Advisory: Pahalgam Attack themed decoys used by APT36 to target the Indian Government

seqrite.com/blog/advisory-pahalgam-attack-themed-decoys-used-by-apt36-to-target-the-indian-government/

April 30, 2025

30 April 2025

Written by Rhishav Kanjilal

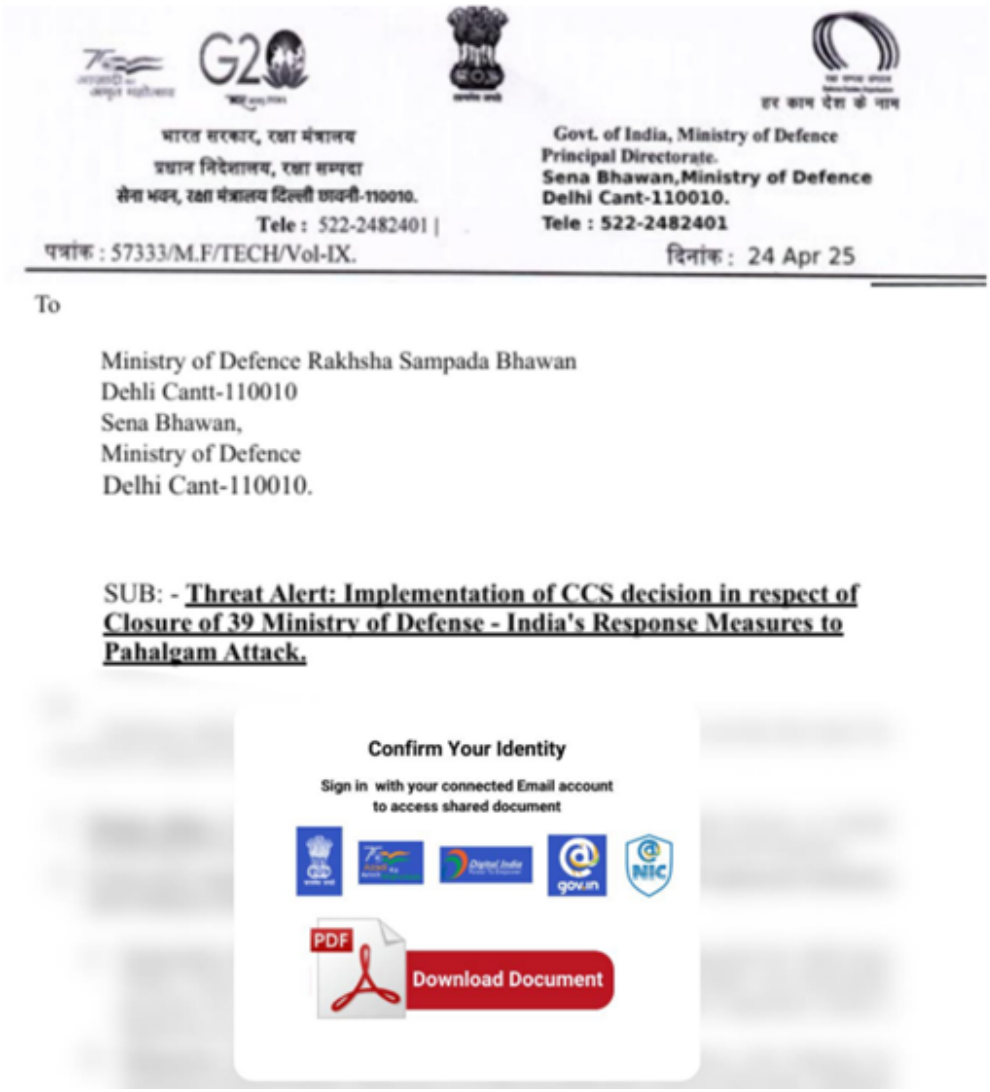
Seqrite Labs APT team has discovered “Pahalgam Terror Attack” themed documents being used by the Pakistan-linked APT group Transparent Tribe (APT36) to target Indian Government and Defense personnel. The campaign involves both credential phishing and deployment of malicious payloads, with fake domains impersonating Jammu & Kashmir Police and Indian Air Force (IAF) created shortly after the April 22, 2025 attack. This advisory alerts about the phishing PDF and domains used to uncover similar activity along with macro-laced document used to deploy the group’s well-known Crimson RAT.

