

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:25:02 UTC

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

Tool: VenomKit

Names	VenomKit
Category	Malware
Type	Loader
Description	(Proofpoint) We use this name to describe documents generated by a builder purchased from the same seller as Taurus builder. Depending on the variant it may exploit CVE-2017-0199, CVE-2017-8570, CVE-2017-8759, CVE-2017-11882, CVE-2018-0802, and/or CVE-2018-8174. Notably, VenomKit often also uses the same CMSTP bypass as Taurus Loader .
Information	< https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers > < https://quointelligence.eu/2018/11/golden-chickens-uncovering-a-malware-as-a-service-maas-provider-and-two-new-threat-actors-using/ >

Last change to this tool card: 10 July 2020

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

All groups using tool VenomKit

Changed	Name	Country	Observed	
APT groups				
	Cobalt Group		2016-Oct 2019	
	Venom Spider, Golden Chickens		2017-Jan 2025	

2 groups listed (2 APT, 0 other, 0 unknown)

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=7ba478cd-6fa7-44ad-a08d-1fb2a8604185>