Nov 2012 Worm Vobfus Samples

contagiodump.blogspot.com/2012/12/nov-2012-worm-vobfus-samples.html

End of the year presents:

This is a sample of W32.Vobfus / Worm_Vobfus

Related News and Analysis:
Nov 2012
Trend Micro What's the Fuss with WORM_VOBFUS?

Download

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

Download pcap 634AA845F5B0B519B6D8A8670B994906 WORM_VOBFUS.SMIS

Files

s70F0B7BD55B91DE26F9ED6F1EF86B456 *323CANON.EXE_WORM_VOBFUS.SM01
7B19B2B8AED0285EB2B2C5CB81313569 *WORM_VOBFUS.SMA3
634AA845F5B0B519B6D8A8670B994906 *WORM_VOBFUS.SMIS
4E15D812491FF0454F1E9393675B1C60 *WORM_VOBFUS.SMM2

File Information

4E15D812491FF0454F1E9393675B1C60 *WORM_VOBFUS.SMM2
759691.zdns.eu

7B19B2B8AED0285EB2B2C5CB81313569 *WORM_VOBFUS.SMA3
SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
qoutu.exe
ns1.helpchecks.net
634AA845F5B0B519B6D8A8670B994906 *WORM_VOBFUS.SMIS
SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN

C:\Documents and Settings\[username]\geoosi.exe
HTTP
443
222.186.36.128
GET http://82747.ddnsd[.]at:443/XEuPCLrf?e
GET http://82747.ddnsd[.]at:443/XEuPCLrf/?e
GET http://82747.ddnsd[.]at:443/1/?e
GET http://82747.ddnsd[.]at:443/wjAtBD/v4
GET http://82747.ddnsd[.]at:443/wjAtBD/v4/

GET /XEuPCLrf?e HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)
Host: 82747.ddnsd.at

HTTP/1.1 301 Moved Permanently
Server: nginx/1.0.0
Date: Fri, 07 Dec 2012 12:16:06 GMT
Content-Type: text/html
Content-Length: 184
Location: http://82747.ddnsd.at:443/XEuPCLrf/?e
Connection: keep-alive
<html>
<head><title>301 Moved Permanently</title></head>
<body bgcolor="white">
<h1>301 Moved Permanently</h1>
<hr> nginx/1.0.0
</body>
</html>

GET /XEuPCLrf/?e HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)

Host: 82747.ddnsd.at
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx/1.0.0
Date: Fri, 07 Dec 2012 12:16:06 GMT
Content-Type: application/octet-stream
Connection: keep-alive
X-Powered-By: PHP/5.1.6
Content-Description: File Transfer
Content-Disposition: attachment; filename=9091
Content-Transfer-Encoding: binary
Expires: 0
Cache-Control: must-revalidate
Pragma: public
Content-Length: 98304

MZ.....@.....!..L.!This program cannot be run in DOS mode.
$.....y.....Rich.....PE..L...
(!.P.....@...0.....T'.....P....@.....<.....

Automatic scans

https://www.virustotal.com/file/e54bbabcaed8ace734f53234a44ad1e697e9cd2252255b59906fc5e3322c1be6/analysis/
SHA256: e54bbabcaed8ace734f53234a44ad1e697e9cd2252255b59906fc5e3322c1be6
File name: 7b19b2b8aed0285eb2b2c5cb81313569
Detection ratio: 25 / 45
Analysis date: 2012-11-29 18:02:20 UTC (1 week ago)

Additional information
Behavioural information
Antivirus Result Update
Agnitum - 20121129
AhnLab-V3 Worm/Win32.Vobfus 20121129
AntiVir Worm/Vobfus.6122548 20121129
Antiy-AVL - 20121128
Avast Win32:VB-AFEA [Trj] 20121129
AVG - 20121129
BitDefender Gen:Variant.VBInject.25 20121129
ByteHero - 20121129
CAT-QuickHeal - 20121129

