Despite the hype, iPhone security no match for NSO spyware

International investigation finds 23 Apple devices that were successfully hacked

Claude Mangin, shown at her home in suburban Paris, has been waging an international campaign to win the freedom of her husband, political activist Naama Asfari, who has been jailed in Morocco for more than a decade. Her iPhone 11 was hacked last month with Pegasus spyware. (Guillaume Herbaut/Agence VU for The Washington Post)

By Craig Timberg, Reed Albergotti and
Elodie Guéguen

July 19, 2021 | Updated yesterday at 11:30 a.m. EDT

1.1k

The text delivered last month to the iPhone 11 of Claude Mangin, the French wife of a political activist jailed in Morocco, made no sound. It produced no image. It offered no warning of any kind as an iMessage from somebody she didn't know delivered malware directly onto her phone — and past Apple's security systems.

Once inside, the spyware, produced by Israel’s NSO Group and licensed to one of its government clients, went to work, according to a forensic examination of her device by Amnesty International’s Security Lab. It found that between October and June, her phone was hacked multiple times with Pegasus, NSO’s signature surveillance tool, during a time when she was in France.

The examination was unable to reveal what was collected. But the potential was vast: Pegasus can collect emails, call records, social media posts, user passwords, contact lists, pictures, videos, sound recordings and browsing histories, according to security researchers and NSO marketing materials. The spyware can activate cameras or microphones to capture fresh images and recordings. It can listen to calls and voice mails. It can collect location logs of where a user has been and also determine where that user is now, along with data indicating whether the person is stationary or, if moving, in which direction.

And all of this can happen without a user even touching her phone or knowing she has received a mysterious message from an unfamiliar person — in Mangin’s case, a Gmail user going by the name “linakeller2203.”

These kinds of “zero-click” attacks, as they are called within the surveillance industry, can work on even the newest generations of iPhones, after years of effort in which Apple attempted to close the door against unauthorized surveillance — and built marketing campaigns on assertions that it offers better privacy and security than rivals.

Mangin’s number was on a list of more than 50,000 phone numbers from more than 50 countries that The Post and 16 other organizations reviewed. Forbidden Stories, a Paris-based journalism nonprofit, and the human rights group Amnesty International had access to the numbers and shared them with The Post and its partners, in an effort to identify who the numbers belonged to and persuade them to allow the data from their phones to be examined forensically.

For years, Mangin has been waging an international campaign to win freedom for her husband, activist Naama Asfari, a member of the Sahrawi ethnic group and advocate of independence for the Western Sahara who was jailed in 2010 and allegedly tortured by Moroccan police, drawing an international outcry and condemnation from the United Nations.

“When I was in Morocco, I knew policemen were following me everywhere,” Mangin said in a video interview conducted in early July from her home in suburban Paris. “I never imagined this could be possible in France.”

Especially not through the Apple products that she believed would make her safe from spying, she said. The same week she sat for an interview about the hacking of her iPhone 11, a second smartphone she had borrowed — an iPhone 6s — also was infected with Pegasus, a later examination showed.

Researchers have documented iPhone infections with Pegasus dozens of times in recent years, challenging Apple’s reputation for superior security when compared with its leading rivals, which run Android operating systems by Google.

The months-long investigation by The Post and its partners found more evidence to fuel that debate. Amnesty’s Security Lab examined 67 smartphones whose numbers were on the Forbidden Stories list and found forensic evidence of Pegasus infections or attempts at infections in 37. Of those, 34 were iPhones — 23 that showed signs of a successful Pegasus infection and 11 that showed signs of attempted infection.

Only three of the 15 Android phones examined showed evidence of a hacking attempt, but that was probably because Android’s logs are not comprehensive enough to store the information needed for conclusive results, Amnesty’s investigators said.

Still, the number of times Pegasus was successfully implanted on an iPhone underscores the vulnerability of even its latest models. The hacked phones included an iPhone 12 with the latest of Apple’s software updates.

In a separate assessment published Sunday, the University of Toronto’s Citizen Lab endorsed Amnesty’s methodology. Citizen Lab also noted that its previous research had found Pegasus infections on an iPhone 12 Pro Max and two iPhone SE2s, all running 14.0 or more recent versions of the iOS operating system, first released last year.

