Facts and myths about antivirus evasion with Metasploit

schierlm.users.sourceforge.net/avevasion.html

When asking people about how to create a Meterpreter payload executable that evades antivirus, you will get different answers, like using encoders, or changing the template. Others say it is useless to use or even improve Metasploit's exe generation since the AV engines will detect the RWX stub, so you have to find your own way to get RWX memory. Some of these answers are just outdated, others still work, but for all of them there is no real evidence available on the Web. The reason for this is simple: AV evasion is like the Heisenberg uncertainty principle: Whenever you scan a piece of malware (and especially when you upload it to services like VirusTotal, you will affect future detection of the same file or similar files. And, a writeup like this will also affect how AV detects files, thus making it harder to evade it. Therefore, most researcher try to keep their information about antivirus private, having the consequence that a lot of research is done a lot of times.

This article tries to given an overview about the current executable generation scheme of Metasploit, how AV detects them, and how to evade them. Note that this document only covers standalone EXE files (for Windows) that replace an EXE template's functionality, and not other payloads for exploits, service executables (like for the `windows/psexec` exploit) or executables that merely add to the original template's functionality (like the `-k` option of msfpayload). Some situations (like some social engineering "exploits", or generating a Java applet that calls native meterpreter) will implicitly create such an EXE file, though, so it helps these use cases as well.

A good writeup about how EXE files are currently generated is available at scriptjunkie's blog.

They were uploaded to VirusTotal for analysis, the actual analysis reports are attached to the end of this document.

As of July 2011 (SVN revision 13090), the basic meterpreter image `default_meterpreter.exe` is detected by 26 of 43 antivirus engines (60%) listed at VirusTotal.

The definitely easiest way to reduce AV detection is using a different EXE template. Almost any native Win32 EXE file can be used, and a typical Windows user has thousands of them on his hard disk. Just pick one and AV detection will go down. The more exotic the software, the better. For this example, I chose `notepad.exe` from a German WinXP SP3 installation.

The default executable template (`msf3\data\templates\template_x86_windows.exe`) is detected by 3 AV engines (CAT-QuickHeal, SUPERAntiSpyware, VirusBuster) as malicious. Conversely, any other Meterpreter payload built from a different template is **not** detected by these three AV engines. For 4 other AV engines (AhnLab-V3, Emsisoft, Ikarus, Panda), the templates themselves are not detected, but payloads built from that template are detected, but not the payloads from the Notepad template. Therefore, just by using a custom template, you can reduce the detection rate from 26 to 19 engines (44%).

Improving payload encoders is much harder, especially since the `x86/shikata_ga_nai` encoder (that uses a polymorphic decoder stub) is excellent for evasion. Testing this option is easy, by testing with EXE files without a payload at all. If they are still detected, encoders will not be able to help avoid detection either. When looking at the overall results, there is not a single antivirus where removing the payload improves detection in all cases. For 6 of them (BitDefender, Emsisoft, F-Secure, Ikarus, NOD32, nProtect), removing the payload sometimes dereases the detection rate, but not in all cases.

As a conclusion, considering the amount of time that would be needed to improve encoders further, improvement of encoders is basically only interesting if it also helps evasion of IDS/IPS or similar systems. We will look at different options in this article, though.

As scriptjunkie wrote in his article, tracing from the entry point over the nop sled to the jump that jumps to the RWX stub is quite easy to do. In case AV is using it for detection, it might be an option to look at opportunities to make that code more complex.

To test this, I modified the EXE generator so that it does not fix the entry point at all, resulting in broken executables that do not run the payload. On the other hand, all the evil code (RWX stub and payload) is still in there, so if the AV does not trace execution but detect the payload in another way, it should still detect the file. The following patch was used to achieve this:

The resulting files were only detected by one antivirus engines (DrWeb); although they still contain the full payload and RWX stub. Some people will now start complaining again that it is pointless to AV check files that do not run at all. To prove them wrong, I tried a simple modification to the encoder so that it does not create a relative jump, but an indirect one to a register that is initialized via XORing two values. I also added a small loop to make tracing the execution flow harder. The following patch was used to achieve this:

That way, the binary without a payload was only detected by 4 AV engines, and a binary with meterpreter was detected by 9 AV engines, which is quite an improvement from 19 engines, considering this primitive way of obfuscation.

Just to make it clear, I do not propose applying this patch to Metasploit - it is easy for the AV guys to update their detections. But having some more complicated way of jumping to the entry point (using polymorphic code, for example) could help quite a bit to reduce AV detection and I think it is easier to write polymorphic "jump anywhere" code than a polymorphic RWX stub...

Obfuscation of the RWX stub is hard, especially since you cannot use self-modifying code. So to obfuscate the RWX stub, you are basically limited to replacing opcodes by others with same/similar effect, and to reordering parts. An alternative might be to do a simple "VM" that reads instructions from heap or stack, because it can modify the instructions there; however, this is quite some amount of work with no guarantee that it will help for long.

To assess the potential success of this method, I tried to build executables that do not make the memory RWX before executing it, using the following patch:

The resulting files were still detected by AVG and DrWeb; when comparing them with the other "broken" files (with the bad entry point), they do not perform better, but actually they perform worse in the sense that only the nop sled seems to be sufficient to make AVG detect it as malicious, while AVG did not detect the executables with the modified entry point. On the other hand, the file with the XORed entry point was detected by AVG again, increasing the probability that it is indeed the nop sled (without the following jump) that make AVG detect the file.

Considering the vast amount of time needed to make a new rwx stub, combined with the low success chance (it will not help against AVG or DrWeb), I'll skip this option for now, and look at the other ones.

Metasploit includes an "old" option called exe-small to build executables from a template that reserves space for the payload and stores its length at a fixed position. Using this template method, no part of the text section has to be modified dynamically, therefore reducing the risk of heuristics detecting the file. On the other hand, the text section is static, making it easy to detect a given sample with static signatures. Therefore, once such a sample is used (and maybe uploaded to VirusTotal, either by you or by your target), the sample has to be considered "burnt" in the sense that a few hours to days later, most AVs will detect your samples with ease. This makes it hard to test the effectiveness of this approach, especially if you want to use the generated samples (if you test them, they will be useless afterwards).

I built a small exe sample using VC++ Express 2008 by creating a console application project without precompiled headers and changed the Runtime Library option from /MTD to /MT (so that it does not link against VC runtime DLLs).

