DustSquad, Golden Falcon - Threat Group Cards: A Threat Actor Encyclopedia

APT group: DustSquad, Golden Falcon

Names	DustSquad *(Kaspersky)* Golden Falcon *(Qihoo 360)* APT-C-34 *(Qihoo 360)* Nomadic Octopus *(ESET)* G0133 *(MITRE)*	
Country	Russia	
Motivation	Information theft and espionage	
First seen	2014	
Description	(Kaspersky) For the last two years we have been monitoring a Russian-language cyberespionage actor that focuses on Central Asian users and diplomatic entities. We named the actor DustSquad and have provided private intelligence reports to our customers on four of their campaigns involving custom Android and Windows malware. In this blogpost we cover a malicious program for Windows called Octopus that mostly targets diplomatic entities. The name was originally coined by ESET in 2017 after the 0ct0pus3.php script used by the actor on their old C2 servers. We also started monitoring the malware and, using Kaspersky Attribution Engine based on similarity algorithms, discovered that Octopus is related to DustSquad, something we reported in April 2018. In our telemetry we tracked this campaign back to 2014 in the former Soviet republics of Central Asia (still mostly Russian-speaking), plus Afghanistan.	
Observed	Sectors: Defense, Government, Media and diplomats and dissidents. Countries: Afghanistan, Kazakhstan and Central Asia.	
Tools used	Harpoon, Octopus, Paperbug, Remote Control System.	
Operations performed	2020	Nomadic Octopus' Paperbug Campaign <https://www.prodaft.com/m/reports/PAPERBUG_TLPWHITE-1.pdf>

Information	<https://securelist.com/octopus-infested-seas-of-central-asia/88200/> <https://www.zdnet.com/article/extensive-hacking-operation-discovered-in-kazakhstan/>
MITRE ATT&CK	<https://attack.mitre.org/groups/G0133/>

Last change to this card: 16 August 2025

Download this actor card in PDF or JSON format
