Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:03:53 UTC

APT group: RedDelta

Names	RedDelta *(Recorded Future)* TA416 *(Proofpoint)*
Country	China
Sponsor	State-sponsored
Motivation	Information theft and espionage
First seen	2020
Description	(Recorded Future) From early May 2020, The Vatican and the Catholic Diocese of Hong Kong were among several Catholic Church-related organizations that were targeted by RedDelta, a Chinese-state sponsored threat activity group tracked by Insikt Group. This series of suspected network intrusions also targeted the Hong Kong Study Mission to China and the Pontifical Institute for Foreign Missions (PIME), Italy. These organizations have not been publicly reported as targets of Chinese threat activity groups prior to this campaign. These network intrusions occured ahead of the anticipated September 2020 renewal of the landmark 2018 China-Vatican provisional agreement, a deal which reportedly resulted in the Chinese Communist Party (CCP) gaining more control and oversight over the country's historically persecuted "underground" Catholic community. In addition to the Holy See itself, another likely target of the campaign includes the current head of the Hong Kong Study Mission to China, whose predecessor was considered to have played a vital role in the 2018 agreement. The suspected intrusion into the Vatican would offer RedDelta insight into the negotiating position of the Holy See ahead of the deal's September 2020 renewal. The targeting of the Hong Kong Study Mission and its Catholic Diocese could also provide a valuable intelligence source for both monitoring the diocese's relations with the Vatican and its position on Hong Kong's pro-democracy movement amidst widespread protests and the recent sweeping Hong Kong national security law. While there is considerable overlap between the observed TTPs of RedDelta and the threat activity group publicly referred to as Mustang Panda, Bronze President (also known as BRONZE PRESIDENT and HoneyMyte), there are a few notable

	distinctions which lead us to designate this activity as RedDelta: • The version of PlugX used by RedDelta in this campaign uses a different C2 traffic encryption method and has a different configuration encryption mechanism than traditional PlugX. • The malware infection chain employed in this campaign has not been publicly reported as used by Mustang Panda. In addition to the targeting of entities related to the Catholic Church, Insikt Group also identified RedDelta targeting law enforcement and government entities in India and a government organization in Indonesia.	
Observed	Sectors: Government, Law enforcement, Telecommunications and The Vatican and Catholic Church-related organizations. Countries: Australia, Cambodia, China, Czech, Ethiopia, Germany, Hong Kong, India, Indonesia, Italy, Mongolia, Myanmar, Slovakia, Spain, Ukraine, USA, Vietnam.	
Tools used	Cobalt Strike, PlugX, Poison Ivy.	
Operations performed	Aug 2020	RedDelta Resumes Its Targeting of the Vatican and Hong Kong Catholic Diocese <https://go.recordedfuture.com/hubfs/reports/cta-2020-0915.pdf>
	Sep 2020	Following the Chinese National Day holiday in September, Proofpoint researchers observed a resumption of activity by the APT actor TA416. <https://www.proofpoint.com/us/blog/threat-insight/ta416-goes-ground-and-returns-golang-plugx-malware-loader>
	Mar 2021	Operation “Dianxun” Operation Diànxùn: Cyberespionage Campaign Targeting Telecommunication Companies <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/operation-dianxun-cyberespionage-campaign-targeting-telecommunication-companies/>
	Feb 2022	Most recently on February 28, 2022, TA416 began using a compromised email address of a diplomat from a European NATO country to target a different country’s diplomatic offices. The targeted individual worked in refugee and migrant services. <https://www.proofpoint.com/us/blog/threat-insight/good-bad-and-web-bug-ta416-increases-operational-tempo-against-european>
	Jul 2023	Chinese State-Sponsored RedDelta Targeted Taiwan, Mongolia, and Southeast Asia with Adapted PlugX Infection Chain

		<https://go.recordedfuture.com/hubfs/reports/cta-cn-2025-0109.pdf>
Information	<https://go.recordedfuture.com/hubfs/reports/cta-2020-0728.pdf>	

Last change to this card: 22 February 2025

Download this actor card in PDF or JSON format
