

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 15:14:27 UTC

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


↪ Tool: Ninja

Names	Ninja
Category	Malware
Type	Reconnaissance , Backdoor , Loader , Tunneling
Description	(Kaspersky) Based on the code logic, it appears that Ninja is a collaborative tool allowing multiple operators to work on the same machine simultaneously. It provides a large set of commands, which allow the attackers to control remote systems, avoid detection and penetrate deep inside a targeted network. Some capabilities are similar to those provided in other notorious post-exploitation toolkits. For example, Ninja has a feature like Cobalt Strike pivot listeners, which can limit the number of direct connections from the targeted network to the remote C2 and control systems without internet access. It also provides the ability to control the HTTP indicators and camouflage malicious traffic in HTTP requests that appear legitimate by modifying HTTP header and URL paths. This feature provides functionality that reminds us of the Cobalt Strike Malleable C2 profile.
Information	< https://securelist.com/toddycat/106799/ >
MITRE ATT&CK	< https://attack.mitre.org/software/S1100 >

Last change to this tool card: 19 June 2024

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

All groups using tool Ninja

Changed	Name	Country	Observed
APT groups			
	ToddyCat		2020-2024

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

Source: <https://apt.eta.or.th/cgi-bin/listgroups.cgi?u=e92858ba-2397-47a2-8861-a72cecfbb672>