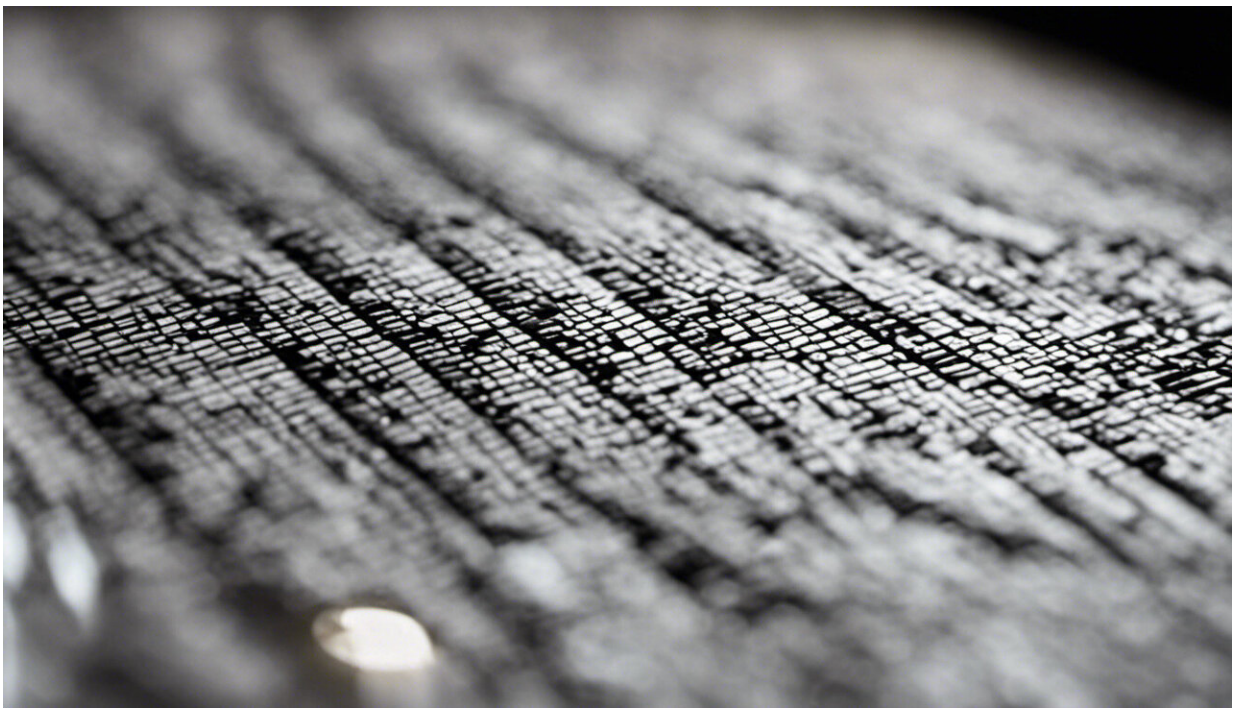
Spyware: Why the booming surveillance tech industry is vulnerable to corruption and abuse

July 23 2021, by Christian Kemp



Credit: AI-generated image (disclaimer)

The world's most sophisticated commercially available spyware may be being abused, according to an investigation by 17 media organizations in ten countries. Intelligence leaks and forensic phone analysis suggests the surveillance software, called Pegasus, has been used to target and spy on

the phones of human rights activists, investigative journalists, politicians, researchers and academics.

NSO Group, the Israeli cyber intelligence firm behind Pegasus, insists that it only licenses its spyware to vetted government clients in the name of combating transnational crime and terrorism. It has labeled reports from investigative journalists a "vicious and slanderous campaign" upon which it will no longer comment.

Yet the founder and chief executive of NSO Group previously admitted that "in some circumstances our customers might misuse the system." Given that the group has sold its spyware to a reported 40 countries, including some with poor records of corruption and human rights violations, it's alleged that Pegasus has been significantly misused, undermining the freedom of the press, freedom of thought and free and open democracies.

