ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

SideWinder Spear-Phishing Campaign Against Bangladesh Leveraging Dual-Format Weaponized Documents

TLP: CLEAR
Distribution: Public
Advisory on: SideWinder Spear-Phishing Campaign Against Bangladesh Leveraging Dual-Format Weaponized Documents
Severity: High
Threat Type: Spear-Phishing, Malicious Document (Maldoc) Delivery, Domain Impersonation/Typosquatting, N-Day Exploitation (CVE-2017-0199), Command-and-Control
Affected Sectors: Bangladesh government ministries, defense entities, financial regulators, diplomatic missions, and national CERT/CIRT stakeholders
Date: 30 July 2026

Executive Summary

SideWinder, a persistent advanced persistent threat (APT) group with suspected India-nexus affiliations, is conducting an active spear-phishing campaign targeting government organizations across South Asia, with Bangladesh identified as one of its primary targets. Between **21 April and 28 July 2026**, the threat actor established an extensive typosquatting infrastructure consisting of **11 parent domains** and **more than 60 impersonation subdomains** designed to mimic government entities across Bangladesh, Sri Lanka, Nepal, and Pakistan. Additional lure infrastructure has also been observed impersonating organizations associated with China, the United Arab Emirates, United States embassies, and the United Nations (UNOCHA).

For Bangladesh, the campaign has been confirmed to impersonate at least **nine government** entities, including the Ministry of Foreign Affairs (MoFA), Ministry of Defence (MoD), Ministry of Home Affairs (MoHA), Directorate of Secondary and Higher Education (DSHE), Ministry of Civil Aviation and Tourism, Cabinet Division, Bangladesh Navy, and the Embassy of Bangladesh in Ankara, in addition to a punycode (IDN homograph) variant of the official MoFA domain. This activity builds upon previously documented SideWinder operations targeting several high-profile Bangladeshi organizations, including the Bangladesh Telecommunication Regulatory Commission (BTRC), Directorate of Inter-Services Public Relations (ISPR), Ministry of Finance, Directorate General of Defence Purchase (DGDP), Directorate General of Forces Intelligence (DGFI), Bangladesh Air Force, Bangladesh Police, and the national government webmail portal (mail.gov.bd). The observed activity demonstrates a sustained and evolving espionage campaign against Bangladesh's government, defence, and diplomatic sectors.

The current campaign employs **weaponized Microsoft Word (DOCX)** and **PDF documents** as active malware delivery and victim-tracking mechanisms. Notably, the attackers continue to exploit the **Microsoft Office Remote Template Injection vulnerability (CVE-2017-0199),** highlighting the continued effectiveness of unpatched legacy vulnerabilities in targeted attacks. This advisory provides an assessment of the threat, outlines the associated tactics, techniques, and procedures (TTPs), presents Bangladesh-related indicators of compromise (IOCs), and recommends mitigation measures to reduce the risk of compromise.

Assessment: The likelihood of continued targeting of Bangladeshi government, defence, and diplomatic organizations by SideWinder is assessed as High. The confirmed impersonation of

multiple government institutions, combined with the group's established history of credential theft and malware deployment against Bangladeshi entities, indicates an ongoing and persistent cyber espionage campaign requiring heightened vigilance and immediate defensive measures.

Threat Actor Profile: SideWinder

Attribute	Detail
Also known as	Rattlesnake, APT-C-17, T-APT-04
Suspected origin/nexus	India (suspected), assessed high confidence
Active since	At least 2012 (Group-IB, Kaspersky, BlackBerry historical reporting)
Regional focus	Pakistan, Bangladesh, Sri Lanka, Nepal, Myanmar, Afghanistan, China, and other South/South-East Asian states
Sector focus	Government ministries, military/defense, diplomatic missions, financial regulators, maritime and nuclear-adjacent infrastructure
Signature techniques	Typosquat government-domain infrastructure, OLE remote template injection, exploitation of legacy CVEs (CVE-2017-0199, CVE-2017-11882), geofenced/server-side polymorphic payload delivery, StealerBot credential-theft implant, DLL sideloading
Attribution confidence (this campaign)	High — based on infrastructure pattern reuse, PDF metadata/hash overlap with tracked SideWinder samples, direct sandbox family classification of Kit 2 payloads as “Sidewinder,” and consistent use of documented SideWinder techniques (template injection + CVE-2017-0199)

SideWinder’s historical cadence shows sustained operational tempo without long dormancy periods, and its infrastructure-registration behavior (batches of domains registered within tight multi-day windows, shared dynamic DNS providers) is a recurring fingerprint also seen in this campaign.

