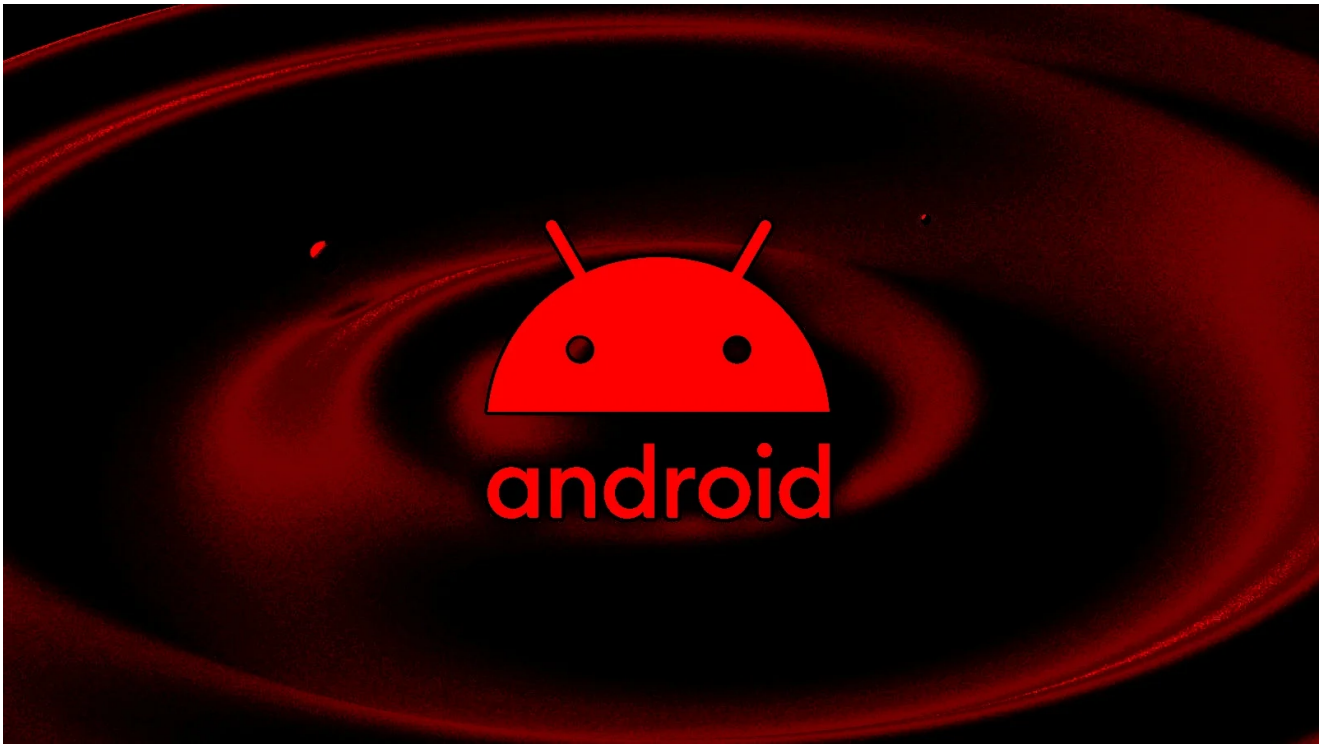
Hacking group updates Furball Android spyware to evade detection

bleepingcomputer.com/news/security/hacking-group-updates-furball-android-spyware-to-evade-detection/

Bill Toulas

By
Bill Toulas

- October 20, 2022
- 05:30 AM
- 0



A new version of the 'FurBall' Android spyware has been found targeting Iranian citizens in mobile surveillance campaigns conducted by the Domestic Kitten hacking group, also known as APT-C-50.

The spyware is deployed in a mass-surveillance operation that has been underway since at least 2016. In addition, multiple cybersecurity firms have reported on Domestic Kitten, which they believe is an Iranian state-sponsored hacking group.