A small patch was required to make Metasploit detect the new template and properly make the section RWX:

(Un-)Fortunately, even the empty template without payload was detected by one antivirus, probably because of that RWX section. Let's try again, this time without the code that makes the section RWX (commenting out the two lines changed by the patch above) but instead copying the payload ourselves into RWX memory:

Now, the empty payload does not trigger any antivirus (which is correct, since it is not malicious; but at least no heuristics caught this template) and the meterpreter payload is detected only by Microsoft, Kaspersky, F-Secure and other engines that I think use either of these engines, resulting in a 6 of 43 detection rate (14%).

The next question that arises: Do those 6 antivirus detect the shikata_ga_nai encoder or do they sandbox the executable and detect the real behaviour (reverse shell)? To test this, I built an executable that uses an empty payload, but encoded with shikata_ga_nai 10 times:

This template is also detected by none of the antivirus engines; the shikata_ga_nai encoder is not the culprit of detection.

As a conclusion, if you have the time and skill to design your own exe stub, it is the best option of all the options tried by now. But remember that you cannot use it very often, since creating signatures for it is very easy (definitely easier than writing the new stub, and also a lot easier than deobfuscating the entry point nop sled), so it is a good option only for "important" targets (or ones where you can be pretty sure it will not be detected). If you have to target one of the antivirus engines that use sandboxing, you will have to evade this separately, though.

To evade sandboxing, there are basically three ways I can think of (maybe there are more):

- Try to use more computing power/time than the sandbox allows you to have
- Call API functions that are hard to emulate, or API functions that indicate the application has started/finished in the hope that the antivirus will give up
- Call API functions where you think a sandbox will emulate them incorrectly, and verify the result; if incorrect, stop immediately (similar to what some current malware does when it detects a VM to complicate reversing)

I thought of a simple code snippet that tries to implement all the three ways: The first one is done by a Sleep() call, the second one by calling PeekMessage (which usually indicates the application finished initializing), and the third one by verifying with GetTickCount that the Sleep call really slept (in case the sandbox just implemented Sleep as a no-op) and by verifying that the received message is really the same that was posted. Of course, there are more sophisticated ways, like starting multiple threads, doing interlocked operations and verifying the results and the timing, but I wanted to start simple.

As a result, almost all previous detections went away - only Microsoft and Kaspersky still believe this is malicious. On the other hand, that code seems to trigger a new heuristic in Sophos, increasing the number of antivirus that still detects the sample to 3 of 43 (7%). Sandbox evasion can be quite effective if your target AV is using it, you just have to be careful not triggering new heuristics with them... It should be possible to put the sandbox evasion into a Metasploit encoder (that prepends it) and encoding the result further to make it harder to detect; this is left as an exercise to the reader, though.

To be continued? I doubt it will get better than 3 of 43...

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.07.01	2011.07.07	-
AntiVir	7.11.10.246	2011.07.07	-

Antiy-AVL	2.0.3.7	2011.07.07	-
Avast	4.8.1351.0	2011.07.06	-
Avast5	5.0.677.0	2011.07.06	-
AVG	10.0.0.1190	2011.07.06	-
BitDefender	7.2	2011.07.07	-
CAT-QuickHeal	11.00	2011.07.08	Win32.Trojan.Swrort.A.4
ClamAV	0.97.0.0	2011.07.07	-
Commtouch	5.3.2.6	2011.07.07	-
Comodo	9303	2011.07.07	-
DrWeb	5.0.2.03300	2011.07.07	-
Emsisoft	5.1.0.8	2011.07.07	-
eSafe	7.0.17.0	2011.07.06	-
eTrust-Vet	36.1.8429	2011.07.06	-
F-Prot	4.6.2.117	2011.07.08	-
F-Secure	9.0.16440.0	2011.07.07	-
Fortinet	4.2.257.0	2011.07.07	-
GData	22	2011.07.07	-
Ikarus	T3.1.1.104.0	2011.07.07	-
Jiangmin	13.0.900	2011.07.06	-
K7AntiVirus	9.107.4883	2011.07.07	-
Kaspersky	9.0.0.837	2011.07.07	-
McAfee	5.400.0.1158	2011.07.08	-
McAfee-GW-Edition	2010.1D	2011.07.07	-
Microsoft	1.7000	2011.07.07	-
NOD32	6275	2011.07.08	-
Norman	6.07.10	2011.07.07	-
nProtect	2011-07-07.01	2011.07.07	-

Panda	10.0.3.5	2011.07.06	-
PCTools	8.0.0.5	2011.07.07	-
Prevx	3.0	2011.07.09	-
Rising	23.65.02.03	2011.07.06	-
Sophos	4.67.0	2011.07.07	-
SUPERAntiSpyware	4.40.0.1006	2011.07.07	Trojan.Backdoor-PoisonIvy
Symantec	20111.1.0.186	2011.07.07	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.07	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.07	-
VBA32	3.12.16.4	2011.07.06	-
VIPRE	9792	2011.07.07	-
ViRobot	2011.7.7.4555	2011.07.07	-
VirusBuster	14.0.114.0	2011.07.07	Trojan.Rosena.Gen.1

Antivirus	**Version**	**Last update**	**Result**
AhnLab-V3	2011.07.09.00	2011.07.08	-
AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.08	-
Avast	4.8.1351.0	2011.07.09	-
Avast5	5.0.677.0	2011.07.09	-
AVG	10.0.0.1190	2011.07.09	-
BitDefender	7.2	2011.07.09	-
CAT-QuickHeal	11.00	2011.07.09	-
ClamAV	0.97.0.0	2011.07.09	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9325	2011.07.09	-
DrWeb	5.0.2.03300	2011.07.09	-

Emsisoft	5.1.0.8	2011.07.09	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.08	-
F-Secure	9.0.16440.0	2011.07.09	-
Fortinet	4.2.257.0	2011.07.09	-
GData	22	2011.07.09	-
Ikarus	T3.1.1.104.0	2011.07.09	-
Jiangmin	13.0.900	2011.07.08	-
K7AntiVirus	9.107.4887	2011.07.08	-
Kaspersky	9.0.0.837	2011.07.09	-
McAfee	5.400.0.1158	2011.07.09	-
McAfee-GW-Edition	2010.1D	2011.07.09	-
Microsoft	1.7000	2011.07.09	-
NOD32	6278	2011.07.09	-
Norman	6.07.10	2011.07.09	-
nProtect	2011-07-09.01	2011.07.09	-
Panda	10.0.3.5	2011.07.09	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.09	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.09	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.09	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.09	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.09	-

