

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:12:07 UTC

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


Tool: BROKEYOLK

Names	BROKEYOLK
Category	Malware
Type	Downloader
Description	(Mandiant) BROKEYOLK is a .NET downloader that downloads and executes a file from a hard-coded command and control (C2) server. The malware communicates via SOAP (Simple Object Access Protocol) requests using HTTP.
Information	< https://www.mandiant.com/media/17826 >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.brokeyolk >

Last change to this tool card: 22 June 2023

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

All groups using tool BROKEYOLK

Changed	Name	Country	Observed
APT groups			
	APT 42		2015-Feb 2024

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f762f9b2-84d9-4caf-b4e1-049673561c8b>