Campaign Overview

- **Window**: 21 April 2026 – 28 July 2026, and ongoing at time of writing.
- **Confirmed compromised/targeted countries**: Bangladesh, Sri Lanka, Nepal, Pakistan.
- **Lure-only / staged / adjacent infrastructure**: China (bait theme only), UAE (staged, not yet tied to confirmed compromise), UN/UNOCHA and other international-organization impersonation.
- **Infrastructure scale**: 11 confirmed parent domains, expanding to 60+ typosquat government/institution subdomains, following the consistent `convention <agency>-gov-<cc>.<parent-domain>`.
- **Two concurrent delivery kits** operate within the same infrastructure and target set.
- **Dual-format active tracking**: Both weaponized DOCX and weaponized PDF lures independently trigger file-type-matched C2 paths (`/office-compatibility-suite for DOCX`, `/adobe-reader for PDF`), meaning either file type alone is sufficient to

compromise and fingerprint a victim — recipients should not treat PDF versions of a lure document as inherently safer than DOCX versions, or vice versa.

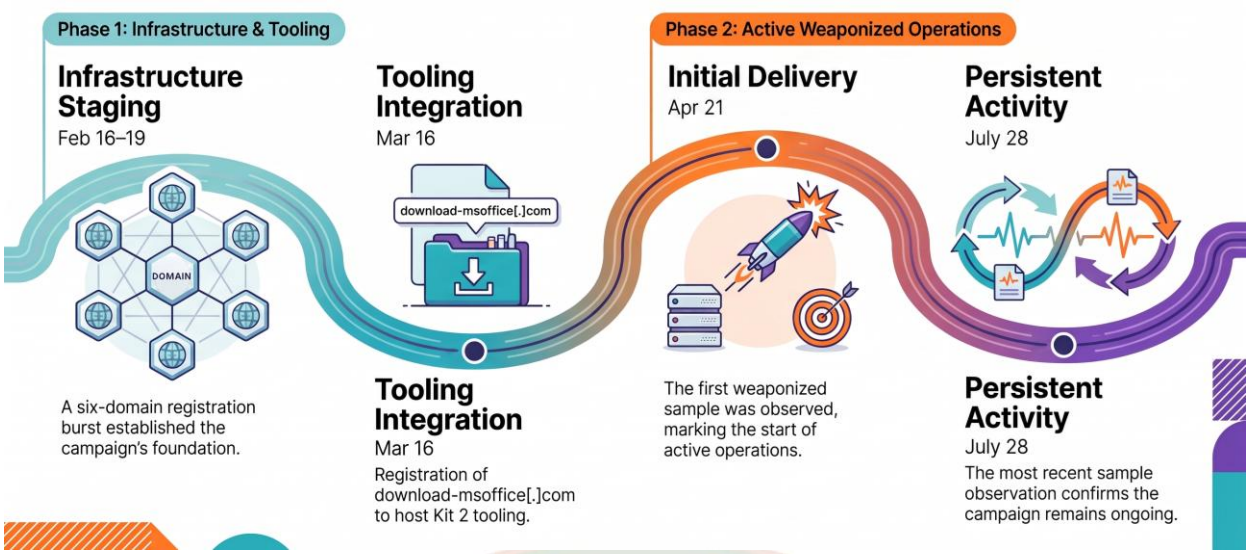

Figure: Campaign Timeline

Bangladesh-Specific Targeting Analysis

Confirmed Bangladesh impersonation identities (current campaign)

Impersonated entity	Subdomain pattern	Notes
Ministry of Foreign Affairs	**mofa-gov-bd**	Also spoofed via IDN/punycode homograph (see below)
Ministry of Defence	**mod-gov-bd**	
Directorate of Secondary and Higher Education	**dshe-gov-bd**	Education-sector targeting — broadens victim pool beyond core security ministries
Ministry of Home Affairs	**moha-gov-bd**, **moha-portal-gov-bd**	Two variants suggest testing of naming conventions or targeting different sub-units
Ministry of Civil Aviation and Tourism	**mocat-gov-bd**	
Bangladesh Navy	**bdnavy**	Hosted on **download-msoffice[.]com**, associated with the Kit 2 CVE-2017-0199 cluster
Cabinet Division	**cabinet-gov-bd**	Central administrative authority — high-value if compromised
Bangladesh Embassy, Ankara	**ankara-mofa-gov-bd**	Diplomatic-mission-specific targeting, indicating operators are mapping overseas mission structure, not just capital-based ministries

MoFA (IDN/punycode homograph)	**xn--mofagovbd-t89dd**	A homograph attack rendering visually as a legitimate-looking MoFA domain in browsers/email clients that don't flag punycode

