Pegasus infections in Jordan in 2022 and 2023: a technical brief

This technical brief outlines efforts by Access Now's Digital Security Helpline to obtain and analyze forensic evidence of spyware deployment against members of civil society in Jordan. The incidents reveal use of NSO Group's Pegasus zero-click exploits in several iOS devices. The brief was developed in collaboration with the Citizen Lab at the Munk School of Global Affairs & Public Policy at the University of Toronto (the Citizen Lab) and highlights the traces of Pegasus exploits on nine devices.

Published in February 2024

Access Now defends and extends the digital rights of people and communities at risk. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

For more information, please visit:
https://www.accessnow.org

I. Background

Access Now's Digital Security Helpline provides real-time, direct technical assistance and advice to civil society groups, activists, media organizations, journalists, bloggers, and human rights defenders worldwide. Its Analyst and Forensics team has strengthened its malware forensic capabilities to conduct root-cause analysis in security incidents, including in the potential use of surveillance technologies to restrict the rights of at-risk communities.

To ensure the quality and safety of its services, the Helpline carefully vets potential beneficiaries by conducting research and basic human rights due diligence, with the support of its network of trusted partners. The activities leading to the following brief involved the confirmation that all victims aided in this report are indeed members of civil society who have made positive contributions to their communities.

After establishing contact with the victims, the Helpline conducted a process aimed at assisting them to detect, diagnose, and overcome abuses against their right to privacy and other human rights. The work of the Helpline seeks to support and empower them in overcoming these challenges, by providing technical support and guidance. The analysis methodology used in this investigation has been independently reviewed and confirmed by the Citizen Lab.

This report covers only a subset of the identified victims in Jordan. Additional cases are described in our broader report ***Between a hack and a hard place: how Pegasus spyware crushes civic space in Jordan*** authored by Access Now in collaboration with the Citizen Lab, Amnesty International's Security Lab, Human Rights Watch, and the Organized Crime and Corruption Reporting Project (OCCRP).

II. Findings

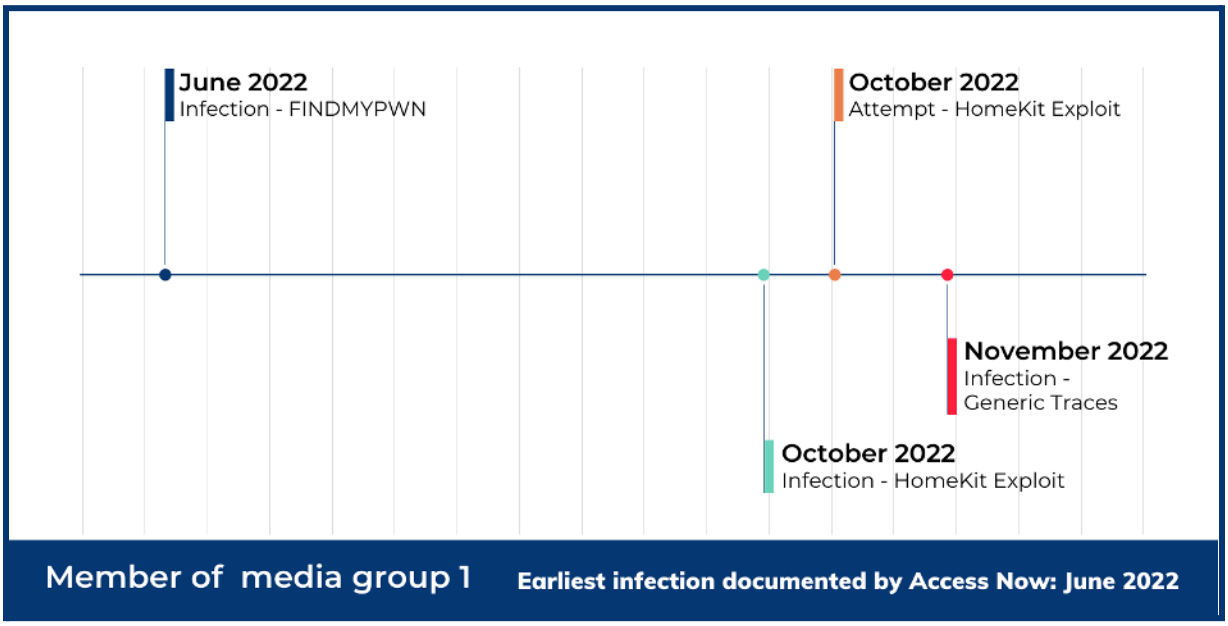
We analyzed logs from a number of devices in Jordan and identified traces of attacks with NSO Group's Pegasus spyware. This report provides a detailed outline of the infection in nine of these cases, focusing on the chronology of the traces identified. Of these, only one victim consented to the use of their name, while others preferred to remain anonymous. The information on the remaining cases is withheld due to privacy considerations.

