carahsoft | HUMAN | NIGHTDRAGON

Protecting Government Benefit Programs from Automated Fraud

By Katherine Hennessey, *Head of Government Services at NightDragon*, and Steven Ahlberg, *VP of Product and Data Intelligence at HUMAN Security*

Nation-states, ransomware gangs, and cyber criminals have a new weapon of choice: AI-powered bots. These systems, which mimic human behavior to automate tasks, have already helped fraudsters siphon hundreds of billions of dollars from federal programs. If left unchecked, this problem will not only cause taxpayers severe financial harm. The incoming administration will need to move quickly to guard against this rapidly growing threat.

The need to better defend the nation's technology infrastructure against AI-powered attacks is not a partisan issue, and it is likely our new cyber leaders can build upon some actions taken by the last administration, including the final cybersecurity EO, issued in January 2025, that highlighted the role that stolen or synthetic identities play in defrauding our government programs. While the focus on instituting modernized digital identity methods may be appropriate, we'd like to offer a few additional considerations for our incoming cyber leaders on how to attack this problem.

The Bots Are Here

Bots are increasingly being used by malicious actors to hack into systems, scrape personal data, or submit fake claims for benefits. At its simplest, they can use credentials and identification information purchased or stolen on the dark web to perpetrate fraud against benefit websites. From overwhelming public benefit portals with credential stuffing attacks to manipulating identity verification systems with precision-targeted scams, bots exploit gaps in digital identity systems at a speed, precision, and scale that is incredibly hard to defend against. And with the advancements in AI, they can increasingly mimic legitimate users to bypass security measures faster than most institutions can adapt.

In fact, in 2021, the Department of Labor found that at least $87 billion of the nearly $900 billion in unemployment insurance awarded under the CARES Act in the aftermath of the COVID pandemic were paid improperly, with a significant, but indeterminable portion attributable to fraud. However, in 2023 alone, bots were responsible for 352 billion attacks targeting login portals, credential verification systems, and transaction flows across industries, according to HUMAN's Quadrillion report.

With 20 percent of login attempts across observed systems linked to account takeover attacks, and 150 million new compromised credential pairs discovered last year, bots are evolving into the ultimate enablers of fraud. If left unchecked, they could amplify the scale of fraud exponentially.

How do we prevent this problem from evolving from merely headline-grabbing to system-crippling?

Our incoming cyber leaders must recognize bots as the major root cause of the fraud problem and refocus attention on deploying cutting-edge new tools on U.S. federal systems to defend the thousands of .gov websites the government administers. This includes deploying applications that can help protect from automated credential stuffing and brute force attempts, block bots from manipulating web applications, prevent data contamination in which bots disseminate fake information to skew metrics, and prevent the unauthorized data harvesting of public websites.

The government must also take the lead in helping private sector entities adopt these tools. The federal government can serve as a catalyst, pushing hold-out organizations to invest in their own fraud defenses. Private businesses are looking for guidance on this issue. Bot detection and counter bot solutions deserve the same level of attention as endpoint detection, patch management, and other fundamental security controls. Proactively embedding bot mitigation into NIST frameworks, for example, will ensure government systems are prepared to defend against automated fraud at scale. Following on this, government guidance relating to how agencies establish Zero Trust architectures should also incorporate bot detection and mitigation.

Finally, we must foster stronger public-private collaboration to advance bot mitigation. Existing bodies for public-private cooperation on cybersecurity must more deliberately include bot intelligence and insight-sharing. We must evolve outdated conceptions of what constitutes cyber threat intelligence (CTI), and endeavor to collect, analyze and report bot intelligence as its own distinct, but highly important category of CTI.

As our incoming cyber leaders in the new administration plan their agenda, it is critical they understand that the root cause of large-scale fraud is not just weak digital identity management methods but AI-powered bots. Bots that undermine the delivery of services and benefits to millions. Combating fraud perpetrated by and with them is a national priority.

About HUMAN

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We ensure that every digital interaction, transaction, and connection is authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information, visit **www.humansecurity.com**