Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:54:47 UTC

Tool: Md_client

Names	Md_client
Category	Malware
Type	Reconnaissance, Backdoor, Downloader, Exfiltration
Description	(Bitdefender) This component uses the UDP and the 53 port to communicate with the C&C server and is capable of: • Collecting system information like computer name, user name, osverion, processor architecture; • Creating a remote shell by running a cmd.exe with stdin/stdout/stderr “connected” to the C&C • Sending the Logical Drive Strings • Listing a directory • Uploading and downloading a file • Deleting a directory • Executing a command using ShellExecuteW • Executing a command using CreateDesktop (“mydktop1”) and CreateProcess
Information	<https://www.bitdefender.com/files/News/CaseStudies/study/379/Bitdefender-Whitepaper-Chinese-APT.pdf>

Last change to this tool card: 06 January 2021

Download this tool card in JSON format

All groups using tool Md_client

Changed	Name	Country	Observed	
APT groups				
	FunnyDream		2018	

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