Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:53:29 UTC

Tool: Drovorub

Names	Drovorub
Category	Malware
Type	Rootkit, Backdoor, Exfiltration, Tunneling
Description	(NSA/FBI) Drovorub is a Linux malware toolset consisting of an implant coupled with a kernel module rootkit, a file tra port forwarding tool, and a Command and Control (C2) server. When deployed on a victim machine, the Drovorub impla provides the capability for direct communications with actor-controlled C2 infrastructure; file download and upload capa execution of arbitrary commands as 'root'; and port forwarding of network traffic to other hosts on the network.
Information	<https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUC <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/on-drovorub-linux-kernel-security-best-practices/>
MITRE ATT&CK	<https://attack.mitre.org/software/S0502/>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool Drovorub

Changed	Name	Country	Observed	
APT groups				
	Sofacy, APT 28, Fancy Bear, Sednit		2004-Apr 2025	

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