iPhone spyware is YOUR problem now

- Sam Sabin

Cybercriminal groups are now using spyware tools once utilized mainly by spies and law enforcement to hack into iPhones, new research shows.

Why it matters: Anyone with an iPhone can now be the target of invasive malware that siphons off personal text messages, photos, notes and calendar data.

Driving the news: In the last month, researchers at Google, iVerify and Lookout uncovered two campaigns exploiting iPhone vulnerabilities.

- Earlier this month, Google researchers said they identified a sophisticated iPhone hacking toolkit, called Coruna, originally built for an unnamed government customer that later ended up in the hands of a Chinese cybercriminal group. TechCrunch later reported that defense contractor L3Harris created the spyware for the U.S. government.
- Hackers deployed Coruna on fake Chinese-language crypto and financial platforms, infecting vulnerable iPhones that visited the sites — no clicks or downloads required.
- On the same server, researchers said Wednesday they found another iPhone hacking kit, dubbed DarkSword, that can instantly infect iPhones visiting a

specific set of websites, including Ukrainian news and government sites, as part of a so-called "watering hole attack."

Zoom in: Researchers have linked DarkSword to a Russian-based hacking group, though it's unclear whether the group is tied to a government agency or a proxy cybercriminal gang.

- Once on a device, DarkSword exfiltrates nearly everything, including messages sent from iMessage, WhatsApp and Telegram, location data, phone contacts, call histories, WiFi configurations, browser history and cookies, according to iVerify.

- Although DarkSword itself was targeting visitors to Ukrainian websites, Lookout researchers say its developers left the underlying JavaScript code on the server unobscured, meaning even low-level cybercriminals could copy and reuse the tool for a broader range of targets.

Yes, but: Apple spokesperson Sarah O'Rourke said that the company has already patched the underlying iOS vulnerabilities that the spyware targets through new versions of iOS in recent years.

- Apple also rolled out an emergency software update last week for older devices that aren't able to download newer version of the operating system.

- Apple's Safari is now blocking the malicious URL domains identified in Google's research, she added.

Threat level: Replicating or acquiring these tools, built on rare and highly valuable iPhone vulnerabilities, was once limited to well-funded government customers.

- State actors have used such tools to monitor activists, journalists and foreign politicians.

- Now, cybercriminals can get their hands on them, lowering the barrier to launching these kinds of attacks and widening the range of potential targets.

- "With the huge influx of investment in commercial spyware vendors, an ecosystem has been created around mobile exploitation that makes these tools, frankly, abundant," Rocky Cole, iVerify's co-founder and COO, told Axios.

The big picture: Apple has long marketed iPhones as highly secure devices, attracting users who prioritize privacy or need to protect sensitive communications.

- But the recent research suggests the devices might not be as secure as once thought, Cole said. "Every single iPhone user has to worry about this now."

- O'Rourke, the Apple spokesperson, said that Apple devices are designed with "multiple layers of security in order to protect against a wide range of potential threats," and that "Apple's security teams around the world work tirelessly to protect users' devices and data."

The intrigue: Justin Albrecht, Lookout's global director of mobile threat intelligence, told Axios the actors behind DarkSword likely used a large language model to help develop parts of their hacking kit, based on how some files are named.

- Inside the code used for data exfiltration, one file was simply labeled "DarkSword file receiver," he said.

- "No one who's doing any kind of (offensive security) would leave that up there with that name," Albrecht said. "I'm not convinced that this group is even very technically capable."

The bottom line: Lockdown Mode, Apple's security mode for preventing spyware infections, would have prevented just parts of the DarkSword exploit, according to iVerify, and all of Coruna, which is designed to halt if Lockdown Mode is enabled.

- While there's no foolproof defense against these watering hole attacks, Albrecht recommends keeping devices updated, enabling Lockdown Mode and using third-party mobile security tools.

- "Those are great steps you can take, but unfortunately, there's very little that you can do as a user even to detect it," he said.

Go deeper: Researchers uncover possible iPhone spyware campaign inside U.S.