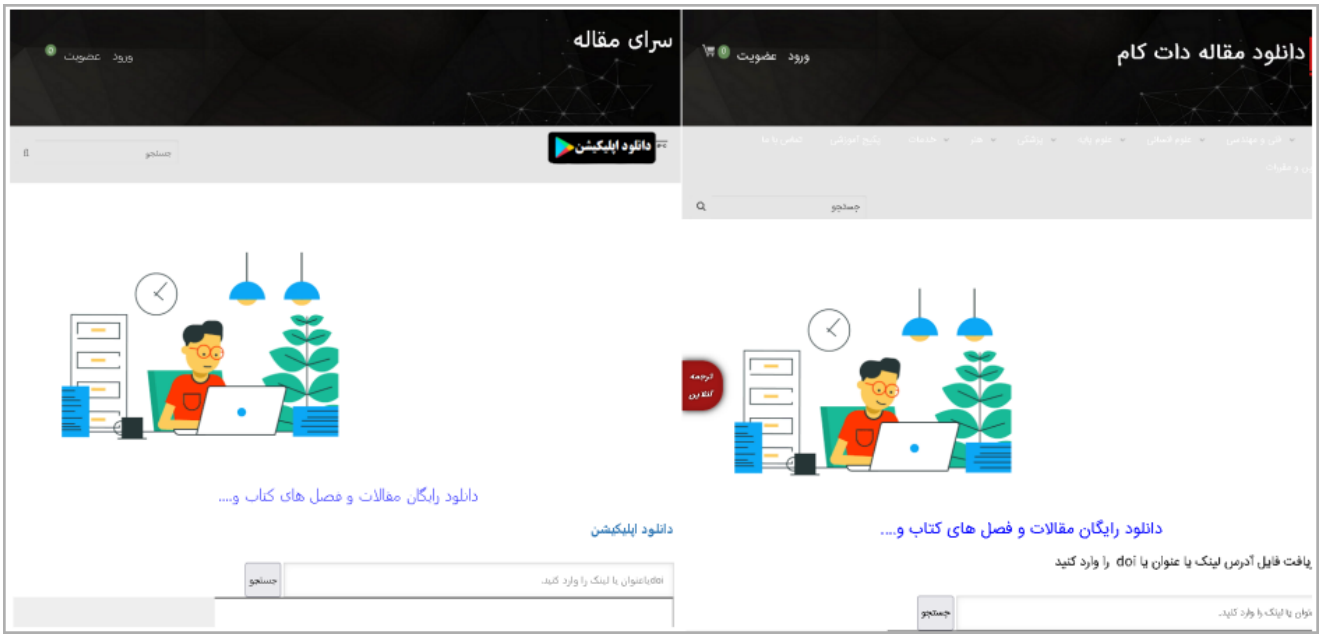
The newest FurBall malware version was sampled and analyzed by ESET researchers, who report it has many similarities with earlier versions, but now comes with obfuscation and C2 updates.

Also, this discovery confirms that 'Domestic Kitten' is still ongoing in its sixth year, which further backs the hypothesis that the operators are tied to the Iranian regime, enjoying immunity from law enforcement.

New FurBall details

The new version of FurBall is distributed via fake websites that are visually clones of real ones, where victims end up after direct messages, social media posts, emails, SMS, black SEO, and SEO poisoning.

In one case spotted by ESET, the malware is hosted on a fake website mimicking an English-to-Persian translation service popular in the country.



Fake site on the left, real site on the right *(ESET)*

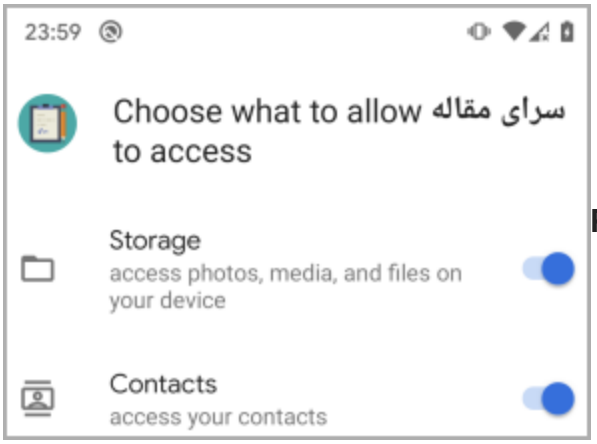
In the fake version, there's a Google Play button that supposedly lets users download an Android version of the translator, but instead of landing on the app store, they are sent an APK file named 'sarayemaghale.apk.'.

