

Malicious Ad for Homebrew Leads to MacSync Stealer

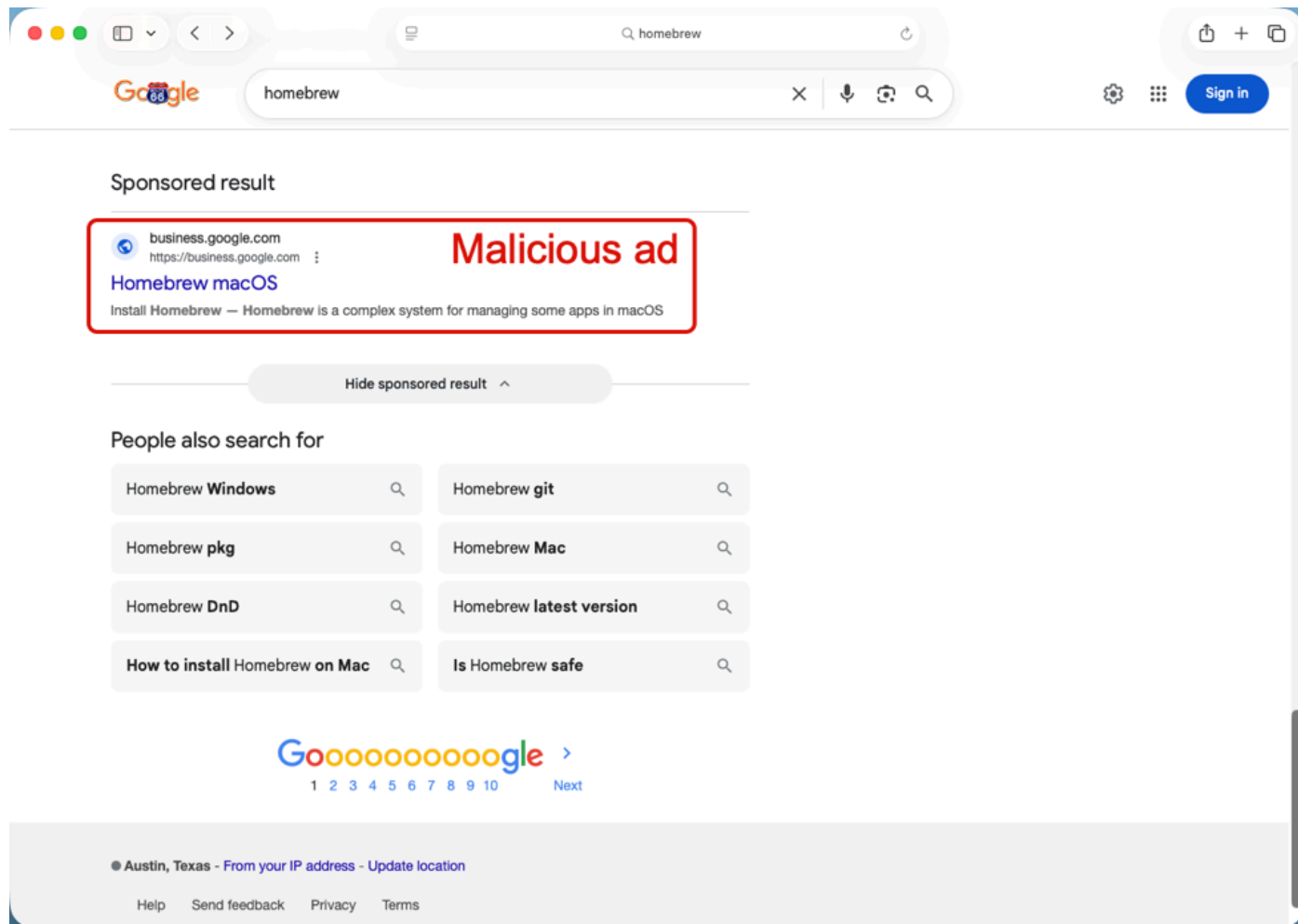
 dshield.org/diary/Malicious+Ad+for+Homebrew+Leads+to+MacSync+Stealer/32942

[0 comment\(s\)](#)

