8.0 Spyware

Commercial spyware[61] is a form of malware that is designed to steal confidential data from the device or appliance it is running on or to access real-time service on the device. Commercial spyware can be used to access a range of personal information and other data to enable threat actors to gain unauthorised access to the services that these credentials are intended to protect. For example, mobile device spyware can steal location data, which then enables tracking of device user location and movement.

This topic was explored in the 2023 GSMA Mobile Telecommunications Security Landscape report and the past year has seen a continuation of this attack type[62]. Spyware has, again, been seen to be deployed against political targets, as reported[63] when an Egyptian presidential candidate was targeted with Cytrox's Predator spyware via links sent on SMS and WhatsApp. This attack reportedly also involved the mobile connection being persistently selected for targeting via network injection attacks (a method to deploy malware including spyware).

Separately, it was reported[64] that at least five civil society victims of QuaDream's spyware had been identified in North America, Central Asia, Southeast Asia, Europe, and the Middle East. The victims included journalists, political opposition figures, and a Non-Governmental Organisation (NGO) worker. Spyware masquerading as modified versions of Telegram have been reportedly[65] identified in the Google Play Store and have been downloaded millions of times. The apps have since been removed by Google. The package name associated with the Play Store version of Telegram is "org.telegram.messenger," whereas the package name for the file directly downloaded from Telegram's website is "org.telegram.messenger.web." The use of "wab" "wcb" and "wob" for the malicious package names highlights typo squatting techniques to fraudulently position the application as the legitimate Telegram app.

Analysis

A range of national and regional responses have been taken including a joint declaration[66] by the governments of Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States, recognising the threat posed by the use of commercial spyware and the need for strict domestic and international controls on its proliferation and use. The EU's PEGA Committee concluded its spyware investigation[67] and identified eight recommendations[68] (including revoking the licenses of (2G – 5G) service providers found to be facilitating unlawful access to mobile signalling infrastructure and regulating the processes through which malicious actors can create new phone numbers).

[61] Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware | Australian Government Department of Foreign Affairs and Trade (dfat.gov.au)
[62] https://www.brusselstimes.com/729331/european-parliament-president-targeted-by-predator-spyware
[63] https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/
[64] Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers - The Citizen Lab
[65] Millions Infected by Spyware Hidden in Fake Telegram Apps on Google Play (thehackernews.com)
[66] Efforts to counter the proliferation and misuse of commercial spyware: joint statement - GOV.UK (www.gov.uk)
[67] EUROPEAN PARLIAMENT DRAFT RECOMMENDATION TO THE COUNCIL AND THE COMMISSION following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware | B9-0260/2023 | European Parliament (europa.eu)
[68] EU's PEGA Committee Adopts 8 Recommendations on Telecom Networks | Enea

Investigations by journalists and Google's Threat Assessment Group[69] (TAG) have also assisted in identifying and constraining this threat.

This is an ongoing threat that significantly impacts device user privacy and even individuals' personal safety if they are targeted. Whilst it is challenging for the mobile industry to respond to the most sophisticated attacks, GSMA and industry activity is focused on the underlying security arrangements in order to make mobile networks hostile environments for threat actors to operate within (as outlined in the mobile app security, malware and ransomware sections of this report). The supporting security controls and approaches described therein can deliver wide-ranging and enduring operational security benefits to counter the spyware threat.

[69] E.g. https://blog.google/threat-analysis-group/0-days-exploited-by-commercial-surveillance-vendor-in-egypt/