

Operation Rusty Flag - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 13:18:13 UTC

[Home](#) > [List all groups](#) > Operation Rusty Flag

APT group: Operation Rusty Flag

Names	Operation Rusty Flag (<i>Deep Instinct</i>)
Country	[Unknown]
Motivation	Information theft and espionage
First seen	2023
Description	<p>(Deep Instinct) The operation has at least two different initial access vectors.</p> <p>The operation is not associated with a known threat actor; the operation was instead named because of their novel malware written in the Rust programming language.</p> <p>One of the lures used in the operation is a modified document that was used by the Tropical Scorpion, RomCom group. This could be a deliberate “false flag”.</p>
Observed	Countries: Azerbaijan .
Tools used	
Information	< https://www.deepinstinct.com/blog/operation-rusty-flag-a-malicious-campaign-against-azerbaijani-targets >

Last change to this card: 12 October 2023

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.etda.or.th/cgi-bin/showcard.cgi?u=ae038cc4-4e81-4107-bfef-32646c33fb5d>