VBA32	3.12.16.4	2011.07.08	-
VIPRE	9813	2011.07.09	-
ViRobot	2011.7.9.4560	2011.07.09	-
VirusBuster	14.0.115.1	2011.07.08	-

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.07.01	2011.07.07	Trojan/Win32.Shell
AntiVir	7.11.10.246	2011.07.07	TR/Crypt.EPACK.Gen2
Antiy-AVL	2.0.3.7	2011.07.07	-
Avast	4.8.1351.0	2011.07.06	Win32:SwPatch [Wrm]
Avast5	5.0.677.0	2011.07.06	Win32:SwPatch [Wrm]
AVG	10.0.0.1190	2011.07.06	Win32/Heur
BitDefender	7.2	2011.07.07	Backdoor.Shell.AC
CAT-QuickHeal	11.00	2011.07.08	Trojan.Swrort.A
ClamAV	0.97.0.0	2011.07.07	-
Commtouch	5.3.2.6	2011.07.07	W32/Swrort.A.gen!Eldorado
Comodo	9303	2011.07.07	-
DrWeb	5.0.2.03300	2011.07.07	Trojan.Swrort.1
Emsisoft	5.1.0.8	2011.07.07	Trojan.Win32.Swrort!IK
eSafe	7.0.17.0	2011.07.06	-
eTrust-Vet	36.1.8429	2011.07.06	-
F-Prot	4.6.2.117	2011.07.08	W32/Swrort.A.gen!Eldorado
F-Secure	9.0.16440.0	2011.07.07	Backdoor.Shell.AC
Fortinet	4.2.257.0	2011.07.07	-
GData	22	2011.07.07	Backdoor.Shell.AC
Ikarus	T3.1.1.104.0	2011.07.07	Trojan.Win32.Swrort
Jiangmin	13.0.900	2011.07.06	-
K7AntiVirus	9.107.4883	2011.07.07	Riskware

Kaspersky	9.0.0.837	2011.07.07	HEUR:Trojan.Win32.Generic
McAfee	5.400.0.1158	2011.07.08	Swrort.d
McAfee-GW-Edition	2010.1D	2011.07.07	Swrort.d
Microsoft	1.7000	2011.07.07	Trojan:Win32/Swrort.A
NOD32	6275	2011.07.08	a variant of Win32/Rozena.AA
Norman	6.07.10	2011.07.07	-
nProtect	2011-07-07.01	2011.07.07	Backdoor.Shell.AC
Panda	10.0.3.5	2011.07.06	Trj/Genetic.gen
PCTools	8.0.0.5	2011.07.07	-
Prevx	3.0	2011.07.09	-
Rising	23.65.02.03	2011.07.06	-
Sophos	4.67.0	2011.07.07	Mal/Swrort-C
SUPERAntiSpyware	4.40.0.1006	2011.07.07	Trojan.Backdoor-PoisonIvy
Symantec	20111.1.0.186	2011.07.07	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.07	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.07	-
VBA32	3.12.16.4	2011.07.06	-
VIPRE	9792	2011.07.07	Trojan.Win32.Swrort.B (v)
ViRobot	2011.7.7.4555	2011.07.07	-
VirusBuster	14.0.114.0	2011.07.07	Trojan.Rosena.Gen.1

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.09.00	2011.07.08	Trojan/Win32.Shell
AntiVir	7.11.11.45	2011.07.08	TR/Crypt.EPACK.Gen2
Antiy-AVL	2.0.3.7	2011.07.08	-
Avast	4.8.1351.0	2011.07.09	Win32:SwPatch
Avast5	5.0.677.0	2011.07.09	Win32:SwPatch

AVG	10.0.0.1190	2011.07.09	Win32/Heur
BitDefender	7.2	2011.07.09	Gen:Variant.Patched.2
CAT-QuickHeal	11.00	2011.07.09	Trojan.Swrort.A
ClamAV	0.97.0.0	2011.07.09	-
Commtouch	5.3.2.6	2011.07.09	W32/Swrort.A.gen!Eldorado
Comodo	9328	2011.07.09	-
DrWeb	5.0.2.03300	2011.07.09	Trojan.Swrort.1
Emsisoft	5.1.0.8	2011.07.09	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.08	W32/Swrort.A.gen!Eldorado
F-Secure	9.0.16440.0	2011.07.09	Gen:Variant.Patched.2
Fortinet	4.2.257.0	2011.07.09	-
GData	22	2011.07.09	Gen:Variant.Patched.2
Ikarus	T3.1.1.104.0	2011.07.09	-
Jiangmin	13.0.900	2011.07.08	-
K7AntiVirus	9.107.4887	2011.07.08	Riskware
Kaspersky	9.0.0.837	2011.07.09	HEUR:Trojan.Win32.Generic
McAfee	5.400.0.1158	2011.07.09	Swrort.d
McAfee-GW-Edition	2010.1D	2011.07.09	Swrort.d
Microsoft	1.7000	2011.07.09	Trojan:Win32/Swrort.A
NOD32	6279	2011.07.09	a variant of Win32/Rozena.AS
Norman	6.07.10	2011.07.09	-
nProtect	2011-07-09.01	2011.07.09	Gen:Variant.Patched.2
Panda	10.0.3.5	2011.07.09	Trj/Genetic.gen
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.09	-

Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.09	Mal/Swrort-C
SUPERAntiSpyware	4.40.0.1006	2011.07.09	Trojan.Backdoor-PoisonIvy
Symantec	20111.1.0.186	2011.07.09	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.09	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.09	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9813	2011.07.09	Trojan.Win32.Swrort.B (v)
ViRobot	2011.7.9.4560	2011.07.09	-
VirusBuster	14.0.115.1	2011.07.08	Trojan.Rosena.Gen.1

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.09.00	2011.07.08	-
AntiVir	7.11.11.45	2011.07.08	TR/Crypt.EPACK.Gen2
Antiy-AVL	2.0.3.7	2011.07.08	-
Avast	4.8.1351.0	2011.07.09	Win32:SwPatch [Wrm]
Avast5	5.0.677.0	2011.07.09	Win32:SwPatch [Wrm]
AVG	10.0.0.1190	2011.07.09	Win32/Heur
BitDefender	7.2	2011.07.09	Backdoor.Shell.AC
CAT-QuickHeal	11.00	2011.07.09	-
ClamAV	0.97.0.0	2011.07.09	-
Commtouch	5.3.2.6	2011.07.09	W32/Swrort.B.gen!Eldorado
Comodo	9328	2011.07.09	-
DrWeb	5.0.2.03300	2011.07.09	Trojan.Swrort.1
Emsisoft	5.1.0.8	2011.07.09	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-

