Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:21:23 UTC

APT group: IronHusky

Names	IronHusky *(Kaspersky)* BBCY-TA1 *(BlackBerry)*	
Country	China	
Motivation	Information theft and espionage	
First seen	2017	
Description	(Kaspersky) IronHusky is a Chinese-speaking actor that we first detected in summer 2017. It is very focused on tracking the geopolitical agenda of targets in central Asia with a special focus in Mongolia, which seems to be an unusual target. This actor crafts campaigns for upcoming events of interest. In this case, they prepared and launched one right before a meeting with the International Monetary Fund and the Mongolian government at the end of January 2018. At the same time, they stopped their previous operations targeting Russian military contractors, which speaks volumes about the group's limitations. In this new campaign, they exploited CVE-2017-11882 to spread common RATs typically used by Chinese-speaking groups, such as PlugX and PoisonIvy.	
Observed	Sectors: Defense, Financial, Government. Countries: Mongolia, Russia.	
Tools used	MysterySnail RAT, Poison Ivy, PlugX.	
Operations performed	Aug 2021	Operation "MysterySnail" In late August and early September 2021, Kaspersky technologies detected attacks with the use of an elevation of privilege exploit on multiple Microsoft Windows servers. <https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/>
Information	<https://securelist.com/apt-trends-report-q1-2018/85280/> <https://securelist.com/mysterysnail-new-version/116226/>	

Last change to this card: 21 April 2025

Download this actor card in PDF or JSON format
