

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:44:26 UTC

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

↪ Tool: Serveo

Names	Serveo
Category	Malware
Type	Backdoor , Tunneling
Description	<p>(ClearSky) Serveo is a free tool for opening outside-facing servers and applications on a corporate network, whether on localhost or elsewhere. Unlike Ngrok, Serveo is an SSH-only server; also, any port that will be defined to it (safe for 22, 80, and 443 which are accessible from outside) will get another, unassigned TCP port instead. Using this service, the attacker was operating different services inside the network. Thus, for instance, the attacker had operated an RDP connection through the localhost on port 3389 (RDP); using Serveo, the attacker has opened this RDP for the outside world through port 12618 (TCP). The attacker has opened an SSH tunneling to another port in order to maintain an encrypted RDP on the attacked target.</p> <p>Moreover, like with the backdoor that had hardcoded and predefined credentials, here too the attacker separated every server that was opened to the outside world.</p>
Information	< https://www.clearskysec.com/wp-content/uploads/2020/02/ClearSky-Fox-Kitten-Campaign-v1.pdf >

Last change to this tool card: 20 April 2020

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

All groups using tool Serveo

Changed	Name	Country	Observed
APT groups			
	Parisite , Fox Kitten , Pioneer Kitten		2017-Nov 2020

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=6f8f3241-ca9b-4fab-9a7e-ed5321c8b9c>