Global: ‘Predator Files’ spyware scandal reveals brazen targeting of civil society, politicians and officials - Amnesty International Security Lab

Published: 2023-10-09 · Archived: 2026-04-02 10:43:44 UTC

Shocking spyware attacks have been attempted against civil society, journalists, politicians and academics in the European Union (EU), USA and Asia, according to a major new investigation by Amnesty International. Among the targets of Predator spyware are United Nations (UN) officials, a Senator and Congressman in the USA and even the Presidents of the European Parliament and Taiwan. The investigation is part of the ‘Predator Files’ project, in partnership with the European Investigative Collaborations (EIC) and backed by additional in-depth reporting by Mediapart and Der Spiegel.

Between February and June 2023, social media platforms X (formerly Twitter) and Facebook were used to publicly target at least 50 accounts belonging to 27 individuals and 23 institutions. The cyber-surveillance weapon used for targeting was an invasive spyware tool called Predator, which was developed and sold by the Intellexa alliance. This alliance, which has advertised itself as “EU based and regulated”, is a complex and often changing group of companies that develops and sells surveillance products, including Predator spyware.

Predator is a type of highly invasive spyware. This means that once it has infiltrated a device it has unfettered access to its microphone and camera and all its data such as contacts, messages, photos and videos, while the user is entirely unaware. Such spyware cannot, at present, be independently audited or limited in its functionality to only those functions that are necessary and proportionate to a specific use.

“Yet again, we have evidence of powerful surveillance tools being used in brazen attacks. The targets this time around are journalists in exile, public figures and intergovernmental officials. But let’s make no mistake: the victims are all of us, our societies, good governance and everyone’s human rights,” said Agnes Callamard, Secretary General at Amnesty International.

“The Intellexa alliance, European-based developers of Predator and other surveillance products have done nothing to limit who is able to use this spyware and for what purpose. Instead, they are lining their pockets and ignoring the serious human rights implications at stake. In the wake of this latest scandal, surely the only effective response is for states to impose an immediate worldwide ban on highly invasive spyware.”

In a comprehensive report published today by Amnesty International’s Security Lab, those targeted – though not necessarily infected – include the President of the European Parliament, Roberta Metsola, the President of Taiwan, Tsai Ing-Wen, U.S. Congressman Michael McCaul, U.S. Senator John Hoeven, the German Ambassador to the United States, Emily Haber and French MEP Pierre Karleskind. Multiple officials, academics and institutions were also targeted.

A brazen barrage of attacks

Amnesty International's Security Lab has been investigating the use of the powerful and highly invasive Predator spyware and its link to the Intellexa alliance for some time.

An attacker-controlled X (previously Twitter) account, named '@Joseph_Gordon16′, shared many of the identified attack links which aimed to infect targets with the Predator spyware. One early target of this account was Berlin-based journalist Khoa Lê Trung, who is originally from Viet Nam. Khoa is editor-in-chief of thoibao.de, a news website blocked in Viet Nam. He has faced death threats over his reporting since 2018. Viet Nam has a repressive media landscape where journalists, bloggers and human rights activists are often intimidated into silence.

The attack, though unsuccessful, is especially significant as the website and journalist are based in the EU, and all EU member states have an obligation to control the sale and transfer of surveillance technologies.

"You can't just sell them to countries like Viet Nam. This also harms the freedom of the press and freedom of expression for the people here in Germany," Khoa told Amnesty International.

The investigation found that the @Joseph_Gordon16 account had close links to Viet Nam and may have been acting on behalf of Vietnamese authorities or interest groups.

In April 2023 Amnesty International's Security Lab began to observe the same '@Joseph_Gordon16' user targeting multiple academics and officials working on maritime issues, specifically researchers and officials responsible for EU and UN policies on illegal or undocumented fishing. Viet Nam was given a 'yellow card warning' by the European Commission in 2017 for illegal, unreported, and unregulated fishing.

