Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:21:15 UTC

APT group: TA459

Names	TA459 *(Proofpoint)* G0062 *(MITRE)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2017	
Description	(Proofpoint) On April 20 [2017], Proofpoint observed a targeted campaign focused on financial analysts working at top global financial firms operating in Russia and neighboring countries. These analysts were linked by their coverage of the telecommunications industry, making this targeting very similar to, and likely a continuation of, activity described in our “In Pursuit of Optical Fibers and Troop Intel” blog. This time, however, attackers opportunistically used spear-phishing emails with a Microsoft Word attachment exploiting the recently patched CVE-2017-0199 to deploy the ZeroT Trojan, which in turn downloaded the PlugX Remote Access Trojan (RAT). Proofpoint is tracking this attacker, believed to operate out of China, as TA459. The actor typically targets Central Asian countries, Russia, Belarus, Mongolia, and others. TA549 possesses a diverse malware arsenal including PlugX, NetTraveler, and ZeroT.	
Observed	Sectors: Financial, Telecommunications and journalists. Countries: Belarus, Mongolia, Russia and Central Asia others.	
Tools used	Gh0st RAT, NetTraveler, PlugX, ZeroT.	
Operations performed	Apr 2022	Tracing State-Aligned Activity Targeting Journalists, Media <https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists>
Information	<https://www.proofpoint.com/us/threat-insight/post/apt-targets-financial-analysts>	
MITRE ATT&CK	<https://attack.mitre.org/groups/G0062/>	

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
