SECURITY ADVISORY

CYBER STASH

April, 2025

CVE-2017-11882 & CVE-2025-2783

# SideWinder APT | Agile Retool and Evolving Tactics

## Context

SideWinder APT — also referred to as APT-C-17, Baby Elephant, Hardcore Nationalist, Leafperforator, Rattlesnake, Razor Tiger, or T-APT-04—has been operational since at least 2012 and continues to demonstrate a high degree of operational maturity, adaptability, and strategic intent. While historically focused on military and government entities in South Asia, SideWinder has significantly broadened its target profile over the past year. This expansion has seen aggressive campaigns against logistics firms, maritime infrastructure, diplomatic missions, and, more recently, nuclear energy organisations—spanning across South and Southeast Asia, the Middle East, and Africa

These campaigns have employed refined spear-phishing techniques, leveraged well-known but still effective vulnerabilities such as CVE-2017-11882, CVE-2025-2783, and deployed bespoke implants designed for stealth and persistence within critical environments.

The targeting of maritime and nuclear infrastructure—combined with post-compromise activity that includes tailored malware deployment and advanced evasion tactics—suggests an intelligence-driven campaign with strategic geopolitical objectives. The group's ability to retool within hours of detection, coupled with its use of complex infection chains and memory-resident payloads, reflects a threat actor that is not only technically sophisticated but also operationally agile.

## Mitigation

Defending against the SideWinder APT requires proactive measures:

**Restrict Unauthorized Software Installation:** Limit user permissions to prevent the installation of unapproved applications, enhancing security against potential threats.

**Block Access to High-Risk Infrastructure:** Proactively restrict access to known high-risk IP addresses, ASNs, and TLDs such as .info, .live, .pro,.site, .services, .email, and .tech, to mitigate exposure to malicious activities.

**Prioritize Browser Patching:** Prioritise regular browser patching to mitigate vulnerabilities and protect against cyberattacks targeting

## Technical Details

The Key tactics that differentiate SideWinder's updated campaign include:

**Rapid Malware Iteration in Response to Detection**

- **What makes it unique:** SideWinder consistently monitors the efficacy of its malware in real-time and responds to detection events by rapidly delivering updated variants—often within five hours.

- **Why it matters:** This fast development-response cycle demonstrates an advanced operational maturity and a dedicated internal capability for agile malware engineering, minimising the effectiveness of traditional static and signature-based detection.

**2. Deep Investment in Post-Exploitation Tooling**

- **What makes it unique:** SideWinder employs a proprietary post-exploitation toolkit—StealerBot—which operates in-memory, avoids disk writes, and is tightly coupled with a custom loader ("Backdoor Loader") that is adapted for each environment.

- **Why it matters:** The use of in-memory implants reduces forensic artefacts, complicates detection, and indicates a focus on long-term espionage and persistence in sensitive networks.

**3. Use of Signed and Legitimate Software for DLL Sideloading**

- **What makes** it unique: SideWinder sideloads malicious libraries by abusing signed, legitimate applications, making use of common DLLs like propsys.dll, winmm.dll, UxTheme.dll, etc.

- **Why it matters:** This shows a nuanced understanding of Windows trust models and enables stealthy execution without triggering standard AV or EDR flags.

**4. Fine-Tuned Anti-Analysis Capabilities**

- **What makes it unique:** SideWinder malware selectively terminates execution if it detects certain environments—such as sandboxes or specific AV products—by checking RAM size, loading uncommon libraries like nlssorting.dll, or matching 137 unique process names linked to security tools.

- **Why it matters:** This behaviour illustrates a deep focus on staying hidden, not just from tools but from the analysts behind them.

### 5. Targeted, Thematic Lures Reflecting Intelligence Priorities

- **What makes it unique:** The lure documents used in phishing campaigns are carefully themed around maritime infrastructure, nuclear energy, diplomatic affairs, and even generic themes when appropriate.
- **Why it matters:** These are not scattergun campaigns—they reflect target-specific reconnaissance and a focus on geopolitical intelligence collection.

