OT-ISAC

OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

Public release note: This document is intended for situational awareness and defensive planning. It is not a claim of direct ICS compromise by SideWinder and should be interpreted alongside sector-specific telemetry, incident reporting, and vendor guidance.

Threat Actor Assessment

Classification	TLP:CLEAR
Date	6 April 2026
Prepared By	OT-ISAC with analytical support from Protos Labs
Actor / Cluster	SideWinder
Analytic Status	Operationally relevant baseline assessment

Table of Contents

I. Executive Summary

SideWinder remains a credible espionage threat to organisations in South Asia and the broader APAC region. Public reporting consistently links the actor to spearphishing, credential harvesting, ClickOnce abuse, modular .NET tooling, DLL side-loading, and short-lived delivery infrastructure targeting government, diplomatic, military, and maritime-linked entities.

For OT/ICS environments, the most credible risk is indirect rather than direct. Reviewed reporting does not confirm ICS-native malware, industrial protocol abuse, or direct manipulation of PLC or SCADA environments. The principal concern is compromise of identities and enterprise systems that support OT operations, including VPN, VDI, vendor access, jump hosts, and engineering-adjacent workstations.

II. Actor Snapshot

Field	Assessment
Aliases / tracking names	SideWinder; Razor Tiger; Rattlesnake; T-APT-04
Assessed affiliation	Unattributed; widely assessed as a likely state-aligned espionage actor based on sustained collection-focused targeting of government, diplomatic, military, and maritime entities.
Primary motivation	Espionage – credential theft, persistent access, and intelligence collection.
Primary targeting	South Asia; government, diplomatic, military, and maritime-linked organisations; transportation overlap; and OT-adjacent energy and manufacturing environments where remote access, shared IT services, or engineering-adjacent systems are exposed.
Regional relevance	High for APAC, particularly where maritime, port, logistics, government, or remote support dependencies are present.
Current status	Active and persistent
Risk rating	Moderate

III. Key Judgments

Attribution confidence	Medium. Multiple vendors align on SideWinder tradecraft and infrastructure patterns, but the reviewed material does not introduce decisive new attribution evidence.
Intent	Espionage and credential collection against politically and operationally valuable entities, with emphasis on South Asian government, diplomatic, military, maritime, and transport-linked targets.
Capability	High. The actor demonstrates mature phishing operations, ClickOnce delivery, credential harvesting, DLL side-loading, modular .NET tooling, and HTTPS-based communications.

Operational tempo	Steady and persistent. Reporting indicates repeated activity over time rather than a single isolated campaign.
OT/ICS Threat Level	Medium. The strongest risk is access to OT-adjacent enterprise systems and identities, not confirmed direct ICS intrusion.

IV. Targeting and OT/ICS Relevance

SideWinder's preferred victimology centres on government, diplomatic, military, and maritime-linked organisations. That profile matters to critical infrastructure defenders because the same environments often depend on shared enterprise services, remote vendor support, and engineering-adjacent systems that can create credible IT-to-OT exposure paths.

Area	Relevance	Why it Matters
Industrial operations	Medium	No direct industrial control compromise is documented, but compromise of engineering workstations, jump hosts, and shared support systems creates a realistic indirect risk to industrial operations.
Remote access and identity	High	Credential theft, phishing-resistant control bypass attempts, VPN/VDI exposure, and abuse of shared IT identities are central to SideWinder's most plausible IT-to-OT pathways.
Public-facing systems	High	Free-hosting credential portals, ClickOnce hosts, open directories, and DDNS-backed staging infrastructure show meaningful reliance on public-facing services and internet-reachable user workflows.

V. Observed Tradecraft

Category	Observed / assessed activity	Operational Notes
Initial Access	Spearphishing attachments, weaponized Word/RTF/PDF lures, and ClickOnce document-based delivery.	User-driven execution remains central to the actor's intrusion chain.
Execution / Persistence	ClickOnce installers, DLL side-loading, staged DLL runtime behaviour, and modular .NET loader or stealer components.	Observed tooling is consistent with mature, repeatable post-compromise access methods.
Credential / Discovery / Lateral	Credential harvesting through free-hosting portals and attacker-controlled collection endpoints.	Credential reuse against VPN, VDI, jump hosts, and engineering-adjacent systems is a realistic

Category	Observed / assessed activity	Operational Notes
Movement		follow-on risk.
Impact / Objectives	HTTPS or web-based communications, rapid infrastructure churn, and short-lived delivery domains.	Static blocklists alone are unlikely to remain effective for long.

VI. Why This Matters for Critical Infrastructure

- SideWinder's activity reinforces that phishing and identity compromise remain credible entry points into OT-adjacent environments even when no ICS-native tooling is observed.
- Maritime, logistics, transport, government, and port ecosystems are especially relevant because they combine operational sensitivity with extensive partner, contractor, and remote-support relationships.
- The actor's use of short-lived infrastructure and public-facing credential collection workflows favors behavior-led detection over heavy reliance on static indicators.
- For APAC defenders, the main concern is not immediate destructive impact, but the establishment of quiet access into environments that support operational continuity and decision-making.

VII. Defensive Considerations

Recommended Actions

Priority	Action	Reason
Immediate	Harden remote access with phishing-resistant MFA, device posture checks, conditional access, and just-in-time access for VPN, VDI, and vendor portals.	Reduces the likelihood that stolen credentials can be replayed into OT-supporting workflows.
Short-term	Restrict or closely monitor ClickOnce execution, mailbox attachment detonation outcomes, and unusual DLL loading from user-writable paths on engineering-adjacent endpoints.	Improves visibility into the actor's most consistent delivery and persistence mechanisms.
Strategic	Strengthen segmentation between enterprise and OT networks, broker access through monitored jump hosts, and reduce shared or over-privileged support accounts.	Constrains the most plausible IT-to-OT pivot pathways and improves forensic visibility.

VIII. References

- *Threat intelligence and vendor reporting reviewed in this assessment include Trellix Advanced Research Center, Hunt Intelligence, Arctic Wolf Labs, Bridewell, and Group-IB.*
- *Infrastructure analysis is derived from reported free-hosting domains, DDNS staging, credential portals, and resolving IP addresses documented in the underlying vendor research.*

- *Additional public reporting and OSINT were used only to supplement primary or specialist security research where appropriate.*
- *OT-ISAC analytic framing distinguishes between confirmed public reporting and analytic judgment about potential OT/ICS exposure pathways.*
- *No public reporting reviewed for this version confirms ICS-native malware, industrial protocol abuse, or direct manipulation of PLC or SCADA environments by SideWinder.*

Appendix A: MITRE ATT&CK Summary

Tactic	Technique / Sub-technique	Observed / Assessed Use
Initial Access	T1566.001 Spearphishing Attachment	Weaponized document delivery and lure-based phishing.
Execution	T1204.002 User Execution: Malicious File	User-driven activation of ClickOnce installers and related payloads.
Persistence / Defense Evasion	T1574.001 DLL Side-Loading	Side-loaded DLLs associated with modular .NET tooling.
Command and Control / Exfiltration	T1071.001 Web Protocols / T1041 Exfiltration Over C2 Channel	HTTPS-based communications and data movement in reviewed reporting.