Government hackers targeted iPhones with zero-day vulnerabilities: Google

February 13, 2024

Online Desk: Government hackers exploited three undisclosed vulnerabilities in iPhone operating systems last year, according to a recent report by Google. As per the report, these vulnerabilities were used to deploy spyware and leveraged ‘zero-day’ vulnerabilities in iPhone unknown to Apple.

Google’s Threat Analysis Group, responsible for investigating state-sponsored hacking, released a report last week which examined that several government campaigns are employing hacking tools from various spyware and exploit vendors, including Variston, a startup based in Barcelona.

In a campaign highlighted by Google, government hackers leveraged three iPhone ‘zero-days’, which are vulnerabilities unknown to Apple when exploited. Variston’s hacking tools were used in this instance, with Google identifying an unknown Variston customer utilising these zero-days in March 2023 to target iPhones in Indonesia. The attack method involved sending an SMS text message containing a malicious link, infecting the victim’s phone with spyware, and redirecting them to a news article by the Indonesian newspaper Pikiran Rakyat.

However, Google did not disclose the identity of Variston’s government client in this case.

The recipients of Variston’s spyware remain unknown. According to Google, Variston collaborates with several organisations in developing and delivering spyware. One such organisation mentioned by Google is Protected AE, based in the United Arab Emirates, described as a cybersecurity and forensic company on its website.

Google’s report sheds light on the expansion of European spyware manufacturers, alongside Israeli counterparts like NSO Group, Candiru, and Quadream. Around 40 spyware makers are tracked by Google researchers, including Italian companies Cy4Gate, RCS Lab, and Negg. RCS Lab, for example, transitioned from selling products for traditional phone wiretapping to developing spyware in recent years.

Google emphasises its commitment to disrupting hacking campaigns associated with these companies’ tools, as they have been implicated in targeted surveillance of journalists, dissidents, and politicians.