Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:24:40 UTC

Tool: Destover

Names	Destover Sierras
Category	Malware
Type	Wiper
Description	(Kaspersky) The most interesting aspects of the destructive functionality of the malware are related to the selection and storage/delivery of the drivers that are now used repeatedly in these kinds of sabotage attacks. The Destover droppers install and run EldoS RawDisk drivers to evade NTFS security permissions and overwrite disk data and the MBR itself. There are implications for data recovery in this. In the case of the DarkSeoul malware, the overwritten data could be restored using a method similar to the restoration of the Shamoon ‘destroyed’ data. Destover data recovery is likely to be the same.
Information	<https://securelist.com/destover/67985/> <https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sierras>

Last change to this tool card: 14 May 2020

Download this tool card in JSON format

All groups using tool Destover

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

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