Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-02 11:11:58 UTC

Tool: SideTwist

Names	SideTwist
Category	Malware
Type	Backdoor, Downloader, Exfiltration
Description	(Check Point) The backdoor in this stage, is a variant we haven't seen before in previous APT34 operations, but provides functionality which is simple and similar to other C based backdoors utilized by the group: DNSpionage and TONEDEAF and TONEDEAF 2.0. The functionality of the backdoor includes download, upload and shell command execution.
Information	<https://research.checkpoint.com/2021/irans-apt34-returns-with-an-updated-arsenal/> <https://nsfocusglobal.com/apt34-unleashes-new-wave-of-phishing-attack-with-variant-of-sidetwist-trojan/> <https://www.trendmicro.com/en_fi/research/23/i/apt34-deploys-phishing-attack-with-new-malware.html>
MITRE ATT&CK	<https://attack.mitre.org/software/S0610/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.sidetwist>

Last change to this tool card: 13 October 2023

Download this tool card in JSON format

All groups using tool SideTwist

Changed	Name	Country	Observed
APT groups			

	OilRig, APT 34, Helix Kitten, Chrysene		2014-Sep 2024	

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

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=0bd63c8b-6c80-46dc-8af6-8dfe4072b37a