Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:02:59 UTC

APT group: OPERA1ER

Names	OPERA1ER *(Group-IB)* DESKTOP-GROUP *(c-APT-ure)* Common Raven *(SWIFT)* NXSMS *(Orange-CERT-CC)* Bluebottle *(Symantec)*	
Country	[Unknown]	
Motivation	Financial crime	
First seen	2016	
Description	(Group-IB) Digital forensics artifacts analyzed by Group-IB and Orange following more than 30 successful intrusions of OPERA1ER between 2018 and 2022 helped to trace down affected organizations in Ivory Coast, Mali, Burkina Faso, Benin, Cameroon, Bangladesh, Gabon, Niger, Nigeria, Paraguay, Senegal, Sierra Leone, Uganda, Togo, Argentina. Many of the victims identified were successfully attacked twice, and their infrastructure was then used to attack other organizations. According to Group-IB's evaluation, between 2018 and 2022, OPERA1ER managed to steal at least $11 million, and the actual amount of damage could be as high as $30 million.	
Observed	Sectors: Financial, Telecommunications. Countries: Argentina, Bangladesh, Benin, Burkina Faso, Cameroon, Cote d'Ivoire, Gabon, Mali, Niger, Nigeria, Paraguay, Senegal, Sierra Leone, Togo, Uganda.	
Tools used	Agent Tesla, BitRAT, BlackNET RAT, Cobalt Strike, Metasploit, NetWire RC, Neutrino, Ngrok, PsExec, RDPWrap, RemcosRAT, Revealer Keylogger, VenomRAT, Living off the Land.	
Operations performed	May 2022	Bluebottle: Campaign Hits Banks in French-speaking Countries in Africa <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/bluebottle-banks-targeted-africa>
Counter operations	Jul 2023	Operation "Nervone" Suspected key figure of notorious cybercrime group arrested in joint operation <https://www.interpol.int/News-and-Events/News/2023/Suspected-

		key-figure-of-notorious-cybercrime-group-arrested-in-joint-operation>
Information	<https://www.group-ib.com/media-center/press-releases/opera1er/>	

Last change to this card: 05 September 2023

Download this actor card in PDF or JSON format
