Leak of Israeli NSO Group Victims List Reminds Us Big Brother is Listening

Foreign governments use NSO Group's Pegasus spyware to hack journalists, activists, and intelligence targets' phones worldwide. What else is new?

On 18 July, news of yet more cyber snooping dropped: military-grade spyware sold by the private Israeli firm NSO Group to foreign governments was found to have been used to hack the phones of journalists, activists, executives, and politicians. Although cyberespionage by governments against foreign and domestic targets isn't exactly news, what made this discovery unusual was that Forbidden Stories and Amnesty International were able to obtain a list of more than 50,000 phone numbers allegedly belonging to targets of these government clients since 2016, including the time and date those numbers were targeted. In short, for the first time, journalists obtained a massive list of the spying priorities of multiple nation-states. For the globally besieged Fourth Estate, it was big news indeed. But is it really?

WHO IS NSO GROUP

NSO Group is an Israeli company that sells Tier 1 Nation State-grade spyware to foreign governments' law enforcement and intelligence agencies. The CEO and cofounder of NSO Group, Shalev Hulio, formerly served in the Israeli Defense Force, and the company claims it is staffed by veterans of elite intelligence agencies. NSO Group promises that its technology is only used to investigate terrorism and crime, and it has claimed that it terminated two contracts in the past year over allegations of human rights abuses. [1, 2, 3] However, it also claims no responsibility for any misuse of its software by client governments, almost certainly an intentional legal loophole to allow its clients to conduct broad surveillance abuse.

1 https://www.nsogroup.com/

2 https://www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-pegasus-project-hacking-allegations/?sh=37ea1607472d

3 https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

Companies like NSO Group and the Italian company Hacking Team[4] have entered the technical surveillance market in recent years to bridge the gap between traditional eavesdropping conducted by nation states and the need to access the communications of individual devices using end-to-end encryption. While most top tier national law enforcement and intelligence agencies have relied on in-house solutions, less technically savvy governments have outsourced the problem to private industry.

WHO'S ON THE LIST

To date, the Pegasus Project[5] has attributed at least 1,000 of the 50,000 phone numbers to individuals including several Arab royal family members, at least 65 business executives, 85 human rights activists, 189 journalists, and more than 600 politicians and government officials — including cabinet ministers, diplomats, and military and security officers. The numbers of several current heads of state and prime ministers also appeared on the list, including the presidents of France, Iraq, and South Africa, and the prime ministers of Pakistan, Egypt, and Morocco. King Mohamed VI of Morocco, as well as several former prime ministers, were also on the list.[6]

The greatest number of attributed phone numbers were Mexican, including those belonging to politicians, union representatives, journalists and other government critics. Mexico was NSO's first international client in 2011, less than a year after the firm was founded in Israel's Silicon Valley equivalent in northern Tel Aviv.[7] However, the second largest share of numbers came from the Middle East, including Qatar, the UAE, Bahrain, and Yemen. This is consistent with the fact that the governments of the UAE, Saudi Arabia and Bahrain are reported to be among NSO clients.[8]

NSO Group has been adamant that the leaked phone numbers are not targets of governments using the company's Pegasus spyware, but are instead part of a larger list of numbers used by its customers for "other purposes." RiskIQ assesses that this could be an effort to evade liability for illegal surveillance, however, given it is obvious these numbers were intended for surveillance.

4 https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire/

5 These media organizations include the Guardian (UK), Le Monde and Radio France (France), Die Zeit, Süddeutsche Zeitung, WDR and NDR (Germany), The Washington Post and Frontline (United States), Haaretz (Israel), Aristegui Noticias and Proceso (Mexico), Knack and Le Soir (Belgium), The Wire (India), Daraj (Syria), Direkt36 (Hungary), and OCCRP. The Pegasus Project is spearheaded by Forbidden Stories, a Paris-based nonprofit journalism organization.