### 6. Precision Deployment of Customised Implants

- **What makes it unique:** In several cases, malware samples were found hardcoded with user-specific paths, such as:

  C:\Users\[REDACTED]\AppData\Roaming\valgrind\[REDACTED FILE NAME]
- **Why it matters:** Indicates manual deployment and victim validation, likely used post-intrusion by operators with direct access, reflecting high-value targeting rather than mass exploitation.

### 7. Infrastructure Scale and Coordination

- **What makes it unique:** The group spun up large, dedicated infrastructure for malware delivery and C2, with diversified domains and hosting strategies.
- **Why it matters: Shows** a high level of operational funding, planning, and coordination—unusual for groups operating at such geographic breadth.

These tactics combined illustrate that SideWinder is not just persistent—it's strategic, adapting its playbook quickly in response to both detections and geopolitical contexts. Including these points in your context section will give CISOs the strategic clarity they need to prioritise visibility and resilience against such adversaries.

# Tactics, Techniques and Procedures

The following TTPs have been observed in relation to SideWinder APT campaign :

| Tactic | Technique | Description | MITRE ATT&CK ID |
|---|---|---|---|
| **Initial Access** | Spear Phishing Attachment | Delivers weaponised .LNK, .INF, and .DLL files via ZIP archives themed to victim interests | T1566.001 |
| **Execution** | DLL Sideloading | Abuses signed, legitimate applications to sideload malicious DLLs | T1574.002 |
| **Execution** | User Execution | Relies on user opening ZIP or launching shortcut file | T1204.002 |
| **Defense Evasion** | Obfuscated Files or Information | Uses malformed ZIPs and obfuscation of payloads to bypass scanning | T1027 |
| **Defense Evasion** | In-Memory Execution | Loads payloads like StealerBot entirely in memory, avoiding disk artefacts | T1055.012 |
| **Defense Evasion** | Virtualisation/Sandbox Evasion | Detects sandboxed or virtual environments based on RAM size, uncommon DLLs, or known analysis processes | T1497.001 |
| **Persistence** | DLL Search Order Hijacking | Drops malicious DLLs into trusted directories to hijack legitimate app loading paths | T1574.001 |
| **Command and Control** | Application Layer Protocol | Uses HTTP(S)-based C2 via custom or masqueraded domains | T1071.001 |
| **Command and Control** | Custom C2 Protocol | Employs a custom C2 protocol used by StealerBot to exfiltrate info and receive tasks | T1095 |
| **Discovery** | System Information Discovery | Collects host details such as usernames, OS version, RAM, running processes | T1082 |
| **Collection** | Clipboard Data | StealerBot accesses clipboard data to capture sensitive information | T1115 |
| **Collection** | Browser Credential Dumping | Captures stored passwords and cookies from browsers | T1555.003 |
| **Collection** | Screenshot Capture | Takes desktop screenshots for context gathering | T1113 |
| **Exfiltration** | Exfiltration Over C2 Channel | Sends collected data back over custom C2 or HTTP(S) channels | T1041 |
| **Exfiltration** | Automated Exfiltration | Periodically exfiltrates data without user interaction | T1020 |

# Exploited Vulnerabilities

This section outlines the key vulnerabilities actively exploited by the SideWinder APT group in their campaigns. These vulnerabilities, often targeted through various infection vectors, allow the attackers to gain unauthorized access, execute malicious payloads, and compromise systems. The vulnerabilities listed include those related to outdated software and unpatched systems, emphasizing the critical need for timely patching and proactive defense mechanisms. By understanding the specific CVEs leveraged by SideWinder, organizations can strengthen their security posture and reduce the risk of similar attacks.

