ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

Ongoing Phishing Campaign targeting Bangladesh

[THIS PAGE IS INTENTIONALLY LEFT BLANK]

Sharing Indicator Protocol

TLP definitions (FIRST - https://www.first.org/tlp/)

Community: Under TLP, a *community* is a group who share common goals, practices, and informal trust relationships. A community can be as broad as all cybersecurity practitioners in a country (or in a sector or region).

Organization: Under TLP, an *organization* is a group who share a common affiliation by formal membership and are bound by common policies set by the organization. An organization can be as broad as all members of an information sharing organization, but rarely broader.

Clients: Under TLP, clients are those people or entities that receive cybersecurity services from an *organization*. Clients are by default included in TLP:AMBER so that the recipients may share information further downstream in order for clients to take action to protect themselves. For teams with national responsibility this definition includes stakeholders and constituents.

a. TLP:RED= For the eyes and ears of *individual* recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

b. TLP:AMBER = Limited disclosure, recipients can only spread this on a need-to-know basis within their *organization* and its *clients*. Note that TLP:AMBER+STRICT restricts sharing to the *organization* only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization **only**, they must specify TLP:AMBER+STRICT.

c. TLP:GREEN = Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.

d. TLP:CLEAR = Recipients can spread this to the *world*, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

Table of Contents

CYBER THREAT ALERT ON ONGOING PHISHING CAMPAIGN TARGETING BANGLADESH

TLP: CLEAR
Distribution: Public
Type of Threat: Ongoing Phishing Campaign Targeting Bangladesh

Date: 04 January 2024

Executive Summary

Cyber Threat Intelligence Unit of BGD e-GOV CIRT has detected a suspicious ongoing phishing campaign by APT group named as *SideWinder* targeted at Bangladeshi entities such as Bangladesh Armed Forces Division (AFD) and Law Enforcement Agencies. The group is known as a highly active hacker group who has shown the capability to conduct several attacks within a short time span and poses threats to organizations in South and East Asia. This alert includes an extensive list of IOCs and the group TTPs in order to help Bangladeshi organizations in taking preventive security measures accordingly. In Primary investigation we noticed that the main target of this APT group is to steal sensitive, confidential and classified documents.

