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

xattr

Created by Jason Trost (@jason_trost)

Description

The xattr command can be used to display, modify or remove the extended attributes of one or more files, including directories and symbolic links. Extended attributes are arbitrary metadata stored with a file, but separate from the filesystem attributes (such as modification time or file size). The metadata is often a null-terminated UTF-8 string, but can also be arbitrary binary data. xattr can be used to bypass Gatekeeper.

Created	Tactics	Tags
2023-04-20	Execution Defense Evasion	xattr quarantine

Paths

- `/usr/bin/xattr`

Use Cases

Bypass Gatekeeper via xattr

Use xattr to remove quaratine extended attribute from a file.

```
xattr -d com.apple.quarantine FILE
```

Bypass Gatekeeper via xattr

Use xattr to remove quaratine extended attribute from multiple files or directories.

```
xattr -d -r com.apple.quarantine *
```

Detections

- Gatekeeper Bypass via Xattr
- Jamf Protect: Detect activity related to xattr and extended attributes

Resources

- Threat Hunting the macOS edition Megan Carney (Report)

- GrrCon 2018: Threat Hunting the macOS edition Megan Carney