BOT MANAGEMENT FOR ADVANCED CYBERSECURITY, ONLINE FRAUD PROTECTION, DATA AND SERVICE INTEGRITY FROM HUMAN

EDITED BY DR. EDWARD AMOROSO
CEO & SENIOR ANALYST, TAG CYBER

TAG CYBER HUMAN

BOT MANAGEMENT FOR ADVANCED CYBERSECURITY, ONLINE FRAUD PROTECTION, DATA AND SERVICE INTEGRITY FROM HUMAN

EDITED BY DR. EDWARD AMOROSO,
CEO & SENIOR ANALYST, TAG CYBER

This anthology was developed by the TAG Cyber analysts in conjunction with the Human Security team. It examines bot management for advanced cybersecurity and online fraud protection, as well as data and service integrity.

SOLUTIONS TO THE BOT CHALLENGE

In today's digital world, businesses and organizations are continuously under threat from cybercriminals and bots. The ever-increasing sophistication and diversity of bot attacks have made them a significant challenge for companies to overcome. Therefore, it is essential to have a comprehensive and proactive bot management strategy to protect against online fraud and ensure data and service integrity.

The TAG Cyber analysts have compiled an ebook that examines the latest trends and insights in bot management, in partnership with HUMAN Security—a leader and innovator in advanced cybersecurity.

This ebook is a valuable resource for any business or organization seeking to enhance its bot management strategy. Each chapter covers a specific industry sector—including finance, streaming services, media, e-commerce, healthcare, insurance, travel, entertainment, and the public sector—providing a comprehensive overview of the current state of bot management while offering practical guidance on how businesses and organizations can protect themselves from cyber threats and online fraud. As shown in Figure 1 below, HUMAN Security's three-pillar approach to bot management will prove an invaluable solution to any organization in its fight against bot attacks.

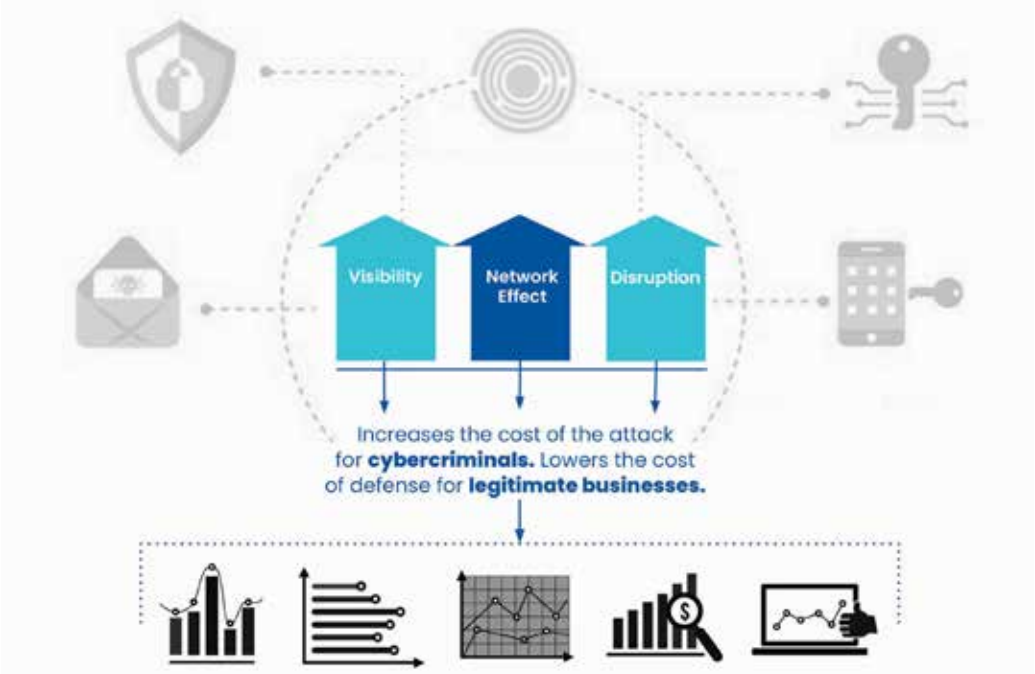


Figure 1. HUMAN Security's Three-Pillar Strategy

THE SCOURGE OF BOTS AGAINST THE FINANCIAL SECTOR

GARY MCALUM, SENIOR ANALYST, TAG CYBER

In the cat-and-mouse arms race of cybersecurity, botnet operators are winning as they "out-innovate" and outpace security teams.