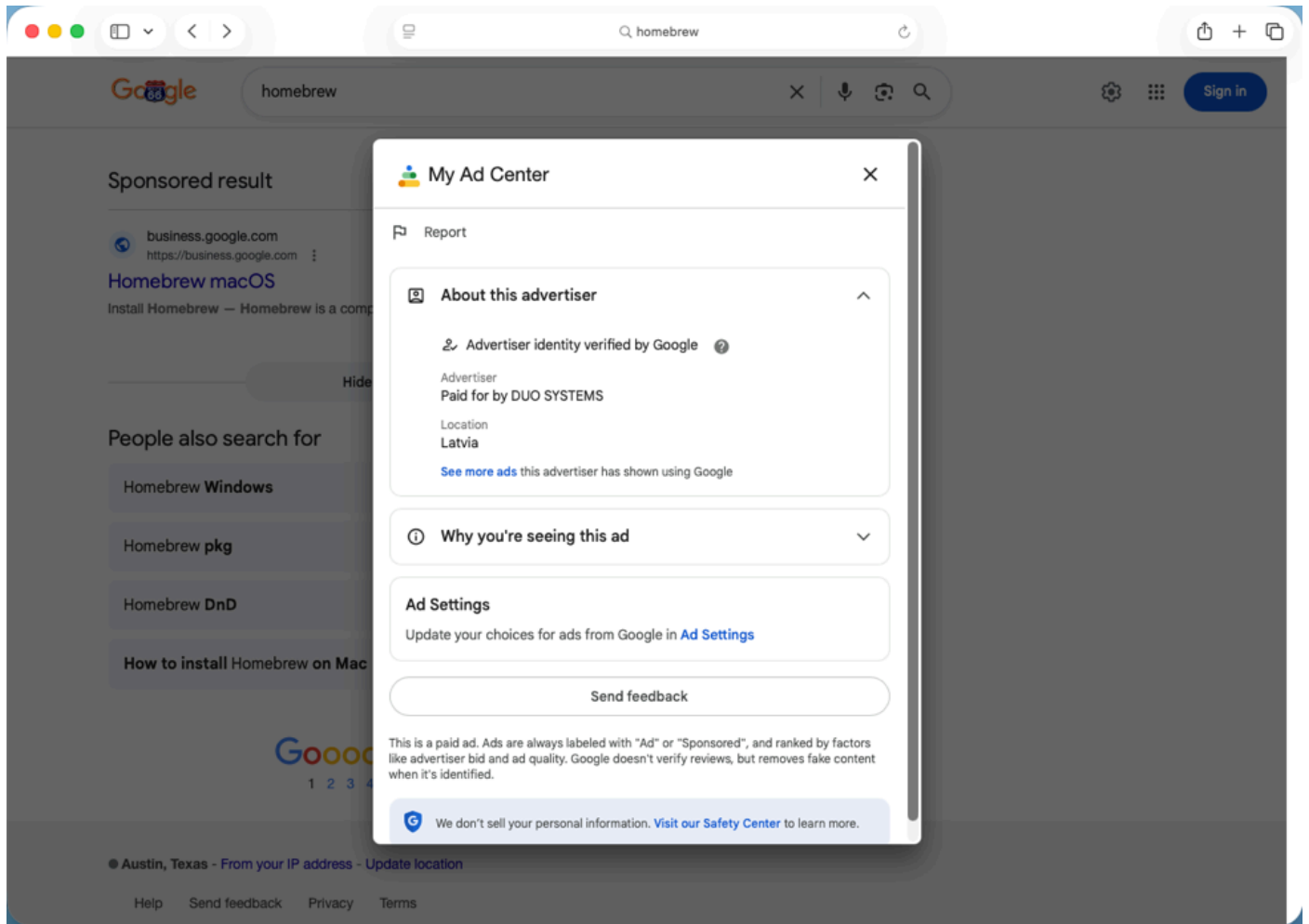
As macbooks and mac minis become more popular, we're seeing more campaigns targeting these macOS hosts. Malicious ads have popped up in search results that can lead potential victims to pages that present themselves as legitimate malware but instead are malware. This diary presents one such example from a malicious ad for a page that impersonates Homebrew we saw on Thursday, 2026-04-30.

Homebrew is a third-party package manager for macOS, and this page pushes MacSync Stealer malware. As I write this today (2026-05-01), the fake Homebrew page at `hxxps[:]//sites.google[.]com/view/brewpage` is still active.

