Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:04:11 UTC

Tool: SharpStage

Names	SharpStage
Category	Malware
Type	Backdoor, Info stealer, Downloader
Description	(Cybereason) The dropper downloaded from the SharpStage C2 has several backdoor capabilities including implementation of a Dropbox client API along with a check for the presence of the Arabic language in order to execute only on desired targets and to evade sandbox detection, as the default language setting is usually English. Prior to the language check, the backdoor automatically captures the screen and saves the image in the %temp% folder.
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/S0546/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sharpstage>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool SharpStage

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

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