The solution in the naming chaos

Ph.D. Ferenc Leitold

Veszprem University - Veszprog Ltd., Hungary

About the Author

Ferenc Leitold graduated from Technical University of Budapest in 1991. He received his Ph.D. at Technical University of Budapest too, in 1997 in the theme of computer viruses. Currently he teaches in the Department of Information Systems at Veszprém University. He teaches computer programming, computer security, and computer networks. His research interest is based on computer viruses: mathematical model of computer viruses, automatic methods for analysing computer viruses. According to the CheckVir project (www.checkvir.com) of Veszprog Ltd. he is dealing with the testing of anti-virus software products.

Mailing Address: Ph.D. Ferenc Leitold, Kupa str. 14. H-8200 Veszprem, HUNGARY;

Phone: +36 30 9599-486; Fax: +36 88 413-241; E-mail: fleitold@veszprog.hu;

URL: www.checkvir.com

Descriptors

computer virus, anti-virus, anti-virus testing, disinfection testing, quality assurance, quality engineering

The solution in the naming chaos

Abstract

As the first computer virus born there were a lot of godfather of it. Every antivirus solution uses its own naming convention so now there are more than hundred-thousand different computer viruses in the world and there are at least one million virus names for them. This problem is highlighted in this paper. Unfortunately it is impossible that antivirus developers change their naming convention and use the same identification of the same computer virus. Virus and worm nomenclature is typically left up to the security vendor which first discovers the malware. Until the beginning of 2004 the process worked, more or less. But the large scale and rapid release of multiple variants of worms in the Netsky, Bagle, MyDoom and other families last year led to confusion, with antivirus firms out of sync in their naming. One vendor would tag a new Bagle as Bagle.w, for instance, while others would call it Bagle.u or Bagle.t.

Introduction

WildList is the most authentic source of information on which viruses are spreading In the Wild. The lists of widespread viruses are based on reports of researchers around the world. These lists are very good information source for experts. They always know which listed virus is which. Unfortunately the average user is unable to identify the listed viruses. There is a great help about it: in the virus descriptions menu point there is some info about the listed viruses, but there are some problems about it:

- At this time (18 March 2005) the latest available description list is from May 2004, however now there are eight(!) published list after May 2004.
- The information is based on only F-Secure database. So it is related to the F-Secure naming convention.
- There are some missing list elements where there is no information.
- There are some viruses where the information of the variants link to the same page.

It means that it is impossible to correctly identify the listed viruses.

Naming standardization strategies

Some organization tried and/or tries to solve the naming problem.

- EICAR started a CAMDIER project. One of its main topic is to develop Unified Naming Convention.
- US-CERT, the federally-funded security clearinghouse, proposed in November 2004 that they would try to put some order to the often-chaotic naming of worms and viruses in early 2005.

Theoretically it is impossible to develop a general naming convention. It is due to the fact that identification algorithms in antivirus solutions are not the same. Let us suppose that there are two antivirus program and there are two computer virus variants. The first AV detects both virus variants as A virus using its own algorithm. This algorith was built to identify both viruses. The second AV detects variants using not the same name because this antivirus includes two different algorithms for each variant. In this case renaming virus names in AV programs can not solve the problem.

Checkvir Real-time AV testing

In this situation the good solution would be the publication of exact comparable names that can be used for identification as well.

Our Real-time AV testing project may be the solution for this purpose. It can provide virus naming information for In-The-Wild viruses. It means that every virus sample should be checked using almost all updates published by AV developers. Our system is able to do this automatically. So if a new upgrade of an AV published it can detect it and the test is executed in some minutes the update process executed. After update procedures executed the whole image of the operating system and the updated AV saved. If a new virus appeared in the wild then it has to be checked by all AV software. But not only the actual ones used, the previous 15-20 versions has to be checked as well. Using this method it can be checked which is the first version of AV that is able to identify the new virus.

