Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 22:24:33 UTC

Tool: nmap

Names	nmap
Category	Tools
Type	Reconnaissance
Description	Nmap ('Network Mapper') is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command-line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).
Information	<https://nmap.org/>
AlienVault OTX	<https://otx.alienvault.com/browse/pulses?q=tag:nmap>

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

All groups using tool nmap

Changed	Name	Country	Observed
APT groups			

	CostaRicto	[Unknown]	2017	
	Energetic Bear, Dragonfly		2010-Mar 2022	
	FIN13	[Unknown]	2016	
	Mustang Panda, Bronze President		2012-Jun 2025	
	TA2101, Maze Team	[Unknown]	2019-Feb 2024	

5 groups listed (5 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=97c602ab-0882-4f2c-ac40-9dc43f2a69fc