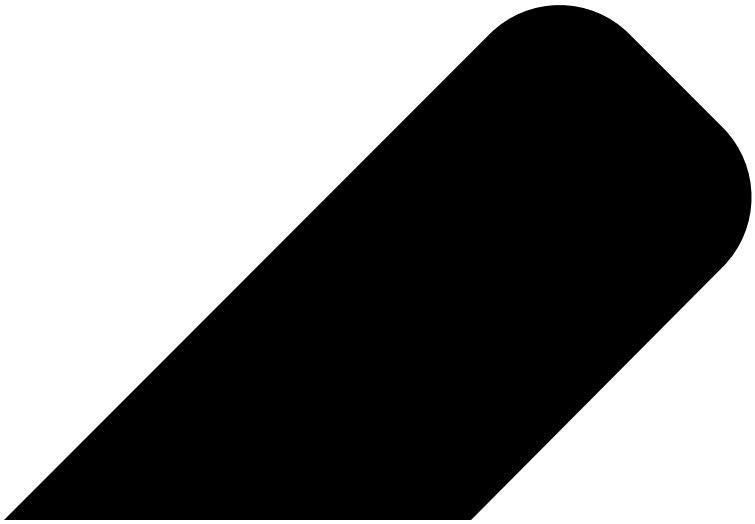
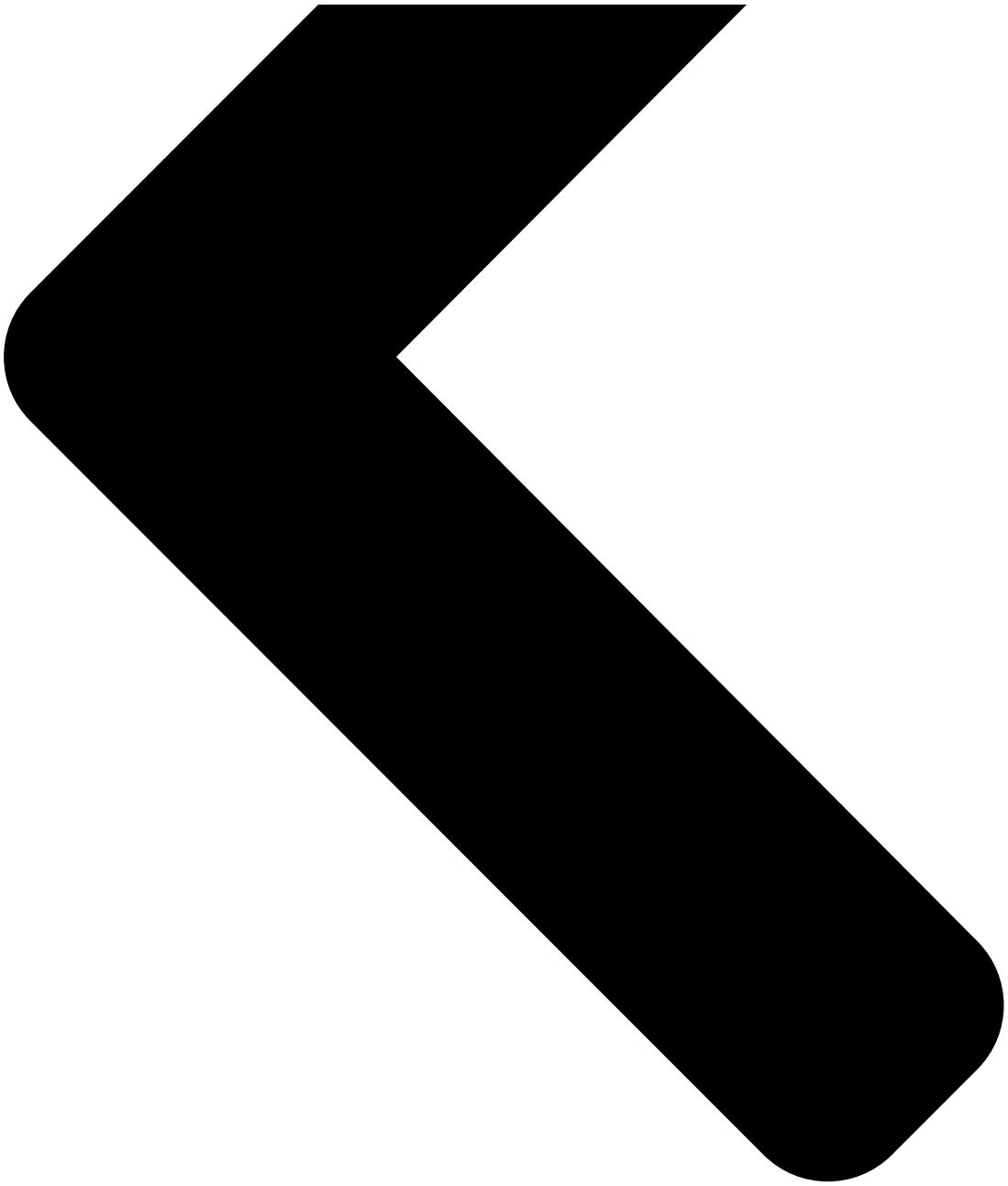
Independent Peer Review of Amnesty International's Forensic Methods for Identifying Pegasus Spyware