ClamAV - 20121129
Commtouch - 20121129
Comodo UnclassifiedMalware 20121129
DrWeb Win32.HLLW.Autoruner1.30327 20121129
Emsisoft Gen:Trojan.Heur.VP2.nm3@aO1nH8pi (B) 20121129
eSafe - 20121128
ESET-NOD32 Win32/Pronny.IG 20121129
F-Prot - 20121129
F-Secure Gen:Variant.VBInject.25 20121129
Fortinet - 20121129
GData Gen:Variant.VBInject.25 20121129
Ikarus Worm.Win32.Vobfus 20121129
Jiangmin Worm/Vobfus.kzc 20121129
K7AntiVirus - 20121129
Kaspersky Worm.Win32.Vobfus.akjm 20121129
Kingsoft Worm.Vobfus.ak.(kcloud) 20121119
McAfee W32/Autorun.worm.aaeh 20121129
McAfee-GW-Edition Artemis!7B19B2B8AED0 20121129
Microsoft Worm:Win32/Vobfus.MA 20121129
MicroWorld-eScan Gen:Variant.VBInject.25 20121129
NANO-Antivirus - 20121129
Norman - 20121128
nProtect - 20121129
Panda Trj/CI.A 20121129
PCTools - 20121129
Rising - 20121129
Sophos Mal/Autorun-AX 20121129
SUPERAntiSpyware Trojan.Agent/Gen-Remnat 20121129
Symantec WS.Reputation.1 20121129
TheHacker - 20121127
TotalDefense - 20121129
TrendMicro WORM_VOBFUS.SMA3 20121129
TrendMicro-HouseCall - 20121129
VBA32 - 20121129
VIPRE Trojan.Win32.Generic!BT 20121129
ViRobot Worm.Win32.A.Vobfus.155648.U 20121129

https://www.virustotal.com/file/7f7e5751277a0169ec2eb4492b0489ca850808f64b52e708f716f46ac160e54b/analysis/
WORM_VOBFUS.SMIS

SHA256: 7f7e5751277a0169ec2eb4492b0489ca850808f64b52e708f716f46ac160e54b

SHA1: 82ad537a7acb18702a02b6dd2c6d12eaac0b3656

MD5: 634aa845f5b0b519b6d8a8670b994906
File size: 188.0 KB (192512 bytes)
File name: 634aa845f5b0b519b6d8a8670b994906
File type: Win32 EXE
Tags: peexe
Detection ratio: 35 / 46
Analysis date: 2012-12-07 00:53:51 UTC (3 hours, 36 minutes ago)

Additional information
Antivirus Result Update
Agnitum - 20121206
AhnLab-V3 Worm/Win32.Vobfus 20121206
AntiVir Worm/Vobfus.9987551 20121207
Antiy-AVL - 20121204
Avast Win32:VB-AFCN [Trj] 20121207
AVG Worm/VB.14.EF 20121207
BitDefender Win32.Worm.TTL 20121206
ByteHero - 20121130
CAT-QuickHeal Worm.Vobfus.A3 20121206
ClamAV - 20121207
Commtouch - 20121206
Comodo TrojWare.Win32.Pronny.HV 20121206
DrWeb Trojan.Siggen4.38386 20121207
Emsisoft - 20121207
eSafe - 20121205
ESET-NOD32 a variant of Win32/VBObfus.GZ 20121206
F-Prot - 20121206
F-Secure Win32.Worm.TTL 20121207
Fortinet W32/Vobfus.AJJQ!worm 20121207
GData Win32.Worm.TTL 20121207
Ikarus Worm.Win32.Vobfus 20121206
Jiangmin Worm/Vobfus.kmt 20121206
K7AntiVirus Trojan 20121206
Kaspersky Worm.Win32.Vobfus.ajjq 20121206
Kingsoft Worm.Vobfus.(kcloud) 20121206
Malwarebytes Worm.SFDC 20121207
McAfee VBObfus.ey 20121207
McAfee-GW-Edition VBObfus.ey 20121206
Microsoft Worm:Win32/Vobfus.LS 20121207