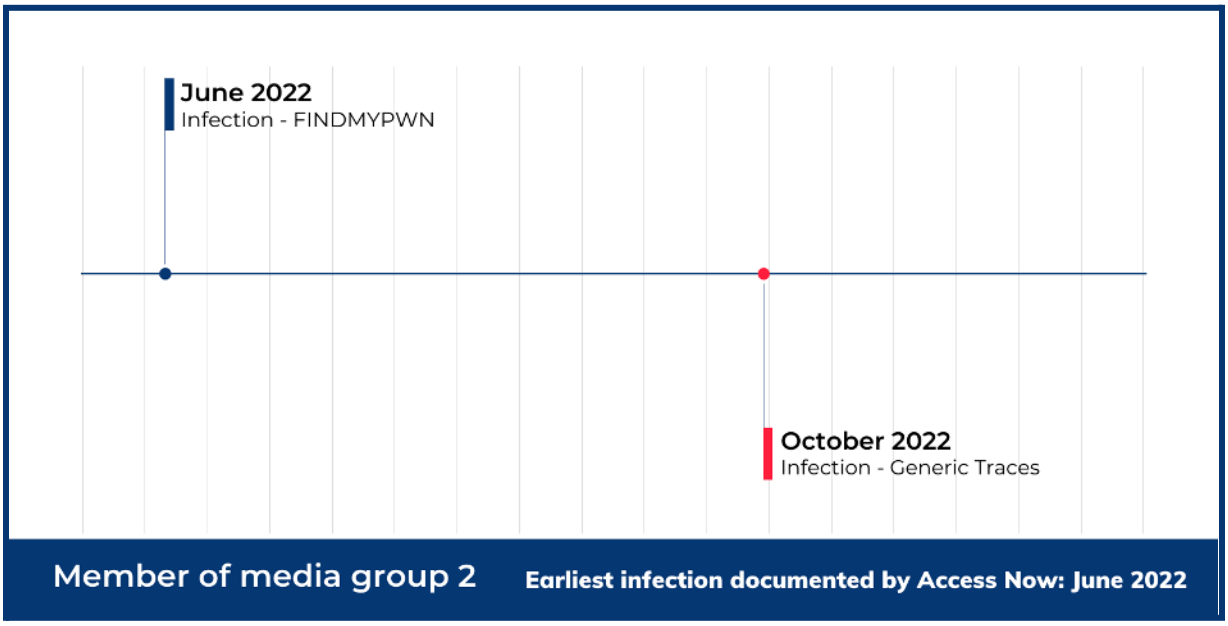
Each timeline shows signs of malicious conduct left by Pegasus on each of the targeted devices. In this group of cases, we detected traces of HomeKit exploits and/or FINDMYPWN exploits, otherwise known as the Pegasus zero-click attacks targeting iOS devices, accompanied by general traces of infection. In some cases, we found hard proof of infection; in others, evidence of an infection attempt; and in others, both successful and potentially unsuccessful attempts, and so on. But each trace documented represents evidence of the device being infected or targeted by Pegasus.