These revelations are the latest indication that the spyware industry is out of control, with licensed customers free to spy on political and civilian targets as well as suspected criminals. We may be heading to a world in which no phone is safe from such attacks.

How Pegasus works

Pegasus is regarded as the most advanced spyware on the market. It can infiltrate victims' devices without their even having to click a malicious link—a so-called "zero-click attack". Once inside, the power Pegasus possesses to transform a phone into a surveillance beacon is astounding.

It immediately sets to work copying messages, pictures, videos and downloaded content to send to the attacker. As if that's not insidious enough, Pegasus can record calls and track a target's location while independently and secretly activating a phone's camera and microphone.

With this capability, an infected phone acts like a fly on the wall, seeing, hearing and reporting back the intimate and sensitive conversations that it watches continuously.

There's previous evidence of Pegasus misuse. It was implicated in the alleged hacking of Jeff Bezos' phone by the crown prince of Saudi Arabia in 2018. The following year, it was revealed that several Indian lawyers and activists had been targeted by a Pegasus attack via WhatsApp.

The new revelations suggest that Pegasus was used to watch Mexico's president Andres Manuel Lopez and 50 members of his inner circle—including friends, family, doctors, and aides—when he was an opposition politician. Pegasus has also been linked to the surveillance of Rahul Gandhi, the current political rival to Indian prime minister Narendra Modi.

A Pegasus infiltration has also now been found among phones belonging to the family and friends of murdered journalist Jamal Khashoggi, and there are indications that Pegasus may also have been used by a Mexican NSO client to target the Mexican journalist Cecilio Pineda Birto, who was murdered in 2017.

Spyware industry

Although the power of Pegasus is shocking, spyware in its various forms is far from a new phenomenon. Basic spyware can be traced back to the early 1990s. Now it's a booming industry with thousands of eager buyers.

At the base of the spyware industry are the lesser snooping tools, sold for as little as $70 (£51) on the dark web, which can remotely access webcams, log computer keystrokes and harvest location data. The use of such spyware by stalkers and abusive partners is a growing, concerning

issue.

Then of course there's the global surveillance estate that Edward Snowden lifted the curtain on in 2013. His leaks revealed how surveillance tools were being used to amass a volume of citizens' personal data that seemed to go well beyond the brief of the intelligence agencies using them.

In 2017, we also learned how a secret team of elite programmers at the US National Security Agency had developed an advanced cyber-espionage weapon called Eternal Blue, only for it to be stolen by the hacker collective Shadow Brokers and sold on the dark web. It was this spyware that would later be used as the backbone of the infamous 2017 Wannacry ransomware attack, which targeted the NHS and hundreds of other organizations.

Why Pegasus is different

When the Snowden leaks were published, many were shocked to learn of the scale of surveillance that digital technologies had enabled. But this mass spying was at least developed and conducted within state intelligence agencies, who had some legitimacy as agents of espionage.

We're no longer debating the right of the state to violate our own rights to privacy. The Pegasus revelations show we've arrived in a new, uncomfortable reality where highly sophisticated spyware tools are sold on an open market. To be under no illusion, we're referring here to an industry of for-profit malware developers creating and selling the same types of tools—and sometimes the very same tools—used by "bad hackers" to bring businesses and government organizations to their knees.

In the wake of the Pegasus revelations, Edward Snowden has called for

an international spyware ban, stating that we're moving towards a world where no device is safe. That will certainly be the case if Pegasus meets the same fate as Eternal Blue, with its source code finding its way onto the dark web for use by criminal hackers.

We've only just begun to fully contemplate the full implications of Pegasus on our collective privacy and democracy. Without transparency, we have no sense of how and under what circumstances Pegasus is licensed, who has authorisation to use Pegasus once it's licensed, under what circumstances a license may be revoked, or what international regulations are in place to police against its abuse. Evidence suggests that Pegasus has been misused and greater accountability and oversight is needed. We must also seek to rekindle important debates around enforceable controls on the creation and sale of corporate spyware. Without this, the threat that Pegasus and future spyware tools pose to privacy will not be limited to the high-profile targets that have so far been revealed, but will be a threat to us all.

Provided by The Conversation