An attacker-centric approach to bot-based security through Modern Defense: An Overview of HUMAN Security, Inc.

Prepared by
Christopher R. Wilder
Research Director & Senior Analyst, TAG Cyber
Forbes Contributor
chris@tag-cyber.com

Version 3.0
June 4, 2022

Bots and botnets pose one of the most existential threats to every organization, government, and consumer. A new approach is required to address this critical risk, utilizing visibility, holistic protection, and disruptions to counter sophisticated bot attacks. HUMAN's commercial offering implements these requirements effectively.

Introduction

HUMAN, a bot and fraud defense company, estimates that 77% of all cyberattacks are bot-based. Despite considerable attention across the cybersecurity community, including enterprise security teams and commercial vendors, the proliferation of complex cybercriminal organizations uses sophisticated bots as their weapon of choice to create significant cyber risk. Effective bot protection requires a holistic approach. Outdated methods and technologies, gaps in the infrastructure, and compromised or hacked systems can expose sensitive and personal data. Effective bot-based security must be proactive and with an attacker-centric mindset.

A modern defense strategy allows organizations to safeguard their applications and infrastructure and improve detection and prevention functionality while improving their response to ever-evolving and sophisticated bot-based attacks from determined hackers & crackers. An additional challenge is an exponential increase in the need for enterprises to defend against and prevent bot-based attacks from reducing customer friction, data contamination, and cybersecurity exposure. So much so that the demand is quickly surpassing many SecOps teams' visibility and ability to protect their environment.

This report provides an overview of the evolution of the bot and fraud security industry, emphasizing the various methods security professionals use to mitigate threats. Next-generation requirements must address bot security challenges and how the commercial HUMAN solution delivers visibility, real-time mitigation, and behavior analysis to win against bot threats.

Managing Today's Bot Security and Fraud Threats

Bots are one of the most menacing and effective attack methods used by nation-states, cybercriminal networks, and bad actors. Bots have become increasingly sophisticated, look and act like humans, lightweight and small footprint software packages that deploy automated web requests programmed to execute specific goals. Examples include:

- **Account takeover (ATO):** These bots leverage credentials purchased on the dark web to target, attack, and take over their intended victims' online accounts. One of the original bots used was to execute distributed denial of service (DDoS) attacks against enterprises, governments, and financial institutions to overwhelm and take down critical systems with targeted attacks.

- **Content scraping:** Cybercriminals steal information and content, infecting systems using a SQL injection to infest organizations with malware, API, or e-commerce attacks to take personal credit information (PCI) or patient healthcare records.

- **Influence:** Attackers will also use bots to influence customer behavior by implementing fake likes, dislikes, and comments to sway opinion on a product or company. Bad actor nation-states use bots to manipulate public perception using disinformation campaigns to affect an election, influence policy, and, most recently, distribute propaganda in the Russia/Ukraine conflict.

- **Fake account creation:** Another key use case impacting enterprises today like Twitter and PayPal is phony account creation. Sophisticated bots can quickly and easily create large numbers of counterfeit new user accounts. The accounts are either completely fake or are made using details where the real human is unaware of the fraud. These new phony accounts carry out malicious activity, such as payment fraud, special offers, discount abuse, and spam and misinformation spreading.

Most cybercriminal organizations start with bots to launch an attack. From a tactics, techniques, and procedures (TTP) perspective, botnet attacks account for over two times more than the next TTP used by bad actors. For example, in the past 30-days, our team at TAG Cyber has been actively tracking nearly 55 newly activated botnet campaigns targeting governments, energy & utilities, enterprise infrastructure, financial institutions, and the media - these are in addition to over 100 campaigns launched in the past year. The usual suspects include TeamTNT, Lazarus Group (N. Korea), the Keksec Group (also known as Nero and Freakout), and Sandworm from Russia, which

has recently launched sophisticated botnet attacks against targets in Ukraine, South Korea, Europe, and the US.

Today's ever-changing threats require a modern defense strategy to safeguard against evolving and sophisticated bot attacks.

