Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 03:23:45 UTC

Tool: Hdump

Names	Hdump
Category	Malware
Type	Credential stealer
Description	(Palo Alto) The threat actor deployed and used Hdump.exe (renamed h64.exe), which is a credential stealing utility that researchers have observed Chinese threat actors using. Threat actors used Hdump to dump credentials from memory using the -a (dump all) flag.
Information	<https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/> <https://valhalla.nextron-systems.com/info/rule/Winnti_APT_Hdump_Tool>

Last change to this tool card: 12 October 2023

Download this tool card in JSON format

All groups using tool Hdump

Changed	Name	Country	Observed	
APT groups				
	Mustang Panda, Bronze President		2012-Jun 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=82482189-4a8a-4419-873f-457067b94c56