Rustock samples and analysis links. Rustock.C, E, I, J and other variants

contagiodump.blogspot.com/2011/10/rustock-samples-and-analysis-links.html

I thought that Russian Matryoshka aka Rustock the Nested Doll would be a good subject after the previous post about Trojan.Matryoshka (Taidoor) analyzed by Jared Myers from CyberESI. Russian rootkit Rustock is as notorious as TDSS or Stuxnet and is very sophisticated. Many researchers made detailed analysis of Rustock and this is why it is a great subject of study. The botnet is down but the malware is here for you to play and try to reverse on your own or following one of the analysis papers posted below.

General File Information

Rustock 23 Virustotal approx. Oct 2009
File timedatestamp. (Thu Oct 01 10:15:30 2009)
VT First seen: 2009-11-07 05:29:52
Size: 269312
MD5: 1A713083A0BC21BE19F1EC496DF4E651

Rustock.NFE Virustotal approx. Mar 2009

File timedatestamp. (Mon Mar 02 12:18:02 2009)
VT First seen: 2009-03-20 01:59:48
Size: 98158
MD5: 8E4994543ADBC2BA2103C6F801898356

Rustock.J Virustotal approx. Aug 2008
VT first seen 2008-08-22 05:08:39
Size: 428168
MD5: 76101675D9CF5BA5238CAE9D5FAC8881

Rustock. I Virustotal approx. Sept 2009
File timedatestamp (Tue Sep 15 16:42:54 2009)
VT First seen: 2009-10-07 18:04:12
Size: 20480
MD5: 4A5E58D6351C342F3EDC145F6F4EEAFE

Rustock. E Virustotal approx. Sep. 2007
timedatestamp. (Wed Sep 26 05:11:12 2007)
Size: 158464
MD5: 04BA40662923BE168CA4DC2DA924A0D0

Rustock.C Virustotal approx. Jan 2007
Timestamp: (Fri Jan 19 09:46:53 2007)
VT First seen: 2007-01-22 08:52:17
Size: 70570
MD5: FDAFB3A14338B2B612C4E5C4F94B3677

Malware Analysis and Botnet research Links

2006 Preliminary Rustock Analysis valsmith Offensive computing
2007 A Case Study of the Rustock Rootkit and Spam Bot Ken Chiang, Levi Lloyd
2008 Rustock.C – секретные техники анализа Крис Касперски
2008 Rustock.C – Unpacking a Nested Doll Threatexpert blog
2008 Rustock and All That Alexander Gostev Kaspersky Lab
2008 Yet another Rustock Analysis ESET Lukasz Kwiatek, Stanislaw Litawa
2008 I-Worm/Nuwar.W + Rustock.E Variant – Analysis Novirusthanks blog
2009 Rustock M86Security
2009 Rootkit Installation and Obfuscation in Rustock By Chandra Prakash Sunbelt Software
2009 What makes the Rustocks tick! Chandra Prakash
2011 An overview of Rustock Fireeye Alex Lanstein

Win32.Ntldrbot (aka Rustock.C) no longer a myth, no longer a threat Dr.Web
2011 Microsoft Hunting Rustock Controllers Krebs on Security
2011 Microsoft Security Intelligence Report Battling the Rustock Threat

Download

Automated Scans

Here are current scans

Rustock 23
Virustotal
malware.exe
Submission date:2011-10-07 02:50:13 (UTC)
Result:36/ 43 (83.7%)
AhnLab-V3 2011.10.06.00 2011.10.06 Win-Trojan/Newrest.269312
AntiVir 7.11.15.141 2011.10.06 TR/Dropper.Gen
Avast 6.0.1289.0 2011.10.06 Win32:Neredr [Drp]
AVG 10.0.0.1190 2011.10.06 BackDoor.Generic12.EG
BitDefender 7.2 2011.10.07 Gen:Trojan.Heur.Rustock.1
CAT-QuickHeal 11.00 2011.10.05 W32.Rustock.J
ClamAV 0.97.0.0 2011.10.07 Trojan.Rustock-23
Commtouch 5.3.2.6 2011.10.07 W32/NewRest.A.gen!Eldorado
Comodo 10368 2011.10.07 TrojWare.Win32.TrojanDownloader.Boltolog.~JH3
DrWeb 5.0.2.03300 2011.10.07 Trojan.Spambot.5077
Emsisoft 5.1.0.11 2011.10.07 Backdoor.WinNT.Rustock!IK
eSafe 7.0.17.0 2011.10.06 Win32.Pandex
eTrust-Vet 36.1.8603 2011.10.06 -
F-Prot 4.6.2.117 2011.10.06 W32/NewRest.A.gen!Eldorado
F-Secure 9.0.16440.0 2011.10.07 Gen:Trojan.Heur.Rustock.1
Fortinet 4.3.370.0 2011.10.06 W32/NewRest.BC!tr.bdr
GData 22 2011.10.07 Gen:Trojan.Heur.Rustock.1
Ikarus T3.1.1.107.0 2011.10.07 Backdoor.WinNT.Rustock
Jiangmin 13.0.900 2011.10.06 Backdoor/NewRest.axy

