Recorded Future®
Sandbox

Malware Analysis Report

2025-10-25 17:04

Sample ID	251025-vhv7yasqcy
Target	latest.icon.png
SHA256	9d1fef4ed8abeaa3cbd53c60aafa4b8774cf03c1bb3ad043c6d8f483528b9e14
Tags	defense_evasion

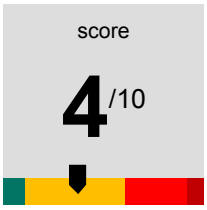
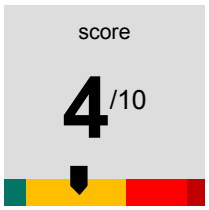


Table of Contents

Part 1. Analysis Overview



SHA256
9d1fef4ed8abeaa3cbd53c60aafa4b8774cf03c1bb3ad043c6d8f483528b9e14

Threat Level: Likely benign

The file latest.icon.png was found to be: Likely benign.

Malicious Activity Summary

defense_evasion

Resource Forking

Part 2. MITRE ATT&CK

2. 1. Enterprise Matrix V16

Reconnaissance TA0043		
Resource Development TA0042		
Initial Access TA0001		
Execution TA0002		
Persistence TA0003		
Privilege Escalation TA0004		
Defense Evasion **TA0005**	Hide Artifacts T1564	
	Resource Forking	T1564.009
Credential Access TA0006		
Discovery TA0007		
Lateral Movement TA0008		
Collection TA0009		
Command and Control TA0011		
Exfiltration TA0010		
Impact TA0040		

Part 3. Analysis: static1

3. 1. Detonation Overview

Reported
2025-10-25 16:59

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 16:59	2025-10-25 17:02	macos-20241101-en	68s	126s

4. 2. Command Line

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

4. 3. Signatures

Resource Forking

defense_evasion

Description	Indicator	Process	Target
N/A	"/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/Java Updater.app/Contents/MacOS/Java Updater" -bgcheck	N/A	N/A
N/A	/System/Library/CoreServices/loginwindow.app/Contents/Resources/LWWeeklyMessageTracer	N/A	N/A

4. 4. Processes

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

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

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

/System/Library/CoreServices/Applications/Feedback Assistant.app/Contents/Library/LaunchServices/seedusaged
```
[/System/Library/CoreServices/Applications/Feedback Assistant.app/Contents/Library/LaunchServices/seedusaged]
```

/usr/libexec/pkreporter
```
[/usr/libexec/pkreporter]
```

/System/Library/PrivateFrameworks/SpeechObjects.framework/Versions/A/SpeechDataInstallerd.app/Contents/MacOS/SpeechDataInstallerd
```
[/System/Library/PrivateFrameworks/SpeechObjects.framework/Versions/A/SpeechDataInstallerd.app/Contents/MacOS/
SpeechDataInstallerd]
```

/System/Library/CoreServices/loginwindow.app/Contents/Resources/LWWeeklyMessageTracer
```
[/System/Library/CoreServices/loginwindow.app/Contents/Resources/LWWeeklyMessageTracer]
```

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

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

/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/Java Updater.app/Contents/MacOS/Java Updater
```
[/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Resources/Java Updater.app/Contents/MacOS/Java Updater -bgcheck]
```

/usr/libexec/xpcproxy
```
[xpcproxy com.apple.nsurlstoraged]
```

/usr/libexec/nsurlstoraged

```
[/usr/libexec/nsurlstoraged --privileged]
```

4. 5. Network

Country	Destination	Domain	Proto
US	8.8.8.8:53	50.courier-push-apple.com.akadns.net	udp

4. 6. Files

/var/db/nsurlstoraged/dafsaData.bin

MD5	64f469698e53d0c828b7f90acd306082
SHA1	bcc041b3849e1b0b4104ffeb46002207eeac54f3
SHA256	d74d0e429343f5e1b3e0b9437e048917c4343a30cff068739ea898bad8e37ffd
SHA512	a8334d1304f2fbd32cfd0ca35c289a45c450746cf3be57170cbbe87b723b1910c2e950a73c1fb82de9dc5ed623166d339a05fec3d78b861a9254dc2cb51fab5f