Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:26:33 UTC

APT group: RedFoxtrot

Names	RedFoxtrot *(Recorded Future)* Nomad Panda *(CrowdStrike)* TEMP.Trident *(FireEye)* Moshen Dragon *(SentinelLabs)*	
Country	China	
Sponsor	State-sponsored, PLA Unit 69010	
Motivation	Information theft and espionage	
First seen	2014	
Description	(Recorded Future) RedFoxtrot has been active since at least 2014 and predominantly targets government, defense, and telecommunications sectors across Central Asia, India, and Pakistan, aligning with the likely operational remit of Unit 69010. Of particular note, within the past 6 months, Insikt Group detected RedFoxtrot network intrusions targeting 3 Indian aerospace and defense contractors; major telecommunications providers in Afghanistan, India, Kazakhstan, and Pakistan; and multiple government agencies across the region. RedFoxtrot maintains large amounts of operational infrastructure and has likely employed both bespoke and publicly available malware families commonly used by Chinese cyber espionage groups, including Icefog, PlugX, Royal Road, Poison Ivy, ShadowPad, and PCShare. RedFoxtrot activity overlaps with threat groups tracked by other security vendors as Temp.Trident and Nomad Panda.	
Observed	Sectors: Defense, Government, Telecommunications. Countries: Afghanistan, India, Kazakhstan, Pakistan.	
Tools used	8.t Dropper, GUNTERS, Icefog, Impacket, PCShare, PlugX, Poison Ivy, ShadowPad Winnti.	
Operations performed	Aug 2021	4 Chinese APT Groups Identified Targeting Mail Server of Afghan Telecommunications Firm Roshan <https://www.recordedfuture.com/chinese-APT-groups-target-afghan-telecommunications-firm/>

Information	<https://www.recordedfuture.com/redfoxtrot-china-pla-targets-bordering-asian-countries/> <https://go.recordedfuture.com/redfoxtrot-insikt-report> <https://www.sentinelone.com/labs/moshen-dragons-triad-and-error-approach-abusing-security-software-to-sideload-plugx-and-shadowpad/>

Last change to this card: 04 May 2022

Download this actor card in PDF or JSON format
