March 2010 Opachki Trojan update and sample

Archived: 2026-04-05 21:53:28 UTC

March 2010 Opachki Trojan update and sample

I already posted a few links for Opachki trojan in November 2009. Here is an update.

Download dropper.exe and dropped rundll32.dll as a password protected archive. Please contact me if you need the password

Details:
2ded7ee112cea2db509ba95dc09fded6 dropper.exe
032e8fced2fbed146c30a47d4989804b rundll32.dll

- Opachki, from (and to) Russia with love by Bojan Zdrnja - Internet Storm Center Diary
- Opachki Link Hijacker Trojan Analysis by Joe Stewart Secure Works
- Opachki Trojan Hijacking Web Links by Dennis Fisher Threatpost
- Trojan:Win32/Opachki : redirections Google by Malekal_morte

March 2010 Virustotal scan results of the available sample. Please note this sample dates to October 2009. Newer versions and samples will have lower detection rate and may get slightly different names.

File dropper.exe received on 2010.03.07 16:46:50 (UTC)
www.virustotal.com/analisis/787d0eae3fb29883b8dba9c3bcc00793baa4a54fbad0921d1aee7f5e6ad86907-1267980410
Result: 37/42 (88.1%)
a-squared 4.5.0.50 2010.03.07 Packed.Win32.Krap!IK
AhnLab-V3 5.0.0.2 2010.03.07 Win-Trojan/Krap.31232.K
AntiVir 8.2.1.180 2010.03.05 TR/Crypt.ZPACK.Gen
Antiy-AVL 2.0.3.7 2010.03.05 Packed/Win32.Krap.gen
Authentium 5.2.0.5 2010.03.06 W32/Trojan2.KMYU
Avast 4.8.1351.0 2010.03.07 Win32:MalOb-R
Avast5 5.0.332.0 2010.03.07 Win32:MalOb-R
AVG 9.0.0.787 2010.03.07 Win32/Cryptor
BitDefender 7.2 2010.03.07 Trojan.Generic.2594388
CAT-QuickHeal 10.00 2010.03.06 Trojan.Krap.ah
Comodo 4091 2010.02.28 TrojWare.Win32.Trojan.Agent.Gen
DrWeb 5.0.1.12222 2010.03.07 Trojan.Packed.683
eSafe 7.0.17.0 2010.03.04 Win32.Horse
F-Prot 4.5.1.85 2010.03.06 W32/Trojan2.KMYU

F-Secure 9.0.15370.0 2010.03.07 Packed:W32/Tikmis.gen!A
Fortinet 4.0.14.0 2010.03.07 W32/Krap.AH
GData 19 2010.03.07 Trojan.Generic.2594388
Ikarus T3.1.1.80.0 2010.03.07 Packed.Win32.Krap
Jiangmin 13.0.900 2010.03.07 Packed.Krap.zvc
K7AntiVirus 7.10.990 2010.03.04 Trojan.Win32.Malware.4
Kaspersky 7.0.0.125 2010.03.07 Packed.Win32.Krap.ah
McAfee 5912 2010.03.06 Opachki.a
McAfee+Artemis 5912 2010.03.06 Opachki.a
McAfee-GW-Edition 6.8.5 2010.03.07 Trojan.Crypt.ZPACK.Gen
Microsoft 1.5502 2010.03.07 Trojan:Win32/Opachki.A
NOD32 4922 2010.03.07 Win32/TrojanDropper.Agent.OLQ
Norman 6.04.08 2010.03.07 W32/Crypt.dam
nProtect 2009.1.8.0 2010.03.07 Trojan/W32.Krap.31232.L
Panda 10.0.2.2 2010.03.07 Trj/Zlob.KH
PCTools 7.0.3.5 2010.03.04 Trojan.Generic
Prevx 3.0 2010.03.07 High Risk Cloaked Malware
Sophos 4.51.0 2010.03.07 Mal/FakeAV-BX
Sunbelt 5780 2010.03.07 Trojan.Win32.Generic!VS
Symantec 20091.2.0.41 2010.03.07 Trojan Horse
TrendMicro 9.120.0.1004 2010.03.07 TROJ_OPACHKI.I
VBA32 3.12.12.2 2010.03.05 BScope.Win32.AntiAV2010
VirusBuster 5.0.27.0 2010.03.06 Trojan.Opachki.EK
Additional information
File size: 31232 bytes
MD5...: 2ded7ee112cea2db509ba95dc09fded6

