Recorded Future®
Triage

Report Analysis Logs

General

Target
caido

Size
95MB

MD5
0f6c73e6b0176fb7375a2348c9b5ef20

SHA1
0fd582ed76284277f7a82d095b8b0d009ce3ed5b

SHA256
65954b0f35bcedb1a3388b4b9244a973f56b0f58815610cda19f8ba4ebe4416f

SHA512
011795e6e359d2d260e2c28657414f909b9e4579cf2efd987943bab9005d57bf544a8717b17b9d73fdc41aca0035fb0489a68d62d791af9d046671265923ef3c

SSDEEP
393216:5YgSodBrkkGX3g7nMXqUfnBNVvCk8d/r9X915hEdejqwZpusLcFSiWJxulNn+6Ud:5zFdBkgzMxPtvCk0/Rn5hy86UZ

Score

7/10

ANTIVM

Signatures

Changes its process name 11 IoCs

Checks CPU configuration 1 TTPs 1 IoCs
Checks CPU information which indicate if the system is a virtual machine.

ANTIVM

Reads runtime system information 3 IoCs

Processes

/tmp/caido **PID:599**
`/tmp/caido`

- /usr/local/sbin/xdg-open **PID:615**
  `xdg-open http://127.0.0.1:8080/`
- /usr/local/bin/xdg-open **PID:615**
  `xdg-open http://127.0.0.1:8080/`
- /usr/sbin/xdg-open **PID:615**
  `xdg-open http://127.0.0.1:8080/`
- /usr/bin/xdg-open **PID:615**
  `xdg-open http://127.0.0.1:8080/`
- /sbin/xdg-open **PID:615**
  `xdg-open http://127.0.0.1:8080/`
- /bin/xdg-open **PID:615**
  `xdg-open http://127.0.0.1:8080/`

/usr/local/sbin/gio

```
gio open http://127.0.0.1:8080/
```

PID:616

/usr/local/bin/gio

```
gio open http://127.0.0.1:8080/
```

PID:616

/usr/sbin/gio

```
gio open http://127.0.0.1:8080/
```

PID:616

/usr/bin/gio

```
gio open http://127.0.0.1:8080/
```

PID:616

/sbin/gio

```
gio open http://127.0.0.1:8080/
```

PID:616

/bin/gio

```
gio open http://127.0.0.1:8080/
```

PID:616

/usr/local/sbin/gnome-open

```
gnome-open http://127.0.0.1:8080/
```

PID:617

/usr/local/bin/gnome-open

```
gnome-open http://127.0.0.1:8080/
```

PID:617

/usr/sbin/gnome-open

```
gnome-open http://127.0.0.1:8080/
```

PID:617

/usr/bin/gnome-open

```
gnome-open http://127.0.0.1:8080/
```

PID:617

/sbin/gnome-open

/sbin/gnome-open

gnome-open http://127.0.0.1:8080/ PID:617

/bin/gnome-open

gnome-open http://127.0.0.1:8080/ PID:617

/usr/local/sbin/kde-open

kde-open http://127.0.0.1:8080/ PID:618

/usr/local/bin/kde-open

kde-open http://127.0.0.1:8080/ PID:618

/usr/sbin/kde-open

kde-open http://127.0.0.1:8080/ PID:618

/usr/bin/kde-open

kde-open http://127.0.0.1:8080/ PID:618

/sbin/kde-open

kde-open http://127.0.0.1:8080/ PID:618

/bin/kde-open

kde-open http://127.0.0.1:8080/ PID:618

Network

 **DNS** api.caido.io

 **DNS** api.caido.io

	DNS	portal-backend.onrender.com.cdn.cloudflare.net	
	216.24.57.253:443	api.caido.io	**tls**
	216.24.57.253:443	api.caido.io	**tls**
	1.1.1.1:53	api.caido.io	**dns**
	1.1.1.1:53	api.caido.io	**dns**
	1.1.1.1:53	portal-backend.onrender.com.cd...	**dns**

MITRE ATT&CK Matrix

ATT&CK v13

Initial Access | Execution | Persistence | Privilege Escalation | Defense Eva

Virtualizatior
T1497

Downloads

/root/.local/share/caido/config.db

Filesize	44KB
MD5	8c2df9d851c2566d796d0194f401c2e3
SHA1	94e35eb53b777fc653333ac8af57fc6c7bf96725
SHA256	8079ca52fc4ef452dc1d45c0499a3bed3a22ab7a7213dac47e574e5...
SHA512	61b8292cf9b39acbebfdde495a85622e1e599e7d3c4b4271ffa7969...

/root/.local/share/caido/logs/logging.2023-08-31.log

Filesize	4KB
MD5	a94c6b223792ed260f95e4ffec69cf0b
SHA1	f261f5aeb13bfc656828ec47e67cd1a4f34129d3
SHA256	dbd58ee1e006849320fc637d0f80699cf39190ead66429cedb863b...
SHA512	42c4dca8d603e864e580d307cb966c01908e37e50ae071fb77e291...

/root/.local/share/caido/secrets.db

Filesize	12KB
MD5	e599e881f5c612e53a784340edd94f72
SHA1	c1b4bd94ffb3292ee19b9d457f807422fd45ce2d
SHA256	ed59da2e05eef4a4e29287162e0e4cb7a574496d045d5ef52891c9...
SHA512	4d5ca89bc1897203f9c04d4454cf953bacb7fbece3dd9e59dd1ea6...