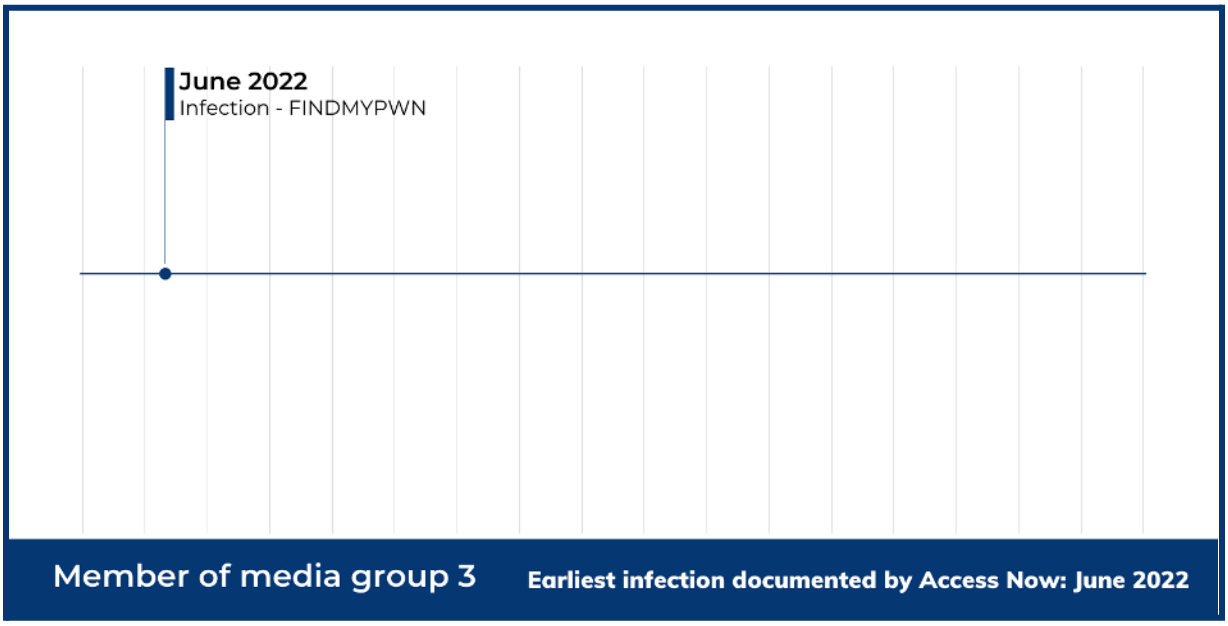
While the analysis could not determine the full scope of Pegasus activities on individual devices, the following presents a timeline for each case, which you can follow to understand the diagnosis.

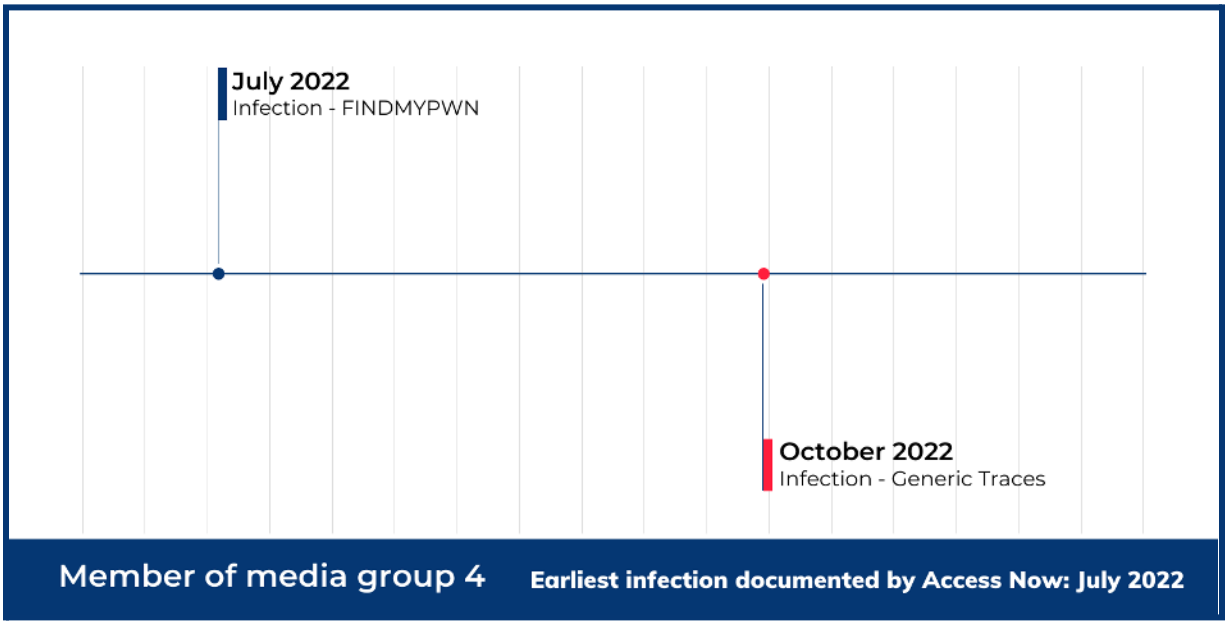
Timeline: nine cases of device targeting

