How a hacked phone may have led killers to Khashoggi

Oren Liebermann
CNN, January 12, 2019

(CNN) — Jamal Khashoggi probably thought the messages he was sending to fellow Saudi dissident Omar Abdulaziz were hidden, cloaked in WhatsApp security. In reality they were compromised -- along with the rest of Abdulaziz's phone, which had allegedly been infected by Pegasus, a powerful piece of malware designed to spy on its users.

Abdulaziz, as CNN reported last month, is suing the creators of Pegasus, Israel-based cyber company NSO Group, accusing them of violating international law by selling the software to oppressive regimes.

NSO has denied any involvement in the death of Khashoggi, insisting its software is "only for use fighting terrorism and crime."

The company was condemned as "the worst of the worst" by NSA whistleblower Edward Snowden during a video conference with an Israeli audience last November.

"The NSO Group in today's world, based on the evidence we have, they are the worst of the worst in selling these burglary tools that are being actively currently used to violate the human rights of dissidents, opposition figures, and activists," Snowden said.

Remembering Jamal Khashoggi, 100 days on 18:33

Big threat

I witnessed the power of Pegasus two years ago. Mobile security experts at Check Point, one of the world leaders in cyber security, showed me how they could hack a phone with one click, gaining complete access to its microphone, camera, keyboard, and data.

They say the malware they used was similar to Pegasus: An apparently innocent message appeared on my phone asking me to update my settings, and that was all they needed to access the phone.

Cyber security expert Michael Shaulov launched a cybersecurity startup in 2010, partly in response to what he saw as the potential threat of Pegasus.

"Even when [NSO Group sells] the software to specifically the law enforcement agency that specifically bought it, in the case that those guys want to go after what we call illegitimate targets, NSO has no control [over it]," he says. "They cannot really prevent it."

NSO Group says it can monitor the usage of all of its software by all of its clients, but would need to actively check how clients were using their products before becoming aware of any possible misuse.

The company's technology takes advantage of what is known as "zero days" -- hidden vulnerabilities in operating systems and apps that grant elite hackers access to the inner workings of the phone. The term is derived from the fact that software developers have had no time to fix them.

Companies like NSO have teams of researchers continuously reverse-engineering Apple and Android operating systems to find bugs in the code they can then exploit, Shaulov says, describing the process of finding zero days as an "art" in the largely black and white world of cyber security.

NSO Group's singular focus on mobile devices has made them the "alpha dog" in the market, Shaulov says.

Finding a zero day can take anywhere from a few months to more than a year, and there is little guarantee of its long-term effectiveness. But if the weakness isn't fixed, it can be exploited repeatedly to hack phones. Software developers such as Apple and Google have teams devoted to finding and fixing vulnerabilities, but it's no easier for them than it is for hackers to find the weak link. In addition, developers' priorities may lie elsewhere, so even known bugs remain unfixed.

"Unless Apple or Google fixes that bug, that vulnerability ... can stay for many, many years and NSO can continuously sell software that can go through those bugs in the software and infect those phones," says Shaulov.

Researchers at the Toronto-based Citizen Lab have tracked the use of NSO Group's Pegasus software to 45 countries where operators "may be conducting surveillance operations," including at least 10 Pegasus operators who "appear to be actively engaged in cross-border surveillance."

TIME magazine names 2018 'Person of the Year' 00:57

Khashoggi: 'God help us'

The software, able to infect a phone after a single click on a link in a fake text message, then grants hackers complete access to the phone. Data stored on the phone, messages, phone calls and even GPS location data are visible, allowing hackers to see where someone is, who he or she is talking to, and about what.

In the case of Khashoggi, Citizen Lab researchers say the text message went to Abdulaziz, disguised as a shipping update about a package he had just ordered. The link, which Citizen Lab says it traced to a domain connected to Pegasus, led to Abdulaziz's phone becoming infected with the malware, giving hackers access to virtually his entire phone, including his daily conversations with Khashoggi.

In one text, before his death on October 2 at the Saudi consulate in Istanbul, Khashoggi learned that his conversations with Abdulaziz may have been intercepted. "God help us," he wrote. CNN was granted access to the correspondence between Khashoggi and Montreal-based activist Abdulaziz.

Two months later Khashoggi entered the building for what he thought was a routine appointment to pick up papers that would allow him to marry his Turkish fiancée, Hatice Cengiz. Minutes later, he was killed in what the Saudi attorney general later acknowledged was a premeditated murder.

The Saudis have presented shifting stories about Khashoggi's fate, initially denying any knowledge before arguing that a group of rogue operators, many of whom belong to Saudi Crown Prince Mohammed bin Salman's inner circle, were responsible for the journalist's death.

Riyadh has maintained that neither bin Salman nor King Salman knew of the operation to target Khashoggi. US officials, however, have said such a mission -- including 15 men sent from Riyadh -- could not have been carried out without the authorization of bin Salman.

WaPo editor: Crown Prince in global thugs club 01:20

NSO speaks out

In the first interview given by NSO Group since the company was implicated in the Khashoggi case, CEO Shalev Hulio categorically denied any involvement in the tracking of the Saudi journalist or his killing. Calling his death a "shocking murder," Hulio said that following checks carried out by NSO Group, the company would have known immediately if their software had been used to track a journalist.

