URL, IP address, domain, or file hash

Al Dia

14
/ 60

Community Score

14 security vendors and no sandboxes flagged this file as malicious

1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c

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

dmg contains-macho checks-hostname

730.99 KB
Size

2023-02-17 13:25:31 UTC
1 hour ago

DMG

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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…
BitDefender	Gen:Variant.Adware.…	Emsisoft	Gen:Variant.Adware.…
eScan	Gen:Variant.Adware.…	GData	Gen:Variant.Adware.…
Kaspersky	Not-a-virus:HEUR:A…	MAX	Malware (ai Score=83)
Sophos	Bundlore (PUA)	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	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefenderTheta	Undetected
Bkav Pro	Undetected	ClamAV	Undetected
CMC	Undetected	Cynet	Undetected
Cyren	Undetected	DrWeb	Undetected
ESET-NOD32	Undetected	F-Secure	Undetected
Fortinet	Undetected	Google	Undetected
Gridinsoft (no cloud)	Undetected	Ikarus	Undetected
Jiangmin	Undetected	K7AntiVirus	Undetected
K7GW	Undetected	Kingsoft	Undetected
Lionic	Undetected	Malwarebytes	Undetected
MaxSecure	Undetected	McAfee	Undetected
McAfee-GW-Edition	Undetected	Microsoft	Undetected
NANO-Antivirus	Undetected	Panda	Undetected
QuickHeal	Undetected	Rising	Undetected
Sangfor Engine Zero	Undetected	SUPERAntiSpyware	Undetected
Symantec	Undetected	TACHYON	Undetected

Symantec	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…		

URL, IP address, domain, or file hash

Al Dia

14
/ 60

Community Score

14 security vendors and no sandboxes flagged this file as malicious

1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c

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

dmg contains-macho checks-hostname

730.99 KB
Size

2023-02-17 13:25:31 UTC
1 hour ago

DMG

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Basic properties

MD5	3fad2dbe37e011cd95fdcb931b903d14
SHA-1	13720d595ac34fd31f0d5c3b09088f5753b053cf
SHA-256	1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c
Vhash	994d89ff972c1ff917143b8782143df8
SSDEEP	12288:hubD4cC55OORtjtKSrCzfwhxMx4xwh1yh3j2Okojg86VmIff+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	2023-02-17 13:44:36 UTC
Last Analysis	2023-02-17 13:25:31 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

URL, IP address, domain, or file hash

Al Dia

14
/ 60

Community Score

14 security vendors and no sandboxes flagged this file as malicious

1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c

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

dmg contains-macho checks-hostname

730.99 KB
Size

2023-02-17 13:25:31 UTC
1 hour ago

DMG

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Contacted Domains (1)

Domain	Detections	Created	Registrar
gateway.fe.apple-dns.net	0 / 88	2014-05-28	CSC CORPORATE DOMAINS, INC.

Contacted IP addresses (16)

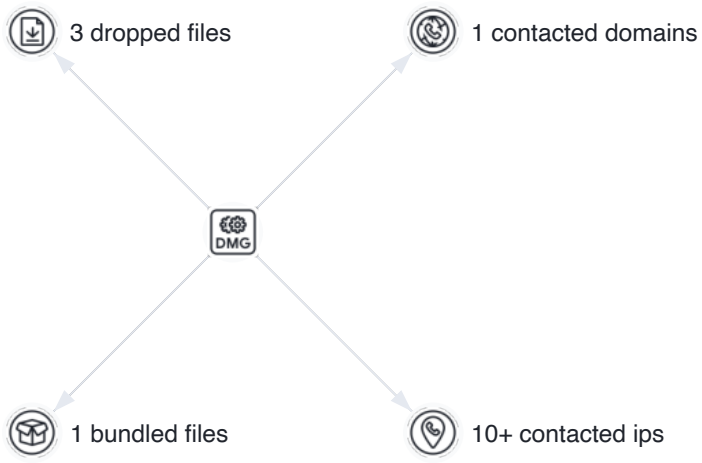
IP	Detections	Autonomous System	Country
104.73.64.163	0 / 88	16625	US
17.248.185.201	0 / 88	714	US
17.248.185.238	0 / 87	714	US
17.248.241.12	0 / 87	714	US
17.248.241.17	0 / 87	714	US
17.248.241.208	0 / 88	714	US
17.248.241.209	0 / 88	714	US

17.248.241.243	0 / 88	714	US
17.248.241.40	0 / 87	714	US
17.248.241.47	0 / 87	714	US

Bundled Files (1)

Scanned	Detections	File type	Name
2023-02-17	19 / 62	Mach-O	/Skim's PDF

Graph Summary



14
/ 60

Community Score

14 security vendors and no sandboxes flagged this file as malicious

1f4426963f8914118abeb1bdd639edcbbb969c85ba7bbfa0e728646df45a0b1c

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

dmg contains-macho checks-hostname

730.99 KB
Size

2023-02-17 13:25:31 UTC
1 hour ago

DMG

URL, IP address, domain, or file hash

AI Dia

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections.

Display grouped sandbox reports

0 4 0 0 4 11

Activity Summary Download Artifacts Full Reports Help

⚠ Detections	Mitre Signatures	IDS Rules	Sigma Rules	Dropped Files	Network comms
NOT FOUND	3 LOW 10 INFO	NOT FOUND	NOT FOUND	1 TEXT	1 DNS 9 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

+ 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)
67.195.204.56:443 (TCP)
72.21.91.29:80 (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

+ /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