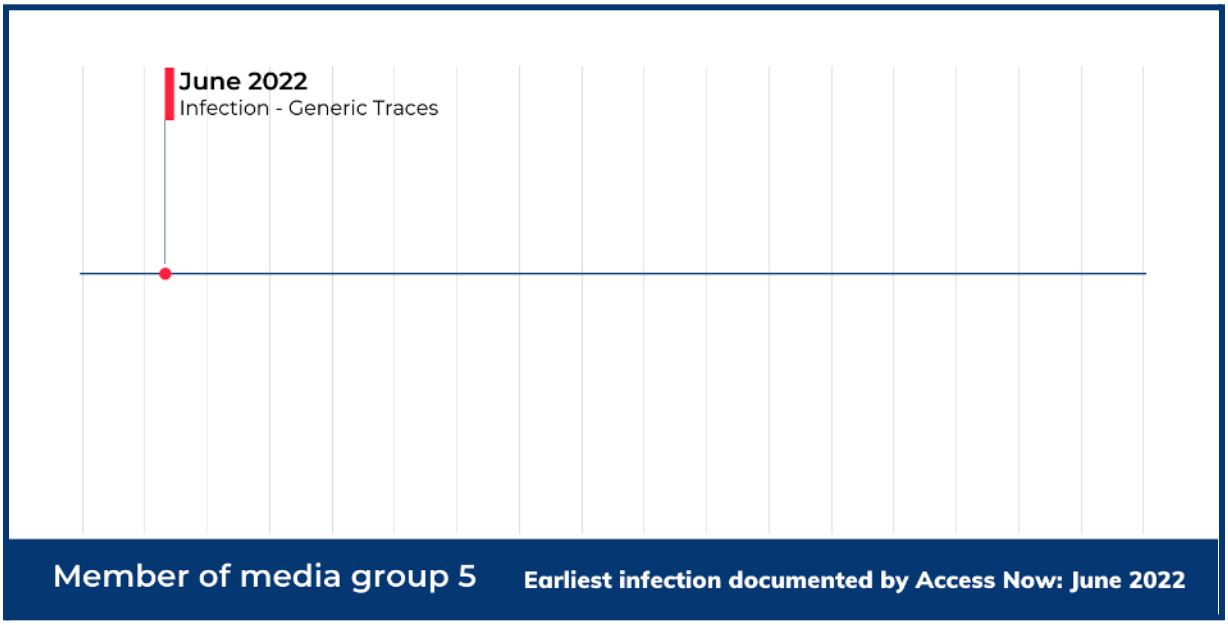
- Infection - FINDMYPWN: trace of infection of FINDMYPWN, an attack that exploits FindMy's vulnerability found by Citizen Lab
- Infection - HomeKit Exploit: trace of infection of HomeKit Exploit, an attack that exploits HomeKit's vulnerability found by Citizen Lab
- Attempt - HomeKit Exploit: trace of an attempt to use the HomeKit Exploit
- Infection - Generic Traces: trace of generic infection attributed to Pegasus

