Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 21:46:11 UTC

Tool: Spyder

Names	Spyder
Category	Malware
Type	Backdoor, Loader
Description	(Dr.Web) In December 2020, the Doctor Web virus laboratory was contacted by a telecommunications company based in Central Asia after its employees discovered suspicious files on their corporate network. During the examination, our analysts extracted and studied a malicious sample, which turned out to be one of the backdoors used by the hacker group known as Winnti.
Information	<https://news.drweb.com/show/?i=14154&lng=en> <https://www.recordedfuture.com/chinese-group-tag-22-targets-nepal-philippines-taiwan/> <https://hello.global.ntt/-/media/ntt/global/insights/white-papers/the-operations-of-winnti-group.pdf> <https://securitynews.sonicwall.com/xmlpost/chinas-winnti-spyder-module/> <https://www.cybereason.com/blog/operation-cuckoobees-a-winnti-malware-arsenal-deep-dive>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.spyder>
AlienVault OTX	<https://otx.alienvault.com/browse/global/pulses?q=tag:spyder>

Last change to this tool card: 19 July 2022

Download this tool card in JSON format

All groups using tool Spyder

Changed	Name	Country	Observed
APT groups			

	APT 41		2012-Jul 2025	
	RedHotel, TAG-22		2021-2022	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=a43f8b27-b8a0-4526-a67e-84b8842c752c