K7AntiVirus 9.115.5248 2011.10.06 Riskware
Kaspersky 9.0.0.837 2011.10.07 Backdoor.Win32.NewRest.bc
McAfee 5.400.0.1158 2011.10.07 Generic BackDoor!bfe
McAfee-GW-Edition 2010.1D 2011.10.07 Generic BackDoor!bfe
Microsoft 1.7702 2011.10.06 Backdoor:WinNT/Rustock.AN
NOD32 6523 2011.10.07 a variant of Win32/Rustock.NKU
Norman 6.07.11 2011.10.06 W32/Suspicious_Gen2.HITO
nProtect 2011-10-06.01 2011.10.06 Backdoor/W32.NewRest.269312.D
Panda 10.0.3.5 2011.10.06 Rootkit/Farfli.X
PCTools 8.0.0.5 2011.10.07 Trojan.Pandex!rem
Sophos 4.70.0 2011.10.06 Mal/Generic-L
Symantec 20111.2.0.82 2011.10.07 Trojan.Pandex
TheHacker 6.7.0.1.318 2011.10.06 Backdoor/NewRest.bc
TrendMicro 9.500.0.1008 2011.10.06 BKDR_RUSTOCK.SMA
TrendMicro-HouseCall 9.500.0.1008 2011.10.07 BKDR_RUSTOCK.SMA
VBA32 3.12.16.4 2011.10.06 Malware-Cryptor.General.3
VIPRE 10685 2011.10.07 Trojan-Dropper.Win32.Rustock.j (v)
VirusBuster 14.0.252.5 2011.10.06 Backdoor.NewRest!90rGdRrhb6c
MD5 : 1a713083a0bc21be19f1ec496df4e651**Rustock.NFE**
File name: malware.exe
2011-10-07 02:54:50 (UTC)
Result: 35/ 42 (83.3%)
Virustotal
AhnLab-V3 2011.10.06.00 2011.10.06 Win-Trojan/Rustock.98158
AntiVir 7.11.15.141 2011.10.06 TR/Rootkit.Gen
Antiy-AVL 2.0.3.7 2011.10.06 Backdoor/Win32.NewRest.gen
Avast 6.0.1289.0 2011.10.06 Win32:RustNT [Rtk]
AVG 10.0.0.1190 2011.10.06 BackDoor.Generic11.CDJ
BitDefender 7.2 2011.10.07 Backdoor.Rustock.NFE
CAT-QuickHeal 11.00 2011.10.05 Trojan.Agent.ATV
Commtouch 5.3.2.6 2011.10.07 W32/SYStroj.S.gen!Eldorado
Comodo 10368 2011.10.07 Backdoor.Win32.NewRest.A
DrWeb 5.0.2.03300 2011.10.07 Trojan.Spambot.8555
Emsisoft 5.1.0.11 2011.10.07 Backdoor.Win32.NewRest!IK
F-Prot 4.6.2.117 2011.10.06 W32/SYStroj.S.gen!Eldorado
F-Secure 9.0.16440.0 2011.10.07 Backdoor.Rustock.NFE
Fortinet 4.3.370.0 2011.10.06 W32/Backdoor!tr
GData 22 2011.10.07 Backdoor.Rustock.NFE
Ikarus T3.1.1.107.0 2011.10.07 Backdoor.Win32.NewRest
Jiangmin 13.0.900 2011.10.06 Backdoor/NewRest.bhg
K7AntiVirus 9.115.5248 2011.10.06 Riskware
Kaspersky 9.0.0.837 2011.10.07 Backdoor.Win32.NewRest.z

