

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:05:59 UTC

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


Tool: SharPyShell

Names	SharPyShell
Category	Malware
Type	Backdoor , Downloader
Description	<p>(ClearSky) An obfuscated ASP.NET WebShell that executes commands received by an encrypted channel compiling them in memory at runtime and deploys a privilege escalation tool.</p> <p>This WebShell enables the attackers to download a 'JuicyPotato' file to the compromised machine so as to obtain extended privileges.</p>
Information	< https://www.clearskysec.com/wp-content/uploads/2021/01/Lebanese-Cedar-APT.pdf >

Last change to this tool card: 19 April 2021

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

All groups using tool SharPyShell

Changed	Name	Country	Observed
APT groups			
	Volatile Cedar		2012-Early 2020

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=ebf035b2-ad91-4908-99ee-4a29b7c40bd4>