Government Business Council

HUMAN

Human or Not?

Bots in the Public Sector

INTRODUCTION

From social media to spam to automated tax assistance, bots have become a key player in the digital world. As organizations transform their digital ecosystem, services have become more efficient, accessible, and responsive. However, the same transformation introduces vulnerabilities that malicious actors are exploiting at unprecedented levels. For government agencies, which harbor some of the most sensitive data in the country but also face mandates to improve their efficiency and cybersecurity, the explosion of bots can be a double-edged sword. One of the most significant and escalating threats in the public sector today is the rise of bad bots that are capable of executing complex cyberattacks at a scale and speed that far exceeds human capabilities.

THE RISE OF BOTS

The proliferation of bots has surged dramatically in recent years, with bot-generated traffic surpassing human-generated traffic for the first time in 2023. While legitimate bots enhance operational efficiency, malicious bots, or "bad bots," pose severe security risks. Bad bots are engineered to carry out illicit activities, including credential stuffing, data scraping, and denial-of-service attacks. Bot attacks result in substantial financial losses for both the public and private sectors, with damages reaching billions of dollars and continuing to grow exponentially.[1]

BOTS IN THE PUBLIC SECTOR

Bots play a dual role in the U.S. federal government, acting as both valuable tools and potential threats. Government agencies can deploy bots to automate repetitive tasks, streamline public services, and enhance citizen engagement. Examples include chatbots that assist with tax inquiries, automated systems for processing benefits applications,

BOT BASICS

Short for **robot**, bots are **automated software programs** that perform repetitive tasks on a network.

Bots follow instructions that **mimic human behavior** much faster than any human could do, and can operate **without human intervention**.

Good bots help an organization scale and automate some of their processes, like chatbots to respond to questions or search engine crawlers that rapidly locate information from disparate sources.

Good bots make up **17.60%** of all internet traffic.

Bad bots also use repetitive actions but for malicious ends, like spambots, fake social media accounts, or in Distributed Denial of Service (DDoS) attacks.

Bad bots make up **32%** of all internet traffic.

and AI-driven analytics tools for detecting fraud. These applications improve efficiency, reduce administrative burdens, and enhance transparency in government operations.

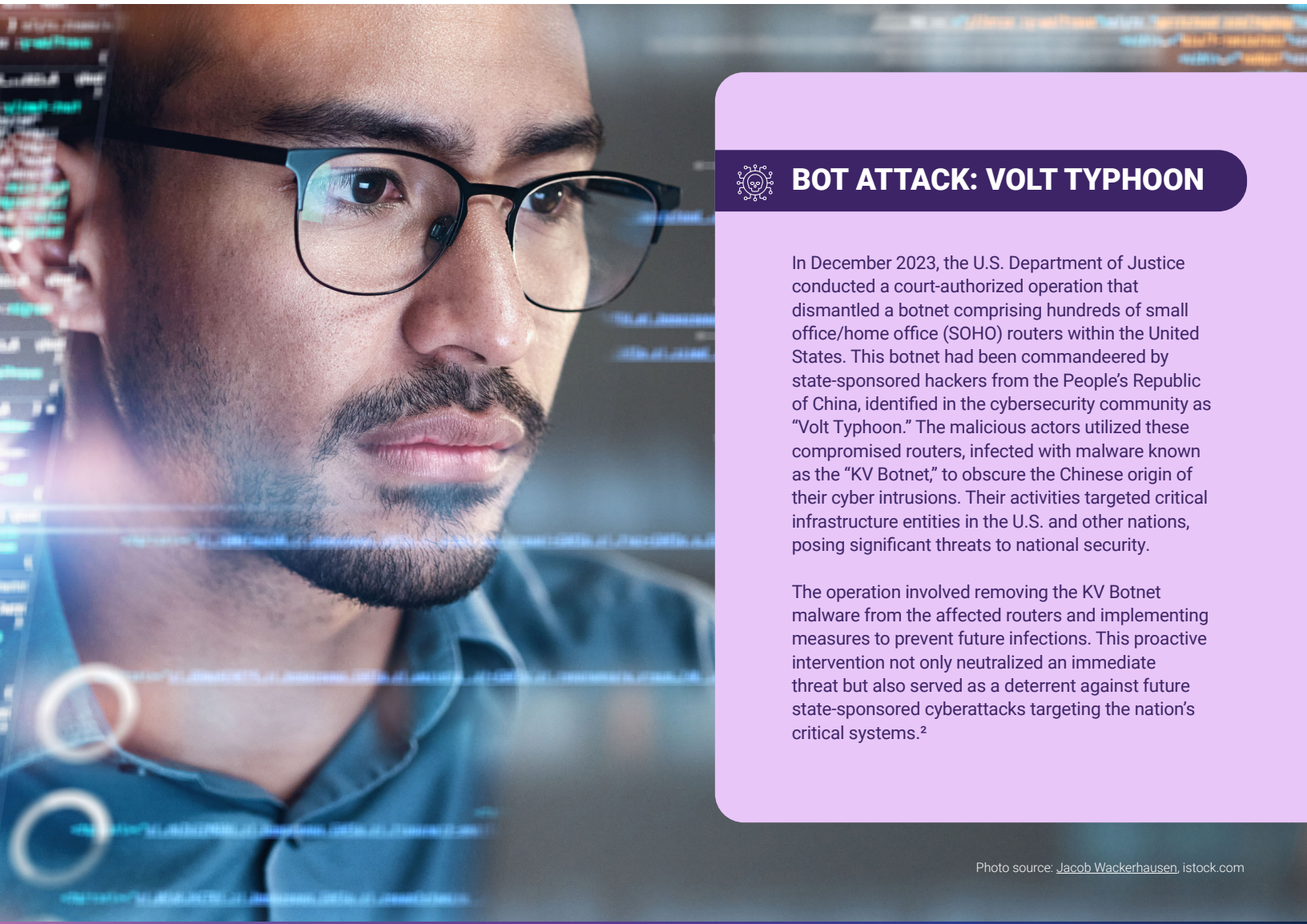
However, the same automation capabilities also make bots a vector for cyber threats. Malicious bots are frequently used by adversaries to target federal agencies through automated hacking attempts, misinformation campaigns, and large-scale data theft. Foreign actors and cybercriminal groups exploit bot networks to launch sophisticated attacks against government infrastructure, potentially compromising national security.

