ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR



SideWinder APT: Targeted Spear-Phishing Campaign Using Government Lookalike Domains and Remote Template Injection

TLP: CLEAR
Distribution: Public
Advisory on: SideWinder APT: Targeted Spear-Phishing Campaign Using Government Lookalike Domains and Remote Template Injection
Severity: High
Threat Category: Advanced Persistent Threat (APT) / Spear-Phishing / Malware
Target Countries: Bangladesh, Pakistan, Nepal, Sri Lanka and China
Target Sectors: Government, military and energy
Affected Platforms: Microsoft Windows / Microsoft Office
Primary Techniques: Spear-Phishing Attachment, Remote Template Injection, Malicious RTF Delivery and Government Domain Impersonation
Date: 23 November 2026

Executive Summary

BGD e-GOV CIRT has identified a targeted spear-phishing campaign attributed to the **SideWinder APT group**, involving the abuse of government-related lookalike domains and weaponised Microsoft Office documents to deliver malicious second-stage content.

The campaign has been observed between 02 November and 12 November 2026. Its targeting includes government and military-related organisations in South and East Asia, with infrastructure impersonating government entities in Bangladesh, Pakistan, Nepal, Sri Lanka and China.

The observed phishing documents impersonate government ministries and institutions, using themes such as pay-scale revisions, travel advisories and official training schedules. The documents are primarily delivered as Office Open XML (DOCX) files, including one document carrying a .zip extension despite internally being a DOCX file.

The infection chain relies on **remote template injection**, a technique that causes Microsoft Word to retrieve an externally hosted template when a weaponised document is opened. The external template reference is embedded within the document's relationship file:

`word/_rels/document.xml.rels`

Upon opening the document, Microsoft Word initiates HTTPS requests to attacker-controlled infrastructure to retrieve a second-stage file named `Fontlayer.rtf`. The observed network sequence includes WebDAV-style OPTIONS → HEAD → OPTIONS requests to a non-Microsoft domain.

The campaign uses two primary infrastructure domains:

- `donwloaad-file[.]org`
- `fetchdrives[.]info`

These domains host multiple government-themed lookalike subdomains. Notably, infrastructure includes hostnames impersonating **Bangladesh's Ministry of Foreign Affairs** and **Directorate of Secondary and Higher Education**.

The investigation identified two associated IP addresses:

- 89[.]46[.]237[.]186
- 168[.]222[.]243[.]49

An additional concern is the use of unique, per-recipient URL paths. Each delivered document contains a distinct URL token, allowing the threat actor to distinguish individual recipients and potentially track document access.

The recovered evidence confirms the infection chain through the retrieval of the second-stage RTF file. However, the subsequent payload execution, command-and-control beaconing and persistence mechanisms could not be independently established from the available behavioral evidence. Certain payload-drop artefacts were observed only in an external sandbox execution and remain unverified.

The presence of Bangladesh-related lookalike domains indicates that Bangladeshi government institutions are included in the infrastructure's impersonation scope. However, this does not independently confirm that the associated documents were delivered to, opened by, or successfully compromised any Bangladeshi organization.

BGD e-GOV CIRT recommends that government organizations and other potentially exposed entities immediately review email gateway logs, DNS queries, proxy traffic, Microsoft Office network activity and endpoint telemetry. Particular attention should be given to remote template retrieval, suspicious DOCX documents, malformed RTF files and communications involving the identified domains and IP addresses.

Threat Overview

BGD e-GOV CIRT

Threat Actor Profile

SideWinder is an advanced persistent threat actor associated with targeted cyber operations against government, military and other strategically significant organizations.

The current campaign demonstrates a continued focus on government-related targets through carefully prepared phishing documents and infrastructure designed to imitate legitimate government services.

The observed activity demonstrates the following characteristics:

- Targeted spear-phishing using government-related themes.
- Impersonation of government ministries and official institutions.
- Weaponized DOCX documents containing remote template references.
- Retrieval of second-stage content over HTTPS.
- Use of malformed RTF files as second-stage delivery artefacts.
- Per-recipient URL paths for individualized tracking.

- Use of lookalike government domains and subdomains.
- Language and system-environment checks that may support target filtering or sandbox evasion.
- Continued expansion of lookalike hostnames beneath existing parent domains.

Campaign Timeline

Date	Observed activity
02 November 2026	Earliest observed campaign submission
06 November 2026	Configuration and infrastructure activity reflected in the campaign artefacts
11 November 2026	Additional document and delivery activity
12 November 2026	Latest observed first-submission date in the analysed campaign window
13 November 2026	Later submissions from additional locations, indicating circulation of previously observed samples

The 12 November date represents the latest observation in the analyzed sample set, not a confirmed termination of the campaign. The associated infrastructure was reported to remain active, with new lookalike hostnames continuing to appear.

Targeted Countries and Sectors

The campaign infrastructure and observed document themes indicate targeting or impersonation involving the following countries:

Country	Observed targeting / impersonation
Bangladesh	Ministry of Foreign Affairs; Directorate of Secondary and Higher Education
Pakistan	Finance Ministry; Commerce Ministry; National Assembly
Nepal	Foreign Affairs Ministry; Home Affairs Ministry
Sri Lanka	Public Administration
China	National Energy Administration

The primary sectors associated with the activity are:

- Government and public administration.
- Military and defense-related organizations.
- Energy and critical infrastructure.

The presence of a government-themed hostname is evidence of impersonation infrastructure, not proof of successful phishing delivery or compromise of the corresponding institution.

Key Technical Findings

The following findings are significant from a defensive perspective:

- Five first-stage Office Open XML documents were identified, including one document with a misleading .zip extension.
- The documents contain remote template injection references.
- Microsoft Word retrieves a second-stage RTF file named `Fontlayer.rtf` over HTTPS.
- The second-stage RTF contains a non-standard header: Rich Text Format data, version 2, ANSI.

