

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 20:23:37 UTC

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


## Tool: hcdLoader

Names	hcdLoader
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a>
Description	( <a href="#">Anomali</a> ) The Wekby group has exhibited a preference to use a tool named HcdLoader which often persists as a Windows Service on externally facing servers for remote access.
Information	< <a href="https://www.anomali.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop">https://www.anomali.com/blog/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop</a> >
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S0071/">https://attack.mitre.org/software/S0071/</a> >

Last change to this tool card: 22 April 2020

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

### All groups using tool hcdLoader

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">APT 18, Dynamite Panda, Wekby</a>		2009-May 2016

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

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a16b2002-e66b-4202-b032-44a0d43acb65>