Prior corroborating targeting (2024–2025 SideWinder activity against Bangladesh)

Independent of the current campaign, public reporting over the prior year documents sustained SideWinder interest in Bangladesh:

- Ministry of Defence, Bangladesh Telecommunication Regulatory Commission (BTRC), Directorate of Inter-Services Public Relations (ISPR), and Ministry of Finance were referenced in lure content and phishing infrastructure tied to the domain `army-govbd[.]info`, alongside confirmed targeting in Sri Lanka and Pakistan.
- A separate credential-harvesting infrastructure cluster impersonated the Directorate General of Defence Purchase (DGDP), Directorate General of Forces Intelligence (DGFI), Bangladesh Air Force (BAF), Bangladesh Ordnance Factories (BOF), the national webmail portal (mail.gov.bd), and Bangladesh Police, funneling stolen credentials to centralized backend collection domains (`mailbox3-inbox1-bd[.]com`, `mailbox-inbox-bd[.]com`) hosted on a Frankfurt-based VPS.
- Earlier 2025 telemetry (Hunt.io "Operation SouthNet") also identified supporting SideWinder activity touching Bangladesh alongside Pakistan, Sri Lanka, Nepal, and Myanmar, using free-hosting platforms (**Netlify, Pages.dev**) for credential-harvesting portals.

Assessment: The current campaign is not a one-off — it is the latest iteration of at least 12–18 months of continuous, evolving SideWinder targeting of Bangladeshi government, defense, and law-enforcement institutions, with the actor progressively expanding both its impersonated-entity list (now including Cabinet Division, an overseas mission, and an education directorate) and its technical tooling (moving between credential-harvesting portals, CVE-2017-0199/CVE-2017-11882 exploitation, and now dual-format OLE template injection).

Technical Attack Chain

Two delivery kits operate concurrently against the same infrastructure and target set, including Bangladesh.

Kit 1 — OLE Remote Template Injection (DOCX and PDF)

```
Weaponized .docx (VHash ba8a8dcf308b74616714221e0d3b3a1e)
  -> OLE relationship (word/_rels/document.xml.rels) references
external template with TargetMode="External"
```

```
  ->          https://<agency>-gov-<cc>.<typosquat-domain>/office-
compatibility-suite

Weaponized .pdf (VHash 9bdaee3d3d16a209244ef6d74b2e5ebb4)
  -> https://<agency>-gov-<cc>.<typosquat-domain>/adobe-reader
  -> ALL samples additionally beacon to e7[.]knd[.]vg for victim
fingerprinting
```

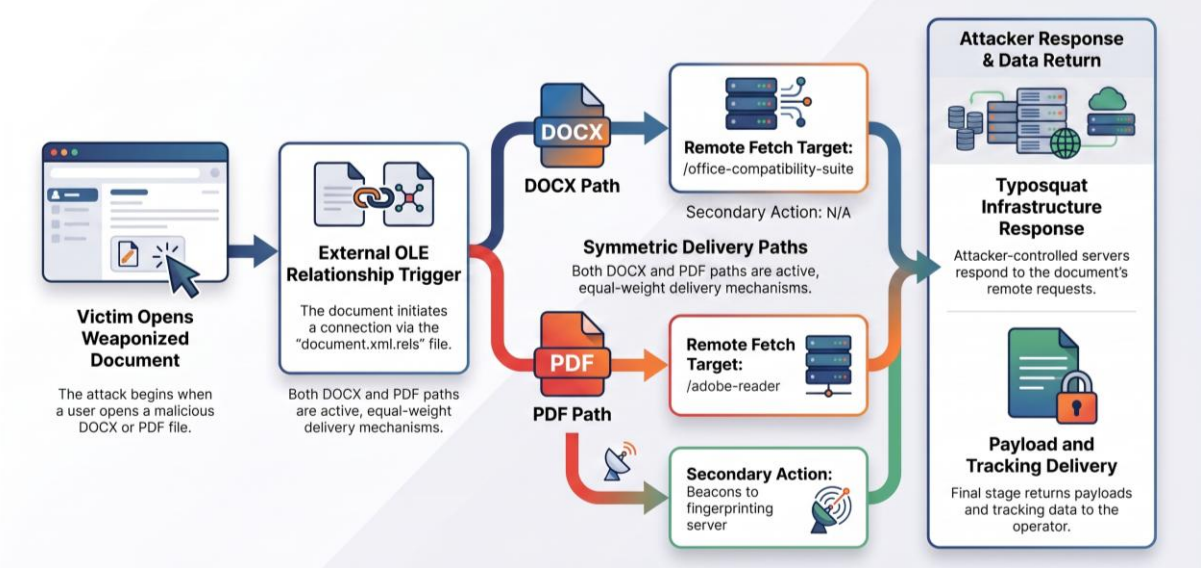

Figure: Kit 1 Attack Chain (OLE Remote Template Injection)

Both file types independently function as active delivery and tracking vectors — opening either a Bangladesh-themed DOCX or PDF bearing these VHashes will trigger outbound contact to attacker infrastructure without requiring further user interaction beyond opening the file, provided legacy "automatically update linked data"/remote-content behaviors are not disabled at the endpoint.

