Graphite Caught First Forensic Confirmation of Paragon's iOS Mercenary Spyware Finds Journalists Targeted

citizenlab.ca/2025/06/first-forensic-confirmation-of-paragons-ios-mercenary-spyware-finds-journalists-targeted/

Bill Marczak, John Scott-Railton June 12, 2025

Introduction

On April 29, 2025, a select group of iOS users were notified by Apple that they were targeted with advanced spyware. Among the group were two journalists that consented for the technical analysis of their cases. The key findings from our forensic analysis of their devices are summarized below:

- Our analysis finds forensic evidence confirming with high confidence that both a prominent European journalist (who requests anonymity), and Italian journalist Ciro Pellegrino, were targeted with Paragon's Graphite mercenary spyware.
- We identify an indicator linking both cases to the same Paragon operator.
- Apple confirms to us that the zero-click attack deployed in these cases was mitigated as of iOS 18.3.1 and has assigned the vulnerability CVE-2025-43200.

Our analysis is ongoing.

Case 1: Prominent European Journalist

We analyzed Apple devices belonging to a prominent European journalist who has requested to remain anonymous. On April 29, 2025, this journalist received an Apple notification and sought technical assistance.

Our forensic analysis concluded that one of the journalist's devices was compromised with Paragon's Graphite spyware in January and early February 2025 while running iOS 18.2.1. We attribute the compromise to Graphite with high confidence because logs on the device indicated that it made a series of requests to a server that, during the same time period, matched our published Fingerprint P1. We linked this fingerprint to Paragon's Graphite spyware with high confidence.

Graphite spyware server contacted by the journalist's device:

https://46.183.184[.]91/

The server appears to have been rented from VPS provider EDIS Global. The server remained online and continued to match Fingerprint P1 until at least April 12, 2025.

