Threat Group Cards: A Threat Actor Encyclopedia

APT group: TA413

Names	TA413 *(Proofpoint)* White Dev 9 *(PWC)*
Country	China
Motivation	Information theft and espionage
First seen	2019
Description	(Proofpoint) Beginning in the first half of 2020, the rapid international spread of the COVID-19 virus introduced a shift within the threat landscape towards pandemic-themed social engineering lures. Public research has noted several Chinese APT groups adopting COVID-19 phishing lures in recent months to carry out espionage campaigns against established and expanding target sets. In March 2020, Proofpoint researchers observed a phishing campaign impersonating the World Health Organization's (WHO) guidance on COVID-19 critical preparedness to deliver a new malware family that researchers have dubbed "Sepulcher". This campaign targeted European diplomatic and legislative bodies, non-profit policy research organizations, and global organizations dealing with economic affairs. Additionally, a sender email identified in this campaign has been linked to historic Chinese APT targeting of the international Tibetan community using payloads linked to LuckyCat malware. Subsequently, a phishing campaign from July 2020 targeting Tibetan dissidents was identified delivering the same strain of Sepulcher malware. Operator email accounts identified in this campaign have been publicly linked to historic Chinese APT campaigns targeting the Tibetan community delivering ExileRAT malware. Based on the use of publicly known sender addresses associated with Tibetan dissident targeting and the delivery of Sepulcher malware payloads, Proofpoint researchers have attributed both campaigns to the APT actor TA413, which has previously been documented in association with ExileRAT. The usage of publicly known Tibetan-themed sender accounts to deliver Sepulcher malware demonstrates a short-term realignment of TA413's targets of interest. While best known for their campaigns against the Tibetan diaspora, this APT group associated with the Chinese state interest prioritized intelligence collection around Western economies reeling from COVID-19 in March 2020 before resuming more conventional targeting later this year.

	An overlap in infrastructure has been observed with Lucky Cat.	
Observed	Countries: Tibet and Europe.	
Tools used	ExileRAT, Sepulcher.	
Operations performed	Jan 2021	TA413 Leverages New FriarFox Browser Extension to Target the Gmail Accounts of Global Tibetan Organizations <https://www.proofpoint.com/us/blog/threat-insight/ta413-leverages-new-friarfox-browser-extension-target-gmail-accounts-global>
	May 2022	Chinese-linked threat actors are now actively exploiting a Microsoft Office zero-day vulnerability (known as 'Follina') to execute malicious code remotely on Windows systems. <https://www.bleepingcomputer.com/news/security/windows-msdt-zero-day-now-exploited-by-chinese-apt-hackers/>
	2022	Chinese State-Sponsored Group TA413 Adopts New Capabilities in Pursuit of Tibetan Targets <https://www.recordedfuture.com/chinese-state-sponsored-group-ta413-adopts-new-capabilities-in-pursuit-of-tibetan-targets>
Information	<https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic>	

Last change to this card: 18 November 2022

Download this actor card in PDF or JSON format
