Hamas Android Malware On IDF Soldiers-This is How it Happened

By etal

Published: 2020-02-16 · Archived: 2026-04-05 21:45:08 UTC

Introduction:

Earlier today, IDF's spokesperson revealed that IDF (Israel Defense Force) and ISA (Israel Security Agency AKA "Shin Bet") conducted a joint operation to take down a Hamas operation targeting IDF soldiers, dubbed 'Rebound'.

In this article, we will describe the capabilities and provide technical analysis of the malware used, along with the attack's affiliation to APT-C-23, a hacking group with previously reported attacks in the Middle East

Technical Analysis:

This MRAT (Mobile Remote Access Trojan) is disguised as a set of dating apps, "GrixyApp", "ZatuApp", and "Catch&See", all with dedicated websites, and descriptions of dating applications.

The victims received a link to download the malicious application from a Hamas operator disguising themselves as an attractive woman. Once the application is installed and executed, it shows an error message stating that the device is not supported, and the app will uninstall itself – which actually does not happen, and the app only hides its icon.

Figure 1 – Fake error message

While hidden, the application communicates with the same server it was downloaded from, using the MQTT protocol.

The main functionality of this malware is to collect data on the victim such as phone number, location, SMS messages and more, while having the capability to extend its code via a received command. The command can provide the application with a URL to a DEX file, which is then downloaded and executed.

Figure 2 – Code to download an additional DEX file

Figure 3 – Communication with the C&C

Figure 4 – Collecting device information

Figure 5 – Collecting a list of installed applications

Figure 6 – Collecting storage information

Video Player

Figure 7 – Application hiding demo

Affiliation:

The tactics, techniques and procedures (TTPs) used in this new wave of attacks are similar to ones used in the past by previous APT-C-23 campaigns.

First, the threat group develops backdoors for Android devices that are usually disguised as chatting applications.

Figure 8 – Promotion websites

Second, dedicated and specially crafted websites are set up by the threat group to promote those backdoors, explain their functionality, and offer a direct link to download them. Those domains, and others that are used for C&C communications by known APT-C-23 samples, are usually registered using NameCheap, and this was also the case with the newly discovered websites.

Lastly, malicious samples affiliated with APT-C-23 made references to names of actors, TV characters and celebrities both in their source code and C&C communication. Although the new backdoors lacked those references, we were able to see name of celebrities and known figures such as Jim Morrison, Eliza Doolittle, Gretchen Bleiler and Dolores Huerta in the backdoor's website, catchansee[.]com.

Figure 9 – References to celebrities in server code

This campaign serves as a sharp reminder that effort from system developers alone is not enough to build a secure Android eco-system. It requires attention and action from system developers, device manufacturers, app developers, and users, so that vulnerability fixes are patched, distributed, adopted and installed in time.

It is also another example for why organizations and consumers alike should have an advanced mobile threat prevention solution installed on the device to protect themselves against the possibility of unknowingly installing malicious apps, even from trusted app stores.