Depending on what permissions are defined in the Android app's AndroidManifest.xml file, the spyware is capable of stealing the following information:

- Clipboard contents
- Device location
- SMS messages
- Contact list
- Call logs
- Record calls
- Content of notifications
- Installed and running apps

- Device info

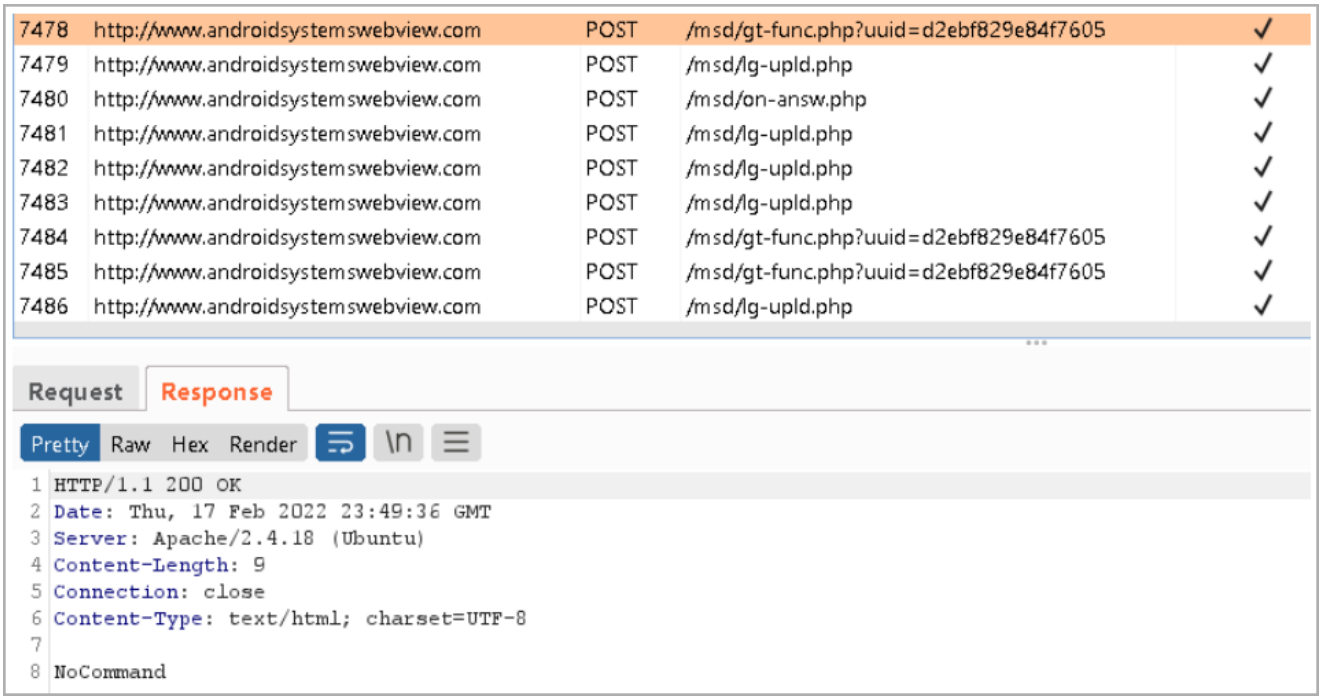
However, ESET says that the sample it analyzed has limited functionality, only requesting access to contacts and storage media.



Permissions requested upon installation *(ESET)*

These permissions are still powerful if abused, and at the same time, won't raise suspicions to the targets, which is likely why the hacking group restricted FurBall's potential.

If needed, the malware can receive commands to execute directly from its command and control (C2) server, which is contacted via an HTTP request every 10 seconds.



C2 response returning no command for execution *(ESET)*

In terms of the new obfuscation layer, ESET says it includes class names, strings, logs, and server URI paths, attempting to evade detection from anti-virus tools.

Previous versions of Furball didn't feature any obfuscation at all. Hence, VirusTotal detects the malware on four AV engines, whereas previously, it was flagged by 28 products.

Related Articles:

New BadBazaar Android malware linked to Chinese cyberspies

New Android malware 'RatMilad' can steal your data, record audio

Android file manager apps infect thousands with Sharkbot malware

New SandStrike spyware infects Android devices via malicious VPN app

Android malware droppers with 130K installs found on Google Play

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.