McAfee 5.400.0.1158 2011.10.07 W32/Rustock
McAfee-GW-Edition 2010.1D 2011.10.07 W32/Rustock
Microsoft 1.7702 2011.10.06 Backdoor:WinNT/Rustock.E
NOD32 6523 2011.10.07 a variant of Win32/Rustock.NKU
Norman 6.07.11 2011.10.06 W32/Rustock.ALF
nProtect 2011-10-06.01 2011.10.06 Backdoor/W32.Rustock.98158
Panda 10.0.3.5 2011.10.06 Generic Backdoor
PCTools 8.0.0.5 2011.10.07 Backdoor.Rustock.C!rem
Sophos 4.70.0 2011.10.06 Mal/TDSSPack-G
Symantec 20111.2.0.82 2011.10.07 Backdoor.Rustock.B
TheHacker 6.7.0.1.318 2011.10.06 Backdoor/NewRest.z
TrendMicro 9.500.0.1008 2011.10.06 BKDR_RUSTOCK.SMB
TrendMicro-HouseCall 9.500.0.1008 2011.10.07 BKDR_RUSTOCK.SMB
VBA32 3.12.16.4 2011.10.06 Malware-Cryptor.General.3
VIPRE 10685 2011.10.07 Backdoor.Rustock
VirusBuster 14.0.252.5 2011.10.06 Backdoor.NewRest!n6q3ymQd7tQ
MD5 : 8e4994543adbc2ba2103c6f801898356**Rustock.J** Virustotal
c25a91a3c1301c877870d0a9c7287a3b19ed5802
Submission date:2011-07-02 03:20:19 (UTC)
AhnLab-V3 2011.07.02.00 2011.07.01 Trojan/Win32.ADH
AntiVir 7.11.10.197 2011.07.01 TR/Dropper.Gen
Avast 4.8.1351.0 2011.07.01 Win32:Foxer
Avast5 5.0.677.0 2011.07.01 Win32:Foxer
AVG 10.0.0.1190 2011.07.01 Downloader.FraudLoad.AO
BitDefender 7.2 2011.07.02 Trojan.Rootkit.Rustock.J
Comodo 9248 2011.07.02 TrojWare.Win32.Trojan.DNSChanger.VD0
eTrust-Vet 36.1.8421 2011.07.01 Win32/ASuspect.HDFDS
F-Secure 9.0.16440.0 2011.07.02 Trojan-Dropper:W32/Agent.FDD
GData 22 2011.07.02 Trojan.Rootkit.Rustock.J
Ikarus T3.1.1.104.0 2011.07.01 Win32.SuspectCrc
Jiangmin 13.0.900 2011.07.01 TrojanDropper.Agent.qig
K7AntiVirus 9.107.4863 2011.07.01 Trojan
Kaspersky 9.0.0.837 2011.07.02 -
McAfee 5.400.0.1158 2011.07.02 Generic.dx
McAfee-GW-Edition 2010.1D 2011.07.02 Generic.dx
Microsoft 1.7000 2011.07.01 TrojanDropper:Win32/Alureon.N
Norman 6.07.10 2011.07.01 W32/Suspicious_Gen2.IRVW
nProtect 2011-07-01.01 2011.07.01 Trojan.DNSChanger.VD
Panda 10.0.3.5 2011.07.01 Trj/CI.A
PCTools 8.0.0.5 2011.07.01 Trojan.ADH
Sophos 4.67.0 2011.07.02 Mal/Generic-L
Symantec 20111.1.0.186 2011.07.02 Trojan.ADH

