

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 15:15:10 UTC

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



Tool: KerrDown

Names	KerrDown
Category	Malware
Type	Downloader
Description	A downloader that ultimately downloads a Cobalt Strike beacon.
Information	< https://unit42.paloaltonetworks.com/tracking-oceanlotus-new-downloader-kerrdown/ > < https://blog.cystack.net/word-based-malware-attack/ >
MITRE ATT&CK	< https://attack.mitre.org/software/S0585/ >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.kerrdown >

Last change to this tool card: 30 December 2022

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

All groups using tool KerrDown

Changed	Name	Country	Observed	
APT groups				
	APT 32, OceanLotus, SeaLotus		2013-Aug 2024	

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=4c663e41-4e54-4182-8f71-b992cc7ab859>