Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:34:37 UTC

Tool: Tdrop2

Names	Tdrop2
Category	Malware
Type	Downloader
Description	(Palo Alto) The new malware variant, which we call TDrop2, proceeds to select a legitimate Microsoft Windows executable in the system32 folder executes it, and then uses the legitimate executable's process as a container for the malicious code, a technique known as process hollowing. Once successfully executed, the corresponding process then attempts to retrieve the second-stage payload. The second-stage instruction attempts to obfuscate its activity by retrieving a payload that appears to be an image file, but upon further inspection appears actually to be a portable executable. The C2 server replaces the first two bytes, which are normally 'MZ', with the characters 'DW', which may allow this C2 activity to evade rudimentary network security solutions and thus increase the success rate of retrieval. Once downloaded, the dropper will replace the initial two bytes prior to executing it. This second stage payload will once again perform process hollowing against a randomly selected Windows executable located in the system32 folder.
Information	<https://unit42.paloaltonetworks.com/tdrop2-attacks-suggest-dark-seoul-attackers-return/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:tdrop2>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool Tdrop2

Changed	Name	Country	Observed

APT groups

	Lazarus Group, Hidden Cobra, Labyrinth Chollima		2007-May 2025	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=88ec0db2-4836-4b8e-b9d9-e03118c2de08