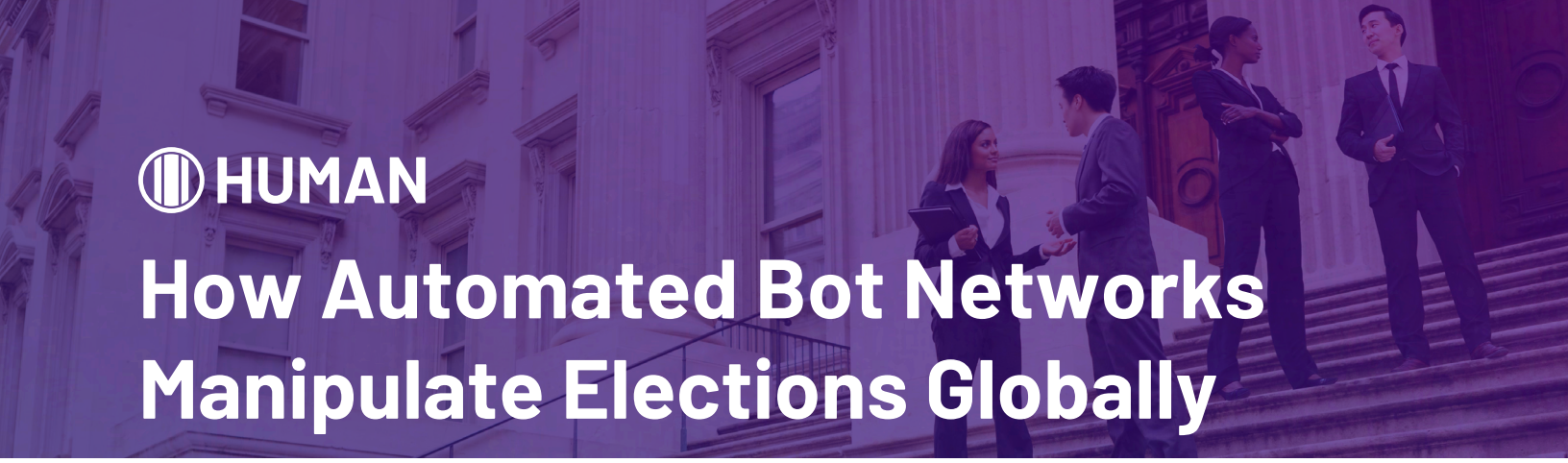

HUMAN

How Automated Bot Networks Manipulate Elections Globally

By Steven Ahlberg
VP of Data Intelligence & Product, HUMAN Security
July 2024

A new and pressing threat has emerged: the influence of automated bot networks on electoral processes worldwide. These sophisticated tools, mimicking human behavior online to disrupt and manipulate democratic elections. From shaping public opinion via social media to compromising election infrastructure, bots challenge the foundations of democracy.

This threat is real and has impacted significant elections globally. Examples include the 2020 U.S. presidential election and the 2017 French presidential election, which highlight the devastating effects of bot-driven disinformation campaigns. These botnets inundate social media with false information, misleading millions and fracturing public trust. **Nearly half (47%) of all internet traffic in 2022 came from bots**, with malicious bots at 30.2% —the highest level since 2013. Cybercriminals leverage bots for automation and scale—**bots are involved in 77% of attacks**.

Bots exploit vulnerabilities in digital communication channels, manipulating public sentiment, eroding electoral confidence, and destabilizing institutions. To combat this threat, electoral bodies must adopt advanced bot detection and mitigation strategies. By leveraging cutting-edge technologies and robust security measures, we can safeguard electoral accuracy and reliability, ensuring democratic principles remain resilient against digital manipulation.

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:

- **Disseminating Misinformation:** Bots can flood social media platforms and online forums with false information, aiming to sway public opinion, create confusion, and undermine the credibility of electoral processes.
- **Compromising Infrastructure:** Bots can target election infrastructure, attempting to disrupt voting systems, alter results, or steal sensitive voter data.
- **Manipulating Public Sentiment:** By creating fake accounts and generating artificial interactions, bots can manipulate online polls, amplify divisive content, and create the illusion of public consensus or dissent.
- **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.

By leveraging cutting-edge technologies and robust security measures, electoral bodies can safeguard electoral accuracy and reliability, ensuring that democratic principles remain resilient against digital manipulation. However, 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, in Estonia's 2019 parliamentary elections, encrypted communication protocols ensured the secure transmission of digital votes. This prevented bot interference and maintained public trust in the results.

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. During the 2017 French presidential election, Facebook removed tens of thousands of fake accounts spreading misinformation. This action demonstrated the effectiveness of AI-driven detection systems but also highlighted the scale of the problem.

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

Monitoring Critical Infrastructure

Election vendor systems are vulnerable to botnet attacks, jeopardizing voter registration data and vote tabulation processes. In the 2016 US elections, Illinois' voter registration system was targeted by bots, prompting enhanced monitoring and rapid response protocols that have since been adopted nationwide.

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 manipulate online polls to influence public perception and sway voter sentiment, undermining poll accuracy. 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:** Utilize sophisticated analysis tools to monitor and mitigate bot-driven misinformation on social media, 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 against new threats.
4. **Behavioral Analysis and Anomaly Detection:** Use behavioral analysis to distinguish human 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.

Conclusion

As societies increasingly rely on digital platforms for democratic participation, fortifying electoral cybersecurity measures is imperative. The pervasive threat of automated bot networks manipulating public discourse and electoral outcomes necessitates proactive and collaborative efforts across nations and stakeholders. By implementing advanced technologies and rigorous strategies, electoral bodies can safeguard 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.

Get Your Threat Assessment

Contact Us to learn how you can protect your organization from bot-driven threats: https://www.humansecurity.com/demo-request

Citations

1. Stanford Internet Observatory. (2020). "The Long Fuse: Misinformation and the 2020 Election."
2. The Washington Post. (2020). "How misinformation spread in the 2020 election."
3. Estonian National Electoral Committee. (2019). "Securing the 2019 parliamentary elections."
4. Reuters. (2017). "Facebook removes tens of thousands of fake accounts in France."
5. NBC News. (2016). "Illinois' voter registration system targeted by hackers."
6. CNN. (2020). "States bolster election security amid concerns over cyber threats."
7. The New York Times. (2020). "CAPTCHA technology and online polling security."
8. The Wall Street Journal. (2020). "Campaign finance and the battle against donation fraud."

About HUMAN Security

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. Protect your digital business with HUMAN.

To Know Who's Real, visit **https://www.humansecurity.com/solutions/industry/public-sector**.