Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:53:23 UTC

APT group: YoroTrooper

Names	YoroTrooper *(Talos)* Silent Lynx *(Seqrite)*
Country	Kazakhstan
Motivation	Information theft and espionage
First seen	2022
Description	(Talos) Cisco Talos has identified a new threat actor, which we are naming “YoroTrooper,” that has been running several successful espionage campaigns since at least June 2022. YoroTrooper’s main targets are government or energy organizations in Azerbaijan, Tajikistan, Kyrgyzstan and other Commonwealth of Independent States (CIS), based on our analysis. We also observed YoroTrooper compromise accounts from at least two international organizations: a critical European Union (EU) health care agency and the World Intellectual Property Organization (WIPO). Successful compromises also included Embassies of European countries including Azerbaijan and Turkmenistan. We assess the actor also likely targets other organizations across Europe and Turkish (Türkiye) government agencies. Information stolen from successful compromises include credentials from multiple applications, browser histories & cookies, system information and screenshots.
Observed	Sectors: Energy, Financial, Government. Countries: Azerbaijan, Kyrgyzstan, Tajikistan, Turkey, Turkmenistan and Europe.
Tools used	Loda, Meterpreter, Stink, Warzone RAT.
Information	<https://blog.talosintelligence.com/yorotrooper-espionage-campaign-cis-turkey-europe/> <https://blog.talosintelligence.com/attributing-yorotrooper/> <https://www.seqrite.com/blog/silent-lynx-apt-targeting-central-asian-entities/>

Last change to this card: 22 February 2025

Download this actor card in PDF or JSON format