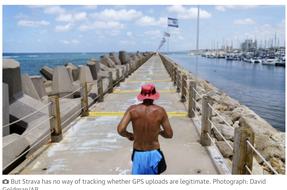
Espionage

Shadowy Strava users spy on Israeli military with fake routes in bases

Exclusive: Personnel risk identification by running GPS 'segments' around top-secret sites



But Strava has no way of tracking whether GPS uploads are legitimate. Photograph: David Goldman/AP

Alex Hern *UK technology editor*

alexhern

Tue 21 Jun 2022 05.00 BST

Unidentified operatives have been using the fitness tracking app Strava to spy on members of the Israeli military, tracking their movements across secret bases around the country and potentially observing them as they travel the world on official business.

By placing fake running "segments" inside military bases, the operation - the affiliation of which has not been uncovered – was able to keep tabs on individuals who were exercising on the bases, even those who have applied the strongest possible account privacy settings.

In one example seen by the Guardian, a user running on a top-secret base thought to have links to the Israeli nuclear programme could be tracked across other military bases and to a foreign country.

The surveillance campaign was discovered by the Israeli open-source intelligence outfit FakeReporter. The group's executive director, Achiya Schatz, said: "We contacted the Israeli security forces as soon as we became aware of this security breach. After receiving approval from the security forces to proceed, FakeReporter contacted Strava, and they formed a senior team to address the issue."

Strava's tracking tools are designed to allow anyone to define and compete over "segments", short sections of a run or bike ride that may be regularly raced over, like a long uphill climb on a popular cycling route or a single circuit of a park. Users can define a segment after uploading it from the Strava app, but can also upload GPS recordings from other products or services.

But Strava has no way of tracking whether those GPS uploads are legitimate, and allows anyone to define a segment by uploading - even if they may not have been to the place they are tracking. In fact, some uploaded segments are clearly artificially generated, with average paces of hundreds of kilometres an hour, unnaturally straight lines and instant vertical leaps up clifftops all recorded.

Some of those fake uploads may have been used for the purposes of cheating on friendly competitions, or setting up a segment to guide others: but at least one set appears to have a more malicious purpose. An anonymous user, with their location given as "Boston, Massachusetts", had set up a series of fake segments across a number of military establishments in Israel, including outposts of the country's intelligence agencies and highly secure bases thought to be associated with its nuclear programme.

"By exploiting the capability to upload engineered files, revealing the details of users anywhere in the world, hostile elements have taken one alarming step closer to exploiting a popular app in order to harm the security of citizens and countries alike," Schatz said.

The fake segment approach also bypasses some of Strava's privacy settings. Users can set their profiles to be only visible to "followers", which prevents prying eyes from tracking their movements across time. But unless they also set each individual run to be actively secured, then their profile picture, first name, and initial will show up on segments they have run, in the spirit of friendly competition. With enough segments scattered across the map, individuals can still be identified: one user, for instance, tracked their participation in a publicly reported race, which they won, as well as running in secure military establishments.

In a statement, the fitness company said: "We take matters of privacy very seriously and have been made aware by an Israeli group, FakeReporter, of a segment issue regarding a specific user account and have taken the necessary steps to remedy this situation.

"We provide readily accessible information regarding how information is shared on Strava, and give every athlete the ability to make their own privacy selections. For more information on all of our privacy controls, please visit our privacy centre as we recommend that all athletes take the time to ensure their selections in Strava represent their intended experience."

The discovery has echoes of a scandal from 2018 when a new Strava feature published a visualisation of all activity on the fitness tracking platform across the world. The heat map showed popular running, cycling and swimming routes, and an announcement from Strava highlighted that it could be used to spot locations like the route of the Ironman triathlon in Hawaii. But it also laid out routes that were less public: the location and layout of multiple military bases in Helmand Province, Afghanistan, were clearly visible, as was a popular outdoor swimming spot next to RAF Mount Pleasant in the Falkland Islands. The map even recorded the route of a lone cyclist in Area 51, Nevada.

Strava's response to the uproar was to advise military users to opt out of its visualisation, arguing that the information was made public by the users who uploaded it. In an echo of the latest privacy vulnerability, some users were tracked in alarming detail: one US air force service member could be tracked from a tour in Djibouti, where she ran the 7km loop of the runway, to an airbase in Germany where she was transferred in 2016.