"We observed dozens of instances in which '@Joseph_Gordon16' pasted a malicious link to Predator in public social media posts. Sometimes the link seemed to be a benign news outlet, such as The South China Morning Post, to lull the reader into clicking on it," said Donncha Ó Cearbhaill, Head of Amnesty International's Security Lab.

"Our analysis demonstrated that clicking the link could lead to the reader's device being infected with Predator. We do not know if any device was infected, and we cannot say with absolute certainty that the perpetrator was within the government of Viet Nam itself, but both the interests of the account and the Viet Nam authorities were very closely aligned."

The investigation also uncovered evidence that a company within the Intellexa alliance signed a multi-million euro deal for "infection solutions" with Viet Nam's Ministry of Public Security (MOPS) in early 2020, codenamed "Angler Fish". Documents and export records also confirmed the sale of Predator to MOPS through broker companies.

"We believe this Predator attack infrastructure is associated with a government actor in Vietnam," Google's security researchers who also independently analysed the malicious links, told Amnesty International.

EU regulated spyware free to run wild across the world

Predator can also be used in zero click attacks, meaning it can infiltrate a device without the user having clicked on a link. This can be done, for example, by so-called "tactical attacks" which can infect nearby devices. Highly

invasive spyware cannot currently be independently audited or limited in its functionality. It is, therefore, exceedingly difficult to investigate abuses linked to its use.

The investigation found the presence of Intellexa alliance products in at least 25 countries across Europe, Asia, the Middle East and Africa, and documents how they have been used to undermine human rights, press freedom, and social movements across the globe.

The Intellexa alliance has corporate entities in various states including France, Germany, Greece, Ireland, Czech Republic, Cyprus, Hungary, Switzerland, Israel, North Macedonia, and the United Arab Emirates (UAE). Amnesty International is calling on all these states to immediately revoke all marketing and export licences issued to the Intellexa alliance. These states must also conduct an independent, impartial, transparent investigation to determine the extent of unlawful targeting.

“Intellexa says it is an ‘EU-based and regulated company which is, in itself, a damning indictment of how EU member states and institutions have failed to prevent the ever-expanding reach of these surveillance products despite a series of investigations such as the ‘Pegasus Project’ in 2021. So much so that, as this investigation highlights, even EU officials and institutions themselves were caught in its net,” said Agnès Callamard, Amnesty International’s Secretary General.

The Predator Files investigation found Intellexa alliance products had been sold to at least 25 countries including Switzerland, Austria and Germany. Other clients include Congo, Jordan, Kenya, Oman, Pakistan, Qatar, Singapore, the UAE and Viet Nam.

The Intellexa alliance should stop the production and sale of Predator and any other similarly invasive spyware that does not include technical safeguards allowing for its lawful use under a human rights respecting regulatory framework. It should also provide adequate compensation or other forms of effective redress to victims of unlawful surveillance.

Amnesty International’s analysis of recent technical infrastructure linked to the Predator spyware system indicates related activity, in one form or another, in Angola, Egypt, Mongolia, Kazakhstan, Indonesia, Madagascar, Sudan and Viet Nam among others. Amnesty International has published indicators of compromise to help civil society technologists identify and respond to this spyware.

Amnesty International reached out to the entities involved for comment but received no response. However, EIC did receive a response from the main shareholders and former executives of Nexa group. In their response they claim that the Intellexa alliance has ceased to exist. In relation to Viet Nam, they claim that Nexa Group only honoured part of the contract related to cybersecurity. They also claim that the entities of Intellexa alliance “scrupulously respected export regulations”, while acknowledging that they established “commercial relations” with countries that ”were far from perfect in terms of the rule of law,” further stating that it was often a function of “political choices” from the French government.

Amnesty International wrote to Viet Nam’s Ministry of Public Security for comment but did not receive a response.

Click here for the ‘The Predator Files: Caught in the Net’ full report.

Amnesty International has also published an in-depth technical analysis of the surveillance products offered by the Intellexa Alliance on 6 October as part of the *'Predator Files'* investigation.