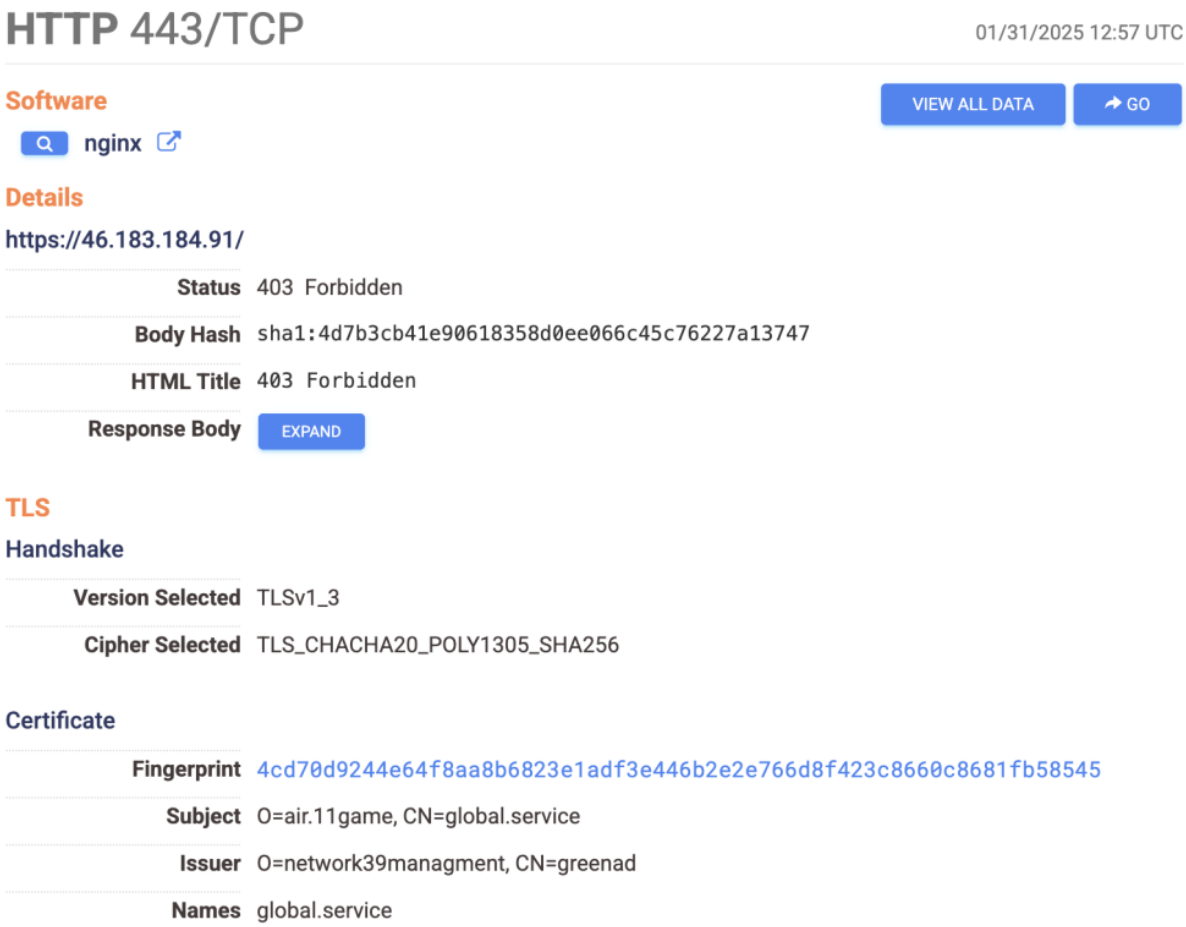

Figure 1. Censys result for the IP address contacted by the journalist's phone during the infection period.

We identified an iMessage account present in the device logs around the same time as the phone was communicating with the Paragon server `46.183.184[.]91`. We redact the account and refer to it as **ATTACKER1**. Based on our forensic analysis, we conclude that this account was used to deploy Paragon's Graphite spyware using a sophisticated iMessage zero-click attack. We believe that this infection would not have been visible to the target. Apple confirms to us that the zero-click attack deployed here was mitigated as of iOS 18.3.1 and has assigned CVE-2025-43200 to this zero-day vulnerability.

Case 2: Ciro Pellegrino

Ciro Pellegrino is a journalist and head of the Naples newsroom at *Fanpage.it,* where he has reported on numerous high-profile cases. On April 29, 2025, Mr. Pellegrino received an Apple notification and sought our technical assistance.

We analyzed artifacts from Mr. Pellegrino's iPhone and determined with high confidence that it was targeted with Paragon's Graphite spyware. Our analysis of the device's logs revealed the presence of the same **ATTACKER1** iMessage account used to target the journalist from **Case 1**, which we associate with a Graphite zero-click infection attempt.