Bots and botnets pose some of the most significant cyberthreats to organizations doing business on the internet today. While they can be found in every industry sector, they are highly prevalent in the financial services (FinServ) sector and are routinely used by cybercriminals against a range of FinServ organizations—from traditional banks to neobanks and payment exchanges. While many financial organizations employ some form of bot mitigation, the sophistication of today's bot threat has typically outpaced most of these traditional countermeasures.

While financial institutions—and traditional banks, in particular—have a long history of dealing with consumer fraud, they have usually been behind the power curve, as consumer business moved increasingly online, and services, such as e-commerce, web bill pay, money transfers, etc., became more accepted. The shock of COVID-19 further exacerbated the move away from in-person banking to digital banking. During this same timeframe, the world of cybercrime has steadily capitalized on technology to automate, scale, and improve fraud operations against the financial sector. Instead of one cybercriminal per fraudulent transaction attempt, as in the good old days, the stakes were quickly raised when bots and botnets became a standard (and perhaps favorite) tool within the criminal's toolbox. Now, thousands, tens of thousands, or even hundreds of thousands of transactions can be executed with a botnet by a single individual or small group. Like a sophisticated military weapon, once the botnet logic has been programmed, it can be launched as a "fire-and-forget" operation on a massive scale, either targeted against a particular organization or on a more indiscriminate, widespread basis. In the financial sector, most of the threats remain the same, but at much greater volume—for example, fake account creation, account takeovers, new account promotion fraud, and socially-engineered scams.

The advent of bot technology has also introduced new threats against the financial sector, which are focused on the more sophisticated exploitation of online accounts and services. While defenses have incrementally

improved, bot techniques are increasingly able to mimic expected human behavior and circumvent security controls. Many financial institutions use some level of bot mitigation, typically based on rudimentary technical detection indicators such as velocity, volumetric, or frequency variables. While these techniques achieve some success, most sophisticated botnet operations easily defeat these relatively ineffective countermeasures.

An effective botnet defense strategy enables FinServ organizations to improve detection and prevention functionality while also boosting their response to ever-evolving and sophisticated bot-based attacks from determined cybercriminals. Many financial organizations don't even realize they have a bot problem until fraud losses suddenly spike and an extensive analysis leads to the rude awakening, "Houston, we have a bot problem."

Bots Targeting the Financial Sector

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; they look and act like humans and have lightweight, small-footprint software packages that deploy automated web requests programmed to execute specific goals. A **recent report** on bots confirms that the financial sector is the most heavily targeted and has the most "bad bot traffic." Within the financial sector, typical targets include:

- **Traditional Banks of All Sizes.** Traditional banking institutions and their customers are continuously targeted by botnets. Typical defenses used content delivery networks (CDNs) and web application firewalls (WAFs), providing some relief but often falling short.
- **Insurance Companies.** When opening new accounts and processing claims, insurers capture, process, and retain large amounts of data, including publicly identifiable information. Insurers are linked through multiple networks, including acquisition, capital raising, and debt issue activities to other financial institutions. They also conduct mergers and acquisitions or other changes that can impact cybersecurity in the organizational structure.
- **Neobanks and Fintech Startups.** As one of the most rapidly growing sectors, Neobanks and FinTech banking services have also become a main target of bot attacks. Their success provides a lucrative attack vector for bad bots conducting fraudulent transactions, account takeovers, new account promotion fraud, and more.
- **Payment Services.** Online payment platforms are also a juicy target for bots. For example, botnets can be used to command and control large-scale, targeted phishing attacks. One recently discovered botnet was designed to generate scams targeting users of the payment app Zelle. Botnets can conduct massive schemes to collect data and gain access to networks with little effort from the attackers. According to a report by the industry consulting firm **Javelin Strategy and Research,** some 18 million Americans were defrauded in schemes perpetrated on person-to-person money transfer apps like Zelle in 2020.