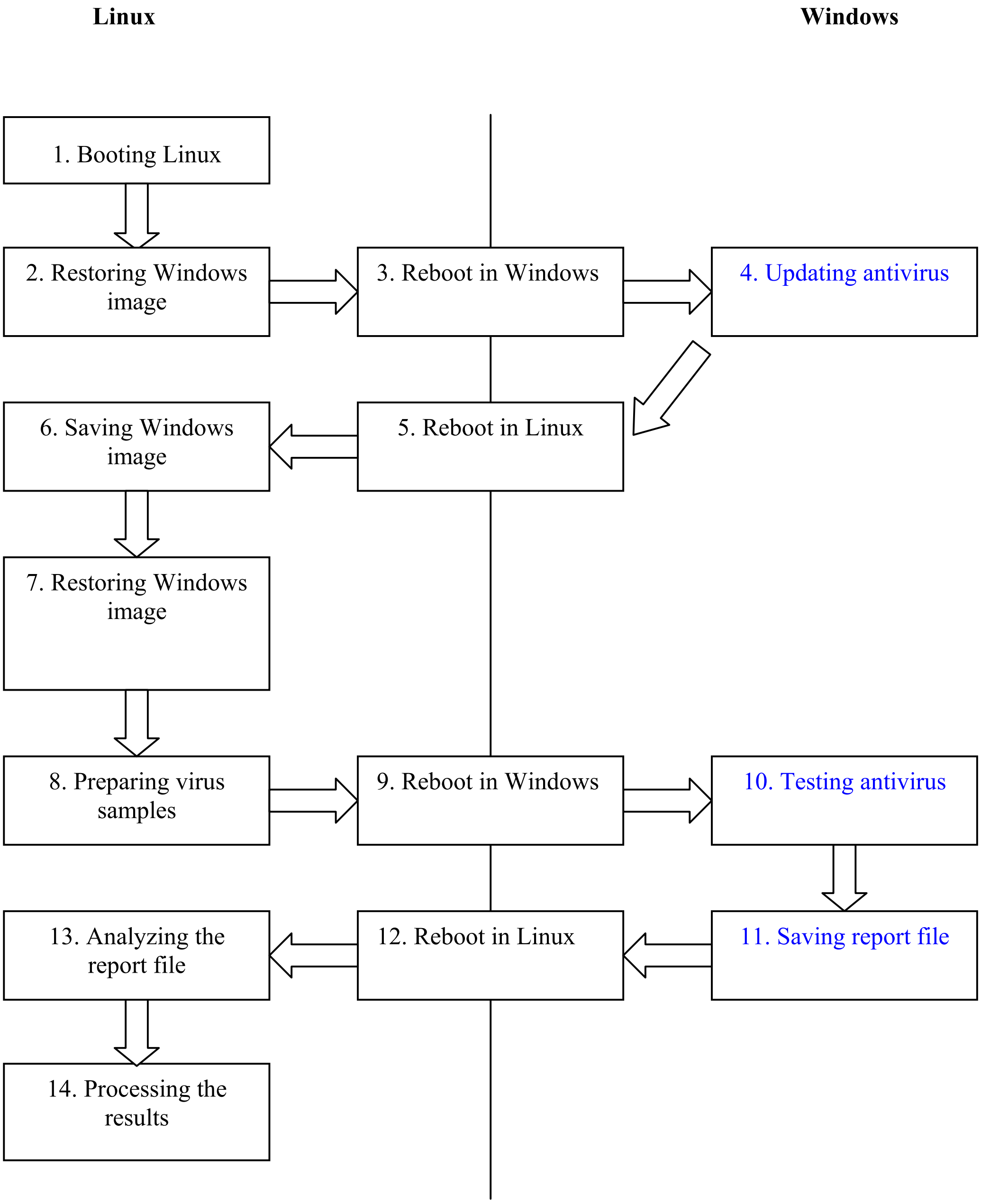
CheckVir Real time AV tests can provide exact information for virus identification including AV product name, version, build number, virus database version, ... It is possible to search for earlier information as well. It is possible to identify if an AV vendor changes the name of a virus.

Testing procedure

The testing procedure includes a lot of basic step. For this purpose two different computer is used continuously. One of them is used for updating the AV software and for creating the and saving the Windows image of it. The second computer is a secured environment whitout any Internet connection. It is used for testing against virus samples. Both computer includes a Linux and a Windows operating system. Windows is used for testing, Linux is used for controlling, saving and restoring the Windows image, managing the virus samples, saving the results.