Target: Someone sends what's known as a trap link to a smartphone that persuades the victim to tap and activate — or activates itself without any input, as in the most sophisticated "zero-click" hacks.

Infect: The spyware captures and copies the phone's most basic functions, NSO marketing materials show, recording from the cameras and microphone and collecting location data, call logs and contacts.

Track: The implant secretly reports that information to an operative who can use it to map out sensitive details of the victim's life.

Read more about why it's hard to protect yourself from hacks.

Ivan Krstić, head of Apple Security Engineering and Architecture, defended his company's security efforts.

"Apple unequivocally condemns cyberattacks against journalists, human rights activists, and others seeking to make the world a better place. For over a decade, Apple has led the industry in security innovation and, as a result, security researchers agree iPhone is the safest, most secure consumer mobile device on the market," he said in a statement. "Attacks like the ones described are highly sophisticated, cost millions of dollars to develop, often have a short shelf life, and are used to target specific individuals. While that means they are not a threat to the overwhelming majority of our users, we continue to work tirelessly to defend all our customers, and we are constantly adding new protections for their devices and data."

Apple burnished its reputation for guarding user privacy during its high-profile legal fight with the FBI in 2016 over whether the company could be forced to unlock an iPhone used by one of the attackers in a San Bernardino, Calif., mass shooting the previous year. The FBI ultimately withdrew from the legal clash when it found an Australian cybersecurity firm, Azimuth Security, that could unlock the iPhone 5c without any help from Apple.

Outside researchers praise Apple for its stand — and for continuing to improve its technology with each new generation of iPhones. The company last year quietly introduced BlastDoor, a feature that seeks to prevent malware delivered through iMessages from infecting iPhones, making Pegasus-style attacks more difficult.

The investigation's conclusions also are likely to fuel a debate about whether tech companies have done enough to shield their customers from unwanted intrusions. The vulnerability of smartphones, and their widespread adoption by journalists, diplomats, human rights activists and businesspeople around the world — as well as criminals and terrorists — has given rise to a robust industry offering commercially available hacking tools to those willing to pay.

NSO, for example, reported $240 million in revenue last year, and there are many other companies that offer similar spyware.

On Sunday, NSO's chief executive, Shalev Hulio, told The Post that he was upset by the investigation's reports that phones belonging to journalists, human rights activists and public officials had been targeted with his company's software, even though he disputed other allegations reported by The Post and its partner news organizations. He promised an investigation. "Every allegation about misuse of the system is concerning to me," Hulio said. "It violates the trust we are giving the customer."

Apple is not alone in dealing with potential intrusions. The other major target of Pegasus is Google's Android operating system, which powers smartphones by Samsung, LG and other manufacturers.

Google spokeswoman Kaylin Trychon said that Google has a threat analysis team that tracks NSO Group and other threat actors and that the company sent more than 4,000 warnings to users each month of attempted infiltrations by attackers, including government-backed ones.

She said the lack of logs that help researchers determine whether an Android device has been attacked was also a

“While we understand that persistent logs would be more helpful for forensic uses such as the ones described by Amnesty International’s researchers, they also would be helpful to attackers. We continually balance these different needs,” she said.

Advocates say the inability to prevent the hacking of smartphones threatens democracy in scores of nations by undermining newsgathering, political activity and campaigns against human rights abuses. Most nations have little or no effective regulation of the spyware industry or how its tools are used.

“If we’re not protecting them and not providing them with tools to do this dangerous work, then our societies are not going to get better,” said Adrian Shahbaz, director of technology and democracy for Freedom House, a Washington-based pro-democracy think tank. “If everyone is afraid of taking on the powerful because they fear the consequences of it, then that would be disastrous to the state of democracy.”

Hatice Cengiz, the fiancee of slain Washington Post contributing columnist Jamal Khashoggi, said she used an iPhone because she thought it would offer robust protection against hackers.

“Why did they say the iPhone is more safe?” Cengiz said in a June interview in Turkey, where she lives. Her iPhone was among the 23 found to have forensic evidence of successful Pegasus intrusion. The infiltration happened in the days after Khashoggi was killed in October 2018, the examination of her phone found.