- The observed network sequence includes OPTIONS → HEAD → OPTIONS requests from Microsoft Word to a non-Microsoft host.
- The campaign uses two parent domains and two associated IP addresses.
- Fourteen government and organization lookalike hostnames were identified beneath the infrastructure.
- Bangladesh-related lookalike domains include `mofa-gov-bd.fetchdrives[.]info` and `dshe-gov-bd.fetchdrives[.]info`.
- The campaign uses per-recipient URL paths containing campaign identifiers, target identifiers and unique file tokens.

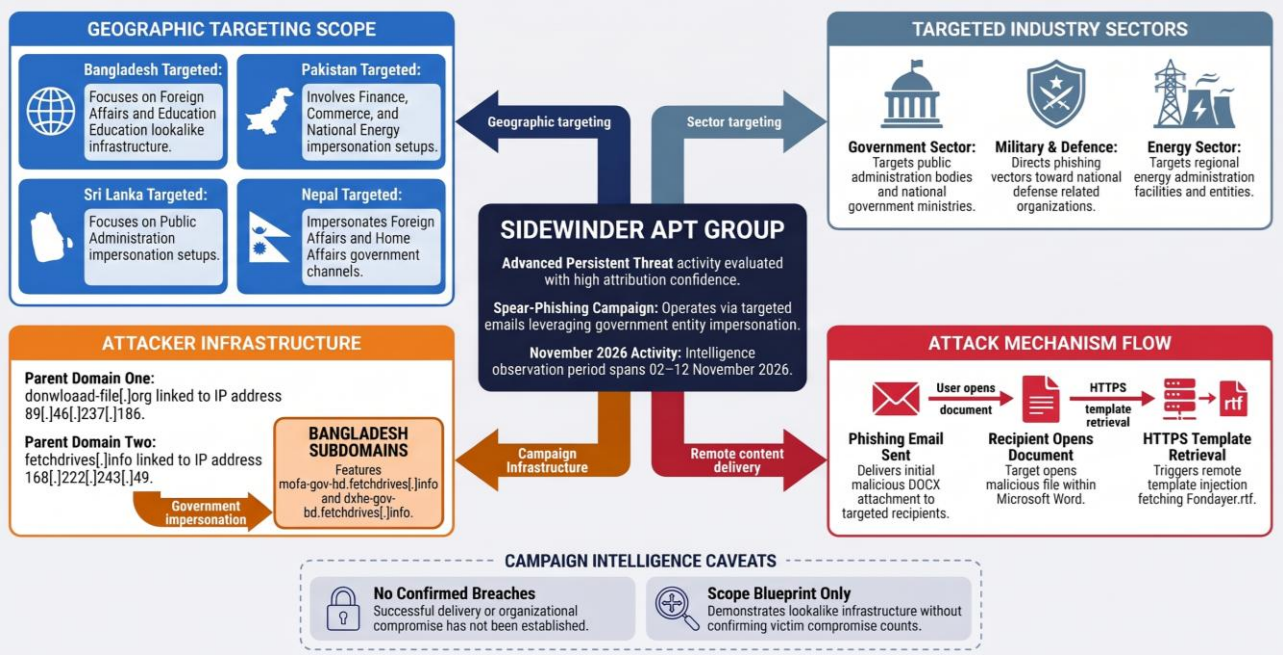

Figure: Overview of the SideWinder campaign, targeted sectors and government impersonation infrastructure

BGD e-GOV CIRT

Technical Analysis and Infection Chain

Initial Access – Spear-Phishing Delivery

The campaign begins with targeted spear-phishing emails carrying weaponized Microsoft Office documents as attachments. The documents use government-related subjects intended to appear relevant to the recipient's professional responsibilities.

Observed document themes include:

- Pay-scale revisions.
- Travel advisories.
- Official training schedules.
- Government administrative information.

The documents impersonate finance, commerce and foreign-affairs ministries, particularly those associated with Pakistan and Nepal.

Five first-stage documents were identified. All are Office Open XML documents (DOCX), including one file named: `Revision of Basic Pay Scales_2026[.]zip`

Despite its `.zip` extension, the file is internally a DOCX document.

This distinction is important for security monitoring because attachment filtering based solely on filename extensions may not correctly identify the underlying file format.

Remote Template Injection

The first-stage documents use remote template injection to retrieve an externally hosted template.

The technique is implemented through the document relationship file:

`word/_rels/document.xml.rels`

Within this file, an external `attachedTemplate` reference points to a remote resource hosted on attacker-controlled infrastructure. When the victim opens the document in Microsoft Word, the application attempts to retrieve the external template over HTTPS. The observed behavior does not require the user to enable macros. The remote template request is initiated through the document's template relationship.

This is particularly significant because organizations that rely exclusively on macro-blocking controls may not prevent this initial retrieval mechanism.

The campaign uses the following MITRE ATT&CK technique:

- **T1221 – Template Injection**

The remote template reference is associated with the exploitation mechanism commonly discussed in relation to CVE-2017-0199. However, the presence of remote template injection markers should not automatically be treated as proof that the vulnerability was successfully exploited on every affected endpoint.

Observed Network Communication Sequence

The analyzed documents generate a WebDAV-style request sequence when opened in Microsoft Word. The observed sequence is: OPTIONS → HEAD → OPTIONS

The requests are directed to a non-Microsoft host over HTTPS. An example of the observed request pattern is:

```
OPTIONS https://mofa-gov-np[.]donwloaad-
file[.]org/19328/1/38665/2/32/0/0/m/files-608fc3a9/

HEAD https://mofa-gov-np[.]donwloaad-
file[.]org/19328/1/38665/2/32/0/0/m/files-608fc3a9/Fontlayer.rtf
```

```
OPTIONS https://mofa-gov-np[.]donwloaad-
file[.]org/19328/1/38665/2/32/0/0/m/
The recovered RC4 key is: 88042CFF2F4810520D31E711973A5BFA
```

The sequence is an important detection opportunity because an external HTTPS request from Microsoft Word alone may not be sufficient to distinguish malicious activity from legitimate application behavior. The combination of the requesting process, HTTP methods, destination domain and URL structure provides a more specific detection pattern.

Some samples also contact the legitimate Microsoft Office template service:

```
templateservice[.]office[.]com
```

This may make the malicious template retrieval activity appear similar to ordinary Office template operations.

