Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:20:04 UTC

Tool: DCSync

Names	DCSync
Category	Malware
Type	Credential stealer
Description	(Stealthbits) DCSync is a late-stage kill chain attack that allows an attacker to simulate the behavior of Domain Controller (DC) in order to retrieve password data via domain replication. Once an attacker has access to a privileged account with domain replication rights, the attacker can utilize replication protocols to mimic a domain controller. DCSync itself is a command within Mimikatz and relies on utilizing specific commands within the Microsoft Directory Replication Service Remote Protocol (MS-DRSR) to simulates the behavior of a domain controller and asks other domain controllers to replicate information by using the Directory Replication Service Remote Protocol (MS-DRSR). Utilizing these protocols, this attack takes advantage of valid and necessary functions of Active Directory, which cannot be turned off or disabled.
Information	<https://blog.stealthbits.com/what-is-dcsync-an-introduction/>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool DCSync

Changed	Name	Country	Observed	
APT groups				
	↳ Subgroup: Scattered Spider	[Unknown]	2022-Aug 2025	
	Calypso		2016-Aug 2021	

	Mustang Panda, Bronze President		2012-Jun 2025	

3 groups listed (3 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7a686766-5739-4691-bc3a-3f6f8279ec28