Digital Forensics Show S.A.R. Geelani's Phone Was Hacked, Likely With Zero-Click Exploit

thewire.in/rights/sar-geelani-pegasus-spyware-phone-messages

S.A.R. Geelani. Photo: Twitter

Rights

Potential target for surveillance was 'Committee for the Release of Political Prisoners', with the phone numbers of scholars and activists also appearing in leaked list.

Sukanya Shantha

Government

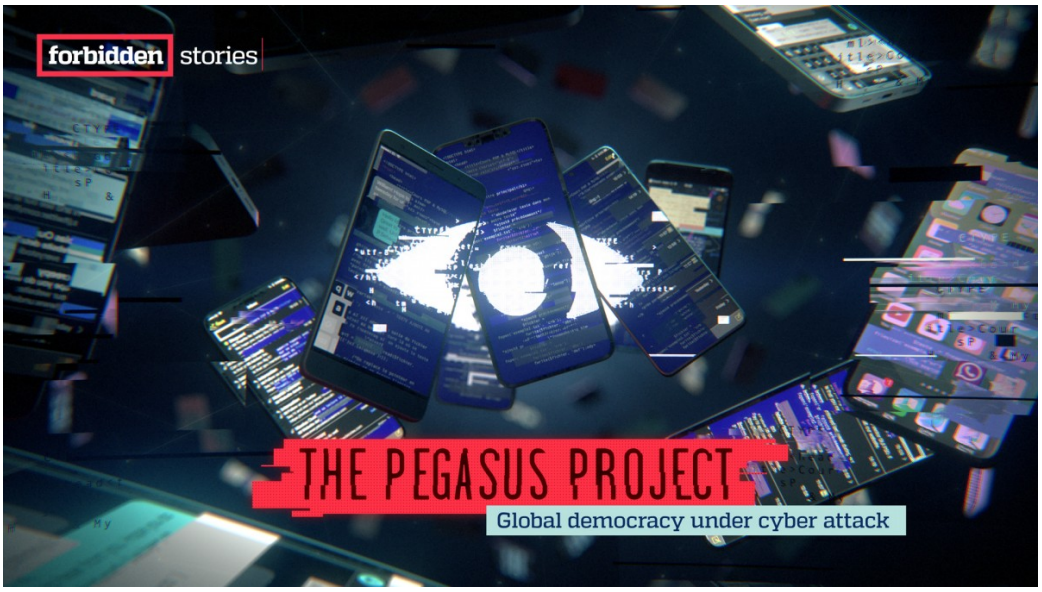
Rights

Tech

18/Jul/2021

Mumbai: Sometime in mid-2017, former Delhi University professor Syed Abdul Rahman Geelani received a barrage of SMSes on his mobile phone. "*United Nations launches online portal for the independence of Kashmir*," read one.

Another message, a few days later, claimed: "*Another incident showing Indian army beating librandu Kashmiri youth mercilessly to chant Pakistan Murdabad*."



There were several more – all unique, tailor-made messages, specifically designed to capture Geelani's attention – sent from what looked like an international number.

Geelani's number, selected as a target for hacking by an government client of Israel's NSO Group, was infected between 2017 and 2019, according to the results of an independent digital forensics study conducted on his phone in the last month.

Amnesty International's Security Lab carried out a forensic analysis of Geelani's phone, an iPhone still preserved by his family, the results of which the organsation say confirm that the phone was compromised on and off for over two years.

Geelani's phone was infected with Pegasus spyware – the Tel Aviv-based firm's flagship product, which allows operators of the tool to gain unauthorised access to a user's mobile device and functions.

It's unclear if the SMS-based attacks worked, but specific forensic analysis conducted by Amnesty International's Security Lab show that the phone was compromised by Pegasus on and off between February 2018 and January 2019, and then again from September 2019 to October 2019. At least one of these attacks, Amnesty notes, was carried out through a zero-click iMessage exploit.

Also read: FAQ: On the Pegasus Project's Digital Forensics

The France-based media non-profit, Forbidden Stories, and Amnesty International's Security Lab gained access to these records, which they shared with *The Wire* and 15 other news organisations worldwide as part of a collaborative investigation and reporting project.

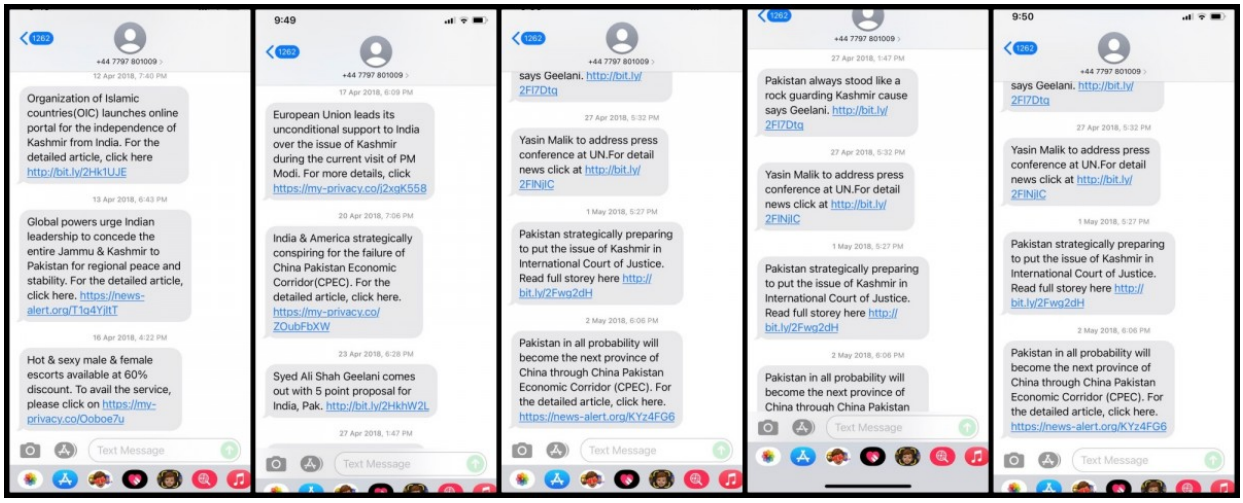
Geelani, who used to teach Arabic at Delhi University's Zakir Hussain College, was arrested in connection with the parliament attack case but was later acquitted for "want of evidence" by the Delhi high court in October 2003, a decision later upheld by the Supreme Court in August 2005.