Analysis

The PDF in question was created on April 24, 2025, with the author listed as “Kalu Badshah”. The names of this phishing document are related to the response measures by the Indian Government regarding the attack.

- “Action Points & Response by Govt Regarding Pahalgam Terror Attack .pdf”
- “Report Update Regarding Pahalgam Terror Attack.pdf”

RESTRICTED

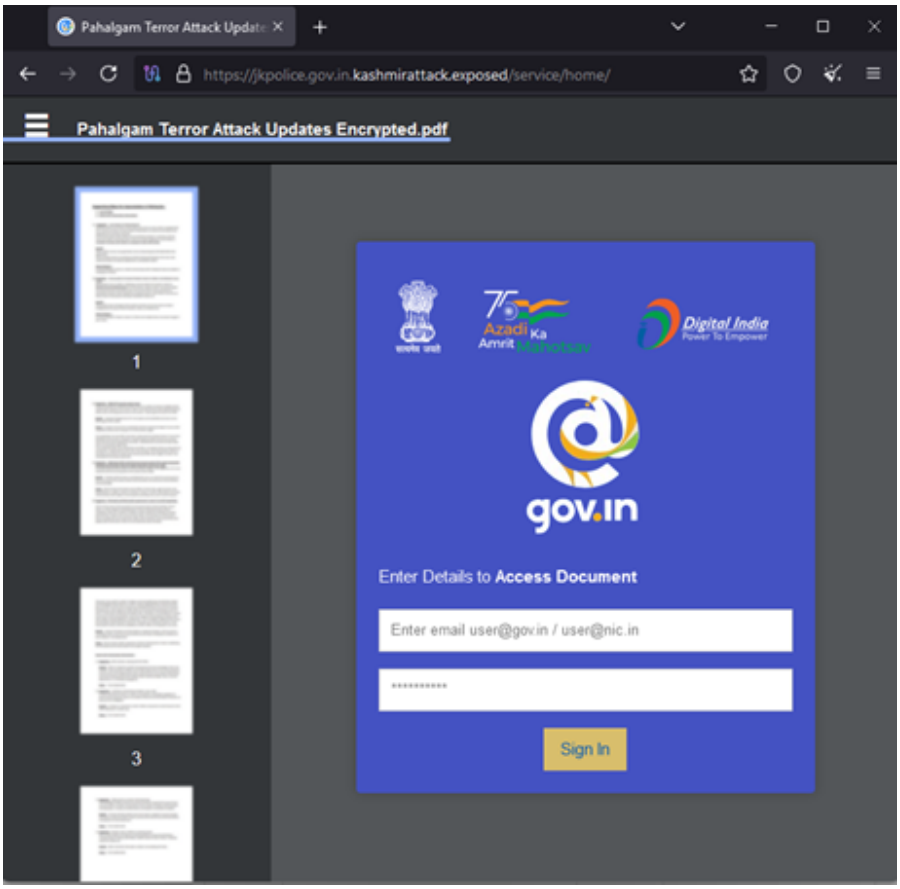


Picture 1

The content of the document is masked and the link embedded within the document is the primary vector for the attack. If clicked, it leads to a fake login page which is part of a social engineering effort to lure individuals. The embedded URL triggered is:

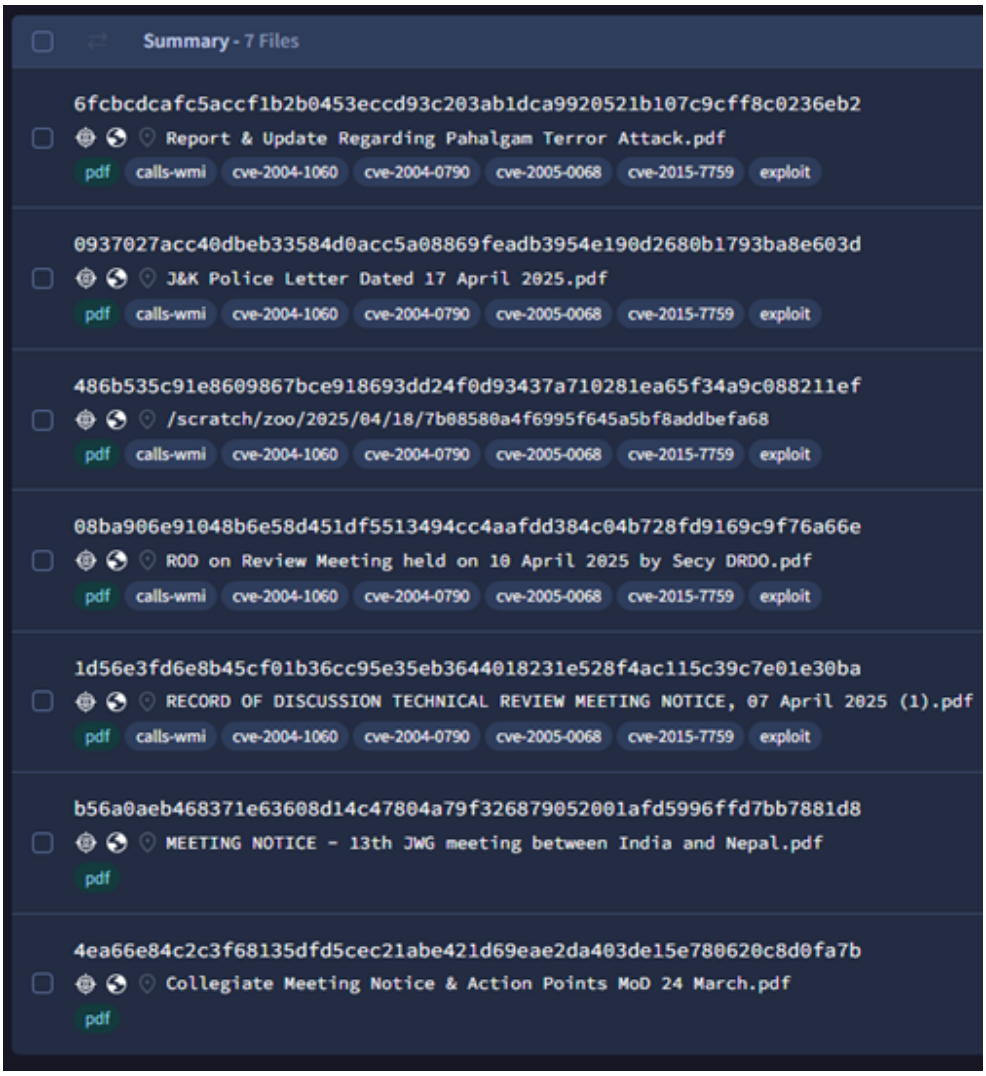
hxxps://jkpolice[.]gov[.]in[.]kashmirattack[.]exposed/service/home/

The domain mimics the legitimate Jammu & Kasmir Police (*jkpolice[.]gov[.]in*), an official Indian police website, but the fake one introduces a subdomain **kashmirattack[.]exposed**.



Picture 2

The addition of “kashmirattack” indicates a thematic connection to the sensitive geopolitical issue, in this case, related to the recent attack in the Kashmir region. Once the government credentials are entered for @gov.in or @nic.in, they are sent directly back to the host. Pivoting on the author’s name, we observed multiple such phishing documents.



Picture 3

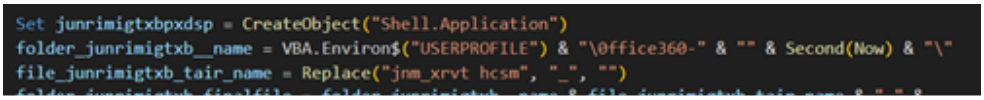
Multiple names have been observed for each phishing document related to various government and defence meetings to lure the targets, showcasing how quickly the group crafts lures around ongoing events in the country:

- Report & Update Regarding Pahalgam Terror Attack.pdf
- Report Update Regarding Pahalgam Terror Attack.pdf
- Action Points & Response by Govt Regarding Pahalgam Terror Attack .pdf
- J&K Police Letter Dated 17 April 2025.pdf
- ROD on Review Meeting held on 10 April 2025 by Secy DRDO.pdf
- RECORD OF DISCUSSION TECHNICAL REVIEW MEETING NOTICE, 07 April 2025 (1).pdf
- MEETING NOTICE – 13th JWG meeting between India and Nepal.pdf
- Agenda Points for Joint Venture Meeting at IHQ MoD on 04 March 2025.pdf
- DO Letter Integrated HQ of MoD dated 3 March.pdf
- Collegiate Meeting Notice & Action Points MoD 24 March.pdf
- Letter to the Raksha Mantri Office Dated 26 Feb 2025.pdf
- pdf