Kit 2 — CVE-2017-0199 OLE2Link Exploitation

```
Weaponized .docx (tag: cve-2017-0199, calls-wmi)
  -> OLE2Link exploit (CVE-2017-0199, patched by Microsoft in April
2017)
  ->    attacker    infrastructure:    download-msoffice[.]com    /
vagued[.]live / mail-svr[.]co / direct880[.]net / filenest[.]live
  -> sandbox family classification: "Sidewinder"
```

The Bangladesh Navy (bdnavy) impersonation subdomain is hosted on download-msoffice[.]com, which is part of this Kit 2 cluster — meaning Bangladesh Navy-themed lures in this campaign may be delivered via the still-effective 2017 exploit chain rather than (or in addition to) the newer template-injection method. Prior Acronis TRU reporting confirms SideWinder chains CVE-2017-0199 with CVE-2017-11882 (Equation Editor memory corruption) to deliver multistage shellcode loaders culminating in the StealerBot credential-

harvesting implant — endpoints still running unpatched Office 2007–2016 installations, common in many government environments, remain fully exploitable by this technique.

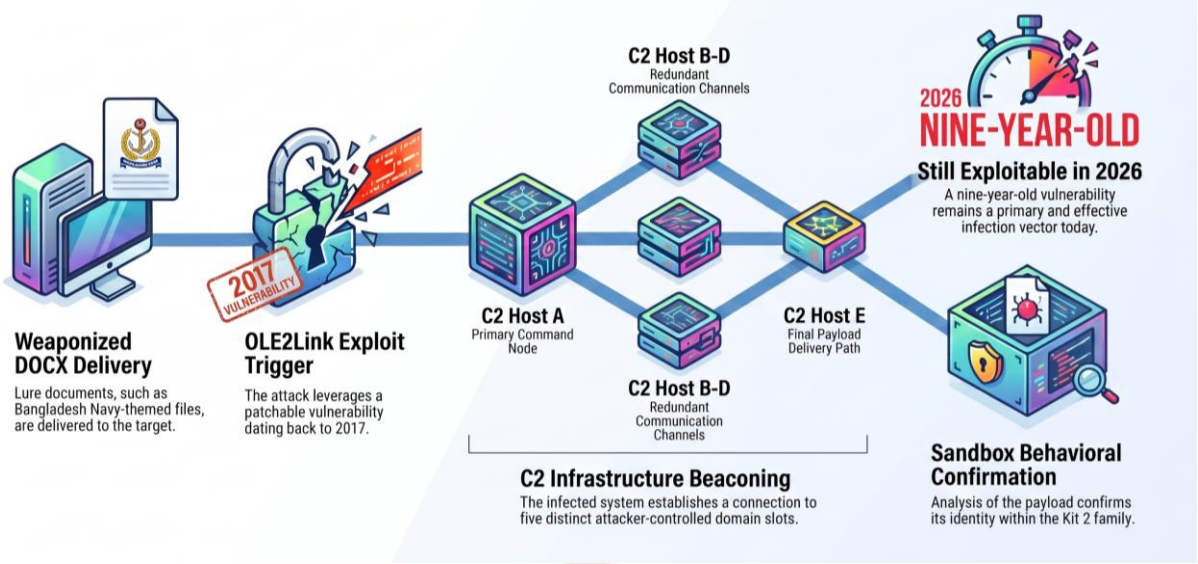

Figure: Kit 2 Attack Chain (Legacy Exploit Path)