| Vulnerability | CVE | Versions Impacted | Description | Exploitation |
|---|---|---|---|---|
| **Microsoft Equation Editor** | CVE-2017-11882 | Microsoft Office 2007, 2010, 2013, 2016, and 2019 (and Office 365) - All versions with Equation Editor enabled | Vulnerability in Microsoft Office's Equation Editor, allowing remote code execution through specially crafted documents. | Used in spear-phishing emails with malicious Office documents. |
| **Microsoft Office/ WordPad** | CVE-2017-0199 | Microsoft Office 2007, 2010, 2013, 2016, 2019 and WordPad in Windows 7, 8, 8.1, and 10 (without patch) | A vulnerability in Microsoft Office and WordPad allowing remote code execution via malicious documents. | Exploited in phishing campaigns with malicious Office documents. |
| **Windows CryptoAPI** | CVE-2020-0601 (CurveBall) | Windows 10 (versions 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004) and Windows Server 2016, 2019 | A flaw in Windows CryptoAPI that allows attackers to spoof the validity of cryptographic certificates. | Exploited to deliver malware that evades detection by bypassing certificate validation. |
| **Remote Desktop Services** | CVE-2019-0708 (BlueKeep) | Windows 7, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2016 (without patching) | A critical vulnerability in RDS that allows remote code execution without authentication. | Exploited in network-based attacks to propagate malware across vulnerable systems. |
| **VMware vCenter Server** | CVE-2021-21985 | VMware vCenter Server 6.7, 7.0 (prior to patch) | A remote code execution vulnerability in VMware vCenter Server's Virtual SAN plugin. | Exploited to gain access to sensitive systems within enterprise networks. |
| **Google Chrome (Mojo)** | CVE-2025-2783 | Versions prior to 134.0.6998.177<br>Update to version 134.0.6998.177 or later. | Sandbox escape vulnerability in Mojo component, allowing remote attackers to escape the sandbox on Windows. | Exploited in targeted attacks like APTs |

## Cyber Threat Intelligence

Understanding SideWinder's operations through the lens of geopolitics and regional dynamics reveals critical insights into the group's evolving motivations and target selection. This is not merely opportunistic cybercrime—it reflects calculated moves shaped by political interests, military priorities, and regional influence campaigns.

### Geopolitical Motivations

SideWinder's focus on South and Southeast Asia, the Middle East, and increasingly Africa aligns with regions marked by strategic tension and emerging power shifts. The group's sustained interest in military, diplomatic, and governmental entities—especially in Pakistan, Sri Lanka, and Nepal—strongly suggests a nation-state affiliation, potentially aimed at intelligence gathering, surveillance, and influence operations.

- **South Asia Tensions:** Long-standing political and territorial disputes, especially between India and Pakistan, make the targeting of defence and diplomatic assets in the region unsurprising.

- **Indian Ocean and Maritime Chokepoints:** The increasing interest in maritime and logistics infrastructure coincides with a broader strategic competition in the Indian Ocean Region (IOR), where port control and shipping routes are critical for trade, military presence, and economic influence.

- **Energy Security:** The targeting of nuclear energy institutions hints at attempts to monitor or potentially disrupt energy development in adversary nations—a tactic commonly aligned with strategic espionage and deterrence models.

### Strategic Assessment

SideWinder's operations reflect a long-term, state-aligned agenda aimed at intelligence collection, geopolitical influence, and regional dominance. Their evolving TTPs and broad targeting across government, defence, energy, and telecom sectors highlight a sophisticated understanding of regional dynamics. Notably, their activity suggests a willingness to exploit trusted relationships within supply chains—including MSPs, IT contractors, and procurement platforms—to bypass hardened perimeters and gain indirect access to high-value targets. This layered intrusion approach enables scalable credential theft, passive reconnaissance, and stealthy malware distribution.

## Yara Detection Rules

The following YARA rules are designed to detect specific indicators and tactics associated with the SideWinder APT campaign, including infection vectors, suspicious infrastructure, and tools used in the attack. These rules provide a proactive method for identifying and mitigating potential threats in your environment.

### Detect the Backdoor Loader

```
rule Detect_Backdoor_Loader {
  meta:
    description = "Detects Backdoor Loader associated with SideWinder APT"
    author = "CyberStash"
    last_modified = "2025-04-06"
  strings:
    $backdoor_loader1 = "propsys.dll"
    $backdoor_loader2 = "vsstrace.dll"
    $backdoor_loader3 = "JetCfg.dll"
    $backdoor_loader4 = "policymanager.dll"
    $backdoor_loader5 = "winmm.dll"
    $backdoor_loader6 = "xmllite.dll"
    $backdoor_loader7 = "dcntel.dll"
    $backdoor_loader8 = "UxTheme.dll"
  condition:
    any of ($backdoor_loader*) and filesize < 500KB
}
```

