

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:12:41 UTC

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

Tool: Anchor

Names	Anchor Anchor_DNS
Category	Malware
Type	Backdoor
Description	(Cybereason) During our investigation, we found several unidentified malware samples related to TrickBot infections. The malware is dubbed Anchor by its authors and has been active since August 2018. Unlike Anchor_DNS, the Anchor malware does not implement communication over DNS. However, it does share many behavioral, code, and string similarities with Anchor_DNS and some similarities to TrickBot.
Information	< https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware > < https://www.bleepingcomputer.com/news/security/trickbots-new-linux-malware-covertly-infects-windows-devices/ > < https://thedfirreport.com/2021/03/08/bazar-drops-the-anchor >
MITRE ATT&CK	< https://attack.mitre.org/software/S0504/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.anchor >

Last change to this tool card: 30 December 2022

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

All groups using tool Anchor

Changed	Name	Country	Observed	
APT groups				
	FIN6, Skeleton Spider	[Unknown]	2015-Oct 2021	

	Wizard Spider, Gold Blackburn		2014-May 2025	
--	---	---	---------------	---

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6bbe4681-573c-417b-bb91-657aef026509>