Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:27:55 UTC

APT group: UltraRank

Names	UltraRank *(Group-IB)*	
Country	[Unknown]	
Motivation	Financial crime	
First seen	2015	
Description	(Group-IB) In August 2020, Group-IB published the report 'UltraRank: the unexpected twist of a JS-sniffer triple threat'. The report described the operations of the cybercriminal group UltraRank, which in five years of activity had successfully attacked 691 eCommerce stores and 13 website service providers. In November 2020, Group-IB experts discovered a new wave of UltraRank attacks. Even though new attacks were detected at the time, part of the group's infrastructure remained active and some sites were still infected. The cybercriminals did not use existing domains for new attacks but switched to a new infrastructure to store malicious code and collect intercepted payment data.	
Observed		
Tools used	SnifLite.	
Operations performed	Nov 2020	Group-IB experts discovered a new wave of UltraRank attacks. <https://www.group-ib.com/blog/ultrarank>
Information	<https://www.group-ib.com/blog/ultrarank>	

Last change to this card: 07 January 2021

Download this actor card in PDF or JSON format