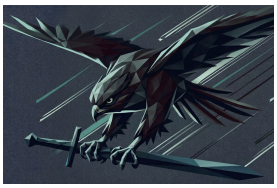
Lookout

Mobile Threat of the Month

April 2026

DarkSword iOS Exploit



Lookout Threat Labs has discovered DarkSword, a highly sophisticated, commercial grade iOS exploit chain targeting iPhones running iOS versions between 18.4 and 18.6.2.

Deployed by a likely Russia-backed threat actor known as UNC6353, the malware is designed for both espionage and rapid financial theft.

Unlike traditional spyware that lingers for long-term surveillance, **DarkSword** is engineered for the "smash-and-grab." It prioritises velocity over persistence, scraping high-value corporate and personal intelligence before vanishing.

DarkSword targets the most sensitive layers of a user's digital life, including:

Credentials: Saved browser passwords and cryptographic keys.
Communications: Full messaging histories from WhatsApp and Telegram, alongside private emails.
Cloud Storage: Corporate documents stored within iCloud Drive.

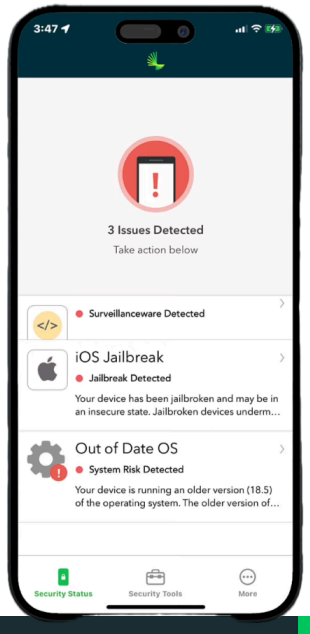
The most distinctive feature of this malware is its exit strategy: DarkSword executes a complete self-deletion protocol within minutes of infection, leaving virtually no forensic footprint for security teams to follow.

DarkSword has evolved from a sophisticated, niche threat into a commoditised exploit with global reach. Following its leak on GitHub, the malware is now significantly easier to adapt and scale. This transition highlights a pivotal shift in the threat landscape: high-tier surveillance capabilities are now public, and mobile devices are the primary frontline.

Lookout Mobile Security

For businesses, the question is no longer whether mobile devices introduce risk. The question is whether you can see that risk and stop it in real time. Lookout offers a multi-pronged defense strategy to secure corporate fleets against elite, fast-moving threats like DarkSword.

Proactive Safe Browsing: Lookout's Safe Browsing features actively monitor and block connections to known malicious infrastructure (such as DarkSword's command servers and exploit delivery domains).



Out-of-Date OS Detection: DarkSword relies on specific vulnerabilities patched in newer iOS versions. Lookout empowers IT admins to quickly identify vulnerable devices in their fleet and enforce updates. (Devices running iOS 18.7.3+ or iOS 26.3+ are entirely immune to this exploit).

Device Compromise Detection: Post-exploitation behavioral monitoring flags the privilege escalation and unauthorized system access attempted by the DarkSword payloads.

Web History Feed Tracking: Lookout provides telemetry that allows security teams to identify if any devices in their fleet have previously been exposed to or compromised by the domains associated with the DarkSword campaign.

For more information visit Lookout.com