Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 01:05:24 UTC

Tool: SPICA

Names	SPICA
Category	Malware
Type	Backdoor, Reconnaissance, Credential stealer, Info stealer, Downloader, Exfiltration
Description	(Google) SPICA is written in Rust, and uses JSON over websockets for command and control (C2). It supports a number of commands including: • Executing arbitrary shell commands • Stealing cookies from Chrome, Firefox, Opera and Edge • Uploading and downloading files • Perusing the filesystem by listing the contents of it • Enumerating documents and exfiltrating them in an archive • There is also a command called “telegram,” but the functionality of this command is unclear Once executed, SPICA decodes an embedded PDF, writes it to disk, and opens it as a decoy for the user. In the background, it establishes persistence and starts the main C2 loop, waiting for commands to execute.
Information	<https://blog.google/threat-analysis-group/google-tag-coldriver-russian-phishing-malware/>
MITRE ATT&CK	<https://attack.mitre.org/software/S1140>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.spica>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool SPICA

Changed	Name	Country	Observed

APT groups

	Cold River		2019-Jan 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=070ba31e-1ec7-411f-9325-57391a1ca6cc