Pegasus Software Used Against A Newsroom Again

In December 2020, an extensive investigation by **Citizen Lab** detected Pegasus on the personal iPhones of 36 journalists and media executives; most worked at Al-Jazeera, but an Al-Araby TV journalist was among the targets. The Pegasus software gives an attacker the ability to monitor, record, and collect existing and future data from the phone. The investigation attributed the attacks to government agents, probably from Saudia Arabia and the United Arab Emirates, and said it was likely that only a fraction of targets had been detected.

Ela Stapley, HP Risk Management's and the CPJ's Digital Security Strategist, outlines the risks from the Pegasus spyware and how journalists can protect themselves.

What is Pegasus?

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.

Whereas previous attacks involved tricking users into installing the spyware on their devices through clicking on links included in messages, more recent attacks focus instead on using vulnerabilities in apps or software on the phone requiring no interaction from the user at all, according to a June 2020 report by **Amnesty International.**

Both Whatsapp and Iphone Messenger vulnerabilities have been used to seize access to devices. Once on the device, 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 surroundings.

Previous Attacks

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 journalists 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.)

In June 2020, an investigation by **Amnesty International** found that a Moroccan journalist's phone had become infected after internet traffic on the phone was rerouted to a malicious website controlled by the attackers. Once the phone's internet browser was connected to the site,

attackers likely exploited vulnerabilities in the software to compromise the device, the report found. The report states that this attack was either carried out by rerouting cell phone internet traffic using a rogue cell tower, a device that mimics the job of a cell phone tower, or through gaining access to the target's cell phone provider.

In 2018, **Citizen Lab** said it had detected Pegasus in over 45 countries. Pegasus could have been deployed 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.

Immediate Steps To Take If You Suspect You Have Been Hacked

Pegasus is designed to be installed on phones running Android, BlackBerry OS, and iOS without alerting the 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**.
- If it is essential to use the device before you can replace it, carry out a factory reset and ensure that your operating system, apps, and browsers, are updated to the latest version.

Installation & How To Minimise The Risk

Network injection attack

A network injection attack does not require any interaction with the user; instead, it involves the automatic redirecting of browsers or apps to sites controlled by attackers. This is also known as a Man in the Middle Attack (MITM). Once connected to the malicious site, attackers infect the device through vulnerabilities in the software.

A journalist is highly unlikely to know whether they have been the target of this type of network injection attack and protecting against it can be difficult. To minimize risk, media workers should use a Virtual Private Network (VPN) on both their cell phones and on their computers.

When choosing a VPN, journalists should consider the following:

- They should check the law with regards to the use of a VPN in the country they are living in or travelling to.

- Research the VPN company to ensure that it does not store data on users, including browser history and log in details, as this could be accessed by governments.
- Check whether the VPN provider has close links to government bodies or is owned by governments. They should choose a service that is located outside the country they live in and that has a good track record of privacy.

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 a missed call or who had made it.

The December 2020 **Citizen Lab** report found that attackers deployed spyware via a vulnerability in the iMessenger app, and required no interaction from the device's owner. The vulnerability appears to have been fixed in the iOS 14 update.

Protecting yourself against a zero-day attack is difficult. Journalists who may be targeted by a sophisticated adversary such as a government should consider changing cheap, burner phones every few months as a precaution. You should ensure that you regularly update your phone's operating system as well as apps and browsers. Regularly review the apps on your phone and delete ones that you are not using. 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 or 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 organization.
- 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 on.
- 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.

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

- Verify the link with the sender through a different channel of communication. This should preferably be 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 utilizes 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 mimicking 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 for 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 use.
- 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, or 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 reduce 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 and 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**.

HP Risk Management works with a number of newsrooms and journalist associations, providing on-call risk assessment support, safety advice and training. We continuously support journalists working in high risk and/or challenging environments. For more information please contact info@hpriskmanagement.com

Disclaimer: *This document has been prepared by HP Risk Management (herein "HP) and is based on information available at the time of writing. The information contained is advisory in nature and any actions taken by clients or third parties are their own responsibility. HP accepts no liability for any loss (direct or indirect) or damage suffered as a result of reliance on the information provided. While every care has been taken to ensure that the content is useful and accurate, HP gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information provided. Any errors or omissions brought to the attention of HP will be corrected as soon as possible. Any links to external websites or documents referenced should not be taken as an endorsement by HP. We assume no responsibility or liability for content provided via third party websites or any software viruses or harmful materials that they may contain.*