

Max size 650MB

8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698

8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698

8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698.dmg

Size
742.87 KB

Last Analysis Date
a moment ago

DMG

Community Score

dmg contains-macho

Sign in Sign up

Search

Favourites

All

Accessories

Administration

Games

Graphics

Internet

Office

Pentesting

Preferences

Privacy

Programming

Sound & Video

System Services

System Tools

Universal Access

Control Center

Menu

COMMUNITY

Sorry, no items found

and crowdsourced detections, plus an API key to [automate checks.](#)

Family labels misc

Do you want to automate checks?

[Misc]	AVG	⚠️ MacOS:MalwareX-gen [Misc]
X.Amos.ak	Microsoft	⚠️ Program:Script/Wacapew.AIml
	Acronis (Static ML)	✅ Undetected
	AliCloud	✅ Undetected
	Antiy-AVL	✅ Undetected
	Avira (no cloud)	✅ Undetected
	BitDefender	✅ Undetected

ApplicationsPlacesSystem

Mon Apr 21, 18:08

MalwareBazaar | DownloadVirusTotal - File - 8e0964

https://www.virustotal.com/gui/file/8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698?nocache=1

Import bookmarks...Parrot OSHack The BoxOSINT ServicesVuln DBPrivacy and SecurityLearning Resources

Max size 650MB

8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698

Sign inSign up

/ 61

Community Score

8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698

8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698.dmg

Size742.87 KB

Last Analysis Datea moment ago

DMG

DETECTIONDETAILSRELATIONSBEHAVIORCOMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label ⓘ miscFamily labels misc

Security vendors' analysis ⓘDo you want to automate checks?

Avast	ⓘ MacOS:MalwareX-gen [Misc]	AVG	ⓘ MacOS:MalwareX-gen [Misc]
Kaspersky	ⓘ HEUR:Trojan-PSW.OSX.Amos.ak	Microsoft	ⓘ Program:Script/Wacapew.AIml
Sophos	ⓘ OSX/InfoStl-EQ	Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected	AliCloud	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Avira (no cloud)	✓ Undetected
Baidu	✓ Undetected	BitDefender	✓ Undetected

MenuVirusTotal - File - 8e0...

123

ApplicationsPlacesSystem

Mon Apr 21, 18:09

MalwareBazaar | Download

VirusTotal - File - 8e0964

https://www.virustotal.com/gui/file/8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698/details

Import bookmarks...Parrot OSHack The BoxOSINT ServicesVuln DBPrivacy and SecurityLearning Resources

8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698

Sign inSign up

Basic properties ⓘ

MD52b71f93006c82496af73e275f6acddf8

SHA-1647c919fbdd65648e618905078dad3f9e3511f5b

SHA-2568e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698

Vhash994d89ff972c1ff917143b8782143df8

SSDEEP12288:TaGwWPOJaGwOdRydq4P8YfMJJa12FnEjmr2XnRtk6GisS9AK8+0TBdZfme9nEabT:WGwsOkGwgwo49MckFYnRGK9AK8T1PfBN

TLSHT15BF4237BE91CB848ED95A1F54430D74C0ECF2BC3497142EBB07A1E7D3D9AB19E81A096

File typeMacintosh Disk Imageexecutablemacdmg

MagicDOS/MBR boot sector, extended partition table (last) (zlib compressed data)

TrIDMacintosh Disk image (BZlib compressed) (97.6%) | ZLIB compressed data (best comp.) (2.3%)

MagikaDMG

File size742.87 KB (760700 bytes)

History ⓘ

First Submission2025-04-21 18:03:22 UTC

Last Submission2025-04-21 18:03:22 UTC

Last Analysis2025-04-21 18:03:22 UTC

Names ⓘ

8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698.dmg

DMG info ⓘ

XML Property List Entries

ID:0

RISKY Table

Menu

VirusTotal - File - 8e0...

