ESPIONAGE AGAINST THE EUROPEAN PARLIAMENT

Member of Committee Investigating Spyware Hacked with Pegasus

July 3, 2026
Report No. 194

By John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Kate Pundyk, Siena Anstis, and Ron Deibert.

THECITIZENLAB

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

Copyright

Suggested Citation

John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Kate Pundyk, Siena Anstis, and Ron Deibert. “Espionage Against the European Parliament: Member of Committee Investigating Spyware Hacked with Pegasus,” Citizen Lab Report 194, University of Toronto, July 3, 2026.

Acknowledgements

Thanks to Rebekah Brown and Adam Senft for careful review, and to Anna Mackay and Claire Posno for communications and layout support. We are very grateful to Stelios Kouloglou and Thanasis Koukakis for consenting to be named in and participating in this research. Special thanks to Zacharias Kesses and TNG.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is a world-renowned research unit led by Professor Ronald J. Deibert at the University of Toronto's Munk School of Global Affairs & Public Policy. We investigate novel threats to democracy, human rights, and global security in the digital ecosystem. Over the past 25 years, the Citizen Lab's evidence-based research has played a critical role in demonstrating how digital technologies are used to undermine human rights. The Citizen Lab has published more than 180 evidence-based, peer-reviewed research reports, available online.

Contents

Excerpt

We found that former Member of the European Parliament Stelios Kouloglou was hacked with Pegasus spyware while serving on the PEGA committee, which investigated Pegasus and other spyware abuses in Europe. Through forensic analysis of his device, we found that the attackers could have had access to confidential documents and committee deliberations.

Key Findings

- Former Member of the European Parliament, **Stelios Kouloglou**, was repeatedly hacked with NSO Group's Pegasus spyware while on the committee investigating Pegasus spyware abuses.
- Kouloglou was infected during key periods of PEGA committee activity, and the spyware would have likely captured non-public information about committee activities, possibly breaching EU parliamentary confidentiality and privilege frameworks.
- We are not attributing these infections to a particular government at this time, and found no indications that the Greek Government is responsible. Instead, we note an overlap between the first infection and a previously identified Pegasus campaign targeting Russian and Belarusian-speaking exiled journalists and activists in Europe, suggesting a Pegasus customer with authorization to spy in multiple European countries is responsible.

Background

Stelios Kouloglou is a prominent Greek investigative journalist who was elected as a Member of the European Parliament in 2015. He reported for Greek radio and TV from Paris (1983-84), Moscow (1989-93), and Yugoslavia (1992-95). He later founded and reported for Television Without Borders (TVXS) starting in 2008.

Figure 1: Greek journalist and MEP Stelios Kouloglou.

Kouloglou was elected to the European parliament as an independent in the Syriza party's electoral list (affiliated with the Left). He was elected to the next parliamentary term in the 2019 European elections.

Kouloglou was a substitute member of the European Parliament's *Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware* (PEGA Committee) from March 24, 2022 to July 18, 2023. The PEGA Committee was established on March 10, 2022 following the 2021 publication of the Pegasus Project and other reporting which revealed European governments used spyware to surveil journalists, activists, politicians, and other citizens. Led by MEP Sophie in 't Veld, the PEGA Committee was tasked to investigate the scope of spyware usage in contravention of EU law, focusing on "Pegasus and equivalent surveillance spyware."
While sitting as an MEP, Kouloglou continued to write opinion pieces and report for TVXS. He left the Syriza party in October 2023 and sat as an independent until the elections of June 2024, after which he served as a member of the New Left. His parliamentary term ended in July 2024.

Kouloglou Infected with Pegasus Spyware

In May 2026, Kouloglou contacted the Citizen Lab and we conducted a forensic analysis of artifacts from his iPhone. We found with high confidence that his device was successfully infected with Pegasus spyware on or around October 21, 2022, and again on March 6 and 7, 2023.

