

# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:53:53 UTC

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


## Tool: VBShower

Names	VBShower
Category	<a href="#">Malware</a>
Type	<a href="#">Loader</a>
Description	( <a href="#">Trend Micro</a> ) VBShower delivers Cloud Atlas' second-stage payload, a backdoor that uses WebDAV to communicate with a cloud storage service. More notably, VBShower also delivers a PowerShell-based implant named <a href="#">PowerShower</a> , which is the main payload in Cloud Atlas's previous routine.
Information	< <a href="https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/cloud-atlas-group-updates-infection-chain-with-polymorphic-malware-to-evade-detection">https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/cloud-atlas-group-updates-infection-chain-with-polymorphic-malware-to-evade-detection</a> >
MITRE ATT&CK	< <a href="https://attack.mitre.org/software/S0442/">https://attack.mitre.org/software/S0442/</a> >

Last change to this tool card: 30 December 2022

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

### All groups using tool VBShower

Changed	Name	Country	Observed
<b>APT groups</b>			
	<a href="#">Inception Framework, Cloud Atlas</a>		2012-2024

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