Amazon Shuts Down NSO Group Infrastructure

By Joseph Cox

Published: 2021-07-19 · Archived: 2026-04-05 14:56:52 UTC

Amazon Web Services (AWS) has shut down infrastructure and accounts linked to Israeli surveillance vendor NSO Group, Amazon said in a statement.

The move comes as a group of media outlets and activist organizations published new research into NSO's malware and phone numbers potentially selected for targeting by NSO's government clients.

Videos by VICE

"When we learned of this activity, we acted quickly to shut down the relevant infrastructure and accounts," an AWS spokesperson told Motherboard in an email.

Amnesty International published a forensic investigation on Sunday that, among other things, determined that NSO customers have had access to zero-day attacks in Apple's iMessage as recently as this year. As part of that research, Amnesty wrote that a phone infected with NSO's Pegasus malware sent information "to a service fronted by Amazon CloudFront, suggesting NSO Group has switched to using AWS services in recent months." The Amnesty report included part of the same statement from Amazon, showing Amnesty contacted the company before publication.

Citizen Lab, in a peer review of Amnesty's findings, said in its own post that the group "independently observed NSO Group begin to make extensive use of Amazon services including CloudFront in 2021."

Do you work at NSO Group, did you used to, or do you know anything else about the company? We'd love to hear from you. You can contact Joseph Cox securely on Signal on +44 20 8133 5190, Wickr on josephcox, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.

CloudFront is a content delivery network (CDN) that allows customers, in this case NSO, to more quickly and reliably deliver content to users.

"Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment," CloudFront's website reads.

CloudFront infrastructure was used in deployments of NSO's malware against targets, including on the phone of a French human rights lawyer, according to Amnesty's report. The move to CloudFront also protects NSO somewhat from researchers or other third parties trying to unearth the company's infrastructure.

"The use of cloud services protects NSO Group from some Internet scanning techniques," Amnesty's report added.

Amazon has previously remained silent on NSO using its infrastructure. In May 2020 when Motherboard uncovered evidence that NSO had used Amazon infrastructure to deliver malware, Amazon did not respond to a request for comment asking if NSO had violated Amazon's terms of service.

The Amnesty report said NSO is also using services from other companies such as Digital Ocean, OVH, and Linode.

On Sunday, journalistic organization Forbidden Stories and its media partners published a series of stories based in part on a leak of more than 50,000 phone numbers that were allegedly selected by NSO's clients for potential surveillance.

In a statement to The Guardian, NSO said "NSO does not operate the systems that it sells to vetted government customers, and does not have access to the data of its customers' targets. NSO does not operate its technology, does not collect, nor possesses, nor has any access to any kind of data of its customers. Due to contractual and national security considerations, NSO cannot confirm or deny the identity of our government customers, as well as identity of customers of which we have shut down systems."

Subscribe to our cybersecurity podcast, CYBER.

Source: https://www.vice.com/en/article/xgx5bw/amazon-aws-shuts-down-nso-group-infrastructure