OSX/Flashback.K sample + Mac OS malware study set (30+ older samples)

contagiodump.blogspot.com/2012/04/osxflashbackk-sample-mac-os-malware.html

Update April 12, 2012 Added another binary sv.4 - with plist fle (edited to remove userid)

OSX Flashback malware has been in the news a lot after Kaspersky's announcement about 600,000 botnet "Kaspersky Lab Confirms Flashfake / Flashback Botnet Infected more than 600,000 Mac OS X Computers, Describes Ramifications and Remedies "

I got a sample tonight thanks to Tim Strazzere and I have not analyzed it but I want to try. Meanwhile, I am posting this sample and 30+ other Mac OS malware samples accumulated by Contagio and also from vxheavens collection (thank you all). They are dated by the year and provide a good historical set to study the evolution of Mac malware - I would start here: SANS Mac OS X Malware Analysis or check out Reverse Engineering Mac Defender (OS X) malware analysis for beginners

Malware information

F-Secure removal procedure

Flashback checker (check if your computer/vm is infected)

ET signature

> **alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET TROJAN OSX/Flashback.K/I User-Agent"; flow:established,to_server; content:" WOW64|3b| rv|3a|9.0.1|3b| sv|3a|"; http_header; content:" id|3a|"; http_header; within:6; reference:url,f-secure.com/v-descs/trojan-downloader_osx_flashback_k.shtml; reference:url,vms.drweb.com/virus/?i=1816029; reference:url,f-secure.com/v-descs/trojan-downloader_osx_flashback_i.shtml; classtype:trojan-activity; sid:2014534; rev:3;)**

Download

Please email me if you need the password scheme

 Download OSX/Flashback.K C898CDE665DB8D62FEA634C28E284139

Download recent OSX Contagio samples
Download the historical MacOS malware set

Update April 12, 2012Download 5616687FAC5D040AE65CB1B08717A6AA

File information

Update April 12, 2012
com.sun.jsched.plist (from *~/Library/LaunchAgents/com.sun.jsched.plist*
Plist file contents (user name replaced with USERNAME)
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd"><plist version="1.0"><dict>
<key>Label</key><string>com.sun.jsched</string><key>ProgramArguments</key><array>
<string>/Users/USERNAME/.jsched</string></array><key>RunAtLoad</key><true/>
<key>StartInterval</key><integer>4212</integer><key>StandardErrorPath</key>
<string>/dev/null</string><key>StandardOutPath</key><string>/dev/null</string></dict>
</plist>

.jsched from *Users/USERNAME/.jsched*. If you must have UUID, email me.
Size: 59844
MD5: 5616687FAC5D040AE65CB1B08717A6AA

DOMAINS and UA from 5616687FAC5D040AE65CB1B08717A6AA

2012-Apr-10 12:38:16

client: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0.1; sv:4; id:4341D6B3-97DC-58F3-A696-D8AAE9EC1A08) Gecko/20100101 Firefox/9.0.1 (uuid changed)

174.129.221.183
rfffnahfiywyd.com
rfffnahfiywyd.net
rfffnahfiywyd.info
rfffnahfiywyd.in
rfffnahfiywyd.kz
cvsqsmuiaaiyh.com
cvsqsmuiaaiyh.net
cvsqsmuiaaiyh.info
cvsqsmuiaaiyh.in
cvsqsmuiaaiyh.kz

scfoijdccqtmj.com
scfoijdccqtmj.net
scfoijdccqtmj.info
scfoijdccqtmj.in
scfoijdccqtmj.kz

End of Update April 12, 2012

==========

OSX/Flashback.K
Size: 59844
MD5: C898CDE665DB8D62FEA634C28E284139

Other malware recent
2011 Olyx Backdoor 93a9b55bb66d0ff80676232818d5952f - Contagio
2011 MacDefender fb6f092624d48fe9a496c50f615b424b27cf3515
and MacProtector 1f8e9cd3f0717a85b96f350e4f4a539a - Contagio
2010 OSX/Boonana.A facebook trojan 7a04e9185daf9551edd90e7bff2daa8e and 2533F62C321117C46D6DF6122C3009BD - Contagio

