Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:35:06 UTC

Tool: MoleNet

Names	MoleNet
Category	Malware
Type	Backdoor, Downloader
Description	(Cybereason) Perhaps one of the most intriguing tools discovered in this campaign is the MoleNet downloader. Even though the tool itself is previously undocumented, the Nocturnus Team found evidence that it has been in active development since at least 2019 with infrastructure operating as far back as 2017 while remaining under the radar. The MoleNet downloader is just one of the tools in Molerats' arsenal, and was discovered in this campaign being delivered by the DropBook backdoor along with the SharpStage and Spark backdoors. It is also written in .NET, and heavily obfuscated.
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/S0553/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.molenet>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool MoleNet

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=9fba1892-f6ba-483d-92b0-a69bf4bfff96