NSO said in a statement that it had found no evidence that Cengiz’s phone had been targeted by Pegasus. “Our technology was not associated in any way with the heinous murder of Jamal Khashoggi,” the company said.

A head-to-head comparison of the security of Apple’s and Google’s operating systems and the devices that run them is not possible, but reports of hacks to iPhones have grown in recent years as security researchers have discovered evidence that attackers had found vulnerabilities in such widely used iPhone apps as iMessage, Apple Music, Apple Photos, FaceTime and the Safari browser.

The investigation found that iMessage — the built-in messaging app that allows seamless chatting among iPhone users — played a role in 13 of the 23 successful infiltrations of iPhones. IMessage was also the mode of attack in six of the 11 failed attempts Amnesty’s Security Lab identified through its forensic examinations.

One reason that iMessage has become a vector for attack, security researchers say, is that the app has gradually added features, which inevitably creates more potential vulnerabilities.

“They can’t make iMessage safe,” said Matthew Green, a security and cryptology professor at Johns Hopkins University. “I’m not saying it can’t be fixed, but it’s pretty bad.”

One key issue: IMessage lets strangers send iPhone users messages without any warning to or approval from the recipient, a feature that makes it easier for hackers to take the first steps toward infection without detection. Security researchers have warned about this weakness for years.

“Your iPhone, and a billion other Apple devices out-of-the-box, automatically run famously insecure software to preview iMessages, whether you trust the sender or not,” said security researcher Bill Marczak, a fellow at Citizen Lab, a research institute based at the University of Toronto’s Munk School of Global Affairs & Public Policy. “Any Computer Security 101 student could spot the flaw here.”

Google’s Project Zero, which searches for exploitable bugs across a range of technology offerings and publishes its findings publicly, reported in a series of blog posts last year on vulnerabilities to iMessage.

The encrypted chat app Signal adopted new protections last year requiring user approval when an unfamiliar user attempts to initiate a call or text — a protection Apple has not implemented with iMessage. Users of iPhones can choose to filter unfamiliar users by activating a feature in their devices’ settings, though research for many years has shown that ordinary users of devices or apps rarely take advantage of such granular controls.

In a 2,800-word email responding to questions from The Post that Apple said could not be quoted directly, the company said that iPhones severely restrict the code that an iMessage can run on a device and that it has protections against malware arriving in this way. It said BlastDoor examines Web previews and photos for suspicious content before users can view them but did not elaborate on that process. It did not respond to a question about whether it would consider restricting messages from senders not in a person’s address book.

The Amnesty technical analysis also found evidence that NSO’s clients use commercial Internet service companies, including Amazon Web Services, to deliver Pegasus malware to targeted phones. (Amazon’s executive chairman, Jeff Bezos, owns The Post.)

Kristin Brown, a spokeswoman for Amazon Web Services, said, “When we learned of this activity, we acted quickly to shut down the relevant infrastructure and accounts.”

Hard lessons

The infiltration of Mangin’s iPhones underscores hard lessons about privacy in the age of smartphones: Nothing held on any device is entirely safe. Spending more for a premium smartphone does not change that fact, especially if some nation’s intelligence or law enforcement agencies want to break in. NSO reported last month that it has 60 government customers in 40 countries, meaning some nations have more than one agency with a contract.

New security measures often exact costs to consumers in terms of ease of use, speed of apps and battery life, prompting internal struggles in many technology companies over whether such performance trade-offs are worth the improved resistance to hacking that such measures provide.

One former Apple employee, who spoke on the condition of anonymity because Apple requires its employees to sign agreements prohibiting them from commenting on nearly all aspects of the company, even after they leave, said it was difficult to communicate with security researchers who reported bugs in Apple products because the company’s marketing department got in the way.

“Marketing could veto everything,” the person said. “We had a whole bunch of canned replies we would use over and over again. It was incredibly annoying and slowed everything down.”

Apple also restricts the access outside researchers have to iOS, the mobile operating system used by iPhones and iPads, in a way that makes investigation of the code more difficult and limits the ability of consumers to discover when they’ve been hacked, researchers say.

In its email response to questions from The Post, Apple said its product marketing team has a say only in some interactions between Apple employees and outside security researchers and only to ensure the company’s messaging about new products is consistent. It said it is committed to giving tools to outside security researchers and touted its Security Research Device Program, in which the company sells iPhones with special software that researchers can use to analyze iOS.

