Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:05:30 UTC

APT group: AeroBlade

Names	AeroBlade *(BlackBerry)*
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2022
Description	(BlackBerry) BlackBerry has uncovered a previously unknown threat actor targeting an aerospace organization in the United States, with the apparent goal of conducting commercial and competitive cyber espionage. The BlackBerry Threat Research and Intelligence team is tracking this threat actor as AeroBlade. The actor used spear-phishing as a delivery mechanism: A weaponized document, sent as an email attachment, contains an embedded remote template injection technique and a malicious VBA macro code, to deliver the next stage to the final payload execution. Evidence suggests that the attacker's network infrastructure and weaponization became operational around September 2022. BlackBerry assesses with medium to high confidence that the offensive phase of the attack occurred in July 2023. The attacker improved its toolset during that time, making it stealthier, while the network infrastructure remained the same. Given the final payload functionality and the subject of the attack, BlackBerry assesses with medium to high confidence that the goal of this attack was commercial cyber espionage.
Observed	Sectors: Aerospace. Countries: USA.
Tools used	
Information	<https://blogs.blackberry.com/en/2023/11/aeroblade-on-the-hunt-targeting-us-aerospace-industry>

Last change to this card: 16 January 2024

Download this actor card in PDF or JSON format