

Forum:[Hack Forums](#)

Thread: [x47.c LOADER FAST FLUX EDITION \[C\] STEALTHY PERSISTENT](#)

WraithTools - April 1, 2026, 9:56 am

Technical Analysis: x47.c Fast Flux Domain Edition

Family: x47.c

Variant: Fast Flux Domain Edition

Platform: Windows (x86/x64)

Language: Pure C (bot), C++/Qt (operator GUI), Node.js (C2 server)

Overview

x47.c Fast Flux Domain Edition is a modular HTTP-based botnet built around fast flux DNS infrastructure for maximum C2 resilience. The bot is written in pure C with zero runtime dependencies, uses process hollowing for stealth, and cycles through multiple operator-controlled domains with automatic failover. Two independent layers of resilience — DNS-level IP rotation and bot-side domain rotation — ensure the botnet survives partial takedowns, IP blocks, and domain seizures.

Architecture

The system runs on a four-tier model: bots, DNS, proxy nodes, and the operator layer.

Bots communicate outbound over HTTPS to one of several hardcoded domains. Each domain is configured with very short DNS TTL values so the IPs behind them rotate constantly. Those IPs are disposable proxy nodes that forward traffic to the real C2 server. The operator's true server IP is never exposed.

The operator controls everything through a Qt GUI connected to the C2 via WebSocket. The GUI includes a bot management panel and a live Domain Monitor showing which domains are healthy and how many bots are reaching each one.

Bot Behavior

On first run the bot performs process hollowing into svchost.exe for stealth. The hollowing is fully ASLR-aware and works on both x86 and x64 targets. Once migrated, the original binary exits and the bot continues running inside a legitimate-looking system process.

Persistence is established via a file copy to AppData and a registry Run key. Both are self-healing

— re-checked and re-written every check-in cycle, so manual removal is ineffective unless the process itself is killed.

The binary is compiled with no C runtime. All string, memory, and JSON parsing functions are hand-written. This keeps the binary small with a minimal import table.

Fast Flux Domain Rotation

The bot holds an array of domains and a current index. Every check-in it tries the current domain over HTTPS. If the connection fails for any reason it immediately rotates to the next domain and retries. This walks through the entire list before giving up for that cycle.

Once a domain succeeds the bot stays on it until it fails again. The botnet naturally converges on whichever domains are alive.

Resilience comes from two layers working together:

DNS-level — Each domain uses short TTL DNS that returns different proxy IPs on every query. Blocking one IP does nothing because a new one appears within a minute.

Domain-level — If an entire domain is seized or sinkholed, bots fall through to the next one within seconds. Domains spread across different registrars and TLDs means a full takedown requires simultaneous coordination across all of them.

In practice: one domain goes down, bots rotate to the next, and the operator sees the dead domain turn red on the Domain Monitor while the remaining domains absorb the traffic.

C2 Communication

Bots check in via HTTPS POST to a /gate endpoint with a JSON body containing an auth key, bot ID, OS info, and which domain they connected through. The server responds with any pending commands.

Supported commands include download-and-execute, bot update, uninstall, and botkiller scan/clean. Command results are reported back through the same /gate endpoint using the same domain rotation for delivery reliability.

User-Agent is spoofed as a common browser string to blend with normal HTTPS traffic.

C2 Server

Node.js application handling bot HTTP endpoints and operator WebSocket connections. Maintains an in-memory bot registry tracking status, country, version, and which flux domain each bot last used.

Domain stats are computed live and pushed to the GUI on every bot event — no polling needed on the operator side.

Operator GUI

Qt-based control panel with two tabs:

Bots — Lists all connected bots with OS, country, unique ID, online/offline status, and which flux domain they're reaching through. Supports single-target commands or broadcast to all.

Domain Monitor — Live table showing each flux domain with bot count, last check-in time, and color-coded health status. Green means active, yellow means recently seen but stale, red means down. Summary bar shows how many domains are currently alive.

PRICE

LIFETIME INCLUDING SERVER FILES \$700

1 MONTH (HOSTED) \$200

3 MONTHS (HOSTED) \$400

Start contract or PM please

[contract=tid]Start Contract[/contract]