Interview

Anywhere You Look, Civil Rights Activists Are Surveilled, Says Citizen Lab Researcher

John Scott-Railton, a senior researcher at the University of Toronto's Citizen Lab, spoke to Calcalist about his work with WhatsApp to uncover NSO Group's alleged hack of its servers

Omer Kabir 10:46 05.11.19

TAGS: NSO Citizen Lab Surveillance Cyber

John Scott-Railton, a senior researcher at the University of Toronto's Citizen Lab, a digital and human rights research group focused on cyber-surveillance, has been monitoring NSO Group for years. He and his colleagues tenaciously published reports about the company's surveillance technology and the way it was used to spy on human rights activists, political opposition members, and journalists. But while these reports made some headlines, not much has changed, and NSO kept on operating unchecked.

All that changed last week, when it came out that encrypted messaging app WhatsApp and its parent company Facebook were suing NSO and its Luxembourg-based affiliate Q Cyber Technologies Ltd. The media giant is alleging that NSO used WhatsApp servers to deliver malware to approximately 1,400 devices for the purpose of monitoring certain Whatsapp users.

John Scott-Railton. Photo: PR

Until now, spyware companies had succeeded in blocking the attempts humans rights organizations made to curb them, even working within the legal system, Scott-Railton said in a recent interview with Calcalist. "But now things have been turned around."

Scott-Railton was a member of the Citizen Lab team that helped Facebook investigate NSO's hack and identify its victims. After the matter was first reported by the Financial Times in May, Citizen Lab volunteered to help WhatsApp investigate, eventually uncovering at least 100 cases in 20 countries where civil activists were targeted for reasons unrelated to law enforcement, he said.

Among the targets uncovered were journalists, well-known news anchors, academics, political opposition members, civil rights lawyers, prominent women who were victims of online violence, and religious leaders of different faiths, Scott-Railton said. In some cases, the people targeted by NSO's malware were also the target of assassination attempts or the family members of people who were assassinated.

NSO has consistently responded to criticism by saying that it sells its technology only to governments and law enforcement agencies and that its ethical code prohibits using the technology to track human rights activists. According to Scott-Railton, this is a well-known tactic of surveillance companies, who want the prestige of working with governments but not the responsibility that comes with providing them with such destructive tools. The WhatsApp lawsuit, he said, pops that bubble by making it clear that NSO is not as removed from the implementation of its technology as it portrays itself to be, and that it should be made to bear responsibility. It is a precedent case, he added.

Citizen Lab has been tracking digital threats for over 15 years, focusing primarily on the Chinese regime and its actions against the Tibetian people and other ethnic minorities. In recent years, the research lab has documented a growing phenomenon, which saw certain governments who are unable to develop their own surveillance technology buy it instead from private cyber companies, Scott-Railton explained. Citizen Lab performed extensive research to understand the scope of the issue, and realized that no matter where they looked, there was action carried out against civil activists, Scott-Railton said.

Groups like NSO justify their technology by saying law enforcement uses it for legitimate investigation against unlawful or immoral groups, but there is a third side, Scott-Railton said: countries that use the technology to spy on other countries. The question is not whether we can accept that a technology used for legitimate purposes will also be used, in some cases, for illegitimate purposes, but rather how the ability of a growing number of countries to use sophisticated surveillance tools against whoever they want harms global cybersecurity, he said.

For years, people had been victimized by NSO's spyware and their testimonies had been played down, Scott-Railton said. Following NSO's self-acquisition earlier this year, the company ran a campaign promising it is turning over a new leaf. Any misuse of the technology, if it existed at all, would no longer be allowed to take place. But the WhatsApp hack makes it clear that not only is the problematic use of NSO's technology far from being eliminated, it is a daily occurrence, Scott-Railton said. The lawsuit in itself is a win for human and privacy rights, he said, as it is clear that the industry is unwilling and incapable of policing itself.

Related stories:

- NSO Spyware Used to Target Moroccan Human Rights Activists, Says Amnesty
- NSO Denies Using WhatsApp to Infect Hundreds of Users With Surveillance Malware
- Self Probe Won't Cut it for Israeli Spyware Company NSO, Says Citizen Lab Researcher

There is a certain irony in the fact that Facebook, which has faced continued criticism over its use of personal data, is now leading the charge against NSO. People should always ask themselves if a company is working for their benefit, is Scott-Railton's opinion. Facebook aside, WhatsApp integrated encryption technology into its product, and in this case is not just saying it is taking action to protect users, but actively taking the matter to court, he said.

Companies like Facebook have mechanisms in place that enable governments and law enforcement agencies to file for information in legitimate ways, Scott-Railton explained. In this case, those mechanisms were passed over in the quest for information. Bottom line, it is clear that governments use NSO's technology not just for the purposes the group writes on its charter. Even if the technology is used for legitimate purposes like catching criminals, the concern of the court is whether the law has been broken to do so, he said. "And according to WhatsApp, NSO's conduct violated the law."

One Comment

Write Comment

1. **our moral police**
   David Frank, (06.11.19)

Buzz

The truth behind the Lemonade surge, America's most successful IPO of 2020

05.07.2020 Sophie Shulman

Israeli autonomous vehicle startup VayaVision acquired by Canada's LeddarTech

07.07.2020 Hagar Ravet

AI cancer treatment startup Nucleai raises $6.5 million in series A round

07.07.2020 Meir Orbach

Next Food aiming for $7.5 million in first-of-its-kind IPO

05.07.2020 Meir Orbach

Co-living is wasted on the youth, Israeli startup Willa is offering urban living for midlifers

05.07.2020 Ron Friedman

Software giant Amdocs set to lay off 1,000 employees

02.07.2020 Meir Orbach