Operation TunnelSnake - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:01:17 UTC

APT group: Operation TunnelSnake

Names	Operation TunnelSnake *(Kaspersky)*
Country	China
Motivation	Information theft and espionage
First seen	2018
Description	(Kaspersky) In this blog post we will focus on the following key findings that came up in our investigation: • A newly discovered rootkit that we dub 'Moriya' is used by an unknown actor to deploy passive backdoors on public facing servers, facilitating the creation of a covert C&C communication channel through which they can be silently controlled; • The rootkit was found on networks of regional diplomatic organizations in Asia and Africa, detected on several instances dating back to October 2019 and May 2020, where the infection persisted in the targeted networks for several months after each deployment of the malware; • We observed an additional victim in South Asia, where the threat actor deployed a broad toolset for lateral movement along with the rootkit, including a tool that was formerly used by APT1. Based on the detection timestamps of that toolset, we assess that the attacker had a foothold in the network from as early as 2018; • A couple of other tools that have significant code overlaps with Moriya were found as well. These contain a user mode version of the malware and another driver-based utility used to defeat AV software.
Observed	Countries: Asia and Africa.
Tools used	Moriya.
Information	<https://securelist.com/operation-tunnelsnake-and-moriya-rootkit/101831/>

Last change to this card: 27 June 2025

Download this actor card in PDF or JSON format