HUMAN

UNMASKING THE THREAT: How Automated Bot Networks Manipulate Elections Globally

INTRODUCTION

A significant and evolving threat to democratic processes has emerged: the deployment of automated bot networks by malicious actors. These sophisticated systems mimic human behavior online, allowing threat actors to manipulate public opinion, spread disinformation and compromise electoral infrastructure. Notably, international governments and state-sponsored groups have increasingly been implicated in utilizing these networks to influence elections, underscoring the global nature of the challenge.

The proliferation of bots can be largely attributed to advancements in automation and artificial intelligence technologies, which have significantly lowered the entry barrier for deploying complex cyber attacks. HUMAN's **Quadrillion Report: 2024 Cyberthreat Benchmarks**[1] reveals a staggering volume of malicious activity, with more than 352 billion blocked attempts at cyberattacks in 2023, including account takeovers, carding and sensitive data scraping. These types of automated systems enable cybercriminals to scale operations easily and cheaply, leveraging bots to create fake accounts, conduct coordinated disinformation campaigns and manipulate public narratives. The rapid dissemination of false or misleading information via bot networks amplifies their impact, facilitating the erosion of public trust in democratic institutions.

To counter this threat, it is imperative that electoral bodies and organizations adopt advanced bot detection and mitigation strategies. By implementing targeted technologies and robust security measures, we can protect the integrity of electoral processes and ensure that democratic principles remain resilient against digital manipulation.

THE HISTORICAL EVOLUTION OF BOT NETWORKS

Since their inception, bots have evolved from simple automated scripts to sophisticated networks capable of mimicking human behavior. Early uses were relatively benign, but recent advancements have enabled complex disinformation campaigns and direct attacks on electoral systems. The 2016 U.S. presidential election marked a pivotal moment, showcasing the power of state-sponsored bots in shaping political discourse.

UNDERSTANDING BOTS: A CRITICAL THREAT TO GOVERNMENT OPERATIONS

A bot is a software application that automates tasks on the internet at scale, performing actions ranging from the benign to the malicious. In the context of government operations and elections, bots can be particularly nefarious, engaging in activities such as:

- **Spreading & Amplifying Disinformation:** Bots can flood social media platforms and online forums with false, misleading or biased to manipulate public opinion, create confusion and undermine the credibility of electoral processes.
- **Compromising Infrastructure:** Bots can target election infrastructure, including voter registration databases, voting machines and the systems used to tally and report results. The intent by attackers is to disrupt voting systems, alter results or steal sensitive voter data.
- **Fraudulent Activities:** Bots can automate fraudulent voter registrations, influence online donation platforms to generate fake contributions and exploit vulnerabilities in government systems to gain unauthorized access. According to HUMAN's Quadrillion Report, more than 200,000 fake account creation attempts and 40,000 post-login account compromise attempts per customer were identified in 2023. This highlights the scale at which automated systems can execute fraudulent activities, further complicating the detection and prevention of such schemes.

In addition to domestic threats, international governments and state-sponsored entities have been known to deploy bots for malicious purposes. For example, Russian and Chinese state-backed groups have used bots to target foreign electoral systems, aiming to destabilize political environments and undermine trust in democratic processes.

The relentless evolution of bot-driven threats necessitates continuous innovation in detection and mitigation strategies, much like those developed by leading cybersecurity firms specializing in digital integrity and defense.

EVIDENCE OF MANIPULATION

Recent elections have provided clear examples of how bot-driven disinformation campaigns can significantly impact democratic processes. Below are several cases illustrating the pernicious effects of these campaigns, along with measures taken to mitigate such threats:

Securing Election Tabulation Transmission

In various elections, automated bots have intercepted and manipulated transmission data, potentially altering vote counts and eroding voter confidence. For example, the Voatz mobile voting application was found to have security flaws that allowed attackers to intercept and potentially alter votes due to insufficient encryption protocols[2]. Similarly, during the March 2023 Estonian parliamentary elections, cyberattacks targeted the country's internet voting system, attempting to disrupt the process. While Estonia attacks were ultimately unsuccessful, they highlighted the constant threat to electoral systems.

