

Android Spyware Targeting Tanzania Premier League | blog

By Shivang Desai

Published: 2020-07-29 · Archived: 2026-04-05 19:03:08 UTC

The Zscaler ThreatLabZ team is always hunting for malware out in the wild. Recently, there have been endless cases where attackers were targeting mobile users with malware leveraging the COVID-19 pandemic.

Amidst all the COVID-related malware activities, we actually came across some Android malware samples that weren't COVID-19 related. Instead, they were targeting the ongoing Tanzania Mainland Premier League football season. The Tanzania Mainland Premier League is the top-level professional football (or soccer, as it is most commonly known here in the United States) league in Tanzania, Africa.

We came across some of the Android Packages (APKs) that were targeting two of the most famous football clubs in Africa, namely Simba SC and Yanga (Young Africans) SC.

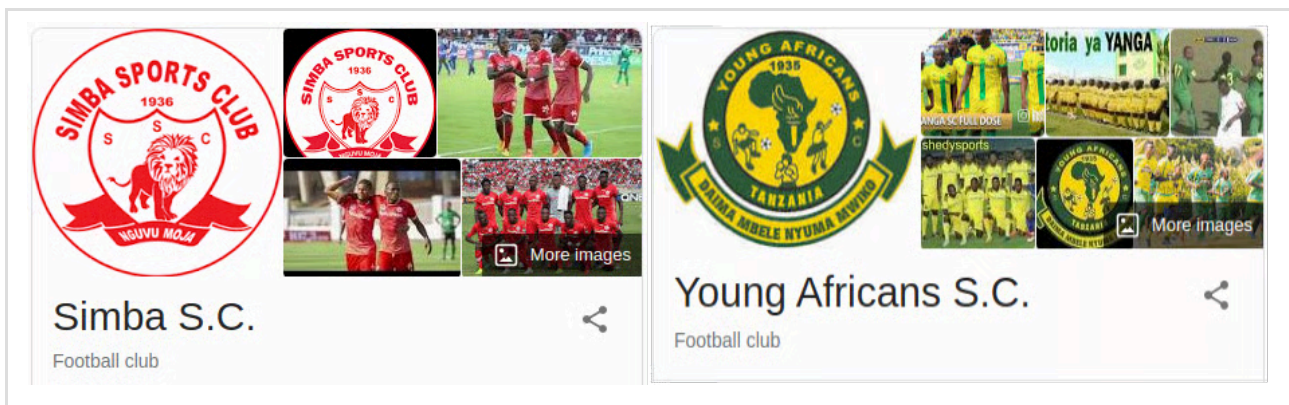


Figure 1: Logos for the Tanzania football clubs targeted in a recent scam.

We also found some legit apps on the Google Play store that are related to these clubs. As seen in Figure 2, the spyware portrays itself as official apps of the above-mentioned teams.



Figure 2: Real vs. fake logos for Simba SC and Yanga SC.

These apps are basically spyware, which include the following capabilities:

- Read SMS messages
- Fetch contacts
- Record audio
- Calling functionality
- Access real-time location
- Read/write external storage
- Steal photos
- Access the camera

These capabilities basically sum up a perfectly developed spyware with full-fledged features to spy on anyone.

Upon further analysis, these APKs turned out to be developed using a popular surveillance tool named SpyMax. Its predecessor, SpyNote, was one of the most widely used spyware frameworks. In the past, there were instances where SpyNote was notoriously used to [victimise Netflix users](#) and a [wide range](#) of other Android users.

SpyMax seems to be *new favorite* among attackers in the underground forums. We found some evidence where SpyMax has been developed in these underground forums with its main focus on the latest Android compatibility and antivirus evasion.

