

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:14:33 UTC

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

Tool: AcidPour

Names	AcidPour
Category	Malware
Type	Wiper
Description	(SentinelOne) On March 16th, 2024, we identified a suspicious Linux binary uploaded from Ukraine. Initial analysis showed surface similarities with the infamous AcidRain wiper used to disable KA-SAT modems across Europe at the start of the Russian invasion of Ukraine (commonly identified by the ‘Viasat hack’ misnomer). Since our initial finding, no similar samples or variants have been detected or publicly reported until now. This new sample is a confirmed variant we refer to as ‘AcidPour’, a wiper with similar and expanded capabilities.
Information	< https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/ >
MITRE ATT&CK	< https://attack.mitre.org/software/S1167 >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/elf.acidpour >

Last change to this tool card: 28 June 2025

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

All groups using tool AcidPour

Changed	Name	Country	Observed
Unknown groups			
	_ [Interesting malware not linked to an actor yet] _		

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=9ccc7961-d80b-4406-b644-214e82cdf048>