Threat Group Cards: A Threat Actor Encyclopedia

APT group: Operation RusticWeb

Names	Operation RusticWeb *(Seqrite)*
Country	Pakistan
Motivation	Information theft and espionage
First seen	2023
Description	(Seqrite) SEQRITE Labs APT-Team has uncovered a phishing campaign targeting various Indian government personnel since October 2023. We have also identified targeting of both government and private entities in the defence sector over December. New Rust-based payloads and encrypted PowerShell commands have been utilized to exfiltrate confidential documents to a web-based service engine, instead of a dedicated command-and-control (C2) server. With actively modifying its arsenal, it has also used fake domains to host malicious payloads and decoy files. This campaign is tracked as Operation RusticWeb, where multiple TTPs overlap with Pakistan-linked APT groups – Transparent Tribe, APT 36 and SideCopy. It also has similarities with Operation Armor Piercer report released by Cisco in 2021, and the targeting with the ESSA scholarship form of AWES was observed by our team back in the same year.
Observed	Sectors: Defense, Government. Countries: India.
Tools used	
Information	<https://www.seqrite.com/blog/operation-rusticweb-targets-indian-govt-from-rust-based-malware-to-web-service-exfiltration/>

Last change to this card: 16 January 2024

Download this actor card in PDF or JSON format