- Alleged Case of Sexual Harassment by Senior Army Officer.pdf
- Agenda Points of Meeting of Dept of Defence held at 11March 25.html
- Action Points of Meeting of Dept of Defence held at 10March 25.html
- Agenda Points of Meeting of External Affairs Dept 10 March 25.pdf.html

PowerPoint PPAM Dropper

A PowerPoint add-on file with the same name as of the phishing document *“Report & Update Regarding Pahalgam Terror Attack.ppam”* has been identified which contains malicious macros. It extracts both the embedded files into a hidden directory under user’s profile with a dynamic name, determines the payload based on the Windows version and eventually opens the decoy file with the same phishing URL embedded along with executing the Crimson RAT payload.



Picture 4

The final Crimson RAT dropped has internal name “jnmxrvt hcsm.exe” and dropped as “WEISTT.jpg” with similar PDB convention:

C:\jnmhxrv cstm\jnmhxrv cstm\obj\Debug\jnmhxrv cstm.pdb

All three RAT payloads have compilation timestamp on 2025-04-21, just before the Pahalgam terror attack. As usual the hardcoded default IP is present as a decoy and the actual C2 after decoding is – 93.127.133[.]58. It supports the following 22 commands for command and control apart from retrieving system and user information.

Commands	Functionality
procl / getavs	Get a list of all processes
endpo	Kill process based on PID
scrsz	Set screen size to capture
cscreen	Get screenshot
dirs	Get all disk drives
stops	Stop screen capture
filsz	Get file information (Name, Creation Time, Size)
dowf	Download the file from C2
cnls	Stop uploading, downloading and screen capture
scren	Get screenshots continuously
thumb	Get a thumbnail of the image as GIF with size ‘of 200×150.’
putsrt	Set persistence via Run registry key
udlt	Download & execute file from C2 with ‘*vdhairtn*’ name
delt	Delete file
file	Exfiltrate the file to C2
info	Get machine info (Computer name, username, IP, OS name, etc.)
runf	Execute command
afile	Exfiltrate file to C2 with additional information
listf	Search files based on extension
dowr	Download file from C2 (No execution)
fles	Get the list of files in a directory
fldr	Get the list of folders in a directory

Infrastructure and Attribution

The phishing domains identified through hunting have the creation day just one or two days after the documents were created.

Domains	Creation	IP	ASN
jkpolice[.]gov[.]in[.]kashmirattack[.]exposed	2025-04-24	37.221.64.134 78.40.143.189	AS 200019 (Alexhost Srl) AS 45839 (Shinjiru Technology)
iaf[.]nic[.]in[.]ministryofdefenceindia[.]org	2025-04-16	37.221.64.134	AS 200019 (Alexhost Srl)
email[.]gov[.]in[.]ministryofdefenceindia[.]org	2025-04-16	45.141.58.224	AS 213373 (IP Connect Inc)
email[.]gov[.]in[.]departmentofdefenceindia[.]link	2025-02-18	45.141.59.167	AS 213373 (IP Connect Inc)
email[.]gov[.]in[.]departmentofdefence[.]de	2025-04-10	45.141.58.224	AS 213373 (IP Connect Inc)
email[.]gov[.]in[.]briefcases[.]email	2025-04-06	45.141.58.224 78.40.143.98	AS 213373 (IP Connect Inc) AS 45839 (Shinjiru Technology)
email[.]gov[.]in[.]modindia[.]link	2025-03-02	84.54.51.12	AS 200019 (Alexhost Srl)
email[.]gov[.]in[.]defenceindia[.]ltd	2025-03-20	45.141.58.224 45.141.58.33	AS 213373 (IP Connect Inc)
email[.]gov[.]in[.]indiadefencedepartment[.]link	2025-02-25	45.141.59.167	AS 213373 (IP Connect Inc)
email[.]gov[.]in[.]departmentofspace[.]info	2025-04-20	45.141.58.224	AS 213373 (IP Connect Inc)
email[.]gov[.]in[.]indiangov[.]download	2025-04-06	45.141.58.33 78.40.143.98	AS 213373 (IP Connect Inc) AS 45839 (Shinjiru Technology)
indianarmy[.]nic[.]in[.]departmentofdefence[.]de	2025-04-10	176.65.143.215	AS 215208
indianarmy[.]nic[.]in[.]ministryofdefenceindia[.]org	2025-04-16	176.65.143.215	AS 215208

