bizcommunity

Lessons learned from the latest WhatsApp hack

We were once again reminded that mobile devices, the one thing most of us never leave home without, are vulnerable to attacks. And once again, private individuals were attacked.

Source: pixabay.com

Several news organisations reported on Monday, 13 May 2009, that attackers exploited a vulnerability in WhatsApp, the popular global messaging app installed on 1.5 billion devices worldwide, and successfully installed spyware on several victims' devices.

Unbeknownst to the victims, the attackers obtained complete access to everything on their mobile devices personal and corporate information, email, contacts, camera, microphone, and the individual's location.

WhatsApp is encouraging customers to update their apps as quickly as possible and to keep their mobile operating system up to date.

Remarkably, the attackers used the vulnerability to insert malicious code and steal data from Android and iPhone smartphones simply by placing a WhatsApp call, even if the victim didn't pick up the call.

The spyware erases all logs of the call so that victims remain unaware that their device has been hacked.

The WhatsApp hack illustrates that despite their best efforts, Apple and Google cannot completely secure the users of mobile devices running their operating systems. In order to ensure users are properly protected, a mobile threat defence solution must be in a place that can prevent spyware from gathering intelligence on their targets.

The solution involves multiple steps:

- Identifying advanced rooting and jailbreaking techniques

- Detecting unknown malware
- Preventing malicious outbound communications to command and control servers

All the steps above must be enabled to best prevent sophisticated attacks like the WhatsApp hack. If spyware is simply detected after infecting the device it is too late. It is paramount to ensure that the attack prevented before it actually infects the mobile device. If, however the device becomes infected, it’s critica that no data be exfiltrated from of the device.