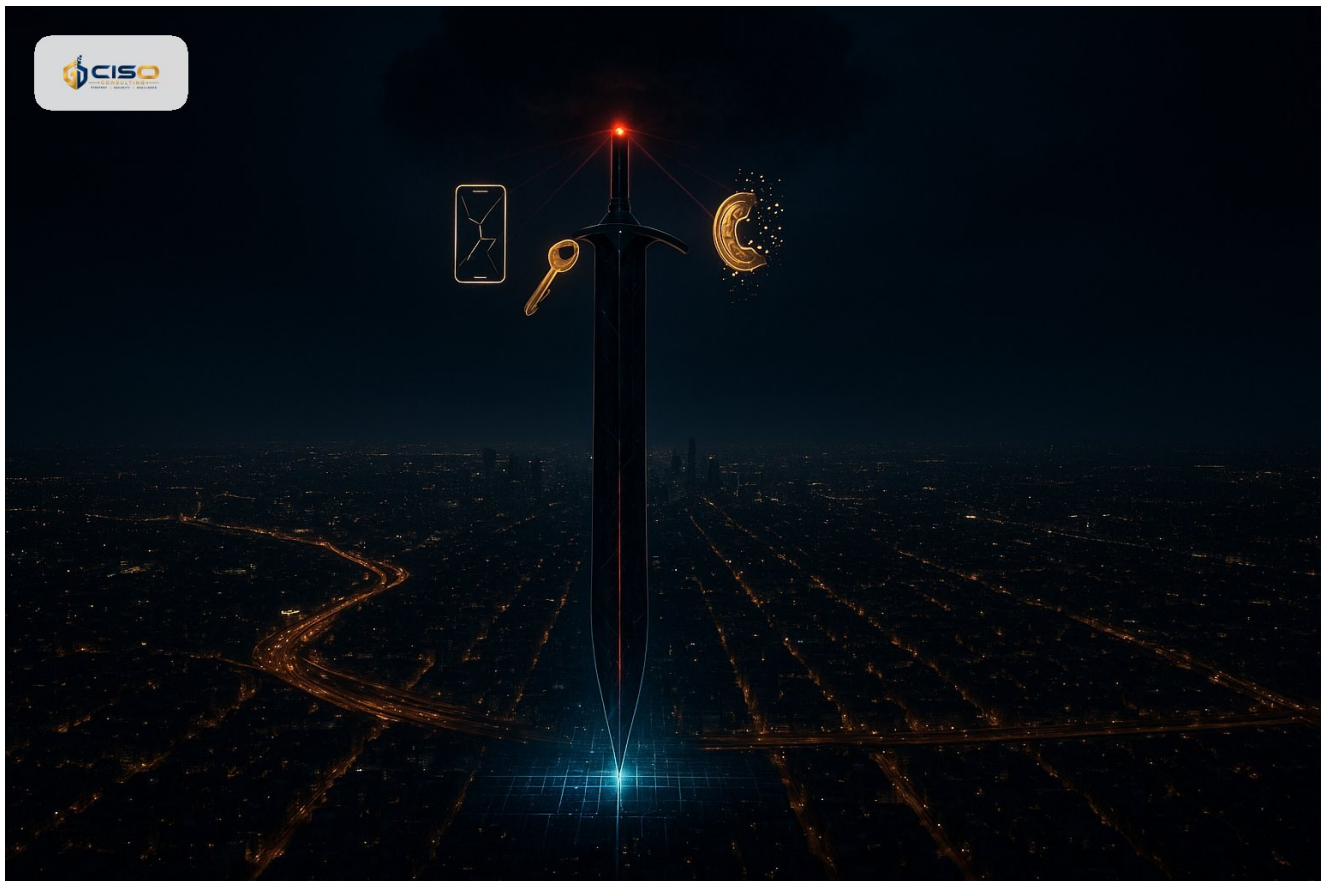


P7 DarkSword iOS exploit kit adds wallet theft and remote commands



iVerify has described P7 DarkSword, a new variant of the DarkSword iOS exploit kit. It leaves a smaller footprint on the device, steals keychain and crypto-wallet data, and supports two-way communication with attacker servers.

- iVerify published details of P7, a previously unseen variant of the DarkSword iOS exploit kit.
- P7 reduces its on-device footprint compared with variants seen before.
- It adds theft of keychain data and crypto-wallet data from the device.
- It adds two-way command-and-control communication with the attacker's infrastructure.

Researchers at iVerify have disclosed a previously unseen variant of the DarkSword iOS exploit kit, named P7 DarkSword, in a report published on Thursday.

What is new in P7

According to iVerify, P7 differs from the variants its team usually observes in three ways. It reduces its footprint on the device, which can make traces harder to find. It adds theft of keychain contents and crypto-wallet data held on the device. It also adds two-way command-and-control (C2) communication, so the attacker's infrastructure can exchange instructions and data with the compromised phone.

Why it matters for regulated institutions

The keychain is where an iPhone stores saved credentials, so theft from it can expose access to corporate and personal accounts. A smaller on-device footprint also means that routine checks on the device may reveal less. The source excerpt does not give details on infection method, targets, affected iOS versions or patches, so teams should not assume a specific exposure level until the full iVerify report is reviewed.

A calm, practical response is to confirm that mobile device management covers iOS fleets, that update policies are enforced, and that incident procedures treat a compromised phone as a possible credential exposure event.

What to do now

1. Read the full iVerify report and extract indicators and affected iOS versions for your environment.
2. Confirm all corporate and BYOD iPhones are enrolled in MDM and run the latest iOS release.
3. Treat a suspected compromised iPhone as a credential exposure event: reset passwords and revoke sessions for accounts used on it.
4. Advise staff handling crypto assets or high-privilege access to report unusual device behaviour promptly.
5. Add iOS compromise scenarios to the incident response playbook and mobile threat monitoring.