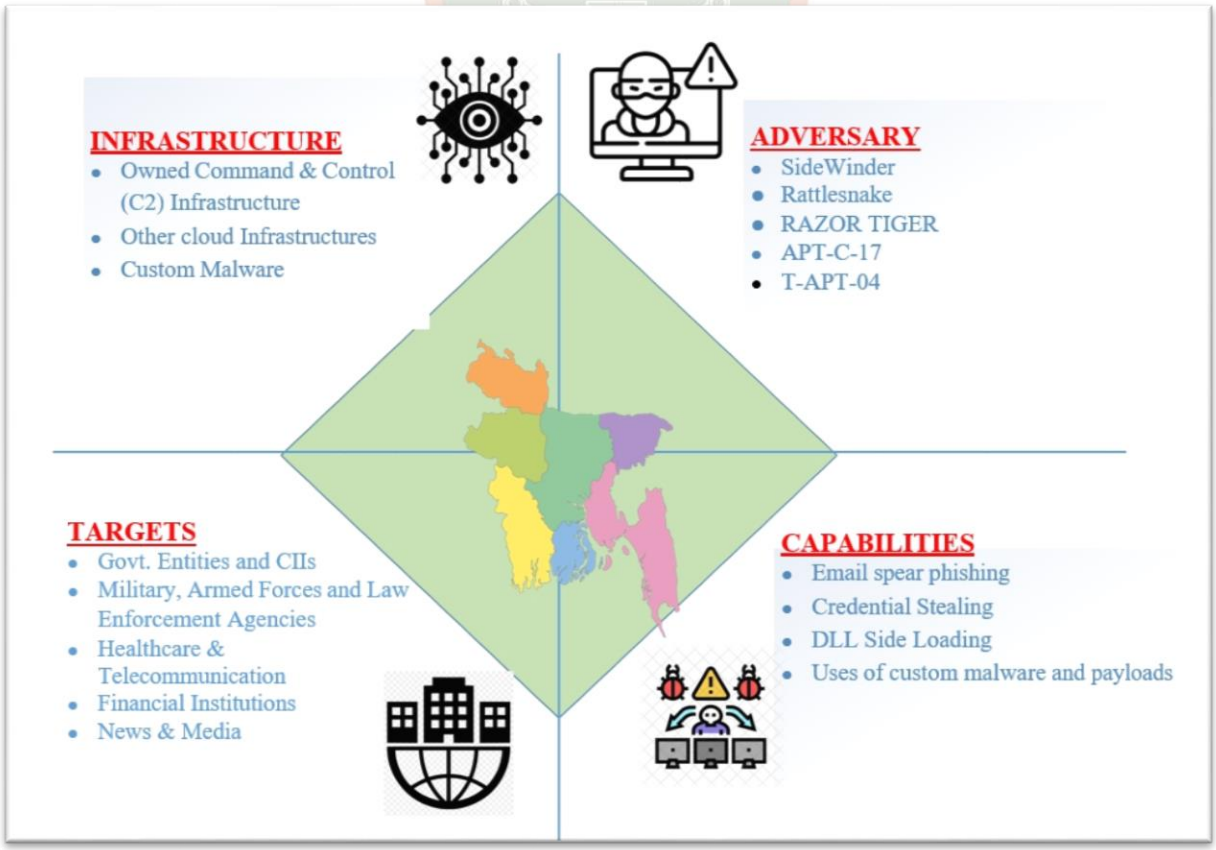

Fig 1: Threat model of SideWinder APT group

Sources of Alert: *Threat intelligence research*

Research Conducted by: *Cyber Threat Intelligence Unit, BGD e-GOV CIRT*

Threat level: *High*

Associated Malware/ Tools/ Techniques: *Spear phishing attachment/ links, document exploitation, DLL Side Loading*

Targeted Organization: *Government, Defense and Law Enforcement Agencies*

Attack Surface: *Windows and Android systems*

Threat Index

With coordination of threat intelligence sources, peer organizations feeds and OSINT assessments BGD e-GOV CIRT identifies some attributes, IOCs and other associated information about the persistent group activities.

Threat Actor

The threat actor behind the phishing campaign is known as '**Sidewinder**'. The group is identified as a prolific nation-state group that has been active since at least 2012. They have been observed to primarily use spear phishing attacks as a method to gain entry to target systems such as government, military, and business entities throughout Asia, primarily focusing on Pakistan, China, Nepal, Afghanistan, **Bangladesh**, Myanmar, Philippines, Qatar, Singapore and Turkey.

Threat motives

Sensitive, Confidential and Classified information theft and cyber espionage.

Alias

RAZOR TIGER, Rattlesnake, APT-C-17, T-APT-04, Hardcore Nationalist (HN2)

Target Sectors

Government, Military, Law enforcement, HealthCare, Telecommunication, Financial Institutions, News and Media

Target Countries

Afghanistan, Armenia, China, **Bangladesh**, Belarus, Bhutan, Brazil, China, India, Israel, Kazakhstan, Kyrgyzstan, Mexico, Moldova, Myanmar, Nepal, Pakistan, Philippines, Poland, Qatar, Russian Federation, Saudi Arabia, Singapore, Sri Lanka, Tajikistan, Thailand, Turkey, Turkmenistan, Ukraine, Uzbekistan.

