Data breach reveals extensive government spying on journalists and political activists

Alex Findijs
18 July 2021

A data breach of the Israeli spy company NSO Group has revealed that the company's Pegasus software is being used by governments around the world to spy on political dissidents and journalists. The breach, obtained by French media non-profit Forbidden Stories and Amnesty International, included a list of 50,000 phone numbers targeted for infection with the Pegasus spyware.

Many identified targets of NSO's software are prominent individuals, including hundreds of business executives, religious leaders, academics, union and government officials—including several yet to be named cabinet ministers, presidents and prime ministers—as well as employees of Non-Governmental Organizations (NGOs).

The list consists of at least 180 targeted journalists, with reporters, executives, and editors from the *Financial Times*, CNN, the *New York Times*, France 24, the *Economist*, Associated Press and Reuters, all identified by the Pegasus project. The *Guardian*, which has produced a series reporting on the leak titled "The Pegasus project" in coordinating with 16 other news outlets, has stated that it will release further information about the targeted individuals in the coming days as part of its reporting on the issue.

Without forensic analysis of each phone number listed, it is impossible to determine how many phones were actually infected. However, an analysis of a sample of the listed phones by the Pegasus project determined that half, 37 of 67, were infected, indicating potentially tens of thousands of infections.

Regardless of how many phones were actually infected, the determination by government agencies that it was necessary to spy on tens of thousands of people, and hundreds of journalists and activists, is a warning of the lengths that capitalist governments will go to suppress any and all opposition to their rule and trample on democratic rights.

The revelations of the scale and extent of NSO's spying operations are an astonishing exposure of the ability of governments and intelligence agencies around the world to spy on their populations. An extensive investigation by over a dozen news outlets has discovered disturbing details about the capabilities of the Pegasus spyware.

According to the *Guardian*, Pegasus software is capable of monitoring all information stored on a smartphone, including texts, emails, and images, as well as encrypted data and contacts lists. It is even capable of accessing the victim's GPS, as well as activating a cell phone microphone or camera to record the target's conversations.

Such capabilities suggest that it may have been the GPS tracking features of Pegasus that facilitated the assassination of Mexican journalist Cecilio Pineda Birto in 2017. Pineda was gunned down by four men at a car wash in Altamirano, Mexico just weeks after his addition to the list by one of NSO's Mexican clients.

Even more concerning is the ability of Pegasus to infect a target's phone with ease. Earlier infection models relied on texting or emailing a link through which the virus would enter the target's device. This method was often unreliable, with some known targets sent links that failed to complete the infection. However, recent advancements in NSO's spyware have allowed it to infect phones through what are called "zero-click" attacks that significantly reduce the risk of failure.

Such attacks enable NSO to infect target devices without any interaction on the part of the victim. These methods exploit "zero-day" vulnerabilities such as bugs in the operating system of a phone that the developer may not even know exist. In 2019, for example, WhatsApp revealed that NSO had been able to send malware to 1,400 devices by exploiting a zero-day vulnerability that allowed Pegasus to infect the device through a phone call, regardless of whether the target answered the call or not.

NSO has also been working to exploit weaknesses in Apple's iMessage app. Claudio Guarnieri, director of Amnesty International's Security Lab, has been able to identify Pegasus infections of Apple devices as recently as this month, even penetrating Apple's most recent security updates.

The target may also have their phone targeted remotely through an agent operating a wireless transceiver, and, according to NSO itself, a phone can be infected manually if an agent is able to steal the phone and download the spyware directly.

Using these techniques, Pegasus is virtually impossible to stop. The software is effectively undetectable, living in the temporary memory of a device and leaving no trace once the device is shut down. Furthermore, once infected, the spyware is capable of activating administrative privileges for itself. "Pegasus can do more than what the owner of the device can do," Guarnieri explained to the *Guardian* .

Guarnieri continued, "This is a question that gets asked to me pretty much every time we do forensics with somebody: 'What can I do to stop this happening again?' The real honest answer is nothing."

The consequences of the widespread deployment of this software are apparent: NSO is facilitating the extensive spying on journalists and political dissidents by governments with impunity.

According to NSO, it provides its services only to verified military, law enforcement and intelligence agencies in 40 unnamed countries and conducts extensive vetting of clients' human rights records. Ostensibly, the software is only used to target high profile criminals and terrorists.

However, based on information about NSO's clients obtained by the Pegasus project, this appears to be patently false. Not only have journalists, political activists and even high-ranking politicians been targets, but the ten countries so far identified by the Pegasus project as clients of NSO are Azerbaijan, Bahrain, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India and the United Arab Emirates.

Among this list are governments notorious for violating the human rights of journalists and citizens. Notably, Saudi Arabian crown prince Mohammed bin Salman was found to have ordered the assassination of *Washington Post* journalist Jamal Khashoggi. Several members of Khashoggi's family, as well as close associates and Turkish officials investigating the murder, were targets for NSO's spyware.

Khashoggi's fiancée, Hatice Cengiz, was allegedly hacked with Pegasus spyware just four days after his murder.

Mexico, with multiple agencies purchasing Pegasus and a suspected 15,000 targets, is the most dangerous country for journalists in the world outside of active war zones. Since 2010, 86 journalists have been killed, including two just last month. Those who investigate the connections and corruption between organized crime, the government and the security forces are often targeted for intimidation and threats of violence.

NSO and its government clients, the list of which will undoubtedly grow with time, is enabling the covert surveillance of any person deemed a threat by the capitalist governments and their intelligence agencies.

Such software will undoubtedly be used to record every move of independent, left wing and socialist journalists and political activists across the globe. This spying will be used to intimidate and threaten them, using the potential of violence as a bludgeon against critical journalism and political dissent. It will also be only a matter of time before such technology is used by companies to spy on their employees and crack down on the efforts of workers to organize against their bosses.

The attempts of governments to use spyware against journalists and their people must be opposed. But the defense of democratic rights cannot be entrusted to the capitalist parties that have assaulted democratic rights for decades and carried out mass surveillance of all electronic communications, as was exposed by NSA whistleblower Edward Snowden in 2013.

In the United States, the Republican Party passed the anti-democratic Patriot Act and the Democratic Party voted to extend it in 2019. In Germany, the grand coalition of the conservative Christian Democrats and liberal Social Democrats voted this June to further expand the surveillance powers of the state.

In every country, it is imperative for the working class to break with these parties, which embrace the assault on democratic rights, and build an independent socialist movement for the defense of democratic rights and freedom of the press.