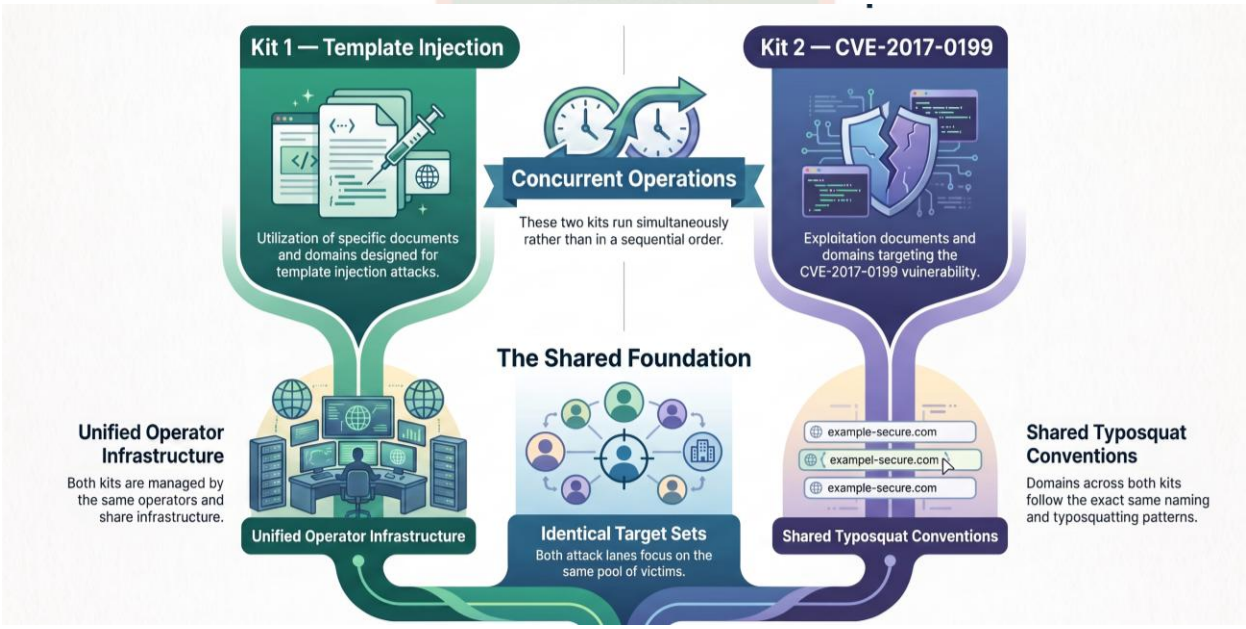

Figure: Dual-Kit Infrastructure Overlap

Document Phishing (.eml) Using Genuine Bangladeshi Government Content

A third delivery method uses phishing emails built around genuine, publicly available documents as bait, rather than weaponized attachments. These emails explicitly reference the legitimate mofa.gov.bd domain to increase perceived legitimacy, while routing sender/reply infrastructure through attacker-controlled mail domains `nih[.]mail-egov[.]org and nih[.]pk[.]mail-egov[.]org`. Because the attached document itself is unweaponized, this technique is designed to bypass attachment-sandboxing and file-hash-based detection, relying instead on social engineering and domain trust — recipients should

independently verify sender domains (not just the "From" display name) whenever a message purports to originate from mofa.gov.bd or any *.gov.bd address.

Decoy Pairing

Operators distribute at least one lure (the "China Power Supply Development Report 2026") in both a clean, unweaponized version and a weaponized Kit 1 version, allowing the malicious version to be swapped in while the benign document circulates as cover. Bangladeshi recipients of any HR/circular/pay-scale-themed or training-correspondence document should assume weaponized and benign versions of the same-titled document may circulate simultaneously — file appearance and title alone are not a reliable safety indicator.

Lure Themes Relevant to Bangladesh

Based on the confirmed audience segmentation in this campaign, Bangladeshi personnel in the following roles should be considered elevated-risk recipients:

- **Civil service/HR staff** — HR/pay-scale/allowance/promotion notices (e.g., disparity reduction allowance, basic pay scale revisions) are a confirmed lure theme; Cabinet Division and MoHA personnel handling such circulars are plausible targets.
- **Training/professional-development staff** — CEH (Certified Ethical Hacker) training enquiry/acceptance correspondence is used as a lure; ironically, cybersecurity and IT staff pursuing certifications are themselves a targeted demographic.
- **Military/defense personnel** — the named military exercise theme (EXERCISE_CARAT_2026) and Bangladesh Navy impersonation indicate defense-exercise-themed lures are plausible against Bangladeshi military recipients.
- **Diplomatic staff** — MoFA and Ankara-mission impersonation indicates diplomatic-cable or circular-themed lures targeting foreign-service officers.
- **Education-sector staff** — DSHE impersonation suggests administrative circulars or notices are being used as lure cover for education-directorate personnel

Infrastructure Analysis — Bangladesh-Relevant Nodes

All confirmed parent domains follow the same typosquat convention (`<agency>-gov-<cc>.<parent-domain>`). Registration-timing clustering is a strong single-operator indicator.