Solution: Implement robust encryption, real-time monitoring, and multi-factor authentication to safeguard transmission channels. These measures ensure that only authorized entities can access and modify election data, preserving the accuracy and reliability of vote tabulation.

Combating Misinformation

Bots amplify false narratives across social media, swaying public opinion and distorting voter behavior. In the lead-up to the 2017 French presidential election, Facebook took measures to combat disinformation, including removing tens of thousands of fake accounts suspected of spreading false information[3]. This action demonstrated the effectiveness of AI-driven detection systems but also highlighted the scale of the problem.

Solution: Implement advanced algorithms to detect and neutralize bot-driven disinformation campaigns. By identifying and countering false narratives, electoral bodies uphold the integrity of public discourse and informed decision-making.

Monitoring Critical Infrastructure

Election systems worldwide are frequently targeted by cyberattacks, putting voter registration data and vote tabulation processes at risk. In the 2020 U.S. elections, cybersecurity agencies reported[4] increased phishing campaigns and ransomware attacks aimed at election officials and systems. These incidents, while not resulting in vote alterations, underscored the persistent threat landscape. Similarly, during the 2021 German federal elections, Russian-linked groups were observed[5] attempting to disrupt digital systems and spread disinformation. In the 2022 Philippine presidential election, there were significant concerns following an attempt to hack systems associated with the Commission on Elections (COMELEC).[6]

Solution: Implement proactive monitoring and rapid response strategies to mitigate botnet threats targeting election systems. Strengthening security measures ensures the integrity and confidentiality of voter information crucial for democratic operations.

Protecting and Monitoring Voter Registration Vendors

Bots exploit vulnerabilities in voter registration systems, attempting fraudulent registrations or disrupting database integrity. During the 2020 US elections, several states implemented advanced IP filtering techniques to protect voter registration databases from bot-driven attacks.

Solution: Deploy IP filtering and behavioral analysis tools to detect and block suspicious bot activities. Securing voter registration processes safeguards against unauthorized access and maintains the accuracy of voter rolls.

Upholding Electoral Integrity

Bots skew online polls to mislead public perception and sway voter sentiment, compromising the accuracy of these measures. During various elections, news outlets have used CAPTCHA technology to prevent bots from skewing online poll results, ensuring more accurate reflections of public sentiment.

Solution: Implement stringent monitoring and CAPTCHA technologies to prevent bot interference in online polls. By ensuring the authenticity of voter interactions, electoral bodies preserve the credibility and reliability of poll results.

Abusing Donation Systems

Bots exploit online donation platforms to generate fraudulent contributions, compromising campaign finance transparency. In recent election cycles, several campaigns have adopted advanced fraud detection algorithms to protect against bot-driven donation fraud, ensuring compliance with finance regulations.

Solution: Integrate robust fraud detection mechanisms into donation systems to identify and block bot-driven fraudulent transactions. Upholding transparency in campaign finance operations safeguards electoral integrity and prevents illicit financial influence.

RECOMMENDATIONS: STRENGTHENING ELECTION SECURITY AGAINST BOT THREATS

As we navigate the complexities of bot-driven election interference, it’s essential to implement robust, tailored strategies that go beyond traditional security measures. These recommendations aim to fortify electoral systems against the sophisticated nature of modern bot threats:

1. **Advanced Bot Detection:** Employ AI-driven technologies to detect and neutralize bot activity in real time, preventing bots from influencing electoral outcomes.
2. **Social Media Monitoring:** Employ AI-driven technologies, such as machine learning algorithms that analyze behavioral patterns to detect and neutralize bot activity in real

time, ensuring public discussions remain authentic.

3. **Threat Intelligence:** Use real-time threat intelligence to stay updated on emerging bot tactics and threat actors, keeping electoral systems secure from new threats.
4. **Behavioral Analysis and Anomaly Detection:** Use sophisticated analysis tools to monitor and mitigate bot-driven disinformation on social media and online publications to distinguish humans from bot interactions and quickly address unusual activity patterns indicating bot interference.
5. **Automated Response Systems:** Implement automated systems to respond instantly to detected bot activities, deploying countermeasures like blocking, isolating or redirecting bots to protect election integrity.