### Detect the Downloader Module

```
rule Detect_Downloader_Module {
  meta:
    description = "Detects Downloader Module used by SideWinder APT"
    author = "CyberStash"
    last_modified = "2025-04-06"
  strings:
    $dll1 = "app.dll"
    $dll2 = "WScript.Shell"
    $dll3 = "COMPLUS_Version"
    $dll4 = "base64-encoded .NET serialized stream"
  condition:
    any of ($dll*) and filesize < 200KB
}
```

## Detect the JavaScript Loader

```
rule Detect_JavaScript_Loader {
  meta:
    description = "Detects JavaScript loader in SideWinder campaign"
    author = "CyberStash"
    last_modified = "2025-04-06"
  strings:
    $js_loader = { "eval(\"var gShZVnyR = new ActiveXObject('WScript.Shell');gShZVnyR.Run('mshta.exe" "mshta.exe" "javascript:eval" "https://dgtk.depo-govpk" }
  condition:
    any of ($js_loader*) and filesize < 150KB
}
```

## Detect the RTF Exploit

```
rule Detect_RTF_Exploit {
  meta:
    description = "Detects RTF exploit used in SideWinder campaign"
    author = "CyberStash"
    last_modified = "2025-04-06"
  strings:
    $rtf_exploit1 = "CVE-2017-11882"
    $rtf_exploit2 = "mshta.exe"
    $rtf_exploit3 = "javascript:eval"
  condition:
    any of ($rtf_exploit*) and filesize < 100KB
}
```

## Detect APP.DLL Malware

```
rule Detect_App_DLL_Malware {
  meta:
    description = "Detects App.dll malware behavior"
    author = "CyberStash"
    last_modified = "2025-04-06"
  strings:
    $avast = "Avast"
    $avg = "AVG"
    $mshta = "mshta.exe"
    $pcalua = "pcalua.exe"
    $payload = "%TEMP%\\"
    $xor_key = { 00 00 00 00 00 00 00 00 }
  condition:
    any of ($avast, $avg) and ($mshta or $pcalua) and $payload and $xor_key
}
```

## Detect Infection Vectors (Spear-Phishing and RTF)

```
rule Detect_Infection_Vector {
  meta:
    description = "Detects infection vectors such as spear-phishing and RTF in SideWinder campaign"
    author = "CyberStash"
    last_modified = "2025-04-06"
  strings:
    $spear_phishing1 = "freelance video game developer"
    $spear_phishing2 = "renting a car in Bulgaria"
    $spear_phishing3 = "nuclear power plants"
    $spear_phishing4 = "maritime infrastructures"
    $spear_phishing5 = "CVE-2017-11882"
  condition:
    any of ($spear_phishing*) and filesize < 200KB
}
```

## Detecting SideWinder Infrastructure

```
rule Detect_SideWinder_Infrastructure {
  meta:
    description = "Detects suspicious infrastructure used by SideWinder APT"
    author = "CyberStash"
    last_modified = "2025-04-06"
  strings:
    $url1 = "nextgen.paknavy-govpk.net"
    $url2 = "premier.moittpk.org"
    $url3 = "cabinet-division-pk.fia-gov.com"
    $url4 = "navy-lk.direct888.net"
    $url5 = "srilanka-navy.lforvk.com"
    $url6 = "portdjibouti.pmd-office.org"
    $url7 = "portdedjibouti.shipping-policy.info"
    $url8 = "mofa-gov-sa.direct888.net"
    $url9 = "mod-gov-bd.direct888.net"
    $url10 = "mmcert-org-mm.donwloaded.com"
    $url11 = "opmcm-gov-np.fia-gov.net"
  condition:
    any of ($url*) and filesize < 150KB
}
```

## References

### IOCs:

- https://github.com/RedDrip7/APT_Digital_Weapon/blob/master/Sidewinder/Sidewinder_hash.md
- https://github.com/StrangerealIntel/CyberThreatIntel/blob/master/Indian/APT/SideWinder/25-12-19/analysis.md
- https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/

### Public Intelligence:

- https://securelist.com/sidewinder-apt/114089/
- https://thehackernews.com/2025/03/sidewinder-apt-targets-maritime-nuclear.html
- https://www.kaspersky.com/blog/forum-troll-apt-with-zero-day-vulnerability/53215/
- https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/
- https://circleid.com/posts/exploring-the-sidewinder-apt-groups-dns-footprint