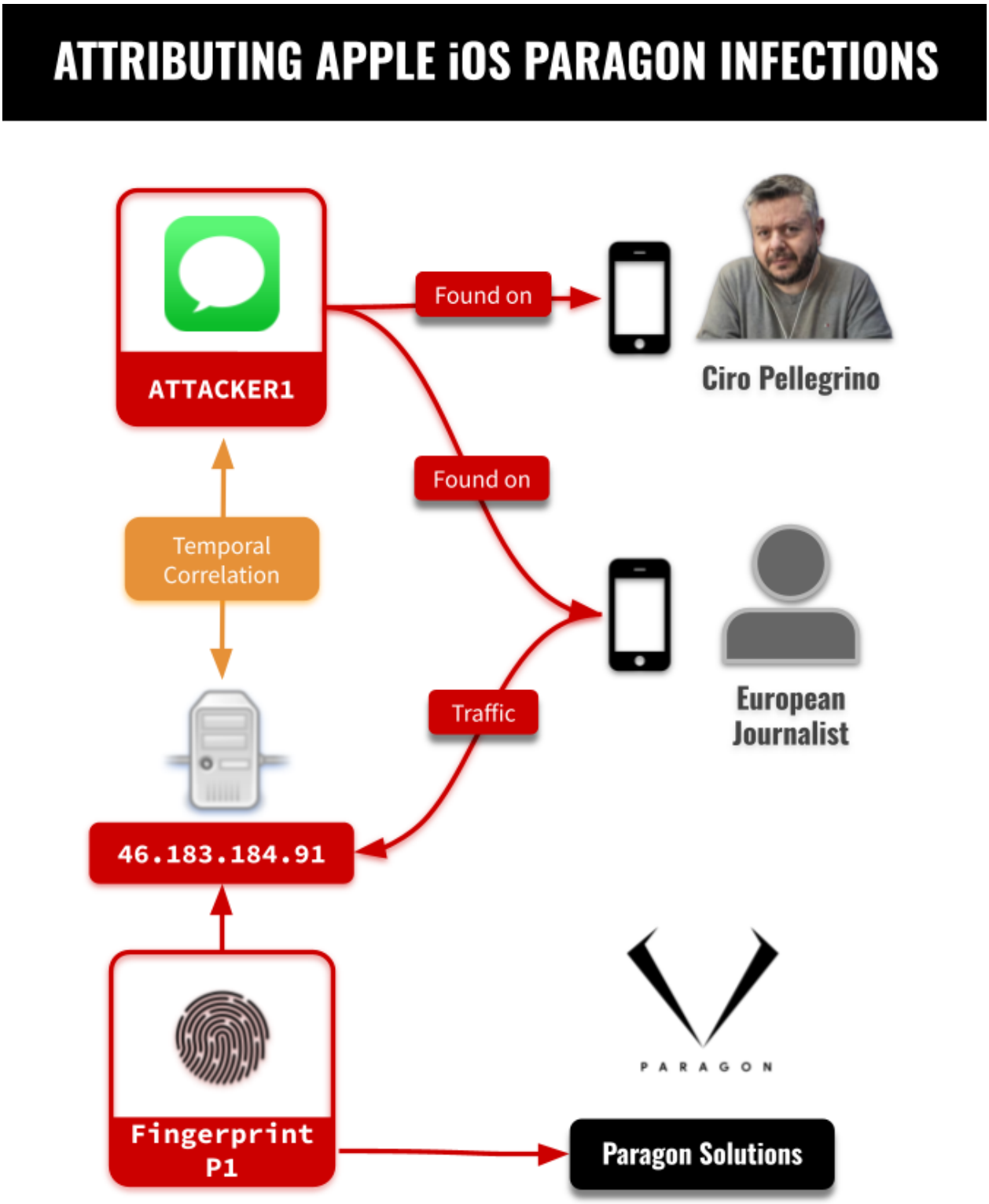

Figure 2. Attribution to Paragon's Graphite spyware via artifacts found on the devices of Ciro Pellegrino and the unnamed prominent European journalist.

It is standard for each customer of a mercenary spyware company to have its own dedicated infrastructure. Thus, we believe that the **ATTACKER1** account would be used exclusively by a single Graphite customer / operator, and we conclude that this customer targeted both individuals.

Our forensic analyses of these attacks, and Paragon's iOS capabilities, are ongoing.

The Fanpage.it Paragon Cluster

Mr. Pellegrino's close colleague and *Fanpage.it* editor, Francesco Cancellato, was notified in January 2025 by WhatsApp that he was targeted with Paragon's Graphite spyware.

The Citizen Lab has been conducting forensic analysis of Mr. Cancellato's Android device. However, as of our initial report, we were unable to obtain forensic confirmation of a successful infection of Mr. Cancellato's Android. As we explained at the time: "Given the sporadic nature of Android logs, the absence of a finding of BIGPRETZEL on a particular device does not mean that the phone wasn't successfully hacked, simply that relevant logs may not have been captured or may have been overwritten."

Following Mr. Cancellato's case, the identification of a second journalist at Fanpage.it targeted with Paragon suggests an effort to target this news organization This appears to be a distinct cluster of cases that warrants further scrutiny.

Statements by Paragon and the Italian Government

On June 5, 2025, the Italian government's parliamentary committee overseeing Italy's intelligence services (COPASIR: Comitato Parlamentare per la Sicurezza della Repubblica) published the report of their inquiry into the Paragon affair in Italy.

The report acknowledged that the Italian government had used Paragon's Graphite spyware against Luca Casarini and Dr. Giuseppe "Beppe" Caccia, the two individuals where we found forensic evidence of Graphite present (via the BIGPRETZEL Android indicator). However, the report stated that they were unable to determine who might have targeted Mr. Cancellato with Graphite.

On June 9, 2025, *Haaretz* reported that Paragon had offered to assist the Italian government in investigating the case of Mr. Cancellato, an offer that they say was rejected by the Italian government. Paragon also suggested that they had unilaterally terminated Italy's contracts.

In response later that day, the Italian Department of Security Intelligence (DIS: Dipartimento delle Informazioni per la Sicurezza), which coordinates Italy's intelligence services, stated that it had rejected Paragon's offer because of national security concerns with exposing their activities to Paragon. They stated that providing Paragon such access would impact the reputation of Italy's security services among peer services around the world. They denied that the contract termination was unilateral. Later the same day, the COPASIR committee stated that they had chosen not to proceed with Paragon's offer, but instead elected to directly query the Paragon databases, having deemed the approaches to be equivalent.[1] The committee also stated a willingness to declassify Paragon's testimony to the committee.

Response from Paragon Solutions

On June 10, 2025, we sent a summary of our latest findings to Paragon Solutions and offered them the opportunity to reply, which we undertook to publish in full. As of the time of publication we have not received a response.

Europe's Continuing Spyware Crisis: Journalists at Risk

At the time of publishing, three European journalists have been confirmed as targets of Paragon's graphite mercenary spyware. Two of these confirmations are now forensically based, and the third follows from a notification by Meta. Yet to date, there has been no explanation as to who is responsible for spying on these journalists.

Furthermore, the confirmation of a second case linked to a specific Italian news outlet (*Fanpage.it*) adds urgency to the question of which Paragon customer is responsible for this targeting, and pursuant to what legal authority (if any) this targeting took place.

The lack of accountability available to these spyware targets highlights the extent to which journalists in Europe continue to be subjected to this highly invasive digital threat, and underlines the dangers of spyware proliferation and abuse.

Our analysis of Paragon targeting on iOS and Android is ongoing. We thank Access Now for their support.

Have You Received a Warning?

If you are a journalist, human rights defender, or other member of civil society and received a spyware warning from Apple, Meta, WhatsApp, Google or others, take it seriously and seek expert assistance.

