Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:56:06 UTC

Tool: DropBook

Names	DropBook
Category	Malware
Type	Backdoor, Info stealer, Exfiltration
Description	(Cybereason) The newly discovered DropBook backdoor used fake Facebook accounts or Simplenote for command and control (C2) operations, and both SharpStage and DropBook implement a Dropbox client in order to exfiltrate the data stolen from their targets to a cloud storage, as well as for storing their espionage tools. DropBook can download and execute an extended arsenal of payloads stored on Dropbox, such as: MoleNet Downloader, QuasarRAT, SharpStage Backdoor, an updated version of DropBook, and ProcessExplorer, a legitimate tool by Microsoft to monitor Windows processes, often used by attackers for reconnaissance and to dump credentials.
Information	<https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf>
MITRE ATT&CK	<https://attack.mitre.org/software/S0547/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.dropbook>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool DropBook

Changed	Name	Country	Observed	
APT groups				
	Molerats, Extreme Jackal, Gaza Cybergang	[Gaza]	2012-Jul 2023	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7ff05b70-6c5f-4aa1-b95e-1c29508fded7