French President Macron among those targeted by international Pegasus smartphone spyware operation

Kevin Reed
20 July 2021

The Pegasus Project media consortium published new revelations on Tuesday about the targeting of the smartphones of as many as 50,000 journalists, business and political figures and dissidents with spyware by governments around the world. According to the *Washington Post*, the list of identified targeted individuals contained fourteen prominent heads of state and governments.

Although none of those who were identified offered their phones up for forensic analysis so the infiltration of their devices with the spyware could not be confirmed, the *Post* report said the list of targeted leaders included "three presidents, 10 prime ministers and a king."

The identities of the fourteen individuals were derived from the list of 50,000 phone numbers that was leaked to the French media non-profit Forbidden Stories and Amnesty International and then reviewed by the 17 news organizations that comprise the Pegasus Project.

The *Post* reported that the three sitting presidents are France's Emmanuel Macron, Iraq's Barham Salih and South Africa's Cyril Ramaphosa. Three current prime ministers are Pakistan's Imran Khan, Egypt's Mostafa Madbouly and Morocco's Saad-Eddine El Othmani. Seven former prime ministers are Yemen's Ahmed Obeid bin Daghr, Lebanon's Saad Hariri, Uganda's Ruhakana Rugunda, France's Édouard Philippe, Kazakhstan's Bakitzhan Sagintayev, Algeria's Noureddine Bedoui and Belgium's Charles Michel. The one king is Morocco's Mohammed VI.

The *Post* said the media groups within the Pegasus Project confirmed the ownership of the phone numbers "through public records, journalists' contact books and queries to government officials or other close associates of the potential targets."

The revelations about the scope of Pegasus spyware use internationally is resulting in a series of lawsuits and political crises around the world. On Tuesday, for example, the French government demanded an investigation into the report that President Macron was one of the individuals who had been targeted by the hacking operation.

French Prime Minister Jean Castex told the National Assembly that the government had ordered investigations. An official Élysée Palace statement said, "If the facts are confirmed, they are clearly very serious. All light will be shed on these press revelations. Certain French victims have already announced that they would take legal action, and therefore judicial inquiries will be launched."

The Pegasus spyware—developed by the cybersecurity firm NSO Group—has been contracted by governments since 2016 to transform smartphones running the latest versions of either iOS or Android operating systems into 24-hour surveillance devices. The initial versions of the software used a technique called "spear-phishing" in which text or email messages are used to get the device owner to click on a malicious link that would then download the spyware onto the phone.

Since these methods have become less effective, NSO developed more advanced methods of getting Pegasus onto the smartphones such as "zero-click" attacks that do not require the device owner to do anything for the spyware to be actuated. The zero-click methods exploit flaws in the operating system security to gain entry into a targeted smartphone. The *Guardian* reported on Sunday, for example, that NSO had been

exploiting vulnerabilities in WhatsApp by placing the malicious code directly into the program and infecting a user's phone as soon as they download it. More recently NSO has been exploiting a weakness in Apple's iMessage to gain "backdoor access to hundreds of millions of iPhones."

The *Guardian* also said that, "Pegasus can also be installed over a wireless transceiver located near a target, or, according to an NSO brochure, simply manually installed if an agent can steal the target's phone."

Once a phone has been hacked by Pegasus, the operators of the spyware can harvest any data on the device included phone call records, text messages, address books, calendars, email messages, internet browsing histories, geolocation and map data and also activate the microphone and camera.

NSO Group—named after the first names of its founders Niv Carmi, Shalev Hulio and Omri Lavie who are all ex-members of Unit 8200, the Israeli Intelligence Corps—was founded in 2010 in Tel Aviv. The use of NSO's software for spying on journalists and political oppositionists was initially exposed in 2012 following the signing of a $20 million contract with the government of Mexico.

In 2014, NSO Group was purchased by the American private equity firm Francisco Partners for $130 million, and these investors then flipped the cybersecurity company for $1 billion three years later.

By 2018, Amnesty International accused NSO Group of helping the regime of Saudi Arabia to spy on a member of the organization's staff. It was later alleged that NSO's Pegasus software played a role in the murder of journalist Jamal Khashoggi by the Saudi regime by tracking his whereabouts in the months leading up to his death. In 2019, WhatsApp accused NSO Group of injecting spyware into its system by exploiting the call feature of the software.

NSO Group has denied all along that it is responsible for the ongoing malicious software attacks. When WhatsApp presented evidence of smartphone hacking with NSO's tools, the company blamed the hacks on its customers. The company has recently stated publicly that it has sold licenses for Pegasus to 40 unnamed countries and continues to maintain that it does not maintain any of the data of its clients or operate the software once it is sold to a country.

NSO Group has also maintained that it is technologically impossible for its spyware to be installed on smartphones within the US. According to Slate, the company claims that the Pegasus software will "self-destruct if it finds itself within American borders."

Responding to the absurd statements by NSO Group, Edward Snowden, the whistleblower and former intelligence analyst who exposed a global US government electronic surveillance program, tweeted on Tuesday afternoon, "NSO's claim that it is 'technologically impossible' to spy on American phone numbers is a bald-faced lie: an exploit that works against Macron's iPhone will work the same on Biden's iPhone. Any code written to prohibit targeting a country can also be unwritten. It's a fig leaf."

Earlier in the day, Snowden commented on the revelation that French President Macron was on the target list, "No one is safe from the out-of-control designer spyware industry. Export controls have failed as a means of regulating this easily abused technology. Without an immediate global moratorium on the trade, this will only get worse."

Snowden also denounced the *Washington Post* for its editorial response to the Pegasus revelations. "WaPo's editorial solution to the NSO scandal is so embarrassingly weak that it is itself a scandal. These companies (and their hosts) claim 'transparency, accountability, and licensing requirements' are already in place! You ask for less than nothing."