Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:22:41 UTC

Tool: RawDisk

Names	RawDisk
Category	Tools
Description	RawDisk is a legitimate commercial driver from the EldoS Corporation that is used for interacting with files, disks, and partitions. The driver allows for direct modification of data on a local computer's hard drive. In some cases, the tool can enact these raw disk modifications from user-mode processes, circumventing Windows operating system security features.
Information	<https://web.archive.org/web/20160303200515/https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Destructive-Malware-Report.pdf> <https://www.itprotoday.com/windows-78/eldos-provides-raw-disk-access-vista-and-xp>
MITRE ATT&CK	<https://attack.mitre.org/software/S0364/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:rawdisk>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool RawDisk

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=327e1f94-7307-4f57-a992-f7e7cc206f5e