In due minuti l'iPhone può essere svuotato di dati e soldi: cos'è la minaccia DarkSword

Una serie di attacchi rivolti contro le versioni non aggiornate di iOS puntano a sottrarre informazioni sensibili degli utenti iPhone. (Fonte: https://www.corriere.it/ 21 marzo 2026)

Che arrivi dalla Russia è quasi certo. Con amore, non proprio, tanto per parafrasare un film di 007. Perché di spionaggio sempre si parla. A distanza di poco più di una settimana dalla condivisione delle scoperte sul malware Coruna, arrivano altre novità in termini di sicurezza per gli **utenti di iPhone**. La nuova minaccia, battezzata con il nome di **DarkSword** giusto per incutere quel timore che non guasta, **è in grado di violare gli iPhone e sottrarre dati, informazioni (e denaro) in pochi minuti**. Come la precedente violazione, anche questa è stata scoperta da **Google Threat Intelligence Group**, insieme ad **iVerify** e **Lookout**. Non si tratta di un malware, ma di una serie di attività malevole che possono **compromettere il device** e portarlo all'esecuzione di software all'insaputa dell'utente, con lo scopo di **sottrarre informazioni sensibili**.

Cos'è DarkSword

DarkSword non è di recentissima fattura, le prime tracce risalgono infatti a **novembre 2025**. Le sue capacità sono state sfruttate da più entità, tra cui operatori di sorveglianza commerciale e a gruppi sospettati di attività statale, tra questi il gruppo **UNC6353**, riconducibile ad attività di **spionaggio russo** e già legato a **Coruna**. Le campagne ai danni dei target degli utilizzatori del framework sono disseminati tra Arabia Saudita, Turchia, Malesia e Ucraina.

L'attacco e i rischi

Secondo **iVerify** i criminali informatici sfruttano scenari da **watering hole**, ovvero una modalità d'attacco in cui vengono compromessi siti Web utilizzati da un determinato target di utenti al fine di infettare i propri dispositivi. Tra gli esempi riportati dal team di **Google**, uno dei siti violati era stato pensato a tema **Snapchat** e sfruttato per colpire gli **utenti sauditi**. L'attacco proveniva da un sito compromesso che diverse volte ha poi però reindirizzato gli utenti a siti legittimi, così da rendere nascosta l'attività malevola. Di recente, Cupertino ha anche condiviso **una nota** in cui **esorta i propri clienti ad aggiornare i propri iPhone per rimanere al sicuro**.

iPhone spalanca tutti i suoi dati

I pericoli per i device infettati, secondo quanto riportato da **Lookout**, sono diversi. **DarkSword può fornire pieno accesso alle informazioni presenti sullo smartphone**. Dalle chiamate, ai messaggi, alla posizione, password del Wi-Fi, **persino foto**, i dati del browser e ai portafogli di criptovalute. Per proteggersi, i consigli sono gli stessi forniti per Coruna. Tenere aggiornato il dispositivo ed, eventualmente, come maggior precauzione per chi sentisse di essere a rischio, attivare la **Lockdown Mode** o Modalità isolamento attraverso il percors**o** Impostazioni -> Privacy e Sicurezza -> Modalità isolamento. Ricordiamo che la Modalità Isolamento rafforza la sicurezza dello smartphone, ma nel limita le capacità e quindi non va utilizzata senza consapevolezza.

Più nello specifico sono sei le vulnerabilità sfruttate da DarkSword per compromettere i melafonini e puntano alle versioni più recenti non ancora aggiornate. Per funzionare, l'attacco prende di mira i dispositivi in cui sono installate **le versioni di iOS dalla 18.4 fino alla 18.7**. Più nel dettaglio, le vulnerabilità sono le **CVE-2025-31277, CVE-2025-43529, CVE-2026-20700, CVE-2025-14174, CVE** riguardano **ANGLE**, **JavaScriptCore/WebKit** e **kernel iOS**.

Apple ha corretto queste vulnerabilità e i bug con l'ultima versione di iOS, la 26.3, anche se diverse erano già state corrette in precedenza.