Typical Examples of Successful Bot Attacks Against the FinServ Sector
While there are many cybersecurity threats that are of concern for to security teams, botnets are a constant threat for to financial service companies. According to a recent **Forbes article,** cybercriminals use botnet assaults to accomplish a variety of tasks, including gaining access to financial and personal data; overwhelming reputable web services; extorting funds from victims; selling access to other criminals; employing scams involving cryptocurrency; exploiting backdoors created by viruses and worms; and deploying malware, such as keystroke loggers. Some areas of particular concern in the financial sector include the following:

- **Fake Account Creation.** Digital account openings are a vital function of any transaction-based company, particularly in the digital banking and financial services space. But even the most security-conscious organizations remain vulnerable to potential fraud and financial loss. Customer expectations for real-time decisions also drive up risk. Cybercriminals routinely use stolen identity data combined with bots to open accounts at a very fast rate. In a recent blatant example of bot-enabled fraud, PayPal Holdings Inc. said it **"closed 4.5 million accounts** and lowered its forecast for new customers after finding 'bad actors' were taking advantage of its incentives and rewards programs." Given the vast amount of personally identifiable information (PII) available on the black market due to countless data breaches over the years, it's clear that this trend will only increase.

- **Account Takeovers.** Account takeovers (ATOs) are an increasingly popular attack vector and of particular concern for organizations, due to potential compliance violations that can result from the loss of personally identifiable information, and brand damage achieved incurred through the loss of customer trust. ATOs are often facilitated by large-scale credential-stuffing attacks that attempt to link stolen credentials against consumer financial accounts. According to a **recent report** by Aberdeen Strategy Research, automated fraud (e.g., fraud facilitated through botnets) has gone from being a cost of doing business to a material business risk for financial institutions. Of even greater concern are the results from a recent study, **Three Out of Four Attacks: Sophisticated Bots and What Enterprise Security is Missing.** Conducted on 100 cybersecurity and IT professionals at companies with 500 or more employees, this study found that during the last 12 months, organizations experienced, or believe they experienced, attacks that could pose major issues to their operations, including site slowdowns caused by overwhelming traffic (35%), credential stuffing (25%), ATOs (21%), and content manipulation (20%). For most organizations (81%), the need to protect public-facing websites and applications from bot-driven attacks, fraud, and logic abuse were ranked among their top 10 priorities. In practice, however, just a quarter (24%) used bot-management tools, and only 7% used a specialized bot-management solution. Finally, a related issue driven by ATO is the increasing focus of fraudsters on Buy Now,

Pay Later (BNPL) schemes. In a recent **blog,** Imperva warned that new and emerging sectors like BNPL are often the favorite targets of fraudsters, as they may initially have gaps in security and regulation that can be exploited. Both ATO and new account fraud (NAF) could impact the BNPL sector.

- **New Account Promotion Fraud.** Digital promotions are an excellent way to drive sales and increase brand awareness. Many financial companies leverage promotions over social media and other channels by promoting special rates, prizes, or other rewards to entice new customers. Unfortunately, contests, sweepstakes, and other games are particularly vulnerable to botnets and cybercriminals as they attempt to cheat or manipulate outcomes. Bots are easily used by fraudsters to generate entries or votes. In other cases, it's easy to create multiple fake accounts to increase the odds of success. Many cheaters use bots to generate entries or vote for themselves in contests and sweepstakes. Others may simply manually sign up for them with multiple fake email addresses or social media accounts.