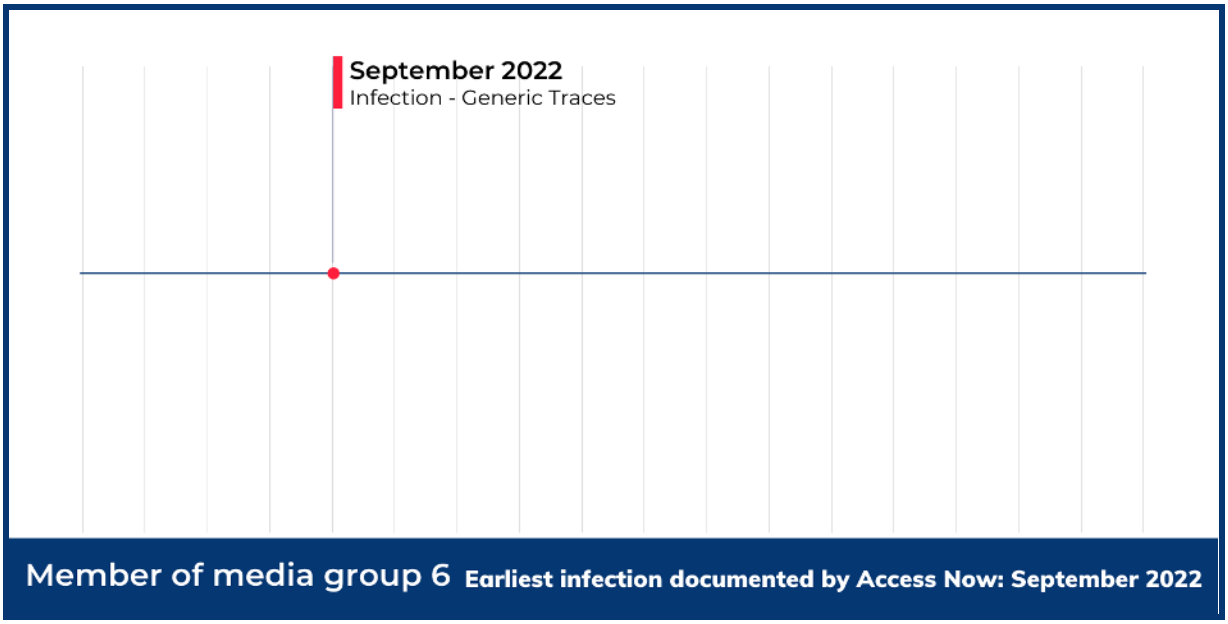


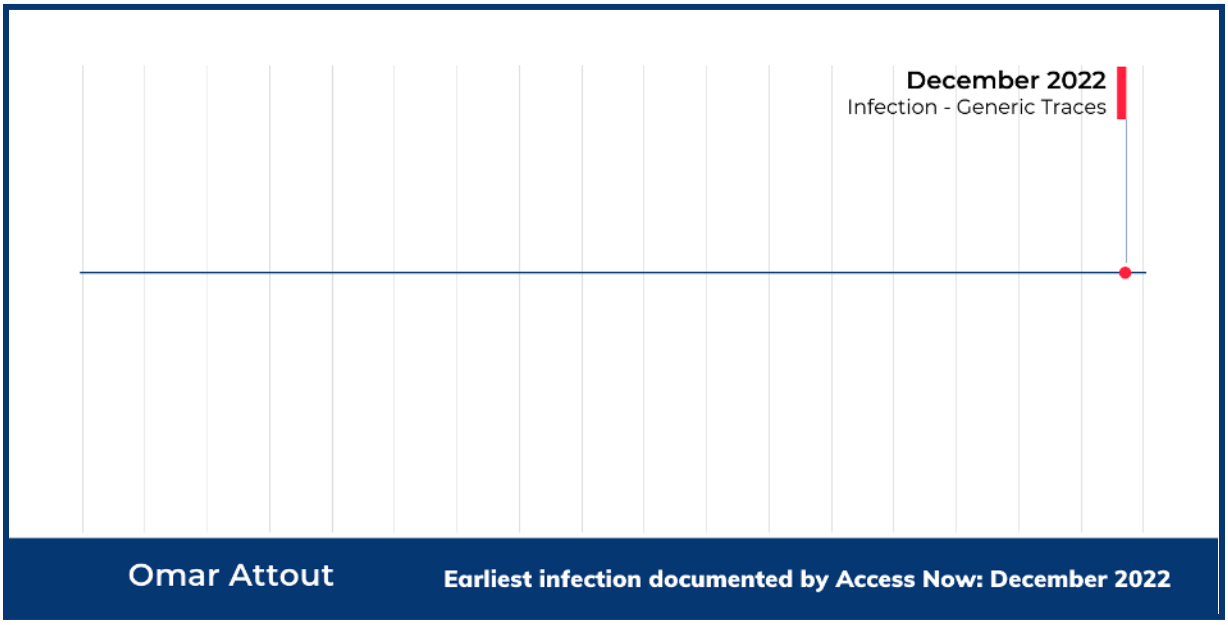

June 2022
Infection - FINDMYPWN
October 2022
Infection - Generic Traces
Member of media group 2
