16bafdf741e7a13137c489f3c8db1334f171c7cb13b62617d691b0a64783cc48

Sign in Sign up

20 / 58

Community Score

20/58 security vendors flagged this file as malicious

Reanalyze Similar More

16bafdf741e7a13137c489f3c8db1334f171c7cb13b62617…

org.hworkout.OnlineWorkout

dmg checks-hostname contains-macho signed

Size 503.40 KB

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 6 0 5 9 30

VirusTotal… 0 0 0 0 0 2 8

Activity Summary Download Artifacts Full Reports Help

Detections
NOT FOUND

Mitre Signatures
4 LOW 23 INFO

IDS Rules
NOT FOUND

Sigma Rules
1 HIGH 1 MEDIUM 3 LOW

Dropped Files
1 ZIP 1 XML 1 MACH_O 1 TEXT 1 APPLE_PLIST 1 JAVASCRIPT 2 OTHER

Network comms
12 DNS 23 IP 3 JA3

Behavior Tags

checks-hostname

MITRE ATT&CK Tactics and Techniques

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

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 1 MEDIUM 1 LOW 3

Matches rule Potentially Suspicious Execution From Tmp Folder by Joseliyo Sanchez, @Joseliyo_Jstnk at Sigma Integrated Rule Set (GitHub)
↳ *Detects a potentially suspicious execution of a process located in the '/tmp/' folder*

Matches rule Execution Of Script Located In Potentially Suspicious Directory by Joseliyo Sanchez, @Joseliyo_Jstnk at Sigma Integrated Rule Set (GitHub)
↳ *Detects executions of scripts located in potentially suspicious locations such as "/tmp" via a shell such as "bash", "sh", etc.*

Matches rule Decode Base64 Encoded Text -MacOs by Daniil Yugoslavskiy, oscd.community at Sigma Integrated Rule Set (GitHub)
↳ *Detects usage of base64 utility to decode arbitrary base64-encoded text*

Matches rule Startup Items by Alejandro Ortuno, oscd.community at Sigma Integrated Rule Set (GitHub)
↳ *Detects creation of startup item plist files that automatically get executed at boot initialization to establish persistence.*

See all

Network Communication

DNS Resolutions

_aaplcache._tcp.local
_aaplcache1._tcp.local
_aaplcache2._tcp.local
_aaplcache3._tcp.local
_aaplcache4._tcp.local

IP Traffic

TCP 104.76.210.92:443
TCP 104.71.143.208:443
TCP 184.31.52.187:443
TCP 104.76.210.80:443
TCP 184.31.53.176:443
TCP 17.248.195.73:443
TCP 17.248.200.64:443 (mask-api.icloud.com)
TCP 44.232.224.125:443 (pubingress-feedback-1a6fe9caff1148fe.elb.us-west-2.amazonaws.com)
TCP 184.25.164.143:443
TCP 17.57.172.5:443

JA3 Digests

773906b0efdefa24a7f2b8eb6985bf37
1d9437ff1aa1e958ed34a0fb0313f206
656b9a2f4de6ed4909e157482860ab3d

TLS

lcdn-locator.apple.com
gsa.apple.com

Behavior Similarity Hashes

OS X Sandbox	960b49a32d5b030e0ef0b41c24f14c6e
VirusTotal Box of Apples	2e8191ee3adc954f51712607fd9ec56f

File system actions

Files Opened

/Library/Application Support/CrashReporter/DiagnosticMessagesHistory.plist
/Library/Application Support/CrashReporter/SubmitDiagInfo.domains
/Library/Preferences/com.apple.networkd.plist
/Library/Preferences/com.apple.networkextension.uuidcache.plist
/System/Library/CoreServices/.SystemVersionPlatform.plist
/System/Library/CoreServices/CoreTypes.bundle/Contents/Library/InternalAppExceptions.bundle/Contents/Resources/Exceptions.plist
/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/Exceptions.plist

Files Written

/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE.zip
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Info.plist
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/MacOS/downloader
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/PkgInfo
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/AppIcon.icns
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/Assets.car
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/Base.lproj/MainMenu.nib
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/README.md
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/paramsJson.json
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/_CodeSignature/CodeResources

Files Deleted

/Users/maria/Library/Caches/com.apple.remindd/fsCachedData_remove
/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/.LINKS/B53AF0F1-BB93-418E-A0C4-5AA419020840
/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/.LINKS/DAF55ED4-0EA2-4D29-B837-72F92A13EBAA
/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/tmpsqlitetruncatedbTgYaaU
/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/tmpsqlitetruncatedbTgYaaU-journal