On 2022-10-21 10:16, there was a lookup for a HomeKit email address **rauharepo888 [@]gmail.com**. Two minutes later, a Pegasus process used mobile data. We assess that the phone was hacked with the ***PWNYOURHOME*** zero-click exploit at this point. PWNYOURHOME appeared to first involve the attacker sending a specially crafted NSKeyedArchive that landed in HomeKit, followed by malicious content that landed in MessagesBlastDoorService. Apple mitigated the first issue with a change to HomeKit in iOS 16.3.1, though we assess that they fixed the MessagesBlastDoorServiceissue earlier, likely in iOS 16.1. We additionally saw Pegasus activity on Kouloglou's device between 2023-03-06 09:49 and 2023-03-07 07:30 that we assess is likely linked to the same exploit. On the 2022 and 2023 dates, we assess that the device was running iOS 15.5 (19F77).

These findings do not preclude the possibility of additional infections that we have been unable to capture due to limitations of available forensic data.

Apple Notifications

Further validating our finding of targeting, our forensic analysis shows Kouloglou received multiple Apple threat notifications about targeting with mercenary spyware on three occasions: March 2, 2023, August 29, 2023, and April 10, 2024. It is important to note that threat notifications from Apple and other companies are not real-time alerts. They are typically sent to users in batches, often months or more after targeting takes place.

Kouloglou reports to us that he did not recall receiving the Apple notifications we observed.

Targeting Context and PEGA Committee Activities

Kouloglou helped the Citizen Lab reconstruct his activities during the periods when he was targeted with Pegasus spyware (see the detailed timeline in the Appendix). Throughout the period under consideration, Kouloglou wrote numerous articles and gave frequent interviews about spyware abuses. We summarize the key contextual details in the following sections.

First Pegasus Infection Period: PEGA Hearing Prep, Country Visits

The date of the first known Pegasus infection of Kouloglou's device – **October 21, 2022** – aligns with a particularly intense period of activity around the PEGA Committee's deliberations and investigations.

First, a series of PEGA Committee hearings were about to commence following the infection date, including "Big Tech and Spyware" (October 26), "Spyware and e-privacy" (October 26), and spyware and fundamental rights (October 27).

Importantly, the PEGA Committee was also in the midst of preparations for the publication of its first draft report. Drafts of the report were being discussed and circulating among PEGA Committee members and their staff in the weeks leading up to this publication. Kouloglou confirms that the first infection date (October 21, 2022) coincided with a period of intense discussion and exchange that primarily took place over text messages and email. The first draft of the PEGA Committee Report was delivered by MEP in 't Veld on November 8, 2022. The draft focused on allegations of spyware in Poland, Hungary, Greece, Cyprus, and Spain.

In addition to the hearing and report drafting, PEGA Committee members had visited several European countries as part of their mission. Throughout October, the PEGA committee was planning its research visits to Greece and Cyprus scheduled for November 1 to 4, 2022. Kouloglou helped with planning and participated in both visits as part of the PEGA Committee deliberations. Kouloglous' device was hacked ten days prior to the start of this trip, at a time when communications were being exchanged about the visits.

Meeting with Thanasis Koukakis

On October 21, 2022, the exact date of the infection, Kouloglou was in the hospital for elective surgery. He was visited in his hospital room by Greek investigative journalist Thanasis Koukakis, who has worked closely on mercenary spyware issues in Greece, and had testified to the PEGA Committee the previous month. In March 2022, the Citizen Lab had confirmed Koukakis was himself targeted with Intellexa's Predator spyware and he was at this time pursuing legal remedies and formal complaints with relevant authorities in Greece about the spying. Koukakis memorialized his meeting with Kouloglou with a photograph (**Figure 2**).

Figure 2: Photograph taken of Stelios Kouloglou by Greek journalist Thanasis Koukakis on the date on which Kouloglou's phone was hacked with Pegasus spyware. Published with the consent of both parties.

Given that the infection took place while Kouloglou was a patient at a Greek hospital, it is possible that confidential medical information could have been intercepted from his device, including discussions going on in his room. If the spyware captured conversations between Kouloglou and medical staff, or details stored on the phone concerning appointments, medical results, diagnoses, and other health related information, then the hacking of his device may implicate Greece's laws concerning confidentiality of health-related data, which are considered a special category of personal data and are subject to enhanced protections (Law 4624/2019 under the Greek Penal Code).

Second Pegasus Infection Period: Intense PEGA Deliberations

Kouloglou's device was hacked with Pegasus spyware a second time, on **March 6 and 7, 2023**. According to Kouloglou, during this time frame, the PEGA committee was engaged in intense discussions

related to the final drafting process. On March 6, 2023 Kouloglou traveled from Athens to Brussels and was in Brussels on March 6 and 7 during the timeframe of the infection.

It may also be significant that, at this time, PEGA Rapporteur MEP in 't Veld was in Greece as part of a mission with the LIBE Committee (Committee on Civil Liberties, Justice and Home Affairs), which is a standing committee of the European Parliament primarily responsible for drafting legislation and providing democratic oversight around issues concerning human rights, data protection, asylum, immigration, and anti-discrimination. On that mission, the LIBE delegation questioned the Greek Director of the National Transparency Authority and other officials on the Greek spyware scandal (report para 183).

As with the previous infection dates, the date of this infection was also followed by a string of PEGA hearings and a research trip to Spain (although Kouloglou did not participate in that trip himself). This infection took place approximately two months prior to the adoption of the first PEGA Committee report (May 8, 2023).

Separately, Kouloglou and Thanasis Koukakis had made tentative plans over WhatsApp to meet on or around March 6 and 7, 2023, but ultimately their in person meeting did not take place.

The European Parliament Under Surveillance

This is the first time a member of the PEGA Committee has been publicly identified as a victim of Pegasus spyware while serving on the Committee.

There have been a few public cases of MEP targeting prior to the creation of the PEGA Committee. Four Catalan MEPs were either directly or indirectly targeted with Pegasus: MEP Diana Riba's devices were infected in October 2019. Catalan MEP Jordi Solé was targeted in June 2020, just prior to taking his seat in the European Parliament. Two other Catalan MEPs were targeted through their staff or family members: Clara Ponsati (July 2020) and Carles Puigdemont (October 2019 and July 2020). Riba, Solé, and Puigdemont all joined the PEGA Committee: Riba as Vice-Chair, Puigdemont as a member, and Solé as a substitute. They testified about their experiences to the PEGA Committee, alongside Antoni Comín and Nikos Androulakis (whose device was targeted with Predator spyware).

Outside of the PEGA Committee, in February 2024, Politico reported that MEPs on the security and defence subcommittee were asked to have their phones checked after traces of spyware were found on two devices. French MEP Nathalie Loiseau, chair of the committee, confirmed she was targeted with Pegasus. The European Parliament's IT Services informed Bulgarian MEP Elena Yoncheva that her device had been targeted in late October 2023. In May 2024, following the conclusion of the PEGA Committee proceedings, German MEP Daniel Freund announced he had been targeted with Candiru's mercenary spyware.

Attribution

While we assess with high confidence that Kouloglou was targeted and infected with NSO Group's Pegasus mercenary spyware, we are not attributing these investigations to a specific NSO Group customer.

Since 2022, when the Citizen Lab first discovered the hacking of Thanasis Koukakis' device with Predator spyware, the Greek government has been embroiled in a growing surveillance scandal involving abusive targeting of civil society. However, we have no indications that this hacking was the work of the Greek government. There are no reports that Greece is or was a customer of NSO Group or a user of Pegasus spyware. While the Greek government is known to have extensively abused Intellexa's Predator mercenary spyware, the Citizen Lab is unaware of any technical indicators suggesting Greek security and intelligence services had access to NSO Group's Pegasus spyware.

However, we believe that the same operator targeted both Kouloglou in 2022 and the targets we highlighted in our May 2024 joint report with Access Now. In that report, we found that seven Russian and Belarusian-speaking independent journalists and opposition activists based in Europe were targeted and/or infected with NSO Group's Pegasus mercenary spyware. One of the redacted Apple IDs (**Email 1**) from that report is rauharepo888[@]gmail.com, the same HomeKit email that targeted Kouloglou. In our understanding of Pegasus infection infrastructure during this period, we believe that these emails are unique to specific operators. We are unable to say whether the second infection in 2023 is similarly connected to this operator, or a different operator.

We further note that infections appear to have been present on his phone in at least two European jurisdictions (Greece and Belgium).[1] Based on what we know of NSO Group's licensing, this would likely indicate that the customer had a license that enabled infections in multiple EU jurisdictions, narrowing the list of potential Pegasus operators that could be responsible for this case.

