Bad Magic, RedStinger - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:42:22 UTC

APT group: Bad Magic, RedStinger

Names	Bad Magic *(Kaspersky)* RedStinger *(Malwarebytes)* CloudWizard *(Kaspersky)*	
Country	[Unknown]	
Motivation	Information theft and espionage	
First seen	2020	
Description	(Kaspersky) In October 2022, we identified an active infection of government, agriculture and transportation organizations located in the Donetsk, Lugansk, and Crimea regions. Although the initial vector of compromise is unclear, the details of the next stage imply the use of spear phishing or similar methods. The victims navigated to a URL pointing to a ZIP archive hosted on a malicious web server.	
Observed	Sectors: Defense, Food and Agriculture, Government, Transportation. Countries: Ukraine.	
Tools used	CommonMagic, PowerMagic.	
Operations performed	2020	Uncovering RedStinger - Undetected APT cyber operations in Eastern Europe since 2020 <https://www.malwarebytes.com/blog/threat-intelligence/2023/05/redstinger>
	May 2023	CloudWizard APT: the bad magic story goes on <https://securelist.com/cloudwizard-apt/109722/>
Information	<https://securelist.com/bad-magic-apt/109087/>	

Last change to this card: 21 June 2023

Download this actor card in PDF or JSON format
