BROWSE

All LOOBins 53

TACTICS

Collection 11
Command and Control 4
Credential Access 6
Defense Evasion 22
Discovery 27
Execution 9
Exfiltration 3
Impact 3
Lateral Movement 2
Persistence 5
Privilege Escalation 1
Reconnaissance 4
Resource Development 1

TAGS

bash 22
clipboard 3
compress 2
configuration 6
dylib 2
files 2
gatekeeper 2
groups 2
network 5
oneliner 13
osascript 3
pbpaste 2
users 3
XCSSET 2
zsh 13

hdiutil

Created by Mark Morowczynsk (@markmorow)

Description

hdiutil manipulates disk images such as DMG and ISO files. You can mount, unmount, create, resize and verify disk images. Including encrypted images.

Created	Tactics	Tags
2023-05-21	Execution Collection	bash zsh disk

Paths

- `/usr/bin/hdiutil`

Use Cases

Mount a malicious dmg file

Uses hdiutil to mount a malicious dmg file to

```
hdiutil mount malicious.dmg
```

Mount a malicious dmg file

Uses hdiutil to mount a malicious dmg file to

```
hdiutil attach malicious.dmg
```

Mount a malicious iso file

Uses hdiutil to mount a malicious iso file to

```
hdiutil mount malicious.iso
```

Mount a malicious iso file

Uses hdiutil to mount a malicious iso file to

```
hdiutil attach malicious.iso
```

Exfiltrate data in dmg file

Uses hdiutil to create a dmg file to store exfiltrate data

```
hdiutil create -volname "Volume Name" -srcfolder /path/to/folder -ov diskimage.dmg
```

Exfiltrate data in encrypted dmg file

Uses hdiutil to create a dmg file to store exfiltrate data

```
hdiutil create -encryption -stdinpass -volname "Volume Name" -srcfolder /path/to/f
```

Detections

- No detections at time of publishing

Resources

- Microsoft finds new macOS vulnerability, Shrootless, that could bypass System Integrity Protection