Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:13:29 UTC

Tool: LESLIELOADER

Names	LESLIELOADER
Category	Tools
Type	Loader
Description	(Kroll) The loader achieves its goal by decoding and decrypting a secondary payload binary, then injecting it into a notepad.exe instance. This injection allows the malware to blend with legitimate system activity as it shares the memory space of a legitimate application. Despite detection tools' ability to mitigate process injections, they remain a common evasion tactic.
Information	<https://www.kroll.com/en/insights/publications/cyber/leslieloader-undocumented-loader-observed> <https://go.recordedfuture.com/hubfs/reports/cta-2024-0716.pdf>

Last change to this tool card: 27 August 2024

Download this tool card in JSON format

All groups using tool LESLIELOADER

Changed	Name	Country	Observed	
APT groups				
	TAG-100		2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=532e4f3e-a52a-4e25-ba6e-c3d79e3d9ecd