Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:41:13 UTC

Tool: AcidRain

Names	AcidRain
Category	Malware
Type	Wiper
Description	(SentinelOne) AcidRain's functionality is relatively straightforward and takes a bruteforce attempt that possibly signifies that the attackers were either unfamiliar with the particulars of the target firmware or wanted the tool to remain generic and reusable. The binary performs an in-depth wipe of the filesystem and various known storage device files. If the code is running as root, AcidRain performs an initial recursive overwrite and delete of non-standard files in the filesystem.
Information	<https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/> <https://therecord.media/a-deeper-look-at-the-malware-being-used-on-ukrainian-targets/> <https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works>
MITRE ATT&CK	<https://attack.mitre.org/software/S1125>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.acidrain>

Last change to this tool card: 19 June 2024

Download this tool card in JSON format

All groups using tool AcidRain

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

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