

Forum:[Hack Forums](#)

Thread: [\[Umbra Vision RAT\] Can infect Windows, MacOS & Linux](#)

D 3 I M 0 S - September 26, 2026, 6:48 pm

[Video: <https://youtu.be/zpuoS1n5Wks>]

Core Features [+] Native compiled wrapper via Go shim (win_x64, lnx_x64, lnx_arm64, osx_arm64, osx_x64)

- [+] True cross-platform native support across Windows, macOS, and Linux
- [+] 18 on-demand modules (in-memory only, loaded reflectively, nothing drops to disk)
- [+] Modular architecture (activate only what the operation requires)
- [+] End-to-end encrypted Custom Binary Protocol operating over SOCKS5 / TCP
- [+] Multi-client management server console with live telemetry and session overviews
- [+] Zero-configuration Tor Hidden Service integration (v3 .onion)
- [+] Automatic Tor SOCKS5 Gateway Tunneling
- [+] Adaptive Dual-Transport Layer (Seamlessly switches between Onion Routing and Direct TCP)
- [+] Two-Stage Dropper decouples initial access vector from the core payload
- [+] Full Unicode support for all languages and regions

Remote Control & Surveillance

- [+] Hidden Virtual Desktop (hVNC)
- [+] File Manager (fully featured remote browsing, transfer, upload, and execution)
- [+] Task Manager (live process listing, suspend, kill, and injection capabilities)
- [+] Advanced Keylogger (real-time live streaming with offline buffering & bulk exfiltration)
- [+] Webcam Capture (silent image snapshotting and live video streaming)
- [+] Live Microphone (real-time environmental audio capture and streaming)
- [+] Registry Manager (full read/write/delete capabilities across all hives)
- [+] Startup Manager (dynamic persistence control from the server)
- [+] Reverse Proxy (pivot the compromised host into a network exit node)
- [+] Interactive Shell (full reverse shell and terminal access)
- [+] Desktop Surveillance (live active desktop screenshot capture and streaming)
- [+] Power Controls (remote shutdown, restart, and sleep execution)
- [+] Network Spreader (automated movement across local networks)
- [+] USB Spreader
- [+] Fleet Updater (hot-swap payloads dynamically across your entire node network)

Advanced Persistence

- [+] Windows: Registry-based autorun and scheduled tasks
- [+] macOS: LaunchAgent plist under ~/Library/LaunchAgents/
- [+] Linux: systemd user unit injection and crontab cascades

Evasion & Anti-Analysis

- [+] Process Hollowing (in-memory execution within trusted process hosting)
- [+] AMSI Patching (runtime bypass of the Antimalware Scan Interface)
- [+] ETW Bypass (Event Tracing for Windows suppression)
- [+] NTDLL Unhooking (dynamic removal of security tool hooks)
- [+] macOS Gatekeeper Bypass (automated quarantine attribute stripping & ad-hoc codesigning)

- [+] Linux Evasion (ptrace TRACEME and advanced container detection)
- [+] Multi-Layer Anti-Analysis (comprehensive Anti-VM, Anti-Sandbox, and Anti-Debug checks)
- [+] Benign Masquerading (detached execution under deterministic OS daemon names)
- [+] Polymorphic Engine (dynamically mutates signature and structure upon deployment)
- [+] Build-Time Crypter (absolute cryptographic obfuscation unique to every single build)

Intelligence Gathering & Privilege Escalation

- [+] UAC Bypass
- [+] Credential Harvesting (extracts saved passwords, cookies, and tokens from all major browsers)
- [+] Crypto Wallet Stealer
- [+] Ransomware Engine

Builder & Deployment

- [+] Dynamic Obfuscation (unique encryption of strings, configs, and payloads per build)
 - [+] LNK Wrappers
 - [+] Agent Binding (EXE, Word, Excel & PDFs)
- Monero only payments accepted.

- [+] 1 MONTH: \$350
- [+] 3 MONTHS: \$700
- [+] 1 YEAR: \$2,925

Middleman/escrow services are welcome at your own expense.

ONLY Contacts:

Signal: @deimos.09

Telegram: @D_3_I_M_0_S

Latest scan with antiscan me

? loading encrypted image... [contract=tid]Start Contract[/contract]

uncle red - September 27, 2026, 11:32 am

no video no vouches just trying to scam users

Astraviruzz - September 27, 2026, 11:33 am

vouch copy available ?

D_3_I_M_0_S - September 27, 2026, 11:36 am

(Sep 27, 2026 11:33 AM)Astraviruzz Wrote: [\[CITE\]](#) vouch copy available ?

I can setup a trial license, send me a message.

(Sep 27, 2026 11:32 AM)uncle red Wrote: [\[CITE\]](#) no video no vouches just trying to scam users
Lol chill. Anyone who asked for a vouch got offered a trial, and I just uploaded a video. Way too quick to scream 'scam' bro.

Binance - September 28, 2026, 9:15 am

Law enforcement is going to bend you over raw for just one of those screenshots.

Transporter007 - September 28, 2026, 6:56 pm

Vouch copy available ?

D_3_I_M_0_S - September 28, 2026, 10:41 pm

(Sep 28, 2026 06:56 PM)Transporter007 Wrote: [\[CITE\]](#) Vouch copy available ?
Yes, a trial license is available, hit me up and il set you up

DarkCore - September 30, 2026, 1:15 am

Was this created with 1 prompt? pd; saw some similarities with my thread

cltrade - September 30, 2026, 7:11 am

Does it also grab credentials from email clients?

Can I have a vouch?

D_3_I_M_0_S - September 30, 2026, 9:58 am

(Sep 30, 2026 01:15 AM)DarkCore Wrote: [\[CITE\]](#) Was this created with 1 prompt? pd; saw some similarities with my thread

I might have taken some thread styling inspiration from you xD

(Sep 30, 2026 07:11 AM)cltrade Wrote: [\[CITE\]](#) Does it also grab credentials from email clients?

Can I have a vouch?

Yes it does, i do offer trials. Hit me up

CompulsivePurchaser - October 1, 2026, 10:54 am

Is it a working, defender fud USB auto run?

D_3_I_M_0_S - October 1, 2026, 3:31 pm

(Oct 1, 2026 10:54 AM)CompulsivePurchaser Wrote: [\[CITE\]](#) Is it a working, defender fud USB auto run?

Yes

D_3_I_M_0_S - October 5, 2026, 5:10 pm

Uploaded a longer video of Umbra, removed images from the post as they were no longer needed due to the showcase video.

CL1B - October 7, 2026, 4:54 am

(Sep 30, 2026 09:58 AM)D_3_I_M_0_S Wrote: [\[CITE\]](#) I might have taken some thread styling inspiration from you xD

Classic modern day skid activities ?

#MakeMalwareGreatAgain

Invictus100 - October 7, 2026, 3:56 pm

(Sep 28, 2026 06:56 PM)Transporter007 Wrote: [\[CITE\]](#) Vouch copy available ?
Did you test? You can put honest feedback here

D_3_I_M_0_S - October 7, 2026, 6:01 pm

(Oct 7, 2026 04:54 AM)CL1B Wrote: [\[CITE\]](#) Classic modern day skid activities ?

#MakeMalwareGreatAgain

Please do enlighten us c0d3 g0d ?

Stanley - October 13, 2026, 9:57 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP

(Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley