Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:11:07 UTC

Other threat group: Yingmob

Names	Yingmob *(real name)*	
Country	China	
Motivation	Financial gain	
First seen	2016	
Description	(Check Point) Check Point Mobile Threat Prevention has detected a new, unknown mobile malware that targeted two customer Android devices belonging to employees at a large financial services institution. Mobile Threat Prevention identified the threat automatically by detecting exploitation attempts while examining the malware in the MTP emulators. The infection was remediated after the system notified the devices owners and the system administrators. The infection vector was a drive-by download attack, and the Check Points Threat-Cloud indicates some adult content sites served the malicious payload. Called HummingBad, this malware establishes a persistent rootkit with the objective to generate fraudulent ad revenue for its perpetrator, similar to the Brain Test app discovered by Check Point earlier this year. In addition, HummingBad installs fraudulent apps to increase the revenue stream for the fraudster.	
Observed	Countries: Algeria, Bangladesh, Brazil, China, Colombia, Egypt, India, Indonesia, Malaysia, Mexico, Nepal, Pakistan, Philippines, Romania, Russia, Thailand, Turkey, Ukraine, USA, Vietnam and others.	
Tools used	DroidPlugin, Eomobi, HummingBad, HummingWhale, Yispecter.	
Operations performed	Jan 2017	A Whale of a Tale: HummingBad Returns <https://blog.checkpoint.com/2017/01/23/hummingbad-returns/>
Information	<https://blog.checkpoint.com/2016/02/04/hummingbad-a-persistent-mobile-chain-attack/> <http://blog.checkpoint.com/wp-content/uploads/2016/07/HummingBad-Research-report_FINAL-62916.pdf>	

Last change to this card: 14 April 2020

Download this actor card in PDF or JSON format
