An Invasive Spyware Attack on Military Mobile Devices

By bferrite

Published: 2018-07-05 · Archived: 2026-04-05 19:13:09 UTC

Earlier this week, Israeli security agencies announced that the Hamas terrorist organization had installed spyware on Israeli soldiers' smartphones in its latest attempt to collect information on its long time enemy. About 100 people fell victim to the attack that came in the form of fake World Cup and online dating apps that had been uploaded to the Google Play Store, the official app store of Google.

Once the apps were installed onto the victims' phones, the highly invasive malware was then able to carry out a number of malicious activities:

- Record the user's phone calls.
- Take a picture when the user receives a call.
- Steal the user's contacts.
- Steal the user's SMS messages.
- Steal all images and videos stored on the mobile device and information on where they were taken.
- Capture the user's GPS location.
- Take random recordings of the user's surroundings.
- Steal files and photos from the mobile device's storage.

This attack involved the malware bypassing Google Play's protections and serves as a good example of how attackers hide within legitimate apps which relate to major popular events and take advantage of them to attract potential victims.

Indeed, while many like to imagine and predict a 'Cyber 9/11' and other ways in which terrorism could play a role in today's hyper-connected world, this latest attack demonstrates a more realistic picture of how terrorists use malware to carry out their attacks.

But it is not the first time these tactics have been used, either against this specific target or other government agencies around the world. In early 2017, the Viperat spyware targeted Israeli soldiers serving around the Gaza strip, leveraging social engineering techniques to steal photos and audio files from their smartphones. In March 2016, 'SmeshApp', a calling and messaging app on Google Play store, was allegedly used by Pakistan in to spy on Indian military personnel and again in 2016, a Russian APT group was suspected of using Android spyware to track Ukrainian field artillery units.

However, these cases of espionage do not only affect militaries and governments but rather serve as just another example of how cyber threats are evolving and continue to use mobile as their attack vector. Furthermore, whether these threats come from non-state actors or cyber-crime gangs, they often use sophisticated techniques and malware to bypass traditional controls to reach their target.

Regardless of where these campaigns are targeted, though, they serve as a reminder as to how much we rely on our mobile devices as our main tool of communication and how much personal, as well as work related, information they contain. It certainly provides food for thought as to the measures government agencies, armed forces and enterprise corporations alike should take into account in order to protect their staff and network from outside threats.

With consumers and company employees often using their smartphones as the preferred method of accessing the internet, corporate resources, or storing private information, knowing which apps get downloaded onto them should very much be a priority, for both them and their organization, in order to protect the data they store. Furthermore, although third party app stores do all they can to block malicious apps from being uploaded, sophisticated attacks such as this will always find a devious way of bypassing them, making on device protection even more necessary.

SandBlast Mobile: The Advanced Threat Prevention Solution

Cyber thieves and unwanted parties know that without the right protection the information on our smartphones and tablets is theirs for the taking. But what is the right protection for our mobile devices?

Organizations and consumers alike need an innovative approach to mobile security for both iOS and Android devices that detects and stops mobile threats before they start. Whether your data is at rest on a device or in flight through the cloud, Mobile Threat Prevention helps protect you from vulnerabilities and attacks that could put that data at risk.

Indeed, the technology used by Check Point's SandBlast Mobile provides a complete mobile security solution that protects devices from threats on the device (OS), in applications, and in the network, and delivers the industry's highest threat catch rate for iOS and Android. This fifth generation advanced technology uses malicious app detection to find known and unknown threats by applying threat emulation, advanced static code analysis, app reputation and machine learning.

In addition, it safeguards devices from unprotected Wi-Fi® network access and Man-in-the-Middle attacks and stops access to the network when a threat is detected. It also uses real-time risk assessments at the device-level (OS) to reduce the attack surface by detecting attacks, vulnerabilities, changes in configurations and advanced rooting and jailbreaking. Provision for flexibility is also made by allowing organizations to set adaptive policy controls based on unique thresholds for mitigation and elimination of threats on the device.

After all, wherever there is sensitive data, whether it be on the smartphone of military personnel or a company employee, there will always be those who find that data valuable for their own gain. As a result, government agencies and companies of all sizes cannot afford to let this information remain unprotected and are advised to protect these devices today, before they fall victim to the next mobile surveillance campaign.

For enterprises, read more about Check Point's Sand Blast Mobile, and for consumers Check Point's Zone Alarm Mobile, to learn how you can protect devices from malicious and invasive mobile malware and the type of threats that could impact your business.

Source: https://blog.checkpoint.com/2018/07/05/an-invasive-spyware-attack-on-military-mobile-devices/