
CyberStrikeAI: The Tool Behind FortiGate Campaign

CyberStrikeAI: The Open-Source Tool That Automates Hacking with AI Agents

The same threat actor that breached hundreds of Fortinet FortiGate firewalls in a recent AI-assisted campaign has been linked to an open-source security testing platform called CyberStrikeAI. CyberStrikeAI integrates over 100 security tools with an intelligent orchestration engine, enabling even low-skilled operators to automate full attack chains against exposed edge devices.

CyberStrikeAI and the FortiGate Campaign

Last month, we reported on an AI-assisted hacking operation that compromised more than 500 FortiGate devices in five weeks. The threat actor behind the campaign used multiple servers, including a web server at IP address 212.11.64[.]250.

In a new investigation, researchers identified a "CyberStrikeAI" service banner running at that same IP address. They observed network communications between the server and the Fortinet FortiGate devices the threat actor targeted.

What Is CyberStrikeAI?

CyberStrikeAI describes itself as an "AI-native security testing platform built in Go." Its features include:

- Integration with 100+ security tools, including nmap, masscan, sqlmap, nikto, gobuster, Metasploit, pwntools, hashcat, John the Ripper, mimikatz, BloodHound, and Impacket.
- An intelligent orchestration engine that automates attack workflows.
- Predefined security roles and a skills system for structured operations.
- Native MCP protocol and AI agents enabling end-to-end automation from conversational commands to vulnerability discovery.
- Attack-chain analysis, knowledge retrieval, and result visualization with full audit logging.
- AI decision engine compatible with models like GPT, Claude, and DeepSeek.
- Password-protected web UI with SQLite persistence and a dashboard for vulnerability management.

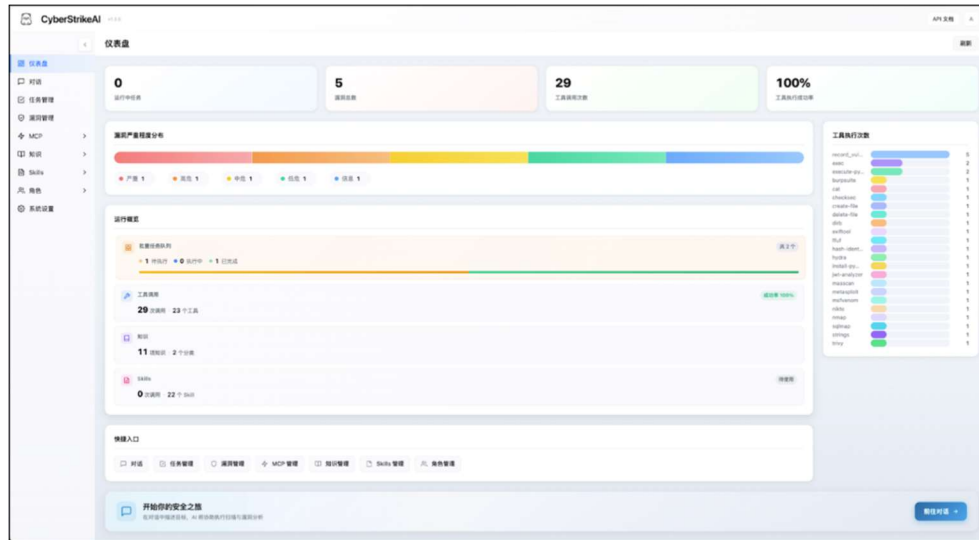


Figure 1 CyberStrikeAI Dashboard from GitHub

How Attackers Use It?

By combining these tools with AI agents and an orchestrator, CyberStrikeAI enables operators to:

- Conduct network scanning and reconnaissance.
- Perform web and application testing.
- Launch exploitation frameworks.
- Run password cracking and post-exploitation tools.
- Automate the entire attack chain against targets with minimal manual intervention.

The tool essentially packages decades of offensive security tooling into an AI-powered interface that any operator can direct through conversational commands. Between January 20 and February 26, 2026, researchers observed 21 unique IP addresses running CyberStrikeAI. Servers were primarily hosted in China, Singapore, Hong Kong, and additional infrastructure was spotted in the United States, Japan, and Europe.

