Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:09:44 UTC

Tool: PINEFLOWER

Names	PINEFLOWER CORRUPT KITTEN
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(FireEye) CORRUPT KITTEN was the author's chosen name for an Android implant that, according to the blog, 'supports a full range of spying and device management capability'. The blog contained a summary analysis of this CORRUPT KITTEN implant and an MD5 hash for a DEX file allegedly using the same C&C server. Notably, the author also noted that the malware stored files ready for exfiltration in a directory named '.data_gsc98647a3', the string we identified in our PINEFLOWER samples. It seemed likely that CORRUPT KITTEN and PINEFLOWER were one and the same.
Information	<https://vblocalhost.com/uploads/VB2021-Haeghebaert.pdf>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/apk.pineflower>

Last change to this tool card: 22 June 2023

Download this tool card in JSON format

All groups using tool PINEFLOWER

Changed	Name	Country	Observed	
APT groups				
	APT 42		2015-Feb 2024	
	Magic Hound, APT 35, Cobalt Illusion, Charming Kitten		2012-Jun 2025	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=8a823fe9-e03f-4c37-be82-3288c05ec213