The procedure includes the following steps:

1. Starting Linux
2. Restoring a Windows image (including installed antivirus)
3. Reboot in Windows
4. Update the antivirus
5. Reboot in Linux
6. Saving the Windows image (with the updated antivirus)
7. Restoring the Windows image in the secured environment
8. Preparing virus samples for testing
9. Reboot in Windows
10. Testing the antivirus solution (on-demand and/or on-access)
11. Saving the report file, creating screenshot(s)
12. Reboot in Linux
13. Analysing the report file
14. Processing the results


Linux
Windows
1. Booting Linux
2. Restoring Windows image
3. Reboot in Windows
4. Updating antivirus
5. Reboot in Linux
6. Saving Windows image
7. Restoring Windows image
8. Preparing virus samples
9. Reboot in Windows
10. Testing antivirus
11. Saving report file
12. Reboot in Linux
13. Analyzing the report file
14. Processing the results

Sample output

This sample outputs were generated using the results of the CheckVir regular antivirus testing of some AV products.

W32/Zafi.A

Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus Workstation	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 87139 (known viruses)	I-Worm.Zafi
Kaspersky Anti-Virus Workstation	4.5.0.95, 89257 (known viruses)	I-Worm.Zafi
Kaspersky Anti-Virus Personal	5.0.121, 91566 (known viruses)	I-Worm.Zafi
Kaspersky Anti-Virus Workstation	4.5.0.95, 93606 (known viruses)	I-Worm.Zafi.a
Kaspersky Anti-Virus Workstation	4.5.0.95, 96130 (known viruses)	I-Worm.Zafi.a

Product name	Version(s)	Virus name(s)
McAfee VirusScan Enterprise	7.1.0, 4313 (virus definitions), 4.2.60 (scan engine)	New Malware.b (Virus)
McAfee VirusScan Enterprise	7.1.0, 4327 (virus definitions), 4.2.60 (scan engine)	New Malware.b (Virus)
McAfee VirusScan Enterprise	7.1.0, 4339 (virus definitions), 4.3.20 (scan engine)	New Malware.b (Virus)
McAfee VirusScan Enterprise	7.1.0, 4351 (virus definitions), 4.3.20 (scan engine)	New Malware.b (Virus)
McAfee VirusScan	v4.5.1 SP1, 4.0.4360 (virus definitions), 4.3.20 (scan engine)	W32/Zafi@MM
McAfee VirusScan Enterprise	7.1.0, 4367 (virus definitions), 4.3.20 (scan engine)	W32/Zafi.a@MM
McAfee VirusScan Enterprise	7.1.0, 4380 (virus definitions), 4.3.20 (scan engine)	W32/Zafi.a@MM
McAfee VirusScan	v4.5.1 SP1, 4.0.4385 (virus definitions), 4.3.20 (scan engine)	W32/Zafi.a@MM

Product name	Version(s)	Virus name(s)
NOD32 Antivirus System	2.000.9, 1.601 (virdef ver), 4157 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.633 (virdef ver), 4239 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.686 (virdef ver), 4368 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.725 (virdef ver), 4459 (virdef build)	Win32/Zafi.A worm
NOD32 Antivirus System	2.000.9, 1.767 (virdef ver), 4558 (virdef build)	Win32/Zafi.A worm
NOD32 Antivirus System	2.000.9, 1.792 (virdef ver), 4620 (virdef build)	Win32/Zafi.A worm
NOD32 Antivirus System	2.000.9, 1.820 (virdef ver), 4696 (virdef build)	Win32/Zafi.A worm
NOD32 Antivirus System	2.000.9, 1.840 (virdef ver), 4748 (virdef build)	Win32/Zafi.A worm

W32/Bobax.C

Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus Workstation	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 87139 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 89257 (known viruses)	TrojanProxy.Win32.Bobax.c
Kaspersky Anti-Virus Personal	5.0.121, 91566 (known viruses)	TrojanProxy.Win32.Bobax.c
Kaspersky Anti-Virus Workstation	4.5.0.95, 93606 (known viruses)	TrojanProxy.Win32.Bobax.c
Kaspersky Anti-Virus Workstation	4.5.0.95, 96130 (known viruses)	TrojanProxy.Win32.Bobax.c

Product name	Version(s)	Virus name(s)
McAfee VirusScan Enterprise	7.1.0, 4313 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4327 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4339 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4351 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan	v4.5.1 SP1, 4.0.4360 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4367 (virus definitions), 4.3.20 (scan engine)	W32/Bobax.worm.c.dll, W32/Bobax.worm.c
McAfee VirusScan Enterprise	7.1.0, 4380 (virus definitions), 4.3.20 (scan engine)	W32/Bobax.worm.c.dll, W32/Bobax.worm.c
McAfee VirusScan	v4.5.1 SP1, 4.0.4385 (virus definitions), 4.3.20 (scan engine)	W32/Bobax.worm.c.dll, W32/Bobax.worm.c

