Threat Group Cards: A Threat Actor Encyclopedia

APT group: Rancor

Names	Rancor *(Palo Alto)* Rancor Group *(Palo Alto)* Rancor Taurus *(Palo Alto)* G0075 *(MITRE)*
Country	China
Motivation	Information theft and espionage
First seen	2017
Description	(Palo Alto) Throughout 2017 and 2018 Unit 42 has been tracking and observing a series of highly targeted attacks focused in South East Asia, building on our research into the KHRAT Trojan. Based on the evidence, these attacks appear to be conducted by the same set of attackers using previously unknown malware families. In addition, these attacks appear to be highly targeted in their distribution of the malware used, as well as the targets chosen. Based on these factors, Unit 42 believes the attackers behind these attacks are conducting their campaigns for espionage purposes. We believe this group is previously unidentified and therefore have we have dubbed it “Rancor”. The Rancor group’s attacks use two primary malware families which we describe in depth later in this blog and are naming DDKONG and PLAINTEE. DDKONG is used throughout the campaign and PLAINTEE appears to be new addition to these attackers’ toolkit. Kaspersky found connections between this group and DragonOK.
Observed	Sectors: Government and political entities. Countries: Cambodia, Singapore, Vietnam and Southeast Asia.
Tools used	8.t Dropper, certutil, Cobalt Strike, DDKONG, Derusbi, Dudell, ExDudell, KHRAT, PLAINTEE.
Information	<https://unit42.paloaltonetworks.com/unit42-rancor-targeted-attacks-south-east-asia-using-plaintee-ddkong-malware-families/> <https://research.checkpoint.com/2019/rancor-the-year-of-the-phish/>

	<https://unit42.paloaltonetworks.com/rancor-cyber-espionage-group-uses-new-custom-malware-to-attack-southeast-asia/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0075/>
Playbook	<https://pan-unit42.github.io/playbook_viewer/?pb=rancortaurus>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