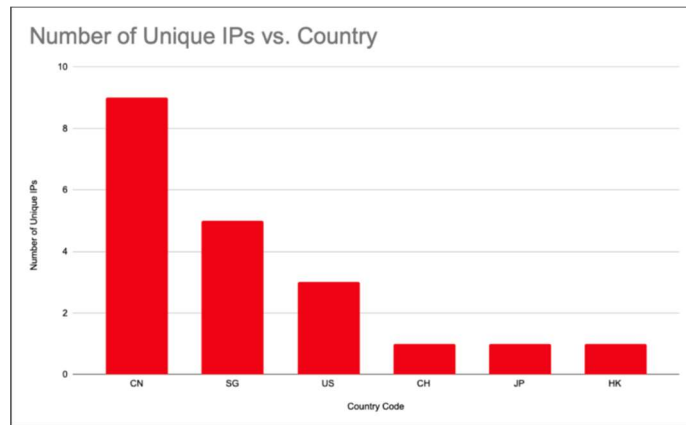


Figure 2 Country code statistics on number of unique IPs hosting CyberStrikeAI servers – Source: Team-cymru

The Developer

The CyberStrikeAI developer's GitHub profile reveals a focus on AI-assisted security tools. Other projects include:

- PrivHunterAI: Uses AI models to detect privilege escalation vulnerabilities.
- InfiltrateX: A privilege escalation scanning tool.

Repositories are primarily written in Chinese, suggesting a Chinese-speaking developer. The era of AI-powered offensive tooling is here. CyberStrikeAI is just the beginning.

Related IP addresses





Indicator	Description	ASN	Organization	GeoIP	Last Seen
103.164.81.110	CyberStrikeAI Server	142002	SCLOUDPTELD-AS Scloud Pte Ltd, SG	SG	02/02/2026
106.52.47.65	CyberStrikeAI Server	45090	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN	CN	25/02/2026
115.120.233.95	CyberStrikeAI Server	55990	HWCSNET Huawei Cloud Service data center, CN	CN	26/02/2026
117.72.103.145	CyberStrikeAI Server	141679	CHINATELECOM-IDC- BTHBD-AP China Telecom Beijing Tianjin Hebei Big Data Industry Park Branch, CN	CN	23/02/2026
118.25.186.119	CyberStrikeAI Server	45090	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN	CN	24/02/2026
142.171.160.137	CyberStrikeAI Server	35916	MULTA-ASN1 - MULTACOM CORPORATION, US	US	29/01/2026

Indicator	Description	ASN	Organization	GeoIP	Last Seen
144.31.224.253	CyberStrikeAI Server	215439	PLAY2GO-NET, GB	US	26/02/2026
146.190.195.154	CyberStrikeAI Server	14061	DIGITALOCEAN-ASN - DigitalOcean, LLC, US	SG	23/01/2026
146.190.82.132	CyberStrikeAI Server	14061	DIGITALOCEAN-ASN - DigitalOcean, LLC, US	SG	24/01/2026
154.219.114.92	CyberStrikeAI Server	401701	COGNETCLOUD-2 - cognetcloud INC, US	HK	12/02/2026
212.11.64.250	CyberStrikeAI Server	42624	SWISSNETWORK02, SC	CH	30/01/2026
38.38.250.182	CyberStrikeAI Server	139659	LUCID-AS-AP LUCIDACLOUD LIMITED, HK	US	25/01/2026
43.106.25.225	CyberStrikeAI Server	45102	ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN	SG	31/01/2026
43.167.237.212	CyberStrikeAI Server	132203	TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue, CN	SG	01/02/2026
47.101.186.156	CyberStrikeAI Server	37963	ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd., CN	CN	25/02/2026
47.95.33.207	CyberStrikeAI Server	37963	ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Ltd., CN	CN	26/02/2026

Indicator	Description	ASN	Organization	GeoIP	Last Seen
60.204.227.64	CyberStrikeAI Server	55990	HWCSNET Huawei Cloud Service data center, CN	CN	08/02/2026
62.234.61.215	CyberStrikeAI Server	45090	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN	CN	25/02/2026
64.176.48.93	CyberStrikeAI Server	20473	AS-VULTR - The Constant Company, LLC, US	JP	24/02/2026
81.70.144.252	CyberStrikeAI Server	45090	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN	CN	26/02/2026
2400:d321:2308:1461::1	CyberStrikeAI Server	141995	CAPL-SG Contabo Asia Private Limited, SG	SG	26/02/2026

Ready to see how AICenturion can secure you against AI risks?
 Request a demo today: hello@cytex.io

Connect with our social media channels

			
https://cytex.io	hello@cytex.io	@cytexsmb	@cytexsecure