Product name	Version(s)	Virus name(s)
NOD32 Antivirus System	2.000.9, 1.601 (virdef ver), 4157 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.633 (virdef ver), 4239 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.686 (virdef ver), 4368 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.725 (virdef ver), 4459 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.767 (virdef ver), 4558 (virdef build)	Win32/Bobax.B worm, Win32/Bobax.B virus
NOD32 Antivirus System	2.000.9, 1.792 (virdef ver), 4620 (virdef build)	Win32/Bobax.B worm, Win32/Bobax.B virus
NOD32 Antivirus System	2.000.9, 1.820 (virdef ver), 4696 (virdef build)	Win32/Bobax.B worm, Win32/Bobax.B virus
NOD32 Antivirus System	2.000.9, 1.840 (virdef ver), 4748 (virdef build)	Win32/Bobax.B worm, Win32/Bobax.B virus

W32/Korgo.A

Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus Workstation	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 87139 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 89257 (known viruses)	
Kaspersky Anti-Virus Personal	5.0.121, 91566 (known viruses)	Worm.Win32.Padobot.b
Kaspersky Anti-Virus Workstation	4.5.0.95, 93606 (known viruses)	Worm.Win32.Padobot.b
Kaspersky Anti-Virus Workstation	4.5.0.95, 96130 (known viruses)	Worm.Win32.Padobot.b

Product name	Version(s)	Virus name(s)
McAfee VirusScan Enterprise	7.1.0, 4313 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4327 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4339 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4351 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan	v4.5.1 SP1, 4.0.4360 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4367 (virus definitions), 4.3.20 (scan engine)	W32/Korgo.worm.d, W32/Korgo.worm.a
McAfee VirusScan Enterprise	7.1.0, 4380 (virus definitions), 4.3.20 (scan engine)	W32/Korgo.worm.d, W32/Korgo.worm.a
McAfee VirusScan	v4.5.1 SP1, 4.0.4385 (virus definitions), 4.3.20 (scan engine)	W32/Korgo.worm.d, W32/Korgo.worm.a

Product name	Version(s)	Virus name(s)
NOD32 Antivirus System	2.000.9, 1.601 (virdef ver), 4157 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.633 (virdef ver), 4239 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.686 (virdef ver), 4368 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.725 (virdef ver), 4459 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.767 (virdef ver), 4558 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.792 (virdef ver), 4620 (virdef build)	Win32/Korgo.A worm
NOD32 Antivirus System	2.000.9, 1.820 (virdef ver), 4696 (virdef build)	Win32/Korgo.A worm
NOD32 Antivirus System	2.000.9, 1.840 (virdef ver), 4748 (virdef build)	Win32/Korgo.A worm

W32/Mimail.V@mm

Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus Workstation	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 87139 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 89257 (known viruses)	I-Worm.Mimail.r
Kaspersky Anti-Virus Personal	5.0.121, 91566 (known viruses)	I-Worm.Mimail.r
Kaspersky Anti-Virus Workstation	4.5.0.95, 93606 (known viruses)	I-Worm.Mimail.r
Kaspersky Anti-Virus Workstation	4.5.0.95, 96130 (known viruses)	I-Worm.Mimail.r

Product name	Version(s)	Virus name(s)
McAfee VirusScan Enterprise	7.1.0, 4313 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4327 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4339 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4351 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan	v4.5.1 SP1, 4.0.4360 (virus definitions), 4.3.20 (scan engine)	W32/Mimail.v@MM
McAfee VirusScan Enterprise	7.1.0, 4367 (virus definitions), 4.3.20 (scan engine)	W32/Mimail.v@MM
McAfee VirusScan Enterprise	7.1.0, 4380 (virus definitions), 4.3.20 (scan engine)	W32/Mimail.v@MM
McAfee VirusScan	v4.5.1 SP1, 4.0.4385 (virus definitions), 4.3.20 (scan engine)	W32/Mimail.v@MM

Product name	Version(s)	Virus name(s)
NOD32 Antivirus System	2.000.9, 1.601 (virdef ver), 4157 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.633 (virdef ver), 4239 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.686 (virdef ver), 4368 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.725 (virdef ver), 4459 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.767 (virdef ver), 4558 (virdef build)	Win32/Moba.A worm
NOD32 Antivirus System	2.000.9, 1.792 (virdef ver), 4620 (virdef build)	Win32/Moba.A worm
NOD32 Antivirus System	2.000.9, 1.820 (virdef ver), 4696 (virdef build)	Win32/Moba.A worm
NOD32 Antivirus System	2.000.9, 1.840 (virdef ver), 4748 (virdef build)	Win32/Moba.A worm

