Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:35:10 UTC

APT group: CostaRicto

Names	CostaRicto *(BlackBerry)*
Country	[Unknown]
Motivation	Financial gain
First seen	2017
Description	(BlackBerry) During the past six months, the BlackBerry Research and Intelligence team have been monitoring a cyber-espionage campaign that is targeting disparate victims around the globe. The campaign, dubbed CostaRicto by BlackBerry, appears to be operated by “hackers-for-hire”, a group of APT mercenaries who possess bespoke malware tooling and complex VPN proxy and SSH tunnelling capabilities. Mercenary groups offering APT-style attacks are becoming more and more popular. Their tactics, techniques, and procedures (TTPs) often resemble highly sophisticated state-sponsored campaigns, but the profiles and geography of their victims are far too diverse to be aligned with a single bad actor’s interests. Although in theory the customers of a mercenary APT might include anyone who can afford it, the more sophisticated actors will naturally choose to work with patrons of the highest profile – be it large organizations, influential individuals, or even governments. Having a lot at stake, the cybercriminals must choose very carefully when selecting their commissions to avoid the risk of being exposed.
Observed	Countries: Australia, Austria, Bahamas, Bangladesh, China, Czech, France, India, Mozambique, Netherlands, Portugal, Singapore, USA.
Tools used	CostaBricks, nmap, PowerSploit, PsExec, SombRAT.
Information	<https://blogs.blackberry.com/en/2020/11/the-costaricto-campaign-cyber-espionage-outsourced>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:CostaRicto>

Last change to this card: 07 January 2021

Download this actor card in PDF or JSON format