Host-Based Evidence of Remote Template Retrieval

During the observed execution, Microsoft Word also writes the remote URL to disk as a literal filesystem path.

An example is:

```
C:\Users\<USER>\Desktop\https:\mofa-gov-np[.]donwloaad-
file[.]org\19328\1\38665\2\32\0\0\m\files-608fc3a9\Fontlayer.rtf
```

This creates an additional host-based detection opportunity. Security teams should inspect unusual files or directory structures containing embedded URL components, especially those associated with Microsoft Word and suspicious external template references.

Second-Stage Payload – Fontlayer.rtf

The remote template retrieval leads to a second-stage file named: `Fontlayer.rtf`

The recovered second-stage RTF files contain a non-standard header:

```
Rich Text Format data, version 2, ANSI
```

A conventional RTF document normally begins with: `{\rtf1`

The observed version-2 header is therefore anomalous and represents a useful file-identification and threat-hunting characteristic. The malformed RTF structure may cause conventional file-type identification tools to classify the file incorrectly or fail to recognize it as a standard RTF document.

The recovered second-stage file has the following SHA-256 value:

```
d03dbcf51a154c26a2bd3f70c5eacd25cbf3caee7618aa35e497cfde9f95c341
```

The file is approximately 8,890 bytes in size.

Payload Drop – Evidence Limitation

Some sandbox observations reported the following file artefacts:

```
%TEMP%\StikyNote.exe

C:\Program Files (x86)\f60fd70d\jusched.exe
```

The first artefact was reported with a `Zone.Identifier / Mark-of-the-Web` alternate data stream. However, these payload-drop artefacts were observed only in an external sandbox execution and were absent from the behavioral evidence available for the analyzed samples. They could not be independently reproduced or confirmed.

Accordingly, these filenames should be treated as secondary hunting leads rather than confirmed indicators of successful payload deployment.

Command-and-Control and Persistence Visibility

The recovered evidence establishes the first-stage document delivery and second-stage RTF retrieval. However, the available behavioral evidence does not establish:

- Successful execution of a third-stage payload.
- The complete functionality of the final malware.
- Subsequent C2 beaconing.
- Persistence mechanisms.
- Lateral movement.
- Data collection or exfiltration.

These activities should not be presented as confirmed outcomes of the analyzed samples. The investigation therefore establishes a reproducible infection chain through stage two, while later execution stages remain unverified.

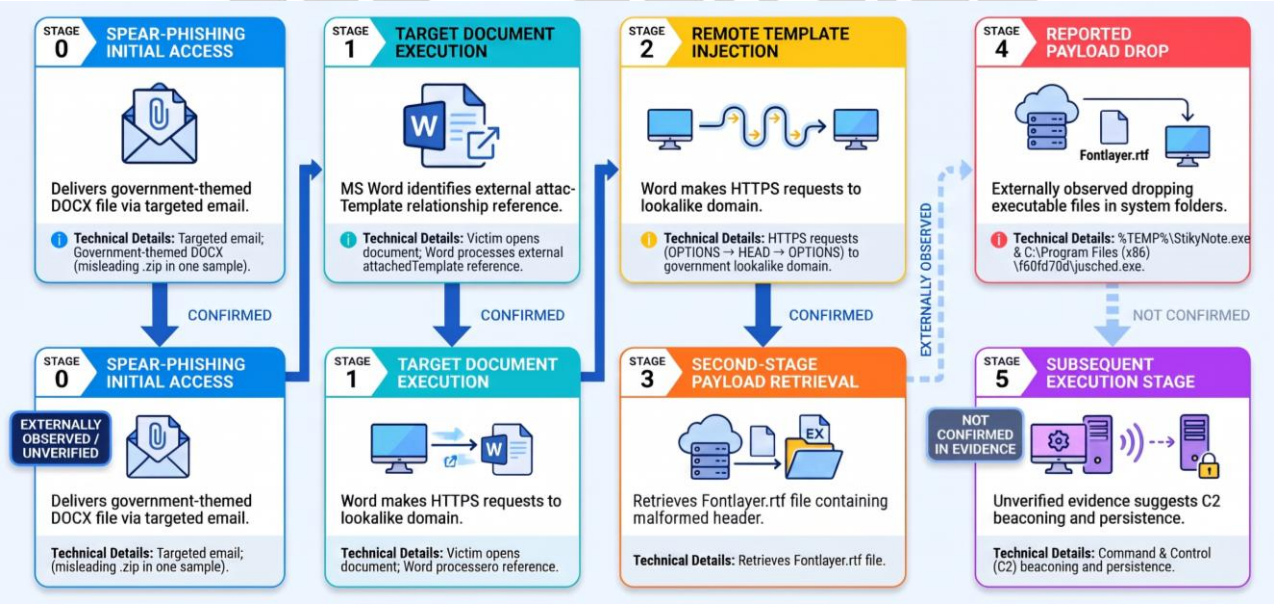

Figure 2: Observed SideWinder infection chain, distinguishing confirmed remote template retrieval from unverified subsequent execution

Infrastructure Analysis

Primary Infrastructure

The campaign operates through two parent domains, with new government-themed hostnames created beneath them.

The identified parent domains and associated IP addresses are:

Parent domain	Associated IP address
donwloaad-file[.]org	89[.]46[.]237[.]186
fetchdrives[.]info	168[.]222[.]243[.]49

The infrastructure is structured to support multiple impersonated organizations without requiring a completely separate domain registration for each target. This approach enables the operator to expand its targeting footprint through the creation of additional subdomains.

Government and Organization Lookalike Domains

The following lookalike hostnames were identified during infrastructure analysis.