citizenlab.ca/2021/07/amnesty-peer-review/

July 18, 2021





Back to News

By Bill Marczak, John Scott-Railton, Siena Anstis, and Ron Deibert
July 18, 2021
On July 18, non-profit journalism organization Forbidden Stories released a major new investigation into NSO Group. The investigation exposes widespread global targeting with Pegasus spyware. The investigation also includes results from the forensic examination of a number of devices that their technical partner, Amnesty International, assessed to be infected.

Forbidden Stories and Amnesty International requested that the Citizen Lab undertake an independent peer review of a sample of their forensic evidence and their general forensic methodology. We were provided with iTunes backups of several devices and a separate methodology brief. No additional context or information about the devices or the investigation was provided to us.

We independently validated that Amnesty International's forensic methodology correctly identified infections with NSO's Pegasus spyware within four iTunes backups. We also determined that their overall methodology is sound. In addition, the Citizen Lab's own research has independently arrived at a number of the same key findings as Amnesty International's analysis.

Methodological Assessment: Sound

The Citizen Lab provides the following assessment of Amnesty's methodology:

- Amnesty's described methodology for **identifying Pegasus Process Names (and email addresses linked to the NSO Pegasus killchain) is sound**. Their method is based on temporal correlation between the items' first appearance in logs and phones' communication with known Pegasus Installation servers, or other Pegasus Process Names.
- Amnesty's described methodology for **identifying times during which phones were compromised is sound**. Their method involves observing Pegasus Process Names in a DataUsage.sqlite file obtained from an iTunes backup, or a netusage.sqlite file obtained from a full filesystem extraction, or other log files on the phone that record process names.
- Amnesty's described methodology for **linking the zero-click compromise they observed on iOS 14.6 to NSO Group is sound.** Their method is the same as above.
- Amnesty's described methodology for **linking the activity they observed involving Amazon CloudFront servers to the NSO Pegasus killchain is sound**. Their method is the same as above.
- Amnesty did in fact **detect Version 4 Pegasus servers**. Citizen Lab and Amnesty Tech conducted mutual sharing of Version 4 domain names we each detected as of July 2020. At that point, it became clear to both groups that we had independently developed substantially similar methods to detect NSO Group's infrastructure.

Additional Independent Support for Amnesty's Findings

The Citizen Lab's own research has independently arrived at several of Amnesty's key findings:

- Citizen Lab independently **employed a similar methodology to Amnesty International in our analysis of potential Pegasus compromise** (i.e., identifying process names proximate to communication with Pegasus servers), and have devised our own list of process names. Amnesty appears to have mentioned 45 process names in their draft report. We computed the intersection of this list with our list, and identified 28 process names in common. We can also confirm that we have not observed Amnesty's list of 45 process names used in association with any benign or legitimate apps.
- Citizen Lab **independently documented NSO Pegasus spyware installed via successful zero-day zero-click iMessage compromises of an iPhone 12 Pro Max device running iOS 14.6, as well as zero-day zero-click iMessage attacks that successfully installed Pegasus on an iPhone SE2 device running iOS version 14.4, and a zero-click (non-zero-day) iMessage attack on an iPhone SE2 device running iOS 14.0.1.** The mechanics of the zero-click exploit for iOS 14.x appear to be substantially different than the KISMET exploit for iOS 13.5.1 and iOS 13.7, suggesting that it is in fact a different zero-click iMessage exploit.
- Citizen Lab **independently observed NSO Group's new design for their hidden infrastructure** which appears to have been launched starting on September 2, 2018, about one month after Amnesty Tech and Citizen Lab published reports on NSO Group in August 2018. The new design is as Amnesty Tech describes in their draft report: "URL Shortener Servers" are separated from "Pegasus Installation Servers," and "Installation DNS Servers" are introduced.
- Citizen Lab **independently conducted similar scanning for Pegasus Infection Server domain names**, as well as Command and Control (C&C) server domain names. Citizen Lab and Amnesty International conducted mutual sharing of these Version 4 domain names we detected in July 2020.
- Citizen Lab **independently observed NSO Group begin to make extensive use of Amazon services** including CloudFront in 2021.
- Citizen Lab observed that **NSO Group's spyware was modified in late 2019 or early 2020 to (incompletely) delete information from the DataUsage.sqlite file.** We have never observed this anomaly outside of Pegasus infection, and in each case where we have observed this anomaly, we are able to correlate it with other indicators of Pegasus infection.

Conclusion

Amnesty International's core forensic methods for analyzing devices to determine that they have been infected with NSO Group spyware are sound.

Further information about the Citizen Lab's own investigations into NSO Group can be found here.