Russia-aligned hackers are targeting Signal users with device-linking QR codes



Signal, as an encrypted messaging app and protocol, remains relatively secure. But Signal's growing popularity as a tool to circumvent surveillance has led agents affiliated with Russia to try to manipulate the app's users into surreptitiously linking their devices, according to Google's Threat Intelligence Group.

While Russia's continued invasion of Ukraine is likely driving the country's desire to work around Signal's encryption, "We anticipate the tactics and methods used to target Signal will grow in prevalence in the near-term and proliferate to additional threat actors and regions outside the Ukrainian theater of war," writes Dan Black at Google's Threat Intelligence blog.

There was no mention of a Signal vulnerability in the report. Nearly all secure platforms can be overcome by some form of

social engineering. Microsoft 365 accounts were recently revealed to be the target of “device code flow” OAuth phishing by Russia-related threat actors. Google notes that the latest versions of Signal include features designed to protect against these phishing campaigns.

The primary attack channel is Signal’s “linked devices” feature, which allows one Signal account to be used on multiple devices, like a mobile device, desktop computer, and tablet. Linking typically occurs through a QR code prepared by Signal. Malicious “linking” QR codes have been posted by Russia-aligned actors, masquerading as group invites, security alerts, or even “specialized applications used by the Ukrainian military,” according to Google.

Apt44, a Russian state hacking group within that state’s military intelligence, GRU, has also worked to enable Russian invasion forces to link Signal accounts on devices captured on the battlefront for future exploitation, Google claims.

https://arstechnica.com/information-technology/2025/02/russia-aligned-hackers-are-targeting-signal-users-with-device-linking-qr-codes/