MALWARE ANALYSIS REPORT

Scarlet

/Users/wraith/Projects-local/Resources/Scarlet.ios.app/Scarlet

HIGH RISK
MALWARE RISK

Analysis Date	2026-11-08 12:02:56 EST
Architecture	AARCH64 (GhidraScript)
Malware Risk Score	75/100
Weaknesses Found	0
Functions	0 extracted
AI Provider	Custom
AI Model	deepseek-v4-1-flash-1017-uncensored

TABLE OF CONTENTS

Click any entry to jump to its section.

1 Binary Information p.3 ›

2 Malware Risk Assessment p.4 ›

3 Binary Protections p.5 ›

4 Malware Family Attribution p.6 ›

5 Similar Prior Samples p.7 ›

6 Indicators of Compromise & C2 p.8 ›

7 Enrichment: Packing, YARA & Threat Intel p.9 ›

8 Suspicious Indicators p.10 ›

9 String Analysis p.11 ›

10 Function Analysis p.12 ›

11 Memory Map p.13 ›

12 Raw Ghidra Output p.14 ›

BINARY INFORMATION

File Name	Scarlet
File Path	/Users/wraith/Projects-local/Resources/Scarlet.ios.app/Scarlet
File Size	8.63 MB (9044304 bytes)
Format	Demand Paged Executable File (GhidraScript)
Architecture	AARCH64 (GhidraScript)
Language/Compiler	Objective-C, Rust, Swift (GhidraScript) / gc (GhidraScript)
Entry Point	Unknown
Image Base	Unknown
MD5	8ce2ca41119d6cec38c931cc9497f356
SHA-256	0c0604637bea101fa25b5aad233c88cc1814055f896d21cb2b03fd8189979826

MALWARE RISK SCORE: 75/100 — HIGH RISK

Multiple weaknesses and/or strong evasion indicators found, consistent with malicious behavior.

ANALYSIS SUMMARY

Critical Weaknesses	0
High Weaknesses	0
Medium Weaknesses	0
Family Attribution	Generic Go RAT / backdoor (heuristic)
IOCs Extracted	39
Obfuscation Indicators	0
Total Functions	0
Memory Segments	56

BINARY PROTECTIONS (MITIGATION AUDIT)

checksec-equivalent audit of exploit mitigations present in this build.

NX / DEP (non-executable stack/heap)	ENABLED
PIE / ASLR base randomization	ENABLED
RELRO	N/A
Stack Canary	DISABLED
FORTIFY_SOURCE / Guard	DISABLED
Stripped Symbols	DISABLED

WHAT THIS MEANS FOR EXPLOITATION

PIE enabled but no canary: an address leak is needed to defeat ASLR, but once the base is known the return address can be overwritten directly.

Generic Go RAT / backdoor (heuristic)

RAT / Backdoor · Confidence: Medium · Signature match: 0/0

RATIONALE

No named family matched, but the binary exhibits 6 malicious capability classes: network pivoting/proxy, command execution, anti-analysis/obfuscation, encryption/encoding, C2 beaconing, persistence.

KEY EVIDENCE

Go build version	n/a
Kerberos (gokrb5)	GetETypeID, AddASN1*, asn1Signature

SIMILAR PRIOR SAMPLES

1 match(es) against samples previously analyzed on this machine (local history only — not shared with any service).

100% — Identical file (SHA-256) 2026-07-18 15:29

Scarlet Generic Go RAT / backdoor (heuristic)

SHA-256: 0c0604637bea101fa25b5aad…

INDICATORS OF COMPROMISE & C2

39 atomic indicators (34 network/C2) for detection, hunting and blocking.

TYPE	INDICATOR	CONTEXT
SHA-256	0c0604637bea101fa25b5aad233c88cc1814055f896d21cb2b…	File hash
MD5	8ce2ca41119d6cec38c931cc9497f356	File hash
URL	http://www.apple.com/DTDs/PropertyList-1.0.dtd	Embedded URL
URL	https://apple.com	Embedded URL
URL	https://debianlibpriv.hop.sh/kbsync?dsid=	Embedded URL
URL	https://f000.backblazeb2.com/file/altstore-staging…	Embedded URL
URL	https://itunes.apple.com/lookup	Embedded URL
URL	https://itunes.apple.com/search	Embedded URL
URL	https://local.usescarlet.com/custom_app.plist	Embedded URL
URL	https://local.usescarlet.com/icon.png	Embedded URL
URL	https://local.usescarlet.com/signedIPA.ipa	Embedded URL
URL	https://p25-buy.itunes.apple.com/WebObjects/MZBuy.…	Embedded URL
URL	https://p25-buy.itunes.apple.com/WebObjects/MZFina…	Embedded URL
URL	https://resources.usescarlet.com/community/cert.dc…	Embedded URL
URL	https://resources.usescarlet.com/mobileconfig.php	Embedded URL
URL	https://resources.usescarlet.com/nil.png	Embedded URL
URL	https://usescarlet.com/	Embedded URL
URL	https://usescarlet.com/fake.png	Embedded URL
URL	https://usescarlet.com/fakedeb.deb	Embedded URL
URL	https://usescarlet.com/fakeplace.deb	Embedded URL
URL	https://usescarlet.com/fakepng.png	Embedded URL
URL	https://usescarlet.com/img/icon.png	Embedded URL
URL	https://usescarlet.com/scarlet.json	Embedded URL
Domain	apple.com	Remote host
Domain	debianlibpriv.hop.sh	Remote host
Domain	f000.backblazeb2.com	Remote host
Domain	itunes.apple.com	Remote host
Domain	local.usescarlet.com	Remote host

Packing / Unpacking

Packer	none detected

YARA (0 rule matches)

Result	no bundled rules matched

VirusTotal

Status	not configured — set VT_API_KEY to enable VirusTotal enrichment
Lookup	https://www.virustotal.com/gui/file/0c0604637bea101fa25b5aad233c88cc1814055f896d21cb2b03fd8189979826

Dynamic Verification

Not performed. Dynamic detonation requires an isolated instrumented VM/sandbox (e.g. CAPE/Cuckoo for PE, an ELF sandbox for Linux). Configure SANDBOX_URL to enable submission. Findings in this report are from static analysis only.