- **Customer Friction.** It may not be a direct effect caused by botnets, but the inevitable pain inflicted on digital consumers has continued to increase as companies attempt to fight off bot attacks. Perhaps the most obvious friction-inducing countermeasure is CAPTCHA, short for "completely automated public Turing test to tell computers and humans apart." CAPTCHA is simply a security test and control designed to stop automated attacks by requiring human-like cognitive capabilities. According to a 2019 **Forbes article,** "Today, the vast majority of e-commerce and travel sites require some sort of CAPTCHA to perform specific, more sensitive tasks for a significant percentage of users. There are multiple types of CAPTCHAs—they can ask users to decode blurry text, determine which parts of a picture contains a tree or a traffic light, solve a simple math problem or comprehend a word against a field of noisy audio." Despite the widespread use of CAPTCHA, however, the bot problem hasn't really been solved, and customers are getting more frustrated. The article goes on to suggest they are doing more harm than good, often discouraging consumers and leading to increased abandonment rates. Online consumers have come to expect an increasingly frictionless experience, especially when making transactions. Businesses ask them to share private information, and, in return, consumers expect easy, fast, and secure engagements. If they can't conduct transactions in a straightforward manner with minimum hassle, they may move on to competitors—and sometimes never come back.

Current Countermeasures are Ineffective and Insufficient

Most financial institutions employ some level of botnet detection and mitigation. While DDoS countermeasures have improved over time, these are typically employed primarily by larger, well-resourced financial institutions. Many other botnet threats, such as credential stuffing, malware

delivery and so forth have outpaced the traditional bot mitigations employed by CDNs and Internet Service Providers. In many cases, financial organizations continue to rely on embedded bot-mitigation features within application security platforms, while others use the features available in discrete tools, such as web application firewalls (WAFs). Many financial institutions use some level of bot mitigation, typically based on rudimentary technical detection indicators such as velocity, volumetric or frequency variables, and static block lists. However, most sophisticated botnet operations are easily able to defeat these relatively ineffective countermeasures. While a consolidated approach can be attractive from an operational and cost perspective, any efficiency gains are quickly lost if the solution is not effective in detecting and preventing attacks. And, of course, CAPTCHAs continue to be used to some degree of moderate effectiveness, despite the consumer pain they inflict.

Unfortunately, in the cat-and-mouse arms race of cybersecurity, botnet operators are winning as they "out-innovate" and outpace security teams. With advances in artificial intelligence and machine learning, botnets can now rapidly adapt and expand cyberattacks while evading existing countermeasures. There is also the growing problem of "Bot-as-a-Service" being used by cybercriminals to outsource attacks. Everyone is jumping on the bot train.

The good news is that there are defenses available for companies that incorporate specialized bot protection tools to detect and mitigate bot attacks. This is a problem where it pays to use a company that is focused predominantly on the bot problem. **HUMAN Security** has significant success in stopping botnets in cooperation with law enforcement and industry. The company has taken an aggressive, collective approach, using top-line signature and behavioral detection techniques that build on hacker intelligence. They synthesize that data with a real-time decision engine that combines technical evidence with machine learning to offer rapid and accurate "bot or not" decisions, ensuring human-only interactions. HUMAN's ability to uncover, reverse engineer, and disrupt bot-driven threats is impressive, especially their cooperative efforts in take down **Methbot.**

Conclusion (and the Future)

Unfortunately, the bot problem is not getting better; in fact, it's only getting worse. According to internal research by HUMAN Security, bots are used in 77% of cybercriminal attacks. Fortunately, it's not an insurmountable problem when the right approach is employed. As nicely summarized in a recent **Forbes article,** "Cybersecurity in general needs a newer and evolved set of strategies that includes threat intelligence, technical tools & expertise, advanced analytics, cost mitigation, and collaboration. Botnets are not going to go away. However, changing the approach to better enable 'the side of good' will help keep us better prepared to defeat sinister threats before and when botnets attack." In other words, there is hope.