F-Prot	4.6.2.117	2011.07.08	W32/Swrort.B.gen!Eldorado
F-Secure	9.0.16440.0	2011.07.09	Backdoor.Shell.AC
Fortinet	4.2.257.0	2011.07.09	-
GData	22	2011.07.09	Backdoor.Shell.AC
Ikarus	T3.1.1.104.0	2011.07.09	-
Jiangmin	13.0.900	2011.07.08	-
K7AntiVirus	9.107.4887	2011.07.08	Riskware
Kaspersky	9.0.0.837	2011.07.09	HEUR:Trojan.Win32.Generic
McAfee	5.400.0.1158	2011.07.09	Swrort.f
McAfee-GW-Edition	2010.1D	2011.07.09	Swrort.f
Microsoft	1.7000	2011.07.09	Trojan:Win32/Swrort.A
NOD32	6279	2011.07.09	a variant of Win32/Rozena.AH
Norman	6.07.10	2011.07.09	-
nProtect	2011-07-09.01	2011.07.09	Backdoor.Shell.AC
Panda	10.0.3.5	2011.07.09	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.09	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.09	Mal/Swrort-C
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.09	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.09	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.09	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9813	2011.07.09	Trojan.Win32.Swrort.B (v)
ViRobot	2011.7.9.4560	2011.07.09	-

VirusBuster	14.0.115.1	2011.07.08	-

Additional information

MD5: 99addd5248236a60aeddbc35024cd2ab

SHA1: c301f74eaa7758734ccc05c5c2832b2398fd9b01

SHA256: 814f72c11bf033d94d35573e47e75646ff13c28221b842a398f0fa1dd21cb596

File size: 73802 bytes

Scan date: 2011-07-09 14:33:12 (UTC)

Additional information

MD5: 8a29b5b5a881c6709f31ff5203f0fac9

SHA1: 9830c89ace9de8b6df83f11795abf30b60f528a9

SHA256: 8f1e5763839c7f5443ef7ee7c8b11bb423b0eadb4b4f8d9bd2e5b406ceb2a781

File size: 70144 bytes

Scan date: 2011-07-09 12:36:41 (UTC)

Additional information

MD5: 3c915479051a19fe98de4fdabc27d021

SHA1: ed50f6dde7f5268d90d99ad2f90d7009b38124a4

SHA256: 1da67224417944b7912bad1c0c539d01a7408c3e30ff9293b62fb751fe860ec0

File size: 73803 bytes

Scan date: 2011-07-09 13:24:18 (UTC)

Additional information

MD5: 292cbc755151d1101102f3ab0db06036

SHA1: a22e6d9dc8b8b5f510f7979b1f69c5b82d7a75fd

SHA256: ecad74a8388c08a406c7e1269eee5b55fa76f54e1bae478b39be4fb41b074cc0

File size: 73803 bytes

Scan date: 2011-07-09 13:18:05 (UTC)

Additional information

MD5: a7e8d86f70a3f9473a8dca70076ac623

SHA1: 8d29cfd9afc49f9a408894070b3959a7d7f5249e

SHA256: 2237e22f1b063a9fa7c2fb9a7b577e12b8989a74d3df6720f70123e4149a4244

File size: 70145 bytes

Scan date: 2011-07-09 13:20:56 (UTC)

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.09.00	2011.07.08	-
AntiVir	7.11.11.45	2011.07.08	TR/Crypt.EPACK.Gen2
Antiy-AVL	2.0.3.7	2011.07.08	-
Avast	4.8.1351.0	2011.07.09	Win32:SwPatch [Wrm]
Avast5	5.0.677.0	2011.07.09	Win32:SwPatch [Wrm]
AVG	10.0.0.1190	2011.07.09	Win32/Heur
BitDefender	7.2	2011.07.09	-
CAT-QuickHeal	11.00	2011.07.09	-
ClamAV	0.97.0.0	2011.07.09	-
Commtouch	5.3.2.6	2011.07.09	W32/Swrort.B.gen!Eldorado
Comodo	9328	2011.07.09	-
Emsisoft	5.1.0.8	2011.07.09	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.08	W32/Swrort.B.gen!Eldorado
F-Secure	9.0.16440.0	2011.07.09	-
Fortinet	4.2.257.0	2011.07.09	-
GData	22	2011.07.09	Win32:SwPatch
Ikarus	T3.1.1.104.0	2011.07.09	-
Jiangmin	13.0.900	2011.07.08	-

K7AntiVirus	9.107.4887	2011.07.08	Riskware
Kaspersky	9.0.0.837	2011.07.09	HEUR:Trojan.Win32.Generic
McAfee	5.400.0.1158	2011.07.09	Swrort.d
McAfee-GW-Edition	2010.1D	2011.07.09	Swrort.d
Microsoft	1.7000	2011.07.09	Trojan:Win32/Swrort.A
NOD32	6279	2011.07.09	-
Norman	6.07.10	2011.07.09	-
nProtect	2011-07-09.01	2011.07.09	-
Panda	10.0.3.5	2011.07.09	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.09	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.09	Mal/Swrort-C
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.09	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.09	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.09	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9813	2011.07.09	Trojan.Win32.Swrort.B (v)
ViRobot	2011.7.9.4560	2011.07.09	-
VirusBuster	14.0.115.1	2011.07.08	-

Additional information

MD5: 3f231ff4e57caaedb4a95eea4cc1d626

SHA1: 7f93736091bff6409be9ed44c637cecea58cd340

SHA256: 000095fd3d919c235f3bfc3b717c0652959b9ab59fc4dc699ef73b92e3ba8af3

File size: 70145 bytes

Scan date: 2011-07-09 13:22:34 (UTC)

Additional information

MD5: ca64f5016c6dfb90d517ded4074444e7

SHA1: c5453ce82daa312538f9d2c4a62de678c20cc29c

SHA256: 8d64cdea4caed41c10f4e8df3cbdd04000bab7251d5995d14568c6715018e55e

File size: 70145 bytes

Scan date: 2011-07-09 18:15:01 (UTC)