6 https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

7 https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

8 https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

WHO'S NOT ON THE LIST

So far, no US companies or phone numbers have been identified as targets of Pegasus spyware, according to the Pegasus Project and previous exposés of NSO Group. While the numbers of approximately a dozen Americans working overseas were discovered on the list, in all but one case those phones were registered to foreign cellular networks. The Pegasus Project has not found evidence of any successful spyware penetration of phones with the US country code. Given that the Israeli Ministry of Defense must approve sale of NSO Group's spyware to foreign governments,[9] this may reflect a national policy prohibiting targeting of Israel's top ally. Conversely, NGO Group may have feared that US targets would detect the spyware and trace it back to the company.

HOW WERE THE PHONE NUMBERS COLLECTED?

The 50,000 phone numbers were likely derived from home location register (HLR) data.[10] The HLR is a database containing wireless customer data to enable routing calls and texts.[11] Conducting an HLR lookup is a customary first step in the process of targeting someone for technical surveillance. Legitimate businesses, such as call centers, also use HLR lookups to ensure phone numbers on their calling lists are turned on and live.[12] Although the phone numbers on the leaked list indicate the targeting priorities of NGO Group's customers, those numbers weren't all necessarily successfully hacked. Some of them may not have even had Pegasus spyware against them.

HOW PEGASUS WORKS

The Pegasus software enables its users to remotely and covertly access a target's phone and collect location data, voice and VoIP calls, contacts, and application data such as from Skype or WhatsApp. Pegasus exploits can overcome encryption, SSL, and proprietary protocols and are available across device platforms, including Android, BlackBerry, iOS and Symbian-based devices.[13] Since Pegasus software likely costs about $100,000 a month, nation-states likely use it only for high priority targets.[14]

A Pegasus exploit can begin in several different ways and may be customized to the target.[15] For example, it can take the form of a malicious link in a SMS text message or an iMessage. In some cases, a user must click on the link to start the infection, but NSO Group also advertises an Over-the-Air installation, which is delivered to a target's phone without any notification. The target would not even need to touch the phone for the exploit to be successful. The below diagram from NSO Group's marketing materials demonstrates how this process has been so successfully automated that all the client has to do is input a phone number and the Pegasus software will do the rest.

9 https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/

10 https://www.theguardian.com/news/2021/jul/23/how-nso-became-the-company-whose-software-can-spy-on-the-world

11 https://www.gartner.com/en/information-technology/glossary/hlr-home-location-register

12 https://www.hlrlookup.com/

13 https://www.riskiq.com/wp-content/uploads/2021/08/NSO-Pegasus.pdf

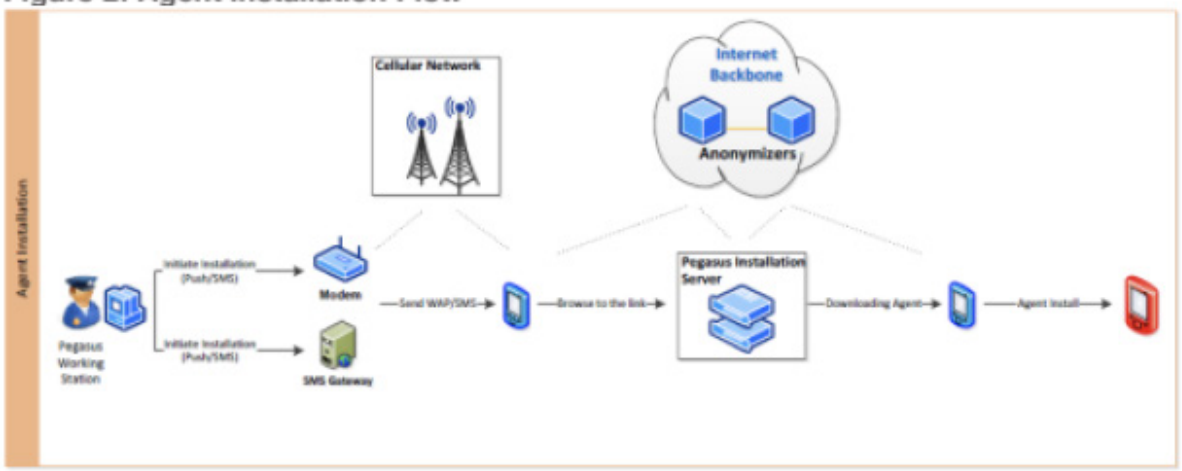
14 https://www.haaretz.com/israel-news/podcasts/PODCAST-listen-how-pegasus-spyware-became-part-of-israel-s-diplomatic-arsenal-1.10036432

