TECH SPOTLIGHT HUMAN SECURITY

Adapting to AI-driven bot threats

Strategies for safeguarding public sector government data

Bots were once simple tools — tiny bits of code built to automate menial digital tasks. But today's bots are far from basic. In fact, many are dangerously intelligent.

Today's AI-powered bots use machine learning and natural language processing to better understand and interact with systems, bypassing traditional security defenses like CAPTCHA with higher sophistication.

Bots increasingly target government entities whose sprawling digital ecosystems and often outdated security infrastructure present high-value targets for adversaries seeking to disrupt services, steal data or undermine trust.

As bots continue to evolve, the risk to the government grows. Combating these threats requires more than reactive defenses. It demands modernization, cross-sector collaboration, and proactive threat intelligence.

Smarter bots, bigger risks

According to The Quadrillion Report: 2025 Cyberthreat Benchmarks, account fraud attacks rose dramatically in 2024. On an individual company level, post-login compromises detected by the Human Defense Platform more than doubled compared to the previous year. At the same time, fake account creation attempts surged dramatically, increasing by over 360%.

But account takeover is only one tactic in a growing arsenal.

"AI-driven agents are much more capable of mimicking human behaviors and learning and adapting their threat vectors over time," said Joe Rogers, Vice President of Public Sector at HUMAN Security. "We see AI-powered bots conducting sophisticated attacks like credential stuffing, phishing, DDoS and other kinds of attacks aimed at exploiting vulnerabilities within critical infrastructure."

One of the most alarming incidents came in 2023, when cyber attackers targeted a power grid in Eastern Europe using AI algorithms to analyze energy distribution patterns. They identified the most disruptive times to strike and launched their attacks accordingly by learning from earlier attempts, adapting its tactics, and successfully bypassing detection systems to exploit vulnerabilities in the grid's operational technology.

"Traditional security tools are ineffective against AI-powered bots that can mimic human behavior. They're dynamically changing tactics and they learn from prior interactions," he said. "A lot of public systems that rely on outdated threat detection methods can't keep up with the speed and complexity of what we're seeing from modern attacks."

The consequences of bot-driven attacks extend beyond cybersecurity — they strike at the heart of public trust and national stability. A successful attack can shut down services, delay benefits, expose citizen data and paralyze operations across agencies.

Turning the tables: Using AI detection to fight an AI-assisted defense

While AI-powered bots can pose serious risks, AI-assisted defense solutions can also become powerful allies. When deployed strategically, these tools can help public sector agencies stay one step ahead of adversaries, automating threat detection and response in ways that traditional defenses simply can't match.

An AI-assisted defense can excel at pattern recognition, making them ideal for monitoring network activity and identifying anomalies that may signal an attack. Unlike human analysts, they can process massive volumes of data in real time, flagging suspicious behavior before it spirals into a breach.

"WE SEE AI-POWERED BOTS CONDUCTING SOPHISTICATED ATTACKS LIKE CREDENTIAL STUFFING, PHISHING, DDOS AND OTHER KINDS OF ATTACKS AIMED AT EXPLOITING VULNERABILITIES WITHIN CRITICAL INFRASTRUCTURE."

JOE ROGERS
VICE PRESIDENT OF PUBLIC SECTOR AT HUMAN SECURITY

Perhaps most importantly, an AI-assisted defense can act instantly. Once they identify a threat, bots can execute automated response actions, such as blocking access, isolating systems or initiating countermeasures, without waiting for human intervention. This dramatically reduces response time and limits the damage of an attack.

Building resilience through partnership

To effectively defend against bot-driven threats, public sector organizations must go beyond standalone tools. A comprehensive, layered approach is essential — one that combines traditional defenses with advanced, AI-powered capabilities.

According to Rogers, key best practices include:

– **Layered security architecture:** Combine firewalls, intrusion detection and behavioral analytics to strengthen defenses across systems.

– **Dynamic challenges:** Use intent-based CAPTCHAs and behavioral biometrics that distinguish between humans and bots in real time.

– **Credential monitoring:** Integrate threat intelligence to detect breached credentials and block potential account takeovers.

– **Protect critical touchpoints:** Focus defenses on login flows, payment forms and other high-value endpoints where attackers stand to gain most.

– **Continuous education and MFA:** Train employees and implement multi-factor authentication to reduce the risk of human error and social engineering.

Even with these practices in place, staying ahead of threats takes a dedicated partner with deep expertise in automated threat defense. That's where HUMAN comes in.

"We offer high-fidelity decisioning and unmatched precision that enable public sector agencies to detect and mitigate bot-driven threats effectively," Joe Rogers said.

With the Human Defense Platform, users can detect behavioral anomalies, correlate signals across massive datasets and automatically respond to attacks in real time, giving agencies the speed and precision they need to stop bot-driven threats before they escalate.

"Partnering with HUMAN opens the door to other forms of threat research and understanding the ecosystem and latest threats and vulnerabilities directly from a partner who does nothing but this every day, every night, 24/7," said Joe Rogers. "We offer a comprehensive detection, protection and response capability set that really will enable public sector agencies to maintain trust in their digital interactions, as well as safeguard their data."

Bots are becoming more sophisticated every day. With the right approach, an AI-assisted defense doesn't just present a challenge — they become part of the solution.

ISTOCK // IMAGINIMA