Threat Group Cards: A Threat Actor Encyclopedia

Other threat group: ResumeLooters

Names	ResumeLooters *(Group-IB)*
Country	[Unknown]
Motivation	Financial gain
First seen	2023
Description	(Group-IB) In November 2023, Group-IB's Threat Intelligence unit detected a massive malicious campaign targeting employment agencies and retail companies primarily located in the APAC region, to steal and sell sensitive user data. The campaign was attributed to a previously unknown group. Due to the threat actor's focus on job search platforms and the theft of resumes, Group-IB dubbed it ResumeLooters. Overall, the researchers identified 65 websites compromised by ResumeLooters between November 2023 and December 2023. By using SQL injection attacks against websites, the threat actor attempts to steal user databases that may include names, phone numbers, emails, and DOBs, as well as information about job seekers' experience, employment history, and other sensitive personal data. The stolen data is then put up for sale by the threat actor in Telegram channels, identified by Group-IB's Threat intelligence platform.
Observed	Sectors: Financial, Retail and Delivery, Job seeking, Professional services and Real estate.. Countries: Australia, Brazil, China, India, Taiwan, Thailand, Turkey, Vietnam.
Tools used	
Information	<https://www.group-ib.com/blog/resumelooters/>

Last change to this card: 06 March 2024

Download this actor card in PDF or JSON format