No.	Lookalike hostname	Impersonated organisation / country
1	finance-gov-pk.donwloaad-file[.]org	Pakistan Finance
2	mofa-gov-np.donwloaad-file[.]org	Nepal Foreign Affairs
3	un-org.donwloaad-file[.]org	United Nations
4	commerce-gov-pk.fetchdrives[.]info	Pakistan Commerce
5	finance-gov-pk.fetchdrives[.]info	Pakistan Finance
6	www-finance-gov-pk.fetchdrives[.]info	Pakistan Finance
7	na-gov-pk.fetchdrives[.]info	Pakistan National Assembly
8	moha-gov-np.fetchdrives[.]info	Nepal Home Affairs
9	mofa-gov-bd.fetchdrives[.]info	Bangladesh Foreign Affairs
10	dshe-gov-bd.fetchdrives[.]info	Bangladesh Secondary and Higher Education
11	pubad-gov-lk.fetchdrives[.]info	Sri Lanka Public Administration
12	nea-gov-cn.fetchdrives[.]info	China National Energy Administration
13	www-nea-gov-cn.fetchdrives[.]info	China National Energy Administration
14	xn--wwwneagovcn-nf3fdd.fetchdrives[.]info	China National Energy Administration – IDN homoglyph

Bangladesh-specific observation:

Two identified hostnames imitate Bangladesh government institutions:

- mofa-gov-bd.fetchdrives[.]info
- dshe-gov-bd.fetchdrives[.]info

These hostnames are significant because they indicate that Bangladesh-related government identities have been incorporated into the campaign's lookalike infrastructure. However, their presence does not independently establish that a phishing document was delivered to either organization or that any system was compromised.

Additional Infrastructure Hostnames

The following additional hostnames were identified under the two parent domains:

- donwloaad-file[.]org
- fetchdrives[.]info
- secure.donwloaad-file[.]org
- zhanghaozhongxin.donwloaad-file[.]org
- 9t.fetchdrives[.]info
- pk.fetchdrives[.]info
- alertmanager.donwloaad-file[.]org
- console-dev.donwloaad-file[.]org
- db.donwloaad-file[.]org
- edge.donwloaad-file[.]org
- infra.donwloaad-file[.]org
- media.donwloaad-file[.]org
- my.donwloaad-file[.]org
- shop.donwloaad-file[.]org
- www.donwloaad-file[.]org
- www.fetchdrives[.]info

These hostnames should be considered in infrastructure monitoring and DNS threat hunting. Their inclusion in the observed domain set does not mean that each hostname was used directly for phishing delivery.

IP Address and Hosting Observations

The two associated IP addresses are:

IP address	Associated domain
89[.]46[.]237[.]186	donwloaad-file[.]org
168[.]222[.]243[.]49	fetchdrives[.]info

The infrastructure analysis indicates inconsistent geolocation and network attribution for these addresses across available datasets. The IP addresses also showed limited malicious reputation reporting during the observation period. This is operationally important because infrastructure with limited reputation signals may not be blocked automatically by reputation-based security controls.

Organizations should therefore correlate infrastructure indicators with URL paths, process behavior and DNS telemetry rather than depending exclusively on external reputation scores.

Per-Recipient URL Tracking

The campaign uses a structured URL format for retrieving the second-stage RTF file.

The observed URL pattern is:

```
/<5-digit campaign>/1/<5-digit target>/2/32/0/0/m/files-<8-hex>/Fontlayer.rtf
```

The observed campaign identifiers include:

- 19173
- 19328
- 19385
- 19412

The observed target identifiers include:

- 32731
- 38665
- 38669

Each delivered document contains a unique combination of campaign ID, target ID and file token. This allows the operator to distinguish individual document recipients and track requests associated with specific deliveries.

An example URL is:

```
hxxps://mofa-gov-np[.]donwloaad-file[.]org/19328/1/38665/2/32/0/0/m/files-608fc3a9/Fontlayer.rtf
```

Another observed URL is:

```
hxxps://commerce-gov-pk[.]fetchdrives[.]info/19173/1/32731/2/32/0/0/m/files-75be64e5/Fontlayer.rtf
```

The URL structure is a valuable detection opportunity because its format may remain useful even if the operator changes individual subdomains.

Internationalized Domain Name (IDN) Homoglyph

One of the identified hostnames uses an internationalized domain name (IDN) homoglyph technique:

```
xn--wwwneagovcn-nf3fdd.fetchdrives[.]info
```

The hostname decodes to a visually similar version of:

```
www-nea-gov-cn.fetchdrives[.]info
```

The difference involves the use of the Unicode U+2010 HYPHEN character instead of the standard ASCII hyphen U+002D. This technique can make a malicious hostname visually similar to a legitimate government-related hostname. Detection systems that rely exclusively on literal ASCII string matching may fail to identify such variations.

Organizations should implement IDN-aware domain monitoring and normalize internationalized domain names before comparing them with trusted government domain inventories.

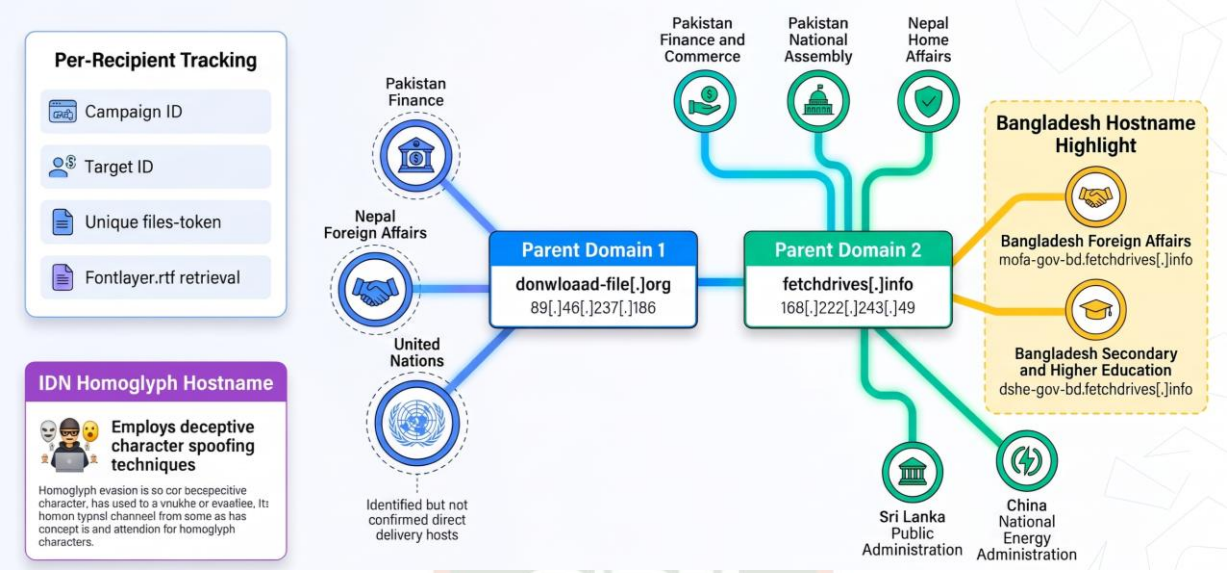

Figure: SideWinder's lookalike domain architecture and infrastructure associated with targeted government identities.