Companies like HUMAN are pushing the envelope in cybersecurity innovation, helping the financial sector and others keep pace with the dynamic and ever-changing scourge of botnets. Ultimately, it takes sophisticated and agile solutions to beat the sophistication and agility of today's cybercriminals and their unrelenting bot campaigns. HUMAN's counter-bot strategy is based on three pillars: visibility, network effect and disruption—all of which are focused on increasing the cost of the attack for cybercriminals while lowering the cost of defense for legitimate businesses (See Figure 1).

This strategy has clearly worked; they have partnered with law enforcement in some of the highest-visibility bot takedowns to date. HUMAN played a leading role in thwarting the self-proclaimed "King of Fraud!" Aleksandr Zhukov's Methbot operation, one of the largest private/public sector collaborations in cyber history. With no sign of the bot problem slowing down, HUMAN is here to release the counter-bot hounds!

HOW BOTS ARE AFFECTING STREAMING SERVICES AND MEDIA

DR. EDWARD AMOROSO, CEO, TAG CYBER

The problem bots create for streaming and media services is that they make gaining an accurate picture of the true market, based on real human users, difficult.

In recent years, the term "streaming wars" has joined the business lexicon as a meaningful reference. Fought by the great media giants, this ongoing global battle is all about gaining hypergrowth from binge-watching consumers around the world. Tactics involve everything from mergers and acquisitions to spin-offs and anything else the boardroom believes can create a marketing advantage.

One poorly understood backdrop to this public and highly visible streaming battle is a somewhat invisible threat—one that can easily undermine the entire streaming and media industry if not properly controlled. This threat stems from something known as a "bad bot" (or just bot), which can be thought of as a computer program masquerading as a human user, generally for malicious purposes, such as taking over an online account.

The problem bots create for streaming and media services is that they make gaining an accurate picture of the true market, based on real human users, difficult, and the development of usage metrics can be significantly clouded if accounts belong to bots that are generated to commit fraud. Certainly, the motivations for bot creation will vary, but most streaming-focused bot threats have a financial goal, such as spin fraud, as well as stealing sign-up bonuses, vouchers, or accounts.

Nevertheless, a healthy streaming and media industry simply *must* include some means to determine whether a given account belongs to John, the human being from Madison, New Jersey, or *John,* an automated bot running on a containerized instance in AWS and controlled by a hacker in Russia. Without the ability to differentiate between human and non-human activity, one wonders if the streaming war might be lost by all participants.

Enter companies such as HUMAN Security. Their platform is designed to specifically address threats such as account takeovers and fake account creation by bots. It also enables streaming and media customers to take response action against these bad bots. This is done through advanced heuristics and technical strategies that leverage the indicators of a bot. Streaming and media companies can benefit from such determination.

The HUMAN Security approach and **modern defense strategy** should resonate with readers familiar with the well-known Turing test—although the company's modern solution goes way beyond the original "Are you a human" algorithms from early computer-science classrooms. Along with their three-pillar approach to bot management (See Figure 1), HUMAN uses a range of powerful techniques to reduce the risk of account takeover, fake account creation, payment fraud, content manipulation, content scraping, spin fraud and more.

From a TAG Cyber analyst perspective, we cannot imagine a security and anti-fraud technology better suited to the ongoing specific challenges of streaming and media companies. While greater clarity about bots may impact the industry by producing some near-term jolts of truth into the common metrics used by marketing teams, the long-term benefit of high-integrity management for streaming and media services is immeasurable. If you are in this industry, we strongly recommend that you contact the HUMAN Security team and listen to their story. The time will be well spent.

HOW BOTS ARE AFFECTING E-COMMERCE AND DIRECT-TO-CONSUMER BUSINESS CHANNELS

GARY MCALUM, SENIOR ANALYST, TAG CYBER

Companies often discover, after the fact, skewed traffic metrics or volume stats that don't make sense when looking at overall sales and completed transactions.

