

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 02:02:17 UTC

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

Tool: Ctealer

Names	Ctealer
Category	Malware
Type	Info stealer , Credential stealer
Description	(Group-IB) The threat actor also created two custom stealers, dubbed Cucky and Ctealer by Group-IB. When launched on the victims' device, the stealers are able to steal passwords, history, logins, and cookies from dozens of web browsers. In this campaign, the threat actors also wrote script that allowed them to transfer their malware to USB devices connected to the compromised machine, and also spread their malware across network shares.
Information	< https://www.group-ib.com/media-center/press-releases/dark-pink-apt/ >

Last change to this tool card: 15 February 2023

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

All groups using tool Ctealer

Changed	Name	Country	Observed
APT groups			
	Dark Pink	[Unknown]	2022-Feb 2023

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=e9a7ee71-bc81-4449-ad9a-cf0e280cf682>