www.washingtonpost.com /world/2022/02/10/bhima-koregaon-india-sentinelone/

Indian activist charged with terrorism was targeted by hackers linked to prominent cyber espionage attacks, new report finds

Niha Masih, Gerry Shih ⋮⋮ 2/10/2022

NEW DELHI — In early 2021, India was jolted by revelations that a jailed human rights activist and vocal government critic was targeted by hackers who planted incriminating evidence on his laptop before he was arrested on terrorism charges.

Now, a year later, a report by U.S. experts says the activist, Rona Wilson, was targeted by two separate groups, including one group that has been linked to widely documented cyberespionage campaigns against military targets in China and Pakistan, India's top foreign adversaries.

The report notes that the other group, responsible for planting documents on the activist's device, dubbed ModifiedElephant by SentinelOne, shared hacking infrastructure with an attacker that researchers have long suspected of state-sanctioned political espionage.

The findings, published in a report by the California-based cybersecurity firm SentinelOne, shed light on what amounted to a concerted, nearly decade-long effort to surveil a group of dissidents. It also offers new clues about the connections between groups that cybersecurity experts have observed targeting foreign adversaries and domestic critics.

The report does not identify the people who carried out the attacks or the entity that ordered them but notes that ModifiedElephant's activity "aligns with Indian state interests."

"Two separate groups going after the same target suggests they were tasked with the job by the same entity," said Juan Andres Guerrero-Saade, a principal threat researcher and co-author of the SentinelOne report.

According to SentinelOne researchers, Wilson received dozens of emails — often from other activists he knew and sometimes disguised as news articles — that contained malware designed to infiltrate his computer.

The Washington Post reported in April on a separate forensic analysis that found that, years before his arrest, an unknown hacker compromised Wilson's computer and planted at least 32 documents, including a letter discussing a plot to assassinate Prime Minister Narendra Modi that authorities have cited as evidence against him.

SentinelOne found that ModifiedElephant shared web domains with a hacking group known as Hangover. SentinelOne's research built on a 2013 report that found Hangover had attacked commercial businesses and national security interests in Europe, the United States and Pakistan.

The SentinelOne report identified the second group targeting Wilson as SideWinder, a group that is well known to international cybersecurity researchers who have tracked its operations against government and military targets in Pakistan and China.

Three independent experts in the United States and Europe reviewed the SentinelOne report at The Post's request and concurred with its conclusions.

The new findings suggest Wilson, a 50-year-old human rights activist awaiting trial in a jail outside Mumbai, was the target of an extensive cyberattack campaign that involved more than one hacker and spanned nearly a decade, a longer time frame than previously known.

India's National Investigation Agency, the prosecuting authority in the case, did not respond to a request for comment.

Wilson's case has sparked controversy in India at a time when Modi's government is battling allegations of hacking and surveillance of its opponents.

Last year, an investigation by a global consortium including The Post revealed that hundreds of phone numbers from India appeared on a global list that included some numbers selected for surveillance by NSO Group's clients using its Pegasus tool, which is licensed only to government agencies. Those on the list included Indian activists, journalists and opposition party leaders.

The Indian government has neither confirmed nor denied that it is an NSO client. In December, Amnesty International said a forensic analysis of a backup of Wilson's iPhone 6s found traces of Pegasus spyware.

Wilson was arrested in 2018 along with lawyers and academics in what is known as the Bhima Koregaon case, which began as an investigation into a violent clash between Hindu nationalists and Dalits, formerly known as "untouchables." Prosecutors charged Wilson and 15 others under an anti-terrorism law, alleging they had ties with a banned Maoist militant group, charges they deny.

U.N. experts have called on the Modi government to release the defendants. Last July, one of the defendants, an 84-year-old Jesuit priest, died in a hospital after his health deteriorated in jail.

Last year, Arsenal Consulting, a Massachusetts-based digital forensics firm, found that the computers of Wilson and a co-defendant, lawyer Surendra Gadling, had been hacked by an attacker that planted dozens of documents on them, later cited by prosecutors as evidence. Arsenal analyzed electronic copies of their computers at the request of the defense team and worked pro bono.

SentinelOne's report takes the findings further.

ModifiedElephant, the main hacker, sent emails with documents or attachments — laden with commercially available malware like NetWire and DarkComet — that were tailored to the victim's interests and were often copied to multiple recipients they knew, SentinelOne said. Wilson received at least 32 emails from ModifiedElephant, and Gadling was the recipient of 40 such mails from the group.

Dozens of other members of civil society, including other co-defendants, were also targeted by ModifiedElephant, though it is not known how many were successfully infiltrated.

SentinelOne based its research on an analysis of Arsenal's findings, malware infrastructure and more than 100 phishing emails received by Wilson and his co-defendants. SentinelOne requested the emails from the defense team and conducted the work pro bono.

The researchers said the earliest attack on Wilson can be traced back to a decade ago, though the email attacks intensified in 2014 and continued until at least 2016.

The phishing emails were traced to two distinct groups that sent messages from free services such as Gmail and Yahoo around the same time. Besides ModifiedElephant, SideWinder, a group that typically attacks foreign targets and has been tracked for years by international researchers, sent at least four malicious emails to Wilson between 2013 and 2014. It is unknown whether the SideWinder attacks were successful.

In 2019, the Pakistani government issued an advisory detailing attacks on its defense and government offices by SideWinder and calling it an Indian attacker.

SentinelOne identified the two groups by tracking the Web domains associated with the emails.

The report also found evidence that links ModifiedElephant to Hangover.

At least two web domains used by ModifiedElephant for sending phishing emails to Wilson were linked to Hangover, suggesting an overlap between the two groups, SentinelOne said. Hangover was accused of attacking Norway's state-owned telecom company in 2013.

Snorre Fagerland, a Norwegian cybersecurity researcher who co-wrote a 2013 report on Hangover, said the newest details about the campaign against Wilson contribute to a better understanding of the ties between attackers who may be operating in India and targeting foreign adversaries and domestic dissidents alike.

"It's safe to say that we have learned a lot over the last decade," Fagerland said, "not only about the methods, but also about targeting and how the Indian advanced persistent threat ecosystem works."