Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 14:43:47 UTC

Tool: Moriya

Names	Moriya
Category	Malware
Type	Rootkit, Backdoor
Description	(Kaspersky) Based on string artefacts within the malware's binaries, we named this rootkit Moriya. This tool is a passive backdoor which allows attackers to inspect all incoming traffic to the infected machine, filter out packets that are marked as designated for the malware and respond to them. This forms a covert channel over which attackers are able to issue shell commands and receive back their outputs.
Information	<https://securelist.com/operation-tunnelsnake-and-moriya-rootkit/101831/https://securelist.com/operation-tunnelsnake-and-moriya-rootkit/101831/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.moriya>

Last change to this tool card: 28 December 2021

Download this tool card in JSON format

All groups using tool Moriya

Changed	Name	Country	Observed	
APT groups				
	Earth Kurma		2020	
	Operation TunnelSnake		2018	

2 groups listed (2 APT, 0 other, 0 unknown)