Parent domain	Registered	Nameserver	Bangladesh-relevant hosting
fetchdrives[.]info	—	**impreza[.]host**	Hosts **mofa-gov-bd** and **dshe-gov-bd** impersonation subdomains, alongside Sri Lanka Public Admin, Pakistan National Assembly, Nepal

Parent domain	Registered	Nameserver	Bangladesh-relevant hosting
			MoHA, Pakistan Finance, and the China NEA lure
min-pk[.]com	18 Feb 2026	**dyna-ns[.]net** (shared with **fia-g0v[.]net**, **download-msoffice[.]com**, **vagued[.]live**)	Hosts Bangladesh/Nepal MoFA and Sri Lanka Public Admin subdomains
interior-ministry[.]com	19 Feb 2026	**registrar-servers[.]com** (shared with **direct880[.]net**)	Hosts Bangladesh MoFA/MoD, Nepal MoHA, Pakistan SBP and NDMA subdomains
filenest[.]live	— (suspended)	**ns1[.]verification-hold[.]suspended-domain[.]com**	Prior to suspension hosted the widest spread observed, including the Bangladesh MoFA IDN homograph (**xn--mofagovbd-t89dd**), AJK Pakistan, Sri Lanka Treasury/Central Bank, and multiple Bangladesh/Nepal ministries
download-msoffice[.]com	16 Mar 2026	**dyna-ns[.]net**	Hosts CEH-training and Circular lure subdomains (Kit 2 / CVE-2017-0199) plus **Bangladesh Navy (bdnavy)** and Pakistan Cabinet Division impersonation
mail-svr[.]co	19 Feb 2026	—	Flagged malicious/C2, strongly negative reputation. Impersonates UN/UN-OCHA alongside **MoFA Bangladesh**, Nepal, Pakistan, and Sri Lanka Public Admin
fia-g0v[.]net	16 Feb 2026	**dyna-ns[.]net** (shared with **min-pk[.]com**)	Zero-homoglyph “g0v” domain; impersonates Pakistan FIA plus a wide set of Pakistan, **Bangladesh**, and Sri Lanka ministries

Registration-clustering observation relevant to defenders: Six domains — `mail-egov[.]org`, `fia-g0v[.]net`, `direct880[.]net` (16 Feb 2026), `min-pk[.]com`, `pk-mailgov[.]com` (18 Feb 2026), and `interior-ministry[.]com`, `mail-svr[.]co` (19 Feb 2026) — were registered within a four-day window, several sharing the dyna-ns[.]net dynamic DNS nameserver. Bangladesh-facing subdomains appear across nearly all of these parent

domains, meaning defenders should treat the entire cluster (not just domains with an obvious Bangladesh string) as relevant to Bangladesh's threat exposure.

