22

27

9

3

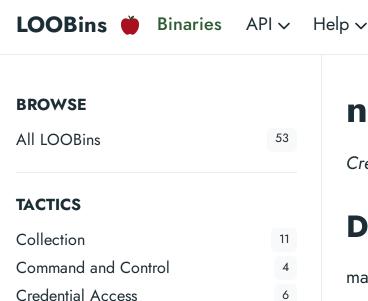
3

2

5

4

1



TAGS

Defense Evasion

Lateral Movement

Privilege Escalation

Resource Development

Reconnaissance

Discovery

Execution

Exfiltration

Persistence

Impact

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

nscur

Created by Leo Pitt (@_D00mfist)

Description

macOS version of curl that is used to download files to a target without applying the quarantine extended attribute

Search LOOBins...

Ctrl + /

6

Created	Tactics		Та	gs
2023-05-22	Defense Evasion	Command and Control		

Paths

/usr/bin/nscurl

Use Cases

Download file

Download file and ignore cert checking

nscurl -k https://google.com -o /private/tmp/google

Download file

Download file to the Downloads directory using -dl

nscurl https://google.com -dl

Download file

Download file to a designated directory using -dir

nscurl https://google.com -dir /private/tmp/google

Detections

- Jamf Protect: Detect all curl and nscurl activity
- Jamf Protect: Detect file downloads using the insecure argument for curl and nscurl
- Sigma: File Download Via Nscurl MacOS

Resources

- How to Diagnose App Transport Security Issues using nscurl and OpenSSL
- Living-off-the-Land: Exploring macOS LOOBins and Crafting Detection Rules nscurl