How a Saudi woman's iPhone revealed hacking around the world

reuters.com/technology/how-saudi-womans-iphone-revealed-hacking-around-world-2022-02-17/

Joel Schectman, Christopher Bing

1/4
Saudi activist Loujain al-Hathloul makes her way to appear at a special criminal court for an appeals hearing, in Riyadh, Saudi Arabia March 10, 2021. REUTERS/Ahmed Yosri

WASHINGTON, Feb 17 (Reuters) - A single activist helped turn the tide against NSO Group, one of the world's most sophisticated spyware companies now facing a cascade of legal action and scrutiny in Washington over damaging new allegations that its software was used to hack government officials and dissidents around the world.

It all started with a software glitch on her iPhone.

An unusual error in NSO's spyware allowed Saudi women's rights activist Loujain al-Hathloul and privacy researchers to discover a trove of evidence suggesting the Israeli spyware maker had helped hack her iPhone, according to six people involved in the incident. A mysterious fake image file within her phone, mistakenly left behind by the spyware, tipped off security researchers.

Register now for FREE unlimited access to Reuters.com

The discovery on al-Hathloul's phone last year ignited a storm of legal and government action that has put NSO on the defensive. How the hack was initially uncovered is reported here for the first time.

Al-Hathloul, one of Saudi Arabia's most prominent activists, is known for helping lead a campaign to end the ban on women drivers in Saudi Arabia. She was released from jail in February 2021 on charges of harming national security. read more

Soon after her release from jail, the activist received an email from Google warning her that state-backed hackers had tried to penetrate her Gmail account. Fearful that her iPhone had been hacked as well, al-Hathloul contacted the Canadian privacy rights group Citizen Lab and asked them to probe her device for evidence, three people close to al-Hathloul told Reuters.

After six months of digging through her iPhone records, Citizen Lab researcher Bill Marczak made what he described as an unprecedented discovery: a malfunction in the surveillance software implanted on her phone had left a copy of the malicious image file, rather than deleting itself, after stealing the messages of its target.

He said the finding, computer code left by the attack, provided direct evidence NSO built the espionage tool.

"It was a game changer," said Marczak "We caught something that the company thought was uncatchable."

Bill Marczak poses for a portrait at Berkeley's university campus in Berkeley, California, U.S., January 26, 2022. Picture taken on January 26, 2022. REUTERS/Carlos Barria
The discovery amounted to a hacking blueprint and led Apple Inc (AAPL.O) to notify thousands of other state-backed hacking victims around the world, according to four people with direct knowledge of the incident.

Citizen Lab and al-Hathloul's find provided the basis for Apple's November 2021 lawsuit against NSO and it also reverberated in Washington, where U.S. officials learned that NSO's cyberweapon was used to spy on American diplomats.

In recent years, the spyware industry has enjoyed explosive growth as governments around the world buy phone hacking software that allows the kind of digital surveillance once the purview of just a few elite intelligence agencies.

Over the past year, a series of revelations from journalists and activists, including the international journalism collaboration Pegasus Project, has tied the spyware industry to human rights violations, fueling greater scrutiny of NSO and its peers.

But security researchers say the al-Hathloul discovery was the first to provide a blueprint of a powerful new form of cyberespionage, a hacking tool that penetrates devices without any interaction from the user, providing the most concrete evidence to date of the scope of the weapon.

In a statement, an NSO spokesperson said the company does not operate the hacking tools it sells – “government, law enforcement and intelligence agencies do.” The spokesperson did not answer questions on whether its software was used to target al-Hathloul or other activists.

But the spokesperson said the organizations making those claims were “political opponents of cyber intelligence,” and suggested some of the allegations were “contractually and technologically impossible.” The spokesperson declined to provide specifics, citing client confidentiality agreements.

Without elaborating on specifics, the company said it had an established procedure to investigate alleged misuse of its products and had cut off clients over human rights issues.

A man walks past the logo of Israeli cyber firm NSO Group at one of its branches in the Arava Desert, southern Israel July 22, 2021. REUTERS/Amir Cohen

DISCOVERING THE BLUEPRINT

Al-Hathloul had good reason to be suspicious - it was not the first time she was being watched.

