Togo: Prominent activist targeted with Indian-made spyware linked to notorious hacker group

Published: 2021-10-07 · Archived: 2026-04-05 16:39:04 UTC

- Togolese activist targeted with spyware by the Donot Team hacker group.
- Amnesty International exposes links between the Donot Team attacks and Innefu Labs, a cybersecurity company based in India.
- First time Donot Team publicly linked to cyberattacks targeting activists outside of South Asia.
- Spyware-loaded emails and fake Android applications could access device's camera and microphone, steal photos and files, and read WhatsApp messages.

Activists in Togo risk being targeted by shadowy cyber-mercenaries who use covert digital attacks to try and steal victims' private information to sell to private clients, a new Amnesty International investigation has uncovered.

In a new report released today, Amnesty International reveals how fake Android applications and spyware-loaded emails tied to the notorious Donot Team hacker group were used to target a prominent Togolese human rights defender in an attempt to put them under unlawful surveillance. The discovery is the first time Donot Team spyware was found in attacks outside of South Asia. The investigation also discovered links between the spyware and infrastructure used in these attacks, and Innefu Labs, a cybersecurity company based in India.

> Across the world, cyber-mercenaries are unscrupulously cashing in on the unlawful surveillance of human rights defenders
>
> *Danna Ingleton, Deputy Director of Amnesty Tech*

The Togolese activist, who wishes to remain anonymous for security reasons, has a history of working with civil society organizations and is an essential voice for human rights in the country. Their devices were targeted between December 2019 and January 2020, during a tense political climate ahead of the 2020 Togolese presidential election.

"Across the world, cyber-mercenaries are unscrupulously cashing in on the unlawful surveillance of human rights defenders," said Danna Ingleton, Deputy Director of Amnesty Tech.

"Anyone can be a target – attackers living hundreds of miles away can hack your phone or computer, watch where you go and who you talk to, and sell your private information to repressive governments and criminals."

The persistent attacks over WhatsApp and email tried to trick the victim into installing a malicious application that masqueraded as a secure chat application. The application was in fact a piece of custom Android spyware designed to extract some of the most sensitive and personal information stored on the activist's phone.

The spyware would have enabled attackers to access the camera and microphone, collect photos and files stored on the device, and even read encrypted WhatsApp messages as they are being sent and received. The covert nature of such attacks makes it extremely difficult for activists to detect whether their devices have been compromised.

“Having realized that this was an attempt at digital espionage, I felt in danger. I can’t believe that my work could be so disturbing to some people that they would try to spy on me. I am not the only one working for human rights in Togo. Why me?”, the Togo-based human rights defender told Amnesty International.

Amnesty International’s investigation uncovered a trail of technical evidence left by the attackers which identified links between the attack infrastructure and an Indian-based, Innefu Labs. The company which advertises digital security, data analytics, and predictive policing services to law enforcement and armed forces and claims to work with the Indian government. Innefu Labs does not have a human rights policy and does not appear to carry out human rights due diligence – despite the enormous risks their products pose to civil society. Amnesty International has observed additional evidence of Donot Team attacks against organizations and individuals across Asia, mostly concentrated in the north of India, Pakistan and Kashmir.

Activists under attack

The space for human rights work in Togo has been shrinking – in 2019, the year preceding the presidential election, Amnesty International documented the adoption of laws curtailing the rights to freedom of expression and peaceful assembly and cases of human rights violations committed by authorities, particularly against pro-democracy activists.

Several religious and opposition political figures in Togo have reportedly been targeted with digital surveillance tools. In August 2020, The Guardian and Citizen Lab revealed that two Catholic clergy members, Bishop Benoît Alowonou and Father Pierre Chanel Affognon had been targeted using a NSO Group-linked WhatsApp vulnerability.

The Pegasus Project, coordinated by Forbidden Stories with the technical support of Amnesty International’s Security Lab, earlier this year revealed that hundreds of Togolese numbers were listed as potential targets of NSO Group’s Pegasus spyware. Those on the list included independent journalists and members of political opposition groups.

The threat of targeted surveillance, whether real or not, can inflict a huge psychological toll on activists and cause a devastating chilling effect on their human rights work. Little is known about the wild-west cyber surveillance industry, despite Amnesty International’s and other civil society’s repeated requests for more transparency, and even less is known about the flourishing hacker-for-hire industry.

“The surveillance industry is out of control with companies and cyber-mercenaries alike operating entirely in the shadows.”

“Surveillance companies must stop putting profit over people and ensure repressive regimes are not using their technology to put a stranglehold on civil society,” said Danna Ingleton.

Amnesty International is calling on:

- Innefu Labs to publish in full the findings of an external audit the company commissioned into links between its spyware tools and infrastructure used in the attack against the Togo activist. The company must also implement a human rights policy.

- The Indian government to investigate cyberattacks linked to Innefu Labs and take urgent action to ensure India-based surveillance companies are not involved in the targeting of activists – which is unambiguously illegal under international human rights law.
- The Togolese government to ensure that everyone, including activists, is protected from human rights abuses, and to investigate and redress any harm caused by cyberattacks carried out by private sector actors.

In a written response to Amnesty International, Innefu Labs denied "the existence of any link whatsoever between Innefu Labs and the spyware tools associated with the 'Donot Team'" and the attack against the human rights activist in Togo. Innefu Labs also stated that they are not aware of any use of their IP address for the alleged activities.

There is no evidence to suggest Innefu Labs had a direct involvement or knowledge of the targeting of the human rights defender in Togo using the Donot Team spyware tools. The activity linked to the Donot Team may involve multiple distinct actors or organisations with access to the same custom spyware toolset and shared infrastructure.