Geelani, who had garnered massive support at the time of his incarceration, dedicated his life to working for those jailed, especially for their political views. He, along with his friend Rona Wilson – named as a prime accused in the 2018 Elgar Parishad case – founded the Committee for Release of Political Prisoners (CRPP). Associated with several causes relating to human rights violations across the country, Geelani later became a core part of the 17-member Committee for Defence and Release of G.N. Saibaba.

Saibaba, a Delhi University professor, was sentenced to life under several sections of the Unlawful Activities (Prevention) Act (UAPA) for his alleged links with a banned Maoist organisation. With over 90% physical disability, Saibaba has faced severe hardships in jail but been denied bail multiple times both by the lower and higher judiciary.

Also read: Old RTI Response Enough To Deny Govt-Pegasus Link, Media Didn't Do Due Diligence: MeitY

Geelani's son Sayed Atif Geelani, a Delhi-based lawyer, who had preserved the phone even after his father's death in October 2019, told *The Wire* that the forensic report has only confirmed the fears they had lived under for decades. "We have always feared that the family is being tracked. For months after his (Geelani's) death, his phone would notify us about attempts made to hack into his email and phone. This forensic result has only confirmed our suspicion," Atif said.



Screenshots of malware-laden messages sent to S.A.R. Geelani's iPhone. He was one of the initial victims of the Pegasus attack.

Besides Geelani, the leaked data has also thrown up the numbers of nine more members and close supporters of the Saibaba Defence Committee.

Wilson and his co-accused in the Elgar Parishad case and an associate professor from Delhi University, Hany Babu, were also on the list. Hany Babu was also a core team member of both CRPP and the Saibaba Defence Committee; he mainly handled the press releases and his email ID and phone numbers were usually printed on the press statements.

Other members or close supporters of the Saibaba Defence Committee and CRPP to be selected as potential targets were retired professor G. Haragopal, chairman of the Defence Committee, Saroj Giri and Rakesh Ranjan, both assistant professors in Delhi University who would regularly attend solidarity meetings, Saibaba's wife Vasantha Kumari and two other academics who did not wish to be named from Delhi.

To be clear, it is not possible to know whether the phones of Babu, Wilson and other members of the committee saw attempted targeting or were compromised by an infection without digital forensic analysis.

The Wire had arranged for a forensic analysis of Haragopal's Android phone devices. However, the results were inconclusive because unlike iPhones, Androids do not log the kind of information needed for Amnesty's technical investigation.

While the Saibaba Defence Committee is a separate entity, many associated with it have been questioned by the National Investigating Agency in the Elgar Parishad case too. Atif told *The Wire* that the family had feared Geelani's arrest in the Elgar Parishad case. "If my father hadn't died in October, we are pretty certain that they would have found a way to implicate him too in the case," claimed Atif.

Also read: Read: NSO Group's Response to the Pegasus Project and Our Take

Vasantha said the period of surveillance overlaps with many significant meetings and protests organised across India demanding Saibaba's release. "Soon after Saibaba's conviction, the Defence Committee had organised several meetings across different cities. The activities were all in the public domain, with press statements published regularly on different social media platforms," she said.

Vasantha was not surprised that she was also one of the potential targets of Pegasus. "I have been facing threats and intimidation ever since Saibaba was falsely charged in 2014 and I began participating in public meetings and speaking against his false arrest and later his conviction. This is an extension of the targeted harassment I have been enduring over the past decade," she added.

Hany Babu's wife Jenny Rowena, also an associate professor at DU's Miranda College, feels that her husband came to be targeted because of his identity. "He is a Muslim man, an OBC (Other Backward Classes) and spoke against the state machinery for criminalising people from similar marginalised identities."

Ranjan and Giri told to *The Wire* that although they weren't office-bearers of the committee, they would participate in meetings regularly. "Saibaba's arrest and conviction was widely opposed. Like most others, I too would participate in those meetings regularly," Ranjan confirmed.

Giri said his long association with both Saibaba and Wilson may have made him a target. "I have been an integral to the committee which has been demanding his release. In the last few years, I have tried to mobilise support for the incarcerated DU professor G.N. Saibaba," he told *The Wire*. When Saibaba's house was raided twice before his arrest his 2014, Giri was by his side, defending and mobilising people against the arrest. Later when Saibaba was out on bail, Giri says, he would take him to the hospital many times. "His condition was critical then. I would travel with him to hospitals regularly."

Read The Wire's coverage as part of the Pegasus Project here.