Additional information

MD5: db9c0ca624fa95fb3b71832befbd9655

SHA1: f79cde024a8a744878019ce420759aa81a4951ab

SHA256: d25468d87e4e677ea106bfd4da3f85e6c568556d933c082106fd34760b013aa4

File size: 70145 bytes

Scan date: 2011-07-09 18:16:53 (UTC)

Additional information

MD5: 88df7d9f6f6a813898c0a51725af249a

SHA1: 76d7c6f628bcb5980dd25fefb5299f0516a2e127

SHA256: a8a0e6794092393aa48fa99b67c8e79da07a037bf3281d17233fe7a848a373f7

File size: 70145 bytes

Scan date: 2011-07-09 19:39:55 (UTC)

Additional information

MD5: d8b595c0b1847cc4b8d9336559a9249f

SHA1: 26462902466e2067a02cc1459003fb92091ffe1b

SHA256: a5a1537c76fc0c9776b1ae30b4b2c9562d17f257aa735f44e02aeeef3ce61e96

File size: 70145 bytes

Scan date: 2011-07-09 19:41:44 (UTC)

Additional information
MD5: 08408325f4b213d3397942548f8b7d73
SHA1: 45e88b91937d49e650b933082277ee30e9ccc3d6
SHA256: e7b9c016d5b099370b6a664d8a8bc2fdbab25524aa61963b137b29256ce14437
File size: 70145 bytes
Scan date: 2011-07-10 11:08:45 (UTC)

Additional information
MD5: 8af8fa0d364b61b63a6d95dadd06b0c5
SHA1: 9924993eb0e578d69f6045e59a1705053a9819b3
SHA256: 387fe8b710782d5358da4c2e590f4c693dbd9d11944b2707dcf00d28348b830a
File size: 45612 bytes
Scan date: 2011-07-10 12:00:12 (UTC)

Additional information
MD5: 8af8fa0d364b61b63a6d95dadd06b0c5
SHA1: 9924993eb0e578d69f6045e59a1705053a9819b3
SHA256: 387fe8b710782d5358da4c2e590f4c693dbd9d11944b2707dcf00d28348b830a
File size: 45612 bytes
Scan date: 2011-07-10 12:00:12 (UTC)

Additional information
MD5: 4853b2a430fdd90c624a98013767e1fe
SHA1: 66f179cd4f38b6d2b0952c1db4890dc19fe79015
SHA256: 44ad92d3b918dff3b847e473e9d21a0741087b44df588354ce57d4ac1646d1b1
File size: 45592 bytes
Scan date: 2011-07-10 11:55:31 (UTC)

Additional information

MD5: eb30f25063035781debe461c3ad4c96d

SHA1: 59b3557cede21c179bafe5cb92ab34cba5155b42

SHA256: b41defcdf1ec28c85ed21e97a1ba4556b4e4bd4291c7ade0fc2aeac38dae625c

File size: 45633 bytes

Scan date: 2011-07-10 12:18:41 (UTC)

Additional information

MD5: 26fe79da63ff00f5f99667949e09eb6a

SHA1: e1169f7a1b9c2565421b889f3695a014ebc6443d

SHA256: 81c28ae7edb8d27f035953deab55c7e374706fbe35271b08f0410c64f2d001e8

File size: 45610 bytes

Scan date: 2011-07-10 12:15:38 (UTC)

Additional information

MD5: a6d0be6d7178bb53a65071700ca0cf81

SHA1: 5f487b855772da4a619bad4b341fece41204583b

SHA256: 6bcc6009e474ae7b492591c7f68843f2e8bf20870574eeecb912f2e850a1f473

File size: 45582 bytes

Scan date: 2011-07-10 13:31:19 (UTC)

Additional information

MD5: d992fa49dd63caf87baeeb36cdd96ee7

SHA1: b6d96467320ca03d111c8f4594ccd90bb8177ce0

SHA256: 543978da6f38c9ee2c06feb9879decbe815ab02b83f353d789d8bc715020b2d6

File size: 46145 bytes

Scan date: 2011-07-10 18:35:17 (UTC)

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.10.00	2011.07.09	-

AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.09	-
Avast	4.8.1351.0	2011.07.09	-
Avast5	5.0.677.0	2011.07.09	-
AVG	10.0.0.1190	2011.07.09	-
BitDefender	7.2	2011.07.09	-
CAT-QuickHeal	11.00	2011.07.09	-
ClamAV	0.97.0.0	2011.07.09	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9328	2011.07.09	-
DrWeb	5.0.2.03300	2011.07.09	Trojan.Swrort.1
Emsisoft	5.1.0.8	2011.07.09	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.09	-
F-Secure	9.0.16440.0	2011.07.09	-
Fortinet	4.2.257.0	2011.07.09	-
GData	22	2011.07.09	-
Ikarus	T3.1.1.104.0	2011.07.09	-
Jiangmin	13.0.900	2011.07.09	-
K7AntiVirus	9.107.4887	2011.07.08	-
Kaspersky	9.0.0.837	2011.07.09	-
McAfee	5.400.0.1158	2011.07.09	-
McAfee-GW-Edition	2010.1D	2011.07.09	-
Microsoft	1.7000	2011.07.09	-
NOD32	6279	2011.07.09	a variant of Win32/Kryptik.EVQ
Norman	6.07.10	2011.07.09	-

nProtect	2011-07-09.01	2011.07.09	-
Panda	10.0.3.5	2011.07.09	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.09	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.09	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.09	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.09	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.09	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9816	2011.07.09	-
ViRobot	2011.7.9.4560	2011.07.09	-
VirusBuster	14.0.116.0	2011.07.09	-

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.10.00	2011.07.09	-
AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.09	-
Avast	4.8.1351.0	2011.07.09	-
Avast5	5.0.677.0	2011.07.09	-
AVG	10.0.0.1190	2011.07.09	-
BitDefender	7.2	2011.07.09	-
CAT-QuickHeal	11.00	2011.07.09	-
ClamAV	0.97.0.0	2011.07.09	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9328	2011.07.09	-