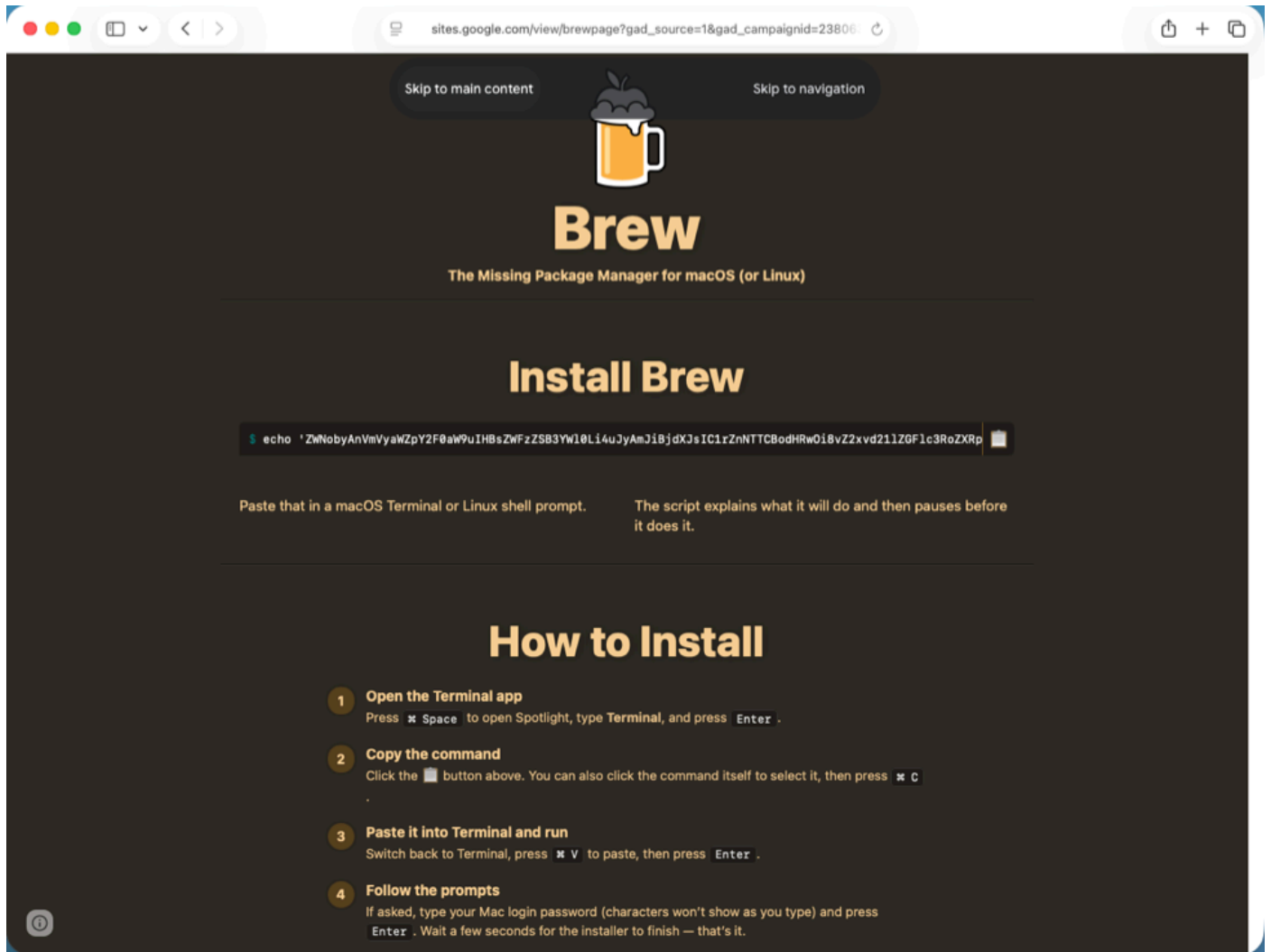
Images



Shown above: Malicious ad in search results leading to fake Homebrew page.