THE RISK OF BOTS

Some of the most common threats from bots include:

COMPROMISED USER ACCOUNTS

One of the most alarming threats posed by bad bots is their role in account takeover (ATO) attacks. Using stolen or leaked credentials, attackers leverage botnets to systematically infiltrate user accounts, gaining unauthorized access to sensitive government data. These attacks can compromise not only individual accounts but also entire federal databases, increasing the risk of espionage and fraud.



BOT ATTACK: VOLT TYPHOON

In December 2023, the U.S. Department of Justice conducted a court-authorized operation that dismantled a botnet comprising hundreds of small office/home office (SOHO) routers within the United States. This botnet had been commandeered by state-sponsored hackers from the People's Republic of China, identified in the cybersecurity community as "Volt Typhoon." The malicious actors utilized these compromised routers, infected with malware known as the "KV Botnet," to obscure the Chinese origin of their cyber intrusions. Their activities targeted critical infrastructure entities in the U.S. and other nations, posing significant threats to national security.

The operation involved removing the KV Botnet malware from the affected routers and implementing measures to prevent future infections. This proactive intervention not only neutralized an immediate threat but also served as a deterrent against future state-sponsored cyberattacks targeting the nation's critical systems.[2]

Photo source: Jacob Wackerhausen, istock.com

BOT ATTACK: HEALTH AND HUMAN SERVICES

In March 2020, as the COVID-19 pandemic began to escalate, the U.S. Department of Health and Human Services (HHS) experienced a significant DDoS cyberattack targeting its digital infrastructure. The cyber intrusion involved an unprecedented electronic assault on HHS systems while the department was coordinating national efforts to combat the emerging health crisis.

While the full scope of the breach was not publicly disclosed at the time, the attackers' attempt to undermine public confidence and hinder the dissemination of vital information was described by the department's former Chief Information Officer as a "nation-state level assault." The incident underscored the vulnerabilities in the U.S. healthcare system's cybersecurity defenses, especially during periods of national emergency, and emphasized the need for robust protective measures to safeguard critical public health operations against such malicious activities.[5]

EXFILTRATED SENSITIVE DATA

Government databases contain vast amounts of sensitive information, including classified intelligence, personally identifiable information (PII), and financial records. Attackers leverage sophisticated scraper bot techniques to extract confidential data, often evading traditional cybersecurity measures. These unauthorized extractions can lead to large-scale data breaches, jeopardizing national security and exposing citizens to identity theft and fraud. The average cost of the most expensive data breach in 2024 was $4.88 million – 10% higher than the year before, highlighting the escalating urgency of protecting sensitive data.[3]

DISRUPTED GOVERNMENT SERVICES

Automated attacks such as distributed denial-of-service (DDoS) attacks have the potential to cripple essential public services. By overwhelming government websites and online portals with excessive traffic, DDoS attacks render critical systems inoperable, disrupting functions such as tax filings, social security benefits, and emergency response coordination. Critical infrastructure sectors saw a 55% increase in DDoS attacks over the past four years.[4]

THE AI IMPACT

Artificial intelligence (AI) is revolutionizing the landscape of bot-driven activity, both in terms of efficiency and security threats. AI-powered bots have become more advanced, leveraging machine learning algorithms to make them harder to detect and more effective at evading traditional security measures. These bots can analyze patterns of cybersecurity defenses, refine their attack vectors, and execute adaptive strategies to breach security frameworks. Enhanced phishing attacks are already a significant cybersecurity risk, as AI can craft personalized and realistic phishing messages that significantly increase the likelihood of success.

