

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:10:02 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool RustDown

Tool: RustDown

Names	RustDown
Category	Malware
Type	Backdoor
Description	(Intezer) In October 2023, we discovered a new malware written in Rust. The sample is a 32-bit Windows executable masquerading as a PHP framework component. While the codebase is new, the malware consistently shares TTPs used by the WildCard threat actor in both SysJoker and its variants. The name of the malware is derived from the developers, as evidenced by a leftover PDB path.
Information	< https://intezer.com/blog/research/wildcard-evolution-of-sysjoker-cyber-threat/ >

Last change to this tool card: 30 November 2023

Download this tool card in [JSON](#) format

All groups using tool RustDown

Changed	Name	Country	Observed
APT groups			
	WildCard	[Unknown]	2021

1 group listed (1 APT, 0 other, 0 unknown)

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=b6f78f30-6781-4ba2-81d3-9a36e1eb4723>