Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:20:58 UTC

Other threat group: Pacha Group

Names	Pacha Group *(Intezer)*	
Country	China	
Motivation	Financial gain	
First seen	2018	
Description	(Intezer) Antd is a miner found in the wild on September 18, 2018. Recently we discovered that the authors from Antd are actively delivering newer campaigns deploying a broad number of components, most of them completely undetected and operating within compromised third party Linux servers. Furthermore, we have observed that some of the techniques implemented by this group are unconventional, and there is an element of sophistication to them. We believe the authors behind this malware are from Chinese origin. We have labeled the undetected Linux.Antd variants, Linux.GreedyAntd and classified the threat actor as Pacha Group.	
Observed		
Tools used	Antd, DDG, Korkerds, XMRig.	
Operations performed	Sep 2018	Intezer has evidence dating back to September 2018 which shows Pacha Group has been using a cryptomining malware that has gone undetected on other engines. <https://www.intezer.com/blog-pacha-group-deploying-undetected-cryptojacking-campaigns/>
	May 2019	Pacha Group Competing against Rocke, Iron Group Group for Cryptocurrency Mining Foothold on the Cloud <https://www.intezer.com/blog-technical-analysis-cryptocurrency-mining-war-on-the-cloud/>
Information	<https://www.intezer.com/blog-technical-analysis-pacha-group/>	

Last change to this card: 15 April 2020

Download this actor card in PDF or JSON format
