GoldenCup: New Cyber Threat Targeting World Cup Fans

By About the Author

Archived: 2026-04-06 15:16:47 UTC

Officials from the Israeli Defense Force recently uncovered an Android Spyware campaign targeting Israeli soldiers and orchestrated by "Hamas." The latest samples attributed to this campaign were discovered by security researchers from ClearSky.

In our research, we focus on the most recent sample, an application dubbed as "Golden Cup", launched just before the start of World Cup 2018.

Distribution / Infection

When this campaign started at the start of 2018, the malware ("GlanceLove", "WinkChat") was distributed by the perpetrators mainly via fake Facebook profiles, attempting to seduce IDF soldiers to socialize on a different platform (their malware). As this approach was not a great success, their last attempt was to quickly create a World Cup app and this time distribute it to Israeli citizens, not just soldiers.


GoldenCup: New Cyber Threat Targeting World Cup Fans


The official “Golden Cup” Facebook page. The short URL redirects to the application page at Google Play.

The official “Golden Cup” Facebook page. The short URL redirects to the application page at Google Play.

We assume it was rushed because, unlike GlanceLove, it lacked any real obfuscation. Even the C&C server side was mostly exposed with the file listing available for everyone to traverse through it. It contained approximately 8GB of stolen data.


A recent whois of “goldncup.com”. Creation date is a week before the start of the tournament.

A recent whois of “goldncup.com”. Creation date is a week before the start of the tournament.

How it Works

In order to get into the Google Play Store, the malware uses a phased approach which is quite a common practice for malware authors these days. The original app looks innocent, with most of its code aimed at implementing the real features that the app claims to provide. In addition, it collects identifiers and some data from the device.

After getting a command from the C&C, the app is able to download a malicious payload in the form of a .dex file that is being dynamically loaded adding the additional malicious capabilities.

In this way, the malware authors can submit their app and add the malicious capabilities only after their app is live on the Play Store.

Communication with the C&C

In order to communicate with its C&C, the app uses the MQTT (Message Queuing Telemetry Transport) protocol, which is transported over TCP port 1883.

Initiating the MQTT client.


Initiating the MQTT client.

The app connects to the MQTT broker with hardcoded username and password and a unique device identifier generated for each device.


The MQTT connection to broker

The MQTT communication is used primarily to update the device state and get commands from the C&C. It uses different topics that include the unique device identifier, which side is sending the message, and whether it is information message or command.

HTTP Communication

In addition to the MQTT communication, the app also uses plain text HTTP communication in order to download the .dex file and upload collected data.

All of the files that are being uploaded or downloaded are zip files encrypted by AES with ECB mode. The key for each file is generated randomly and stored in the encrypted file with a fixed offset.

In order to upload the file, the app uses a basic REST communication with the server, checking if the file exists and uploading it if it isn't.

The path that is used for the uploads is:

http://<domain>/apps/d/p/op.php

The communication looks like this:

First Phase

The first phase of the app's attack flow collects device information and a list of apps installed on the device. These are then uploaded to the C&C HTTP server.


The collection of basic device information.

In addition, at this stage the app can process one of these commands:

- Collect device info
- Install app
- Is online?
- Change server domain

Out of these, the most interesting command is the “install app” command that downloads an encrypted zip file containing the second phase dex file, unpacks and loads it.

Second Phase

The second phase dex file contains 3 main services that are being used:

- ConnManager - handles connections to the C&C
- ReceiverManager - waits for incoming calls / app installations
- TaskManager - manages the data collection tasks

The C&C server address is different than the one that is used by the first phase, so the app reconnects to the new server as well as starts the periodic data collector tasks.

By analyzing the TaskManager class we can see the new commands that are supported at this stage:

As can be seen in the code snippet above, there are quite a lot of data collection tasks that are now available:

- Collect device info
- Track location
- Upload contacts information
- Upload sent and received SMS messages
- Upload images
- Upload video files
- Send recursive dirlist of the external storage
- Upload specific files
- Record audio using the microphone
- Record calls
- Use the camera to capture bursts of snapshots

Those tasks can either run periodically, on event (such as incoming call) or when getting a command from the C&C server.

Mitigations

Stay protected from mobile malware by taking these precautions:

- Do not download apps from unfamiliar sites
- Only install apps from trusted sources

- Pay close attention to the permissions requested by apps
- Install a suitable mobile security app, such as SEP Mobile or Norton, to protect your device and data
- Keep your operating system up to date
- Make frequent backups of important data

Indicators of Compromise (IoCs)

Package names:

- anew.football.cup.world.com.worldcup
- com.coder.glancelove
- com.winkchat

APK SHA2:

166f3a863bb2b66bda9c76dccf9529d5237f6394721f46635b053870eb2fcc5a
b45defca452a640b303288131eb64c485f442aae0682a3c56489d24d59439b47
d9601735d674a9e55546fde0bffde235bc5f2546504b31799d874e8c31d5b6e9
2ce54d93510126fca83031f9521e40cd8460ae564d3d927e17bd63fb4cb20edc
67b1a1e7b505ac510322b9d4f4fc1e8a569d6d644582b588faccfeeaa4922cb7
1664cb343ee830fa94725fed143b119f7e2351307ed0ce04724b23469b9002f2

Loaded DEX SHA2:

afaf446a337bf93301b1d72855ccdd76112595f6e4369d977bea6f9721edf37e

Domain/IP:

- goldncup[.]com
- glancelove[.]com
- autoandroidup[.]website
- mobilestoreupdate[.]website
- updatemobapp[.]website
- 107[.]175[.]144[.]26
- 192[.]64[.]114[.]147

 GoldenCup: New Cyber Threat Targeting World Cup Fans

 Roy Iarchy

Roy Iarchy

Head of Research, Modern OS Security

 Eyal Rynkowski

Eyal Rynkowski

Symantec Security analyst, Modern OS Security
