

Forum:[Hack Forums](#)

Thread: [iOS KERNEL EXPLOIT & C2 FRAMEWORK DARKSWORD v2.6.0](#)

CYBERWAR WEAPONS - May 26, 2026, 3:54 pm

? C Y B E R W A R W E A P O N S ?
iOS KERNEL EXPLOIT & C2 FRAMEWORK — DARKSWORD v2.6.0

THREAD BY: CYBERWAR WEAPONS · PROGRAM: DARKSWORD v2.6.0 · TARGET: iOS
15.0–18.7 · ARCH: arm64 / arm64e

??

? [01. INTRODUCTION]

CYBERWAR WEAPONS presents DarkSword — a full-chain iOS kernel exploitation and Command & Control framework engineered for iOS 15.0 through 15.8.4 and iOS 18.0 through 18.7 on arm64 and arm64e devices.

DarkSword is not a script. It is a multi-stage exploitation framework built from the ground up in Objective-C, implementing a complete 7-stage chain from raw kernel primitive acquisition to persistent remote agent deployment — all mapped to the AegisFlow 42-subsystem security model.

??

? [02. EXPLOIT CHAIN — 7 STAGES]

STAGE
NAME
METHOD
TARGET ARCHITECTURE

§0
Kernel Exploit
IOSurface UaF / CoreTrust PPL race
iOS 15 + iOS 18

§1
PAC Bypass
FEAT_PAuth2 · AMCC write-gate · diversity=0x6A79
arm64e (A12+)

§2
PPL Bypass
AMCC register-level write-gate
iOS 15 + iOS 18

§3
Privilege Escalation
allproc walk · uid=0 · cs_flags -> CS_PLATFORM_BINARY
All targets

§4
Sandbox Escape
MAC label slot[0] detach · Sandbox.kext bypass
All targets

§5
GHOSTBLADE Deploy
LaunchDaemon + AMFI trust cache + dylib inject
All targets

§6
Persistence
PAC-signed arm64e stub · SpringBoard injection
arm64e exclusive

??

? [03. GHOSTBLADE — PERSISTENT REMOTE AGENT]

GHOSTBLADE is DarkSword's primary persistent agent. Once deployed it survives reboots and device wipes of the userland partition.

LaunchDaemon persistence — installs as com.apple.nehelper2, starts at boot, auto-restarts on crash

Dylib injection — injects into SpringBoard and backboardd (arm64e PAC-signed stubs) AMFI trust

cache insertion — CDHash inserted into static trust cache; binary treated as platform-signed

C2 channel — TLS 1.3 / AES-256-GCM / X25519 key exchange; cert pinned with SHA-256 SPKI

Heartbeat — 60s interval; self-healing reconnect on network change

Self-destruct — remote wipe command zeroes binary on disk and removes all artefacts

??

? [04. GHOSTKNIFE — FORENSIC EXTRACTION]

GHOSTKNIFE is the DarkSword extraction payload. Deploys post-sandbox-escape with full filesystem and keychain access.

Full Keychain extraction — all access groups, all classes (GenericPassword, InternetPassword, Certificate, Key)
Browser credentials — Safari saved passwords, Chrome, Firefox iOS Encrypted app databases — Signal SQLCipher (key from Keychain), WhatsApp, Telegram
iCloud authentication tokens — com.apple.account.* Keychain access group Full filesystem traversal — /private/var, /var/mobile/Containers (Data + Bundle)
Exfiltration — zlib compressed, AES-256-GCM encrypted envelope, POST to ingest endpoint

??

? [05. C2 WEB PANEL]

Every license includes access to the DarkSword C2 Panel — a React/Vite web dashboard styled as a dark terminal interface.
Overview — live C2 traffic chart, audit event rate, exploit chain stage progress bars
Device Registry — all connected devices with iOS version, kernel slide, exploit stage, latency
Payload Management — GHOSTBLADE/GHOSTKNIFE config, AegisFlow \$N subsystem status
Remote Terminal — interactive shell with command history and real remote responses Audit Log — Merkle-linked forensic-grade event log with live streaming and hash chain viewer
Per-user access — each buyer gets their own registered panel login (HF username based)

??

? [06. SUPPORTED DEVICES & iOS VERSIONS]

iOS Branch
Versions
Architecture
Devices

iOS 15.x
15.0 -> 15.8.4 (all minors)
arm64 + arm64e
iPhone 6s -> iPhone 13

iOS 18.x
18.0 -> 18.7 (all minors)
arm64e
iPhone XS -> iPhone 16 Pro Max

Kernel struct offsets are bundled for all supported minor versions in signed plist files. Automatic version detection on runtime.

??

? [07. AEGISFLOW — SECURITY ARCHITECTURE]

DarkSword is built on the AegisFlow 42-subsystem security model to ensure every component is structurally accounted for, auditable, and clear of common forensic indicators.

- Key AegisFlow subsystems implemented:
- §1 MemoryTagManager — all kread/kwrite tagged with access class (Kernel, UserData, PPLProtected)
 - §2 CapabilityRegistry — signed tokens with permission bitmask + TTL required before any kernel write
 - §3 FormalVerifier — stage ordering enforced; chain cannot proceed out of order
 - §4 SecurityMonitor — every exploit event logged with subject/object/timestamp
 - §17 AuditBridge — Merkle-linked audit chain; tamper-evident event log
 - §22 CFIGuard (inverse) — PAC bypass using AMCC diversity value extraction
 - §29 CryptoRNGGuard — SecRandomCopyBytes for all IV generation
 - §39 CryptoAlgorithmGuard — AES-256-GCM only for C2 and exfil paths

??
[contract=tid]Start Contract[/contract]

Scary - May 26, 2026, 4:18 pm
How many people still use iOS 18?? I have a iPhone 13 and its iOS 26 and I don't even remember installing any updates myself on it.