Fig 2: Graphical Representation of targeted countries

Related CVEs

This threat actors primarily used to exploit the below mentioned CVEs to accomplish their operations

CVE-2017-11882	CVE-2023-38831	CVE-2022-42889	CVE-2018-0798	CVE-2022-47966
CVE-2020-1472	CVE-2022-37969	CVE-2022-42475	CVE-2017-11882	CVE-2022-41264
CVE-2021-33764	CVE-2019-2215	CVE-2023-36884		

Associated Malware/Software

We observed they use the below mentioned custom malwares to achieve their goals

SideWinder.HTA.Downloader	SideWinder.Stager	SideWinder.StealerPy
SideWinder.ReverseShell	SideWinder.RAT	Chisel
Cobalt Strike	SideWinder.AntiBot.Script	WarHawk
SideWinder.RAT.b (a remote access Trojan)		

SideWinder's Cyberattack Chain

We observed and identified the infection chain performed by the threat actor in different phases of attack

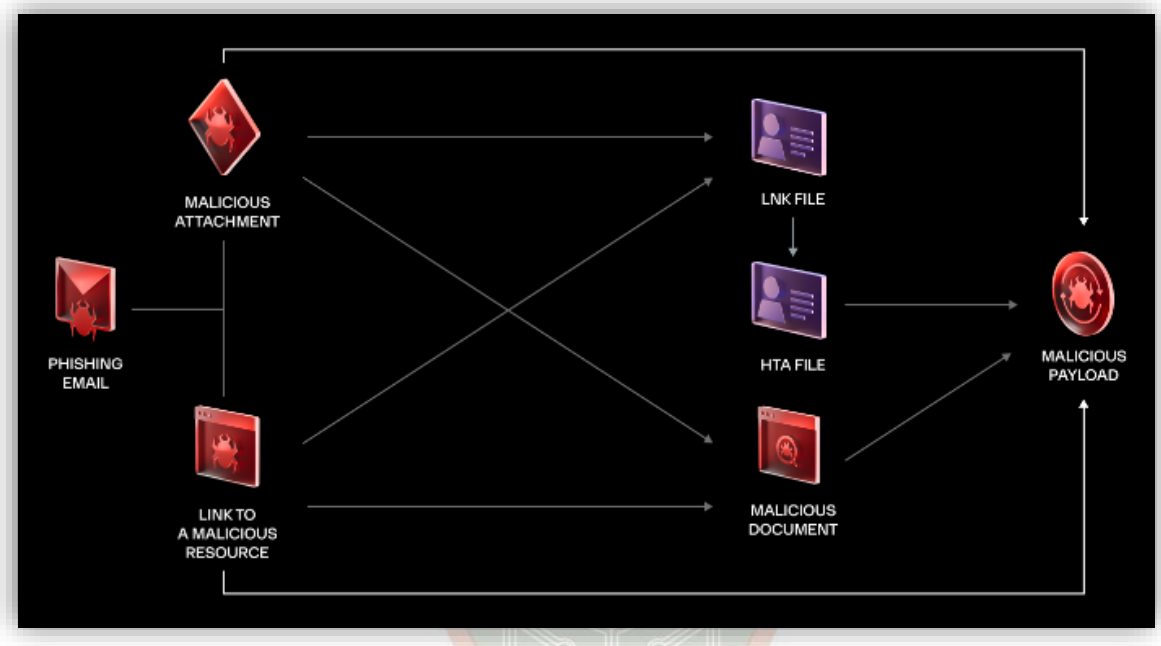

Fig 3: SideWinder's attack chain

Initial access vector

SideWinder has been using **spear phishing** as its primary initial attack vector against their victims. The attack is initiated by a victim receiving a phishing email containing a malicious attachment or URL. The email lures are often crafted for the target organization and include contents that the recipients would find relatable or interested in learning about. They used emails pertaining to domains which look-a-like several government, military and law enforcement agencies' domains of Bangladesh (e.g. cirt-gov-bd.donwloaded[.]com)

Code execution

- When a user clicks on the malicious link/attached file (RTF, DOCX, ZIP, LNK,..etc.), a code execution is initiated to download a **remote HTA file** from the group's controlled server.
- The HTA file run leads to the execution of the payload malware through DLL side loading technique. (The malware can be a remote access Trojan (RAT) or an information stealer)
- The Malware starts collecting sensitive and confidential info./files and send it to the C2 server.