15 https://www.riskiq..com/wp-content/uploads/2021/08/NSO-Pegasus.pdf

Agent Installation Flow

Remote agent installation flow is shown in Figure 2.

Figure 2: Agent Installation Flow



In order to initiate a new installation, the operator of the Pegasus system should only insert the target phone number. The rest is done automatically by the system, resulting in most cases with an agent installed on the target device.

COULD I BE A PEGASUS TARGET?

Although a list of 50,000 targeted phone numbers sounds daunting, in reality, to date almost no private businesses have been identified from that list and only a handful of executives. The most likely Pegasus targets are persons of interest to the intelligence services of identified NSO clients; specifically, Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo and the United Arab Emirates.[16, 17] Judging from current analysis of the leaked phone numbers and open source reporting about these countries' intelligence priorities, RiskIQ assesses Pegasus targets are likely to include the following categories of individuals:

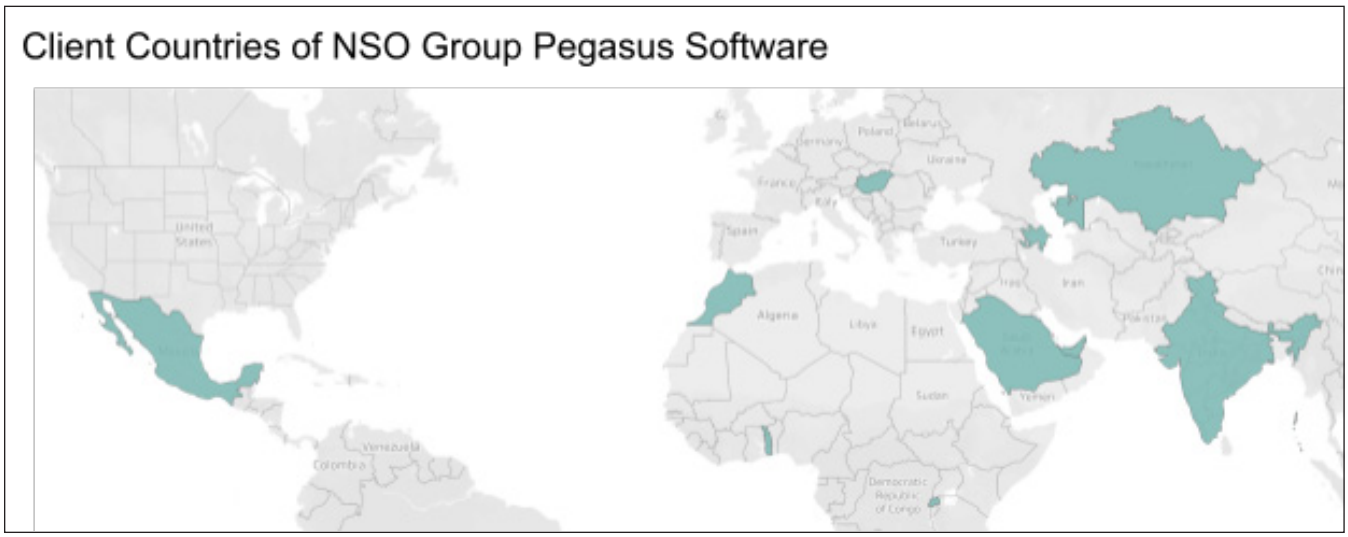
- **National political leaders.** Several phone numbers belonged to the heads of state of neighbouring countries, countries actively involved in a client country, or countries with geopolitical interests in the client's region. For example, French President Emmanuel Macron's phone number was allegedly targeted by Morocco.[18]
- **Domestic dissidents, human rights activists and journalists.** Many clients appear to have used Pegasus to spy on their own journalists and activists.

16 https://www.cpomagazine.com/cyber-security/data-leak-reveals-pegasus-spyware-found-in-use-unlawfully-in-20-countries-with-capability-to-break-current-iphone-security/#:~:text=The%20leaked%20data%20led%20to,United%20Arab%20Emirates%20(UAE).

17 https://www.theguardian.com/news/2021/jul/23/how-nso-became-the-company-whose-software-can-spy-on-the-world

18 https://www.bbc.com/news/world-europe-57937867

- **High-profile expats.** Although the motivations for spying on expats may vary, clients appeared to have some interest in snooping on high-profile foreign residents. For example, the phone number of Pavel Durov, the CEO of Telegram, was allegedly targeted by the UAE after he moved there.[19]
- **Executives or top researchers of high profile companies involved in a client country or in industries of strategic importance to a client country.** Clients almost certainly have used Pegasus for economic espionage to boost their domestic industries or collect on companies' plans and intentions that may impact their national economic security.
- **Targets with strategic or military intelligence value.** Given Pegasus's obvious foreign intelligence collection capability, it's no surprise that many clients likely used it to bolster their signals intelligence collection efforts. For example, the Yemeni phone numbers on the list are likely intelligence targets of Saudia Arabia and the UAE, which have been militarily involved in Yemen's civil war in the past several years.[20]
- **Criminals.** The NSO Group's CEO claimed in an interview with Forbes that NSO tools enabled the prevention of more than 15 terror attacks, the arrest of more than 100 pedophiles across Europe, and the identification of major cybercriminals.21 Obviously, it would fall to individual clients to define what criminal activity they are monitoring and to what extent that surveillance is judicially sanctioned.



While the full list of 50,000 phone numbers has not been publicly released, Amnesty International has released a tool that enables users to check their phone for Pegasus spyware. It is available at https://github.com/mvt-project/mvt.

19 https://gizmodo.com/telegram-ceos-number-found-on-list-of-potential-nso-spy-1847336533

20 https://www.middleeasteye.net/news/uae-yemen-conflict-deeply-involved-experts-say

21 https://www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-pegasus-project-hacking-allegations/?sh=37ea1607472d

WHAT'S NEXT?

For all the current news flurry about the Pegasus leak, governmental espionage activity like this is exposed all the time. In May, President Macron slammed the US for its operation to spy on European leaders by tapping underwater Internet cables between 2012 and 2014.[22] In 2015, the British Government Communications Headquarters (GCHQ) was exposed as running the world's biggest data mining operation, creating profiles on every visible internet user's browsing habits and recording 50 billion sessions a day. The same year, the New Zealand government was revealed to have been using XKeyscore to spy on candidates for the World Trade Organization director general position and members of the Solomon Islands government. And that doesn't even count the cyber espionage groups known to work for Russia, China, Vietnam, Iran, North Korea, etc.

The fact that foreign governments spy on private citizens and companies is no surprise. The fact that some have begun to outsource their operations to non-governmental agencies, however, likely signals a new dawn for cyberespionage: while top tier countries like the US, UK, Russia, and China will continue to develop their own technical surveillance tools, other countries will likely pursue private, third party vendors. This expands the playing field by allowing previously shut-out governments to begin accessing targets of interest. NSO Group's spyware and its clients may have been exposed, but half a dozen more companies will rise up to take its place. Instead of breaking into hotel rooms and tapping phone lines, the future will be spyware and malicious code.

22 https://www.washingtonpost.com/world/europe/nsa-spying-macron-merkel/2021/05/31/b4b13940-c22f-11eb-89a4-b7ae22aa193e_story.html

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com