5907d59ec1303cfb5c0a0f4aaca3efc0830707d86c732ba6b9e842b5730b95dc

Sign in Sign up

26
/ 62

Community Score

26/62 security vendors flagged this file as malicious

Reanalyze Similar More

5907d59ec1303cfb5c0a0f4aaca3efc0830707d86c732ba6b9...
com.intermessenger.hornfish

dmg contains-macho persistence checks-hostname

Size
1.29 MB

Last Analysis Date
4 months ago

DMG

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

☑ Display grouped sandbox reports

☑ OS X Sand... ⚠ 0 8 3 0 4 25

Activity Summary

Download Artifacts Full Reports Help

⚠ Detections

NOT FOUND

Mitre Signatures

2 LOW 35 INFO

IDS Rules

1 HIGH 2 LOW

Sigma Rules

NOT FOUND

Dropped Files

1 JAVASCRIPT 1 ZIP 1 MACH_O

Network comms

1 HTTP 7 DNS 16 IP 1 JA3

Behavior Tags ⓘ

checks-hostname persistence

MITRE ATT&CK Tactics and Techniques

+ Execution TA0002
+ Persistence TA0003
+ Privilege Escalation TA0004
+ Defense Evasion TA0005
+ Credential Access TA0006
+ Discovery TA0007
+ Collection TA0009
+ Command and Control TA0011

Crowdsourced IDS rules ⓘ

⚠ Matches rule MALWARE-CNC User-Agent known malicious user-agent string - Elite Keylogger at Snort registered user ruleset
↳ *trojan-activity*

⚠ Matches rule (http_inspect) invalid status line at Snort registered user ruleset
↳ *unknown*

⚠ Matches rule ET STREAM 3way handshake wrong seq wrong ack at Suricata
↳ *Generic Protocol Command Decode*

We use cookies and related technologies to remember user preferences, for security, to analyse our traffic, and to enable website functionality. Learn more about cookies in our Privacy Notice.

Ok

Sign in Sign up

HTTP Requests

+ GET http://dfgftt4ecf1of.cloudfront.net/assets/getmediaplayerpro_1496803053/images/mediaplayerpromac.zip 200

DNS Resolutions

+ dfgftt4ecf1of.cloudfront.net

getunzippro.com

+ mask-api.fe.apple-dns.net

+ mask-api.icloud.com

os.maxemem.com

IP Traffic

TCP 23.63.242.90:443
TCP 23.208.144.168:443
TCP 23.223.199.187:443
TCP 17.253.5.207:443
TCP 23.208.144.24:443
TCP 18.154.131.55:80 (dfgftt4ecf1of.cloudfront.net)
TCP 192.229.211.108:80
TCP 17.253.1.202:443
TCP 17.248.193.17:443 (mask-api.icloud.com)
TCP 44.235.78.64:443 (pubingress-feedback-1a6fe9caff1148fe.elb.us-west-2.amazonaws.com)

JA3 Digests

773906b0efdefa24a7f2b8eb6985bf37

TLS

+ gsa.apple.com

Behavior Similarity Hashes ⓘ

OS X Sandbox	0d1d59607374fab0d052794d822be545

File system actions ⓘ

Files Opened

/Applications
/Library/Apple/System/Library/CoreServices/SafariSupport.bundle
/Library/Apple/System/Library/CoreServices/SafariSupport.bundle/Contents
/Library/Apple/System/Library/CoreServices/SafariSupport.bundle/Contents/Info.plist
/Library/Apple/System/Library/PrivateFrameworks/MobileDevice.framework/Versions/A/Resources
/Library/Application Support/CrashReporter/AnonymousIdentifier_564D2B9B-D136-1F94-5C72-8887AA0D0417.plist
/Library/Application Support/CrashReporter/SubmitDiagInfo.domains
/Library/Frameworks/Mono.framework/Versions/6.12.0/bin
/Library/Managed Preferences/com.apple.MCXDebug.plist
/Library/Preferences/com.apple.MCXDebug.plist

Files Written

/Users/maria/Library/Caches/com.apple.ap.adprivacyd/fsCachedData/854F653F-BD5F-4B7C-9E6D-7F7E3F1F6B90.tmp
/private/var/db/powerlog/Library/PerfPowerTelemetry/MetadataReports/.dat.nosync0353.4BTar6
/private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/NSCreateObjectFileImageFromMemory-DxzxfYTC