Phishing Domains (look-a-like Bangladeshi Govt. owned) used by SideWinder

Cyber threat intelligence unit of BGD e–GOV CIRT through its research and analysis has detected some phishing domains that mimic Bangladeshi official websites and domains. The findings have raised the alarm of an ongoing phishing campaign conducted against entities in the country. By analyzing those malicious domains, hash files, and IP addresses, it has been discovered that they are attributed to SideWinder APT group, which targets government and law enforcement organizations in Bangladesh. Some of those identified phishing domains are listed below:

Phishing domain	
police-gov-bd.fia-gov[.]net	bangladesh.tni-mil[.]com
police-circular-gov-bd.fia-gov[.]net	afd-gov-bd.donwloaded[.]com
mofa-gov-bd.fia-gov[.]net	cirt-gov-bd.donwloaded[.]com
police-gov-bd.donwloaded[.]com	

As shown in the below image, the IP address of **5.230.54.3** hosts malicious subdomains which mimic Bangladeshi organizations. Later found that the IP address belongs to SideWinder APT network.

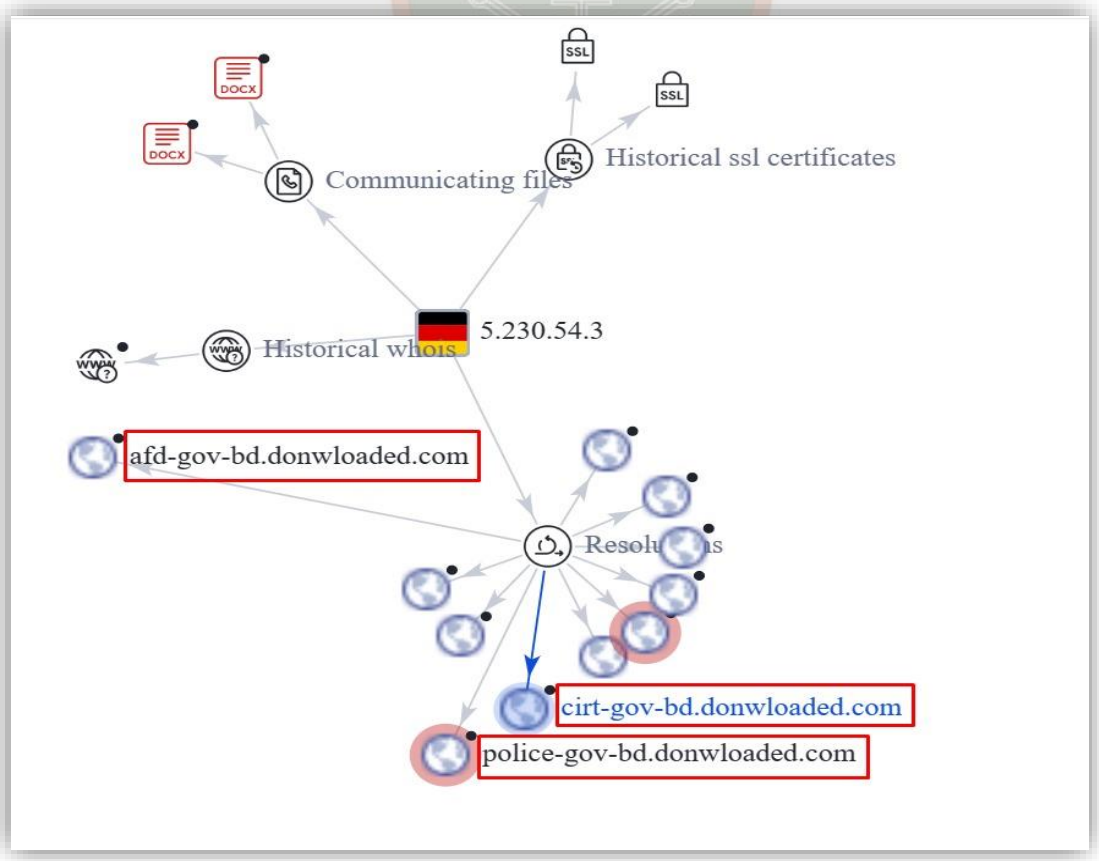

Fig 4: 5.230.54.3 IP address attributed to SideWinder APT host malicious phishing domains (Source: VirusTotal)

We observed that the file type mostly used by the group in its phishing attacks targeted at Bangladeshi entities is "***RTF***", a **rich text document file**. It is worth mentioning that the APT group uses **Server-Side Polymorphism** which is a technique used by the group in an attempt to evade detection by traditional antiviruses which are based on signatures to detect malicious files.