Conclusion

The infection of a European MEP and PEGA Committee member's device is a significant and troubling finding. It is made more troubling by the fact that we are unsure of the status of the phones of many of the other Committee members during the time of its proceedings. Short of a comprehensive screening, there is no way to know whether any other PEGA Committee members or their staff may have been similarly infected.

Whichever entity is responsible for the hacking, the infection could have exposed strictly confidential exchanges among PEGA Committee members and their staff, and other sensitive and confidential parliamentary proceedings, including to parties under investigation by the Committee itself.

The finding that a PEGA Committee member was targeted with Pegasus spyware during the Committee's work highlights the serious threat that mercenary spyware poses to the integrity of democratic processes.

As outlined above, this case is not the first that a Member of the European Parliament has had their devices either targeted or hacked with mercenary spyware, which illustrates the corrosive nature of unregulated mercenary hacking.

While we are unable to conclusively attribute these infections to a particular government agency at this time, and we have no evidence that the Greek government was responsible for this case, overlap with an operator responsible for hacking the devices of exiled Russian and Belarusian-speaking journalists and activists based in Europe warrants further investigation.

Recommendations

In light of our discovery, we recommend that European Union institutions open immediate investigations to determine the scope and scale of this breach of EU privacy and process.

MEPs and Staff: Get Screened

- We urge **MEPs and their staff that participated in the PEGA Committee to immediately seek forensic screening for signs of spyware infection**, and preserve work and personal devices that may have been targeted.
    - The Directorate-General for Information Technologies and Cybersecurity (DG ITEC) offers this spyware screening.
- **Exercise vigilance for state-sponsored attack warnings**, and seek prompt expert assistance when such warnings are received.
- The work of MEPs exposes them to more sophisticated threats. EU MEPs should **enable Lockdown mode (iPhone) and Advanced Protect for Android**. This mode strongly increases the protection of a device against mercenary spyware. The DG ITEC may be able to provide additional cybersecurity guidance.

European Parliament: Investigate, Increase Reporting & Screening

- The European Parliament should **conduct an immediate investigation into spyware attacks targeting MEPs and parliamentary processes**, given the surveillance of the PEGA committee detailed in this report.
    - Since some time has passed since this particular attack, prompt investigation is a matter of urgency to ensure that forensic traces are not lost.
- We urge the Parliament to **commission an annual report on cyber and surveillance threats to the Parliament** and members to identify areas of vulnerabilities, and make recommendations on how to increase parliamentary security.

    - Such a report could be produced by the European Parliamentary Research Service (EPRS) or other entities.
- DG ITEC offers optional screening for spyware for MEPs and staff. This case suggests that this capability may be underused. **We urge DG ITEC to develop a plan to achieve substantially higher screening rates, and publish yearly statistics** on the number of devices screened and rates of discovery.
    - We also urge DG ITEC to regularly **circulate specific guidance for MEPs and staff about vigilance to state sponsored attack warnings** from companies like Apple and Google.
- We recommend that DG ITEC consider (optionally) collecting (optionally) and providing to large platforms account information associated with MEPs and their staff. DG ITEC could request additional scrutiny be devoted to threats against these accounts, and that platforms inform them when they send these accounts state-sponsored threat warnings. This information could ensure that state-sponsored attack warnings are quickly acted on and that patterns are observed.

European Commission: Screen Commissioners & Staff for Spyware

- We urge the European Commission to undertake their own investigation and screening to determine whether commissioners or commission staff have been targeted with mercenary spyware.
- We urge the Commission's Directorate-General for Digital Services (DG DIGIT) to develop a comprehensive spyware screening and response capability, alongside regular screenings, and we note that DG ITEC may be a useful interlocutor in this endeavor.

Parliamentary Assembly of the Council of Europe (PACE): Screen Members & Staff for Spyware

- Given past PACE committee work on mercenary spyware abuses in Europe, we urge an investigation into whether Members or staff have been targeted with mercenary spyware.
- We urge the Council's Directorate of Information Technology (DIT) to consult with peer organizations and conduct regular screening of PACE Members and their staff for signs of mercenary spyware targeting.

National Parliaments: Screen and Secure Your Members

- While this case concerns a MEP, there is a long history of lawmakers targeted with Pegasus and similar mercenary spyware. We commend the DG ITEC for having developed techniques for screening members and we encourage the security services and oversight bodies of national parliaments to copy this model.