Potential future areas of AI-driven bot proliferation include:

AUTOMATED CREDENTIAL STUFFING

Using vast datasets of stolen credentials to conduct highly efficient login attempts, reducing the time required to gain unauthorized access.

AUTONOMOUS DATA SCRAPING

Extracting sensitive government data more efficiently, making detection and mitigation increasingly difficult.\

INTELLIGENT EVASION TECHNIQUES
Learning from failed attacks, modifying their approach, and bypassing security measures with minimal human intervention.

Hybrid Attack Structures

Hybrid attack structures are also becoming more common, in which bots augment human cybercriminals' skills to execute more sophisticated attacks. Some key aspects of hybrid attacks include:

AI-assisted human hacking – Cybercriminals use AI-powered bots to conduct reconnaissance, identify vulnerabilities, and recommend attack strategies that humans execute. This type of structure has already been anecdotally identified to defraud the Social Security Administration, where scammers steal a victim's information and use a chatbot to call the SSA to change beneficiary data.[6]

Automated disinformation campaigns – AI bots are deployed in large numbers to spread false narratives, influencing public perception and decision-making within government agencies.

Adaptive malware deployment – AI-powered malware can alter its code in real time to bypass antivirus and endpoint security solutions, making mitigation significantly more challenging.



HYBRID ATTACKERS: THOUGHTNETS

AI-powered "Thoughtnets" pose a growing threat to the public sector by merging cyberattacks with sophisticated disinformation campaigns. These AI-driven bots infiltrate digital spaces, mimicking real users to manipulate narratives, spread misinformation, and erode public trust in government institutions. By leveraging machine learning, they adapt in real time, targeting public agencies, elections, and crisis communications to sow confusion and destabilize civic discourse.

As Thoughtnets evolve, they can generate realistic fake content—audio, video, and text—making it increasingly difficult for citizens to discern truth from falsehood. Their activities extend beyond information warfare to influencing public policy debates and disrupting essential government services. The convergence of cyber and narrative attacks underscores the urgent need for robust cybersecurity frameworks that safeguard both digital infrastructure and the integrity of public information.[7]

Photo source: yacobchuk, istock.com

BEST PRACTICES

Federal agencies must prioritize proactive defense strategies to combat the evolving threat landscape posed by bots. Best practices for agencies looking to implement a robust cybersecurity framework should include:

1. **Advanced bot detection technologies**
   Implementing AI-driven bot detection solutions can help distinguish between legitimate and malicious automated activities, minimizing the risk of infiltration.

2. **Multi-factor authentication (MFA)**
   Strengthening authentication mechanisms can reduce the success rate of ATO attacks, ensuring that unauthorized access is prevented even if credentials are compromised.

3. **Zero trust architecture**
   Implement a zero trust model that continuously verifies users and devices, ensuring that no access is granted based solely on network location.

4. **Preventative resilience**
   Prepare for DDoS attacks and credential stuffing attempts by deploying rate-limiting strategies, CAPTCHAs, and web application firewalls, as well as leveraging behavioral analytics to identify abnormal bot activity.

5. **Public-private collaboration**
   Engaging in cross-sector partnerships with cybersecurity experts and industry leaders fosters knowledge-sharing and enhances defensive capabilities against emerging bot threats, including threat intelligence integration.

CONCLUSION

The ability of bots to operate autonomously, tirelessly, and at scale makes them a formidable adversary for government agencies, who can struggle to keep pace with the rapidly evolving threat landscape. As bad bots become more sophisticated and pervasive, the increasing reliance on digital platforms amplifies these threats. Federal agencies and programs face an ongoing challenge in mitigating the risks posed by bots and safeguarding critical infrastructure and sensitive information from their malicious activities.By embracing proactive detection, mitigation, and collaborative security strategies, the government can safeguard its digital infrastructure and ensure the resilience of critical public services.

