W32/Vaklik!ITW#64.......[..............] 11/08 PaTl
W32/Vaklik!ITW#65.......[..............] 11/08 PaTl
W32/Vaklik!ITW#66.......[..............] 11/08 PaTl
W32/VB!ITW#150..........[..............] 11/08 PaSt
W32/VB!ITW#161..........[..............] 8/08 AoTl
W32/VB!ITW#163..........[..............] 10/08 AoStTl
W32/VB!ITW#164..........[..............] 10/08 AoRsTl
W32/VB!ITW#165..........[..............] 10/08 AoSjStTl
W32/VB!ITW#166..........[..............] 10/08 RsTl
W32/VB!ITW#167..........[..............] 10/08 AoSt
W32/VB.DW...............[..............] 9/08 StTl

Virus Bulletin (virusbtn.com)

Větší rozdíly jen ve starších testech

Koho zajímá detekce v roce 2001?

Rising	…	VIRUS 100	VIRUS 100	VIRUS 100	…
Sophos	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100
Symantec	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100
VirusBuster	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100	VIRUS 100
Webroot	…	VIRUS 100	…	VIRUS 100	…

VIRY.CZ
...když se havěť stává obětí !

AV-Comparatives

Rakušan Andreas Clementi

- www.av-comparatives.org

- klasické "ZOO" testy
- netypický retrospective/proactive test
- další specializované testy

AV-Comparatives

Retrospective/proactive testy

- "zmrazí" aktualizace AV
- tři měsíce "sbírá" novou havěť
- po třech m. "pouští" neaktualizované AV

AV-Comparatives

Otestuje schopnosti:

- heuristické detekce
- generické detekce

Hodnotí i úroveň FP

I 20% je úspěchem

AV-Comparatives

Problém – nehodnotí:

- HIPS (behaviour blocker)
- situaci přesně v momentě šíření havěti

AV-Test

V čele němec Andreas Marx

- www.av-test.org

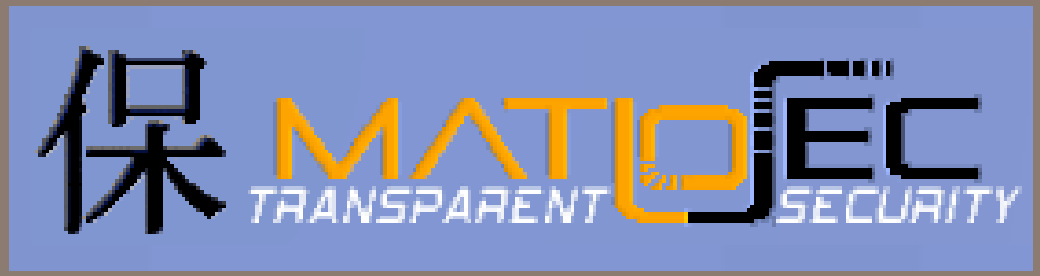
- Obvykle "mega" testy na "zakázku" (časopisy)
  - kvalitní zpracování
  - avšak často špatné zadání (metodika)

Matousec.com

Český test: David Matoušek

- www.matousec.com
- test personálních firewallů

Kvalitní metodika, kvalitní provedení…



VIRY.CZ
...když se havěť stává obětí !

Matousec.com

ALE:

- v reálu je testována funkcionalita HIPS
  v definici FW není nic o HIPS
- při testu nebyl využit škodlivý kód
  tak proč to detekovat?
- řeší až situace, kdy je PC infikováno

PassMark

Všemožné testy mimo kvality detekce

- www.passmark.com

- zabraná paměť
- rychlost náběhu PC
- rychlost spuštění GUI
- …

PassMark

"Problém" na straně 31:

Symantec Corporation funded the production of this report and ***supplied some of the test scripts used for the tests***

Virus.gr

Ukázka nejhoršího veřejného testu

- www.virus.gr

The 246705 virus samples were chosen using VS2000 according to Kaspersky, F-Prot, Nod32, Dr.Web, BitDefender and McAfee antivirus programs. Each virus sample was unique by virus name, meaning that ***AT LEAST 1 antivirus program detected it as a new virus****.*

VIRY.CZ
...když se havěť stává obětí !

Virus.gr

- Ve sbírce jsou čisté soubory (FP),
- autor neví, kolik má ve sbírce inf. soub.,
- tudíž nedokáže určit úspěšnost v %.

- Netestuje na čisté sadě

Pokud dodrží metodiku:

Pro vítězství stačí označit vše za infikované!

"Domácí" testy

- Nedostatečně reprez. sbírka havěti
- Sbírka získana z toho, co detekoval "můj" antivirus, je tak logicky vítězem ☺
- Jeden incident nestačí k celkovém h.
- *“5 let používám AV X, teď jsem nainstaloval AV Y a našel 30 virů!"*

 => *"AV X je k ničemu!"*

VIRY.CZ
...když se havěť stává obětí !

Závěr

Test zůstane testem, realita realitou!

Test vs realita, neslučitelné pojmy ☺

Test používat pouze jako jeden s ukazatelů při výběru AV řešení!

VIRY.CZ
...když se havěť stává obětí !

Děkuji za pozornost!

Navštivte VIRY.CZ/FORUM!

Igor Hák, igi@viry.cz

VIRY.CZ
...když se havěť stává obětí !