Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 12:11:38 UTC

Tool: DanDrop

Names	DanDrop
Category	Malware
Type	Dropper
Description	(SecureWorks) The threat actors use this malicious macro to extract the DanBot payload from the weaponized document and then Base64-decode and install the malware using a scheduled task. The basic form and function of the macro have remained constant across analyzed samples, but the threat actors have made incremental improvements to obfuscate the macro and refactor some of the functionality.
Information	<https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool DanDrop

Changed	Name	Country	Observed	
APT groups				
	Hexane		2017-Jun 2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=580fa928-850c-4a8e-9b58-406a68f57e13