Here is an example of one such notification:

Figure 3. An excerpt of the Apple threat notification received by Ciro Pellegrino that triggered our investigation.

Organizations like Access Now and their Digital Security Helpline can assist you in understanding the attack, and quickly taking the next steps to increase your device security. We work with Access Now to ensure that cases get expert support. Similarly, the Security Lab at Amnesty International also maintains a resource and investigative contact point for notification recipients.

Appendix: Confirmed Paragon Targeting in Italy, Current Knowledge

As there are now multiple cases and reports of Paragon targeting and infection, we are providing a table with an overview of each case, along with the associated evidentiary basis. Importantly, we use the term “Targeted” describing an individual being selected for infection by a Paragon operator and reserve “Infected” to describe a forensic confirmation of a successful infection. In many cases, full forensic findings may not be available even in cases where an infection has likely happened, due to limitations in logs and efforts by Paragon to delete traces of the infection.

For example, Mr. Caccia is doubly confirmed as a Paragon target from both WhatsApp's notification and Citizen Lab's previously published forensic analysis. Additionally, we were able to identify specific dates that **BIGPRETZEL** was on his device, helping to illuminate the timeframe of the Paragon infection.

Meanwhile, Mr. Cancellato is confirmed as a Paragon target via a notification from WhatsApp, but our Citizen Lab analysis has yet to identify forensic evidence on the device providing additional information about Paragon targeting or infection. This is not necessarily surprising given forensic limitations when conducting research on Android devices.The following table summarizes these cases:

Name	Type of notification received & notification type	Device forensic analysis confirms Paragon targeting	Additional forensic Findings concerning Paragon infection(s)
Ciro Pellegrino	Notification from Apple: Targeted with unspecified advanced spyware	Yes. Citizen Lab found artifacts on the Apple device that we attribute with high confidence to Paragon spyware targeting.	Presence of **ATTACKER1** iMessage account that we link to a customer of Paragon's spyware.
"Prominent European Journalist"	Notification from Apple: Targeted with unspecified advanced spyware	Yes. Citizen Lab found artifacts on the Apple device that we attribute with high confidence to Paragon spyware targeting.	Graphite infection present in January and early February 2025 (exact dates redacted). Communication with **https://46.183.184[.]91**, a server that we attribute to a Paragon customer. Presence of **ATTACKER1**, an iMessage account we attribute to a Paragon customer.
Luca Casarini	Notification from WhatsApp: Targeted with Paragon's Spyware	Yes. Citizen Lab found artifacts on the Android device that we attribute with high confidence to Paragon spyware targeting.	Graphite infection present on seven dates between 2024-12-22 – 2025-01-31 (**BIGPRETZEL** present)
Giuseppe Caccia	Notification from WhatsApp: Targeted with Paragon's Spyware	Yes. Citizen Lab found artifacts on the Android device that we attribute with high confidence to Paragon spyware targeting.	Graphite infection present on 2024-12-23 (**BIGPRETZEL** present)
Francesco Cancellato	Notification from WhatsApp: Targeted with Paragon's Spyware	Not at this time, analysis ongoing.	

In addition to the cases listed above, two individuals have been described in our prior reporting: David Yambio and Father Mattia Ferrari. At the time of writing this report neither individual has been confirmed as a Paragon mercenary spyware target, although both are connected to the cases listed above.

Name	Type of notification received & notification type	Device Forensic Finding
David Yambio	Notification from Apple: Targeted with unspecified advanced spyware	Citizen Lab confirmed that the device was targeted with spyware, and affirms the presence of the **SMALLPRETZEL** forensic indicator. Compromise was not attributed to a specific actor, but the report notes proximity to multiple Paragon targets.
Father Mattia Ferrari	Notification from Meta: targeted by a "sophisticated attacker"	Not at this time, analysis ongoing.

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.

The Citizen Lab does not take general or unsolicited inquiries related to individual concerns regarding information security and cannot provide individual assistance with security concerns.

Acknowledgements

We wish to acknowledge the victims that chose to work with us and graciously consented to have their cases discussed. Without them, such research would not be possible. Their participation contributes to our collective digital security.

We thank our Citizen Lab colleagues, especially Bahr AbdulRazzak for technical investigative support, and Siena Anstis, Rebekah Brown, M. Scott and Adam Senft for review, editing and feedback and Alyson Bruce for editing and communications support.

Research for this project was supervised by Professor Ronald J. Deibert.

Special thanks to TNG.

We thank Access Now for their support.

1. This paragraph has been corrected to reflect the fact that the Committee did have knowledge of the offer, but declined it. It had originally stated that the Committee denied knowledge of the offer. We wish to thank the COPASIR committee for bringing this to our attention and providing us with a translation of their original statement. 2025-06-12 ↩