Recorded Future®
Sandbox

Malware Analysis Report

2025-10-25 16:58

Sample ID	251025-vennpafx9c
Target	icon.png
SHA256	53f8dda136f73dc690d8e82b9e5ff20420f576e6876d327eb63f02b6ecb123dd
Tags	

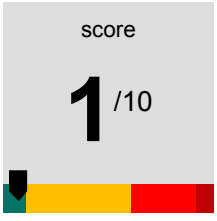

Table of Contents

Part 1. Analysis Overview

SHA256
53f8dda136f73dc690d8e82b9e5ff20420f576e6876d327eb63f02b6ecb123dd

Threat Level: No (potentially) malicious behavior was detected

The file icon.png was found to be: No (potentially) malicious behavior was detected.

Malicious Activity Summary

N/A

Part 2. MITRE ATT&CK

N/A

Part 3. Analysis: static1

3. 1. Detonation Overview

Reported
2025-10-25 16:54

3. 2. Signatures

N/A

Part 4. Analysis: behavioral1

4. 1. Detonation Overview

Submitted	Reported	Platform	Max time kernel	Max time network
2025-10-25 16:54	2025-10-25 16:57	macos-20250619-en	125s	137s

4. 2. Command Line

```
[sh -c sudo /bin/zsh -c "/Users/run/icon.png"]
```

4. 3. Signatures

N/A

4. 4. Processes

/bin/sh
```
[sh -c sudo /bin/zsh -c "/Users/run/icon.png"]
```

/bin/bash
```
[sh -c sudo /bin/zsh -c "/Users/run/icon.png"]
```

/usr/bin/sudo
```
[sudo /bin/zsh -c /Users/run/icon.png]
```

/bin/zsh
```
[/bin/zsh -c /Users/run/icon.png]
```

/Users/run/icon.png
```
[/Users/run/icon.png]
```

/usr/libexec/xpcproxy
```
[xpcproxy com.apple.audio.AudioComponentRegistrar]
```

/System/Library/Frameworks/AudioToolbox.framework/AudioComponentRegistrar
```
[/System/Library/Frameworks/AudioToolbox.framework/AudioComponentRegistrar -daemon]
```

/bin/launchctl
```
[/bin/launchctl kill SIGTERM system/com.microsoft.OneDriveUpdaterDaemon]
```

/bin/launchctl
```
[/bin/launchctl kill SIGTERM system/com.microsoft.OneDriveStandaloneUpdaterDaemon]
```

/usr/libexec/xpcproxy
```
[xpcproxy com.apple.corespotlightservice.725FD30A-6064-6C02-CC51-5DDB8891B57E]
```

/System/Library/Frameworks/CoreSpotlight.framework/CoreSpotlightService
```
[/System/Library/Frameworks/CoreSpotlight.framework/CoreSpotlightService]
```

4. 5. Network

Country	Destination	Domain	Proto
GB	17.57.146.152:5223		tcp

US	52.168.117.168:443		tcp
DE	17.253.15.208:80		tcp
US	8.8.8.8:53	44-courier.push.apple.com	udp
GB	17.250.81.66:443		tcp
BR	17.253.10.201:80	valid.apple.com	tcp
US	8.8.8.8:53	mobile.events.data.trafficmanager.net	udp
US	52.168.117.168:443		tcp
US	8.8.8.8:53	cds.apple.com	udp
BR	17.253.10.204:443	cds.apple.com	tcp
US	8.8.8.8:53	help.apple.com	udp
US	17.253.7.145:443	help.apple.com	tcp
US	17.253.7.145:443	help.apple.com	tcp
US	8.8.8.8:53	world-gen.g.aaplimg.com	udp
US	17.253.7.144:443	help.apple.com	tcp
US	8.8.8.8:53	help.origin-apple.com.akadns.net	udp
BR	17.253.10.202:443	world-gen.g.aaplimg.com	tcp
US	8.8.8.8:53	world-gen.g.aaplimg.com	udp
BR	17.253.10.202:443	world-gen.g.aaplimg.com	tcp
US	8.8.8.8:53	help.origin-apple.com.akadns.net	udp
BR	17.253.10.202:443	help.origin-apple.com.akadns.net	tcp

4. 6. Files

N/A