How does the Pegasus spyware work, and is my phone at risk

Paul Haskell-Dowland, *Edith Cowan University* and Roberto Musotto, *Edith Cowan University*

A major journalistic investigation has found evidence of malicious software being used by governments around the world, including allegations of spying on prominent individuals.

From a list of more 50,000 phone numbers, journalists identified more than 1,000 people in 50 countries reportedly under surveillance using the Pegasus spyware. The software was developed by the Israeli company NSO Group and sold to government clients.

Among the reported targets of the spyware are journalists, politicians, government officials, chief executives and human rights activists.

Reports thus far allude to a surveillance effort reminiscent of an Orwellian nightmare, in which the spyware can capture keystrokes, intercept communications, track the device and use the camera and microphone to spy on the user.

How did they do it?

The Pegasus spyware can infect the phones of victims through a variety of mechanisms. Some approaches may involve an SMS or iMessage that provides a link to a website. If clicked, this link delivers malicious software that compromises the device.

Others use the more concerning “zero-click” attack where vulnerabilities in the iMessage service in iPhones allows for infection by simply receiving a message, and no user interaction is required.

The aim is to seize full control of the mobile device’s operating system, either by rooting (on Android devices) or jailbreaking (on Apple iOS devices).

Usually, rooting on an Android device is done by the user to install applications and games from non-supported app stores, or re-enable a functionality that was disabled by the manufacturer.

Similarly, a jailbreak can be deployed on Apple devices to allow the installation of apps not available on the Apple App Store, or to unlock the phone for use on alternative cellular networks. Many jailbreak approaches require the phone to be connected to a computer each time it’s turned on (referred to as a “tethered jailbreak”).

Rooting and jailbreaking both remove the security controls embedded in Android or iOS operating systems. They are typically a combination of configuration changes and a “hack” of core elements of the operating system to run modified code.

In the case of spyware, once a device is unlocked, the perpetrator can deploy further software to secure remote access to the device’s data and functions. This user is likely to remain completely unaware.

Most media reports on Pegasus relate to the compromise of Apple devices. The spyware infects Android devices too, but isn’t as effective as it relies on a rooting technique that isn’t 100% reliable. When the initial infection attempt fails, the spyware supposedly prompts the user to grant relevant permissions so it can be deployed effectively.

But aren’t Apple devices more secure?

Apple devices are generally considered more secure than their Android equivalents, but neither type of device is 100% secure.

Apple applies a high level of control to the code of its operating system, as well as apps offered through its app store. This creates a closed-system often referred to as “security by obscurity”. Apple also exercises complete control over when updates are rolled out, which are then quickly adopted by users.

Apple devices are frequently updated to the latest iOS version via automatic patch installation. This helps improve security and also increases the value of finding a workable compromise to the latest iOS version, as the new one will be used on a large proportion of devices globally.

On the other hand, Android devices are based on open-source concepts, so hardware manufacturers can adapt the operating system to add additional features or optimise performance. We typically see a large number of Android devices running a variety of versions — inevitably resulting in some unpatched and insecure devices (which is advantageous for cybercriminals).

Ultimately, both platforms are vulnerable to compromise. The key factors are convenience and motivation. While developing an iOS malware tool requires greater investment in time, effort and money, having many devices running an identical environment means there is a greater chance of success at a significant scale.

While many Android devices will likely be vulnerable to compromise, the diversity of hardware and software makes it more difficult to deploy a single malicious tool to a wide user base.

How can I tell if I’m being monitored?

While the leak of more than 50,000 allegedly monitored phone numbers seems like a lot, it’s unlikely the Pegasus spyware has been used to monitor anyone who isn’t publicly prominent or politically active.

It is in the very nature of spyware to remain covert and undetected on a device. That said, there are mechanisms in place to show whether your device has been compromised.

The (relatively) easy way to determine this is to use the Amnesty International Mobile Verification Toolkit (MVT). This tool can run under either Linux or MacOS and can examine the files and configuration of your mobile device by analysing a backup taken from the phone.

While the analysis won’t confirm or disprove whether a device is compromised, it detects “indicators of compromise” which can provide evidence of infection.

In particular, the tool can detect the presence of specific software (processes) running on the device, as well as a range of domains used as part of the global infrastructure supporting a spyware network.

What can I do to be better protected?

Unfortunately there is no current solution for the zero-click attack. There are, however, simple steps you can take to minimise your potential exposure — not only to Pegasus but to other malicious attacks too.

1) Only open links from known and trusted contacts and sources when using your device. Pegasus is

deployed to Apple devices through an iMessage link. And this is the same technique used by many cybercriminals for both malware distribution and less technical scams. The same advice applies to links sent via email or other messaging applications.

2) Make sure your device is updated with any relevant patches and upgrades. While having a standardised version of an operating system creates a stable base for attackers to target, it's still your best defence.

If you use Android, don't rely on notifications for new versions of the operating system. Check for the latest version yourself, as your device's manufacturer may not be providing updates.

3) Although it may sound obvious, you should limit physical access to your phone. Do this by enabling pin, finger or face-locking on the device. The eSafety Commissioner's website has a range of videos explaining how to configure your device securely.

4) Avoid public and free WiFi services (including hotels), especially when accessing sensitive information. The use of a VPN is a good solution when you need to use such networks.

5) Encrypt your device data and enable remote-wipe features where available. If your device is lost or stolen, you will have some reassurance your data can remain safe.

Correction: this article was changed to reflect reports iPhone users targeted with the Pegasus spyware seem to have been targeted specifically with zero-click attacks.

Paul Haskell-Dowland, Associate Dean (Computing and Security), *Edith Cowan University* and Roberto Musotto, Research fellow, *Edith Cowan University*