DrWeb	5.0.2.03300	2011.07.09	Trojan.Swrort.1
Emsisoft	5.1.0.8	2011.07.09	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.09	-
F-Secure	9.0.16440.0	2011.07.09	-
Fortinet	4.2.257.0	2011.07.09	-
GData	22	2011.07.09	-
Ikarus	T3.1.1.104.0	2011.07.09	-
Jiangmin	13.0.900	2011.07.09	-
K7AntiVirus	9.107.4887	2011.07.08	-
Kaspersky	9.0.0.837	2011.07.09	-
McAfee	5.400.0.1158	2011.07.09	-
McAfee-GW-Edition	2010.1D	2011.07.09	-
Microsoft	1.7000	2011.07.09	-
NOD32	6279	2011.07.09	-
Norman	6.07.10	2011.07.09	-
nProtect	2011-07-09.01	2011.07.09	-
Panda	10.0.3.5	2011.07.09	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.09	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.09	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.09	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.09	-

TrendMicro-HouseCall	9.200.0.1012	2011.07.09	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9816	2011.07.09	-
ViRobot	2011.7.9.4560	2011.07.09	-
VirusBuster	14.0.116.0	2011.07.09	-

Antivirus	**Version**	**Last update**	**Result**
AhnLab-V3	2011.07.10.00	2011.07.09	-
AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.09	-
Avast	4.8.1351.0	2011.07.09	-
Avast5	5.0.677.0	2011.07.09	-
AVG	10.0.0.1190	2011.07.09	Win32/Heur
BitDefender	7.2	2011.07.09	Backdoor.Shell.AC
CAT-QuickHeal	11.00	2011.07.09	-
ClamAV	0.97.0.0	2011.07.09	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9328	2011.07.09	-
DrWeb	5.0.2.03300	2011.07.09	Trojan.Swrort.1
Emsisoft	5.1.0.8	2011.07.09	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.09	-
F-Secure	9.0.16440.0	2011.07.09	Backdoor.Shell.AC
Fortinet	4.2.257.0	2011.07.09	-
GData	22	2011.07.09	Backdoor.Shell.AC
Ikarus	T3.1.1.104.0	2011.07.09	-
Jiangmin	13.0.900	2011.07.09	-

K7AntiVirus	9.107.4887	2011.07.08	-
Kaspersky	9.0.0.837	2011.07.09	HEUR:Trojan.Win32.Generic
McAfee	5.400.0.1158	2011.07.09	-
McAfee-GW-Edition	2010.1D	2011.07.09	-
Microsoft	1.7000	2011.07.09	Trojan:Win32/Swrort.A
NOD32	6280	2011.07.09	a variant of Win32/Rozena.AH
Norman	6.07.10	2011.07.09	-
nProtect	2011-07-09.01	2011.07.09	Backdoor.Shell.AC
Panda	10.0.3.5	2011.07.09	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.09	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.09	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.09	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.09	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.09	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9817	2011.07.09	-
ViRobot	2011.7.9.4560	2011.07.09	-
VirusBuster	14.0.116.0	2011.07.09	-

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.10.00	2011.07.09	-
AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.09	-
Avast	4.8.1351.0	2011.07.09	-

Avast5	5.0.677.0	2011.07.09	-
AVG	10.0.0.1190	2011.07.09	Win32/Heur
BitDefender	7.2	2011.07.09	-
CAT-QuickHeal	11.00	2011.07.09	-
ClamAV	0.97.0.0	2011.07.09	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9328	2011.07.09	-
DrWeb	5.0.2.03300	2011.07.09	Trojan.Swrort.1
Emsisoft	5.1.0.8	2011.07.09	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.09	-
F-Secure	9.0.16440.0	2011.07.09	-
Fortinet	4.2.257.0	2011.07.09	-
GData	22	2011.07.09	-
Ikarus	T3.1.1.104.0	2011.07.09	-
Jiangmin	13.0.900	2011.07.09	-
K7AntiVirus	9.107.4887	2011.07.08	-
Kaspersky	9.0.0.837	2011.07.09	HEUR:Trojan.Win32.Generic
McAfee	5.400.0.1158	2011.07.09	-
McAfee-GW-Edition	2010.1D	2011.07.09	-
Microsoft	1.7000	2011.07.09	Trojan:Win32/Swrort.A
NOD32	6280	2011.07.09	-
Norman	6.07.10	2011.07.09	-
nProtect	2011-07-09.01	2011.07.09	-
Panda	10.0.3.5	2011.07.09	-
PCTools	8.0.0.5	2011.07.08	-

Prevx	3.0	2011.07.09	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.09	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.09	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.09	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.09	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9817	2011.07.09	-
ViRobot	2011.7.9.4560	2011.07.09	-
VirusBuster	14.0.116.0	2011.07.09	-

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.10.00	2011.07.09	-
AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.10	-
Avast	4.8.1351.0	2011.07.10	-
Avast5	5.0.677.0	2011.07.10	-
AVG	10.0.0.1190	2011.07.10	Win32/Heur
BitDefender	7.2	2011.07.10	-
CAT-QuickHeal	11.00	2011.07.10	-
ClamAV	0.97.0.0	2011.07.10	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9337	2011.07.10	-
DrWeb	5.0.2.03300	2011.07.10	Trojan.Packed.196
Emsisoft	5.1.0.8	2011.07.10	-
eSafe	7.0.17.0	2011.07.07	-

eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.09	-
F-Secure	9.0.16440.0	2011.07.10	-
Fortinet	4.2.257.0	2011.07.10	-
GData	22	2011.07.10	-
Ikarus	T3.1.1.104.0	2011.07.10	-
Jiangmin	13.0.900	2011.07.09	-
K7AntiVirus	9.108.4891	2011.07.10	-
Kaspersky	9.0.0.837	2011.07.10	-
McAfee	5.400.0.1158	2011.07.10	-
McAfee-GW-Edition	2010.1D	2011.07.09	-
Microsoft	1.7000	2011.07.10	-
NOD32	6280	2011.07.10	-
Norman	6.07.10	2011.07.10	-
nProtect	2011-07-10.01	2011.07.10	-
Panda	10.0.3.5	2011.07.09	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.10	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.10	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.10	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.10	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.10	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9822	2011.07.10	-

