

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:06:16 UTC

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

Tool: VenomLNK

Names	VenomLNK
Category	Exploits
Type	Loader
Description	(QuoINT) We have observed a Windows Shortcut file dubbed as VenomLNK used in various campaigns involving different infection chains. We hypothesize this is a new variation of a previously highlighted malicious document kit builder known as VenomKit , a building-kit tool that threat actors use to craft malicious Rich Text File (RTF) documents that exploit multiple vulnerabilities. Successful exploitation of those vulnerabilities leads to the delivery of batch and scriptlet files on a system and execution to download the second stage payload from a Web resource.
Information	< https://quointelligence.eu/2020/01/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors/ > < https://medium.com/@quoscient/the-chicken-keeps-laying-new-eggs-uncovering-new-gc-maas-tools-used-by-top-tier-threat-actors-531d80a6b4e9 >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.venom_lnk >

Last change to this tool card: 24 April 2021

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

All groups using tool VenomLNK

Changed	Name	Country	Observed
APT groups			
	Venom Spider, Golden Chickens		2017-Jan 2025

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=9a5487b5-7aeb-4cfa-8756-3354a0130f02>