HUMAN

Mitigating the Zero Trust Bot Gap

The Zero Trust framework has emerged as a critical paradigm in cybersecurity—emphasizing the need to protect sensitive data and systems by defaulting to a position of "do not trust" for all users, devices, and networks. While this provides a robust security approach, there is a critical gap that often goes unnoticed: the Zero Trust Bot Gap. This is the vulnerability that exists when bots infiltrate secure environments by riding along with trusted human or device authentication, allowing them to gain undetected access.

The Zero Trust Bot Gap undermines the effectiveness of traditional security measures, including multi-factor authentication (MFA), as bots can hijack session tokens, manipulate authentication processes, and cause havoc within secure environments long before the tokens expire.

To close this gap, organizations must integrate advanced bot detection and mitigation techniques within their Zero Trust framework. This will help them strengthen their security posture and ensure that authentication remains reliable and secure against bot-driven attacks.

What is a Bot? How Big a Threat is It?

A bot is simply a software app that runs automated tasks on the internet at scale—from scooping up tickets to popular events to spreading false information about elected officials. Bots can carry out tasks as simple as completing a form to more complex assignments like scraping websites for data.

The use of bots has grown dramatically over the years. Security Today reported in May 2023 that **nearly half (47%) of all internet traffic in 2022 came from bots**. More alarming, the report found **the volume of malicious bots grew to 30.2%**—the highest level of bad bot activity since the first report in 2013. Malicious bots can compromise user accounts, steal data, increase infrastructure and support costs, degrade online services, and even threaten elections and other government activities. Cyber criminals use bots for automation and scale when they attack—**bots are in 77% of such attacks**.

Incorporating Bot Protection into the Zero Trust Framework

The bot gap exists because the current Zero Trust framework does not include advanced bot detection and mitigation. By integrating these capabilities into the framework, an organization can tighten protections around sensitive data, systems and personnel and significantly improve its overall security posture. Advanced bot protection measures can integrate into each of the five interconnected pillars of the Zero Trust framework.

Pillar 1: Workforce Security and User Identity

Ensuring the integrity of user identities is fundamental to maintaining a secure environment within the Zero Trust framework. Advanced bot detection and mitigation systems are crucial for safeguarding user identities and preventing unauthorized access attempts. By integrating continuous identity verification that uses multi-factor authentication (MFA) with sophisticated bot detection techniques, organizations can prevent compromised credentials and establish a robust defense against bot-driven attacks.

While users can't be responsible for continually monitoring the safety of the apps they use or the devices that access those apps, user education and awareness are still vital to a comprehensive identity protection strategy. Organizations should provide comprehensive training and awareness programs to educate users, regularly communicate security policies and procedures, and reinforce the importance of identity protection to foster a security-conscious culture within the organization.

Pillar 2: Device Security

Already, organizations understand the significance of device security within the Zero Trust framework, and they employ various measures to prevent devices from being compromised and exploited via bot-driven cyberattacks. Monitoring and assessing devices connecting to the network is key to this effort.

Through mandatory, continuous device monitoring, organizations can proactively track and evaluate the behavior and security posture of each device. Certifications, such as Service Organization Control Type 2 (SOC 2), should be used to ensure device security best practices are implemented. In addition, organizations should implement specialized bot protection measures tailored for IoT devices. This includes deploying sophisticated bot detection and mitigation systems that can identify and neutralize bot-driven attacks targeting IoT devices.

Organizations also can employ infrastructure fingerprinting techniques as part of their advanced bot mitigation strategies. This will allow them to identify and block interactions with known malicious infrastructure or infrastructure associated with criminal actors. By maintaining an up-to-date database of malicious IP addresses, domains, or command-and-control servers, organizations can proactively block communication with these sources, effectively preventing bots from establishing connections and launching attacks. And no organization can compile, maintain or update a comprehensive database of malicious sources; instead, work with platform and technology providers that offer collective protection from observed botnet threats before they occur.

Pillar 3: Network

Network-level bot detection and mitigation systems are also essential to an effective Zero Trust security strategy. They reduce the risk of bots breaching the network, which enhances overall network security. By implementing a comprehensive policy that includes micro-segmentation of networks, continuous monitoring for bot-driven activities, and incident response procedures, organizations can better protect all sensitive data and systems connected to the network and significantly improve their overall security posture.

Pillar 4: Workload

Workload-level bot protection systems monitor and safeguard an organization's applications and workloads. They allow organizations to more effectively detect and mitigate bot-driven attacks at the workload level—particularly those involving ransomware. When they detect an attack, these systems can isolate compromised workloads, block malicious processes, and equip organizations to take immediate action to stop the spread and prevent further damage.

Pillar 5: Data Security

Data-level bot detection and mitigation focuses on safeguarding sensitive information from unauthorized access and ensuring data integrity. By integrating bot protection at the data level, organizations can monitor data access patterns, detect anomalies, and prevent unauthorized access to sensitive information. This requires a policy that includes data classification, encryption, and continuous monitoring—all necessary to execute appropriate security controls and access policies. Encryption, both in transit and at rest, ensures that data remains protected even if it falls into the wrong hands.

