Dec 2012 Linux.Chapro - trojan Apache iframer

contagiodump.blogspot.com/2012/12/dec-2012-linuxchapro-trojan-apache.html
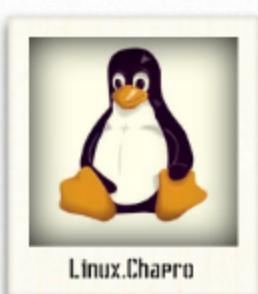
Here is another notable development of 2012 - Linux malware ([see Wirenet trojan posted earlier too](#))

Research: ESET Malicious Apache module used for content injection: Linux/Chapro.A

All the samples are below. I did not test it thus no pcaps this time.

------Linux/Chapro.A   e022de72cce8129bd5ac8a0675996318
------Injected iframe   111e3e0bf96b6ebda0aeffdb444bcf8d
------Java exploit   2bd88b0f267e5aa5ec00d1452a63d9dc
------Zeus binary   3840a6506d9d5c2443687d1cf07e25d0

Download

 Download. (Email me if you need the password scheme - see profile for email)
------Linux/Chapro.A   e022de72cce8129bd5ac8a0675996318
------Java exploit   2bd88b0f267e5aa5ec00d1452a63d9dc
------Zeus binary   3840a6506d9d5c2443687d1cf07e25d0

Automatic scans

 Analysis ESET Malicious Apache module used for content injection:

https://www.virustotal.com/file/345a86f839372db0ee7367be0b9df2d2d844cef406407695a2f869d6b3380ece/analysis/
SHA256: 345a86f839372db0ee7367be0b9df2d2d844cef406407695a2f869d6b3380ece

SHA1: 2ccb789d57d3ce3dd929307eb78878e6e5c61ccf
MD5: e022de72cce8129bd5ac8a0675996318
File size: 38.3 KB (39176 bytes)
File name: e022de72cce8129bd5ac8a0675996318
File type: ELF
Tags: elf
Detection ratio: 19 / 46
Analysis date: 2012-12-21 19:12:13 UTC (2 days, 11 hours ago)
AVG Generic6_c.CLGW 20121221
BitDefender Backdoor.Linux.Agent.E 20121221
CAT-QuickHeal - 20121220
Commtouch - 20121221
Comodo UnclassifiedMalware 20121221
DrWeb Linux.Iframe.1 20121221
ESET-NOD32 Linux/Chapro.A 20121221
F-Secure Backdoor.Linux.Agent.E 20121221
GData Backdoor.Linux.Agent.E 20121221
Ikarus Backdoor.Linux.Apmod 20121221
Jiangmin Backdoor/Linux.fs 20121221
K7AntiVirus Trojan 20121221
Kaspersky HEUR:Backdoor.Linux.Apmod.gen 20121221
MicroWorld-eScan Backdoor.Linux.Agent.E 20121221
nProtect Backdoor.Linux.Agent.E 20121221
PCTools Malware.Linux-Chapro 20121221
Sophos Troj/Apmod-D 20121221
SUPERAntiSpyware - 20121221
Symantec Linux.Chapro 20121221
TrendMicro ELF_CHAPRO.A 20121221
TrendMicro-HouseCall ELF_CHAPRO.A 20121221
ViRobot Linux.A.Apmod.39176 20121221

Exploit:Java/CVE-2012-1723
https://www.virustotal.com/file/a70a8891829344ad3db818b3c4ad76e38a78b0ce3c43d7aaf6
5752fe56d10e09/analysis/
SHA256: a70a8891829344ad3db818b3c4ad76e38a78b0ce3c43d7aaf65752fe56d10e09
SHA1: d01f76f5467c86bfa266c429e1315e7aad821f93
MD5: 2bd88b0f267e5aa5ec00d1452a63d9dc
File size: 30.2 KB (30957 bytes)
File name: nYCND
File type: ZIP
Tags: exploit zip cve-2012-1723
Detection ratio: 2 / 43

Analysis date: 2012-11-23 09:54:46 UTC (1 month ago)
Kaspersky UDS:DangerousObject.Multi.Generic 20121123
Microsoft Exploit:Java/CVE-2012-1723!generic 20121123

https://www.virustotal.com/file/12f38f9be4df1909a1370d77588b74c60b25f65a098a08cf81389c97d3352f82/analysis/
SHA256: 12f38f9be4df1909a1370d77588b74c60b25f65a098a08cf81389c97d3352f82
SHA1: 5050b57e01bb2aa9730f826f36ad4d41477d8bd9
MD5: 3840a6506d9d5c2443687d1cf07e25d0
File size: 222.0 KB (227328 bytes)
File name: 3840a6506d9d5c2443687d1cf07e25d0
File type: Win32 EXE
Tags: peexe
Detection ratio: 32 / 44
Analysis date: 2012-12-22 20:02:23 UTC (1 day, 10 hours ago)
Agnitum Trojan.Injector!5xrrtg7IXGQ 20121222
AntiVir TR/PSW.Zbot.2884 20121222
Avast Win32:Crypt-OMW [Trj] 20121222
AVG PSW.Generic10.AOEA 20121222
BitDefender Trojan.Generic.8218925 20121222
Comodo TrojWare.Win32.Trojan.Agent.Gen 20121222
DrWeb Trojan.PWS.Panda.368 20121222
ESET-NOD32 a variant of Win32/Injector.ZRA 20121222
F-Secure Trojan.Generic.8218925 20121222
Fortinet W32/Zbot.ARO!tr 20121222
GData Trojan.Generic.8218925 20121222
Ikarus Trojan.Win32.Yakes 20121222
Jiangmin TrojanSpy.Zbot.csit 20121221
K7AntiVirus Spyware 20121221
Kaspersky Trojan-Spy.Win32.Zbot.gmeq 20121222
Kingsoft Win32.Troj.Zbot.gm.(kcloud) 20121217
Malwarebytes Trojan.Agent 20121222
McAfee PWS-Zbot.gen.aro 20121222
McAfee-GW-Edition PWS-Zbot.gen.aro 20121222
Microsoft PWS:Win32/Zbot 20121222
Norman W32/ZBot.DIJG 20121222
nProtect Trojan.Generic.8218925 20121222
Panda Trj/Genetic.gen 20121222
PCTools Trojan-PSW.Generic!rem 20121222
Sophos Mal/Zbot-JM 20121222
SUPERAntiSpyware Trojan.Agent/Gen-Zbot 20121222
Symantec Infostealer 20121222
TheHacker Trojan/Injector.zra 20121222

TrendMicro TROJ_GEN.R21CDLF 20121222
TrendMicro-HouseCall TROJ_GEN.R21CDLF 20121222
VBA32 TrojanSpy.Zbot.gmeq 20121221
VIPRE Trojan.Win32.Generic!BT 20121222