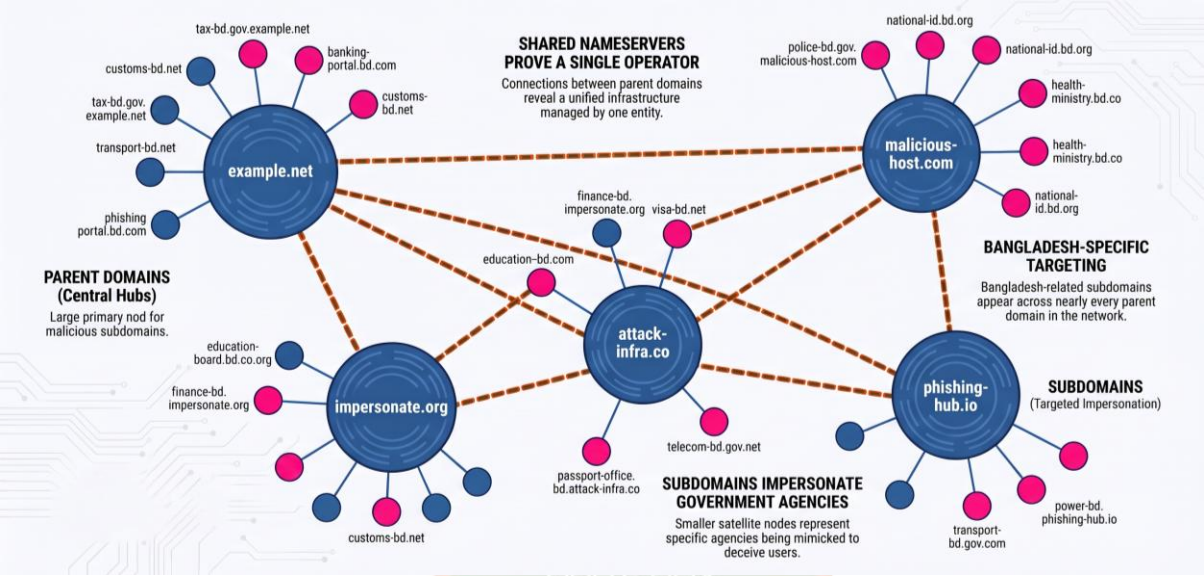

Figure: Infrastructure Relationship Graph

Cross-cutting beacon: `e7[.]knd[.]vg` is embedded in every Kit 1 PDF sample regardless of which parent typosquat domain delivered it — this single indicator should be blocked network-wide irrespective of which specific ministry-themed subdomain was used in a given lure.

MITRE ATT&CK Mapping

Tactic	Technique	ID
Reconnaissance / Resource Development	Acquire Infrastructure: Domains	T1583.001
Resource Development	Establish Accounts: Email Accounts	T1585.002
Initial Access	Spearphishing Attachment	T1566.001
Initial Access	Spearphishing Link	T1566.002
Execution	Exploitation for Client Execution (CVE-2017-0199)	T1203
Execution / Defense Evasion	Template Injection	T1221
Defense Evasion	Masquerading: Match Legitimate Name or Location	T1036.005
Command and Control	Application Layer Protocol: Web Protocols	T1071.001
Collection / Exfiltration	Data Staged / Exfiltration over C2 Channel	T1074 / T1041

Persistence (historical StealerBot chain)	DLL Side-Loading	T1574.002

Indicators of Compromise (IoC)

Sample hashes

Type	VHash	Notes
Weaponized DOCX (Kit 1)	**ba8a8dcf308b74616714221e0d3b3a1e**	OLE remote template injection
Weaponized PDF (Kit 1)	**9bdaee3d3d16a209244ef6d74b2e5ebb4**	Also beacons to **e7.knd.vg**
PDF metadata pattern	Adobe Acrobat DC 23.008.20470 / **Document_7032**	Matches prior tracked SideWinder reference samples

Domains (parent typosquat infrastructure, current campaign)

`fetchdrives[.]info, min-pk[.]com, interior-ministry[.]com, filenest[.]live (suspended), download-msoffice[.]com, vagued[.]live, mail-svr[.]co, pk-mailgov[.]com, fia-g0v[.]net, direct880[.]net, mail-egov[.]org, mailnavymilbd[.]govpk[.]net, mailnepalarmy[.]mofagov[.]com,`

Confirmed Bangladesh-themed subdomains

`mofa-gov-bd, mod-gov-bd, dshe-gov-bd, moha-gov-bd, moha-portal-gov-bd, mocat-gov-bd, bdnavy, cabinet-gov-bd, ankara-mofa-gov-bd, xn--mofagovbd-t89dd, mail-bcc-gov-bd, bccgov-bd-production, webmaii-bcc-gov-bd-newfiles, dgdp-account-file-data-doc-procuremen, mail-bof-gov-file-account-conf-files, mail-baf-mil-bd-account-data-files-document, mail-bfsa-gov-bd`

Attacker mail infrastructure (document-phishing / .eml vector)

`nih[.]mail-egov[.]org, nih[.]pk[.]mail-egov[.]org`

Beacon / fingerprinting infrastructure

`e7[.]knd[.]vg`

Prior-campaign infrastructure (2024–2025, for historical correlation and retro-hunting in Bangladesh environments)

`army-govbd[.]info, mailbox3-inbox1-bd[.]com, mailbox-inbox-bd[.]com` (resolving to **146.70.118.226**, Frankfurt), `mail.gov.bd`-themed phishing pages