"We conducted a thorough check of all our clients, not just one client who may be a potential suspect involved in the case, but also other clients who might perhaps have an interest in following him for some reason," explained Hulio in the interview with Yedioth Ahronoth, one of Israel's largest newspapers. "We checked all our clients, both through conversations with them, and through a fool-proof technological check.

The systems produce their own documentation, and it is not possible to act against this or that target without us being able to check it."

"I'm saying on the record that after all these checks there was no use of any NSO product or technology on Khashoggi; and that includes tapping, monitoring, finding location, or gathering intelligence. Exclamation mark! The story is simply not true."

Shalev Hulio -- whose first name is the "S" in NSO -- says NSO Group can disconnect a client's software if it is used inappropriately or against improper targets, like journalists or human rights activists who are just doing their jobs.

"In cases where the system is misused, assuming we are aware of it, the technological system that we sold them will be immediately disconnected; that is something we are able to do both technologically and legally."

Hulio said that NSO has "permanently" shut off the systems of three clients because of misuse, though he did not specify which clients.

Asked repeatedly if Pegasus had been sold to Saud al-Qahtani, a high-ranking Saudi official accused by Saudi prosecutors of playing a major role in Khashoggi's murder, who has close ties to Crown Prince Mohammed bin Salman, Hulio said it had not, and insisted that NSO does not sell to "private elements."

"All sales are authorized by Israel's Defense Ministry and are only made to states and their police and law enforcement organizations," he said, and "only for use fighting terrorism and crime."

Asked point blank if NSO Group sold the system to Saudi Arabia, Hulio said, "We do not comment on any questions about specific clients. We can neither deny or confirm."

Worldwide, Hulio said there are no more than 150 "active targets" currently being tracked with NSO's technology. He said the previous year was the best in the company's history and that the system had been sold to "dozens of countries worldwide on all continents apart from Antarctica."

Hulio repeatedly portrayed his company as one that helped the world's intelligence agencies fight terrorism, touting the lives saved by the technology.

"I will say with modesty that thousands of people in Europe owe their lives to the hundreds of workers [we have] in Herzliya," he said referring to the Israeli town where the company is based. "I reiterate that any use [of our technology] that goes beyond the criteria of saving human lives at risk from crime or terror will prompt our company to take immediate steps, unequivocally and decisively."

Potential attack surface

The findings of Citizens Lab, which Hulio dismissed as inaccurate, paint "a bleak picture of the human rights risk" of Pegasus, Citizen Lab say, adding that "at least six countries with significant Pegasus operations have previously been linked to abusive use of spyware to target civil society, including Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia, and the United Arab Emirates."

Apple, Google and other tech firms are constantly working to fix bugs and close zero days in their software. New features they introduce brings with it new code, introducing the possibility of new vulnerabilities. The software developers devote millions of dollars to close these vulnerabilities before they're discovered; hackers devote time and energy to discover them before they're closed. It's a 21st century digital arms race.

Adam Donenfeld, a researcher who focuses on mobile security at Zimperium, says the number of places to hack a phone, called potential attack surfaces, are nearly limitless.

Donenfeld says it's hard to pin down precisely how many exist, "but way more than people think. There are a lot of them ... there are always new vulnerabilities being introduced to devices."

Any interaction, however simple, between a device and a phone is a potential attack surface. Donenfeld uses the example of chat applications, but says it's not just chat apps that provide potential ways in for hackers.

If a hacker sends a video to your phone, even before you open it, your phone has already received some metadata about the video. It has also notified the hacker that the video has been received. You don't need to click on the video or accept the message to create a potential attack surface.

"I can send you a malicious data packet that can cause some memory corruption on your phone that can happen remotely just by you having [a chat app]," explains Donenfeld. "You receive messages even if the app is closed because it runs in the background, [so] there is the possibility of running code on your device without you knowing about it."

Value of malware

Though the number of potential attack surfaces may by nearly limitless, very few offer the complete access elite hackers seek. In addition, there are relatively few cyber experts who understand how to take advantage of the zero day vulnerabilities.

The scarcity of zero days, coupled with the technical difficulty needed to uncover them, makes them incredibly valuable to the right buyer.

"If you have a working complete chain, it is definitely [worth] more than a million dollars," says Donenfeld. "There's always demand. There's always someone going to buy them."

NSO Group has apparently capitalized on that demand, making them a multi-million-dollar company with a powerful product.

But that product -- Pegasus -- has also put NSO at the center of a series of lawsuits that alleged use of the malware, as in the case of Jamal Khashoggi, violated international law.

NSO told CNN in December Abdulaziz's lawsuit was "completely unfounded," and that it showed "no evidence that the company's technology was used."

"The lawsuit appears to be based on a collection of press clippings that have been generated for the sole purpose of creating news headlines," NSO said in a statement. "In addition, products supplied by NSO are operated by the government customer to whom they are supplied, without the involvement of NSO or its employees."