Historical MacOS malware set

1992	Virus.Mac.Code252.a	F446DEB312A955713B97DB2169165CF5
1992	Virus.Mac.Init1984.a	EDD3A891DA59A0A3CD8E880F175DAFCD
1994	Virus.Mac.Init29.a	66CE0EAF0175D9113CE1D06FCD459FD0
2000	Virus.Mac.Init9403.a	F8DC251414AE7B61535DAE3E740BE9EC
2000	Virus.Mac.Mdef.a	A7A6389FC1B557A3271984B543E62419
2000	Virus.Mac.Mdef.c	CA9ADCA2E776C2B814D775F1F495665F
2000	Virus.Mac.Mdef.d	D934045683902939454B8B73DE839241
2000	Virus.Mac.Mdef.e	92305C6780AB3286AEC6660652C29A26
2000	Virus.Mac.Nvir.a	D80E0F45387447504435ADD8572FECEC
2000	Virus.Mac.Nvir.b	36A0E2A4C6A3166FC017A0CDA942157C
2000	Virus.Mac.Wdef.a	0B1565AE48EA70FC620308A357F261DA
2000	Virus.Mac.Wdef.b	9A223E402D4121E8E421ABCA0BC05820
2000	Virus.Mac.Zuc.a	1425EB1FDEE4B1835E0AC2AE031501EB
2000	Virus.Mac.Zuc.b	9B750CFE7B7730B30DC4A93A56A2D4F0
2000	Virus.Mac.Zuc.c	4B4A8F711957BB37A2747CA7036189E7
2001	Virus.Mac.Simpsons.a	3EDF7343D6A5DCD6AE748482B90386AA
2002	Virus.Mac.Init666.a	14BECD6024A447F0B3A927E968F11127
2005	irus.Mac.Sevendust.b	1AF001A295BDDECE107BEA633A4110A8
2005	Virus.Mac.Cdef.a	E256064B76351A3C37937843EC439F61
2005	Virus.Mac.ChinaTalk.a	A68E971FCD602161701E3E139A3B1BC1
2005	Virus.Mac.Code1.a	EE86680A66BD953E309CD5A461010D29
2005	Virus.Mac.MacMag.a	329E85AF8A6D719AA088E8195021A0B8
2005	Virus.Mac.MacMag.b	29A126B98C43AD3FB96659719E8479CE
2005	Virus.Mac.Scores.a	F96F50C90C591BF45B96E9EB40ECCA44
2005	Virus.Mac.Sevendust.a	18B3A5437E6E6448AC80D10139AEE099
2005	Virus.Mac.Sevendust.d	860F251EE934B10EACD5559E6BAD2285
2005	Virus.Mac.Sevendust.e	9898A5F12B06BEB87CA18C61309FA36A
2005	Virus.Mac.T4.a	ED9008767028E449AB8938C02D2E3EF8
2007	Worm.OSX.Niqtana.a	2C25908053ECC1474D2FB2C530EA5CFA
2008	Backdoor.Mac.Hovdy.b	FED713CAC7012D25F60B236E6DDCF513
2008	Trojan-PSW.OSX.Corpref.a	DF464DE7A6EB04FEB95504D74F7505DA
2009	Trojan-Downloader.OSX.Jahlav.a	FB79A75A6152EF47BBF88AE8544545CC
200x	Exploit.Mac.Small.c	3DC01743FB42E917E9F9EDE5009F10CD
200x	Virus.Mac.Flag.a	E3F82C900CD71C070CAAF0B09EA02900
200x	Virus.Mac.Anti.a	62CC37E947C425A3BB2CB15544D2EF9E