W32/Sasser.B

Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus Workstation	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 87139 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 89257 (known viruses)	Worm.Win32.Sasser.a
Kaspersky Anti-Virus Personal	5.0.121, 91566 (known viruses)	Worm.Win32.Sasser.a
Kaspersky Anti-Virus Workstation	4.5.0.95, 93606 (known viruses)	Worm.Win32.Sasser.a
Kaspersky Anti-Virus Workstation	4.5.0.95, 96130 (known viruses)	Worm.Win32.Sasser.a

Product name	Version(s)	Virus name(s)
McAfee VirusScan Enterprise	7.1.0, 4313 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4327 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4339 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4351 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan	v4.5.1 SP1, 4.0.4360 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.b, W32/Sasser.worm.c
McAfee VirusScan Enterprise	7.1.0, 4367 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.b, W32/Sasser.worm.c
McAfee VirusScan Enterprise	7.1.0, 4380 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.b, W32/Sasser.worm.c
McAfee VirusScan	v4.5.1 SP1, 4.0.4385 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.b, W32/Sasser.worm.c

Product name	Version(s)	Virus name(s)
NOD32 Antivirus System	2.000.9, 1.601 (virdef ver), 4157 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.633 (virdef ver), 4239 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.686 (virdef ver), 4368 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.725 (virdef ver), 4459 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.767 (virdef ver), 4558 (virdef build)	Win32/Sasser.B worm, Win32/Sasser.C worm
NOD32 Antivirus System	2.000.9, 1.792 (virdef ver), 4620 (virdef build)	Win32/Sasser.B worm, Win32/Sasser.C worm
NOD32 Antivirus System	2.000.9, 1.820 (virdef ver), 4696 (virdef build)	Win32/Sasser.B worm, Win32/Sasser.C worm
NOD32 Antivirus System	2.000.9, 1.840 (virdef ver), 4748 (virdef build)	Win32/Sasser.B worm, Win32/Sasser.C worm

W32/Sasser.D

Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus Workstation	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 87139 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 89257 (known viruses)	Worm.Win32.Sasser.c
Kaspersky Anti-Virus Personal	5.0.121, 91566 (known viruses)	Worm.Win32.Sasser.c
Kaspersky Anti-Virus Workstation	4.5.0.95, 93606 (known viruses)	Worm.Win32.Sasser.c
Kaspersky Anti-Virus Workstation	4.5.0.95, 96130 (known viruses)	Worm.Win32.Sasser.c

Product name	Version(s)	Virus name(s)
McAfee VirusScan Enterprise	7.1.0, 4313 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4327 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4339 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4351 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan	v4.5.1 SP1, 4.0.4360 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.d
McAfee VirusScan Enterprise	7.1.0, 4367 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.d
McAfee VirusScan Enterprise	7.1.0, 4380 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.d
McAfee VirusScan	v4.5.1 SP1, 4.0.4385 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.d

Product name	Version(s)	Virus name(s)
NOD32 Antivirus System	2.000.9, 1.601 (virdef ver), 4157 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.633 (virdef ver), 4239 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.686 (virdef ver), 4368 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.725 (virdef ver), 4459 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.767 (virdef ver), 4558 (virdef build)	Win32/Sasser.D worm
NOD32 Antivirus System	2.000.9, 1.792 (virdef ver), 4620 (virdef build)	Win32/Sasser.D worm
NOD32 Antivirus System	2.000.9, 1.820 (virdef ver), 4696 (virdef build)	Win32/Sasser.D worm
NOD32 Antivirus System	2.000.9, 1.840 (virdef ver), 4748 (virdef build)	Win32/Sasser.D worm

W32/Sasser.E

Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus Workstation	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 87139 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 89257 (known viruses)	Worm.Win32.Sasser.d
Kaspersky Anti-Virus Personal	5.0.121, 91566 (known viruses)	Worm.Win32.Sasser.d
Kaspersky Anti-Virus Workstation	4.5.0.95, 93606 (known viruses)	Worm.Win32.Sasser.d
Kaspersky Anti-Virus Workstation	4.5.0.95, 96130 (known viruses)	Worm.Win32.Sasser.d

