Detecting and protecting your smartphone from **PEGASUS Spyware**

What is Pegasus?

The spyware Pegasus has been attributed to the NSO Group, an Israeli company. As per recent reports this spyware has been used to facilitate human rights violations worldwide on a massive scale. It is a program that allows the attacker to access the infected smartphone's microphone and camera. One can even gain access to messages, emails and collect location data, giving near-complete access to one's smartphone.

The malware is commercial and sold to anyone willing to pay. It secretly roots a target's mobile phone and transforms it into a listening device.

NSO says it licenses the tool exclusively to government agencies to combat terrorism and other serious crimes. As per the NSO Group, the program has been sold only to fight against terrorism and crime.

The Kaspersky report mentions that Pegasus was discovered in 2017 by Ahmed Mansoor, a UAE human rights activist. He happened to be one of its targets through spear-phishing attacks.

How Does It Infect Your Smartphone?

WhatsApp is considered a secure platform, but it couldn't prevent its users from being attacked by the Pegasus spyware.

Pegasus was initially used to gain access to a phone through a malicious web link through a message or email attempted on Ahmed Mansoor. Once a user clicks on the link, Pegasus is automatically installed on the phone.

The spyware has also gained some new abilities. Researchers found that a phone can be infected with Pegasus just by calling via WhatsApp. The user doesn’t even have to pick up the call, and the device will still get infected; making it zero-click spyware needing no input from a victim.

Moreover, once it has access to the device, it can delete any call logs making it impossible for the victim to know that their phone was a target of the spyware.

Pegasus for Android does not rely on zero-day vulnerabilities. Instead, it uses a well-known rooting method called Framaroot, which is undetected to the victim. For iOS, it relied on three zero-day vulnerabilities that allowed it to jailbreak the device and install surveillance software silently.

How Do You Know If You Have Been Affected?

This malware is designed to evade forensic analysis, detection by anti-virus software, and has self-destruction features. Kaspersky researchers called it a 'tool for total surveillance.'

Pegasus spyware is nearly impossible to detect. After it is uninstalled, it doesn't leave any trace, and there is no way to tell whether the device was affected in the past.

Your phone will not show any lags or visible signs when it is infected by Pegasus.

One way to find out if you are infected with Pegasus is through WhatsApp. The app sends critical alert messages to the list of affected users, asking them to update to the application's latest version.

Till now, the message from WhatsApp and Citizen Lab is the only visible indicator that tells you whether your phone has been affected.
Another method to discover if you have been infected by the spyware on Android mobiles is to check if your device has been rooted without your knowledge using any root reviewing application.

Prevention/Staying Safe

Several cybersecurity analysts and experts have found that the only way to get completely rid of Pegasus is to discard the phone that has been affected.

According to Citizen Lab, even factory resetting your smartphone will not be helpful as it cannot eliminate the spyware. The attackers can continue to access your online accounts even after your device is no longer infected.

To ensure your online accounts are safe, change the passwords of all the applications and services you use on the infected device.

Diagnosis for Presence of Pegasus Spyware

1. Monitor the change in the daily data usage (The data usage is higher if the phone is infected by the spyware).
2. Check for any unknown WhatsApp missed calls.
3. Check for the unknown applications & processes running in the background.
4. Sudden battery drainage.
5. Poor and slow performance of your device.
6. Check for permissions of camera and microphone for unintended applications using these permissions.
7. WhatsApp alerts are important; WhatsApp will send regular alerts for updates.
8. Check whether the phone has been rooted (or jailbroken, in case of iPhones).
9. Other applications crash more often.

Mitigation

1. Users can deploy the Mobile Verification Toolkit (MVT) to detect the presence of Pegasus spyware. This tool works on both Android and iOS devices.
2. It is developed by Amnesty International, and it's a technical and command line or terminal-based tool.
3. First, it creates an encrypted backup by using either iTunes or Finder on a Mac or PC.
4. After the data backup and encryption, if you're using a Mac to run the check, you'll first need to install both Xcode (which can be downloaded from the App Store) and Python3 before you can install and run MVT. The easiest way to obtain Python3 is using a program called Homebrew, which can be installed and run from the Terminal. After installing these, you'll be ready to run through Amnesty's iOS instructions.
5. Illustration for Iphone →
    a. **#mvt-ios decrypt-backup -p PASSWORD -d decrypt ~/Desktop/bkp/orig**
    b. **#mvt-ios check-backup -o logs --iocs ~/Downloads/pegasus.stix2 ~/Desktop/bkp/decrypt**
6. The indicator of the compromised files are called out while running the actual scan, which Amnesty has provided in the form of a file pegasus.stix2.
7. After running the MVT, it will list the suspicious files, but it may not confirm yet whether you have been infected by the spyware or not.

Prevention from Pegasus Spyware

1. Don’t open any suspicious or malicious files and links; only open the links and files received from trusted sources.
2. Avoid using public and free WiFi Services; even if you are accessing them to use VPN (Virtual Private Network).
3. Limit the physical access of your devices.
4. Always make sure that all the applications and phone operating systems are updated with relevant patches and updates.
5. Encrypt your critical data.
6. Keep strong and hard-to-guess passwords for each device.
7. Install a security solution such as an antivirus on each of your devices.
8. Beware of phishing attacks. If you receive a link from an unknown source, do not click the link.

Prevention from Pegasus Spyware

1. https://www.theverge.com/2021/7/21/22587234/amnesty-international-nso-pegasus-spyware-detection-tool-ios-android-guide-windows-mac
2. https://tech.firstlook.media/how-to-defend-against-pegasus-nso-group-s-sophisticated-spyware
3. https://github.com/mvt-project/mvt
4. https://blog.lookout.com/protect-against-pegasus-spyware

SAFE
SECURITY

www.safe.security | info@safe.security

3000, El Camino Real,
Building 4, Suite 200,
Palo Alto, CA - 94304