

Forum:[Hack Forums](#)

Thread: [WHITELOTUS- PREMIUM RUST TELEGRAM RAT | Self-hosted | NO DEPS](#)

Infinity. - October 9, 2026, 1:42 am

Native Rust Binary. Telegram-controlled. Self-hosted relay - you run it on your own box, you own the bot, no shared infrastructure, no operator panel you don't control.

Ships as two binaries: a builder (egui, config + license stamping) and a relay (WebSocket control plane). One bot per customer. Spread as many victims as you want under it.

Why it's different

Most Telegram RATs have every victim polling the same bot, so commands hit a random machine and the rest sit deaf. RedLotus uses a relay: victims dial out over a WebSocket to your relay, the relay owns the bot, and commands route by victim ID - `/4531*info`` runs on victim 4531 and nowhere else. No contention, no collisions, hundreds of victims on one bot.

Relay is a single static binary. Runs on any cheap VPS. No domain, no server-side DB.

Feature set

Control

- Telegram bot as C2 - private chat or group
- Per-victim routing ``/id*cmd``
- Inline keyboard menus + per-victim button grid
- Paginated help
- Verbose mode (per-command acks)
- File transport — anything large ships as a document, chat stays clean
- Auto-registration — victims announce themselves, ``/online`` fills itself

Surveillance

- Keylogger (LL hook, manual shift/caps tracking, window-title tagging)
- Webcam capture
- Per-monitor screenshot
- Microphone capture (WAV, configurable duration)
- Active window title
- Battery / charging state

Credential & data theft

- Chromium browsers (Chrome / Edge / Brave / Opera / Vivaldi): passwords, cookies, autofill, credit cards, history, downloads == v10 + v20 decryption, per-profile
- Firefox / NSS: logins (empty-password profile), key4.db
- Discord token extraction (client + all Chromium browsers, leveldb scan)
- Telegram Desktop: tdata discovery + exfil
- Wallet recovery: Exodus, Electrum, Atomic, Coinomi, Guarda, Ledger Live, Trezor Suite, Bitcoin, Monero + browser extension wallets (MetaMask, Phantom)
- One-command desktop + documents grab (zip)
- Program list / installed software

Execution & control

- Remote PowerShell / CMD
- Process manager = list, kill, path
- File manager = list, copy, delete, download, upload
- SendKeyPress
- Message boxes

- Wallpaper set
- Open URL in default browser
- Minimize / maximize all windows

System

- Full recon - CPU, GPU, RAM, country, city, IP, MACs, HWID
- Shutdown / restart / hibernate / logoff
- Blue Screen of Death
- Privilege elevation (UAC + elevated reconnect)
- Self-uninstall (soft + hard)
- Emergency backup / self-heal

Persistence & evasion

- Self-install to `%APPDATA%\Microsoft\Crypto\<rand>\`
- Persistence: Run key + scheduled task (both names configurable)
- Anti-VM (MAC prefixes, process names)
- Anti-debug (IsDebuggerPresent, PEB)
- Periodic sandbox re-check mid-session
- Self-delete of original from temp/download paths

Licensing

- ed25519 signed licenses, verified against an embedded public key
- Three plans: subscription (30-day issue) or yearly or lifetime
- Builder stamps the license; implant refuses to run without a valid one
- Clock-tamper documented, relay-side enforcement coming

Uploading more screenshots soon

/align]

[align=center]

In progress — landing soon

- Chrome App-Bound Encryption bypass. Chrome 127+ wraps cookies and passwords with a key that a normal process can't unwrap. RedLotus is getting the injection-based IElevator path - the same technique the top-tier tools use - to pull the ABE key from inside the browser. Until it lands: passwords and cookies from pre-127 Chrome, and all other browser data, work today.
 - tdata in-process parse. Currently zips the tdata directory for offline parsing. Live session extraction in the next build.
 - Relay deploy toolkit. `wss://` TLS, systemd/service install, one-page VPS setup.
- Pricing

| Plan | Price |

|---|---|

| Subscription | \$99 first month, then \$20/month |

| Yearly | \$199 1 year updates |

| LIFETIME | \$501 | (REFUND PROVIDED FOR THIS PLAN IF NOT SATISFIED IN 1-2 MONTHS.

Both include:

- Relay binary + builder
- All current features
- All future updates (subscription = active sub only; lifetime = forever)
- Setup help on your first VPS

No hidden fees. No per-victim pricing. You host, you own, you control.

What you need

- A VPS (any \$5 provider works - Hetzner, [censored], DigitalOcean, OVH)
- A Telegram bot (BotFather, 30 seconds)
- A Windows target (Windows 7+)

Everything else is in the package.

FAQ

Do I need to host anything for you?

No. The relay runs on your VPS, with your bot token. Nothing routes through us.

How does the relay know which victim is which?

Stable ID derived from machine GUID + hostname + username. Reconnects keep the same ID.

`/online` lists them all.

Will it survive reboots?

Yes - dual persistence (Run key + scheduled task), plus an emergency backup that re-asserts install if the primary is removed.

Is the browser data extraction working?

Pre-127 Chrome: full. Post-127 (ABE): passwords + cookies are the in-progress item - everything else (history, autofill, cards, downloads, Firefox, Discord, Telegram, wallets) works today. ABE bypass is actively being finished and ships to licensed users at no cost.

OPSEC?

Relay outbound-only from victim. No inbound ports on the target. No shared infrastructure. Victim executable is static, no runtime dependencies.

Contact

DM for purchase, trials, or questions. Serious buyers only — no time-wasters. Vouches available from existing users on request.

Telegram: @defimirai

Session: 054de147087a1dee16dedaebb10a9558cc8f3ce445f9ca430142c60e3a759c7939

[contract=tid]Start Contract[/contract]

Freddy Kru?ger - October 9, 2026, 7:35 am

Good luck with sales champ.

Infinity. - *October 9, 2026, 11:15 pm*

(Oct 9, 2026 07:35 AM)Freddy Kru?ger Wrote: [\[CITE\]](#) Good luck with sales champ.
Thanks a ton mate, sending you a DM

Infinity. - *October 15, 2026, 9:17 am*

Sorry I had forgotten to add Builder screenshots, added them now