The pace of digital transformation has never been greater, and the new post-COVID world has only driven up the volume and frequency of online transactions, particularly in the e-commerce and Direct-to-Consumer (DTC) channels. Not surprisingly, cybercriminals are following the money and targeting these lucrative sites. Online retail is a main target for cyberattacks, with malicious bots playing a primary role. With these automated tools, cybercriminals can attack far more targets in far more damaging ways than they could accomplish manually. These bots are specifically designed to mimic the actions of legitimate users, making them notoriously hard to detect and allowing their operators to perform malicious activities on a site or platform. In 2021, these "bad bots" accounted for **over 50% of all internet traffic,** and no industry was spared.

By any available metric, the amount of bad bot traffic has intensified, jeopardizing the effectiveness of the online shopping experience for everyday digital consumers while also creating a significant challenge for companies struggling to deal with unrelenting daily attacks. Companies often discover, after the fact, skewed traffic metrics or volume stats that don't make sense when looking at overall sales and completed transactions. As an **E-Commerce Times article** states, "Even more concerning is the time it takes to discover these attacks. On average, more than 14 weeks pass between a successful attack and its detection. This makes it difficult to limit the damage done to a business's customer satisfaction, reputation, and bottom line." When it comes to malicious bots, the old saying is true: Time is money. Panic may begin to set in at this point but wait. There's hope! Hang in there a little longer.

The Impact of Bots on E-commerce and DTC Channels

Online retail remains a prime target for automated bot activity. Bots carry out an array of disruptive and even malicious activities on retail sites, including price and content scraping, scalping, denial of inventory, carding, and other types of online fraud. According to the article, **Report: 57% of all E-commerce Cyberattacks are Bot-Driven** the volume of monthly bot attacks on retail websites rose 13% in 2021 compared to the same period of the previous year. This underscores the growing threat retailers and consumers face from bad bot activity. In comparison, bots were to blame for just 33% of total attacks on websites in all other industries.

While there are many bot risks to be concerned about—such as distributed denial of service (DDoS) attacks—bots pose some unique risks against e-commerce and DTC channels, including those listed below.

- **Credential Stuffing.** This is child's play for bot operations, as they seek to validate stolen credentials and gain access to existing online retail accounts. The bots "stuff" usernames and passwords into e-commerce sites, attempting to gain access. Most of these credentials are obtained from data breaches of other sites. Hackers know that many people re-use credential sets across sites, so credential stuffing can often be successful. Once bots gain access to one or more accounts, cybercriminals will further exploit this access directly by making fraudulent purchases, or indirectly, by selling the access on the Dark Web. The traditional countermeasure, CAPTCHA, is almost completely ineffective against today's sophisticated botnets.

- **Inventory Hoarding.** Another common bot attack involves malicious actors that configure bots to automatically place high-demand merchandise into carts. The goal is to hinder true sales and prevent trending SKUs from gaining traction during peak buying periods. Inventory denial bots mimic human traffic; in large volumes, they place items in checkout baskets, fooling systems into thinking that the inventory is sold out. These bots are often used to target theater ticket booking systems for popular shows. They are also used to frustrate customers from making a purchase, thereby driving a backlash of negative feedback against the brand on social media.

- **Scalping Bots.** These malicious bots swarm the internet and social media, searching for hot trending products, such as entertainment tickets. They identify the most profitable targets and then buy all available inventory so cybercriminals can resell these items at multiple times the original retail price. Through sophisticated automation, they can complete the checkout process in a fraction of the time it would take any legitimate user. This essentially results in a "denial of inventory" for legitimate consumers. It is easy for advanced bots to circumvent basic security controls like CAPTCHA. In addition, by continuously guessing until a positive response is

received by the website, scalper bots often circumvent any limit on ticket purchases set by the vendor. They can fill out hundreds of credit card numbers at one time; it would be virtually impossible for any human being to do this manually and without errors.

