

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:13:59 UTC

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

Tool: BASICSTAR

Names	BASICSTAR
Category	Malware
Type	Backdoor
Description	(Volexity) The backdoor deployed by the RAR + LNK infection chain is a previously undocumented backdoor that Volexity track as BASICSTAR.
Information	< https://www.volexity.com/blog/2024/02/13/charmingcypress-innovating-persistence/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/vbs.basicstar >

Last change to this tool card: 27 December 2024

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

All groups using tool BASICSTAR

Changed	Name	Country	Observed	
APT groups				
	Magic Hound , APT 35 , Cobalt Illusion , Charming Kitten		2012-Jun 2025	

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=67cb560e-c250-4fef-ab80-05092651f4ad>