Aug 2012 Backdoor.Wirenet - OSX and Linux

End of the year presents:

Backdoor.Wirenet.1

Related News and Analysis:

August 2012

The first Trojan in history to steal Linux and Mac OS X passwords Dr.Web

Download

Download. (Email me if you need the password scheme - see profile for email)

Files

Linux

File: 9A0E765EECC5433AF3DC726206ECC56E

Size: 64400

OSX

File: C3B48DB40CF810CB63BF36262B7C5B19

Size: 78664

File: D048F7AE2D244A264E58AF67B1A20DB0

Size: 77940

Automatic scans

https://www.virustotal.com/file/35ff79dd456fe3054a60fe0a16f38bf5fc3928e1e8439ca4d945573f8c48c0b8/analysis/1354885555/
SHA256: 35ff79dd456fe3054a60fe0a16f38bf5fc3928e1e8439ca4d945573f8c48c0b8
SHA1: 5996d02c142588b6c1ed850e461845458bd94d17
MD5: 9a0e765eecc5433af3dc726206ecc56e
File size: 62.9 KB (64400 bytes)
File name: 9A0E765EECC5433AF3DC726206ECC56E
File type: ELF
Detection ratio: 18 / 42
Analysis date: 2012-12-07 13:05:55 UTC (1 minute ago)
Additional information
Antivirus Result Update
Avast MacOS:Wirenet-A [Trj] 20121207
AVG BackDoor.Generic_c.EYI 20121207
Comodo UnclassifiedMalware 20121207
DrWeb BackDoor.Wirenet.1 20121207
ESET-NOD32 Linux/Netweird.A 20121207
F-Secure Backdoor:Linux/NetWeirdRC.A 20121207
Fortinet Linux/Wirenet.A!tr.bdr 20121207
GData MacOS:Wirenet-A 20121207
Ikarus Trojan.Win32.Agent 20121207
Jiangmin Backdoor/Linux.fh 20121207
Kaspersky Backdoor.Linux.Wirenet.a 20121207
McAfee Linux/NetWeirdRC 20121207
McAfee-GW-Edition Linux/NetWeirdRC 20121207
Microsoft Backdoor:Linux/NetWiredRC.A 20121207
PCTools Malware.Linux-Backdoor 20121207
SUPERAntiSpyware - 20121207
TrendMicro-HouseCall ELF_NETWRD.A 20121207
VIPRE Trojan.ELF.Netweird.a (v) 20121207
ViRobot Linux.A.Wirenet.64400 20121207

https://www.virustotal.com/file/257da8c8b296dac6b029004ed06253fe622c5438b4a47b7dfbb87323b64f50a1/analysis/1354885571/
SHA256: 257da8c8b296dac6b029004ed06253fe622c5438b4a47b7dfbb87323b64f50a1
SHA1: c36f0943484ce8f8aba2d649aae2ad1243947c4e
MD5: c3b48db40cf810cb63bf36262b7c5b19
File size: 76.8 KB (78664 bytes)
File name: C3B48DB40CF810CB63BF36262B7C5B19
File type: unknown

Detection ratio: 25 / 46
Analysis date: 2012-12-07 13:06:11 UTC (1 minute ago)
Additional information
Antivirus Result Update
Agnitum Backdoor.OSX.NetWeirdRC.A 20121206
AntiVir MACOS/Wirenet.A 20121207
Avast MacOS:Wirenet-A [Trj] 20121207
AVG BackDoor.Generic_c.EYF 20121207
ClamAV Trojan.OSX.Netweird.A 20121207
Comodo UnclassifiedMalware 20121207
DrWeb BackDoor.Wirenet.1 20121207
ESET-NOD32 OSX/Netweird.A 20121207
F-Secure Backdoor:OSX/NetWeirdRC.A 20121207
Fortinet OSX/NetWrdRC.A 20121207
GData MacOS:Wirenet-A 20121207
Ikarus Backdoor.MacOS_X 20121207
Kaspersky Backdoor.OSX.Wirenet.a 20121207
McAfee OSX/NetWeirdRC 20121207
McAfee-GW-Edition OSX/NetWeirdRC 20121207
Microsoft Backdoor:MacOS_X/NetWiredRC.A 20121207
MicroWorld-eScan - 20121207
NANO-Antivirus Trojan.Mac.Wirenet.wpzjm 20121207
PCTools Malware.OSX-Sabpab 20121207
Sophos OSX/NetWrdRC-A 20121207
SUPERAntiSpyware - 20121207
Symantec OSX.Sabpab 20121207
TrendMicro OSX_NETWRD.A 20121207
TrendMicro-HouseCall OSX_NETWRD.A 20121207
ViRobot Backdoor.OSX.A.Wirenet.78664.A 20121207

https://www.virustotal.com/file/137e17ed0c693f5ba23c3f3bf252f7edc29548d97f426625a4e0c5fea0558e45/analysis/
SHA256: 137e17ed0c693f5ba23c3f3bf252f7edc29548d97f426625a4e0c5fea0558e45
SHA1: c520e9099bfc695b54662bdb7e8fa5b2800a72e9
MD5: d048f7ae2d244a264e58af67b1a20db0
File size: 76.1 KB (77940 bytes)
File name: 137e17ed0c693f5ba23c3f3bf252f7edc29548d97f426625a4e0c5fea0558e45
File type: unknown
Detection ratio: 21 / 43
Analysis date: 2012-11-11 16:27:47 UTC (3 weeks, 4 days ago)
AntiVir MACOS/Wirenet.A.1 20121111
Avast MacOS:Wirenet-A [Trj] 20121111

AVG BackDoor.Generic_c.EYJ 20121111
Comodo UnclassifiedMalware 20121111
DrWeb BackDoor.Wirenet.1 20121111
Emsisoft Backdoor.OSX.Wirenet (A) 20121111
ESET-NOD32 a variant of OSX/Netweird.A 20121111
F-Secure Backdoor:OSX/NetWeirdRC.A 20121111
Fortinet W32/OSX_Wirenet.A!tr.bdr 20121111
GData MacOS:Wirenet-A 20121111
Ikarus Backdoor.OSX.Wirenet 20121111
Kaspersky Backdoor.OSX.Wirenet.a 20121111
McAfee OSX/NetWeirdRC 20121111
McAfee-GW-Edition OSX/NetWeirdRC 20121111
Microsoft Backdoor:MacOS_X/NetWiredRC.A 20121111
PCTools Backdoor.Trojan 20121111
Sophos OSX/NetWrdRC-A 20121111
SUPERAntiSpyware - 20121111
Symantec Backdoor.Trojan 20121111
TrendMicro OSX_NETWRD.A 20121111
TrendMicro-HouseCall OSX_NETWRD.A 20121111
ViRobot Backdoor.OSX.A.Wirenet.77940.B 20121111