123

Names ⓘ

8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698.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	751862
XML Length	8326
XML Offset	751862
PLST Keys	resource-fork



ApplicationsPlacesSystem

Mon Apr 21, 18:09

MalwareBazaar | Download

VirusTotal - File - 8e0964

https://www.virustotal.com/gui/file/8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698/behavior

Import bookmarks...Parrot OSHack The BoxOSINT ServicesVuln DBPrivacy and SecurityLearning Resources

8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698

Sign inSign up

There are some sandboxes still analysing the file.

Activity Summary

Download ArtifactsFull ReportsHelp

Detections

NOT FOUND

Mitre Signatures

NOT FOUND

IDS Rules

NOT FOUND

Sigma Rules

NOT FOUND

Dropped Files

2 OTHER

Network comms

4 HTTP5 DNS6 IP2 JA3

Network Communication

HTTP Requests

GET http://ocsp.comodoca.com/MFcwVaADAgEAME4wTDBKMAkGBSsOAwlaBQAEFOsl2JD%2BJyD0HX1qwV7vds9iz6t4BBR1cacZSBm8nZ3qQUfflMRId5nTeQIRAJjBcnaqg2kl3NxbTvi9QXQ%3D

GET http://ocsp.comodoca.com/MFcwVaADAgEAME4wTDBKMAkGBSsOAwlaBQAEFOsl2JD+JyD0HX1qwV7vds9iz6t4BBR1cacZSBm8nZ3qQUfflMRId5nTeQIRAJjBcnaqg2kl3NxbTvi9QXQ= 200

GET http://ocsp.usertrust.com/MFYwVKADAgEAME0wSzBJMAkGBSsOAwlaBQAEFM0w0kw0OoKrHwVwFYrXoQd2KZLpBBRTeb9aqitKz1SA4dibwJ3ysgNmywIQXfq7lXfPq2cfx93%2B0c8gWw%3D%3D

GET http://ocsp.usertrust.com/MFYwVKADAgEAME0wSzBJMAkGBSsOAwlaBQAEFM0w0kw0OoKrHwVwFYrXoQd2KZLpBBRTeb9aqitKz1SA4dibwJ3ysgNmywIQXfq7lXfPq2cfx93+0c8gWw== 200

DNS Resolutions

api.apple-cloudkit.com

apple-finance.query.yahoo.com

ocsp.comodoca.com

ocsp.comodoca.com.cdn.cloudflare.net

Menu

VirusTotal - File - 8e0...

ApplicationsPlacesSystem

Mon Apr 21, 18:09

MalwareBazaar | Download

VirusTotal - File - 8e0964

https://www.virustotal.com/gui/file/8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698/behavior

Import bookmarks...Parrot OSHack The BoxOSINT ServicesVuln DBPrivacy and SecurityLearning Resources

8e09641a82bc73f7a36cdd4fc317b30afa8c63be904626b126e9aceb85a46698

Sign inSign up

Activity Summary

Download ArtifactsFull ReportsHelp

+ ocsp.comodoca.com.cdn.cloudflare.net

+ ocsp.usertrust.com

IP Traffic

UDP 8.8.8.8:53

TCP 104.18.38.233:80 (ocsp.usertrust.com)

UDP 255.255.255.255:67

TCP 172.64.149.23:80 (ocsp.usertrust.com)

TCP 96.6.230.21:443

TCP 67.195.228.56:443 (apple-finance.query.yahoo.com)

JA3 Digests

1d9437ff1aa1e958ed34a0fb0313f206

656b9a2f4de6ed4909e157482860ab3d

Behavior Similarity Hashes

VirusTotal Box of Apples72b8adfe80a802ef2ede1bfda05a545f

File system actions

Files Dropped

+ /Volumes/WeChat/.WeChat

+ /Volumes/WeChat/WeChat.msB

Menu

VirusTotal - File - 8e0...