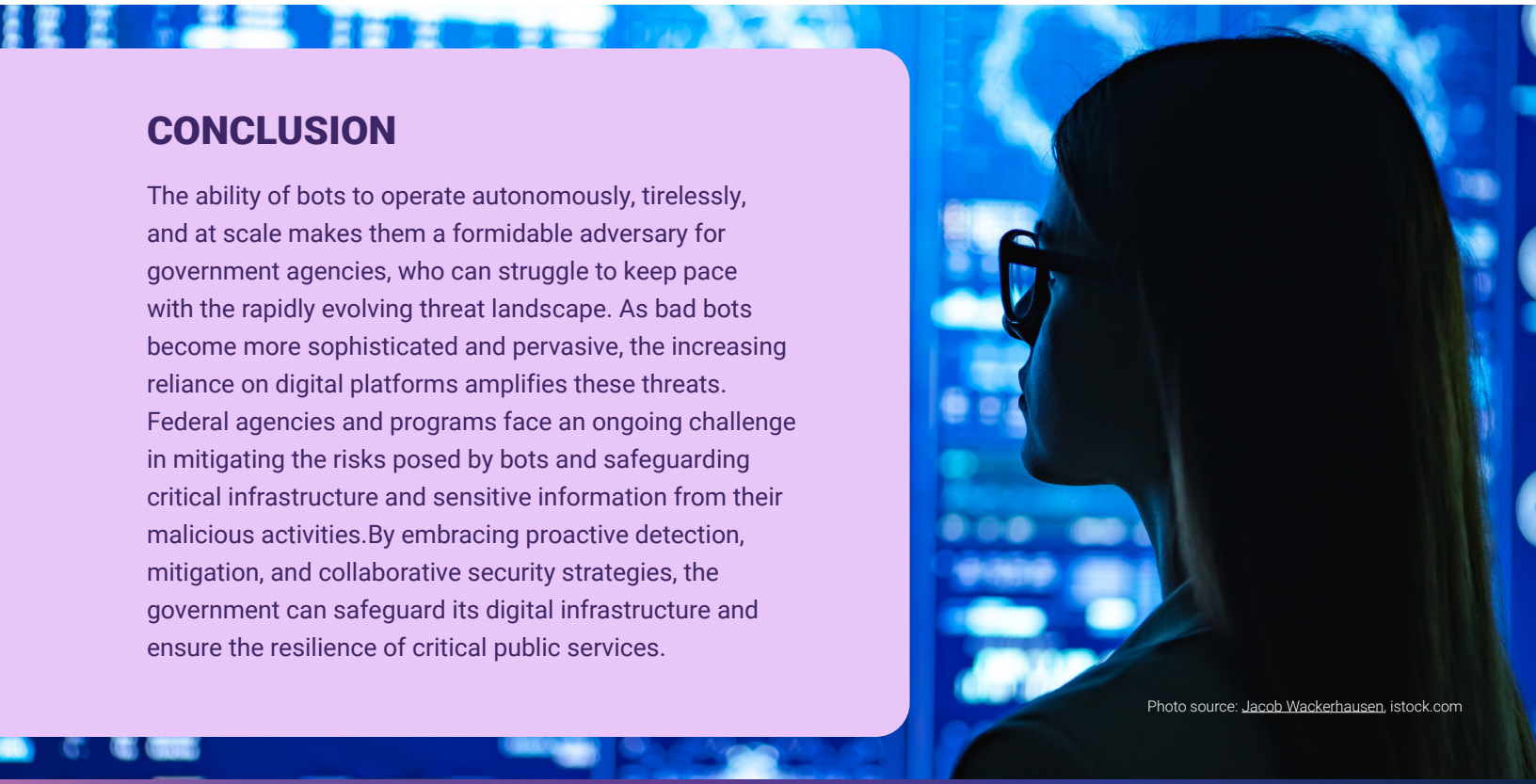


Photo source: Jacob Wackerhausen, istock.com

SOURCES

1. https://www.forbes.com/councils/forbestechcouncil/2023/11/07/bot-attacks-the-financial-impact-of-attacks-beyond-mitigation-costs/
2. https://www.justice.gov/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical
3. https://newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs
4. https://www.csoonline.com/article/3545049/ddos-attacks-are-increasingly-targeting-critical-infrastructure.html
5. https://www.bloomberg.com/news/articles/2023-12-06/hhs-cyberattack-at-2020-covid-onset-was-bigger-than-first-realized
6. https://www.wmar2news.com/matterformallory/government-agency-starting-to-see-scammers-use-a-i-to-steal-benefits
7. https://blackbird.ai/blog/thoughtnet-ai-powered-bots-are-reshaping-cyberwar/

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 about how we can support your organization, please visit www.humansecurity.com/publicsector.

Government Business Council

As GovExec's research division, Government Business Council (GBC) is dedicated to advancing the businessof government through analysis, insight, and analytical independence. An extension of *Government Executive's 50 years* of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision-makers from across government to produce intelligence-based research analysis. For more information, email us at research@govexec.com.

Back page and cover photo source: Alexander Sikov, istock.com