VBA32 3.12.16.4 2011.07.01 Malware-Cryptor.Win32.General.4
VIPRE 9745 2011.07.02 Media Code, Inc (v)
MD5 : 76101675d9cf5ba5238cae9d5fac8881**Rustock. I**
Virustotal
malware.exe
Submission date:2011-10-07 03:27:30 (UTC)
Result:
37/ 43 (86.0%)
AhnLab-V3 2011.10.06.00 2011.10.06 Win-Trojan/Murlo.20480.BI
AntiVir 7.11.15.141 2011.10.06 TR/Dldr.Agent.20478
Avast 6.0.1289.0 2011.10.06 Win32:Trojan-gen
AVG 10.0.0.1190 2011.10.06 BackDoor.Generic11.AYOE
BitDefender 7.2 2011.10.07 Trojan.Generic.2509041
CAT-QuickHeal 11.00 2011.10.05 TrojanDownloader.Murlo.chj
Commtouch 5.3.2.6 2011.10.07 W32/Rustock.I
Comodo 10368 2011.10.07 UnclassifiedMalware
DrWeb 5.0.2.03300 2011.10.07 Trojan.DownLoad.57537
Emsisoft 5.1.0.11 2011.10.07 Trojan-Downloader.Win32.Murlo!IK
eTrust-Vet 36.1.8603 2011.10.06 Win32/Rustock.JG
F-Prot 4.6.2.117 2011.10.06 W32/Rustock.I
F-Secure 9.0.16440.0 2011.10.07 Trojan.Generic.2509041
Fortinet 4.3.370.0 2011.10.06 W32/Agent.OKM!tr.bdr
GData 22 2011.10.07 Trojan.Generic.2509041
Ikarus T3.1.1.107.0 2011.10.07 Trojan-Downloader.Win32.Murlo
Jiangmin 13.0.900 2011.10.06 TrojanDownloader.Murlo.aga
K7AntiVirus 9.115.5248 2011.10.06 Backdoor
Kaspersky 9.0.0.837 2011.10.07 Trojan-Downloader.Win32.Murlo.chj
McAfee 5.400.0.1158 2011.10.07 Generic Downloader.x!bpu
McAfee-GW-Edition 2010.1D 2011.10.07 Generic Downloader.x!bpu
Microsoft 1.7702 2011.10.06 TrojanDownloader:Win32/Rustock.A
NOD32 6523 2011.10.07 Win32/Rustock.NLB
Norman 6.07.11 2011.10.06 W32/DLoader.ABIYA
nProtect 2011-10-06.01 2011.10.06 Trojan-Downloader/W32.MultiDrop.20480.E
Panda 10.0.3.5 2011.10.06 Trj/Downloader.MDW
PCTools 8.0.0.5 2011.10.07 Downloader.Generic
Rising 23.77.04.01 2011.09.30 Trojan.Win32.Generic.122B31C0
Sophos 4.70.0 2011.10.06 Mal/Generic-L
Symantec 20111.2.0.82 2011.10.07 Downloader
TheHacker 6.7.0.1.318 2011.10.06 Trojan/Downloader.Murlo.chj
TrendMicro 9.500.0.1008 2011.10.07 TROJ_MURLO.DQ
TrendMicro-HouseCall 9.500.0.1008 2011.10.07 TROJ_MURLO.DQ
VBA32 3.12.16.4 2011.10.06 Trojan-Downloader.Win32.Murlo.chj

VIPRE 10685 2011.10.07 Trojan.Win32.Generic!BT
ViRobot 2011.10.7.4706 2011.10.07 Trojan.Win32.Downloader.20480.XZ
VirusBuster 14.0.252.5 2011.10.06 Trojan.DL.Rustock!k8yJCVO/R5I
MD5 : 4a5e58d6351c342f3edc145f6f4eeafe
malware.exe
Submission date:2011-10-07 03:32:34 (UTC)
Result:30/ 43 (69.8%)
Virustotal
AntiVir 7.11.15.141 2011.10.06 TR/Rootkit.Gen
Avast 6.0.1289.0 2011.10.06 Win32:Rusty
AVG 10.0.0.1190 2011.10.06 Klone.P
BitDefender 7.2 2011.10.07 Win32.Ntldrbot.A
CAT-QuickHeal 11.00 2011.10.05 W32.Rustock.D
Commtouch 5.3.2.6 2011.10.07 W32/Rustock.E
Comodo 10368 2011.10.07 UnclassifiedMalware
DrWeb 5.0.2.03300 2011.10.07 Win32.Ntldrbot
Emsisoft 5.1.0.11 2011.10.07 Virus.Win32.Rustock!IK
eSafe 7.0.17.0 2011.10.06 Win32.TRRootkit
eTrust-Vet 36.1.8603 2011.10.06 -
F-Prot 4.6.2.117 2011.10.06 W32/Rustock.E
F-Secure 9.0.16440.0 2011.10.07 Win32.Ntldrbot.A
Fortinet 4.3.370.0 2011.10.06 W32/Rustock.fam
GData 22 2011.10.07 Win32.Ntldrbot.A
Ikarus T3.1.1.107.0 2011.10.07 Virus.Win32.Rustock
K7AntiVirus 9.115.5248 2011.10.06 Virus
Kaspersky 9.0.0.837 2011.10.07 Virus.Win32.Rustock.a
McAfee 5.400.0.1158 2011.10.07 Spam-Mailbot.sys!gen
McAfee-GW-Edition 2010.1D 2011.10.07 Spam-Mailbot.sys!gen
Microsoft 1.7702 2011.10.06 Backdoor:WinNT/Rustock.D
NOD32 6523 2011.10.07 Win32/Rustock.A
Norman 6.07.11 2011.10.06 Rustock.CFX
nProtect 2011-10-06.01 2011.10.06 Win32.Ntldrbot.A
Panda 10.0.3.5 2011.10.06 Suspicious file
Rising 23.77.04.01 2011.09.30 Trojan.Win32.Generic.128C3CB1
Sophos 4.70.0 2011.10.06 Mal/RKRustok-B
TrendMicro 9.500.0.1008 2011.10.07 HeurSpy_Rustok1
TrendMicro-HouseCall 9.500.0.1008 2011.10.07 HeurSpy_Rustok1
VIPRE 10685 2011.10.07 Trojan.Win32.Generic!BT
VirusBuster 14.0.252.5 2011.10.06 Rootkit.Rustock.Gen!Pac
MD5 : 04ba40662923be168ca4dc2da924a0d0 **Rustock.C 38/ 43 (88.4%)**
Virustotal
AhnLab-V3 2011.10.06.00 2011.10.06 Win-Trojan/Costrat.25088.B

