The Virus

New Mexico
Supercomputing Challenge
Final Report
April 23rd, 2010

Team Number:
CEPI

Team Members:
Michael Szanto
Devin Hayes
Ryan FitzGerald

Teachers:
Mr. Esquivel
Mr. Stewart

Hypothesis: Our hypothesis is that if anti-virus companies had a cooperative subscription database they would be able to detect viruses faster and more accurately.

Data

-

	AVG	PANDA	F-Secure	KASPERSKY
Virus 1	**Found**	**Miss**	**Miss**	**Miss**
Virus 2	**Miss**	**Found**	**Found**	**Found**
Virus 3	**Miss**	**Miss**	**Found**	**Miss**
Virus 4	**Found**	**Found**	**Found**	**Found**
Virus 5	**Miss**	**Found**	**Miss**	**Miss**
Virus 6	**Miss**	**Miss**	**Miss**	**Found**
Virus 7	**Miss**	**Miss**	**Miss**	**Miss**
Virus 8	**Found**	**Found**	**Miss**	**Found**
Virus 9	**Found**	**Miss**	**Found**	**Found**
Virus 10	**Found**	**Miss**	**Miss**	**Miss**

Test Results: We found that our hypothesis was correct. There were several viruses that were detected by one or two of the anti-viruses, but not the others. Therefore we have proven that a combined A\V detection provides much better protection to the end user.

-

-

-

-

-

-

-

Synopsis:

-

Finding Viruses

-

-

To find viruses for testing, we used P-2-P file sharing networks. We downloaded 100's of files that could possibly be infected. We monitored the execution of the files, and watched for malicious modifications to the computer, by using a program called Sandboxie.

-

To assure our test results, the machine was re-imaged with an up to date Windows XP install after every successful virus infection.

-

First we proved this by quarantining a computer by putting deep freeze (deep freeze will reset EVERY thing that has happened to the computer since it was turned on as soon as you turn it off) on the computer. This will let us put an anti-virus and our viruses making it easier to move on to the next anti-virus, and so there is no permanent damage to the computer.

-

Next we used Sandboxie to test if the virus is doing something to the computer because of the virus doesn't do any thing then it wont be detected. This will help us find good viruses to use in the test. We got the viruses through obvious torrents on www.thepiratebay.org. (Obvious viruses are around 500 kbs). We have at least 10 possible downloads to test with Sandboxie.

-

-

-

-

-

-

Conclusion: Based on conclusions made using the data collected, we have proven that a combined anti-virus company's database is an excellent idea. If a subscription database were provided to all major anti-virus company, viruses would be more quickly detected and removed. It would be beneficial to all parties involved.

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

Down Side: Unfortunately, there are problems with a cooperative database. With a cooperative database, malicious virus developers will be able to more easily test a new variant of their virus for detection. However, this does not negate the benefits of a cooperative database because once any one of the antivirus companies detects it, they all will. A cooperative database is like using a larger fishing net with smaller holes and bigger thread. You're going to catch almost everything. However once a fish adapts in such a way that it is able to fit through one part of the net, it will fit through every part of the net until the net changes.

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

By:
Michael Szanto
Devin Hayes
Ryan FitzGerald

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
