

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 16:26:52 UTC

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

## Tool: PGoShell

Names	PGoShell
Category	<a href="#">Malware</a>
Type	<a href="#">Backdoor</a> , <a href="#">Info stealer</a> , <a href="#">Downloader</a>
Description	( <a href="#">Knownsec 404</a> ) PGoShell is developed in the Go programming language, overall, it offers a rich set of functionalities, including remote shell capabilities, screen capture, and downloading and executing payloads. It was initially named for its primary feature of remote shell capability.
Information	< <a href="https://medium.com/@knownsec404team/the-patchwork-group-has-updated-its-arsenal-launching-attacks-for-the-first-time-using-brute-ratel-175741987d87">https://medium.com/@knownsec404team/the-patchwork-group-has-updated-its-arsenal-launching-attacks-for-the-first-time-using-brute-ratel-175741987d87</a> >

Last change to this tool card: 27 August 2024

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

### All groups using tool PGoShell

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">Patchwork</a> , <a href="#">Dropping Elephant</a>		2013-Jun 2025

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

---

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=762e6de4-062d-4298-b622-97efdf448c6e>