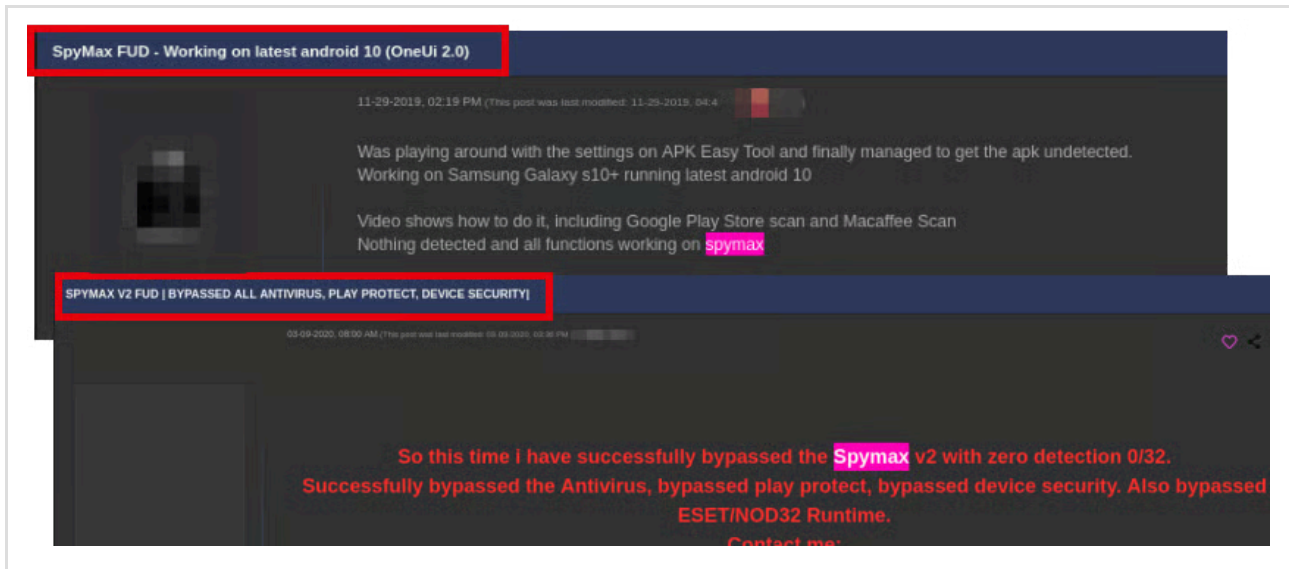


Figure 3: Underground forum discussions about SpyMax.

As seen in Figure 3, many of the discussions are about trying to make SpyMax samples fully undetectable (FUD) from antivirus scans.

Though SpyMax is free in itself, some developers claim to have developed their own versions that are undetected by antivirus software and are selling the samples at rates ranging from \$45 to \$350 per month. The same user in Figure 3 posted about his or her costs as can be seen in Figure 4.

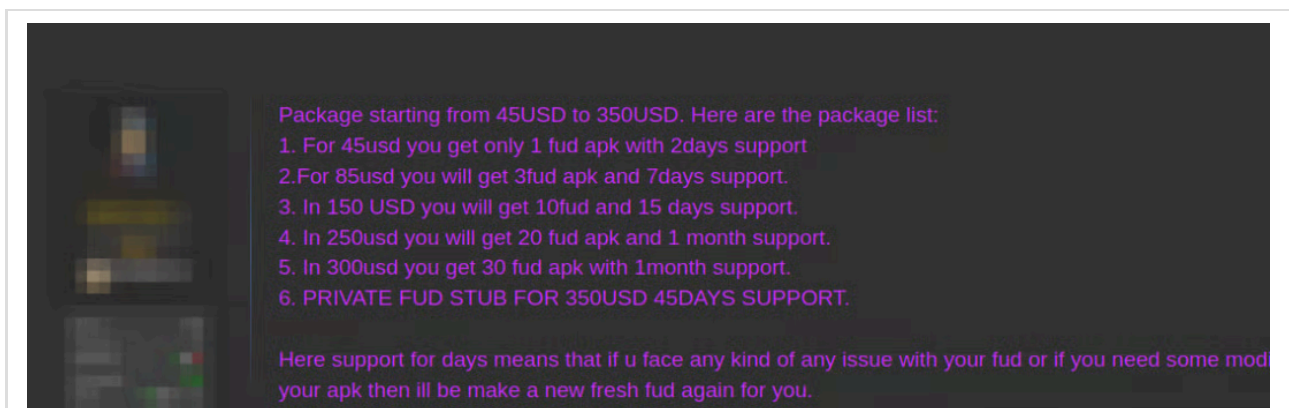


Figure 4: A user discussing the costs of a FUD version of SpyMax.

Getting back to the campaign, we unfortunately could not track back to the command and control (C&C) server, as it was not active during our analysis. But we were able to get hold of some more samples that were designed by

the same attacker or group of attackers. (Hashes can be found in IOC section at the end of this blog.)

One such sample developed by the attacker using SpyMax was a live streaming app that claimed to stream live football matches from the Tanzania Premier League. The main purpose behind this is likely to reach a wide range of football fans and attack their devices. The icons of the app can be seen in Figure 5 (Live Stream is the first from the left).

