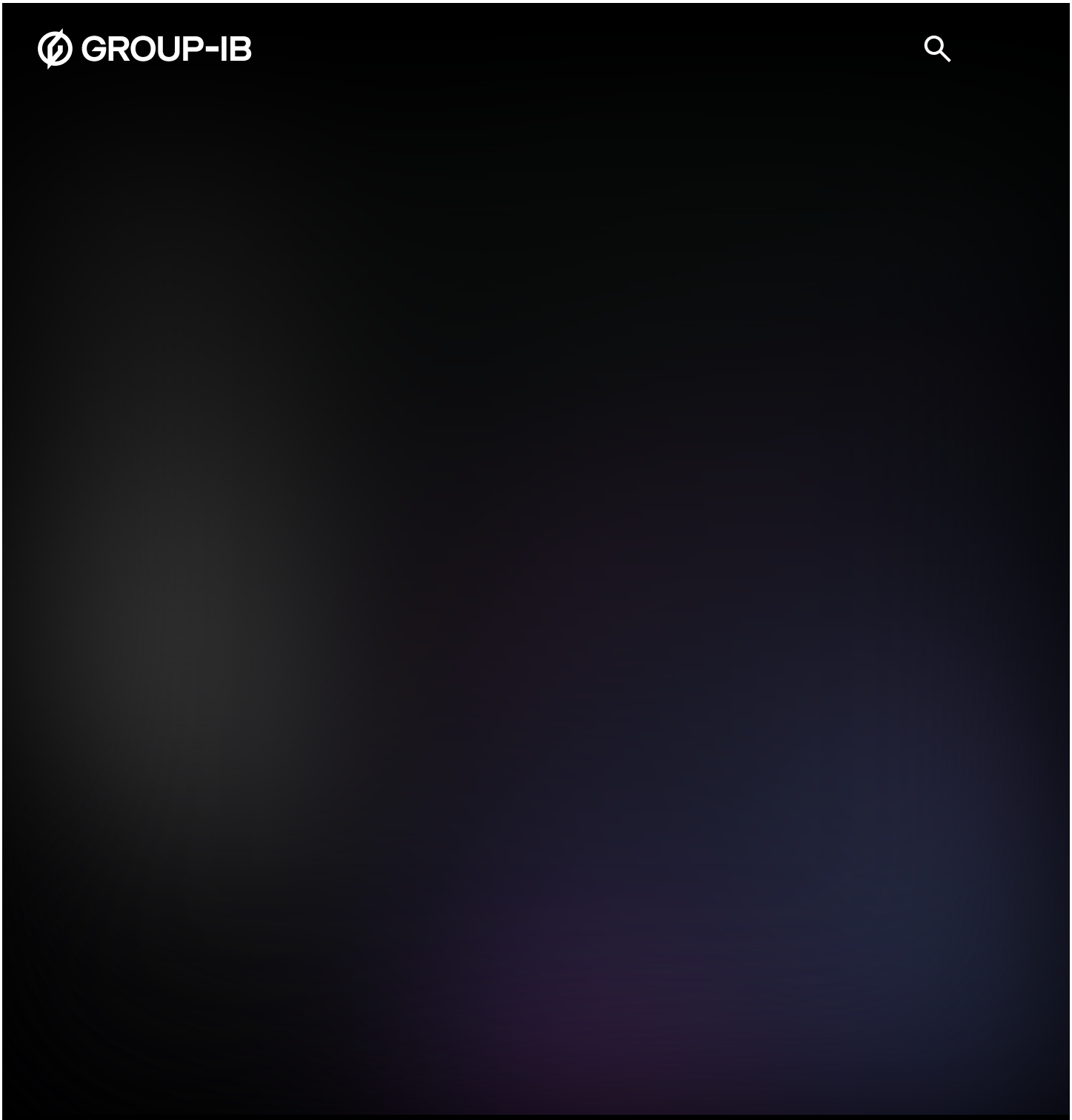
GROUP-IB



Old Snake, New Skin: Analysis of SideWinder

APT activity in 2021

Group-IB Threat Intelligence team uncovered a previously undocumented spear phishing campaign carried out by **APT SideWinder** between June and November 2021. The new threat report details how SideWinder, also known as Rattlesnake, Hardcore Nationalist (HN2), and T-APT4, attempted to target dozens of government organizations in the Asia-Pacific over a period of 6 months. Delve into the group's entire arsenal, network infrastructure, as well as its TTPs (Tactics, Techniques, and Procedures).

Download report

Key highlights from SideWinder's prolific 2021 campaign

61	identified targets in the government, military, financial, law enforcement, and political sectors
5 countries (Afghanistan, Bhutan, Myanmar, Nepal, Sri Lanka)	where SideWinder carried out its 2021 phishing campaign
Phishing mimicking cryptocurrency	indicates the group's growing interest in the crypto industry

BabyElephant and SideWinder	are most likely the same or closely related APTs
Successful 2020 attack on the Maldivian government	attributed to SideWinder by Group-IB
Telegram	has been used by SideWinder as a channel for receiving the results of the malware's commands

Background

The Group-IB Threat Intelligence team's monitoring of state-sponsored threat actors' activity revealed some tools belonging to **SideWinder** that had not been described in the public domain before. In addition to detailing the functionality and techniques employed in **SideWinder's new tools**, the report describes the phishing part of the group's 2021 operations based on backup archives obtained by Group-IB.

The archives contained several phishing projects designed to target government, military, and law agencies in **South and East Asia**, among which were fake websites imitating **the Central Bank of Myanmar** and more.

Despite its long history, **SideWinder** continues to be one of the most active state-sponsored hacker groups that pose a threat to governments in the **Asia-Pacific region**. The techniques and tools described in this report are currently used by the group and therefore relevant.

In This Report

Timeline

The Group-IB team was able to reconstruct an approximate timeline of SideWinder's phishing operations.

New tools

Group-IB malware analysts revealed some tools used by SideWinder that were previously unstated in the public domain.

YARA rules

The new report contains YARA rules for hunting the group and a table with the group's TTPs (Tactics, Techniques, and Procedures) mapped to the MITRE ATT&CK® matrix, providing all the information companies and organizations needed to update their security controls to detect SideWinder.

Advanced protection against cyber threats

Group-IB's security ecosystem provides comprehensive protection for your IT infrastructure based on our unique cyber intelligence and deep analysis of attacks and incident response.

Relevant reports

We see the full picture of the evolving cyber threat landscape thanks to unique tools for monitoring the infrastructure used by cybercriminals and data from battlefields:

Trend Report

Hi-Tech Crime Trends 2022/2023

Benefit from Group-IB's flagship cybersecurity report and explore the current threat landscape trend

Threat Intelligence
Fraud Protection
Managed XDR
Attack Surface Management
Digital Risk Protection
Business Email Protection
Cyber Fraud Intelligence Platform
Unified Risk Platform
Integrations

Research Hub
Success Stories
Knowledge Hub
Certificates
Webinars
Podcasts
TOP Investigations
Ransomware Notes

AI Cybersecurity Hub

Partners

Partner Program
MSSP and MDR Partner Program
Technology Partners
Partner Locator

Company

About Group-IB
Team
CERT-GIB
Careers
Internship
Academic Aliance
Sustainability
Media Center
Contact

Subscription plans

Services

Resource Center

Contact

APAC: +65 3159 3798
EU & NA: +31 20 226 90 90

Subscribe to stay up to date with the latest cyber threat trends

MEA: +971 4 568 1785

info@group-ib.com