Bangladesh-Specific Threat Assessment

Government Impersonation Infrastructure

The campaign's infrastructure includes two hostnames imitating Bangladesh government institutions:

- `mofa-gov-bd.fetchdrives[.]info`
- `dshe-gov-bd.fetchdrives[.]info`

BGD e-GOV CIRT

These hostnames are particularly relevant to Bangladesh because they imitate the identities of:

- Ministry of Foreign Affairs.
- Directorate of Secondary and Higher Education.

The infrastructure demonstrates an attempt to extend the campaign's government impersonation footprint beyond Pakistan and Nepal. The identified hostnames should be treated as potentially malicious infrastructure and reviewed by relevant security teams.

Potential Exposure of Government Organizations

The observed techniques may create exposure for government organizations that:

- Exchange official documents through email.
- Use Microsoft Word for administrative and operational communications.

- Allow Office applications to retrieve external templates.
- Lack visibility into application-generated outbound HTTPS requests.
- Depend on file-extension-based email filtering.
- Do not inspect DOCX internal relationships or embedded external references.
- Have limited DNS and proxy monitoring capabilities.

The use of official-looking document themes may increase the likelihood of user interaction, particularly where recipients routinely receive government circulars, training schedules, travel advisories and administrative notices.

Potentially Exposed Sectors

Sector	Potential exposure
Government and public administration	Government impersonation and targeted administrative document lures
Military and defence	Targeted spear-phishing against sensitive government-related entities
Education	Impersonation of education-related government institutions
Energy	Lookalike infrastructure associated with national energy administration
Financial services	Potential exposure to government-related administrative phishing themes

Assessment of Bangladesh Impact

The available evidence confirms the existence of Bangladesh-related lookalike infrastructure. However, the evidence does not establish:

- Successful delivery of the observed phishing documents to Bangladeshi government employees.
- Confirmed opening of the malicious documents in Bangladesh.
- Successful execution of the second-stage content on Bangladeshi systems.
- Confirmed C2 communication from a Bangladeshi endpoint.
- Confirmed compromise of any specific Bangladeshi organization.

Accordingly, the Bangladesh-specific threat assessment is based on identified impersonation infrastructure and the potential exposure of organizations using the targeted technologies.



Figure: Bangladesh-related government impersonation infrastructure and potential organizational exposure

Attribution and Campaign Assessment

Attribution to SideWinder is assessed with high confidence based on multiple independent technical and behavioral observations contained in the analyzed report.

The attribution assessment is supported by:

- Consistent behavioral classification of the submitted documents as SideWinder activity.
- An independent malware-family signature identifying SideWinder.
- Behavioral analysis linking the malicious documents to the observed infrastructure.
- The use of remote template injection and malformed RTF second-stage files.
- Targeting themes associated with South and East Asian government ministries.
- Per-recipient URL tracking and the associated document delivery structure.
- A recurring document-author metadata value.

Document Metadata and Operator Fingerprint

The analyzed documents contain the document-author metadata value:

```
Jassi Kapur
```

This value appears across multiple documents spanning December 2023 to November 2026.

Its persistence across documents may provide a useful historical correlation pivot, particularly when combined with document hashes, creation metadata, remote template references and infrastructure indicators. However, document metadata should not be used as a standalone attribution mechanism because it can be modified or deliberately forged.

Operator Tradecraft and Evasion

The campaign demonstrates several operational characteristics:

- **Document reuse:** Similar document carriers are reused for multiple intended recipients, with recipient-specific URL paths.
- **Language and environment checks:** Behavioral indicators include language-checking and locale-related operations that may support target filtering or geofencing.
- **Execution timing:** A stealth-timeout behavior may indicate execution guardrails or time-based checks.
- **Sandbox evasion:** Long-sleep and debugger-detection behaviors were identified among the campaign's behavioral indicators.
- **Infrastructure rotation:** New lookalike hostnames are created beneath existing parent domains, allowing the operator to expand the campaign without relying exclusively on new parent-domain registrations.
- **IDN homoglyph:** Unicode character substitution may evade simple domain-string detection.

Attribution Limitations

The attribution assessment should be based on the combined technical evidence rather than any single document-author value, domain name or malware classification.

The observed campaign window is limited to the analyzed samples and submission dates. It does not establish the full operational duration of SideWinder activity.

Indicators of Compromise (IOCs)

The following indicators were identified in the analyzed campaign and are provided for threat hunting, detection and incident investigation.

Network Indicators – Parent Domains

Indicator type	Indicator
Domain	donwloaad-file[.]org
Domain	fetchdrives[.]info

Network Indicators – Lookalike Domains

- `finance-gov-pk.donwloaad-file[.]org`
- `mofa-gov-np.donwloaad-file[.]org`
- `un-org.donwloaad-file[.]org`
- `commerce-gov-pk.fetchdrives[.]info`
- `finance-gov-pk.fetchdrives[.]info`
- `www-finance-gov-pk.fetchdrives[.]info`
- `na-gov-pk.fetchdrives[.]info`
- `moha-gov-np.fetchdrives[.]info`
- `mofa-gov-bd.fetchdrives[.]info`

- dshe-gov-bd.fetchdrives[.]info
- pubad-gov-lk.fetchdrives[.]info
- nea-gov-cn.fetchdrives[.]info
- www-nea-gov-cn.fetchdrives[.]info
- xn--wwwneagovcn-nf3fdd.fetchdrives[.]info

