Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:56:06 UTC

APT group: ChamelGang

Names	ChamelGang *(Positive Technlogies)* CamoFei *(TeamT5)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2021	
Description	(Positive Technologies) In Q2 2021, the PT Expert Security Center incident response team conducted an investigation in an energy company. The investigation revealed that the company's network had been compromised by an unknown group for the purpose of data theft. We gave the group the name ChamelGang (from the word 'chameleon'), because the group disguised its malware and network infrastructure under legitimate services of Microsoft, TrendMicro, McAfee, IBM, and Google. The attackers employed two methods. They acquired domains that imitate legitimate ones. In addition, the APT group placed SSL certificates that also imitated legitimate ones on its servers. To achieve their goal, the attackers used a trending penetration method—supply chain. The group compromised a subsidiary and penetrated the target company's network through it.	
Observed	Sectors: Aviation, Energy, Government. Countries: Afghanistan, Brazil, India, Japan, Lithuania, Nepal, Russia, Taiwan, Turkey, USA, Vietnam.	
Tools used	7-Zip, BeaconLoader, Cobalt Strike, DoorMe, FRP, ProxyT, Tiny SHell.	
Operations performed	2022	ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware <https://www.sentinelone.com/labs/chamelgang-attacking-critical-infrastructure-with-ransomware/>
	Jun 2023	ChamelGang and ChamelDoH: A DNS-over-HTTPS implant <https://stairwell.com/news/chamelgang-and-chameldoh-a-dns-over-https-implant/>
Information	<https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/new-apt-group-chamelgang/>	

Last change to this card: 26 August 2024

Download this actor card in PDF or JSON format

Source: https://apt.etda.or.th/cgi-bin/showcard.cgi?u=832c145a-c7d3-43b4-9f9e-6998371616d7