Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:17:35 UTC

Other threat group: Parinacota

Names	Parinacota *(Microsoft)* Wine Tempest *(Microsoft)*
Country	[Unknown]
Motivation	Financial gain
First seen	2018
Description	(Microsoft) One actor that has emerged in this trend of human-operated attacks is an active, highly adaptive group that frequently drops Wadhrama as payload. Microsoft has been tracking this group for some time, but now refers to them as PARINACOTA, using our new naming designation for digital crime actors based on global volcanoes. PARINACOTA impacts three to four organizations every week and appears quite resourceful: during the 18 months that we have been monitoring it, we have observed the group change tactics to match its needs and use compromised machines for various purposes, including cryptocurrency mining, sending spam emails, or proxying for other attacks. The group's goals and payloads have shifted over time, influenced by the type of compromised infrastructure, but in recent months, they have mostly deployed the Wadhrama ransomware. The group most often employs a smash-and-grab method, whereby they attempt to infiltrate a machine in a network and proceed with subsequent ransom in less than an hour. There are outlier campaigns in which they attempt reconnaissance and lateral movement, typically when they land on a machine and network that allows them to quickly and easily move throughout the environment.
Observed	Countries: Worldwide.
Tools used	Mimikatz, ProcDump, Wadhrama.
Information	<https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>

Last change to this card: 26 April 2023

Download this actor card in PDF or JSON format