File rundll32.dll received on 2010.03.07 16:55:25 (UTC)
http://www.virustotal.com/analisis/8f7684eed8707df29772df1285232df84d2e9be814aced65f3f02c7770632988-1267980925
Result: 37/42 (88.1%)
a-squared 4.5.0.50 2010.03.07 Packed.Win32.Krap!IK
AhnLab-V3 5.0.0.2 2010.03.07 Win-Trojan/Krap.23552.V
AntiVir 8.2.1.180 2010.03.05 TR/PCK.Krap.AH.49
Antiy-AVL 2.0.3.7 2010.03.05 Packed/Win32.Krap.gen
Authentium 5.2.0.5 2010.03.06 W32/Trojan2.KMWX
Avast 4.8.1351.0 2010.03.07 Win32:Malware-gen
Avast5 5.0.332.0 2010.03.07 Win32:Malware-gen
AVG 9.0.0.787 2010.03.07 SHeur2.BMZG

BitDefender 7.2 2010.03.07 Trojan.Renos.OVU
CAT-QuickHeal 10.00 2010.03.06 Trojan.Krap.ah
Comodo 4091 2010.02.28 TrojWare.Win32.Krap.ah
DrWeb 5.0.1.12222 2010.03.07 Trojan.Packed.683
eSafe 7.0.17.0 2010.03.04 Win32.Horse
F-Prot 4.5.1.85 2010.03.06 W32/Trojan2.KMWX
F-Secure 9.0.15370.0 2010.03.07 Trojan.Renos.OVU
GData 19 2010.03.07 Trojan.Renos.OVU
Ikarus T3.1.1.80.0 2010.03.07 Packed.Win32.Krap
Jiangmin 13.0.900 2010.03.07 Packed.Krap.aayt
K7AntiVirus 7.10.990 2010.03.04 Trojan.Win32.Malware.1
Kaspersky 7.0.0.125 2010.03.07 Packed.Win32.Krap.ah
McAfee 5912 2010.03.06 Opachki.a
McAfee+Artemis 5912 2010.03.06 Opachki.a
McAfee-GW-Edition 6.8.5 2010.03.07 Trojan.PCK.Krap.AH.49
Microsoft 1.5502 2010.03.07 Trojan:Win32/Opachki.A
NOD32 4922 2010.03.07 Win32/Opachki.A
Norman 6.04.08 2010.03.07 W32/Smalltroj.UDWN
nProtect 2009.1.8.0 2010.03.07 Trojan/W32.Krap.23552.AZ
Panda 10.0.2.2 2010.03.07 Trj/Zlob.KH
PCTools 7.0.3.5 2010.03.04 RogueAntiSpyware.AntivirusSystemPro
Prevx 3.0 2010.03.07 Medium Risk Malware
Sophos 4.51.0 2010.03.07 Troj/Bredo-N
Sunbelt 5780 2010.03.07 Trojan.Win32.Generic!BT
Symantec 20091.2.0.41 2010.03.07 Trojan Horse
TheHacker 6.5.1.9.223 2010.03.07 Trojan/Krap.ah
TrendMicro 9.120.0.1004 2010.03.07 TROJ_BREDO.D
VBA32 3.12.12.2 2010.03.05 BScope.Win32.AntiAV2010
VirusBuster 5.0.27.0 2010.03.06 Trojan.Sisron.BPV
Additional information
File size: 23552 bytes
MD5...: 032e8fced2fbed146c30a47d4989804b

Threatexpert report
http://www.threatexpert.com/report.aspx?md5=2ded7ee112cea2db509ba95dc09fded6
