Threat Group Cards: A Threat Actor Encyclopedia

Tool: PACMAN

Names	PACMAN
Category	Malware
Type	Reconnaissance, Backdoor, Info stealer, Credential stealer
Description	(FireEye) PACMAN is a backdoor designed to run as a service. Once active, PACMAN calls out to a hard-coded C&C domain. PACMAN has the following capabilities: retrieve drive types, terminate processes, create directories, obtain a directory listing, move files, return file attributes, remove directories, create files, read files, and copy files. PACMAN can also extract credentials from Internet Explorer.
Information	<https://paper.bobylive.com/Security/APT_Report/APT-41.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool PACMAN

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

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