

Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:55:35 UTC

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


Tool: Samurai

Names	Samurai
Category	Malware
Type	Reconnaissance , Backdoor , Loader , Exfiltration , Tunneling
Description	<p>(Kaspersky) The final stage is a formerly unknown modular backdoor that we dubbed Samurai, due to a constant keyword used inside an important dictionary used by the malware to share data between its modules.</p> <p>The library was developed in C# and uses the .NET HTTPListener class to receive and handle HTTP POST requests, looking for specially crafted requests that carry encrypted C# source code issued by the attackers. These programs will be in turn compiled and executed during runtime.</p>
Information	< https://securelist.com/toddycat/106799/ >
MITRE ATT&CK	< https://attack.mitre.org/software/S1099 >

Last change to this tool card: 19 June 2024

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

All groups using tool Samurai

Changed	Name	Country	Observed
APT groups			
	ToddyCat		2020-2024

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

Source: <https://apt.eta.org.th/cgi-bin/listgroups.cgi?u=21f8ae06-a671-47b9-a2ff-158c7974f6c3>