Additional Infrastructure Domains

- secure.donwloaad-file[.]org
- zhanghaozhongxin.donwloaad-file[.]org
- 9t.fetchdrives[.]info
- pk.fetchdrives[.]info
- alertmanager.donwloaad-file[.]org
- console-dev.donwloaad-file[.]org
- db.donwloaad-file[.]org
- edge.donwloaad-file[.]org
- infra.donwloaad-file[.]org
- media.donwloaad-file[.]org
- my.donwloaad-file[.]org
- shop.donwloaad-file[.]org
- www.donwloaad-file[.]org
- www.fetchdrives[.]info

IP Address Indicators

- 89[.]46[.]237[.]186
- 168[.]222[.]243[.]49

BGD e-GOV CIRT

File Hashes – SHA-256

The following SHA-256 values were identified in the analyzed sample set:

- a0edd69d1fcc9b9da7b888418b2123dac12e790d0bf56943ae189f76fbcc358f
- f9c480160c7b3002df41b89d492c6554c90d4cb249b82c6fd5c7247f02ab3ca5
- b27827c243d1cef741e6fcb5a07b0f1999625b072c8ab5efb6a909311d5a70ca
- 09537d375644f048f78eb049b4d23387d5d08051c970cfd0e3f9004d7eb47f0c
- 07213fea47525bfdcd70b5355390c97761cee899929a885a55f8f060b59ffc12
- 6583e8de9112c3e04f4570881fc9530d92cde046ec348ab4f3aa1a03bf616e34

Note: Two additional SHA-256 values were identified as sandbox-generated re-saves of parent documents rather than independent delivered samples. These should be treated as analysis-generated derivatives, not independent campaign deliveries:

- 3f4dbbda772bc6c459c9bc195294bf974b47e158e1b581857495f28a1a0efc89
- 94eef14ab1454eadf4396d5b2835bbfd8ed1b135e31149acf1ac1c8e701811e1

Second-Stage File Indicator

Attribute	Value
Filename	Fontlayer.rtf
File type	RTF
Approximate size	8,890 bytes
SHA-256	d03dbcf51a154c26a2bd3f70c5eacd25cbf3caee7618aa35e497cfde9f95c341
Header	Rich Text Format data, version 2, ANSI

Observed URL Indicators

- hxxps://finance-gov-pk[.]donwloaad-file[.]org/19385/1/38669/2/32/0/0/m/files-c754903e/Fontlayer.rtf
- hxxps://commerce-gov-pk[.]fetchdrives[.]info/19173/1/32731/2/32/0/0/m/files-75be64e5/Fontlayer.rtf
- hxxps://finance-gov-pk[.]donwloaad-file[.]org/19412/1/38665/2/32/0/0/m/files-de2a98ce/Fontlayer.rtf
- hxxps://mofa-gov-np[.]donwloaad-file[.]org/19328/1/38665/2/32/0/0/m/files-608fc3a9/Fontlayer.rtf
- hxxps://finance-gov-pk[.]donwloaad-file[.]org/19412/1/38669/2/32/0/0/m/files-cedc0a31/Fontlayer.rtf
- hxxps://mofa-gov-np[.]donwloaad-file[.]org/19328/1/38669/2/32/0/0/m/files-0abaeb77/Fontlayer.rtf

Host-Based Indicators and Artefacts

Indicator	Description
Fontlayer.rtf	Second-stage RTF filename
word/_rels/document.xml.rels	Document relationship file containing external template reference
attachedTemplate	External template relationship
%TEMP%\StikyNote.exe	Reported in external sandbox only; not independently reproduced
C:\Program Files (x86)\f60fd70d\jusched.exe	Reported in external sandbox only; not independently reproduced
Jassi Kapur	Document-author metadata pivot

URL Pattern for Behavioral Detection

```
/<5-digit campaign>/1/<5-digit target>/2/32/0/0/m/files-<8-hex>/Fontlayer.rtf
```

This pattern is useful for identifying campaign-related second-stage retrieval attempts even when individual subdomains change.

IOC handling note: These indicators are associated with the analysed campaign. Their current operational status may change. Organisations should correlate matches with timestamps, endpoint activity and network evidence before determining compromise.

MITRE ATT&CK Mapping

The following table maps the observed campaign behaviors to relevant MITRE ATT&CK techniques. The mapping represents observed or associated techniques. It does not imply that all mapped techniques were successfully executed on a victim endpoint.

Tactic	Technique	ID	Observed behaviour
Initial Access	Spearphishing Attachment	T1566.001	Delivery of malicious DOCX attachments
Execution	User Execution: Malicious File	T1204.002	Victim opens weaponised Office document
Execution	Exploitation for Client Execution	T1203	Relevant to exploitation-oriented document delivery; successful exploitation is not established by the available evidence
Defence Evasion	Template Injection	T1221	Remote template retrieval through Office document relationship
Defence Evasion	Obfuscated Files or Information	T1027	Obfuscated document and payload characteristics
Defence Evasion	Masquerading	T1036	Misleading filename and government-related impersonation
Defence Evasion	Virtualization/Sandbox Evasion	T1497	Environment checks and long-sleep behaviour
Defence Evasion	Execution Guardrails	T1480	Language, locale and time-related execution checks
Discovery	System Information Discovery	T1082	System-environment checking
Discovery	System Location Discovery	T1614	Language and locale-related checks
Command and Control	Ingress Tool Transfer	T1105	Retrieval of second-stage content
Command and Control	Web Protocols	T1071.001	HTTPS-based remote template retrieval
Resource Development	Acquire Infrastructure: Domains	T1583.001	Use of government-themed lookalike domains

Detection and Threat Hunting

Email Gateway Detection

Email security teams should review:

- DOCX attachments containing misleading file extensions.
- Documents with government-related administrative themes received from external senders.
- Documents containing unexpected external template relationships.
- Attachments that contain little meaningful content but have suspicious metadata.
- Documents with unusual author metadata or very low editing duration.
- Files named as ZIP archives but identified internally as DOCX.

File identification should be based on actual file structure and content rather than extension alone.

