Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:29:36 UTC

Tool: DUSTPAN

Names	DUSTPAN StealthVector
Category	Malware
Type	Dropper
Description	(Mandiant) DUSTPAN is an in-memory dropper written in C/C++ that decrypts and executes an embedded payload. Different variations of DUSTPAN may also load an external payload off disk from a hard-coded file path encrypted in the Portable Executable (PE) file. DUSTPAN may be configured to inject the decrypted payload into another process or create a new thread and execute it within its own process space.
Information	<https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust> <https://cloud.google.com/blog/topics/threat-intelligence/apt41-us-state-governments>
MITRE ATT&CK	<https://attack.mitre.org/software/S1158>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.dustpan>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool DUSTPAN

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

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=023d9604-42c5-4f69-bc1e-625c5795eb1c