Earliest infection documented by Access Now: June 2022

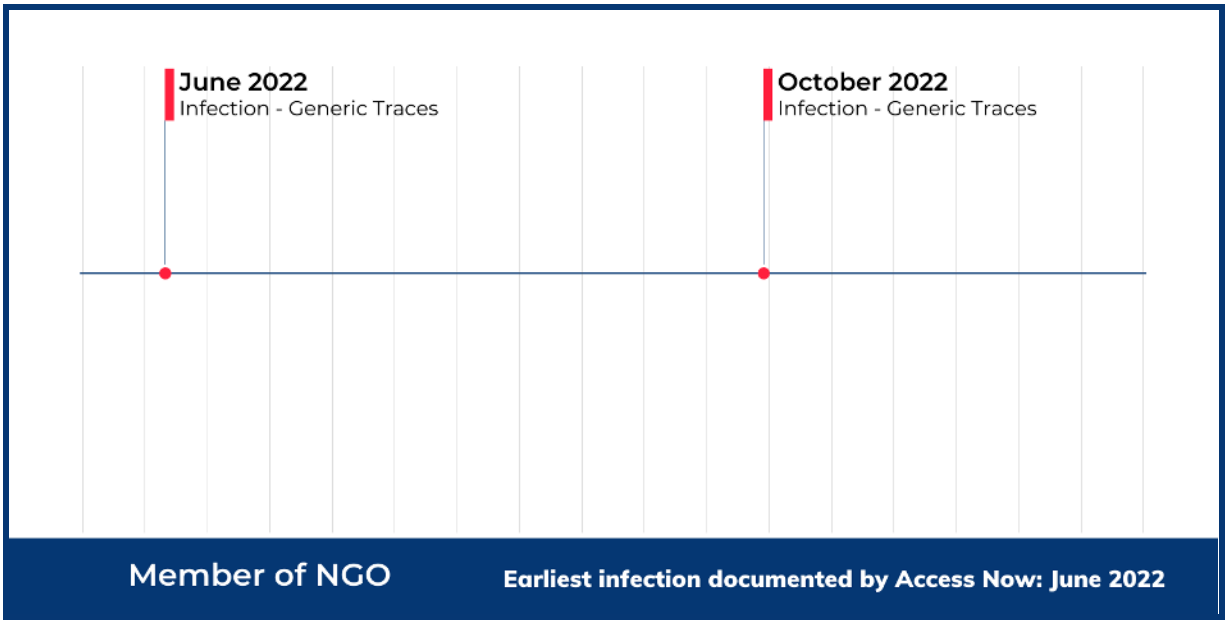

June 2022
Infection - FINDMYPWN
Member of media group 3
Earliest infection documented by Access Now: June 2022