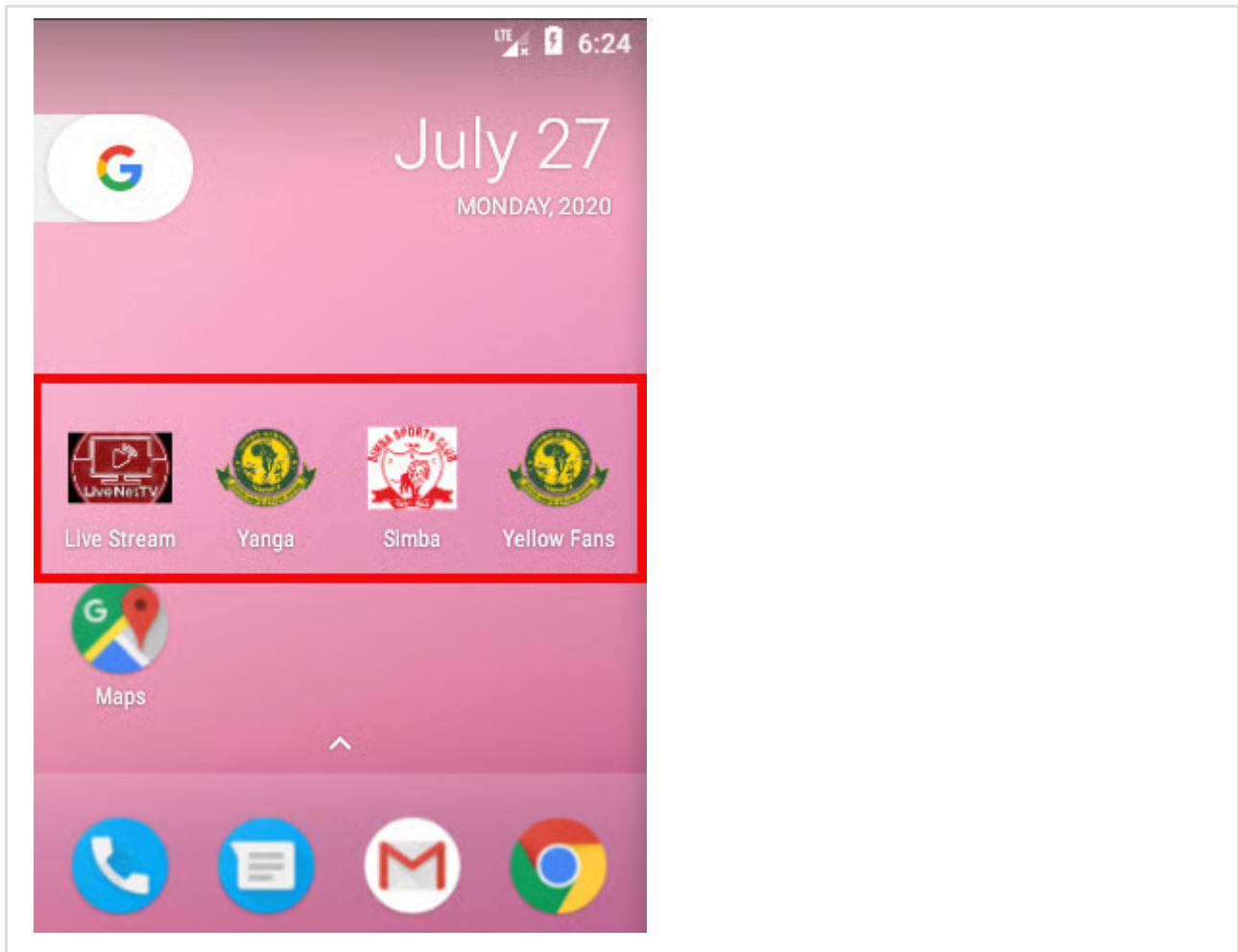


Fig 5: Fake (Spyware) apps

All these apps behave in exact same way. As soon as the victim tries to open the app, it crashes with message saying "App is not installed" before suddenly hiding the icon. This activity makes victim believe that the app might be faulty and got removed implicitly from mobile device. But in reality, the app hides itself from the victim and plays it's hideous activities of spying on the user and sending all the stolen data back to the attacker.

Conclusion

Nowadays, developing high-end surveillance apps (also termed spyware or stalkerware) is as easy as developing a basic Android app with the help of tools, such as SpyMax. Even a novice can develop spyware and attack large number of public. As seen in this case, the attacker used SpyMax to target Android users interested in an ongoing

football season. From a user point of view, it's always advisable to take utmost care when online, especially in times when *work-from-home* has become the norm.

The precautions you take online have been covered extensively; even so, we believe this information bears repeating. Please follow these basic precautions during the current crisis—and at all times:

- Install apps only from official stores, such as Google Play.
- Never click on unknown links received through ads, SMS messages, emails, or the like.
- Always keep the "Unknown Sources" option disabled in the Android device. This disallows apps to be installed on your device from unknown sources.

We would also like to mention that if you come across the incident of app hiding it's icon as seen in case above, always try to search for the app in your device settings. (*Settings -> Apps -> Search for icon that was hidden*)

IOCs

| Hash | Package Name |
|--|---------------------------|
| aa67921f19809edc87f1f79237e123e9c5c67019 | com.yanga.yanga |
| 2ed2d804754d83aa5de32c27b4ca767d959bf3e8 | com.yellowfans.yanga |
| bea206cf83eea30bf5d0734d94764796d956c4f5 | com.livestream.livestream |
| 1cc01da09849e17f83940d9250318d248f7ab77d | com.simba.simba |
| 4c7a41d7b0a225f0fa61fe7dc18695e03c2690c8 | com.yellowfans.yanga |

Explore more Zscaler blogs

Source: <https://www.zscaler.com/blogs/research/android-spyware-targeting-tanzania-premier-league>