	Url	Domain	IPv4
2	http://bdmil.alit.live/3398/1/54346/2/0/0/0/m/files-491dc489/file.rtf	bdmil.alit.live	
3	http://navy-mil-bd.jmicc.xyz/5625/1/8145/2/0/0/0/m/files-b11074b7/file.rtf	navy-mil-bd.jmicc.xyz	
4	http://mailnavybd.govpk.net/5845/1/12/2/0/0/0/m/files-ca78574e/file.rtf	mailnavybd.govpk.net	5.255.112.194
5	https://mailnavymilbd.govpk.net/5848/1/13/2/0/0/0/m/files-57d837e4/file.rtf	mailnavymilbd.govpk.net	
6	http://mailnavymilbd.govpk.net/5848/1/13/2/0/0/0/m/files-57d837e4/file.rtf	mailnavymilbd.govpk.net	
7	http://bdmil.alit.live/3398/1/50073/2/0/0/0/m/files-ac995f17/file.rtf	bdmil.alit.live	
8		mofa-bd.org	
9	https://bangladeshmarineacademylibrary.ppinewsagency.live/5083/1/3417/2/0/0/0/m/files-76793138/file.rtf	bangladeshmarineacademylibrary.ppinewsagency.live	

General Guidelines:

- Use the given IOC list to create hunting rules that can be used to learn about that group's attacks in the making and respond to them proactively.
- As SideWinder relies on targeted spear phishing as the initial vector. It is therefore important for organizations to deploy business email protection solutions that detonate malicious content.
- Implement regular user training on social engineering and phishing attacks. Educate users on identifying suspicious emails and links, not interacting with those suspicious items, and the importance of reporting instances of opening suspicious emails, links, attachments, or other potential lures.
- Enable Domain-based Message Authentication, Reporting, and Conformance (DMARC) for received emails, along with Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM), verify the sending server of received emails by checking published rules. If an email fails the check, it is deemed a spoofed email address.
- Ensure DMARC is set to "reject" for sent emails. This provides robust protection against other users receiving emails that impersonate a domain.
- Review MFA lockout and alert settings and track denied (or attempted) MFA logins.
- Enable MFA and Implement strong password policies.
- Implement DNS filtering or firewall deny lists to block known malicious sites.
- Implement anti-virus solutions to mitigate malware and to stop malware from executing if a malicious hyperlink or attachment from an email is opened.
- Ensure that software applications are set to automatically update so that network software is always upgraded to the latest version. This helps to prevent malicious actors from exploiting vulnerabilities within an organization's network software.
- Avoid interacting with any links or attachments in the suspicious email. They may lead to malicious websites or contain malware.

- Phishing emails may contain errors in spelling, grammar, or formatting. Legitimate organizations typically maintain a professional appearance in their communications
- Hover your mouse over any links in the email (without clicking) to see the actual URL. If it looks suspicious or doesn't match the claimed destination, it's likely a phishing attempt
- If you've inadvertently provided sensitive information, such as login credentials, update your passwords immediately. Enable two-factor authentication where available for an extra layer of security.

➢ **TO PREVENT MALWARE EXECUTION FOLLOWING PHISHING ATTACKS:**

- Use denylists to block known malicious domains, URLs, and IP addresses as well as file extensions such as .scr, .exe, .pif, and .cpl and mislabeled file extensions (e.g., a .exe file that is labeled as a .doc file.)
- Restrict MacOS and Windows users from having administrative rights.
- Implement the principle of least privilege (PoLP) when administering user accounts.
- Implement application allowlists.
- Block macros by default.
- Use Google Safe Browsing to identify and stop malware upon user execution.

