bizcommunity

Media: How to protect your phone from spyware

The Committee to Protect Journalists (CPJ) has issued a global safety advisory for journalists regarding the use of Pegasus spyware to target the media. The spyware gives the attacker the ability to monitor, record, and collect existing and future data from mobile phones.

Image source: Gallo/Getty.

Pegasus is a spyware created for mobile devices which transforms a cellphone into a mobile surveillance station. Researchers have documented it being used to spy on journalists. This raises significant implications for journalists' own security and that of their sources.

In 2018, Citizen Lab said it had detected Pegasus in over 45 countries. Pegasus could have been deploy against journalists and civil society actors in Mexico, Saudi Arabia, Bahrain, Morocco, Togo, Israel, the U.S and the United Arab Emirates, the report found.

In May 2019, a vulnerability was identified in the messaging app WhatsApp that, before it was patched, infected some of its users' phones with spyware, including over 100 human rights defenders and journalis in at least 20 countries, according to Citizen Lab. WhatsApp, which is owned by Facebook, later identified that spyware as Pegasus or a variant produced by the Israel-based NSO Group, which markets tools for investigating crime and terrorism to government agencies. (NSO Group has repeatedly told CPJ that it will not comment on individual cases, but investigates reports that its products were misused in breach of contract.)

The spyware gives the attacker the ability to monitor, record, and collect existing and future data from the phone. This includes calls and information from messaging applications and real-time location data. The spyware is able to remotely activate the camera and microphone to surveil the target and their surrounding

Pegasus is designed to be installed on phones running Android, BlackBerry OS, and iOS without alerting t target to its presence. Journalists will likely only know if their phone has been infected if the device is inspected by a tech expert.

If you have reason to believe you have been targeted and have spyware on your device:

- Stop using the device immediately.
- Put the device somewhere that does not compromise you or your surroundings.
- Log out of all accounts and unlink them from the device.
- From a different device, change all your account passwords.
- Seek expert digital security advice. If you are a freelance journalist or do not have access to tech support, contact the Access Now Helpline.

Pegasus can be installed in a number of ways. Journalists should keep up to date on these methods and take appropriate steps to protect themselves and their sources.

Zero-day attacks

Zero-day attacks exploit vulnerable software, not people. They require no interaction from the user.

Reports from the WhatsApp hack stated that the attack took the form of calls from unknown numbers to users which resulted in the app crashing. The numbers disappeared from the call log, leaving no record of missed call or who had made it.

Protecting yourself against a zero-day attack is difficult. Journalists who may be targeted by a sophisticate adversary such as a government should consider changing cheap, burner phones every few months as a precaution. If possible, contact a digital security expert for one-to-one support.

Spear-phishing attacks

Attackers create tailor-made messages that are sent to a specific journalist. These messages convey a sense of urgency and contain a link or a document which the journalist is encouraged to click on. The messages come in a variety of forms, including SMS, email, through messaging apps such as WhatsApp via messages on social media platforms. Once the journalist has clicked on the link, then the spyware is installed on their phone.

Research by Citizen Lab and Amnesty International found that messages tend to take the following forms:

- Messages purporting to be from a known organization such as an embassy or a local news organisation.
- Messages that warn the target may be facing an immediate security threat.
- Messages that raise any work-related issue, such as covering an event that the target usually reports
- Messages that make appeals on personal matters, such as those relating to compromising photos of partners.
- Financial messages that reference purchases, credit cards, or banking details.
- The suspect messages may also arrive from unknown numbers.
- Pegasus could have been deployed against journalists and civil society actors in Mexico, Saudi Arabi Bahrain, Morocco, Togo, Israel, the U.S., and the United Arab Emirates.

Attackers can target personal and work phones. To better protect themselves and their sources, journalist should:

- Verify the link with the sender through a different channel of communication. This should preferably b through video or voice.

- If the sender is not previously known to you, secondary channels may not provide successful verification of the links, as secondary channels may be set up by the adversary as part of an elaborate cover identity.
- If the link utilises a URL shortener service like TinyURL or Bitly, input the link into a URL expander service such as Link Expander or URLEX. If the expanded link looks suspicious, for instance mimicki a local news website but not being quite the same, do not click on the link.
- If you feel you need to open the link, do not use your primary device. Open the link on a separate, secondary device that does not have any sensitive information or contact details, and is used solely f viewing links. Carry out a factory reset on the device regularly (keeping in mind that this might not remove the spyware). Keep the secondary device turned off, with the battery removed, when not in us
- Use a non-default browser for the phone. Pegasus is believed to target default browsers. The default browser for Android is Chrome and the default browser for iOS is Safari. Use an alternative browser such as Firefox Focus and open the link in that. However, there is no guarantee that Pegasus will not, has not, already targeted other browsers.

Physical installation by an adversary

Pegasus can also be installed on your phone if an adversary gains physical access to the device. To redu risk:

- Do not leave your device unattended and avoid handing over your phone to others.
- When crossing a border or checkpoint ensure that you can see your phone at all times Turn off the phone before arriving at the checkpoint, and have a complex passphrase consisting of both letters ar numbers. Be aware that if your phone is taken then the device may be compromised.

For more information to protect yourself and your sources, consult CPJ's Digital Safety Kit.

**With thanks to Citizen Lab for valuable insight.*