Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:04:11 UTC

Tool: Comet

Names	Comet Meteor Stardust
Category	Malware
Type	Wiper
Description	(Check Point) The wiping procedure itself is pretty simple. First, the malware goes over the files and directories from the paths_to_wipe config, fills them with zero-bytes instead of their real content, and then deletes them. After the wiping procedure, the malware tries to delete the shadow copies by running the following commands: vssadmin.exe delete shadows /all /quiet **and **C:\\Windows\\system32\\wbem\\wmic.exe shadowcopy delete. Finally, the malware enters an infinite loop where it sleeps based on the is_alive_loop_interval value from the configuration file and writes 'Meteor is still alive.' to the log in every iteration. If all this rings familiar to you, it should; it’s all straight out from the ransomware playbook — except this isn’t ransomware, which requires delicate orchestration of public-key and private-key cryptography to make the machine ultimately recoverable; this is Nuke-it-From-Orbit-ware. It’s a one-way trip.
Information	<https://research.checkpoint.com/2021/indra-hackers-behind-recent-attacks-on-iran/>

Last change to this tool card: 01 November 2021

Download this tool card in JSON format

All groups using tool Comet

Changed	Name	Country	Observed	
APT groups				
	Indra	[Unknown]	2019	

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