RedHotel, TAG-22 - Threat Group Cards: A Threat Actor Encyclopedia

APT group: RedHotel, TAG-22

Names	RedHotel *(Recorded Future)* TAG-22 *(Recorded Future)* Fishmonger *(ESET)*	
Country	China	
Sponsor	State-sponsored, I-Soon	
Motivation	Information theft and espionage	
First seen	2021	
Description	(Recorded Future) Recorded Future has identified a suspected Chinese state-sponsored group that we track as Threat Activity Group 22 (TAG-22) targeting telecommunications, academia, research and development, and government organizations in Nepal, the Philippines, Taiwan, and more historically, Hong Kong. In this most recent activity, the group likely used compromised GlassFish servers and Cobalt Strike in initial access operations before switching to the bespoke Winnti, ShadowPad, and Spyder backdoors for long-term access using dedicated actor-provisioned command and control infrastructure. Also see Earth Lusca.	
Observed	Sectors: Aerospace, Education, Government, Media, Telecommunications. Countries: Afghanistan, Bangladesh, Bhutan, Cambodia, Czech, Hong Kong, India, Laos, Malaysia, Nepal, Pakistan, Philippines, Taiwan, Thailand, USA, Vietnam and Palestine.	
Tools used	BIOPASS RAT, Brute Ratel, Cobalt Strike, FunnySwitch, ShadowPad Winnti, SprySOCKS, Spyder, Winnti.	
Operations performed	Jul 2021	BIOPASS RAT: New Malware Sniffs Victims via Live Streaming< <https://www.trendmicro.com/en_us/research/21/g/biopass-rat-new-malware-sniffs-victims-via-live-streaming.html>

	2022	Operation “FishMedley” <https://www.welivesecurity.com/en/eset-research/operation-fishmedley/>
Information	<https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/> <https://go.recordedfuture.com/hubfs/reports/cta-2023-0808.pdf> <https://www.sentinelone.com/labs/unmasking-i-soon-the-leak-that-revealed-chinas-cyber-operations/>	

Last change to this card: 21 April 2025

Download this actor card in PDF or JSON format