MicroWorld-eScan Win32.Worm.TTL 20121206
NANO-Antivirus Trojan.Win32.Siggen4.bcftwa 20121206
Norman W32/Troj_Generic.FVRYE 20121206
nProtect Worm/W32.Vobfus.192512.C 20121206
Panda W32/Vobfus.GEV.worm 20121206
PCTools Malware.Changeup 20121207
Rising - 20121206
Sophos Mal/Autorun-AX 20121206
SUPERAntiSpyware Trojan.Agent/Gen-Vobfus 20121207
Symantec W32.Changeup 20121207
TheHacker - 20121207
TotalDefense Win32/VBDoc.A!generic 20121206
TrendMicro WORM_VOBFUS.SMIS 20121207
TrendMicro-HouseCall WORM_VOBFUS.SMIS 20121207
VBA32 Worm.Vobfus.ajhs 20121205
VIPRE Trojan.Win32.Generic.pak!cobra 20121206

https://www.virustotal.com/file/fe32599d6f2d1a874b65928cfd01a87f9d0a83d2b1e30b8f1148c8ad8aefd985/analysis/
SHA256: fe32599d6f2d1a874b65928cfd01a87f9d0a83d2b1e30b8f1148c8ad8aefd985
File name: 323CANON.exe
Detection ratio: 40 / 46
Analysis date: 2012-12-07 03:11:12 UTC (1 hour, 20 minutes ago)
00
More details
Analysis
Comments
Votes
Additional information
Antivirus Result Update
Agnitum Trojan.VBGent.Gen.1430 20121206
AhnLab-V3 Trojan/Win32.Jorik 20121206
AntiVir TR/Barys.26445896 20121207
Antiy-AVL - 20121204
Avast Win32:VB-ACUI [Trj] 20121207
AVG Win32/Cryptor 20121207
BitDefender Gen:Variant.Barys.2490 20121206
ByteHero - 20121130
CAT-QuickHeal Worm.Vobfus.Gen 20121206
ClamAV - 20121207
Commtouch W32/Vobfus.O.gen!Eldorado 20121206

Comodo Worm.Win32.Pronny.AK 20121206
DrWeb Win32.HLLW.Autoruner1.15857 20121207
Emsisoft Gen:Variant.Barys.2490 (B) 20121207
eSafe - 20121205
ESET-NOD32 Win32/Pronny.AQ 20121206
F-Prot W32/Vobfus.O.gen!Eldorado 20121206
F-Secure Gen:Variant.Barys.2490 20121207
Fortinet W32/Jorik.EGLG!tr 20121207
GData Gen:Variant.Barys.2490 20121207
Ikarus Trojan.Win32.Jorik 20121207
Jiangmin Trojan/VBObf.a 20121206
K7AntiVirus Trojan 20121206
Kaspersky Trojan.Win32.Jorik.Vobfus.cvtk 20121206
Kingsoft Win32.Troj.Generic.(kcloud) 20121206
Malwarebytes Trojan.Downloader.ic 20121207
McAfee VBObfus.dv 20121207
McAfee-GW-Edition VBObfus.dv 20121207
Microsoft Worm:Win32/Vobfus.FB 20121207
MicroWorld-eScan Gen:Variant.Barys.2490 20121206
NANO-Antivirus - 20121207
Norman W32/VB.TN 20121206
nProtect Trojan/W32.Agent.307200.TU 20121207
Panda W32/Vobfus.GEV.worm 20121206
PCTools Malware.Changeup 20121207
Rising Trojan.Win32.VbUndef.a 20121207
Sophos W32/Vobfus-AH 20121207
SUPERAntiSpyware Trojan.Agent/Gen-Vobfus 20121207
Symantec W32.Changeup 20121207
TheHacker Trojan/Jorik.Vobfus.cvtk 20121207
TotalDefense Win32/Vobfus.ADR 20121206
TrendMicro WORM_VOBFUS.SM01 20121207
TrendMicro-HouseCall WORM_VOBFUS.SM01 20121207
VBA32 Trojan.Jorik.Vobfus.cvtk 20121205
VIPRE Trojan.Win32.Vobfus.a (v) 20121206