RDCMan.ps1 - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:35:58 UTC

Tool: Decrypt-RDCMan.ps1

Names	Decrypt-RDCMan.ps1
Category	Malware
Type	Vulnerability scanner
Description	(SecureWorks) Decrypt-RDCMan.ps1 is a component of the PoshC2 penetration testing framework. It is used to decrypt passwords stored in the RDCMan configuration file, which stores details of servers and encrypted credentials to quickly establish remote desktop sessions. Recovered credentials could give the threat actors additional access within the environment. LYCEUM deployed this tool via DanBot approximately one hour after gaining initial access to a compromised environment.
Information	<https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign> <https://github.com/nettitude/PoshC2/blob/master/Modules/Decrypt-RDCMan.ps1>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Decrypt-RDCMan.ps1

Changed	Name	Country	Observed	
APT groups				
	Hexane		2017-Jun 2022	

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