Pegasus Spyware Report - Mohamed Salah Eldin

Introduction:

Pegasus spyware is probably one of the most sophisticated spywares out there in terms of detection and means of attack as it's a Zero-click type of exploitative spyware, meaning it doesn't require an end-user interaction for the most part to inflict damage or surveillance.

Originally developed by the Israeli intelligence firm NSO GROUP established in 2010 and specializes in cyber intelligence and famous for developing the aforementioned Pegasus spyware which wreaked havoc in activists' circles and many other individuals falling victims to its damage.

The purpose of this report is to dive deeper and understand the origins of the spyware, its mechanics, who uses it mainly, and methods of protection against its attacks.

Technical Overview:

- The main aspect and probably the most terrifying is the ability of this spyware to infect easily as well as gain access to a multitude of private functions of devices on what is called a Zero-Click attack. It can access photos\videos, files, location, gain access to camera and microphone recording without a user actually even using them. It can infect mainly IOS and Android devices bypassing encryption in famous apps such as WhatsApp and Signal. Once infected, it's basically meaningless as it can't be detected and has a built-in Self-Destruct Mechanism: it's designed to self-destruct in certain scenarios like for instance failing to gain connections to its command and control servers.

- An older method in early attacks was used mostly on WhatsApp for Android / iMessage for IOS was phishing links that the user clicks on and basically a done deal for said device in terms of privacy and surveillance.

- Whilst its main target of infection is mostly Android and IOS devices, there are reports of it infecting Linux machines as well as Windows, but as for Windows, there have been multiple patches for defense against it through firewall patches.

Key Cases:

- Pegasus spyware since its creation was an intelligence tool sold and controlled by the government of Israel to other governments, intelligence agencies, law enforcement agencies, and militaries of said governments, raising ethical concerns as it was marketed as a tool to help, but tyrannical / democratic governments used it as means of surveillance and outing certain political rivals. E.X it was used on the phones of those who were close to Jamal Khashoggi before his assassination by the Saudi government.

- It's mainly used against activists or political opponents to track them and cause spread fear, extract their information, and extort said victims of such attacks. The main fear is that once NSO sells the

spyware there's actually little to no control over it in terms of usage, which raises concerns of widespread abuse.

- Multiple lawsuits were filed against NSO over its usage and damages done. The two most famous lawsuits were by WhatsApp in 2019 and Apple in 2021, which were both allowed to proceed by the US Supreme Court after denying NSO's appeal.

Methods of Defense:

Defense against Pegasus spyware is actually a great challenge as it leaves little to no traces but there are common practices and tools that could help aid with avoiding it or finding traces of it on devices, but here are some practices that could aid and help users against it:

- Keeping an eye on links and avoiding clicking on suspicious links even through trusted means.

- Using end-to-end encrypted apps for communication and disabling features that aren't used mainly on mobile devices such as Bluetooth - iMessage / FaceTime if not used regularly.

- Keeping devices up to date on security patches.

- Using Amnesty International's Mobile Verification Toolkit (MVT) to find traces of Pegasus spyware on infected devices.

Summary:

Pegasus spyware is an extremely volatile and hard to detect spyware that raises concerns of how it can be used as a state-surveillance tool to oppress political opponents and the importance of cybersecurity and the need for limiting/ending the usage of such spyware.

Resources:

Wikipedia, Guardian interview with Edward Snowden on YouTube, Technical Overview - Amnesty's Forensic Analysis.