Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:25:37 UTC

Tool: DUSTTRAP

Names	DUSTTRAP DodgeBox CurveLoad StealthReacher
Category	Malware
Type	Dropper, Loader
Description	(Mandiant) DUSTTRAP is a multi-stage plugin framework with multiple components. DUSTTRAP begins with a launcher (Stage 1) that AES-128-CFB decrypts an encrypted on-disk PE file .dll.mui and executes it in memory. Decryption relies on the target machine's HKLM\SOFTWARE\Microsoft\Cryptography\MachineGUID, thereby keying the launcher to the victim system. The decrypted PE from the launcher is a memory-only dropper (Stage 2) that is responsible for decrypting an embedded configuration and two or more embedded plugin dynamic-link libraries (DLLs) from its .lrsrc section. Once executed, these DLLs begin the setup of the modular plugin system. The first observed plugin (Stage 3) is responsible for low-level network setup and encryption. The second observed plugin (Stage 4) is responsible for higher-level network operations and may function as a downloader for additional plugins that, when loaded, may register themselves with prior components in the execution chain for additional functionality. We've observed the second plugin to vary in functionality and more plugin variants likely exist.
Information	<https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust>
MITRE ATT&CK	<https://attack.mitre.org/software/S1159>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.dusttrap>

Last change to this tool card: 27 December 2024

Download this tool card in JSON format

All groups using tool DUSTTRAP

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=10f211ca-a8cb-4c7f-9199-a66ab8c99cbd