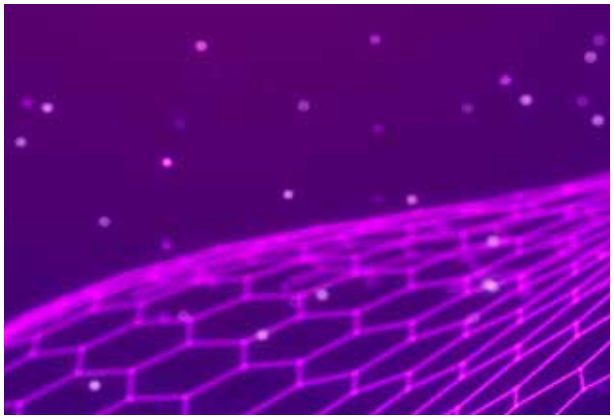
- **Marketing Impact.** Perhaps the most concerning and misunderstood impact of bots is their negative effect on marketing data and analytics. Business decisions are based on data, and bots can severely skew or contaminate the data in such a way that they negate good decision-making processes and ultimately impact the bottom line. IBM research shows that $3.1 trillion is lost each year due to bad data. Sophisticated Invalid Traffic (SIVT) is generated when malicious bots view and click on ads to inflate conversion numbers, resulting in wasted advertiser spend. Many organizations put their budget toward advertising and re-marketing campaigns with the goal of seeing those investments pay off in the form of pipeline and revenue. However, when bots and fake users are present, this can pose serious issues for these initiatives. SIVT can drain budgets by interacting with advertisements, as well as polluting audiences until they are no longer usable.

- **Carding.** In cybercrime, "carding" typically involves using stolen credit card information to make fraudulent purchases or financial transactions via phishing scams, database hacking, or purchasing stolen card information on the black market. Carding is illegal and can result in criminal charges and penalties. Criminals often use malicious bots in carding to automate the process of testing stolen credit card numbers or payment credentials on e-commerce websites or payment processors. These bots attempt to make multiple purchases simultaneously, increasing the chances of success in obtaining goods or services with stolen information. Bots can also test credit card numbers by generating random numbers and validating them on merchant websites to determine which are valid and which they can use for fraud. In addition, bots can scrape credit card information from compromised websites or databases, to be used in carding or sold underground.

Conclusion

As mentioned earlier, despite the sense that this is an overwhelming problem, there is hope! Enter companies such as HUMAN Security. HUMAN has a long track record of helping online retailers deal with the problem of sophisticated botnets targeting their e-commerce platforms and applications. Their anti-bot capabilities are sophisticated, employing a range of powerful techniques that reduce the risk of account takeover, credential stuffing, fake account creation, payment fraud, content manipulation, content scraping, denial of inventory, and more. The issue of malicious bots and fake users is more than just a security and IT problem for online retailers. It is an existential threat to e-commerce platforms, and it must be addressed with countermeasures that are as sophisticated

and agile as the botnets being employed by cybercriminal organizations. Deploying more complicated CAPTCHAs is not the answer! Since malicious bots impact all areas of an organization, more and more online retailers are learning to prioritize go-to-market security as a strategic solution. By mitigating the risk of harmful web traffic, companies can ensure all assets are protected and focus their time on running their business.



HOW FORWARD-THINKING HEALTHCARE AND INSURANCE ORGANIZATIONS ARE DEFENDING AGAINST BOTNET ATTACKS

CHRISTOPHER R. WILDER, TAG CYBER

Nearly 90% of healthcare-related attacks originate from bots that use attack methods.

It is estimated that hackers target the healthcare and insurance industries two times more often than any other industry. In the last 12 months, we have monitored over 1,800 indicators of compromise (IOC), averaging 18 unique tactics, techniques, and procedures (TTPs) targeting the global healthcare industry. Today, nearly 90% of healthcare-related attacks originate from bots that use attack methods. Bot attacks include ransomware, account takeover (ATO), credential stuffing, cracking, content scraping, fake reviews, false appointment scheduling, personal identification information (PII), and new account fraud to steal a victim's identity and defraud healthcare and insurance providers.

Meanwhile, the healthcare industry uses bots mainly to help organizations improve customer service and the communication between patients and providers, as well as reduce human capital. However, bots deployed by bad actors are one of the most terrifying and challenging issues security teams face today. A single breach can cause significant damage, reduce trust, generate expensive compliance penalties, lower productivity, and, most importantly, result in the loss of life.

