# ZeroAccess / Max++ / Smiscer Crimeware Rootkit sample for Step-by-Step Reverse Engineering by Giuseppe Bonfa - << (Update 2011 version available)



**ZeroAccess / Max++ / Smiscer Crimeware Rootkit sample for Step-by-Step Reverse Engineering by Giuseppe Bonfa - << (Update 2011 version available)**

**Post Update Feb 24, 2011**

**The new version is available here, thanks to Guiseppe :)**

**Download MaxRootkit_2011_1.exe as a password protected archive (contact me if you need the password)**

**File name: 392ddf0d2ee5049da11afa4668e9c98f**

Virustotal
Submission date 2011-02-14 14:41:24 (UTC)
Result:25 /43 (58.1%)

| Antivirus | Version | Last Update | Result |
|---|---|---|---|
| AhnLab-V3 | 2011.02.14.02 | 2011.02.14 | Trojan/Win32.Gen |
| AntiVir | 7.11.3.78 | 2011.02.14 | TR/Dropper.Gen |
| Avast | 4.8.1351.0 | 2011.02.14 | Win32:FakeAlert-FC |
| Avast5 | 5.0.677.0 | 2011.02.14 | Win32:FakeAlert-FC |
| AVG | 10.0.0.1190 | 2011.02.14 | Dropper.Generic3.AJH |
| BitDefender | 7.2 | 2011.02.14 | Trojan.Generic.5349632 |
| CAT-QuickHeal | 11.00 | 2011.02.14 | Worm.Sirefef.a |
| DrWeb | 5.0.2.03300 | 2011.02.14 | Trojan.DownLoader2.2219 |
| Emsisoft | 5.1.0.2 | 2011.02.14 | Worm.Win32.Sirefef!IK |
| F-Secure | 9.0.16160.0 | 2011.02.14 | Trojan.Generic.5349632 |
| Fortinet | 4.2.254.0 | 2011.02.14 | W32/Dx.VUZ!tr |
| GData | 21 | 2011.02.14 | Trojan.Generic.5349632 |
| Ikarus | T3.1.1.97.0 | 2011.02.14 | Worm.Win32.Sirefef |
| McAfee | 5.400.0.1158 | 2011.02.14 | Generic.dx!vuz |
| McAfee-GW-Edition | 2010.1C | 2011.02.14 | Heuristic.BehavesLike.Win32.Suspicious.H |
| Microsoft | 1.6502 | 2011.02.14 | Worm:Win32/Sirefef.gen!A |

NOD32 5872 2011.02.14 a variant of Win32/Sirefef.C
Panda 10.0.3.5 2011.02.13 Trj/CI.A
PCTools 7.0.3.5 2011.02.13 Trojan.Gen
Rising 23.45.00.00 2011.02.14 [Suspicious]
Symantec 20101.3.0.103 2011.02.14 Trojan.Gen
TheHacker 6.7.0.1.130 2011.02.13 Trojan/Sirefef.c
TrendMicro 9.200.0.1012 2011.02.14 TROJ_GEN.R3EC1BD
TrendMicro-HouseCall 9.200.0.1012 2011.02.14 TROJ_GEN.R3EC1BD
VIPRE 8416 2011.02.14 Trojan.Win32.Generic!BT
MD5 : 392ddf0d2ee5049da11afa4668e9c98f

### Automated Scans

Max++ downloader install_2010.ex_
Submission date:2010-10-29 17:02:09 (UTC)
http://www.virustotal.com/file-scan/report.html?id=d22425d964751152471cca7e8166cc9e03c1a4a2e8846f18b665bb3d350873db-1288371729
Result:40 /43 (93.0%)
Antivirus Version Last Update Result
AhnLab-V3 2010.10.29.00 2010.10.28 Dropper/Smiscer.79360.B
AntiVir 7.10.13.74 2010.10.29 TR/Drop.Smiscer.HF.1
Authentium 5.2.0.5 2010.10.29 W32/Dropper.AYXZ
Avast 4.8.1351.0 2010.10.29 Win32:Trojan-gen
Avast5 5.0.594.0 2010.10.29 Win32:Trojan-gen
AVG 9.0.0.851 2010.10.28 Crypt.NSQ
BitDefender 7.2 2010.10.29 Trojan.Generic.IS.439387
CAT-QuickHeal 11.00 2010.10.26 TrojanDropper.Smiscer.hf
ClamAV 0.96.2.0-git 2010.10.29 Trojan.Dropper-24318
Comodo 6552 2010.10.29 TrojWare.Win32.TrojanDropper.Agent.783360
DrWeb 5.0.2.03300 2010.10.29 BackDoor.Maxplus.6
Emsisoft 5.0.0.50 2010.10.29 Trojan-Dropper.Win32.Smiscer!IK
eTrust-Vet 36.1.7942 2010.10.29 Win32/ASuspect.HADSN
F-Prot 4.6.2.117 2010.10.29 W32/Dropper.AYXZ
F-Secure 9.0.16160.0 2010.10.29 Trojan.Generic.IS.439387
GData 21 2010.10.29 Trojan.Generic.IS.439387
Ikarus T3.1.1.90.0 2010.10.29 Trojan-Dropper.Win32.Smiscer
Jiangmin 13.0.900 2010.10.29 Backdoor/Agent.ctrw
K7AntiVirus 9.67.2865 2010.10.29 Trojan

Kaspersky 7.0.0.125 2010.10.29 Trojan-Dropper.Win32.Smiscer.hf
McAfee 5.400.0.1158 2010.10.29 Generic Dropper!cev
McAfee-GW-Edition 2010.1C 2010.10.29 Generic Dropper!cev
Microsoft 1.6301 2010.10.29 TrojanDropper:Win32/Sirefef.B
NOD32 5575 2010.10.29 Win32/Sirefef.P
Norman 6.06.10 2010.10.29 W32/Obfuscated.T
nProtect 2010-10-29.01 2010.10.29 Trojan-Dropper/W32.Smiscer.79360
Panda 10.0.2.7 2010.10.29 Trj/Dropper.WF
PCTools 7.0.3.5 2010.10.29 Trojan.Generic
Prevx 3.0 2010.10.29 Medium Risk Malware
Rising 22.71.03.02 2010.10.29 Trojan.Win32.Generic.51F92A9D
Sophos 4.59.0 2010.10.29 Mal/EncPk-NL
Sunbelt 7165 2010.10.29 Trojan.Win32.Generic!BT
SUPERAntiSpyware 4.40.0.1006 2010.10.29 Trojan.Agent/Gen
Symantec 20101.2.0.161 2010.10.29 Trojan Horse
TheHacker 6.7.0.1.073 2010.10.29 Trojan/Dropper.Smiscer.hf
TrendMicro 9.120.0.1004 2010.10.29 TROJ_Gen.CX34I8
TrendMicro-HouseCall 9.120.0.1004 2010.10.29 TROJ_Gen.CX34I8
VBA32 3.12.14.1 2010.10.29 Trojan.Win32.Waledac.45
ViRobot 2010.10.25.4110 2010.10.29 Dropper.Smiscer.79410
VirusBuster 12.70.12.0 2010.10.29 Trojan.DR.Smiscer.LP
MD5 : d8f6566c5f9caa795204a40b3aaaafa2
SHA1 : d0b7cd496387883b265d649e811641f743502c41

---

Source: http://contagiodump.blogspot.com/2010/11/zeroaccess-max-smiscer-crimeware.html