CLASSIFIED // EYES ONLY // RED TEAM ACCESS

DIMITAR PRODROMOV

OFFENSIVE SECURITY ENGINEER // TOOLING ARCHITECT

[E] papica777@gmail.com

[L] linkedin.com/in/dimitar-prodromov-1818b3399

[W] qantum-fortres.github.io

[G] github.com/qantum-fortres

[L] Sofia, Bulgaria

0x01 // MISSION STATEMENT

Elite Security Researcher and Engineer who doesn't just find vulnerabilities—I build the **autonomous systems** that find them. Architect of the **QAntum Vortex**, a custom offensive security OS capable of high-frequency exploitation, polymorphic defense evasion, and AI-driven logic auditing. Seeking to deploy this arsenal for the **Synack Red Team** to uncover critical vulnerabilities in high-value targets.

0x02 // THE ARSENAL (CUSTOM TOOLING)

GHOST PROTOCOL (WAF EVASION)

Designed a polymorphic network layer that rotates **JA3 TLS Fingerprints** (Chrome, Firefox, Safari) and traffic patterns to bypass advanced WAFs (Cloudflare/Akamai) during active scanning.

AI AGENT EXPERT ("THE BRAIN")

built a sovereign AI module using recursive **Chain-of-Thought** reasoning (Opus-level) to automatically analyze code logic, detect zero-day vulnerabilities, and generate proof-of-concept exploits without human intervention.

ATOMIC HFT ENGINE

Engineered a sub-microsecond **High-Frequency Trading engine** (Node.js/C++) capable of race condition exploitation and high-throughput

10 GUARDIANS (DEFENSE IN DEPTH)

Orchestrated a squad of 10 specialized autonomous agents (Red/Blue/Purple) to continuously audit and self-heal the ecosystem, simulating a live **Purple Team** environment for 24/7 security verification.

network syncing, adaptable for DDoS simulation and stress testing.

0x03 // OPERATIONAL EXPERIENCE

Senior Security Engineer & Architect

QANTUM EMPIRE (Stealth)

2023 - PRESENT // Remote

>> Architected **QAntum Vortex**, a monolithic security and trading OS with over 500+ modules and 10 autonomous agents.

>> Developed **"God Mode"** arsenal scripts for automated reconnaissance, vulnerability scanning, and deep-archive data retrieval.

>> Implemented military-grade encryption (AES-256) for the **Omega Vault**, securing sensitive neural weights and API keys.

>> Conducted continuous internal **Red Team engagements** against the system's own defenses to harden the "Fortress" architecture.

Senior QA Automation Engineer

DRAFTKINGS INC.

2021 - 2023 // Sofia, Bulgaria

>> Led automation strategy for high-volume betting platforms, ensuring 99.99% uptime under load.

>> Developed custom testing frameworks (C#/JS) that mirror **fuzzing methodologies** to uncover edge cases in betting logic.

>> Collaborated with InfoSec teams to integrate security checks into the CI/CD pipeline (DevSecOps).

0x04 // TECHNICAL PAYLOAD

OFFENSIVE

Burp Suite Pro, Metasploit, Nmap, SQLMap, Fuzzing, Exploit Dev (Python/JS), Race Conditions, IDOR, XSS, WAF Bypass.

ENGINEERING

TypeScript, Node.js (V8 Internals), C++, Python, React/Next.js, Docker, Kubernetes, AWS/Azure Cloud Security.

INTELLIGENCE

LLM Integration (OpenAI/Anthropic/Google), RAG

CERTIFICATIONS

(Pending) OSCP Preparation, Advanced Web Attacks and Exploitation (AWAE) Methodology.

Architecture, Vector Databases (Pinecone), Autonomous Agents.