Amazon cuts business ties with Israeli spyware maker NSO Group

The logo of Amazon Web Services (AWS) is seen during the 4th annual America Digital Latin American Congress of Business and Technology in Santiago, Chile, September 5, 2018. © REUTERS/Ivan Alvarado

New York, July 20 (RHC)-- Amazon has pulled the plug on infrastructure and other services that it offered to Israeli surveillance firm NSO Group, following allegations that the company's spyware was being used to snoop on journalists and activists.

The tech and retail giant announced on Monday that it had deactivated cloud computing accounts linked to NSO Group. The Israeli company reportedly used Amazon Web Services (AWS) to operate the spyware programs that it marketed to governments around the world. The move comes after Amnesty International's Security Lab conducted a forensic analysis of telephones on a leaked list of targets for NSO's flagship malware, Pegasus. It's believed that the digital surveillance software – which is reportedly capable of accessing and recording texts, videos, photos and web activity, and can even log passwords used on the device – may have been used by foreign governments to target as many as 50,000 people, including business executives, religious figures, academics, NGO workers, presidents and prime ministers.

Liberals in Israeli coalition govt challenge Defense Ministry over reports NSO malware was used to monitor reporters and activistsLiberals in Israeli coalition govt challenge Defense Ministry over reports NSO malware was used to monitor reporters and activists.

The leaked list of purported Pegasus targets goes back to 2016 and was reportedly compiled from requests from NSO clients in 10 countries, Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia and the United Arab Emirates (UAE). Hungary and Morocco have denied using the spyware to snoop on targets at home or abroad.

With media outlets now teasing potentially explosive details about the far-reaching hacking, Amazon wasted little time in distancing itself from the Israeli firm. "When we learned of this activity, we acted quickly to shut down the relevant infrastructure and accounts," an AWS spokesperson said.

NSO Group disputed that AWS had shut down its accounts, prompting Amazon to double down.   "We shut down the infrastructure referenced in this report that was confirmed to be supporting the reported hacking activity, in accordance with our terms of use," a spokesperson for the company reiterated.

Amnesty's analysis of 67 smartphones allegedly targeted by Pegasus found evidence of successful infection on 23 devices and signs of attempted infiltration on 14 others. The NGO also claimed that NSO's malware sent information "to a service fronted by Amazon CloudFront, suggesting NSO Group has switched to using AWS services in recent months."

Citizen Lab, a group at Toronto University that has been tracking Pegasus for years, said in a peer review of Amnesty's finding that it had "independently observed NSO Group begin to make extensive use of Amazon services including CloudFront in 2021."

CloudFront is an Amazon service that allows clients to securely deliver data using high transfer speeds. While Amazon rushed to cut ties with NSO, it was less proactive when media reports revealed in May 2020 that the Israeli firm may have used Amazon infrastructure to deliver malware to unsuspecting victims. At the time, the company failed to respond to a request for comment asking if NSO had breached Amazon's terms of service.

The Israeli surveillance firm has disputed how Pegasus has been characterized by Amnesty and subsequent media reports, claiming that its clients only use the malware in exceptional cases involving legitimate targets of counterterrorism operations or investigations of other serious crimes.

https://www.radiohc.cu/en/noticias/internacionales/264462-amazon-cuts-business-ties-with-israeli-spyware-maker-nso-group

Radio Habana Cuba