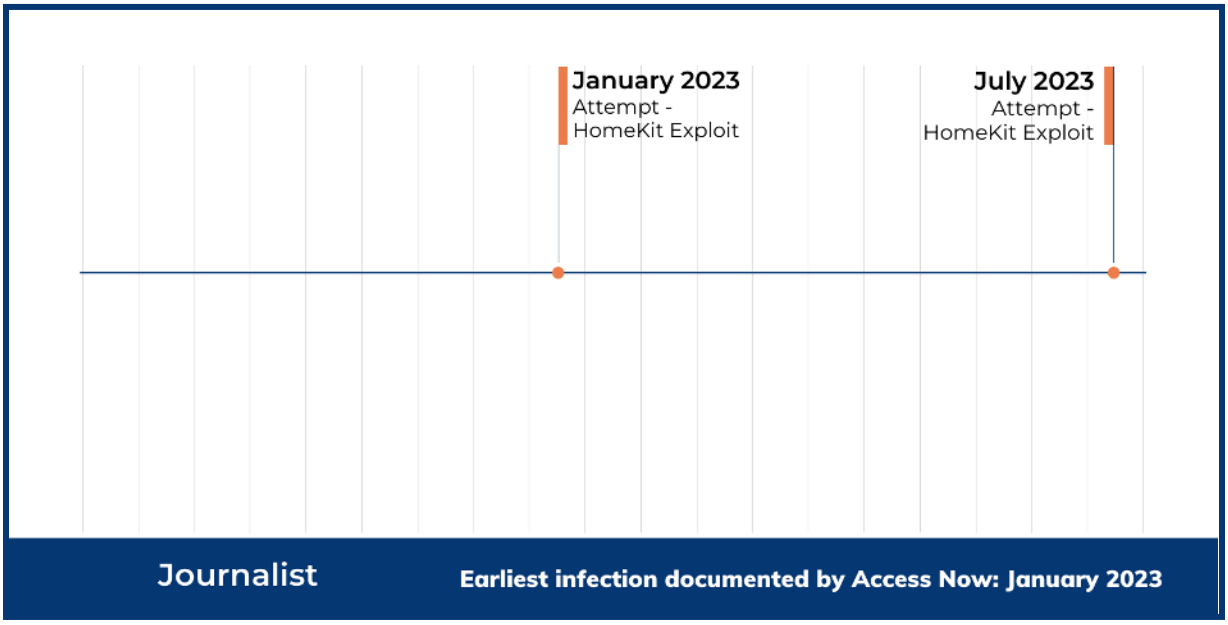

July 2022
Infection - FINDMYPWN
October 2022
Infection - Generic Traces
Member of media group 4
Earliest infection documented by Access Now: July 2022


June 2022
Infection - Generic Traces
Member of media group 5
Earliest infection documented by Access Now: June 2022


September 2022
Infection - Generic Traces
Member of media group 6
Earliest infection documented by Access Now: September 2022


December 2022
Infection - Generic Traces
Omar Attout
Earliest infection documented by Access Now: December 2022


June 2022
Infection - Generic Traces
October 2022
Infection - Generic Traces
Member of NGO
Earliest infection documented by Access Now: June 2022


January 2023
Attempt -
HomeKit Exploit
July 2023
Attempt -
HomeKit Exploit
Journalist
Earliest infection documented by Access Now: January 2023

III. Acknowledgements

The Digital Security Helpline extends its gratitude to members of civil society who were targeted for their crucial role in this investigation. Their trust in and commitment to the pursuit of truth was vital in this project.

We acknowledge the Citizen Lab team for their valuable support and mentoring, which greatly contributed to the progress of this investigation.

We would like to acknowledge the contributions of the Amnesty Tech team for sharing their Mobile Verification Toolkit, an important asset during this project.

IV. Contacts

If you have any questions or require further information regarding this report and the ongoing investigation, please reach out to Access Now at press@accessnow.org. We welcome your inquiries and are here to provide any clarifications you may need.