sysctl

Created by Cedric Owens (@cedowens)

Description

Gets the macOS hardware information, which can be used to determine whether the target macOS host is running on a physical or virtual machine.

Created	Tactics	Tags
2023-04-20	Discovery	bash oneliner sysctl

Paths

- `/usr/sbin/sysctl`

Use Cases

Use sysctl to gather macOS hardware info.

sysctl can be used to gather interesting macOS host data, including hardware information, memory size, logical cpu information, etc.

```
sysctl -n hw.model
```

Detections

- Jamf Protect: Detect activity related to sysctl in an interactive shell

Resources

- Evasions: macOS