03b71eaceadea05bc0eea5cddecaa05f245126d6b16cfcd0f3ba0442ac58dab3

Sign in Sign up

20
/ 65

Community Score -43

20/65 security vendors flagged this file as malicious

Reanalyze Similar More

03b71eaceadea05bc0eea5cddecaa05f245126d6b16cfcd0f...
MarkMakingBot.dmg
dmg

Size
13.05 MB

Last Analysis Date
2 months ago

DMG

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 9

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...	⚠ 1	0	0	0	1	5
☑ VirusTotal...	⚠ 0	0	0	0	13	5

Activity Summary

Download Artifacts Full Reports Help

Detections
1 EVADER

Mitre Signatures
NOT FOUND

IDS Rules
NOT FOUND

Sigma Rules
NOT FOUND

Dropped Files
1 OTHER 1 MACH_O 1 PKG

Network comms
1 HTTP 2 DNS 6 IP

Dynamic Analysis Sandbox Detections

⚠ The sandbox OS X Sandbox flags this file as: EVADER

Network Communication

HTTP Requests

+ POST http://95.213.232.170/ProbActive/index.do

DNS Resolutions

+ a1441.g4.akamai.net

+ radarsubmissions.apple.com.akadns.net

IP Traffic

TCP 23.62.236.178:80 (a1441.g4.akamai.net)
TCP 17.253.27.202:80
TCP 23.219.38.25:443
TCP 95.213.232.170:80
TCP 17.248.136.76:443
TCP 184.28.21.97:80

File system actions

- /Applications
- /Library/Application Support/CrashReporter/SubmitDiagInfo.domains
- /Library/Caches/com.apple.iconservices.store/E7F098B0-E781-6BEA-A8E4-0E1CFB55133B.isdata
- /Library/Filesystems
- /Library/Filesystems/vmhgfs.fs
- /Library/Filesystems/vmhgfs.fs/Contents
- /Library/Filesystems/vmhgfs.fs/Contents/Resources
- /Library/Filesystems/vmhgfs.fs/Contents/Resources/Base.lproj
- /Library/Filesystems/vmhgfs.fs/Contents/Resources/en.lproj
- /Library/Keychains/SupplementalsAssets/AnalyticsSamplingRates.plist

Files Written

- /private/var/db/.dat.nosync0272.rkHbWG
- /private/var/folders/7d/7skpstwd7qnctfwpwp7225xw0000gn/C/mds/mdsDirectory.db_
- /private/var/folders/7d/7skpstwd7qnctfwpwp7225xw0000gn/C/mds/mdsObject.db_
- /Library/Preferences/com.apple.networkextension.cache.plist-lock
- /Library/Preferences/com.apple.networkextension.cache.plist-new
- /Library/Receipts/InstallHistory.plist
- /Users/user1/Library/Caches/.dat.nosync0159.vFYJhB
- /Users/user1/Library/Caches/com.apple.cache_delete/CacheDeleteAnalytics.plist
- /Users/user1/Library/Caches/com.apple.cache_delete/CacheDeleteRecentInfo_v2
- /private/var/run/.dat.nosync116b.iyr0qK

Files Deleted

- /var/db/.InstallerTMExcludes.plist
- /var/folders/7d/7skpstwd7qnctfwpwp7225xw0000gn/C//mds/mdsObject.db
- /var/folders/7d/7skpstwd7qnctfwpwp7225xw0000gn/T//Install.61579YPX6
- /var/folders/7d/7skpstwd7qnctfwpwp7225xw0000gn/T//Install.61579YPX6/Receipts

Files Copied

- /Applications/QtBitcoinTrader.app/Contents/Resources/.com.pkgtrader.plist
- /Library/Preferences/com.apple.networkextension.cache.plist-new
- /Users/user1/Library/Caches/.dat.nosync0159.vFYJhB
- /private/var/run/.dat.nosync116b.iyr0qK
- /var/db/.dat.nosync1178.6vlyDl
- /var/folders/4c/2j7t8wj96cngjk55x3sm1t2c0000gn/C//mds/mdsDirectory.db_
- /var/folders/4c/2j7t8wj96cngjk55x3sm1t2c0000gn/C//mds/mdsObject.db_
- /var/folders/4c/2j7t8wj96cngjk55x3sm1t2c0000gn/C/com.apple.MediaLibraryService//mds/mdsDirectory.db_
- /var/folders/4c/2j7t8wj96cngjk55x3sm1t2c0000gn/C/com.apple.MediaLibraryService//mds/mdsObject.db_
- /var/folders/4c/2j7t8wj96cngjk55x3sm1t2c0000gn/C/com.apple.trustd//mds/mdsDirectory.db_

Files Dropped

- /private/var/db/.dat.nosync0272.rkHbWG
- /Library/Application Support/iLifeMediaBrowser/Plug-Ins/iLMBiPhotoPlugin.ilmbplugin/Contents/MacOS/iLMBiPhotoPlugin
- /Library/Frameworks/iTunesLibrary.framework/Versions/A/iTunesLibrary
- /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/LaunchServices.framework/LaunchServices
- /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/Metadata.framework/Metadata
- /System/Library/Frameworks/GSS.framework/GSS
- /System/Library/Frameworks/Security.framework/Security

+ /System/Library/PrivateFrameworks/Heimdal.framework/Heimdal

Process and service actions

Processes Created

- /Applications/QtBitcoinTrader.app/Contents/Resources/.loader
- /System/Library/CoreServices/Installer.app/Contents/MacOS/Installer
- /System/Library/PrivateFrameworks/PackageKit.framework/Resources/efw_cache_update
- /System/Library/PrivateFrameworks/PackageKit.framework/Resources/install_monitor
- /System/Library/PrivateFrameworks/PackageKit.framework/Resources/shove
- /bin/mv
- /tmp/PKInstallSandbox.0wp1Pj/Scripts/com.bitcointraderpkg.BitcoinTrader.05SEZD/postinstall
- /usr/bin/sw_vers
- /usr/bin/whoami
- /usr/libexec/apfsd