Building an effective defense strategy to safeguard against bot attacks

Building an effective defense strategy combines intelligence to understand what and where threats are deployed and their respective targets. Organizations must deploy smart, adaptable solutions based on automation and intelligence to detect and mediate attacks. A platform-based approach protects all vectors within the organization from applications, databases, hardware, communications systems, its employees, and customers from malicious bot attacks.

Sadly, most security teams are reactive and approach threat management by focusing on the most well-known attacks and ignoring what they don't know. They invest in point solutions to mitigate specific dangers and what they know about, like denial of service (DDoS), viruses & malware, data leakage, and ransomware, without realizing that nearly all these attacks originate from bots.

An effective bot strategy requires an attacker mindset with visibility and insight into what they know and what they don't know. Additionally, and oft-overlooked, is an understanding of the damage an attack can cause from a financial, branding, reputational, trust, and cultural perspective.

An attacker mindset leverages all available resources and weapons and real-time intelligence to deploy the attack, identify vulnerabilities, and emulate outcomes and potential scenarios. HUMAN has a unique approach to deploying a modern defense strategy against sophisticated bot attacks and fraud.

HUMAN's Defense Platform Overview

There are three pillars for an effective counter-bot strategy; 1.) Observation & Detection 2.) Network Effect 3.) Disruption. HUMAN's Modern Defense Strategy helps organizations safeguard against sophisticated bot-based cyber-attacks and fraud. Traditional defense methods such as CAPTCHAs, web application firewalls (WAF), or content delivery networks (CDN) have become obsolete. Determined hackers and crackers have found ways to circumvent these deterrents. HUMAN's approach addresses each of the above pillars.

1. **Observation & Detection through Internet-scale Visibility:** HUMAN's solution to observation and detection is "Internet Visibility." Their unparalleled visibility into the digital ecosystem enables them to verify the humanity of over 15 trillion interactions per week and see over 3 billion devices per month. This visibility

gives HUMAN a "cat-bird" seat to see, verify, and mitigate most bot attacks before they start, protecting their enterprise customers from the most sophisticated bot attacks.

2. **The Network Effect:** Human collectively protects 2,000+ customers, ecosystem partnerships, industry groups, government, and education. Their Human Defense Platform leverages 350 algorithms based on technical, statistical, and machine learning analysis to detect and safeguard an organization's applications, infrastructure, people, and services. Further, HUMAN's network of 2,500 dynamic network, device, and behavioral signals allows them to understand the threats to the enterprise and stay ahead of bad actors at all levels. Their cumulative and continuous adaptation strengthens protection across all customers.

3. **Disruptions through Actionable and Contextually Relevant Threat Intelligence:** Threat intelligence is arguably the best defense against bot attacks and bad actors. HUMAN has amassed over 10-years of intelligence, tradecraft, and best practices for combating advisory attack vectors and TTPs. Bot decisions and insights occur with unmatched scale, speed, and precision, including defending, dropping, deceiving, disabling, and defeating. By disrupting cybercrime enterprises, organizations can reduce the cost of a breach and eliminate the risk of being compromised.

Examples of cybercriminal disruptions from HUMAN include taking down **PARETO**—the most sophisticated connected television (CTV) device impersonation botnet ever found—in cooperation with Roku and Google. Additionally, HUMAN worked with the FBI, Google, Facebook, and many others to disrupt **3ve,** a bot that affects websites and advertisers. Finally, a coordinated effort resulted in the defeasance of **Methbot**, which recently culminated in the self-proclaimed 'King of Fraud' responsible for the operation being **sentenced to 10 years in prison**.

Conclusion

Over the next weeks and months, we will explore strategies, tactics, and challenges when developing a viable modern defense strategy against bots, fraud, and sophisticated cyber-attacks. We will outline protective plans by industry and highlight what top enterprises are doing to protect their brands, reputation, supply chains, and customers from sophisticated bot-based attacks.

Recently TAG Cyber's CEO Ed Amoroso had a sit-down discussion with HUMAN Security Inc's CEO & Co-Founder Tamer Hassan to discuss modern defense strategies for bot mitigation. Click here to learn more.