Product name	Version(s)	Virus name(s)
McAfee VirusScan Enterprise	7.1.0, 4313 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4327 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4339 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4351 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan	v4.5.1 SP1, 4.0.4360 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.e
McAfee VirusScan Enterprise	7.1.0, 4367 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.e
McAfee VirusScan Enterprise	7.1.0, 4380 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.e
McAfee VirusScan	v4.5.1 SP1, 4.0.4385 (virus definitions), 4.3.20 (scan engine)	W32/Sasser.worm.e

Product name	Version(s)	Virus name(s)
NOD32 Antivirus System	2.000.9, 1.601 (virdef ver), 4157 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.633 (virdef ver), 4239 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.686 (virdef ver), 4368 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.725 (virdef ver), 4459 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.767 (virdef ver), 4558 (virdef build)	Win32/Sasser.E worm
NOD32 Antivirus System	2.000.9, 1.792 (virdef ver), 4620 (virdef build)	Win32/Sasser.E worm
NOD32 Antivirus System	2.000.9, 1.820 (virdef ver), 4696 (virdef build)	Win32/Sasser.E worm
NOD32 Antivirus System	2.000.9, 1.840 (virdef ver), 4748	Win32/Sasser.E worm

	(virdef build)	

W32/Sober.E@mm

Product name	Version(s)	Virus name(s)
Kaspersky Anti-Virus Workstation	4.5.0.95, 80673 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 82614 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 84230 (known viruses)	
Kaspersky Anti-Virus Workstation	4.5.0.95, 87139 (known viruses)	I-Worm.Sober.e
Kaspersky Anti-Virus Workstation	4.5.0.95, 89257 (known viruses)	I-Worm.Sober.e
Kaspersky Anti-Virus Personal	5.0.121, 91566 (known viruses)	I-Worm.Sober.e
Kaspersky Anti-Virus Workstation	4.5.0.95, 93606 (known viruses)	I-Worm.Sober.e
Kaspersky Anti-Virus Workstation	4.5.0.95, 96130 (known viruses)	I-Worm.Sober.e

Product name	Version(s)	Virus name(s)
McAfee VirusScan Enterprise	7.1.0, 4313 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4327 (virus definitions), 4.2.60 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4339 (virus definitions), 4.3.20 (scan engine)	
McAfee VirusScan Enterprise	7.1.0, 4351 (virus definitions), 4.3.20 (scan engine)	W32/Sober.e@MM (Virus)
McAfee VirusScan	v4.5.1 SP1, 4.0.4360 (virus definitions), 4.3.20 (scan engine)	W32/Sober.e@MM (Virus)
McAfee VirusScan Enterprise	7.1.0, 4367 (virus definitions), 4.3.20 (scan engine)	W32/Sober.e@MM (Virus)
McAfee VirusScan Enterprise	7.1.0, 4380 (virus definitions), 4.3.20 (scan engine)	W32/Sober.e@MM (Virus)
McAfee VirusScan	v4.5.1 SP1, 4.0.4385 (virus definitions), 4.3.20 (scan engine)	W32/Sober.e@MM (Virus)

Product name	Version(s)	Virus name(s)
NOD32 Antivirus System	2.000.9, 1.601 (virdef ver), 4157 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.633 (virdef ver), 4239 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.686 (virdef ver), 4368 (virdef build)	
NOD32 Antivirus System	2.000.9, 1.725 (virdef ver), 4459 (virdef build)	Win32/Sober.E worm
NOD32 Antivirus System	2.000.9, 1.767 (virdef ver), 4558 (virdef build)	Win32/Sober.E worm
NOD32 Antivirus System	2.000.9, 1.792 (virdef ver), 4620 (virdef build)	Win32/Sober.E worm

NOD32 Antivirus System	2.000.9, 1.820 (virdef ver), 4696 (virdef build)	Win32/Sober.E worm
NOD32 Antivirus System	2.000.9, 1.840 (virdef ver), 4748 (virdef build)	Win32/Sober.E worm

References

Leitold, F. (1995). Automatic Virus Analyser System. Proceedings of the 5th International Virus Bulletin Conference, Boston USA, 1995, pp. 99-107.

Leitold, F. (2002). Independent AV testing. Proceedings of the 11th International EICAR Conference, Berlin Germany, 2002.

EICAR Cyber Attack Methods Detection & Information Exploitation Research Project, http://www.eicar.org/camdier/

Order To Come To Virus Naming Chaos, http://www.techweb.com/wire/security/54200541, November 24, 2004