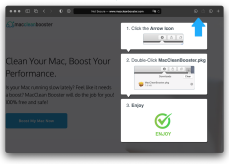
Example event chain leading to OSX/TrojanDownloader.Adload.AF

Ad network



maccleanbooster.com

Sends telemetry to https://app-stream.net/pkg

https://client-products.s3.amazonaws.com/maccleanbooster/MacCleanBooster.pkg

MacCleanBooster.pkg

`1807eb8c3719c9faa0210d8a5df2068d2c89d90d`

Signed by ANDREA CANAVAN (3QYCVT77CW)

Sends telemetry to https://events.maccleanbooster.com/pkg

Downloads and and install from
https://dl.maccleanbooster.com/MacCleanBooster.app.zip

MacCleanBooster.app

Potentially unwanted decoy application

ZIP: `da7f41f5fdc656c367fc4af6467f142d863c4283`

Timestamp in zip: 2020-06-15 04:33:56

Signed by charlesda@avantisteam.com (T8XWH9J4M6)

Downloads and make persistent via LaunchAgent
https://dl.maccleanbooster.com/MacCleanBoosterUpdateAgent.zip

MacCleanBoosterUpdateAgent

ZIP: `2892a72fee63e4ad0a34fd8e9412571d02ee14a8`

Mach-O: `f59602e043f9788b5924f8e1c225483f934bf5d8`

Timestamp in zip: 2020-11-18 17:51:06

Runs Bash script from
https://apinew.maccleanbooster.com/hb/hbnew?machine_id=$MACHINEID&pr=maccleanbooster

Bash script

`8abb0defedb0eddb48a14a2c2721c53c8020ad00`

Sends telemetry to https://d7rp2fva69arq.cloudfront.net/pkg

Downloads and make persistent via LaunchAgent
https://lnzjvpeyarvvvtljxsws.s3.amazonaws.com/ConsoleSoftwareUpdateAgent.zip

ConsoleSoftwareUpdateAgent

`8dbc48768edd795b1446e04e5cc2fd9dbf196410`

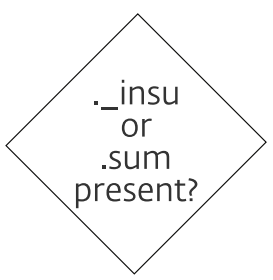
Timestamp in zip: 2021-01-26 08:48:58

Runs Bash script from
https://status.consoleupdateagent.com/prod/ianew?maid=$MACHINEID

Bash script

`6dcd11b70c535dca09208aaf8168d962a9daa13d`

Sends telemetry to https://daqi268hfl8ov.cloudfront.net/pkg

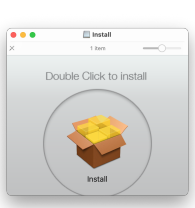


Yes

Don't install next stage, but keep existing persistant malware intalled

No

Download and runs Install.app
https://d2dkq0ln8vjekb.cloudfront.net/ZnVvh?source={TC}&a=5&k=...



Setup.dmg

`9b0fa382642c721b7bab4891b31d640d9a6e4b33`

Timestamp in dmg: 2021-02-23 17:58:40

@ESETresearch