

Forum:[Hack Forums](#)

Thread: [x47.c FASTFLUX BOTNET \[C\]\[NATIVE\]\[RK + WD BYPASS\] \[AI API STEALTH\]](#)

WraithTools - August 3, 2026, 10:38 am

x47.c - Fast Flux Edition

THE PLATFORM

x47.c is a private Windows botnet stack built for operators who refuse to lose bots, refuse truncated loot, and refuse toy panels. Compact stub. Full C2GUI. Fast Flux multi-domain C2 that keeps check-ins alive when a hostname or IP blips. Revolutionary AI Stealth that thinks for the bot and repairs survival on the host. Eighteen-type DDoS including AI API draining. Stealer, SOCKS5, rootkit, botkiller - the full plugin suite in one package.

Technical report

Full architecture / commands / modules write-up:

<https://paste.rs/M8bre>

WHAT SHIPSC2GUI (desktop operator UI - Fast Flux tab, no toy web dashboard)

Matching C2 server for your Ubuntu VPS (HTTPS bots + WebSocket C2GUI + live terminal CLI)

1 custom bot build with 3-10 Fast Flux domains (rotate + multi-A DNS + sticky IP)

Output format choice: EXE, standalone DLL, or both from the same build

1 free rebuild if you need a domain/auth correction or a fix on our side

Modules unlocked to match what you buy (base or full stack)

You provide domains (and your xAI API key for AI Stealth). We deliver the build, server package, and C2GUI access. Builds stay with us.

WHY OPERATORS BUY THISFast Flux C2 - 3-10 operator domains, multi-A resolve, sticky last-good IP, optional flux_ips hints from C2

Revolutionary AI Stealth that keeps bots alive without babysitting every host

EXE + standalone DLL output - drop either form, or both; DLL never depends on the EXE

Full plugin suite: rootkit, SOCKS5, stealer, DDoS, botkiller, persistence, stealth

C2GUI - purpose-built control surface, not a generic dashboard

Live C2 terminal with join/leave panels and fleet status

Tiny hardened Windows stub designed to survive and report (x86 PE - runs on x86 and x64 Windows)

REVOLUTIONARY AI STEALTH

Most loaders "hide once" and hope. x47.c runs a continuous AI stealth monitor on the bot itself. Bot phones home to xAI / Grok with your API key (you bring the key)

Host is scored: persistence present? file hidden? sandbox signals? admin? hollowed?

AI returns allowlisted remediation ops only - no reckless free-form shell

Ops include: repair persistence, rehide file, reapply rootkit, reapply WD exclusion, anti-debug, controlled sleep, noop

If install paths or stealth state break, the bot repairs itself on a jittered schedule

Fallback local remediation if the API blips - survival does not depend on a perfect round-trip

Status events stream to the C2GUI Stealth view so you see what the AI applied

Result: bots that heal. Persistence that comes back. Concealment that re-applies. You keep the fleet alive while competitors watch installs rot after the first cleanup.

FAST FLUX C2 - ACCESS THAT OUTLASTS A SINGLE HOSTNAME

One fixed domain is a single point of failure. x47.c Fast Flux rotates across your operator domain set on every check-in path.

3-10 domains patched into the bot + matching server

Multi-A DNS resolve per domain - shuffle and try; stick to the last-good IP

Optional flux_ips hints from C2 (online bot public IPs) merged into the rotate set

HTTPS C2 with Host/SNI = active domain; SOCKS reverse uses sticky C2 IP:8445

C2GUI Fast Flux tab - configured domains, IP pool, per-bot sticky host/IP

One VPS is enough - point all flux A records at your C2 (short TTL recommended)

This is the difference between "domain burned, fleet gone" and "next domain still answers."

DDoS ENGINE - FULL ARSENAL

Eighteen attack types. Launch and stop from the C2GUI on selected bots.

HTTP flood / HTTP raw / HTTP random

Cloudflare and UAM bypass paths

Slowloris

TCP flood / UDP flood / SYN flood

TLS and raw socket stress

GRE

Amplification: DNS, NTP, SSDP, Memcached

Generic stress mode

AI API drain - burn OpenAI / xAI / compatible chat APIs with heavy completion traffic (token and cost pressure, not just bandwidth)

Controlled targeting. No accidental whole-fleet fire unless you choose it. Stop is first-class.

FULL PLUGIN SUITE

Rootkit

Deeper host concealment on top of base stealth. Harder to spot. Harder to rip out. Re-applicable via AI Stealth when enabled.

SOCKS5 reverse proxy

Turn bots into authenticated SOCKS5 exits through NAT. Reverse tunnel to C2, public entry ports, username/password (RFC 1929). Panel SOCKS tab + health checks. Browse and route through live bots.

