


SideWinder, Rattlesnake - Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 17:54:34 UTC

[Home](#) > [List all groups](#) > SideWinder, Rattlesnake

↔ APT group: SideWinder, Rattlesnake

Names	SideWinder (<i>Kaspersky</i>) Rattlesnake (<i>Tencent</i>) Razor Tiger (<i>CrowdStrike</i>) T-APT-04 (<i>Tencent</i>) APT-C-17 (<i>Qihoo 360</i>) Hardcore Nationalist (?) HN2 (?) APT-Q-39 (?) BabyElephant (?) GroupA21 (?) G0121 (<i>MITRE</i>)												
Country	 India												
Motivation	Information theft and espionage												
First seen	2012												
Description	(Kaspersky) An actor mainly targeting Pakistan military targets, active since at least 2012. We have low confidence that malware might be authored by an Indian company. To spread the malware, they use unique implementations to leverage exploits of known vulnerabilities (such as CVE-2017-11882) and later deploy a Powershell payload in the final stage												
Observed	Sectors: Defense , Government , Maritime and Shipbuilding . Countries: Afghanistan , Bangladesh , Bhutan , Cambodia , China , Djibouti , Egypt , Maldives , Myanmar , Nepal , Pakistan , Lanka , Turkey , UAE , Vietnam .												
Tools used	BroStealer , callCam , Capriccio RAT .												
Operations performed	<table border="1"> <tr> <td>Mar 2019</td> <td>First Active Attack Exploiting CVE-2019-2215 Found on Google Play, Linked to SideWinder APT <https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-on-google-play-linked-to-sidewinder-apt-group/></td> </tr> <tr> <td>Jun 2021</td> <td>Old Snake, New Skin: Analysis of SideWinder APT activity between June and November 2021 <https://www.group-ib.com/resources/research-hub/sidewinder-apt/></td> </tr> <tr> <td>Mar 2022</td> <td>SideWinder’s malicious document, which also exploit the Russia-Ukraine conflict, was uploaded to middle of March. <https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-cyber-espionage/></td> </tr> <tr> <td>May 2022</td> <td>Group-IB Threat Intelligence researchers have discovered a new malicious infrastructure and a cust the APT group SideWinder <https://blog.group-ib.com/sidewinder-antibot></td> </tr> <tr> <td>Nov 2022</td> <td>SideWinder Uses Server-side Polymorphism to Attack Pakistan Government Officials — and Is No Turkey <https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pak></td> </tr> <tr> <td>Oct 2023</td> <td>SideWinder Utilizes New Infrastructure to Target Ports and Maritime Facilities in the Mediterranean <https://blogs.blackberry.com/en/2024/07/sidewinder-targets-ports-and-maritime-facilities-in-the-m></td> </tr> </table>	Mar 2019	First Active Attack Exploiting CVE-2019-2215 Found on Google Play, Linked to SideWinder APT < https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-on-google-play-linked-to-sidewinder-apt-group/ >	Jun 2021	Old Snake, New Skin: Analysis of SideWinder APT activity between June and November 2021 < https://www.group-ib.com/resources/research-hub/sidewinder-apt/ >	Mar 2022	SideWinder’s malicious document, which also exploit the Russia-Ukraine conflict, was uploaded to middle of March. < https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-cyber-espionage/ >	May 2022	Group-IB Threat Intelligence researchers have discovered a new malicious infrastructure and a cust the APT group SideWinder < https://blog.group-ib.com/sidewinder-antibot >	Nov 2022	SideWinder Uses Server-side Polymorphism to Attack Pakistan Government Officials — and Is No Turkey < https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pak >	Oct 2023	SideWinder Utilizes New Infrastructure to Target Ports and Maritime Facilities in the Mediterranean < https://blogs.blackberry.com/en/2024/07/sidewinder-targets-ports-and-maritime-facilities-in-the-m >
Mar 2019	First Active Attack Exploiting CVE-2019-2215 Found on Google Play, Linked to SideWinder APT < https://blog.trendmicro.com/trendlabs-security-intelligence/first-active-attack-exploiting-cve-2019-on-google-play-linked-to-sidewinder-apt-group/ >												
Jun 2021	Old Snake, New Skin: Analysis of SideWinder APT activity between June and November 2021 < https://www.group-ib.com/resources/research-hub/sidewinder-apt/ >												
Mar 2022	SideWinder’s malicious document, which also exploit the Russia-Ukraine conflict, was uploaded to middle of March. < https://research.checkpoint.com/2022/state-sponsored-attack-groups-capitalise-on-russia-ukraine-cyber-espionage/ >												
May 2022	Group-IB Threat Intelligence researchers have discovered a new malicious infrastructure and a cust the APT group SideWinder < https://blog.group-ib.com/sidewinder-antibot >												
Nov 2022	SideWinder Uses Server-side Polymorphism to Attack Pakistan Government Officials — and Is No Turkey < https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pak >												
Oct 2023	SideWinder Utilizes New Infrastructure to Target Ports and Maritime Facilities in the Mediterranean < https://blogs.blackberry.com/en/2024/07/sidewinder-targets-ports-and-maritime-facilities-in-the-m >												

	sea >
2024	SideWinder targets the maritime and nuclear sectors with an updated toolset < https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/ >
Information	< https://securelist.com/apt-trends-report-q1-2018/85280/ > < https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/fireeye-sidewinder-targeted-attac < https://medium.com/@Sebdraven/apt-sidewinder-tricks-powershell-anti-forensics-and-execution-side-loading-5bc1 < https://s.tencent.com/research/report/479.html > < https://s.tencent.com/research/report/659.html > < https://cdn-cybersecurity.att.com/docs/global-perspective-of-the-sidewinder-apt.pdf > < https://thehackernews.com/2022/05/sidewinder-hackers-launched-over-1000.html > < https://www.neosecurendencias2021.com/assets/pdfs/crowdstrike/2021%20Global%20Threat%20Report%20FIN < https://www.group-ib.com/blog/hunting-sidewinder/ > < https://securelist.com/sidewinder-apt/114089/ >
MITRE ATT&CK	< https://attack.mitre.org/groups/G0121/ >

Last change to this card: 16 August 2025

Download this actor card in [PDF](#) or [JSON](#) format

Source: <https://apt.eta.or.th/cgi-bin/showcard.cgi?u=4e925967-099e-4708-9bca-ade4890d847b>