Source : www.thehindu.com Date : 2023-11-02

MALWARE MALICE: THE HINDU EDITORIAL ON THE APPLE CYBERATTACK ALERT

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

November 02, 2023 12:30 am | Updated 12:30 am IST

In a thriving democracy, the Opposition and the press are vital components of a structure controlled by a ruling establishment that requires accountability for it to be effective. That over a dozen Opposition leaders and journalists received email alerts from Apple that their devices were targeted by “state-sponsored attackers” suggests that this could be a repeat of what these members of the first and fourth estate went through in the Pegasus episode recently. In early 2022, an article in The New York Times detailed how Pegasus, a spyware developed by the Israel-based NSO Group, was used as a tool to advance Israeli interests, as Tel Aviv offered it to other countries which used it against Opposition leaders, journalists and dissidents. In July 2021, a reporters’ consortium, the Pegasus Project, found that at least 40 journalists, cabinet Ministers and other officials in India were possibly subject to surveillance using Pegasus software. A Supreme Court of India panel, however, found no conclusive evidence of the spyware on the 29 phones that it had examined; but the apex court also noted, tellingly, that the Union government was not cooperating with the panel. Unlike the Indian government’s lackadaisical and dismissive approach towards the NSO group and its products — which The NYT reported as allegedly bought by the Indian government from Israel as part of a $2 billion package including sophisticated weapons and intelligence gear in 2017 — other governments in the West implemented stringent steps following the disclosures on spyware use.

Apple’s iPhones are used by nearly 20% of smartphone users worldwide, and by nearly 7% of such users in India, largely for their diverse facilities and robust security provisions. Researchers had found that spyware software such as Pegasus had targeted iPhones and the operating system iOS as early as 2016, and Apple had come up with updates to fix Pegasus exploits, besides going on to sue NSO. The company clarified that the alerts sent now did not accuse a “specific state actor”; it also said that it would not be able to disclose how the targets were discovered, but reiterated that the alerts had to be taken seriously. Yet, with the specific targets being Opposition leaders and journalists, the question whether it is the ruling establishment that is subjecting them to surveillance is important. This can only be verified by an independent and empowered investigation, involving the apex court again, which should, this time around, compel the Union government to cooperate. More immediately, the government must come clean on its dealings with NSO and its use of software provided by such agencies and also emulate steps taken by other governments in proscribing such entities.

SHARE

democracy / Israel / technology (general) / mobile phones / politics / Pegasus surveillance / USA / United Kingdom / espionage and intelligence / government / France

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END