Bitdefender detects Pegasus, the most dangerous mobile spyware in the world

Does Bitdefender detect Pegasus, the most dangerous mobile spyware?

Yes, Bitdefender detects Pegasus created by the NSO Group and protects against the latest Pegasus versions developed to hack even iPhones with recent iOS versions – up to iOS 14.6.

Bitdefender anti-malware engines identified the first form of Pegasus spyware back in 2017. Over the years, Bitdefender's anti-malware signatures have been constantly updated to keep up with new forms of Pegasus spyware. Here at Bitdefender, we are on top of the latest threats.

Bitdefender detects Pegasus, the most dangerous mobile spyware in the world

What is Pegasus spyware and how does it infect smartphones?

Pegasus is the most advanced iOS, iPadOS, and Android malware to have ever been detected in real-world usage. It exploits zero-day vulnerabilities in popular applications such as WhatsApp, iMessage, FaceTime to infect smartphones. This sophisticated technique allows compromising devices without the user clicking on an infected link or taking any action for that matter.

Extremely versatile, Pegasus can sniff communications, steal messages and call records from instant messaging like WhatsApp, Facebook, Twitter, Skype, and Gmail. It also packs keylogging and capabilities to take screenshots; it can even take control of the phone's camera and microphone. It's estimated that about three dozen specially selected individuals located in countries such as Israel, Georgia, Mexico, Turkey, UAE, and others have been targeted by this malware.

How do I protect my smartphone and tablet against Pegasus?

Pegasus is a tough reminder about how ill-intended parties can leverage the flexibility of the Android and iOS operating systems and build rogue applications for surveillance and monitoring. Smartphones 'hear' and 'see' almost everything we do 24h a day, 7 days a week, while other Android implementations, such as Smart TVs, see the most intimate moments of our private life.

To protect your mobile devices against Pegasus install apps only from legitimate sources, make sure you have the latest OS updates and security patches, enable a lock screen, check on a regular basis which apps have admin rights on your device, and ensure you run the Bitdefender Mobile Security app on iOS, respectively Bitdefender Mobile Security for Android. Remember to activate the Web Protection feature in your Bitdefender app by tapping the Web Protection icon on the bottom navigation bar of Bitdefender Mobile Security.

NSO Group's Pegasus spyware notable attacks

Back in 2020, security researchers from The Citizen Lab discovered that attackers deployed a zero-day against iOS 13.5.1 and likely had access to the iPhones of 36 people working at Al Jazeera. Zero-day exploits are usually very expensive, and attackers don't normally use them for just anyone. Such vulnerabilities appear in attacks against high-value targets for a simple reason: once they are discovered, the hardware developers try to close the exploit as quickly as possible. In the case of the Al Jazeera hack, the attackers installed NSO Group's Pegasus spyware, a piece of kit that allows the user to remotely monitor devices.

The NSO Group made a name for itself with similar attacks, including the 2019 WhatsApp breach that allowed them to infect more than 1,000 devices. Now, the company focuses more on zero-click exploits and network-based attacks, selling their "products" to governments and other interested parties.

"It is more challenging for researchers to track these zero-click attacks because targets may not notice anything suspicious on their phone," said The Citizen Lab in their report. "Even if they do observe something like 'weird' call behavior, the event may be transient and not leave any traces on the device."

This is exactly what happened with the current Pegasus infection. Al Jazeera's Tamer Almisshal believed he was hacked and allowed security researchers to monitor his traffic.

"The phones were compromised using an exploit chain that we call KISMET, which appears to involve an invisible zero-click exploit in iMessage," the researchers said. "In July 2020, KISMET was a zero-day against at least iOS 13.5.1 and could hack Apple's then-latest iPhone 11. Based on logs from compromised phones, we believe that NSO Group customers also successfully deployed KISMET or a related zero-click, zero-day exploit between October and December 2019."

In total, The Citizen Lab identified 36 infected phones belonging to Al Jazeera employees, but the infections came from four different operators, MONARCHY, SNEAKY KESTREL, CENTER-1, and CENTER-2. It's difficult to pinpoint the operators, but the group says with medium confidence that SNEAKY KESTREL was acting on behalf of the UAE and MONARCHY on behalf of Saudi Arabia.