iVerify Details DarkSword, Second Mass Attack Against iOS Disclosed in Two Weeks

Exploit kit observed in Ukraine impacts iOS 18.4 to 18.6.2 and up to 270 million devices


iVerify logo

BELFAST, NORTHERN IRELAND & NEW YORK, NY, UNITED STATES, March 18, 2026 /EINPresswire.com/ -- iVerify, the leader in advanced mobile endpoint detection and response (EDR) solutions, today announced the details into its investigation of DarkSword, a newly disclosed watering hole attack against iPhones running iOS 18.4 to 18.6.2 in Ukraine. These versions, released in 2025, are still running on up to 270 million devices. The attack was uncovered due to a suspicious-looking URL hosted on the same infrastructure the threat actor from Russia used in the first-known Coruna attack against Ukraine announced on March 3, 2026. Noteworthy is that one of the sites redirecting to the malicious payload is a .gov.ua address, meaning the threat actor managed to compromise the Ukrainian government server. We worked together with CERT UA to ensure the threat was mitigated prior to public disclosure.

Completely written in JavaScript, DarkSword comprises six vulnerabilities across two exploit chains that were patched in stages ending with iOS 26.3. Starting in WebKit and moving down to the kernel, it achieves full iPhone compromise with elegant techniques never publicly seen before. Unlike Coruna that seemed to be targeted mostly at crypto theft, DarkSword appears to be a surveillance and intelligence gathering tool, blanket pulling data including Wi-Fi passwords, text messages, call history, root location history, browser history, SIM card and cellular data as well as health, notes and calendar databases, though it does also look for crypto wallets.

"The second mass attack disclosed in two weeks proves what many of us have been saying, that mobile attacks are widespread and no longer something businesses and governments can ignore," said Rocky Cole, co-founder and COO of iVerify. "Years ago, fileless malware attacks that turned desktop operating systems against the user completely upended enterprise IT. DarkSword is the first iOS exploit to do the same, collecting a vast amount of user data, despite the exploit chain itself not being as complex as Coruna. DarkSword shows that mass iOS surveillance is quite feasible. Will enterprise leaders finally take notice?"

The Russian threat actor deploying this instance of DarkSword has very poor operational security. They left the full JavaScript code unobfuscated, unprotected and easily accessible. This carelessness, along with that of the Chinese criminal group using Coruna, led to both attacks ultimately being uncovered. DarkSword and Coruna exploits captured in the wild are easy to repurpose and redeploy, making it highly likely that more and possibly modified deployments of DarkSword and Coruna spyware are actively infecting unpatched iOS users, in addition to being for sale on the secondary market.

Given that the infiltration server's code contained comments in Russian and the exploit codebase contained original variable names and deployment instructions in English the operator and the developer are probably different entities, which suggests independent acquisition of the exploit chain. Combined with poor operational security, this suggests a few different possibilities. First, the threat actor isn't worried about getting caught because few tools exist to actually detect these iOS attacks. Second, the supply of iOS exploits is so large the threat actor isn't worried about burning one. Third, the threat actor is not aware of the value of the exploit.

Regardless, the evidence continues to mount that low-level criminals and non-sophisticated actors can now get access to advanced exploit tools mirroring the rise of the malware-as-a-service and ransomware-as-a-service economies.

The full technical analysis, published in coordination with our industry partners Google and Lookout, is available on the iVerify blog: https://iverify.io/blog/darksword-ios-exploit-kit-explained.

To check for infection, use the iVerify Basic app free to install from the App Store through May. To learn more about how iVerify can protect your enterprise mobile fleet, request a demo https://iverify.io/contact.

About iVerify
iVerify is a pioneer in mobile endpoint detection and response (EDR) solutions, providing advanced protection against the real threats mobile devices face. The company's comprehensive security platform safeguards organizations from fileless malware, smishing, malicious applications, ransomware operations, and breaches resulting from credential theft. iVerify's solutions span from consumer to enterprise and government sectors, offering both privacy-focused BYOD protection and enterprise-grade security capabilities to ensure every device in the workplace is secure.

For more information, please visit: www.iverify.com.

Monika Hathaway
iVerify
email us here