Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:29:44 UTC

Tool: Hekatomb

Names	Hekatomb
Category	Tools
Type	Credential stealer
Description	Hekatomb is a python script that connects to LDAP directory to retrieve all computers and users informations. Then it will download all DPAPI blob of all users from all computers. Finally, it will extract domain controller private key through RPC uses it to decrypt all credentials.
Information	<https://github.com/Processus-Thief/HEKATOMB>

Last change to this tool card: 29 November 2023

Download this tool card in JSON format

All groups using tool Hekatomb

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: Scattered Spider	[Unknown]	2022-Aug 2025	

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