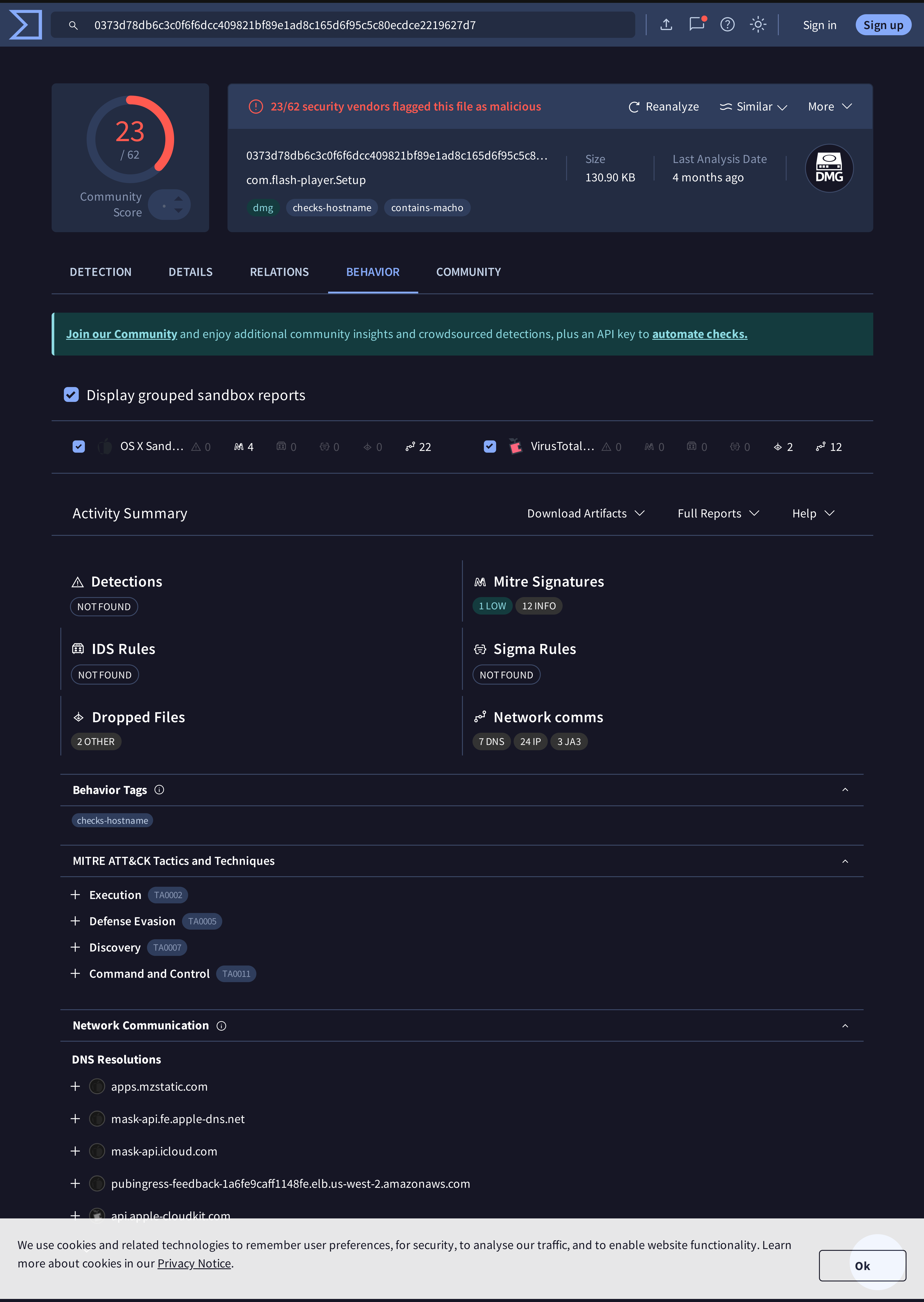
0373d78db6c3c0f6f6dcc409821bf89e1ad8c165d6f95c5c80ecdce2219627d7
Sign in
Sign up