Microsoft Office Remote Template Detection

Security teams should monitor Microsoft Word processes initiating outbound HTTPS connections to external or non-Microsoft domains. A particularly relevant behavioral sequence is:

```
WINWORD.EXE
     |
     +---- HTTPS OPTIONS
     |
     +---- HTTPS HEAD
     |
     +---- HTTPS OPTIONS
```

The following conditions should increase the detection priority:

- Request originates from `WINWORD.EXE`.
- Destination is an external non-Microsoft domain.
- Requests follow the OPTIONS → HEAD → OPTIONS sequence.
- URL path contains the campaign-specific structure.
- The destination domain resembles a government hostname.
- The activity is associated with a recently opened external DOCX attachment.

The request sequence should be correlated with the endpoint's file activity and the originating document.

DOCX Internal Structure Analysis

Security teams should inspect suspicious DOCX files as ZIP-based Office Open XML packages. The following file should receive particular attention:

```
word/_rels/document.xml.rels
```

Look for:

- External relationship references.

- `attachedTemplate` elements.
- Unexpected external HTTPS URLs.
- References to non-Microsoft domains.
- Suspicious or unusual template paths.

A suspicious external template reference should be treated as an investigation lead, even if the document contains no macros.

RTF File Detection

Monitor for files named: `Fontlayer.rtf`

Inspect the file header for: `Rich Text Format data, version 2, ANSI`

The presence of this non-standard header should trigger further investigation, particularly when the file was retrieved by Microsoft Word from an external domain.

DNS and Proxy Detection

Monitor DNS queries and proxy logs for:

- `donwloaad-file[.]org`
- `fetchdrives[.]info`
- Associated government-themed subdomains.
- The two identified IP addresses.
- Unusual external template retrievals from Microsoft Office processes.
- URL paths matching the observed per-recipient tracking structure.

DNS monitoring should include wildcard and subdomain coverage rather than only matching the two parent domains.

IDN and Homoglyph Detection

Security systems should normalize and inspect internationalized domain names.

The identified homoglyph hostname: `xn--wwwneagovcn-nf3fdd.fetchdrives[.]info`

may visually resemble: `www-nea-gov-cn.fetchdrives[.]info`

Detection systems should inspect the Unicode representation and its decoded punycode form.

Document Metadata Hunting

The following document-author metadata value was identified:

`Jassi Kapur`

It can be used as an additional historical hunting pivot across Office documents. However, metadata alone should not be considered sufficient evidence of malicious activity.

Recommended SIEM Correlation Logic

The following pseudocode describes a correlation approach for SOC and SIEM teams:

```
IF
    process_name = "WINWORD.EXE"
AND
    destination_domain is_external = TRUE
AND
    destination_domain NOT IN approved_microsoft_domains
AND
    HTTP_METHOD_SEQUENCE = "OPTIONS, HEAD, OPTIONS"
THEN
    GENERATE ALERT:
    "Potential SideWinder Remote Template Injection"
```

A higher-confidence correlation should include:

```
IF
    WINWORD.EXE initiates external HTTPS connection
AND
    destination matches known SideWinder infrastructure
OR
    URL_PATH matches:
    /<5-digit>/1/<5-digit>/2/32/0/0/m/files-<8-hex>/Fontlayer.rtf
THEN
    GENERATE HIGH-PRIORITY ALERT:
    "SideWinder Campaign Indicator Match"
```

The SIEM implementation should normalize domains, process names and URL paths before applying these conditions.

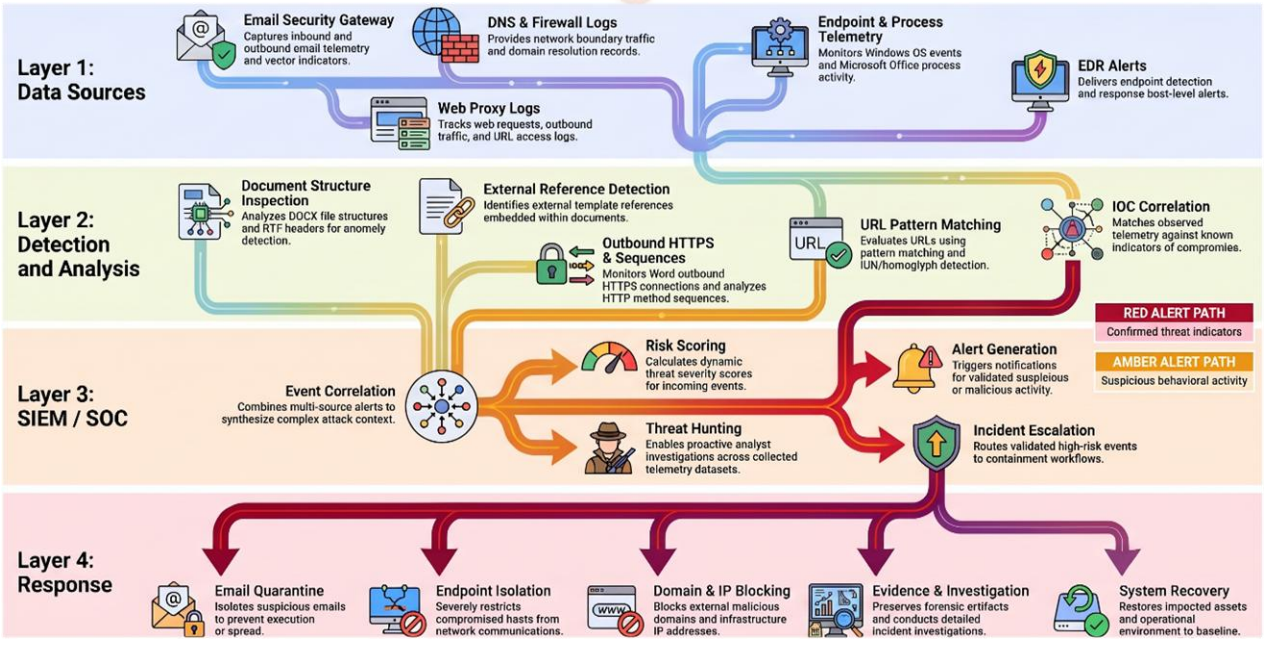

Figure: Recommended SOC detection architecture for identifying SideWinder remote template injection activity.