The combination of data classification, encryption, and continuous monitoring provides a layered defense approach, reducing the risk of unauthorized data access and potential data breaches. This approach aligns with the principles of the Zero Trust framework, ensuring that data remains secure and protected throughout its lifecycle.

Functions for Coordinating Bot Protection Across Pillars

Additionally, bot detection and mitigation can strengthen other key functions across the five pillars of the Zero Trust framework:

Visibility and Analytics

Visibility and analytics play a crucial role in the Zero Trust framework by providing insights into network and security posture. Advanced bot detection and mitigation systems can significantly enhance these capabilities, enabling organizations to identify and respond to bot-driven threats more effectively.

Visibility refers to the ability to gain comprehensive insight into network traffic, user behavior, and system activities. By leveraging advanced bot detection techniques, organizations can analyze network traffic patterns and identify anomalous behavior that may indicate the presence of bots. By monitoring network traffic, organizations can gain visibility into potential bot-driven activities, enabling them to detect and respond to threats in real-time.

Analytics involves the processing and interpretation of data collected from various sources to extract actionable insights. Advanced bot detection and mitigation systems can leverage analytics to identify patterns and trends associated with bot-driven attacks, filtering out bot attacks before they occur - which gives time and resources back to security teams, reduces alert fatigue, and cuts down on incident escalation. By correlating data from different security sources, such as log files, network traffic, and user activity, organizations can identify indicators of compromise and potential bot activities. These insights can help organizations proactively identify and mitigate bot-driven threats before they cause significant harm.

In addition, advanced bot detection and mitigation systems can support the sharing of threat intelligence. By integrating with threat intelligence platforms, organizations can access up-to-date information about emerging bot threats, malicious IP addresses, and botnet activities. This information can enhance their visibility into the threat landscape and enable them to take proactive measures to protect their networks.

Automation and Orchestration

Automation and orchestration enable organizations to respond swiftly and effectively to bot-driven attacks. Integrating advanced bot protection tools with automation and orchestration capabilities allows scaling of remediation or mitigation efforts when combined with better classification of the types of attacks imminent or underway.

Automation and orchestration are two different, though related, activities. Automation involves the use of technology to perform tasks and actions without human intervention. It plays a crucial role in rapidly identifying and responding to bot-driven attacks. Once a bot is identified, automated processes can be triggered to isolate infected systems, block malicious traffic, and initiate remediation actions.

Orchestration entails coordinating and managing multiple security tools and processes to achieve a unified response to security incidents. In the case of bot-driven attacks, orchestration helps streamline response efforts by integrating various systems—such as bot detection tools, incident response platforms, and security information and event management (SIEM) systems. This helps organizations conduct a coordinated and efficient response to bot-driven attacks, reducing the time between detection and mitigation.

A policy that promotes the integration of automation and orchestration within the Zero Trust framework strengthens an organization's overall security posture. Automating bot detection and response processes, leveraging advanced technologies such as AI and machine learning, further bolsters the framework.

Policy Recommendations

To fortify your Zero Trust framework against bot-driven attacks, we recommend incorporating these policies:

1. Continuous identity verification using multi-factor authentication combined with sophisticated bot detection to reduce the risk of data breaches caused by stolen credentials and session tokens.
2. Mandating the monitoring and assessment of devices connecting to organizational networks, coupled with advanced bot protection measures, to reduce the risk of botnet attacks.
3. Micro-segmentation of networks and continuous monitoring for bot-driven activities to enhance network security and mitigate the risk of data breaches.
4. Continuous monitoring and analysis of workloads, along with implementing advanced bot detection techniques, to reduce the risk of ransomware attacks.
5. Data classification, encryption (in transit and at rest), and continuous monitoring using sophisticated bot protection systems to enhance data security and minimize the risk of data breaches.
6. Continuous monitoring of security processes, using AI and machine learning techniques to detect anomalies, to improve the organization's ability to detect and respond to breaches.
7. Integrating automation and orchestration into the deployment and operation of the Zero Trust framework to enhance the organization's overall security posture.

Conclusion

Incorporating robust bot detection and mitigation into the Zero Trust framework is essential to enhancing security and defending against the evolving landscape of cyber threats. By proactively addressing the Zero Trust Bot Gap and implementing comprehensive bot protection policies and technologies, organizations can significantly reduce the risk of bot-driven attacks and safeguard their sensitive data, systems, and personnel.

A bot posture is critical for the future of Zero Trust, as it enables organizations to detect and respond to bot-driven threats in real time. By integrating advanced bot detection techniques into each pillar of the framework—including monitoring user behavior patterns, analyzing network traffic, and detecting anomalies—organizations can identify and mitigate bot-driven attacks before they cause significant damage.

Integrating bot detection and mitigation into the Zero Trust framework establishes a proactive defense approach that aligns with the principles of least privilege, strict access controls, and continuous monitoring. This comprehensive bot posture not only addresses past incidents but also prepares organizations for future bot-driven attacks, minimizing the risk and impact of potential breaches.

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**.