LetMeSpy, a phone tracking app spying on thousands, says it was hacked

A hacker has stolen the messages, call logs and locations intercepted by a widely used phone monitoring app called LetMeSpy, according to the company that makes the spyware.

The phone monitoring app, which is used to spy on thousands of people using Android phones around the world, said in a notice on its login page that on June 21, "a security incident occurred involving obtaining unauthorized access to the data of website users."

"As a result of the attack, the criminals gained access to e-mail addresses, telephone numbers and the content of messages collected on accounts," the notice read.

LetMeSpy is a type of phone monitoring app that is marketed for parental control or employee monitoring. The app is also specifically designed to stay hidden on a phone's home screen, making it difficult to detect and remove. Also known as stalkerware or spouseware, these kinds of phone monitoring apps are often planted by someone — such as spouses or domestic partners — with physical access to a person's phone, without their consent or knowledge.

Once planted, LetMeSpy silently uploads the phone's text messages, call logs and precise location data to its servers, allowing the person who planted the app to track the person in real time.

For their deep level of access to a person's phone, these surveillance apps are notoriously buggy and known for rudimentary security mistakes, with countless spyware apps over the years getting hacked, or leaking and exposing the private phone data stolen from unwitting victims.

LetMeSpy is not much different.

Polish security research blog Niebezpiecznik first reported the breach. When Niebezpiecznik contacted the spyware maker for comment, the hacker reportedly responded instead, claiming to have seized wide access to the spyware maker's domain.

It's not clear who is behind the LetMeSpy hack or their motives. The hacker intimated that they deleted LetMeSpy's databases stored on the server. A copy of the hacked database also appeared online later the same day.

DDoSecrets, a nonprofit transparency collective that indexes leaked datasets in the public interest, obtained a copy of the hacked LetMeSpy data and shared it with TechCrunch. DDoSecrets said it was limiting the distribution of the data to journalists and researchers, given the amount of personally identifiable information in the cache.

TechCrunch reviewed the leaked data, which included years of victims' call logs and text messages dating back to 2013.

The database we reviewed contained current records on at least 13,000 compromised devices, though some of the devices shared little to no data with LetMeSpy. (LetMeSpy claims to delete data after two months of account inactivity.)

In January, LetMeSpy's website said its spyware was used to track over 236,000 devices and collected tens of millions of call logs, text messages and location data points to date. At the time of writing, the site's counters read as zero. Much of the site's functionality also appears to be broken, including the spyware app itself. TechCrunch analyzed the LetMeSpy phone app's network traffic, which showed that the app appeared to be non-functioning at the time of writing.

The database also contained over 13,400 location data points for several thousand victims. Most of the location data points are centered over population hotspots, suggesting the majority of victims are located in the United States, India and Western Africa.

The data also contained the spyware's master database, including information about 26,000 customers who used the spyware for free and the email addresses of customers who bought paying subscriptions.

Source: TechCrunch