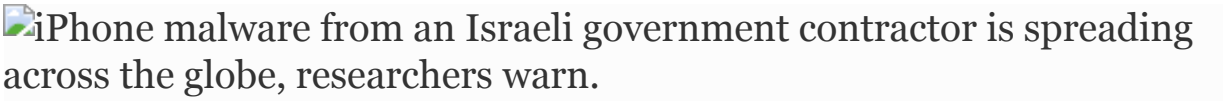
America Infected By Uber-Powerful Jewish Smartphone Spyware

Thomas Brewster Forbes Staff
Cybersecurity
I cover crime, privacy and security in digital and physical forms.



iPhone malware from an Israeli government contractor is spreading across the globe, researchers warn. JAAP ARRIENS/NURPHOTO

Some of the world's most sophisticated Android and iPhone spyware has been found floating around America for the first time. It's one of as many as 45 countries in which NSO Group malware was uncovered. And together they may represent breaches of American and other nations' computer crime laws against cross-border hacking, not to mention a severe concern for citizens' privacy, according to the researchers who uncovered the professional spy software.

The malware of concern, dubbed Pegasus, is the creation of NSO Group, an Israeli company valued at close to $1 billion. It can hide on Apple or Google devices, spying via the camera, listening in on conversations through the microphone, stealing documents and siphoning off once-private messages, amongst other surreptitious activities.

NSO has always protested that its tools are designed to be used to track the most heinous criminals, from terrorists to drug cartels. But the company has been caught up in spying scandals in Mexico and the United Arab Emirates. In both cases, civil rights organizations were up in arms that the iPhone malware had targeted activists, journalists and lawyers, among others who appeared entirely innocent of any crimes. Just last month, *Forbes* reported that an Amnesty researcher focusing on issues in the UAE had been targeted by NSO spyware. And most recently, leaked emails included in lawsuits in Israel and Cyprus against NSO Group appeared to show the company had hacked the phone of a journalist working at an Arab newspaper.

Now it seems infections of NSO's Pegasus tool have metastasized across more nations than previously believed. In a report released Tuesday, researchers from Citizen Lab, based out of the University of Toronto, claimed Pegasus had spread its wings in as many as 45 countries. Previously, Citizen Lab told *Forbes* it had evidence of as many as 174 individual infections across Android and iOS phones.

Bill Marczak, one of the Citizen Lab researchers behind today's report, said it was "very concerning" to see Pegasus infections across as many as 45 countries. He said six of those nations were "known spyware abusers," including Bahrain, UAE, Saudi Arabia, Kazakhstan, Morocco and Mexico. Another two on the list, Togo and Uzbekistan, may not have been caught targeting innocents with malware before but had "dubious human rights records," Marczak added.

"It indicates the market for these tools remains largely unregulated. And as long as that is the case, repressive regimes will use them to

covertly surveil and invisibly sabotage people holding governments to account."

NSO Group, for its part, said its products weren't designed to work in the U.S. and claimed there were inaccuracies in the Citizen Lab report.

Hunting a Pegasus

Citizen Lab was able to track down Pegasus infections by creating "fingerprints." They are formed of unique signifiers of the spy software. For instance, a form of encryption could be unique to the malware, or Web servers associated with its snooping. Citizen Lab is keeping those fingerprints secret for now but found they could then be detected by scanning the internet.

In total, the researchers discovered 36 "distinct operators" of the NSO tool, many of whom are likely customers. Ten appeared to have infected systems across multiple countries, including the U.K. and America, which may be a breach of U.S. law.

As per the Citizen Lab report, handed to *Forbes* ahead of publication: "The scope of this activity suggests that government-exclusive spyware is widely used to conduct activities that may be illegal in the countries where the targets are located.

"For example, we have identified several possible Pegasus customers not linked to the United States, but with infections in U.S. IP space. While some of these infections may reflect usage of out-of-country VPN or satellite internet service by targets, it is possible that several

countries may be actively violating United States law by penetrating devices located within the U.S..”

VPNs, or Virtual Private Networks, typically take internet traffic through different servers across various geographies. It’s possible NSO or its customers have used VPN servers in America, rather than infecting cellphones.

The company has repeatedly tried to break the American market. It once set up a company called Westbridge Technologies to sell into the U.S. that was acquired by an American private equity firm, Francisco Partners, in 2014. But there’s been no clear evidence so far that it managed to find clients within the States.

Marczak said there were suspected infections from three separate operators of the Pegasus malware. Two were interested in matters related to the Middle East, the other on Mexico.

“It's hard to unequivocally rule out factors like VPNs or satellite connections,” Marczak told *Forbes*. “That said, the ISPs where we found the suspected infections were Cox, Comcast and Time Warner. My mental model of these companies is that they provide cable services and not necessarily VPN or satellite teleports.”

Another five operators were found focusing on European countries, including Croatia, Hungary, Latvia, Poland and Switzerland.

NSO response

NSO Group said it worked in full compliance with all countries' applicable laws, including export control regulations.

“Our products have saved the lives of thousands of people, prevented suicide terror attacks, helped convict drug cartel lords, facilitated complex crime investigations and returned kidnapped children to their parents. These are just a few examples of the critical security support our systems have provided worldwide,” a spokesperson said in an emailed statement sent to *Forbes*.

They said there were some problems with the Citizen Lab research. In particular, NSO does not sell in many of the 45 countries listed, the spokesperson added, noting that all contracts went through a business ethics committee.

“The product will not operate outside of approved countries. As an example, the product is specifically designed to not operate in the USA,” the spokesperson said.

Marczak said that, given there were 33 suspected operators with infections across 45 suspected countries, the list necessarily included nations that do not themselves operate Pegasus.

I cover security and privacy for Forbes. I've been breaking news and writing features on these topics for major publications since 2010. As a freelancer, I worked for The Guardian, Vice Motherboard, Wired and BBC.com, amongst many others. I was named BT Security Journalist o... MORE

Got a tip? Get me on Signal on +447837496820 or use SecureDrop to tip anyone at Forbes. Email at TBrewster@forbes.com or tbthomasbrewster@gmail.com for PGP mail.