Incident Response and Investigation

If a suspicious document or associated network activity is identified, organizations should follow the incident response procedures below.

Initial Investigation

- Identify the original email and sender.
- Preserve the suspicious attachment in its original form.
- Record the attachment's SHA-256 hash.
- Identify the actual file format, regardless of its extension.
- Inspect the DOCX internal relationship file.
- Extract and record any external template URL.
- Review DNS, firewall and proxy logs for associated requests.
- Identify the endpoint and user associated with the document.

Endpoint Investigation

Review the affected endpoint for:

- Microsoft Word process activity.
- Outbound HTTPS connections initiated by `WINWORD.EXE`.
- Files named `Fontlayer.rtf`.
- Unusual URL-like filesystem paths.
- Suspicious files created under the user's profile or temporary directories.
- Additional process execution following document opening.
- Unexpected registry, scheduled task or persistence activity.

The reported payload filenames should be treated as secondary leads because they were not independently reproduced in the analyzed evidence.

Network Investigation

Review:

- DNS queries to the identified parent domains and subdomains.
- Connections to `89[.]46[.]237[.]186`.
- Connections to `168[.]222[.]243[.]49`.
- HTTPS requests containing the observed URL structure.
- Web proxy records for the OPTIONS → HEAD → OPTIONS sequence.
- Any additional destinations contacted by the same endpoint.

Containment and Recovery

If malicious activity is confirmed:

- Isolate the affected endpoint from the network.
- Preserve the original phishing email and attachment.
- Collect endpoint, DNS, proxy and firewall logs.
- Block confirmed malicious domains and IP addresses through organizational controls.
- Identify other recipients of the same email or document.
- Review related endpoints for the same document hashes and URL patterns.

- Determine whether any subsequent payload execution occurred.
- Review account activity and privileged access for suspicious behavior.
- Reset affected credentials where compromise or credential exposure is established.
- Rebuild or restore compromised endpoints from trusted sources when required.
- Submit incident findings to BGD e-GOV CIRT through the appropriate official reporting channel.

Recommendations

BGD e-GOV CIRT recommends that government organizations, CII entities and other potentially exposed organizations implement the following controls.

Email Security

- Strengthen email gateway filtering for suspicious Office attachments.
- Validate actual file formats rather than relying exclusively on filename extensions.
- Apply additional scrutiny to DOCX files received from external sources.
- Use sandbox analysis for suspicious documents.
- Quarantine documents containing unexpected external template references.
- Block or restrict suspicious attachment types according to organizational policy.

Microsoft Office Security

- Restrict unnecessary external template retrieval.
- Apply current Microsoft Office security updates.
- Use appropriate Attack Surface Reduction rules and application-control policies.
- Monitor Microsoft Word processes initiating external network connections.
- Review Office trust settings and external content controls.
- Restrict execution of untrusted files from user-writable directories.

DNS and Network Security

- Add the identified domains and IP addresses to appropriate monitoring and blocking controls after validation.
- Implement DNS monitoring for newly observed government-themed lookalike domains.
- Monitor subdomains of the identified parent domains.
- Use IDN normalization and homoglyph detection.
- Review proxy logs for unusual HTTP methods initiated by Microsoft Office applications.
- Retain DNS, firewall and proxy logs for sufficient periods to support incident investigation.

Endpoint Security

- Ensure EDR and antivirus solutions are updated and operational.
- Monitor suspicious child-process activity associated with Microsoft Office.
- Enable endpoint telemetry for file creation and process execution.
- Investigate unexpected files with misleading extensions.
- Implement application allowlisting where operationally feasible.
- Preserve endpoint evidence before remediation.

User Awareness

- Warn users about unexpected government circulars, travel advisories, training schedules and pay-scale documents received by email.
- Advise users not to open unexpected attachments solely because they appear to originate from government institutions.
- Encourage users to verify sensitive documents through official communication channels.
- Conduct targeted phishing-awareness exercises for government personnel.

Bangladesh-Specific Actions

Relevant government organizations should:

- Review DNS and proxy logs for the Bangladesh-related lookalike hostnames.
- Notify internal security teams responsible for the Ministry of Foreign Affairs and education-related institutional systems.
- Monitor for documents containing remote template references to suspicious external domains.
- Review email gateway records for the campaign's observed document themes.
- Share relevant indicators with internal SOC, NOC and incident response teams.
- Report suspected incidents to BGD e-GOV CIRT.

The SideWinder campaign demonstrates a targeted phishing operation that abuses government identities, malicious Office documents and remote template injection to retrieve second-stage content. The use of government-themed lookalike domains, per-recipient URL tracking and malformed RTF files indicates a deliberate approach to targeting and monitoring intended recipients.

The identification of Bangladesh-related infrastructure impersonating the Ministry of Foreign Affairs and the Directorate of Secondary and Higher Education makes this activity particularly relevant to Bangladeshi government organizations. Although the available evidence does not confirm successful compromise of any specific Bangladeshi institution, the identified infrastructure and delivery techniques warrant proactive investigation.

Organizations should priorities monitoring of Microsoft Word outbound HTTPS activity, remote template injection, suspicious DOCX relationships, malformed RTF files and lookalike government domains.

BGD e-GOV CIRT will continue to monitor the associated threat activity and encourages all relevant organizations to strengthen their defensive controls and report suspected incidents through the appropriate channels.

References

- MITRE ATT&CK – Phishing: Spearphishing Attachment (T1566.001)
- MITRE ATT&CK – Template Injection (T1221)
- MITRE ATT&CK – User Execution: Malicious File (T1204.002)
- MITRE ATT&CK – Ingress Tool Transfer (T1105)
- MITRE ATT&CK – Web Protocols (T1071.001)
- MITRE ATT&CK – Obfuscated Files or Information (T1027)
- MITRE ATT&CK – System Location Discovery (T1614)
- CVE-2017-0199 – Microsoft Office Remote Code Execution Vulnerability.
- CVE-2017-0199 – National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2017-0199
- Group-IB - SideWinder: A Lookalike Estate Reaching Beyond South Asia

BGD e-GOV CIRT