23
/ 62
Community Score

23/62 security vendors flagged this file as malicious

0373d78db6c3c0f6f6dcc409821bf89e1ad8c165d6f95c5c8...
com.flash-player.Setup

dmg checks-hostname contains-macho

Size
130.90 KB

Last Analysis Date
4 months ago

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 4 0 0 0 22

☑ VirusTotal... ⚠ 0 0 0 0 2 12

Activity Summary

⚠ Detections
NOT FOUND

Mitre Signatures
1 LOW 12 INFO

IDS Rules
NOT FOUND

Sigma Rules
NOT FOUND

Dropped Files
2 OTHER

Network comms
7 DNS 24 IP 3 JA3

Behavior Tags ⓘ

checks-hostname

MITRE ATT&CK Tactics and Techniques

+ Execution TA0002
+ Defense Evasion TA0005
+ Discovery TA0007
+ Command and Control TA0011

Network Communication ⓘ

DNS Resolutions

+ apps.mzstatic.com
+ mask-api.fe.apple-dns.net
+ mask-api.icloud.com
+ pubingress-feedback-1a6fe9caff1148fe.elb.us-west-2.amazonaws.com
+ api.apple-cloudkit.com

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.

TCP 96.16.55.147:443
TCP 17.248.193.19:443 (mask-api.icloud.com)
TCP 23.60.64.27:443
TCP 17.157.64.66:443
TCP 23.60.64.175:443
TCP 23.72.90.11:443
TCP 23.60.64.179:443
TCP 192.229.211.108:80
TCP 17.253.83.200:443

JA3 Digests

773906b0efdefa24a7f2b8eb6985bf37
1d9437ff1aa1e958ed34a0fb0313f206
656b9a2f4de6ed4909e157482860ab3d

TLS

sandbox.itunes.apple.com

Behavior Similarity Hashes

OS X Sandbox	a35007b1c789596712bb12336e5560ef
VirusTotal Box of Apples	88f4923202889d7be92bf195e3c26e7d

File system actions

Files Opened

/Library/Application Support/CrashReporter/SubmitDiagInfo.domains
/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
/System/Library/CoreServices/CoreTypes.bundle/Contents/Resources/Exceptions.plist
/System/Library/CoreServices/ServerVersion.plist
/System/Library/CoreServices/SystemVersion.bundle
/System/Library/CoreServices/SystemVersion.bundle//Base.lproj
/System/Library/CoreServices/SystemVersion.bundle//English.lproj
/System/Library/CoreServices/SystemVersion.bundle/English.lproj

Files Written

/var/db/analyticsd/aggregate_persist_temp

Files Copied

/var/db/analyticsd/aggregate_persist_temp
/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_wMZgi5/PriorMitmRoots.plist

Files Dropped

/System/Library/Frameworks/Security.framework/Versions/A/PlugIns/csparser.bundle/Contents/MacOS/csparser
/Volumes/Player/Player_10712.app/Contents/MacOS/Setup

Process and service actions

```
/Volumes/Player/Player_10712.app/Contents/MacOS/Setup
/bin/bash /bin/sh -c ioreg -l | grep -e 'VirtualBox' -e 'Oracle' -e 'VMware' -e 'Parallels' | wc -l
/usr/bin/grep grep -e VirtualBox -e Oracle -e VMware -e Parallels
/usr/bin/open /Volumes/Player/Player_10712.app
/usr/bin/wc wc -l
/usr/sbin/ioreg ioreg -l
```

Shell Commands

```
/bin/sh -c ioreg -l | grep -e 'VirtualBox' -e 'Oracle' -e 'VMware' -e 'Parallels' | wc -l
/usr/bin/open /Volumes/Player/Player_10712.app
grep -e VirtualBox -e Oracle -e VMware -e Parallels
ioreg -l
wc -l
```

Processes Tree

```
866 - /usr/bin/open /Volumes/Player/Player_10712.app
868 - /Volumes/Player/Player_10712.app/Contents/MacOS/Setup
  ↳ 869 - /bin/bash /bin/sh -c ioreg -l | grep -e 'VirtualBox' -e 'Oracle' -e 'VMware' -e 'Parallels' | wc -l
    ↳ 870 - /usr/sbin/ioreg ioreg -l
    ↳ 871 - /usr/bin/grep grep -e VirtualBox -e Oracle -e VMware -e Parallels
    ↳ 872 - /usr/bin/wc wc -l
```

Highlighted actions ⓘ

Highlighted Text

""