ViRobot	2011.7.9.4560	2011.07.10	-
VirusBuster	14.0.116.0	2011.07.09	-

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.11.00	2011.07.10	-
AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.10	-
Avast	4.8.1351.0	2011.07.10	-
Avast5	5.0.677.0	2011.07.10	-
AVG	10.0.0.1190	2011.07.10	-
BitDefender	7.2	2011.07.10	Backdoor.Shell.AC
CAT-QuickHeal	11.00	2011.07.10	-
ClamAV	0.97.0.0	2011.07.10	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9337	2011.07.10	-
DrWeb	5.0.2.03300	2011.07.10	-
Emsisoft	5.1.0.8	2011.07.10	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.09	-
F-Secure	9.0.16440.0	2011.07.10	Backdoor.Shell.AC
Fortinet	4.2.257.0	2011.07.10	-
GData	22	2011.07.10	Backdoor.Shell.AC
Ikarus	T3.1.1.104.0	2011.07.10	-
Jiangmin	13.0.900	2011.07.09	-
K7AntiVirus	9.108.4891	2011.07.10	-
Kaspersky	9.0.0.837	2011.07.10	HEUR:Trojan.Win32.Generic

McAfee	5.400.0.1158	2011.07.10	-
McAfee-GW-Edition	2010.1D	2011.07.09	Heuristic.LooksLike.Win32.Suspicious.J!80
Microsoft	1.7000	2011.07.10	Trojan:Win32/Swrort.A
NOD32	6280	2011.07.10	-
Norman	6.07.10	2011.07.10	-
nProtect	2011-07-10.01	2011.07.10	Backdoor.Shell.AC
Panda	10.0.3.5	2011.07.10	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.10	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.10	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.10	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.10	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.10	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9823	2011.07.10	-
ViRobot	2011.7.9.4560	2011.07.10	-
VirusBuster	14.0.116.0	2011.07.09	-

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.11.00	2011.07.10	-
AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.10	-
Avast	4.8.1351.0	2011.07.10	-

Avast5	5.0.677.0	2011.07.10	-
AVG	10.0.0.1190	2011.07.10	-
BitDefender	7.2	2011.07.10	Backdoor.Shell.AC
CAT-QuickHeal	11.00	2011.07.10	-
ClamAV	0.97.0.0	2011.07.10	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9337	2011.07.10	-
DrWeb	5.0.2.03300	2011.07.10	-
Emsisoft	5.1.0.8	2011.07.10	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.09	-
F-Secure	9.0.16440.0	2011.07.10	Backdoor.Shell.AC
Fortinet	4.2.257.0	2011.07.10	-
GData	22	2011.07.10	Backdoor.Shell.AC
Ikarus	T3.1.1.104.0	2011.07.10	-
Jiangmin	13.0.900	2011.07.09	-
K7AntiVirus	9.108.4891	2011.07.10	-
Kaspersky	9.0.0.837	2011.07.10	HEUR:Trojan.Win32.Generic
McAfee	5.400.0.1158	2011.07.10	-
McAfee-GW-Edition	2010.1D	2011.07.09	Heuristic.LooksLike.Win32.Suspicious.J!80
Microsoft	1.7000	2011.07.10	Trojan:Win32/Swrort.A
NOD32	6280	2011.07.10	-
Norman	6.07.10	2011.07.10	-
nProtect	2011-07-10.01	2011.07.10	Backdoor.Shell.AC
Panda	10.0.3.5	2011.07.10	-
PCTools	8.0.0.5	2011.07.08	-

Prevx	3.0	2011.07.10	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.10	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.10	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.10	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.10	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9823	2011.07.10	-
ViRobot	2011.7.9.4560	2011.07.10	-
VirusBuster	14.0.116.0	2011.07.09	-

Antivirus	**Version**	**Last update**	**Result**
AhnLab-V3	2011.07.11.00	2011.07.10	-
AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.10	-
Avast	4.8.1351.0	2011.07.10	-
Avast5	5.0.677.0	2011.07.10	-
AVG	10.0.0.1190	2011.07.10	-
BitDefender	7.2	2011.07.10	-
CAT-QuickHeal	11.00	2011.07.10	-
ClamAV	0.97.0.0	2011.07.10	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9337	2011.07.10	-
DrWeb	5.0.2.03300	2011.07.10	-
Emsisoft	5.1.0.8	2011.07.10	-

eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.09	-
F-Secure	9.0.16440.0	2011.07.10	-
Fortinet	4.2.257.0	2011.07.10	-
GData	22	2011.07.10	-
Ikarus	T3.1.1.104.0	2011.07.10	-
Jiangmin	13.0.900	2011.07.09	-
K7AntiVirus	9.108.4891	2011.07.10	-
Kaspersky	9.0.0.837	2011.07.10	-
McAfee	5.400.0.1158	2011.07.10	-
McAfee-GW-Edition	2010.1D	2011.07.09	Heuristic.LooksLike.Win32.Suspicious.J!80
Microsoft	1.7000	2011.07.10	-
NOD32	6280	2011.07.10	-
Norman	6.07.10	2011.07.10	-
nProtect	2011-07-10.01	2011.07.10	-
Panda	10.0.3.5	2011.07.10	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.10	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.10	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.10	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.10	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.10	-

VBA32	3.12.16.4	2011.07.08	-
VIPRE	9823	2011.07.10	-
ViRobot	2011.7.9.4560	2011.07.10	-
VirusBuster	14.0.116.0	2011.07.09	-

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.11.00	2011.07.10	-
AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.10	-
Avast	4.8.1351.0	2011.07.10	-
Avast5	5.0.677.0	2011.07.10	-
AVG	10.0.0.1190	2011.07.10	-
BitDefender	7.2	2011.07.10	Backdoor.Shell.AC
CAT-QuickHeal	11.00	2011.07.10	-
ClamAV	0.97.0.0	2011.07.10	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9337	2011.07.10	-
DrWeb	5.0.2.03300	2011.07.10	-
Emsisoft	5.1.0.8	2011.07.10	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.09	-
F-Secure	9.0.16440.0	2011.07.10	Backdoor.Shell.AC
Fortinet	4.2.257.0	2011.07.10	-
GData	22	2011.07.10	Backdoor.Shell.AC
Ikarus	T3.1.1.104.0	2011.07.10	-
Jiangmin	13.0.900	2011.07.09	-
K7AntiVirus	9.108.4891	2011.07.10	-

Kaspersky	9.0.0.837	2011.07.10	HEUR:Trojan.Win32.Generic
McAfee	5.400.0.1158	2011.07.10	-
McAfee-GW-Edition	2010.1D	2011.07.09	-
Microsoft	1.7000	2011.07.10	Trojan:Win32/Swrort.A
NOD32	6280	2011.07.10	-
Norman	6.07.10	2011.07.10	-
nProtect	2011-07-10.01	2011.07.10	Backdoor.Shell.AC
Panda	10.0.3.5	2011.07.10	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.10	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.10	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.10	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.10	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.10	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9823	2011.07.10	-
ViRobot	2011.7.9.4560	2011.07.10	-
VirusBuster	14.0.116.0	2011.07.09	-