Critics — both inside and outside the company — say Apple also should be more focused on tracking the work of its most sophisticated adversaries, including NSO, to better understand the cutting-edge exploits attackers are developing. These critics say the company’s security team tends to focus more on overall security, by deploying features that thwart most attacks but may fail to stop attacks on people subject to government surveillance — a group that often includes journalists, politicians and human rights activists such as Mangin.

“It’s a situation where you’re always working with an information deficit. You don’t know a whole lot about what’s out there,” said a former Apple engineer, speaking on the condition of anonymity because Apple does not permit former employees to speak publicly without company permission. “When you have a well-resourced adversary, different things are on the table.”

In its email to The Post, Apple said that in recent years it has significantly expanded its security team focused on tracking sophisticated adversaries. Apple said in the email that it is different from its competitors in that it elects not to discuss these efforts publicly, instead focusing on building new protections for its software. Overall, its security team has grown fourfold over the past five years, Apple said.

Apple’s business model relies on the annual release of new iPhones, its flagship product that generates half of its revenue. Each new device, which typically arrives with an updated operating system available to users of older devices, includes many new features — along with what security researchers call new “attack surfaces.”

Current and former Apple employees and people who work with the company say the product release schedule is harrowing, and, because there is little time to vet new products for security flaws, it leads to a proliferation of new bugs that offensive security researchers at companies like NSO Group can use to break into even the newest devices.

In its email to The Post, Apple said it uses automated tools and in-house researchers to catch the vast majority of bugs before they’re released and that it is the best in the industry.

Apple also was a relative latecomer to “bug bounties,” where companies pay independent researchers for finding and disclosing software flaws that could be used by hackers in attacks.

Krstić, Apple's top security official, pushed for a bug bounty program that was added in 2016, but some independent researchers say they have stopped submitting bugs through the program because Apple tends to pay small rewards and the process can take months or years.

Last week, Nicolas Brunner, an iOS engineer for Swiss Federal Railways, detailed in a blog post how he submitted a bug to Apple that allowed someone to permanently track an iPhone user's location without their knowledge. He said Apple was uncommunicative, slow to fix the bug and ultimately did not pay him.

Asked about the blog post, an Apple spokesman referred to Apple's email in which it said its bug bounty program is the best in the industry and that it pays higher rewards than any other company. In 2021 alone, it has paid out millions of dollars to security researchers, the email said.

People familiar with Apple's security operations say Krstić has improved the situation, but Apple's security team remains known for keeping a low public profile, declining to make presentations at conferences such as the heavily attended Black Hat cybersecurity conference in Las Vegas each summer, where other tech companies have become fixtures.

Once a bug is reported to Apple, it's given a color code, said former employees familiar with the process. Red means the bug is being actively exploited by attackers. Orange, the next level down, means the bug is serious but that there is no evidence it has been exploited yet. Orange bugs can take months to fix, and the engineering team, not security, decides when that happens.

Former Apple employees recounted several instances in which bugs that were not believed to be serious were exploited against customers between the time they were reported to Apple and when they were patched.

Apple said in its email that no system is perfect but that it rapidly fixes serious security vulnerabilities and continues to invest in improving its system for assessing the seriousness of bugs.

But outside security researchers say they cannot be sure how many iOS users are exploited because Apple makes it difficult for researchers to analyze the information that would point to exploits.

"I think we're seeing the tip of the iceberg at the moment," said Costin Raiu, director of the global research and analysis team at cybersecurity firm Kaspersky Lab. "If you open it up and give people the tools and ability to inspect phones, you have to be ready for the news cycle which will be mostly negative. It takes courage."

Dana Priest contributed to this report.

The Pegasus Project is a collaborative investigation that involves more than 80 journalists from 17 news organizations coordinated by Forbidden Stories with the technical support of Amnesty International's Security Lab. Read more about this project.

THE PEGASUS PROJECT

HAND CURATED

Private Israeli spyware used to hack cellphones of journalists, activists worldwide

July 18, 2021

Despite the hype, iPhone security no match for NSO spyware

July 19, 2021

Key question for Americans overseas: Can their phones be hacked?

July 19, 2021

View 3 more stories