# ShadowV2 Botnet Exposes Rise of DDoS-as-a-service Platforms - Against

Data: 2025-09-25 12:18:45

Autor: Inteligência Against Invaders

A new campaign that combines traditional malware with modern DevOps tooling has been observed

by cybersecurity analysts.

TheShadowV2 DDoS operation, discovered by Darktrace, uses a command-and-control framework hosted on GitHub CodeSpaces, a Python spreader that performs multi-stage Docker deployments for initial access and a Go-based remote access trojan that registers and polls a RESTful API to receive commands.

## Initial Access and Deployment

The initial compromise originates from a Python script running in GitHub CodeSpaces, identifiable by headers such as User-Agent: docker-sdk-python/7.1.0 and X-Meta-Source-Client: github/codespaces, and outbound connections from IP address 23.97.62[.]139.

Attackers target exposed Docker daemons on AWS EC2, spawning a temporary setup container, installing tools in it, imaging that container, then deploying a live instance with malware passed via environment variables. This build-on-victim method may reduce forensic artifacts.

“This research points to a maturing criminal market where specialization beats sprawl,” Jason Soroko, senior fellow atcertificate authority, Sectigo, said. “By focusing only on DDoS and selling access to capacity, the operators reduce operational risk, simplify tooling and align incentives with paying customers.”

## Malware Behaviour and Attack Methods

Once live, the Go binary phones home using MASTER_ADDR and VPS_NAME, derives a unique VPS_ID, then maintains two loops: it sends a heartbeat every second and polls for commands every five seconds.

Researchers emulated the implant to capture commands that instruct HTTP2 rapid reset and high-thread HTTP floods, for example, a 120-thread attack against a target hosted in Amsterdam.

The attack client uses Valyala’s fasthttp library and supports flags for random query strings, spoofed forwarding headers, a Cloudflare under-attack-mode bypass using a bundled ChromeDP, and an HTTP2 rapid reset mode that amplifies request throughput.

Read more on Cloudflare bypass techniques: Cloudflare and Palo Alto Networks Victimized in

“The ShadowV2 botnet is another reminder that cybercrime is no longer a side hustle, but an industry,” Shane Barney, CISO at Keeper Security, said. “Threat actors are treating Distributed Denial-of-Service (DDoS) attacks like a business service, complete with APIs, dashboards and user interfaces.”

## API, UI and Platform Design

The campaign exposes an OpenAPI spec implemented with FastAPI and Pydantic, a full login panel and an operator UI built with Tailwind.

The API shows multi-tenant features, privilege distinctions and endpoints to launch attacks that require a list of zombie systems. The site presents a fake seizure notice, yet still reveals an “advanced attack platform” at its login. Key features include:

- Python C2 hosted in CodeSpaces
- Docker-based spreader with on-host image build
- Go RAT with RESTful registration and polling
- DDoS options, including HTTP2 rapid reset and UAM bypass

Darktrace framed this as cybercrime-as-a-service that mirrors legitimate cloud-native apps.

“The presence of a DDoS-as-a-service panel with full user functionality further emphasizes the need for defenders to think of these campaigns not as isolated tools but as evolving platforms,” the cybersecurity firm wrote.

“For defenders, the implications are significant. Effective defense requires deep visibility into containerized environments, continuous monitoring of cloud workloads and behavioral analytics capable of identifying anomalous API usage and container orchestration patterns.”