Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:29:51 UTC

Other threat group: CoralRaider

Names	CoralRaider *(Talos)*	
Country	Vietnam	
Motivation	Financial gain	
First seen	2023	
Description	(Talos) Cisco Talos discovered a new threat actor we're calling "CoralRaider" that we believe is of Vietnamese origin and financially motivated. CoralRaider has been operating since at least 2023, targeting victims in several Asian and Southeast Asian countries. This group focuses on stealing victims' credentials, financial data, and social media accounts, including business and advertisement accounts. They use RotBot, a customized variant of QuasarRAT, and XClient stealer as payloads in the campaign we analyzed. The actor uses the dead drop technique, abusing a legitimate service to host the C2 configuration file and uncommon living-off-the-land binaries (LoLBins), including Windows Forfiles.exe and FoDHelper.exe	
Observed	Countries: Bangladesh, China, Ecuador, Egypt, Germany, India, Indonesia, Japan, Nigeria, Norway, Pakistan, Philippines, Poland, South Korea, Syria, Turkey, UK, USA, Vietnam.	
Tools used	AsyncRAT, LummaC2, NetSupport Manager, Rhadamanthys, RotBot, XClient, Living off the Land.	
Operations performed	Feb 2024	Suspected CoralRaider continues to expand victimology using three information stealers <https://blog.talosintelligence.com/suspected-coralraider-continues-to-expand-victimology-using-three-information-stealers/>
Information	<https://blog.talosintelligence.com/coralraider-targets-socialmedia-accounts/>	

Last change to this card: 18 June 2024

Download this actor card in PDF or JSON format
