Rocket Kitten, Newscaster, NewsBeef - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:30:08 UTC

APT group: Rocket Kitten, Newscaster, NewsBeef

Names	Rocket Kitten *(CrowdStrike)* Newscaster *(Symantec)* NewsBeef *(Kaspersky)* Group 83 *(Talos)* Parastoo *(Flashpoint)*
Country	Iran
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2011
Description	(Kaspersky) Newsbeef/Newscaster will find a way to compromise a web site, usually the vulnerability appears to be CMS related, in an outdated WordPress plugin, Joomla version, or Drupal version. Attackers usually perform one of two things, Newsbeef has been performing the first of the two: - inject a src or iframe link into web pages or css sheets - inject the content of an entire BeEF web page into one of the internally linked javascript helpers The injected link will redirect visitors' browsers to a BeEF server. Usually, the attackers deliver some of the tracking and system/browser identification and evercookie capabilities. Sometimes, it appears that they deliver the metasploit integration to exploit and deliver backdoors (we haven't identified that exploitation activity in our ksn data related to this group just yet). Sometimes, it is used to pop up spoofed login input fields to steal social networking site credentials. We also haven't detected that in ksn, but some partners have privately reported it about various incidents. But we have identified that attackers will redirect specific targets to laced Adobe Flash and other installers from websites that they operate.

	So, the watering hole activity isn't always and usually isn't delivering backdoors. Most of the time, the watering hole injections are used to identify and track visitors or steal their browser history. Then, they deliver the backdoors to the right targets. There is some infrastructure overlap with Magic Hound, APT 35, Cobalt Illusion, Charming Kitten and ITG18.	
Observed	Sectors: Construction, Defense, Education, Embassies, Entertainment, Government, Manufacturing, Media. Countries: Algeria, Brazil, China, Germany, India, Israel, Japan, Kazakhstan, Romania, Russia, Turkey, UK, Ukraine, USA.	
Tools used	BeEF, FireMalv, Ghole.	
Operations performed	2011	Operation "Newscaster" The research firm iSight dubbed the operation Newscaster and said hackers used social-media sites like Twitter, Facebook and LinkedIn to draw their targets and then lure them to check out a bogus news site, NewsOnAir.org, filled with foreign policy and defense articles, The Post reported. The overall aim is that the social-media platform would give the hackers connections with those at the top of public policy — and position them to tap into that information network. <https://www.washingtontimes.com/news/2014/may/29/iranian-hackers-sucker-punch-us-defense-heads-crea/>
	Feb 2015	Operation "Woolen-GoldFish" <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing>
	Feb 2016	In late February 2016, a University website in Iran stood out for thoroughly vetting its current and potential students and staff. The University's web site served repackaged content from the Browser Exploitation Framework (BeEF) with embedded JavaScript content. <https://securelist.com/freezer-paper-around-free-meat/74503/>
	2017	Fake news website BritishNews to infect visitors On the same note, we identified a fake-news agency "established" by the attackers, called "The British news agency" or "Britishnews" (inspired by BBC). Its website domain is britishnews.com[.]co and two other domains, broadcastbritishnews[.] ommand britishnews[.]org redirected to it.
	2017	Blackmailing BBC reporter with 'naked photo' threats Iranian agents blackmailed a BBC Persian journalist by threatening to

		publish revealing photos of her as part of a wider campaign against the British media outlet, staff at the broadcaster told Arab News. New details emerged on Saturday about alleged harassment of BBC Persian reporters' family members and loved ones at the hands of the Iranian security services. <http://www.arabnews.com/node/1195681/media>
Information	<https://securelist.com/freezer-paper-around-free-meat/74503/> <https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf> <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf>	

Last change to this card: 13 September 2022

Download this actor card in PDF or JSON format