Indicators of Compromise (IoCs)

TYPE	INDICATOR
Domain/hostname	police-gov-bd[.]fia-gov[.]net
Domain/hostname	mofa-bd[.]org
Domain/hostname	police-circular-gov-bd[.]fia-gov[.]net
Domain/hostname	mofa-gov-bd[.]fia-gov[.]net
Domain/hostname	bdmil[.]alit[.]live
Domain/hostname	mailnavybd[.]govpk[.]net
Domain/hostname	mailnavymilbd[.]govpk[.]net
Domain/hostname	navy-mil-bd[.]jmicc[.]xyz
Domain/hostname	police-circular-gov-bd.fia-gov[.]net
Domain/hostname	police-gov-bd.donwloaded[.]com
Domain/hostname	bangladesh.tni-mil[.]com
Domain/hostname	afd-gov-bd.donwloaded[.]com
Domain/hostname	cirt-gov-bd.donwloaded[.]com
IP	5.230.54[.]3
hash	61e18a5c50aeb93c34112e566a2761920b5d3dc9e

	6090aa5808ee385e8ca3dd7
hash	4bad3e34a192a8f305e188538b4370ea835 446cc6ba32fe046d9a5f2bc3df172

For getting the full list of the APT group's IOCs, please check the attached ***appendix 2***

Appendix 1 – SideWinder mapping to ATT&CK Framework

- TA0043: Reconnaissance
  - o T1589: Gather Victim Identity Information
    - T1589.002: Email Addresses
    - T1589.003: Employee Names
  - o T1591: Gather Victim Org Information
    - T1591.002: Business Relationships
    - T1591.001: Determine Physical Locations
    - T1591.003: Identify Business Tempo
    - T1591.004: Identify Roles
- TA0042: Resource Development
  - o T1583: Acquire Infrastructure
    - T1583.001: Domains
    - 1583.004: Server
- TA0001: Initial Access
  - o T1566.001: Spearphishing Attachment
  - o T1566.002: Spearphishing Link
- TA0002: Execution
  - o T1059: Command and Scripting Interpreter
    - T1059.007: JavaScript/Jscript
    - T1059.001: PowerShell
    - T1059.005: Visual Basic
  - o T1203: Exploitation for Client Execution
  - o T1204: User Execution
    - T1204.002: Malicious File
    - T1204.001: Malicious Link
- TA0003: Persistence
  - o T1574: Hijack Execution Flow
    - T1574.002: DLL Side-Loading
  - o T1078: Valid Accounts
- TA0004: Privilege Escalation
  - o T1574: Hijack Execution Flow
    - T1574.002: DLL Side-Loading
- TA0005: Defense Evasion
  - o T1574: Hijack Execution Flow

- T1574.002: DLL Side-Loading

- TA0007: Discovery
  - T1087: Account Discovery
    - T1087.001: Local Account
  - T1083: File and Directory Discovery
  - T1120: Peripheral Device Discovery
  - T1069: Permission Groups Discovery
  - T1057: Process Discovery
  - T1518: Software Discovery
  - T1082: System Information Discovery
  - T1007: System Service Discovery
  - T1124: System Time Discovery
- TA0009: Collection
  - T1119: Automated Collection
  - T1602: Data from Configuration Repository
    - T1602.002: Network Device Configuration Dump
  - T1005: Data from Local System
  - T1039: Data from Network Shared Drive
  - T1025: Data from Removable Media
  - T1074: Data Staged
    - T1074.001: Local Data Staging
- TA0011: Command and Control
  - T1071: Application Layer Protocol
- TA0010: Exfiltration
  - T1020: Automated Exfiltration
  - T1041: Exfiltration Over C2 Channel

References:

https://www.group-ib.com/media-center/press-releases/sidewinder-apt-report/

https://cdn-cybersecurity.att.com/docs/global-perspective-of-the-sidewinder-apt.pdf

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

https://www.group-ib.com/blog/hunting-sidewinder/

https://threatfox.abuse.ch/browse/tag/SideWinder/

https://www.virustotal.com/gui/collection/threatfox_win_sidewinder/iocs

https://attack.mitre.org/groups/G0121/

https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pakistan