Pegasus spyware: how does it work?

July 19 2021, by Katy Lee

More recent versions of Pegasus have exploited weak spots in software commonly installed on mobile phones.

Governments around the world are facing bombshell allegations that they used Israeli-made malware to spy on the phones of activists, journalists, corporate executives and politicians.

But how exactly does the Pegasus spyware work? How does it get onto people's phones—and what can it do once it's there?

How does Pegasus sneak its way onto a phone?

Researchers believe that early versions of the hacking software, first detected in 2016, used booby-trapped text messages to install itself onto the phones of targets.

The recipient would have to click on a link in the message in order for the spyware to download.

But this limited the chances of a successful installation—particularly as phone users have grown increasingly wary of clicking on suspicious links.

More recent versions of Pegasus, developed by the Israeli firm the NSO Group, have exploited weak spots in software commonly installed on mobiles.

In 2019 the messaging service WhatsApp sued NSO, saying it used one of these so-called "zero-day vulnerabilities" in its operating system to install the spyware on some 1,400 phones.

By simply calling the target through WhatsApp, Pegasus could secretly download itself onto their phone—even if they never answered the call.

More recently, Pegasus is reported to have exploited weaknesses in Apple's iMessage software.

That would potentially give it access to the one billion Apple iPhones currently in use—all without the owners needing to even click a button.

What does the malware do once it's installed?

"Pegasus is probably one of the most capable remote access tools there is," said Alan Woodward, cybersecurity professor at the University of Surrey in the UK.

"Think of it as if you've put your phone in someone else's hands."

It can be used to read the target's messages and emails, look through the photos they've taken, eavesdrop on their calls, track their location and even film them through their camera.

Pegasus' developers have got "better and better at hiding" all trace of the software, making it difficult to confirm whether a particular phone has been bugged or not, Woodward said.

That is why it remains unclear how many people have had their devices tapped, although new reports by international media say more than 50,000 phone numbers had been identified as being of interest to NSO clients.

However, Amnesty International's Security Lab, one of the organisations investigating Pegasus, said it had found traces of successful attacks on Apple iPhones as recently as this month.

How did NSO develop such powerful spyware?

Multi-billion-dollar tech companies like Apple and Google invest vast amounts of cash each year in making sure they aren't vulnerable to hackers who could bring their systems crashing down.

They even offer "bug bounties" to hackers, paying handsome rewards if they warn the company about flaws in their software before they can be used to launch an attack.

Woodward said Apple, which prides itself on a reputation for security, had "made some fairly big efforts" to identify weak spots.

But "inevitably there will be one or two" flaws in such complex software.

Analysts also believe NSO, whose staff includes elite former members of the Israeli military, likely keeps a close eye on the dark web, where hackers frequently sell information about security flaws they have found.

"It's also worth saying that not everyone has an up-to-date phone with up-to-date software on it," Woodward added.

"Some of the old vulnerabilities that Apple has closed down, and which Google have closed down with Android—they can still be out there."

Is it possible to remove the spyware?

Since it's extremely difficult to know for sure if your phone is carrying the malware, it's also difficult to know definitively that it has been removed.

Woodward said Pegasus may install itself onto the phone's hardware or into its memory, depending on the version.

If it's stored in the memory, rebooting the phone could in theory wipe it off—so he recommended that people at risk of being targeted, such as business leaders and politicians, regularly switch their devices off and on again.

"It sounds like overkill to a lot of people, but there is anti-malware software out there for mobile devices," he added.

"If you're someone at risk, you probably want to have some anti-malware software installed on your phone."

Citation: Pegasus spyware: how does it work? (2021, July 19) retrieved 19 April 2024 from https://techxplore.com/news/2021-07-pegasus-spyware.html