CYBERWAR WEAPONS - May 26, 2026, 4:23 pm
[contract=tid]Start Contract[/contract]

? [08. PRICING & TIERS]

TIER
INCLUDES
PRICE
SLOTS

? TRIAL
C2 Panel access, 3 demo device slots, read-only payloads
FREE
[td]7 total (3 concurrent online)[/td]

? BASIC
Full GHOSTBLADE, C2 Panel, 10 device slots, 30-day license
\$150
Limited

? PRO
GHOSTBLADE + GHOSTKNIFE, C2 Panel, unlimited devices, 90-day license
\$350
Limited

? ELITE

Everything in PRO + source code access + dedicated C2 server + 1yr license
\$800
3 only

Payment accepted: Monero (XMR) only. No BTC, no PayPal, no escrow exceptions.
Delivery: Encrypted archive + panel credentials within 24h of confirmed payment.

[contract=tid]Start Contract[/contract]

[illegible]

? [09. OPSEC & ANTI-FORENSICS]

- No plaintext on disk — all sensitive data AES-256-GCM encrypted at rest
- Binary masquerades as Apple system daemon (nehelper2, com.apple.nehelper2)
- No crash logs — unhandled exceptions caught internally; no CrashReporter entries
- Network traffic — TLS 1.3 on port 443; indistinguishable from normal HTTPS traffic
- Self-destruct — single command wipes all artefacts, logs, and plist entries
- No jailbreak artefacts — does not install Cydia, does not write to /var/lib/dpkg, does not modify /etc/fstab
- Fake entitlement set — binary carries legitimate-looking Apple private entitlements

[illegible]

? [10. FAQ]

Q: Does this work on iPhone 16?

A: Yes. iOS 18.0–18.7 covers iPhone XS through iPhone 16 Pro Max on arm64e.

Q: Does this require physical access?
A: Initial delivery requires physical access or a pre-positioned payload vector. Remote re-exploitation after first deployment does not require physical access.

Q: Will an iOS update break it?
A: Minor updates within supported branches do not break the chain — kernel struct offsets for all minors are pre-bundled. A major iOS version bump (e.g. 18.x -> 19.x) requires a new offset plist which we provide to active license holders.

Q: Can I see a demo?
A: Register for the free trial via [the C2 panel](#) using password _EPIC_SIEZED_CACHE. Full demo environment with 23 concurrent demo device slots.

Q: Will you provide support?
A: Yes. PRO and ELITE tier buyers receive dedicated Jabber/XMPP support. BASIC tier receives thread-based support. Trial is community supported.

Q: Is this based on existing public exploits?

A: The kernel primitive acquisition leverages known vulnerability classes. The full chain — PAC bypass, PPL bypass, privilege escalation, sandbox escape, and persistence — is original work by CYBERWAR WEAPONS.

[illegible]

? [11. VOUCHES & CONTACT]

Vouches: See post #2. All vouches are from HF-verified members with post count >= 100.

Contact:

HF PM: CYBERWAR WEAPONS

* Trial registration: [the C2 panel](#) using password _EPIC_SIEZED_CACHE.

DO NOT contact me via Discord, Telegram, or any clearnet platform. XMR-only payments. No exceptions.

??

? CYBERWAR WEAPONS — DARKSWORD v2.6.0 ?

iOS 15.0–18.7 · arm64/arm64e · AegisFlow §1–§42

© 2026 CYBERWAR WEAPONS · All source code proprietary · Redistribution prohibited

(May 26, 2026 04:18 PM)Scary Wrote: [\[CITE\]](#) How many people still use iOS 18?? I have a iPhone 13 and its iOS 26 and I don't even remember installing any updates myself on it.

The Core Vulnerable Pool: Roughly 221,520,000 devices (representing about 14.2% of active global iPhone users) are running the most susceptible software versions, specifically iOS 18.4 through 18.6.2. The Maximum Extended Pool: If the underlying flaws are successfully chained against all unpatched variations of iOS 18, up to 296,244,000 devices (18.99% of users) could be exposed. [warn]

Scary - May 26, 2026, 4:52 pm

(May 26, 2026 04:23 PM)CYBERWAR WEAPONS Wrote: [\[CITE\]](#) The Core Vulnerable Pool: Roughly 221,520,000 devices (representing about 14.2% of active global iPhone users) are running the most susceptible software versions, specifically iOS 18.4 through 18.6.2. The Maximum Extended Pool: If the underlying flaws are successfully chained against all unpatched variations of iOS 18, up to 296,244,000 devices (18.99% of users) could be exposed. [warn]

How old is that data and where did you even get it from? Regardless its very low amount not worth buying this and even then the devices from that data probably already upgraded to latest version by now. I also see you have very negative rep and you're excited for your low quality thread. DWC this smells like a scam.

nethoodus - May 26, 2026, 8:05 pm

Hi, yes, I would like to test this. Do you have a telegram or something where I can contact you?
Windows and Android remote control

Binance - May 29, 2026, 5:48 am

(May 26, 2026 08:05 PM)nethoodus Wrote: [\[CITE\]](#) Hi, yes, I would like to test this. Do you have a telegram or something where I can contact you?

Windows and Android remote control

<https://hackforums.net/showthread.php?tid=6323419>

It's public.

Just some retard plugging in this to a GPT and exporting a sales thread.

It isn't a GUI RAT for post exploitation.

EXPLOIT PRODUCTS - May 31, 2026, 12:09 pm

(May 26, 2026 08:05 PM)nethoodus Wrote: [\[CITE\]](#) Hi, yes, I would like to test this. Do you have a telegram or something where I can contact you?

Windows and Android remote control

Send me your Telegram.