email[.]gov[.]in[.]indiandefence[.]work	2025-03-10	45.141.59.72	AS 213373 (IP Connect Inc)
email[.]gov[.]in[.]indiangov[.]download	2025-04-06	78.40.143.98	AS 45839 (Shinjiru Technology)
email[.]gov[.]in[.]drdosurvey[.]info	2025-03-19	192.64.118.76	AS 22612 (NAMECHEAP-NET)

This kind of attack is typical in hacktivism, where the goal is to create chaos or spread a political message by exploiting sensitive or emotionally charged issues. In this case, the threat actor is exploiting existing tensions surrounding Kashmir to maximize the impact of their campaign and extract intelligence around these issues.

The suspicious domains are part of a phishing and disinformation infrastructure consistent with tactics previously used by **APT36 (Transparent Tribe)** that has a long history of targeting:

- Indian military personnel
- Government agencies
- Defense and research organizations
- Activists and journalists focused on Kashmir

PPAM for initial access has been used since many years to embed malicious executables as OLE objects. Domain impersonation to create deceptive URLs that mimic Indian government, or military infrastructure has been seen consistently since last year. They often exploit sensitive topics like Kashmir conflict, border skirmishes, and military movements to create lures for spear-phishing campaigns. Hence these campaigns are attributed to APT36 with high confidence, to have involved delivering Crimson RAT, hidden behind fake documents or malicious links embedded in spoofed domains.

Potential Impact: Geopolitical and Cybersecurity Implications

The combination of a geopolitical theme and cybersecurity tactics suggests that this document is part of a broader disinformation campaign. The reference to Kashmir, a region with longstanding political and territorial disputes, indicates the attacker’s intention to exploit sensitive topics to stir unrest or create division.

Additionally, using PDF files as a delivery mechanism for malicious links is a proven technique aiming to influence public perception, spread propaganda, or cause disruptions. Here’s how the impact could manifest:

- **Disruption of Sensitive Operations**: If an official or government worker were to interact with this document, it could compromise their personal or organizational security.

- **Information Operations**: The document could lead to the exposure of sensitive documents or the dissemination of false information, thereby creating confusion and distrust among the public.
- **Espionage and Data Breaches**: The phishing attempt could ultimately lead to the theft of sensitive data or the deployment of malware within the target's network, paving the way for further exploitation.

Recommendations

Email & Document Screening: Implement advanced threat protection to scan PDFs and attachments for embedded malicious links or payloads.

Restrict Macro Execution: Disable macros by default, especially from untrusted sources, across all endpoints.

Network Segmentation & Access Controls: Limit access to sensitive systems and data; apply the principle of least privilege.

User Awareness & Training: Conduct regular training on recognizing phishing, disinformation, and geopolitical manipulation tactics.

Incident Response Preparedness: Ensure a tested response plan is in place for phishing, disinformation, or suspected nation-state activity.

Threat Intelligence Integration: Leverage geopolitical threat intel to identify targeted campaigns and proactively block indicators of compromise (IOCs).

Monitor for Anomalous Behaviour: Use behavioural analytics to detect unusual access patterns or data exfiltration attempts.