Files Copied

+ /var/folders/_2/f1dk13r15vgb7756v1t3kfb40000gn/C//mds/mdsDirectory.db_
+ /var/folders/_2/f1dk13r15vgb7756v1t3kfb40000gn/C//mds/mdsObject.db_
+ /var/folders/zz/zyxvpxvq6csfxvn_n00000b400002s/T/com.apple.trustd/TemporaryItems/NSIRD_trustd_7N7ErO/PriorMitmRoots.plist

Files With Modified Attributes

/Users/maria/Library/Caches/com.apple.remindd/RemoteConfiguration.plist
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Info.plist
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/MacOS/downloader
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/PkgInfo
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/AppIcon.icns
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/Assets.car
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/Base.lproj/MainMenu.nib
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/README.md
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/paramsJson.json
/private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/_CodeSignature/CodeResources

Files Dropped

+ /private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE.zip
+ /private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Info.plist
+ /private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/MacOS/downloader
+ /private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/PkgInfo
+ /private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/Base.lproj/MainMenu.nib
+ /private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/README.md
+ /private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/Resources/paramsJson.json
+ /private/tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/_CodeSignature/CodeResources
+ /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/TemporaryItems/NSIRD_remindd_x8sgP2/RemoteConfiguration.plist
+ /System/Library/Frameworks/Security.framework/Versions/A/PlugIns/csparser.bundle/Contents/MacOS/csparser

Process and service actions

Processes Created

- /Volumes/Installer/Installer.app/Contents/MacOS/OnlineWorkout
- /bin/bash sh -c tail -c +21453 '/Volumes/Installer/Installer.app/Contents/Resources/workout-logo.jpeg' | base64 --decode > /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE.zip
- /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/MacOS/downloader
- /usr/bin/base64 base64 --decode
- /usr/bin/hdiutil -
- /usr/bin/killall killall -e Terminal
- /usr/bin/open /Volumes/Installer/Installer.app
- /usr/bin/tail tail -c +21453 /Volumes/Installer/Installer.app/Contents/Resources/workout-logo.jpeg
- /usr/bin/unzip unzip /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE.zip -d /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE
- /usr/libexec/firmwarecheckers/eficheck/eficheck --integrity-check-daemon

Shell Commands

- /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/MacOS/downloader
- /usr/bin/open /Volumes/Installer/Installer.app
- base64 --decode
- ioreg -rd1 -w0 -c AppleAHCIDiskDriver
- killall -e Terminal
- sh -c /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/MacOS/downloader
- sh -c killall -e Terminal
- sh -c tail -c +21453 '/Volumes/Installer/Installer.app/Contents/Resources/workout-logo.jpeg' | base64 --decode > /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE.zip
- sh -c unzip /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE.zip -d /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE
- tail -c +21453 /Volumes/Installer/Installer.app/Contents/Resources/workout-logo.jpeg

Processes Tree

- 983 - /usr/bin/open /Volumes/Installer/Installer.app
- 984 - /Volumes/Installer/Installer.app/Contents/MacOS/OnlineWorkout
  - ↳ 985 - /bin/bash sh -c tail -c +21453 '/Volumes/Installer/Installer.app/Contents/Resources/workout-logo.jpeg' | base64 --decode > /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE.zip
  - ↳ 986 - /usr/bin/tail tail -c +21453 /Volumes/Installer/Installer.app/Contents/Resources/workout-logo.jpeg
  - ↳ 987 - /usr/bin/base64 base64 --decode
  - ↳ 988 - /usr/bin/unzip unzip /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE.zip -d /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE
  - ↳ 989 - /tmp/54A0A2CD-FAD1-4D4D-AAF5-5266F6344ABE/downloader.app/Contents/MacOS/downloader
    - ↳ 990 - /usr/bin/hdiutil -
    - ↳ 991 - /usr/bin/hdiutil -
    - ↳ 992 - /usr/sbin/ioreg ioreg -rd1 -w0 -c AppleAHCIDiskDriver

Highlighted actions

Highlighted Text

- ""

Sign in Sign up

Our product

Contact Us
Get Support
How It Works
ToS | Privacy Notice
Blog | Releases

Community

Join Community
Vote and Comment
Contributors
Top Users
Community Buzz

Tools

API Scripts
YARA
Desktop Apps
Browser Extensions
Mobile App

Premium Services

Get a demo
Intelligence
Hunting
Graph
API v3 | v2

Documentation

Searching
Reports
API v3 | v2
Use Cases