

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-06 00:23:37 UTC

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

Tool: IconDown

Names	IconDown
Category	Malware
Type	Downloader
Description	IconDown downloads a file from a specific site, decrypts and saves the enclosed executable and runs it.
Information	< https://blogs.jpcert.or.jp/en/2019/11/icondown-downloader-used-by-blacktech.html >
Malpedia	< https://malpedia.caad.fkie.fraunhofer.de/details/win.icondown >

Last change to this tool card: 24 April 2021

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

All groups using tool IconDown

Changed	Name	Country	Observed
APT groups			
	BlackTech , Circuit Panda , Radio Panda		2010-Oct 2020

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=6a1af31d-f0bd-454c-bd77-2f9d513dda41>