Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:22:25 UTC

Tool: Korkerds

Names	Korkerds
Category	Malware
Type	Miner
Description	(Trend Micro) We recently encountered a cryptocurrency-mining malware (detected by Trend Micro as Coinminer.Linux.KORKERDS.AB) affecting Linux systems. It is notable for being bundled with a rootkit component (Rootkit.Linux.KORKERDS.AA) that hides the malicious process' presence from monitoring tools. This makes it difficult to detect, as infected systems will only indicate performance issues. The malware is also capable of updating and upgrading itself and its configuration file.
Information	<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/cryptocurrency-mining-malware-targets-linux-systems-uses-rootkit-for-stealth>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:KORKERDS>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Korkerds

Changed	Name	Country	Observed	
Other groups				
	Pacha Group		2018-May 2019	

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