OSX/Flashback.O sample + some domains

Archived: 2026-04-06 00:03:35 UTC

OSX/Flashback.O sample + some domains

1. A few hours after I posted the Flashback.K, someone anonymously uploaded Flashback.O sample (thank you very much!), which I am posting below. Like in the first case, it is a payload binary from a victim, not the downloader, which makes it impossible to install. If you succeed or have a binary that installs, please share. I personally have not tried to run them yet, did not have a vm.

2. Matt Thompson from Unveillance emailed his comments about the Flackback.K sample please see the quote below.

3. Update April 11 - I will put domains and URLs in a separate post because they relate to various versions of Flashback, not v.40/O

Download

From Matt Thompson regarding the previous Flashback.K
This is the exact payload binary I have been working with.

> I extracted the x86_64 architecture into a thin binary.
>
> At 0x10000158e it sets up an RC4 identity Sbox.
> At 0x1000015b2 it starts the RC4 KSA mix with the Hardware UUID. r9
> contains the pointer to the UUID string
>
> 0x1000041f0 contains the ciphertext length.
> 0x100004200 is the beginning of 4275 bytes of ciphertext.
> 0x1000041e8 contains a flag indicating if the data block is encrypted or
> not. If this is set to 1 the code just memcpy()'s the data into a
> malloc'd buffer rather than decrypting with RC4.
>
> If the Hardware UUID were available from the machine that downloaded
> this binary, it would be trivial to write the plaintext back into the
> binary and set 0x1000041e8 to 1.

Automated Scans

Virustotal
SHA256: 228be46149dd6efe9c57c881cc057d5dc1cfb759f9e9be8445f1d9d2d68875b3
SHA1: 62121738530d17292a75d17421bcd76a4051cad8
MD5: 782c4d24d406538498c1fb79fa0f6d62
File size: 394.2 KB (403676 bytes)

File name: FlashBack.O_ 782C4D24D406538498C1FB79FA0F6D62
File type: unknown
Detection ratio: 19 / 42
Analysis date: 2012-04-11 01:15:36 UTC (38 minutes ago)
Antiy-AVL Trojan/OSX.Flashfake 20120410
BitDefender MAC.OSX.Trojan.FlashBack.O 20120411
ClamAV OSX.Flashback-12 20120411
Comodo UnclassifiedMalware 20120410
DrWeb BackDoor.Flashback.40 20120411
Emsisoft Trojan-Downloader.OSX.Flashfake!IK 20120410
F-Secure MAC.OSX.Trojan.FlashBack.O 20120410
Fortinet OSX/Flshplyr.A 20120411
GData MAC.OSX.Trojan.FlashBack.O 20120411
Ikarus Trojan-Downloader.OSX.Flashfake 20120411
Jiangmin TrojanDownloader.OSX.w 20120410
Kaspersky Trojan-Downloader.OSX.Flashfake.ae 20120410
Microsoft Backdoor:MacOS_X/Flashback.E 20120411
NOD32 OSX/Flashback.I 20120410
nProtect MAC.OSX.Trojan.FlashBack.O 20120410
Sophos OSX/Flshplyr-A 20120411
Symantec OSX.Flashback.K 20120411
TheHacker - 20120410
TrendMicro OSX_FLASHBACK.A 20120411
TrendMicro-HouseCall OSX_FLASHBACK.A 20120411

6144:7tC8qm/SOIMr5lGsl1SFBu5w7FyR5ifPhebUUCNQQFJHvC4SODuanMiiK:Rvqw5lGsl1SFBuVRAZGUUCeQnvR52K
TrID
Java Bytecode (53.2%)
Mac OS X Universal Binary executable (35.5%)
HSC music composer song (11.2%)
ExifTool

MIMEType.....: application/octet-stream
FileType.....: Mach-O fat binary executable
CPUCount.....: 2
ObjectFileType.....: Dynamically bound shared library
CPUType.....: x86 64-bit, x86
CPUSubtype.....: i386 (all) 64-bit, i386 (all)

First seen by VirusTotal
2012-04-05 17:06:28 UTC (5 days, 8 hours ago)
Last seen by VirusTotal
2012-04-11 01:15:36 UTC (38 minutes ago)
File names (max. 25)

1. FlashBack.O_ 782C4D24D406538498C1FB79FA0F6D62

Source: http://contagiodump.blogspot.com/2012/04/osxflashbacko-sample-some-domains.html