Sample IPv4 Addresses

IP Address	IP Address	IP Address	IP Address	IP Address
168.222.243[.]49	104.21.4[.]43	172.67.131[.]165	94.126.224[.]99	91.242.163[.]218
88.119.161[.]40	146.70.118[.]22	5.230.47[.]35	46.202.186[.]194	109.248.161[.]64
52.79.102[.]70	95.179.160[.]235	18.229.249[.]186	3.37.215[.]204	16.162.223[.]161
45.76.84[.]233	185.233.166[.]156	8.210.202[.]98	64.46.102[.]122	64.46.102[.]63
64.46.102[.]26	79.141.171[.]134	207.174.3[.]152	103.151.111[.]61	193.243.147[.]76
79.141.164[.]135	193.29.59[.]77	8.208.11[.]212	47.236.119[.]146	194.68.225[.]186
185.117.88[.]229	185.243.113[.]33	5.255.107[.]177	193.42.36[.]227	103.57.249[.]95
92.243.65[.]243	46.30.190[.]15	5.255.118[.]88	77.83.196[.]59	185.174.135[.]126
5.180.114[.]198	2.58.15[.]71	185.235.138[.]81	5.149.248[.]240	193.42.36[.]173
91.193.18[.]75	172.93.185[.]138	79.141.174[.]58	185.117.89[.]166	5.181.20[.]102
213.109.192[.]93	193.42.36[.]66	35.175.135[.]236	5.230.72[.]173	5.230.72[.]213
5.230.73[.]60	195.133.192[.]40	79.141.174[.]208	45.147.230[.]157	5.230.67[.]108
5.230.68[.]190	193.42.36[.]86	194.71.227[.]64	37.235.56[.]14	45.14.107[.]153
89.248.171[.]166	91.245.253[.]73	149.154.152[.]37	158.255.211[.]188	149.154.154[.]216
151.236.25[.]121	158.255.212[.]140	172.93.162[.]117	172.96.189[.]157	185.174.135[.]57
5.230.72[.]184	5.255.105[.]65	5.255.98[.]158	64.44.167[.]150	192.71.166[.]145
193.200.17[.]199	193.42.36[.]223	193.42.36[.]25	203.24.92[.]115	46.21.153[.]227
46.30.189[.]54	104.128.189[.]242	5.2.77[.]238	5.2.78[.]64	5.230.69[.]72
5.230.71[.]10	198.252.108[.]219	198.252.108[.]33	2.58.15[.]61	172.93.189[.]46
185.117.90[.]144	193.42.36[.]50	5.230.74[.]103	138.68.160[.]176	193.42.39[.]34

Recommendations

- Patch legacy Microsoft Office installations against CVE-2017-0199 and CVE-2017-11882 across all in-scope ministries — these are 2017-era vulnerabilities and their continued exploitability indicates patch-compliance gaps that should be closed as a baseline hygiene measure, independent of this specific campaign.
- Disable automatic remote template/linked-data fetching in Microsoft Office via Group Policy (disable "Update Automatic Links at Open," enforce Protected View for internet-zone documents, and block OLE package activation from untrusted sources).
- Network/DNS-layer blocking:
    - Block/sinkhole all listed parent domains and Bangladesh-themed subdomains, IPv4 Addresses, Hashes.
    - Block the cross-cutting beacon `e7[.]knd[.]vg` network-wide.
    - Implement pattern-based DNS alerting for newly observed domains matching `*-gov-bd*`, `*-gov-np*`, `*-gov-pk*`, `*-gov-lk*` that do not resolve to known legitimate government IP ranges.
    - Alert on DNS queries containing punycode `(xn--)` prefixes combined with government-related strings.
- Email gateway rules: quarantine and sandbox-detonate DOCX/PDF attachments containing OLE relationships with `TargetMode="External"`, and specifically flag any outbound request path matching /`office-compatibility-suite` or /`adobe-reader` observed from detonation sandboxes.
- Endpoint/EDR detection: deploy detection logic for the two confirmed VHashes , and hunt retroactively for the Adobe Acrobat DC 23.008.20470 / `Document_7032` metadata pattern in mail and file-storage systems.
- Retro-hunt for the 2024–2025 legacy infrastructure (`army-govbd[.]info`, `mailbox3-inbox1-bd[.]com`, `mailbox-inbox-bd[.]com`) in historical DNS/proxy logs to determine whether prior compromise occurred that has gone undetected.
- Reinforce that both DOCX and PDF versions of the same document may be independently weaponized — file format is not a safety signal, and a "China Power Supply Development Report"-style dual clean/weaponized pairing shows attackers deliberately exploit this assumption.
- Train staff to verify the actual sending domain (not just display name) on any email referencing mofa.gov.bd or other *.gov.bd addresses, given the confirmed document-phishing technique that spoofs legitimate government domains while routing through attacker-controlled mail infrastructure.

References

- https://www.acronis.com/en/tru/posts/from-banks-to-battalions-sidewinders-attacks-on-south-asias-public-sector/
- https://hunt.io/blog/operation-southnet-sidewinder-south-asia-maritime-phishing
- Flavio Queiroz — THREAT CAMPAIGN: APT SideWinder multi-country spear-phishing, https://www.linkedin.com/posts/flavioqueiroz_threathunting-threatdetection-threatanalysis-activity-7361713711570427905-W8t_
- Group-IB campaign reporting, “SideWinder’s Expanding South Asian Gambit: Government Impersonation at Scale