Tech Companies: Make Your Threat Warnings Count

- This case illustrates that a recipient of *multiple* threat warnings failed to notice them. Since the goal of these notifications should be for a target to take actions, ensuring that the target sees and understands them is critical. UX research, including with past notification recipients, will be

key to creating notifications that capture a recipient's attention, explain the issue, and make the next steps easy.

Note on Research Ethics

All research involving human subjects conducted at the Citizen Lab is governed under research ethics protocols reviewed and approved by the University of Toronto's Research Ethics Board.

Appendix: Timeline of PEGA Deliberations and Infection Dates

Date	Event
January 30, 2015	Journalist, writer, and documentary director Stelios Kouloglou became a member of the European parliament, aligned with the left-wing coalition SYRIZA party of Greece when the elected MEP Georgios Katrougalos left his seat to join the Tsipras' coalition government in Athens.
May 2019	Kouloglou kept his MEP seat in the 2019 European Parliamentary elections.
March 10, 2022	The *Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware* (PEGA) was established.
March 24, 2022	Kouloglou is appointed to serve as a substitute member on the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware (PEGA committee).
October 21, 2022	**Kouloglou's phone is infected with Pegasus spyware** while in the hospital. He is visited by Greek investigative journalist Thanasis Koukakis, who has worked closely on mercenary spyware issues in Greece, has testified to the PEGA committee, and was himself targeted with Intellexa's Predator spyware.
October 26-27, 2022	PEGA holds a string of hearings: – "Big Tech and Spyware" (October 26), – "Spyware and e-privacy" (October 26) – "The impact of Spyware on Fundamental Rights / Democracy and Electoral processes" (October 27).
November 1-4, 2022	The PEGA Committee visits Cyprus and Greece. Kouloglou is a member of the delegation, and actively participates in questioning those interviewed.
November 5, 2022	Greek media reporting revealed a list of 33 more targeted individuals in the Greek wiretapping scandal, all of whom were high profile political, business, and media personalities. This revelation featured heavily in the

	PEGA Committee's final report which concluded that the claim that Predator was used by a private actor is "highly implausible, as it would not explain the choice of targets" (para 141).
November 8, 2022	The PEGA committee rapporteur publishes their draft report.
January 2023	Amendments tabled for PEGA draft report.
February 2023	PEGA hearings and investigations continue and from February 20 to 21, 2023, the Committee undertook a research mission to Hungary (MEP Kouloglou was not a member of this delegation).
March 2, 2023	Kouloglou receives an Apple threat notification about targeting with Pegasus-like mercenary spyware.
March 6 & 7, 2023	**Kouloglou's phone is again infected with Pegasus spyware**. Kouloglou left Athens for Brussels on March 6 and was in Brussels March 6 and 7, 2023.
March 6 to 8, 2023	PEGA Rapporteur MEP in 't Veld was in Greece as part of a mission with the LIBE Committee. On that mission, the LIBE delegation questioned the Director of the National Transparency Authority and other officials on the spyware scandal (see PEGA report para 183).
March 2023	PEGA Hearings in March: – "Exchange of views on a European Security Lab / Research centre on spyware" (March 9) – "Geopolitics of Spyware II" (March 16, continued after hearing faced technical difficulties in Feb) – "Spyware and telecommunication companies" (March 16) On March 20-23, PEGA does a research mission to Spain. Kouloglou does not travel with this delegation.
May 8, 2023	The PEGA committee adopts the first committee report. Several weeks leading up to this date, the committee is engaged in intense discussions around the final draft of the report.
June 15, 2023	The PEGA Committee recommendations were adopted.
August 29, 2023	Kouloglou receives another notification from Apple about targeting with mercenary spyware.
October 23, 2023	Kouloglou left the SYRIZA party after disagreements with party leader Stefanos Kasselakis. He sits as an independent until June 2024, after which point he sits as a member of the New Left.
April 10, 2024	Kouloglou receives another notification from Apple about targeting with mercenary spyware.

July 16, 2024	Kouloglou ceases being a member of the European parliament, at the end of the 9th Parliamentary term.
May 2026	Kouloglou reaches out to the Citizen Lab and requests a forensic analysis of his iPhone, which shows that his device had been infected.