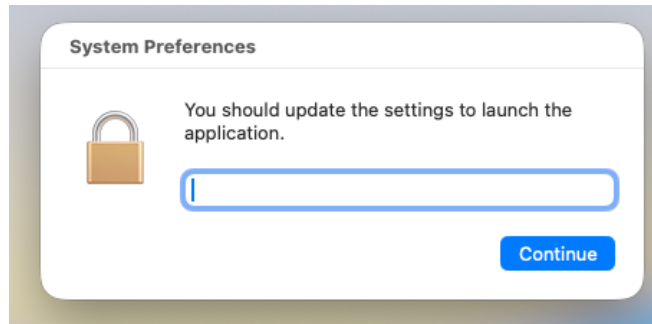
Shown above: Information about the advertiser for the malicious ad.



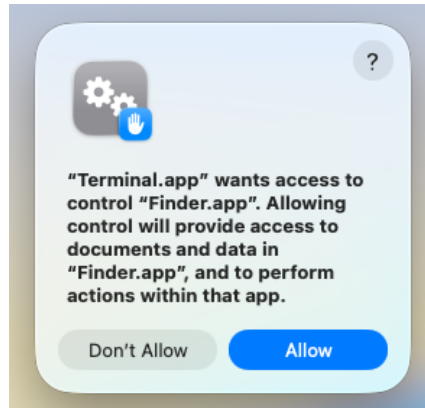
Shown above: Fake Homebrew page with script to copy/paste for potential victims to download malware.



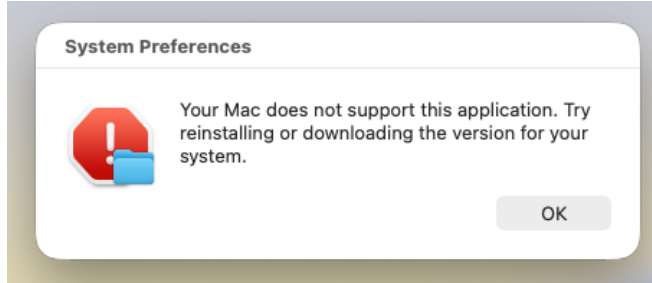
Shown above: Script from fake Homebrew page pasted to a terminal window on a macOS host.



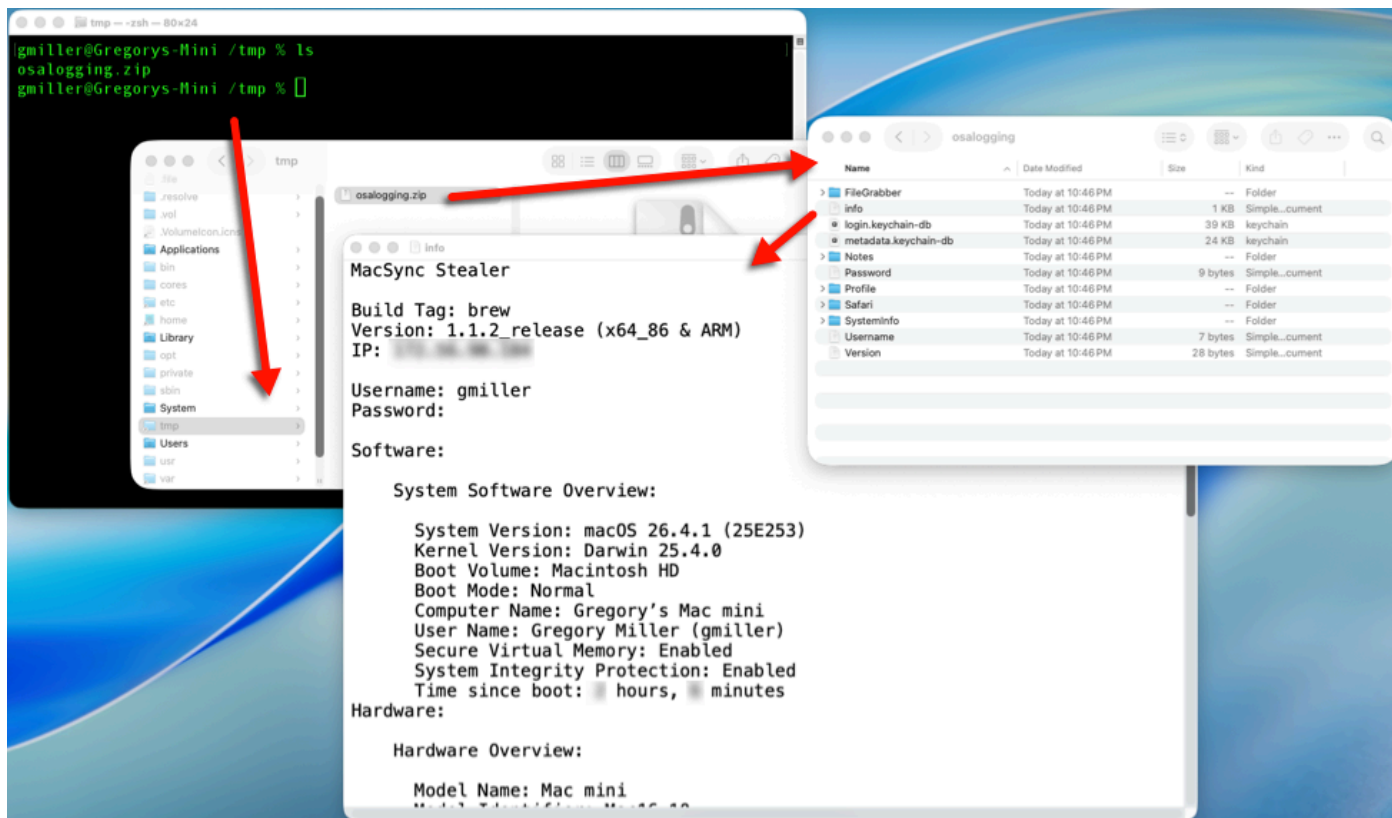
Shown above: After running the script, this popup appears, and it collects the victim's password.



