Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:36:03 UTC

Tool: HDRoot

Names	HDRoot HDD Rootkit
Category	Malware
Type	Backdoor, Rootkit
Description	(Kaspersky) The program parameters are quite self-explanatory – this tool installs a bootkit that infects the operating system during the boot stage with an arbitrary backdoor specified as a parameter. The backdoor has to be a Win32 executable or dynamic link library. This utility is called “HDD Rootkit”; hence the base of our verdict names HDRoot. On 22 August 2006 the version number was 1.2.
Information	<https://securelist.com/i-am-hdroot-part-1/72275/> <https://securelist.com/analysis/publications/72356/i-am-hdroot-part-2/> <http://williamshowalter.com/a-universal-windows-bootkit/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.hdroot>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:hdroot>

Last change to this tool card: 24 April 2021

Download this tool card in JSON format

All groups using tool HDRoot

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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