

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:58:33 UTC

[Home](#) > [List all groups](#) > [List all tools](#) > List all groups using tool Mongall


Tool: Mongall

Names	Mongall
Category	Malware
Type	Backdoor
Description	(SentinelLabs) Mongall is a small backdoor going back to 2013, first described in a report by ESET. According to the report, the threat actor was trying to target the Telecommunications Department and the Vietnamese government. More recently, Aoqin Dragon has been reported targeting Southeast Asia with an upgraded Mongall encryption protocol and Themida packer.
Information	< https://www.sentinelone.com/labs/aoqin-dragon-newly-discovered-chinese-linked-apt-has-been-quietly-spying-on-organizations-for-10-years/ > < https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/wp-operation-quantum-entanglement.pdf >
MITRE ATT&CK	< https://attack.mitre.org/software/S1026/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.mongall >
AlienVault OTX	< https://otx.alienvault.com/browse/pulses?q=tag:Mongall >

Last change to this tool card: 30 December 2022

Download this tool card in [JSON](#) format

All groups using tool Mongall

Changed	Name	Country	Observed
APT groups			
	Aoqin Dragon		2013

	DragonOK		2015-Jan 2017	
	Moafee		2014	

3 groups listed (3 APT, 0 other, 0 unknown)

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=4d5089f2-9389-496e-a4cd-4e45af89f928>