

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 10:49:28 UTC

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

Tool: VIRTUALPIE

Names	VIRTUALPIE
Category	Malware
Type	Backdoor
Description	(Mandiant) VIRTUALPIE is a lightweight backdoor written in Python that spawns a daemonized IPv6 listener on a hardcoded port on a VMware ESXi server. It supports arbitrary command line execution, file transfer capabilities, and reverse shell capabilities. Communications use a custom protocol and are encrypted using RC4.
Information	< https://cloud.google.com/blog/topics/threat-intelligence/esxi-hypervisors-malware-persistence >

Last change to this tool card: 26 August 2024

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

All groups using tool VIRTUALPIE

Changed	Name	Country	Observed
APT groups			
	UNC3886		2021-Early 2025

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

Source: <https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=77c1d60e-6b20-4576-be17-b163b7e2746c>