123

```

GROUPS Visit: https://www.trustedsec.com

Earth Lusca
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


Ember Bear

Select from the menu:
1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

set>

```

ID: G1006

 Associated Groups: TAG-22,
Charcoal Typhoon, CHROMIUM,
ControlX

Version: 2.0

Created: 01 July 2022

Last Modified: 16 September 2024

Version Permalink

Associated Group Descriptions

Name	Description
TAG-22	[2]

`set> 1` ATT&CKcon 6.0 returns October 14-15, 2025 in McLean, VA. More details about tickets and our CFP can be found [here](#)

The Spearphishing module allows you to specially craft email messages and send them to a large (or small) number of people with attached fileformat malicious payloads. If you want to spoof your email address, be sure "Sendmail" is installed (apt-get install sendmail) and change the config/set_config SENDMAIL=OF

<p>Earth Lusca is a suspected China-based cyber espionage group that has been active since at least April 2019. Earth Lusca has targeted organizations in Australia, China, Hong Kong,</p>	<p>ID: G1006</p>
--	------------------

Equation

There are two options, one is getting your feet wet and letting SET do everything for you (option 1), the second is to create your own FileFormat payload and use it in your own attack. Either way, good luck and enjoy!

Evilnum

Mongolia, Nepal, the Philippines, Taiwan, Thailand, Vietnam, the United Arab Emirates, Nigeria, Germany, France, and the United States. Targets included government institutions, news media outlets, gambling companies, educational institutions, COVID-19 research organizations,

Associated Groups: TAG-22, Charcoal Typhoon, CHROMIUM, ControlX

Version: 2.0

- | | |
|--|---|
| Ferocious Kitten
1) Perform a Mass Email Attack
2) Create a FileFormatPayload
3) Create a Social-Engineering Template | Created: 01 July 2022
Last Modified: 16 September 2024 |
|--|---|

99) Return to Main Menu

```
set:phishing>
```

FIN7	Associated Group Descriptions
------	-------------------------------

FIN8	Name	Description
Fox Kitten		
GALLIUM	TAG-22	[2]

ApplicationsPlacesSystem

MATE Terminal

Use the command line

Parrot Terminal

FileEditViewSearchTerminalHelp

utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow /fast.

ATT&CKcon 6.0 returns October 14-15, 2025 in McLean, VA. More details about tickets and our CFP can be found [here](#)

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method

2) Metasploit Browser Exploit Method

3) Credential Harvester Attack Method

4) Tabnabbing Attack Method

5) Web Jacking Attack Method

6) Multi-Attack Web Method

7) HTA Attack Method

99) Return to Main Menu

set:webattack>

Earth Lusca

Earth Lusca has targeted organizations in Australia, China, Hong Kong, Mongolia, Nepal, the Philippines, Taiwan, Thailand, Vietnam, the United Arab Emirates, Nigeria, Germany, France, and the United States. Targets included government institutions, news media outlets, gambling companies, educational institutions, COVID-19 research organizations, telecommunications companies, religious movements banned in China, and cryptocurrency forms; security researchers assess some Earth Lusca operations may be self motivated.

Earth Lusca has used malware commonly used by other Chinese threat groups, including T41 and the Winnti Group cluster, however security researchers assess Earth Lusca's techniques and infrastructure are separate.

Learning Resources

DefensesCTIResourcesBenefactorsBlog

Search

ID: G1006

Associated Groups: TAG-22, Charcoal Typhoon, CHROMIUM, ControlX

Version: 2.0

Created: 01 July 2022

Last Modified: 16 September 2024

Version Permalink

Associated Group Descriptions

Name	Description
TAG-22	[2]

MenuEarth Lusca, TAG-22, ...mobile-attack-v16.1-g...Parrot Terminal

123

192.168.64.2 - - [21/Apr/2025 18:52:09] "POST /ServiceLoginAuth HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLckfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDh
tUFdlldzBENhIfVwsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%99APsBz4gAAAAUy4_
qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=myemail@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=password
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

192.168.64.2 - - [21/Apr/2025 18:52:47] "POST /ServiceLoginAuth HTTP/1.1" 302 -

Google

Gmail Images Sign in

Google Search I'm Feeling Lucky

Level up your smartphone game with the new Google Pixel 9a: big on AI, small on price