Stealer

On-demand harvest (steal_all): Chromium login patterns, wallets, Discord/Telegram, AI-site tokens. Full JSON exfil to C2 - not truncated junk. Logs on disk + live Stealer view in C2GUI.

Botkiller

Scan and clean competing malware artifacts so your bot owns the box.

Persistence + base stealth

Install, survive reboot, stay quiet. Fast Flux register/heartbeat. Commands: dl/exc, update, uninstall, and more.

EXE / DLL dual output

Each build can emit EXE only, DLL only, or both. Same C2, auth, and IOCs. The DLL is fully standalone (rundll32 load) - it does not load or need the EXE. Choose the drop format that fits the host; ship both when you want options.

DDoS

Eighteen attack types from the C2GUI on selected bots or broadcast: HTTP flood / raw / random, Cloudflare and UAM paths, Slowloris, TCP / UDP / SYN flood, TLS and raw socket stress, GRE, amplification (DNS, NTP, SSDP, Memcached), generic stress, and AI API drain - heavy completion

traffic against OpenAI / xAI / compatible chat APIs for token and cost pressure, not just bandwidth. Launch and stop are first-class; targeting stays under your control.

AI Stealth

Continuous host monitor via your xAI / Grok API key. Scores persistence, hide state, sandbox signals, admin, and hollow status, then applies allowlisted remediation only (repair persistence, rehide, reapply rootkit / WD exclusion, anti-debug, controlled sleep, noop). Jittered self-repair plus local fallback if the API blips. Status streams to the C2GUI Stealth view.

CUSTOM C2 PANEL Bot list, filters, multi-select

Bot Details - OS, geo, SOCKS, Fast Flux sticky host/IP

Console for typed commands

SOCKS5 tab

Fast Flux tab (domains - flux_ips pool - sticky table)

Stealer Logs

Stealth / AI status

DDoS launcher

Mobile status page (/hud)

C2 SERVER Ubuntu-ready deploy (setup scripts + full setup guide)

TLS

Auth-gated REST + WebSocket for C2GUI

SOCKS reverse relay (:8445)

Interactive CLI - banner, live joins, status / bots / proxies / help

Runs beside an existing website on a free port (e.g. 8443) if needed

DELIVERY You provide: 3-10 C2 domains (+ xAI API key if taking AI Stealth)

We deliver: 1 patched bot build (EXE, DLL, or both) + matching C2 package + C2GUI access

Included: 1 free rebuild (domain/auth correction or our defect)

Extra rebuilds / domain swaps billed separately

PRICING

Base Loader - \$200

Fast Flux C2, basic commands, botkiller

C2GUI + C2 server

1 build - 3-10 domains - 1 free rebuild

Additional modulesRootkit (RK) - \$100

SOCKS5 - \$200

DDoS - \$150

AI Stealth (xAI API key required) - \$300

Stealer - \$350

Full Stack - \$950

Base + every module above

Fast Flux C2, AI Stealth, DDoS arsenal, SOCKS5, stealer, rootkit, botkiller

C2GUI - multi-domain build - 1 free rebuild

Technical report

Full architecture / commands / modules write-up:

<https://paste.rs/M8bre>

Contact for delivery.

[contract=tid]Start Contract[/contract]

cscscs666 - August 6, 2026, 3:39 am

If you can attack and take down websites, please send me your contact info

WraithTools - August 6, 2026, 12:29 pm

(Aug 6, 2026 03:39 AM)cscscs666 Wrote: [\[CITE\]](#) If you can attack and take down websites, please send me your contact info

We do not condone the use of this botnet for anything other than educational purposes only. It is just a tool that shows how modern malware has evolved and shows examples of modern AI stealth monitoring and attacks.

HF also does no way condone this behavior

WraithTools - August 12, 2026, 11:31 pm

If you know about botnets and are willing to write a thorough review after properly testing it, we have

2 vouch copies available for this. It is designed to be the most resilient botnet on the market and our Ai powered stealth and our own DDoS method is great for stress testing your vibe coded projects!

Stanley - *September 7, 2026, 11:13 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

ViperPrivacy - *September 19, 2026, 1:40 am*

is this botnet with hosting or without hosting?
a Will vics become flux_ips?

WraithTools - *September 19, 2026, 7:10 am*

(Sep 19, 2026 01:40 AM)ViperPrivacy Wrote: [\[CITE\]](#) is this botnet with hosting or without hosting?
a Will vics become flux_ips?

No, for that you want the p2p version of this. They both use a custom C2 as the server, in the P2P version bot's become peers, but it's hybrid not entirely server-less, but if server goes down you can inject into the whole mesh to update the server. With Flux, you make the domains first and they rotate automatically