Shown above: After running the entering the password, this popup appears for the Terminal app to access the Finder app in macOS.



Shown above: This is the final popup that appears after running the script.



Shown above: During the infection, MacSync Stealer collects information from the host, temporarily saves it to /tmp/osaloggging.zip and sends that file to the C2 server.

Time	Dst	Port	Host	Info
2026-04-30 21:18:42	104.21.80.251	80	glowmedaesthetics.com	GET /curl/63810ee8b478575f
2026-04-30 21:18:42	104.21.80.251	80	glowmedaesthetics.com	GET /dynamic?txd=63810ee8b
2026-04-30 21:20:30	104.21.80.251	80	glowmedaesthetics.com	PUT /gate?buildtxd=63810ee

Shown above: Traffic from the infection filtered in Wireshark.

Wireshark · Follow TCP Stream (tcp.stream eq 11) · 2026-04-30-MacSync-Stealer-infection.pcap

```

PUT /gate?
buildtxd=63810ee8b478575f3b2c6c46160c1fd338b213c6fc11bb0069dac9bbb7db237d&upload_id=177
7584030-5cc6ee67417cecb9&chunk_index=0&total_chunks=1 HTTP/1.1
Host: glowmedaesthetics.com
Accept: */*
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
api-key: 5190ef1733183a0dc63fb623357f56d6
Content-Length: 36920
Content-Type: application/x-www-form-urlencoded

PK.....a.\.....PasswordUX..E..iE..i....KK.4K633R..PK..y?.....PK..
....j.\....._MACOSX/UX..X..iX..i....PK.....a..
\....._MACOSX/_PasswordUX..E..iE..i....c`.cg`b`.MLV..V.P.....'.....@..
...RRRQ...8...A..0]...PK..OI.l9...x...PK.....a.\.....login.keychain-
dbUX..E..iE..i....]y\..G..@8B.A... ..QQ..."..m1...@0 ..'}.U....-
xk....Z....L...a6d.....!<..}f...g.yf..V..Ip.t..9..#.=.?|.V.a
.]U....At. ...*....&.....FAZ.A.Tj.j\W./...@....y...@E...BZxd.rLf.?..H...y5...$.w...#5.
{jTdJR...="Rc.cz...E.X&<..Qm|Drr.....$R.....Q.}.....j.H.....%.G.....
$.H..tf.....HG....`N...<*2R&...tfi..vDM.....WTjBJd...q....x.d.>..#.Wl...hR.)....
....$...#...U.u}..'&e%..@....H.S.....&%..`
.).....<.x..f...o.....o..9...[.o.....[.o ..%.<.y.....o....V.[.....<.x>...[.o
.5.6...o..
....o..-V...o.....o..=...;.....;.....#.N.;.....;.....3...g...@A@..@a@.....4.
....wF.2/M....u&..).?....s<.....o.....q....e...g.....zx..`+...=<.n0..0....&.
9Y...g+...d..x>..%Y...H.:
m.....l=-+.."0.....sT12=-=

```

28 client pkts, 1 server pkt, 1 turn.

Entire conversation (38 kB)
 104.21.80.251:80 → 10.4.30.101:49154 (935 bytes)
 10.4.30.101:49154 → 104.21.80.251:80 (37 kB)

Show data as ASCII Stream 11

Find Next

Filter Out This Stream Print Save as... Back * Close

Shown above: Traffic from the infected host sending the /tmp/osaloggging.zip file to the C2 server.

Indicators of Compromise

Example of URL from malicious ad:

```

hxxps[:]//www.google[.]com/aclk?sa=L&
ai=DChsSEwi24vK_v5aUAxXZS38AHRAFIWAYACICCAIQABoCb2E&
co=1&
gclid=EAlaIqobChMltuLyv7-WIAMV2Ut_AB0QBSFgEAMYASAAEgKrq_D_BwE&
cid=CAASugHkaEZtQvhFJBWvSVo_oMtlq6IKBxptjJBacaXOdzM28vxFNm3V2vrefacF48NMD0YvBIV9PCmn_d6X0uiMYDt5bwJYXaT6Lt7Mf3F-
Mc3OK-0ugNt4GfcvQ0IOkP1Sf8WVDXTMPeVMsHE8qxoG43Ta5BRER_Sre0RfChP39oVqtwRkowlKUUojM12uBAYWvvejokVOa_j7-
uGyN1XrQ1ae6Tfaijfc9OvMC9QKQovm7p0DBitWtBJ_d4&
cce=1&
sig=AOD64_2EqeARnVjOoYvCwtJyl1AsolQe7g&q&
adurl&
ved=2ahUKEwjyq-2_v5aUAxU3g2oFHc28JOUQ0Qx6BAhnEAE

```

Example of fake Homebrew site URL:

```

hxxps[:]//sites.google[.]com/view/brewpage?gad_source=1&
gad_campaignid=23806351087&
gbraid=0AAAAACJ6-Kb3hWjjAWCyYLIj0YO5oQvtp&
gclid=EAlaIqobChMltuLyv7-WIAMV2Ut_AB0QBSFgEAMYASAAEgKrq_D_BwE

```

Domain used by C2 server for the MacSync infection:

glowmedaesthetics[.]com

Files from the infection:

SHA256 hash: [a4fcfecc5ac8fa57614b23928a0e9b7aa4f4a3b2b3a8c1772487b46277125571](#)

- File size: 225 bytes
- File type: ASCII text, with no line terminators
- File description: Copy/paste script from the fake Homebrew page.

SHA256 hash: [0d58616c750fc8530a7e90eee18398ddedd08cc0f4908c863ab650673b9819dd](#)

- File size: 1,448 bytes
- File type: Paul Falstad's zsh script text executable, ASCII text
- File location: hxxp[.]/glowmedaesthetics[.]com/curl/63810ee8b478575f3b2c6c46160c1fd338b213c6fc11bb0069dac9bbb7db237d
- File description: Initial download from the copy/paste script

SHA256 hash: [86d0c50cab4f394c58976c44d6d7b67a7dfbbb813fbc622236e183d94fd944f](#)

- File size: 2,647 bytes
- File type: Paul Falstad's zsh script text executable, ASCII text
- File description: Shell script extracted from base64 text in the initial download

Bradley Duncan

brad [at] malware-traffic-analysis.net

Keywords: [Malvertizing Stealer](#) [MacSync](#) [MacSyncStealer](#)
[0 comment\(s\)](#)

Click [HERE](#) to learn more about classes Brad is teaching for SANS

Comments

[Login here to join the discussion.](#)

Diary Archives

- [Homepage](#)
- [Diaries](#)
- [Podcasts](#)
- [Jobs](#)
- [Data](#)
- [Tools](#)
- [Contact Us](#)
- [About Us](#)