SUSPICIOUS INDICATORS

No suspicious indicators detected.

Suspicious Strings (69 of 400 total)

▸ Command Execution

--------	[JITEnabler] executablePath: '%@'
--------	@executable_path/ello
--------	@executable_path/Sys.dylib
--------	@executable_path/db/CydiaSubstrate.framework/CydiaSubstrate
--------	@executable_path/db/Orion.framework/Orion
--------	@executable_path/db
--------	@executable_path/db/libsubstrate.dylib
--------	@executable_path/db/CydiaSubstrate.framework/

▸ URL/Domain

--------	https://f000.backblazeb2.com/file/altstore-staging/altserver/developerdisks.json
--------	https://usescarlet.com/fakeplace.deb
--------	https://usescarlet.com/fakepng.png
--------	https://usescarlet.com/fakedeb.deb
--------	https://usescarlet.com/img/icon.png
--------	https://localhost.usescarlet.com:59070/signedIPA.ipa
--------	https://local.usescarlet.com/signedIPA.ipa
--------	https://localhost.usescarlet.com:59070/icon.png

Suspicious Functions (0 of 0 total)

ADDRESS	FUNCTION NAME	REASON

No suspicious functions detected.

MEMORY MAP

NAME	START	END	SIZE	PERMS	TYPE
__text	0x0000000100008000		4.47 MB	r--	DATA
__stubs	0x000000010047f8f4		16.7 KB	r--	DATA
__stub_helper	0x0000000100483b90		16.6 KB	r--	DATA
__objc_stubs	0x0000000100487e14		39.1 KB	r--	DATA
__gcc_except_t	0x0000000100491a94		28.7 KB	r--	DATA
__const	0x0000000100498d80		78.6 KB	r--	DATA
__cstring	0x00000001004ac7e0		101.6 KB	r--	DATA
__objc_classna	0x00000001004c5e62		2.2 KB	r--	DATA
__objc_methnam	0x00000001004c6756		61.9 KB	r--	DATA
__objc_methtyp	0x00000001004d5ee0		9.2 KB	r--	DATA
__constg_swift	0x00000001004d83e0		18.4 KB	r--	DATA
__swift5_typer	0x00000001004dcd58		67.5 KB	r--	DATA
__swift5_built	0x00000001004edb6c		460 B	r--	DATA
__swift5_refls	0x00000001004edd40		22.1 KB	r--	DATA
__swift5_field	0x00000001004f35c4		20.8 KB	r--	DATA
__swift5_assoc	0x00000001004f891c		3.4 KB	r--	DATA
__swift5_proto	0x00000001004f9694		1.2 KB	r--	DATA
__swift5_types	0x00000001004f9b54		1.0 KB	r--	DATA
__swift5_captu	0x00000001004f9f64		6.4 KB	r--	DATA
__swift5_entry	0x00000001004fb8f4		8 B	r--	DATA
__swift5_proto	0x00000001004fb8fc		44 B	r--	DATA
__swift5_mpenu	0x00000001004fb928		24 B	r--	DATA
__rodata	0x00000001004fb940		608.4 KB	r--	DATA
__unwind_info	0x0000000100593ae8		36.9 KB	r--	DATA
__eh_frame	0x000000010059ceb0		51.3 KB	r--	DATA
__oslogstring	0x00000001005ac000		3 B	r--	DATA
__got	0x00000001005b0000		6.2 KB	r--	DATA

RAW GHIDRA OUTPUT

Raw output from Ghidra analysis pipeline for forensic verification.

[BINARY_INFO]

```
  INFO  Using log config file: jar:file:/opt/ghidra_12.2_DEV/Ghidra/Framework/Generic/lib/
  Generic.jar!/generic.log4j.xml (LoggingInitialization)
  INFO  Using log file: /Users/wraith/Library/ghidra/ghidra_12.2_DEV/application.log
  (LoggingInitialization)
  INFO  Loading user preferences: /Users/wraith/
```

[CREATE_PROJECT]

```
  Created Ghidra project at /Users/wraith/Desktop/AMA/AMA-20261108_120256/ghidra_projects/
  ama_22888B27
```

[IMPORT_BINARY]

```
  Imported Scarlet into project ama_22888B27
  INFO  Using log config file: jar:file:/opt/ghidra_12.2_DEV/Ghidra/Framework/Generic/lib/
  Generic.jar!/generic.log4j.xml (LoggingInitialization)
  INFO  Using log file: /Users/wraith/Library/ghidra/ghidra_12.2_DEV/application.log
  (LoggingInitialization)
  INF
```

[NATIVE_BUILDINFO]

```
  /Users/wraith/Projects-local/Resources/Scarlet.ios.app/Scarlet:     file format mach-o arm64
```

[NATIVE_SECTIONS]

```
  /Users/wraith/Projects-local/Resources/Scarlet.ios.app/Scarlet:     file format mach-o arm64

  Sections:
  Idx Name            Size     VMA              Type
    0 __text          004778f4 0000000100008000 TEXT
    1 __stubs         0000429c 000000010047f8f4 TEXT
    2 __stub_helper   00004284 0000000100483
```

[PATH_RESOLVE]

```
  Resolved package 'Scarlet.ios.app' → main executable 'Scarlet'
```