Testbed consisted of 321 Viruses, Trojans and Worms, all for the Windows32 environment, and all reasonably new samples. I don't have any data on whether some of these are zoo, or ITW, but they are all real threats I feel someone is likely to encounter, since I got them off the internet (and i've verified they are real as each sample must be detected by at least 4 AV's for me to consider it). All scanners were installed on a clean system, without any traces of other anti-virus softwares - between each test the system and directories were cleaned, and the registry was sweeped. Each AV product was treated with a double-reboot, one before, and one after installation. Each scanner was set at its highest possible settings, and was triple checked for proper options and configuration. Most products were the full registered version when possible, others were fully functional unrestricted trials. All products were tested with the current version as of 6-14-04, and the latest definitions for that date. Each product was run through the test set a minimum of 3 times to establish proper settings and reliability, the only product to exhibit some variance on this was F-Secure, which had one scan come up less than the other two without any settings changes indicating a possible stability issue.

The final standings:

1) MKS-Vir
1a) eXtendia AVK
2) Kaspersky 5.0/4.5
2a) McAfee VirusScan 8.0
3) F-Secure
4) GData AVK
5) RAV + Norton (2 way tie)
6) Dr.Web
7) CommandAV + F-Prot + BitDefender (3 Way Tie)
8) ETrust
9) Trend
10) Panda
11) Avast! Pro
12) KingSoft
13) NOD32
14) AVG Pro
15) AntiVIR
16) ClamWIN
17) UNA
18) Norman
19) Solo
20) Proland
21) Sophos
22) Hauri
23) CAT Quickheal
24) Ikarus

Heuristics seemed to play some of a roll in this test, as no AV had every virus in my test in their definitions, and products with stronger heuristics were able to hold their position towards the top of the test. Double/Multi engined products put up strong showings as well, proving to me that the redundacy method works, and I think more AV companies should considering double-engines. The strongest heurisitical AV I noticed was F-Prot/Command, picking up only 247 samples with definitions but they were able to power through 67 additional hits on "Possible Virus" indicators - very strong! Norton with BloodHound activated had 30 Heuristical pickups, and DrWeb rounded up the pack with 20 heuristical pickups. eXtendia AVK grabs the number one slot with double engine scanning, anything the KAV engine missed, the RAV engine picked up with great redundancy on the double engine/definition system. McAfee actually missed only 2 samples with its definitions, but picked those 2 up as "Suspicious File", and therefore, scores nearly perfect as well.

The biggest dissapointments for me were Norman and Nod32. Even with Advanced-Heuristics enabled, NOD32 failed to pick up a large portion of the samples. Norman, while finding some of the toughest samples, managed to completely miss a large portion of them! Showing that their sandbox-emulation system has great potetential, but its far from complete.

Actual test numbers were:

Total Samples/Found Samples (321 total possible) + Number Missed + Detection Percentage

Discovered and tested MKS-Vir2004, from Poland. Surprisingly, this one with caught every sample perfectly on Medium Heuristics. Specifically, nearly 50 samples were picked up Heuristically giving it a perfect score of 321/321. However, when I increased Heuristics to "Super Deep", it picked up an addition 10 more suspicious files. Upon further investigation, it was found that it was picking up signatures of hacktool utilities left over in some of the archives and flagging those files. Indeed, this is impressive. MKS-Vir2004 exhibits the most advanced detection algorithms i've ever seen, clearly it only had signatures for 271 of my samples, but through code emulation, it was able to pick up all 321 samples!! It clearly labeled the Heuristically found ones as things as "Likely Win32 Trojan" or "Highly Suspicious Acting File". In addition, its scanning speed was incredibly quick, and its memory footprint was quite small. Impressive! Furthermore, this is a full featured and fairly polished product that appears to update at least once per day, and tech support responded to me within 5-15 minutes on my emails. Unfortunately, it appears to not be available in the US for purchase at this time.

1a) MKS_Vir 2004 - 321/321 0 Missed - 100%
1b) eXtendia AVK - 321/321 0 Missed - 100%
2a) Kaspersky 5.0 - 320/321 1 Missed - 99.70% (with Extended Database ON)
2b) McAfee VirusScan 8.0 - 319/321 + 2 (2 found as joke programs - heuristically) - 99%
3) F-Secure - 319/321 2 Missed - 99.37%
4) GData AVK - 317/321 4 Missed - 98.75%
5) RAV + Norton (2 way tie) - 315/321 6 Missed - 98.13%
6) Dr.Web - 310/321 11 Missed - 96.57%
7) CommandAV + F-Prot + BitDefender (3 Way Tie) - 309/321 12 Missed - 96.26%
8) ETrust - 301/321 20 Missed - 93.76%
9) Trend - 300/321 21 Missed - 93.45%
10) Avast! Pro - 299/321 22 Missed - 93.14%
11) Panda - 298/321 23 Missed - 92.83%
12) Virus Buster - 290/321 31 Missed - 90.34%
13) KingSoft - 288/321 33 Missed - 89.71%
14) NOD32 - 285/321 36 Missed (results identical with or without advanced heuristics) - 88.78%
15) AVG Pro - 275/321 46 Missed - 85.66%
16) AntiVIR - 268/321 53 Missed - 83.48%
17) Antidote - 252/321 69 Missed - 78.50%
18) ClamWIN - 247/321 74 Missed - 76.94%
19) UNA - 222/321 99 Missed - 69.15%
20) Norman - 215/321 106 Missed - 66.97%
21) Solo - 182/321 139 Missed - 56.69%
22) Fire AV - 179/321 142 Missed - 55.76%
23) V3 Pro - 109/321 212 Missed - 33.95%
24) Per_AV - 75/321 - 246 Missed - 23.36%
25) Proland - 73/321 248 Missed - 22.74%
26) Sophos - 50/321 271 Missed - 15.57%
27) Hauri - 49/321 272 Missed - 15.26%
28) CAT Quickheal - 21/321 300 Missed - 6%
29) Vir_iT - 10/321 311 Missed - 3%
30) Ikarus - Crashed on first virus. - 0%

Interesting also to note, is the detection level of the US AVK version with KAV+RAV engines was higher than the German version with KAV+BitDefender engines. Several vendors have free versions of their for purchase AV's, we didn't test the free versions, as it would serve no purpose for this test, but based on the results, none of the free versions would have been very impressive anyway. The term "Heuristics" seems like it should be taken very liberally, as some products that claim to be loaded with Heuristics scored miserably on items they clearly didn't have definitions for. Scanning speed was not measured, as it was totally irrelevant to my testing, and on-access scanners were not tested, as it would have been too time consuming, but considering most products have similar on-access engines as on-demand, and use the same database, results most likely, would be very similar.

Cut through the hype, cut through the marketing schemes, this was a real test, with real samples, and none of these samples were provided to the antivirus software vendors in advance. This is real world, and these are likely badguys you'll encounter, since I got them in my real encounters, and all were aquired on the internet in daily activities which anyone out there might be involved in. (Installing shareware, filesharing, surfing, etc). Keep in mind that with ITW tests the AV vendors have full disclosure of what they will be tested on in advance, not so here, so heuristics and real detection algorithms will play a big part, as well as the depth and scope of their definition database.

[Edit: After re-testing the Kaspersky products with Extended Database option turned ON, the moved up effectively scoring 100% considering the 1% margin of error]