Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:08:26 UTC

APT group: Ferocious Kitten

Names	Ferocious Kitten *(Kaspersky)* G0137 *(MITRE)*
Country	Iran
Motivation	Information theft and espionage
First seen	2015
Description	(Kaspersky) Ferocious Kitten is an APT group that has been active against Persian-speaking individuals since 2015 and appears to be based in Iran. Although it has been active over a large timespan, the group has mostly operated under the radar and, to the best of our knowledge, has not been covered by security researchers. It only recently attracted attention when a lure document was uploaded to VirusTotal and was brought to public knowledge by researchers on Twitter. Subsequently, one of its implants was analyzed by a Chinese intelligence firm. We have been able to expand some of the findings on the group and provide insights on additional variants. The malware dropped from the aforementioned document is dubbed MarkiRAT and is used to record keystrokes and clipboard content, provide file download and upload capabilities as well as the ability to execute arbitrary commands on the victim's machine. We were able to trace the implant back to at least 2015, along with variants intended to hijack the execution of the Telegram and Chrome applications as a persistence method. Interestingly, some of the TTPs used by this threat actor are reminiscent of other groups operating in the domain of dissident surveillance. For example, it used the same C2 domains across its implants for years, which was witnessed in the activity of Domestic Kitten. In the same vein, the Telegram execution hijacking technique observed in this campaign by Ferocious Kitten was also observed being used by Rampant Kitten, as covered by Check Point. In our private report, we expand the details on these findings as well as provide analysis and mechanics of the MarkiRAT malware.
Observed	Sectors: Persian-speaking individuals.
Tools used	MarkiRAT.

Information	<https://securelist.com/apt-trends-report-q1-2021/101967/> <https://securelist.com/ferocious-kitten-6-years-of-covert-surveillance-in-iran/102806/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0137/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