A 2019 Reuters investigation revealed that she was targeted in 2017 by a team of U.S. mercenaries who surveilled dissidents on behalf of the United Arab Emirates under a secret program called Project Raven, which categorized her as a “national security threat” and hacked into her iPhone.

She was arrested and jailed in Saudi Arabia for almost three years, where her family says she was tortured and interrogated utilizing information stolen from her device. Al-Hathloul was released in February 2021 and is currently banned from leaving the country.

Reuters has no evidence NSO was involved in that earlier hack.

Al-Hathloul’s experience of surveillance and imprisonment made her determined to gather evidence that could be used against those who wield these tools, said her sister Lina al-Hathloul. “She feels she has a responsibility to continue this fight because she knows she can change things.”

The type of spyware Citizen Lab discovered on al-Hathloul’s iPhone is known as a “zero click,” meaning the user can be infected without ever clicking on a malicious link.

Zero-click malware usually deletes itself upon infecting a user, leaving researchers and tech companies without a sample of the weapon to study. That can make gathering hard evidence of iPhone hacks almost impossible, security researchers say.

But this time was different.

The software glitch left a copy of the spyware hidden on al-Hathloul's iPhone, allowing Marczak and his team to obtain a virtual blueprint of the attack and evidence of who had built it.

"Here we had the shell casing from the crime scene," he said.

Marczak and his team found that the spyware worked in part by sending picture files to al-Hathloul through an invisible text message.

The image files tricked the iPhone into giving access to its entire memory, bypassing security and allowing the installation of spyware that would steal a user's messages.

The Citizen Lab discovery provided solid evidence the cyberweapon was built by NSO, said Marczak, whose analysis was confirmed by researchers from Amnesty International and Apple, according to three people with direct knowledge of the situation.

The spyware found on al-Hathloul's device contained code that showed it was communicating with servers Citizen Lab previously identified as controlled by NSO, Marczak said. Citizen Lab named this new iPhone hacking method "ForcedEntry." The researchers then provided the sample to Apple last September.

Having a blueprint of the attack in hand allowed Apple to fix the critical vulnerability and led them to notify thousands of other iPhone users who were targeted by NSO software, warning them they had been targeted by "state-sponsored attackers."

It was the first time Apple had taken this step.

Saudi women's rights activist Loujain al-Hathloul is seen in this undated handout picture.
Marieke Wijntjes/Handout via REUTERS
While Apple determined the vast majority were targeted through NSO's tool, security researchers also discovered spy software from a second Israeli vendor QuaDream leveraged the same iPhone vulnerability, Reuters reported earlier this month. QuaDream has not responded to repeated requests for comment. read more

The victims ranged from dissidents critical of Thailand's government to human rights activists in El Salvador.

Citing the findings obtained from al-Hathloul's phone, Apple sued NSO in November in federal court alleging the spyware maker had violated U.S. laws by building products designed "to target, attack, and harm Apple users, Apple products, and Apple." Apple

credited Citizen Lab with providing "technical information" used as evidence for the lawsuit, but did not reveal that it was originally obtained from al-Hathloul's iPhone.

NSO said its tools have assisted law enforcement and have saved "thousands of lives." The company said some of the allegations attributed to NSO software were not credible, but declined to elaborate on specific claims citing confidentiality agreements with its clients.

Among those Apple warned were at least nine U.S. State Department employees in Uganda who were targeted with NSO software, according to people familiar with the matter, igniting a fresh wave of criticism against the company in Washington.

In November, the U.S. Commerce Department placed NSO on a trade blacklist, restricting American companies from selling the Israeli firm software products, threatening its supply chain. read more

The Commerce Department said the action was based on evidence that NSO's spyware was used to target "journalists, businesspeople, activists, academics, and embassy workers."

In December, Democratic Senator Ron Wyden and 17 other lawmakers called for the Treasury Department to sanction NSO Group and three other foreign surveillance companies they say helped authoritarian governments commit human rights abuses.

"When the public saw you had U.S. government figures getting hacked, that quite clearly moved the needle," Wyden told Reuters in an interview, referring to the targeting of U.S. officials in Uganda.

Lina al-Hathloul, Loujain's sister, said the financial blows to NSO might be the only thing that can deter the spyware industry. "It hit them where it hurts," she said.

Reporting by Joel Schectman and Christopher Bing; editing by Kieran Murray and Edward Tobin