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.11.00	2011.07.10	-
AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.10	-
Avast	4.8.1351.0	2011.07.10	-
Avast5	5.0.677.0	2011.07.10	-

AVG	10.0.0.1190	2011.07.10	-
BitDefender	7.2	2011.07.10	-
CAT-QuickHeal	11.00	2011.07.10	-
ClamAV	0.97.0.0	2011.07.10	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9337	2011.07.10	-
DrWeb	5.0.2.03300	2011.07.10	-
Emsisoft	5.1.0.8	2011.07.10	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.09	-
F-Secure	9.0.16440.0	2011.07.10	-
Fortinet	4.2.257.0	2011.07.10	-
GData	22	2011.07.10	-
Ikarus	T3.1.1.104.0	2011.07.10	-
Jiangmin	13.0.900	2011.07.09	-
K7AntiVirus	9.108.4891	2011.07.10	-
Kaspersky	9.0.0.837	2011.07.10	-
McAfee	5.400.0.1158	2011.07.10	-
McAfee-GW-Edition	2010.1D	2011.07.09	-
Microsoft	1.7000	2011.07.10	-
NOD32	6280	2011.07.10	-
Norman	6.07.10	2011.07.10	-
nProtect	2011-07-10.01	2011.07.10	-
Panda	10.0.3.5	2011.07.10	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.10	-

Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.10	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.10	-
TheHacker	6.7.0.1.250	2011.07.08	-
TrendMicro	9.200.0.1012	2011.07.10	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.10	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9823	2011.07.10	-
ViRobot	2011.7.9.4560	2011.07.10	-
VirusBuster	14.0.116.0	2011.07.09	-

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.11.00	2011.07.10	-
AntiVir	7.11.11.45	2011.07.08	-
Antiy-AVL	2.0.3.7	2011.07.10	-
Avast	4.8.1351.0	2011.07.10	-
Avast5	5.0.677.0	2011.07.10	-
AVG	10.0.0.1190	2011.07.10	-
BitDefender	7.2	2011.07.10	-
CAT-QuickHeal	11.00	2011.07.10	-
ClamAV	0.97.0.0	2011.07.10	-
Commtouch	5.3.2.6	2011.07.09	-
Comodo	9337	2011.07.10	-
DrWeb	5.0.2.03300	2011.07.10	-
Emsisoft	5.1.0.8	2011.07.10	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-

F-Prot	4.6.2.117	2011.07.09	-
F-Secure	9.0.16440.0	2011.07.10	-
Fortinet	4.2.257.0	2011.07.10	-
GData	22	2011.07.10	-
Ikarus	T3.1.1.104.0	2011.07.10	-
Jiangmin	13.0.900	2011.07.09	-
K7AntiVirus	9.108.4891	2011.07.10	-
Kaspersky	9.0.0.837	2011.07.10	-
McAfee	5.400.0.1158	2011.07.10	-
McAfee-GW-Edition	2010.1D	2011.07.09	-
Microsoft	1.7000	2011.07.10	-
NOD32	6281	2011.07.10	-
Norman	6.07.10	2011.07.10	-
nProtect	2011-07-10.01	2011.07.10	-
Panda	10.0.3.5	2011.07.10	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.10	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.10	-
SUPERAntiSpyware	4.40.0.1006	2011.07.09	-
Symantec	20111.1.0.186	2011.07.10	-
TheHacker	6.7.0.1.252	2011.07.10	-
TrendMicro	9.200.0.1012	2011.07.10	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.10	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9823	2011.07.10	-
ViRobot	2011.7.9.4560	2011.07.10	-

VirusBuster	14.0.116.0	2011.07.09	-

Antivirus	Version	Last update	Result
AhnLab-V3	2011.07.11.00	2011.07.10	-
AntiVir	7.11.11.46	2011.07.10	-
Antiy-AVL	2.0.3.7	2011.07.10	-
Avast	4.8.1351.0	2011.07.10	-
Avast5	5.0.677.0	2011.07.10	-
AVG	10.0.0.1190	2011.07.10	-
BitDefender	7.2	2011.07.10	-
CAT-QuickHeal	11.00	2011.07.10	-
ClamAV	0.97.0.0	2011.07.10	-
Commtouch	5.3.2.6	2011.07.10	-
Comodo	9339	2011.07.10	-
DrWeb	5.0.2.03300	2011.07.10	-
Emsisoft	5.1.0.8	2011.07.10	-
eSafe	7.0.17.0	2011.07.07	-
eTrust-Vet	36.1.8434	2011.07.08	-
F-Prot	4.6.2.117	2011.07.10	-
F-Secure	9.0.16440.0	2011.07.10	-
Fortinet	4.2.257.0	2011.07.10	-
GData	22	2011.07.10	-
Ikarus	T3.1.1.104.0	2011.07.10	-
Jiangmin	13.0.900	2011.07.10	-
K7AntiVirus	9.108.4891	2011.07.10	-
Kaspersky	9.0.0.837	2011.07.10	HEUR:Trojan.Win32.Generic
McAfee	5.400.0.1158	2011.07.10	-
McAfee-GW-Edition	2010.1D	2011.07.10	-

Microsoft	1.7000	2011.07.10	Trojan:Win32/Swrort.A
NOD32	6282	2011.07.10	-
Norman	6.07.10	2011.07.10	-
nProtect	2011-07-10.01	2011.07.10	-
Panda	10.0.3.5	2011.07.10	-
PCTools	8.0.0.5	2011.07.08	-
Prevx	3.0	2011.07.10	-
Rising	23.65.04.03	2011.07.08	-
Sophos	4.67.0	2011.07.10	Mal/FakeAV-FS
SUPERAntiSpyware	4.40.0.1006	2011.07.10	-
Symantec	20111.1.0.186	2011.07.10	-
TheHacker	6.7.0.1.252	2011.07.10	-
TrendMicro	9.200.0.1012	2011.07.10	-
TrendMicro-HouseCall	9.200.0.1012	2011.07.10	-
VBA32	3.12.16.4	2011.07.08	-
VIPRE	9826	2011.07.10	-
ViRobot	2011.7.9.4560	2011.07.10	-
VirusBuster	14.0.117.0	2011.07.10	-