IOCs

Phishing Documents

c4fb60217e3d43eac92074c45228506a

172fff2634545cf59d59c179d139e0aa

7b08580a4f6995f645a5bf8addbefa68

1b71434e049fb8765d528ecabd722072

c4f591cad9d158e2fbb0ed6425ce3804

5f03629508f46e822cf08d7864f585d3

f5cd5f616a482645bbf8f4c51ee38958

fa2c39adbb0ca7aeab5bc5cd1ffb2f08

00cd306f7cdcfe187c561dd42ab40f33

ca27970308b2fdeaa3a8e8e53c86cd3e

Phishing Domains

jkpolice[.]gov[.]in[.]kashmirattack[.]exposed

iaf[.]nic[.]in[.]ministryofdefenceindia[.]org

email[.]gov[.]in[.]ministryofdefenceindia[.]org

email[.]gov[.]in[.]departmentofdefenceindia[.]link

email[.]gov[.]in[.]departmentofdefence[.]de

email[.]gov[.]in[.]briefcases[.]email

email[.]gov[.]in[.]modindia[.]link

email[.]gov[.]in[.]defenceindia[.]ltd

email[.]gov[.]in[.]indiadefencedepartment[.]link

email[.]gov[.]in[.]departmentofspace[.]info

email[.]gov[.]in[.]indiangov[.]download

indianarmy[.]nic[.]in[.]departmentofdefence[.]de

indianarmy[.]nic[.]in[.]ministryofdefenceindia[.]org

email[.]gov[.]in[.]indiandefence[.]work

email[.]gov[.]in[.]indiangov[.]download

email[.]gov[.]in[.]drdosurvey[.]info

Phishing URLs

hxxps://iaf[.]nic[.]in[.]ministryofdefenceindia[.]org/publications/default[.]htm

hxxps://jkpolice[.]gov[.]in[.]kashmiraxxack[.]exposed/service/home

hxxps://email[.]gov[.]in[.]ministryofdefenceindia[.]org/service/home/

hxxps://email[.]gov[.]in[.]departmentofdefenceindia[.]link/service/home/

hxxps://email[.]gov[.]in[.]departmentofdefence[.]de/service/home/

hxxps://email[.]gov[.]in[.]indiangov[.]download/service/home/

hxxps://indianarmy[.]nic[.]in[.]departmentofdefence[.]de/publications/publications-site-main/index[.]html

hxxps://indianarmy[.]nic[.]in[.]ministryofdefenceindia[.]org/publications/publications-site-main/index[.]htm

hxxps://email[.]gov[.]in[.]briefcases[.]email/service/home/

hxxps://email[.]gov[.]in[.]modindia[.]link/service/home/

hxxps://email[.]gov[.]in[.]defenceindia[.]ltd/service/home/

hxxps://email[.]gov[.]in[.]indiadefencedepartment[.]link/service/home/

hxxps://email[.]gov[.]in[.]departmentofspace[.]info/service/home/

hxxps://email[.]gov[.]in[.]indiandefence[.]work/service/home/

PPAM/XLAM

d946e3e94fec670f9e47aca186ecaabe

e18c4172329c32d8394ba0658d5212c2

2fde001f4c17c8613480091fa48b55a0

c1f4c9f969f955dec2465317b526b600

Crimson RAT

026e8e7acb2f2a156f8afff64fd54066

fb64c22d37c502bde55b19688d40c803

70b8040730c62e4a52a904251fa74029

3efec6ffcbfe79f71f5410eb46f1c19e

b03211f6feccd3a62273368b52f6079d

93.127.133.58 (Ports – 1097, 17241, 19821, 21817, 23221, 27425)

104.129.27.14 (Ports – 8108, 16197, 19867, 28784, 30123)

MITRE ATT&CK

Reconnaissance	T1598.003	Phishing for Information: Spearphishing Link
Resource Development	T1583.001	Acquire Infrastructure: Domains
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Execution	T1204.001 T1059.005	User Execution: Malicious Link Command and Scripting Interpreter: Visual Basic
Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
Discovery	T1033 T1057 T1082 T1083	System Owner/User Discovery Process Discovery System Information Discovery File and Directory Discovery
Collection	T1005 T1113	Data from Local System Screen Capture
Exfiltration	T1041	Exfiltration Over C2 Channel

Authors:

Sathwik Ram Prakki

Rhishav Kanjilal

Rhishav is a Security Researcher at Seqrite Labs, Quick Heal, specializing in threat intelligence, deep and dark web investigations, vulnerability assessments, and...

Articles by Rhishav Kanjilal »

Resources

- White Papers
- Datasheets

- Threat Reports
- Manuals
- Case Studies

About Us

- About Seqrite
- Leadership
- Awards & Certifications
- Newsroom

Archives

- By Date
- By Category

Email*

Subscribe

Privacy Policies Cookie Policies