AntiVir 7.11.15.141 2011.10.06 TR/Dropper.Gen
Avast 6.0.1289.0 2011.10.06 Win32:Trojan-gen
AVG 10.0.0.1190 2011.10.06 Obfustat.ITG
BitDefender 7.2 2011.10.07 Backdoor.Rustock.Gen.1
ByteHero 1.0.0.1 2011.09.23 -
CAT-QuickHeal 11.00 2011.10.05 Rootkit.Rustock
ClamAV 0.97.0.0 2011.10.07 Trojan.Clicker-950
Commtouch 5.3.2.6 2011.10.07 W32/Rustock.C
Comodo 10368 2011.10.07 Trojan-Clicker.Win32.Costrat.bk
DrWeb 5.0.2.03300 2011.10.07 Trojan.Spambot
Emsisoft 5.1.0.11 2011.10.07 Backdoor.WinNT.Rustock!IK
eSafe 7.0.17.0 2011.10.06 Win32.Rustock.B
eTrust-Vet 36.1.8603 2011.10.06 -
F-Prot 4.6.2.117 2011.10.06 W32/Rustock.C
F-Secure 9.0.16440.0 2011.10.07 Backdoor.Rustock.Gen.1
Fortinet 4.3.370.0 2011.10.06 W32/Generic.CON!tr
GData 22 2011.10.07 Backdoor.Rustock.Gen.1
Ikarus T3.1.1.107.0 2011.10.07 Backdoor.WinNT.Rustock
Jiangmin 13.0.900 2011.10.06 TrojanClicker.Costrat.ml
K7AntiVirus 9.115.5248 2011.10.06 Riskware
Kaspersky 9.0.0.837 2011.10.07 Trojan-Clicker.Win32.Costrat.bk
McAfee 5.400.0.1158 2011.10.07 Generic.dx
McAfee-GW-Edition 2010.1D 2011.10.07 Generic.dx
Microsoft 1.7702 2011.10.06 Backdoor:WinNT/Rustock.C
NOD32 6523 2011.10.07 a variant of Win32/Rootkit.Kryptik.BP
Norman 6.07.11 2011.10.06 W32/Agent.ECMM
nProtect 2011-10-06.01 2011.10.06 Trojan-Clicker/W32.Costrat.70570
Panda 10.0.3.5 2011.10.06 Trj/Agent.EDT
PCTools 8.0.0.5 2011.10.07 Backdoor.Rustock.C!rem
Prevx 3.0 2011.10.07 Medium Risk Malware
Rising 23.77.04.01 2011.09.30 Trojan.Win32.Generic.122F6627
Sophos 4.70.0 2011.10.06 Mal/RKRustok-A
Symantec 20111.2.0.82 2011.10.07 Backdoor.Rustock.B
TheHacker 6.7.0.1.318 2011.10.06 Trojan/Clicker.Costrat.bk
TrendMicro 9.500.0.1008 2011.10.07 BKDR_RUSTOCK.AR
TrendMicro-HouseCall 9.500.0.1008 2011.10.07 BKDR_RUSTOCK.AR
VBA32 3.12.16.4 2011.10.06 Malware-Cryptor.Win32.015
VIPRE 10685 2011.10.07 Backdoor.Rustock
VirusBuster 14.0.252.5 2011.10.06 Trojan.Rustock!gMcRHMfFn+E
MD5 : fdafb3a14338b2b612c4e5c4f94b3677