It is crucial to foster international cooperation, developing global standards and sharing intelligence to counter the influence of nation-state actors effectively. By collaborating, countries can enhance their defensive capabilities against these sophisticated threats.

Future Trends and Projections

As AI and machine learning continue to advance, bot networks are expected to become more sophisticated and challenging to detect. Key trends include:

1. **Enhanced AI Capabilities:** Bots will leverage advanced AI technologies, such as natural language processing and deep learning, to better mimic human behavior and evade detection systems.
2. **Deepfake Technology:** The use of deepfakes in disinformation campaigns could increase, creating realistic but false audio and video to mislead the public and influence elections.
3. **Personalized Disinformation:** Bots may use data analytics to deliver highly targeted and personalized disinformation, making campaigns more effective in shaping public opinion.
4. **Scalability and Automation:** Future bot networks will likely operate on a larger scale, with greater automation allowing for widespread, coordinated attacks across multiple platforms.
5. **IoT Integration:** As IoT devices proliferate, they could become new vectors for botnet expansion, posing additional security challenges.

The evolving nature of these threats will require continuous advancements in detection technologies and international cooperation to ensure the security and integrity of democratic processes. By anticipating these developments and preparing accordingly, we can better defend against the complex challenges posed by future bot networks.

CONCLUSION

As societies increasingly rely on digital platforms for democratic participation, fortifying electoral cybersecurity measures becomes imperative. The pervasive threat of automated bot networks manipulating public discourse and electoral outcomes necessitates proactive and collaborative efforts across nations and stakeholders.Recognizing the role of international governments and nation-state actors in this arena is essential for developing a comprehensive defense. By fostering global cooperation and implementing robust cybersecurity measures, we can protect the integrity of elections and uphold democratic principles amidst evolving digital threats.

Call to Action

Governments, technology companies and civil society must work together to develop and deploy comprehensive cybersecurity measures. Investing in next-generation bot detection and mitigation tools, fostering international cooperation and enhancing public awareness are crucial steps in protecting democratic processes from the evolving threat of automated bots. By staying ahead of these threats, we can ensure that elections remain free, fair and resilient against digital manipulation.

SOURCES

1 **HUMAN**. (2024). *The Quadrillion Report: 2024 Cyberthreat Benchmarks.*
https://www.humansecurity.com/learn/blog/its-all-in-the-numbers-the-quadrillion-report-2024-cyber-threat-benchmarks

2 **MIT News.** (2020). *MIT Researchers Identify Security Vulnerabilities in Voting App.*
https://news.mit.edu/2020/voting-voatz-app-hack-issues-0213

3 **National Endowment for Democracy (NED).** (2020). *Issue Brief: Distinguishing Disinformation from Propaganda, Misinformation, and "Fake News".*
https://www.ned.org/issue-brief-distinguishing-disinformation-from-propaganda-misinformation-and-fake-news/

4 **CISA (Cybersecurity and Infrastructure Security Agency).** (2020). J*oint Statement from Elections Infrastructure Government Coordinating Council & The Election Infrastructure Sector Coordinating Executive Committees.*
https://www.cisa.gov/news-events/news/joint-statement-elections-infrastructure-government-coordinating-council-election

5 **Associated Press.** (2021). *Germany Accuses Russia of Pre-Election Cyber Attacks.*
https://apnews.com/article/technology-europe-russia-elections-germany-26ea77a3b96b94d5760aab48c9dfc008

6 **2022 Philippine Presidential Election: Search Foundation.** (2022). *Marcos Election Victory Illegitimate.*
https://www.search.org.au/marcos_elaction_victory_illegitimate

About HUMAN

HUMAN is a cybersecurity company that protects organizations by disrupting bot attacks, digital fraud and abuse. We leverage modern defense to disrupt the economics of cybercrime by increasing the cost to cybercriminals while simultaneously reducing the cost of collective defense. Today we verify the humanity of more than 20 trillion digital interactions per week across advertising, marketing, e-commerce, government, education and enterprise security, putting us in a position to win against cybercriminals. To Know Who's Real, visit **www.humansecurity.com**.