Sign in Sign up

```
/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/.dat.nosync0344.rU8PRz
```

Files Deleted

```
/Users/maria/Library/Caches/com.apple.ap.adprivacyd/fsCachedData/854F653F-BD5F-4B7C-9E6D-7F7E3F1F6B90
/Users/maria/Library/Caches/com.intermessenger.hornfish/Cache.db-journal
/Users/maria/Library/Caches/com.intermessenger.hornfish/fsCachedData_remove
/Users/maria/Library/WebKit/LocalStorage/StorageTracker.db
/var/db/powerlog/Library/BatteryLife/Archives/powerlog_2023-07-09_B07496DD.PLSQL-shm
/var/db/powerlog/Library/BatteryLife/Archives/powerlog_2023-07-10_91E73498.PLSQL-shm
/var/db/powerlog/Library/BatteryLife/Archives/powerlog_2023-07-11_9F718964.PLSQL-shm
/var/db/powerlog/Library/BatteryLife/Archives/powerlog_2023-07-12_5CA67A31.PLSQL-shm
/var/db/powerlog/Library/BatteryLife/Archives/powerlog_2023-07-13_D83C3E6E.PLSQL-shm
/var/db/powerlog/Library/BatteryLife/Archives/powerlog_2023-07-14_59EF6E54.PLSQL-shm
```

Files With Modified Attributes

```
/private/var/db/powerlog/Library/PerfPowerTelemetry/MetadataReports/MetadataStore
```

Files Dropped

```
+ /Users/maria/Library/Caches/com.apple.ap.adprivacyd/fsCachedData/854F653F-BD5F-4B7C-9E6D-7F7E3F1F6B90.tmp
+ /assets/getmediaplayerpro_1496803053/images/mediaplayerpromac.zip
+ /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/NSCreateObjectFileImageFromMemory-DxzxfYTC
+ /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/mediaplayerpromac.zip
```

Process and service actions

Processes Created

```
/Volumes/Installer/Installer.app/Contents/MacOS/Asclepiadaceae
/bin/bash /bin/sh -c codesign -dvv '$BUNDLE_PATH' 2>&1 | grep -a 'Authority=Developer ID Application:' | xargs echo -n
/bin/bash /bin/sh -c ioreg -l | grep -e 'USB Vendor Name'
/bin/echo -
/usr/bin/codesign codesign -dvv /Volumes/Installer/Installer.app
/usr/bin/grep grep -a Authority=Developer ID Application:
/usr/bin/grep grep -e USB Vendor Name
/usr/bin/hdiutil -
/usr/bin/open /Volumes/Installer/Installer.app
/usr/bin/xargs xargs echo -n
```

Shell Commands

```
/bin/sh -c codesign -dvv '$BUNDLE_PATH' 2>&1 | grep -a 'Authority=Developer ID Application:' | xargs echo -n
/bin/sh -c ioreg -l | grep -e 'USB Vendor Name'
/usr/bin/open /Volumes/Installer/Installer.app
codesign -dvv /Volumes/Installer/Installer.app
grep -a Authority=Developer ID Application:
grep -e USB Vendor Name
ioreg -l
xargs echo -n
```

Processes Tree

```
832 - /usr/libexec/adprivacyd
833 - /usr/bin/open /Volumes/Installer/Installer.app
836 - /Volumes/Installer/Installer.app/Contents/MacOS/Asclepiadaceae
```

```
↳ 840 - /bin/bash /bin/sh -c ioreg -l | grep -e 'USB Vendor Name'
  ↳ 841 - /usr/sbin/ioreg ioreg -l
  ↳ 842 - /usr/bin/grep grep -e USB Vendor Name
↳ 843 - /bin/bash /bin/sh -c codesign -dvv '$BUNDLE_PATH' 2>&1 | grep -a 'Authority=Developer ID Application:' | xargs echo -n
  ↳ 844 - /usr/bin/codesign codesign -dvv /Volumes/Installer/Installer.app
```

Highlighted actions

Highlighted Text

""