



VirusTotal is a [service that analyzes suspicious files and URLs](#) and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware detected by antivirus engines. [More information...](#)

0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is goodware. 0 VT Community user(s) with a total of 0 reputation credit(s) say(s) this sample is malware.

File name: **windows_ -_shell_reverse_tcp-mspaint.exe-[cmd_ -_generic_sh]-5.exe**
 Submission date: **2011-09-26 08:02:32 (UTC)**
 Current status: **finished**
 Result: **25 /44 (56.8%)**

VT Community



not reviewed
Safety score: -

[Compact](#)

[Print results](#)

| Antivirus | Version | Last Update | Result |
|-------------------|---------------|-------------|-----------------------------|
| AhnLab-V3 | 2011.09.25.00 | 2011.09.26 | - |
| AntiVir | 7.11.15.30 | 2011.09.25 | TR/Crypt.EPACK.Gen2 |
| Antiy-AVL | 2.0.3.7 | 2011.09.26 | - |
| Avast | 4.8.1351.0 | 2011.09.25 | Win32:SwPatch [Wrm] |
| Avast5 | 6.0.1289.0 | 2011.09.26 | Win32:SwPatch [Wrm] |
| AVG | 10.0.0.1190 | 2011.09.25 | Win32/Heur |
| BitDefender | 7.2 | 2011.09.26 | Backdoor.Shell.AC |
| ByteHero | 1.0.0.1 | 2011.09.23 | Trojan.Win32.Heur.Gen |
| CAT-QuickHeal | 11.00 | 2011.09.26 | - |
| ClamAV | 0.97.0.0 | 2011.09.26 | - |
| Commtouch | 5.3.2.6 | 2011.09.26 | W32/Swrort.B.gen!Eldorado |
| Comodo | 10246 | 2011.09.26 | - |
| DrWeb | 5.0.2.03300 | 2011.09.26 | Trojan.Swrort.1 |
| Emsisoft | 5.1.0.11 | 2011.09.26 | Virus.Win32.Heur!IK |
| eSafe | 7.0.17.0 | 2011.09.26 | - |
| eTrust-Vet | 36.1.8578 | 2011.09.23 | - |
| F-Prot | 4.6.2.117 | 2011.09.26 | W32/Swrort.B.gen!Eldorado |
| F-Secure | 9.0.16440.0 | 2011.09.26 | Backdoor.Shell.AC |
| Fortinet | 4.3.370.0 | 2011.09.25 | W32/Swrort.C!tr |
| GData | 22 | 2011.09.26 | Backdoor.Shell.AC |
| Ikarus | T3.1.1.107.0 | 2011.09.26 | Virus.Win32.Heur |
| Jiangmin | 13.0.900 | 2011.09.25 | - |
| K7AntiVirus | 9.113.5184 | 2011.09.23 | Riskware |
| Kaspersky | 9.0.0.837 | 2011.09.26 | HEUR:Trojan.Win32.Generic |
| McAfee | 5.400.0.1158 | 2011.09.26 | Swrort.f |
| McAfee-GW-Edition | 2010.1D | 2011.09.25 | Swrort.f |
| Microsoft | 1.7702 | 2011.09.26 | Trojan:Win32/Swrort.A |
| NOD32 | 6493 | 2011.09.26 | a variant of Win32/Ducky.AA |
| Norman | 6.07.11 | 2011.09.25 | W32/Swrort.A |
| nProtect | 2011-09-26.01 | 2011.09.26 | Backdoor.Shell.AC |
| Panda | 10.0.3.5 | 2011.09.25 | Suspicious file |
| PCTools | 8.0.0.5 | 2011.09.26 | - |
| Prevx | 3.0 | 2011.09.26 | - |
| Rising | 23.77.00.02 | 2011.09.26 | - |
| Sophos | 4.69.0 | 2011.09.26 | Mal/Swrort-C |
| SUPERAntiSpyware | 4.40.0.1006 | 2011.09.24 | - |
| Symantec | 20111.2.0.82 | 2011.09.26 | - |
| TheHacker | 6.7.0.1.310 | 2011.09.25 | - |

| | | | |
|----------------------|----------------|------------|---------------------------|
| TrendMicro | 9.500.0.1008 | 2011.09.26 | - |
| TrendMicro-HouseCall | 9.500.0.1008 | 2011.09.26 | - |
| VBA32 | 3.12.16.4 | 2011.09.23 | - |
| VIPRE | 10586 | 2011.09.26 | Trojan.Win32.Swrort.B (v) |
| ViRobot | 2011.9.26.4688 | 2011.09.26 | - |
| VirusBuster | 14.0.231.0 | 2011.09.25 | - |

Additional information

[Show all](#)

MD5 : dd27f1aec1248722d577e2b77af98f98

SHA1 : 528ff379f572a9624a88f0b4dd7ac3e4d0dfef16

SHA256: 034da59223454a2fd674a7ae8d1e295dcf31ea0e53d44d388c27cf00b3421e88

VT Community

This file has never been reviewed by any VT Community member. Be the first one to comment on it!

Virustotal Team

Add your comment... **Remember that when you write comments as an anonymous user they receive the lowest possible reputation. So if you have not signed in yet don't forget to do so. How to markup your comments?** [i](#)

- | | | |
|--|---|---|
| <input type="checkbox"/> Goodware | <input type="checkbox"/> Malware | <input type="checkbox"/> Spam attachment/link |
| <input type="checkbox"/> P2P download | <input type="checkbox"/> Propagating via IM | <input type="checkbox"/> Network worm |
| <input type="checkbox"/> Drive-by-download | | |

[Preview comment](#)[Post comment](#)

⚠ ATTENTION: VirusTotal is a free service offered by Hispasec Sistemas. There are no guarantees about the availability and continuity of this service. Although the detection rate afforded by the use of multiple antivirus engines is far superior to that offered by just one product, **these results DO NOT guarantee the harmlessness of a file.** Currently, there is not any solution that offers a 100% effectiveness rate for detecting viruses and *malware*.