Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:31:13 UTC

APT group: Void Balaur

Names	Void Balaur *(Trend Micro)* Rockethack *(self given)*
Country	[Unknown]
Motivation	Financial gain
First seen	2017
Description	(Trend Micro) This research looks into a threat actor group that can be considered a cybermercenary, but one that prefers to stay in the shadows. To our knowledge, this hacker-for-hire group does not operate out of a physical building, nor does it have a shiny prospectus that describes its services. The group does not try to wriggle out of a difficult position by justifying its business, nor is it involved in lawsuits against anybody attempting to report on their activities. Instead, this group is quite open about what it does: breaking into email accounts and social media accounts for money. This threat actor is also involved in selling highly sensitive personal data like cell tower phone logs, passenger flight records, banking data, and passport details.
Observed	Countries: Armenia, Australia, Belarus, Belgium, Brazil, Canada, Czech, Egypt, France, Germany, India, Italy, Japan, Kazakhstan, Netherlands, New Zealand, Norway, Poland, Portugal, Russia, Slovakia, South Africa, Spain, Sweden, Turkey, UAE, UK, Ukraine, USA, Uzbekistan.
Tools used	
Information	<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-far-reaching-attacks-of-the-void-balaur-cybermercenary-group> <https://documents.trendmicro.com/assets/white_papers/wp-void-balaur-tracking-a-cybermercenarys-activities.pdf> <https://www.sentinelone.com/labs/the-sprawling-infrastructure-of-a-careless-mercenary/>

Last change to this card: 18 November 2022

Download this actor card in PDF or JSON format