Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:33:59 UTC

Tool: Tdrop

Names	Tdrop
Category	Malware
Type	Dropper
Description	(McAfee) TDrop is the third generation of HTTP Troy. TDrop uses one of two DLL files, payload32.dll and payload64.dll, and injects one, depending on operating system, into svchost.exe. Previous versions used bs.dll, which contained the code for communicating with the IRC botnet. TDrop has some further functionality not present in HTTP Troy that extends this Trojan's ability to operate on 64-bit machines and to evade automated analysis systems and emulation technologies.
Information	<https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-dissecting-operation-troy.pdf>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Tdrop

Changed	Name	Country	Observed	
APT groups				
	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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