Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:46:28 UTC

Description(Citizen Lab) Israel-based “Cyber Warfare” vendor NSO Group produces and sells a mobile phone spyware suite called Pegasus. To monitor a target, a government operator of Pegasus must convince the target to click on a specially crafted exploit link, which, when clicked, delivers a chain of zero-day exploits to penetrate security features on the phone and installs Pegasus without the user’s knowledge or permission. Once the phone is exploited and Pegasus is installed, it begins contacting the operator’s command and control (C&C) servers to receive and execute operators’ commands, and send back the target’s private data, including passwords, contact lists, calendar events, text messages, and live voice calls from popular mobile messaging apps. The operator can even turn on the phone’s camera and microphone to capture activity in the phone’s vicinity.

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ff64b1c1-6846-4f3f-9dae-0e23f866299e