Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:10:50 UTC

Other threat group: Yanbian Gang

Names	Yanbian Gang *(?)*	
Country	China	
Motivation	Financial crime	
First seen	2013	
Description	(Trend Micro) In 2014, we took a close look at the Chinese underground market and found that it continued to thrive. But what we did not see was that even cybercriminals in remote parts of the country—Yanbian—were successfully profiting from the Android™ mobile banking customers in a neighboring country—South Korea. What we have dubbed the "Yanbian Gang" has successfully been siphoning millions from their victims' accounts since 2013. The hackers used fake banking and other popular apps to victimize more than 4,000 South Korean Android mobile banking customers throughout 2013 and 2014. They also used effective social engineering lures like "The Interview" to bait victims into installing their fake apps.	
Observed	Countries: South Korea.	
Tools used		
Operations performed	Dec 2020	Yanbian Gang Malware Continues with Wide-Scale Distribution and C2 <https://www.riskiq.com/blog/external-threat-management/yanbian-gang-malware-distribution/>
Information	<https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-south-korean-fake-banking-app-scam.pdf>	

Last change to this card: 21 April 2021

Download this actor card in PDF or JSON format