

BROWSE

All LOOBins

53

TACTICS

- Collection11
- Command and Control4
- Credential Access6
- Defense Evasion22
- Discovery27
- Execution9
- Exfiltration3
- Impact3
- Lateral Movement2
- Persistence5
- Privilege Escalation1
- Reconnaissance4
- Resource Development1

TAGS

- bash22
- clipboard3
- compress2
- configuration6
- dllib2
- files2
- gatekeeper2
- groups2
- network5
- oneliner13
- osascript3
- pbpaste2
- users3
- XCSSET2
- zsh13

tmutil

Created by Brendan Chamberlain (@infosecb)

Description

A tool for managing Time Machine, the native macOS backup utility.

Created	Tactics	Tags
2023-05-01	<div>ImpactCollectionPrivilege EscalationDefense Evasion</div>	<div>backupdeleterestoreunprivileged</div>

Paths

- /usr/bin/tmutil

Use Cases

Disable Time Machine

The following command disables Time Machine. An attacker can use this to prevent backups from occurring.

```
tmutil disable
```

Delete a backup

The following command deletes the specified backup. An adversary may perform this action before launching a ransomware attack to prevent the victim from restoring their files.

```
tmutil delete /path/to/backup
```

Restore a backup

The following command restore the specified backup. An attacker can use this to restore a backup of a sensitive file that was deleted.

```
tmutil restore /path/to/backup
```

Tamper with system logs

An adversary can use the snapshot and restore commands together to tamper with system logs. This is fixed in macOS 10.15.4+.

```
mkdir /tmp/snapshot
tmutil localsnapshot
tmutil listlocalsnapshots /
mount_apfs -o noowners -s com.apple.TimeMachine.2023-05-01-090000.local /System/Volumes/
open /tmp/snapshot
sudo vim /var/log/system.log
tmutil restore com.apple.TimeMachine.2023-05-01-090000.local
```

Exclude path from backup

An adversary could exclude a path from Time Machine backups to prevent certain files from being backed up.

```
tmutil addexclusion /path/to/exclude
```

Detections

- [Jamf Protect: Detect the deletion of localsnapshots](#)
- [Sigma: Time Machine Backup Deletion Attempt Via Tmutil - MacOS](#)
- [Sigma: Time Machine Backup Disabled Via Tmutil - MacOS](#)
- [Sigma: New File Exclusion Added To Time Machine Via Tmutil - MacOS](#)

Resources

- [mount_apfs TCC bypass and privilege escalation](#)
- [Manage Time Machine backups](#)
- [Living-off-the-Land: Exploring macOS LOOBins and Crafting Detection Rules - tmutil](#)