Good Bot, Bad Bot

Bots are prolific, being used and abused for good and bad purposes. For example, we have seen a significant increase in nefarious bot activity in counterfeit drug rings—Viagra and Cialis are the two most sold on the Dark Web. After the initial release of COVID-19 vaccines, there was a flood of counterfeit vaccinations on the market. In counterfeit rings, bad bots establish a massive network of fake affiliate websites with fraudulent

product links. Once one website or link gets taken down, bots deploy dozens more automatically. Service providers and law enforcement cannot respond fast enough to keep up.

What can healthcare and insurance organizations do to reduce the threat of bot attacks? The first and most obvious is to enforce a universal strong multi-factor authentication (MFA) policy. Secondly, though not as effective against advanced or sophisticated bots, many healthcare organizations use IP blacklisting, known as bot signatures. Unfortunately, sophisticated bots can quickly cycle through hundreds of thousands of IP addresses to bypass the organization's protection systems, and blocking is often not the best option.

The most effective anti-bot strategy must be a holistic approach that understands the risks, builds effective defenses against attacks, prepares for the uncertainties of a compromise or breach, and implements protections without sacrificing productivity or collaboration with customers, partners or employees. Because of the complexities and threats to the healthcare and insurance industries, TAG Cyber recommends deploying an end-to-end platform solution for mitigating bot threats, rather than a piecemeal or point-solution approach. HUMAN addresses many of the above challenges when enhancing bot defense in healthcare organizations.

HUMAN's Bot Defense Solutions for Healthcare and Insurance

For many years, the healthcare industry has battled against relentless attacks from determined, organized hackers and sophisticated botnet attacks, and the COVID-19 era took bad actor efforts to a new level. HUMAN's Bot Defender helps healthcare organizations protect critical customer systems, mobile applications, application programming interfaces (APIs), and websites.. Bot Defender reduces fraud, counterfeiting and other emerging threats such as fake account creation, stolen credentials, credential stuffing, ATOs, brute force and other known and unknown TTPs. Its seamless platform minimizes friction while augmenting authentication capabilities and enhancing MFA and CAPTCHA policies.

Conclusion

While many solution providers offer end-to-end solutions, HUMAN's Bot Defender provides functionality that focuses on key challenges while mitigating the various advisory techniques facing healthcare and insurance organizations. We believe HUMAN offers a formidable foundation for reducing the threat of bots and bad actors inside and outside the healthcare and insurance industries.

THE ROLE OF BOTS ON THE TRAVEL AND ENTERTAINMENT INDUSTRIES

JOHN J. MASSERINI, SENIOR ANALYST, TAG CYBER

Botnets can set up thousands of accounts within moments or leverage stolen user credentials to purchase goods with pre-existing accounts.

It's 9:59 am. You've been waiting since before the pandemic to see your favorite band in concert again. You've logged in, got your credit card, and are ready to lock in your 100-level seats on the band's page. You watch the clock turn to 10:00 am. You hit refresh. You find the best seats you can and click Add to Cart—only to get the message: SOLD OUT. It's now 10:03 am. Sixty thousand seats are gone in three minutes.

WELCOME TO THE WORLD OF SCALPING BOTS.

While botnets are often thought of when it comes to distributed denial of Service (DDoS) attacks, account takeover tools, or ransomware distribution mechanisms, the travel and entertainment industries have been dealing with autonomous shopping and inventory bots for quite some time.

In comparison to the rather rudimentary botnets used for malicious attacks and ransomware distribution, shopping and inventory botnets are significantly more advanced, decked out with rich feature sets and options. Oftentimes, such botnets can set up thousands of accounts within moments or leverage stolen user credentials to purchase goods with pre-existing accounts. While scalping is generally associated with concert tickets, in truth, scalpers make money on anything that is in high demand—concert tickets, video game consoles, or special holiday toys, to name a few—all of which are available online these days. In the case of that long-awaited concert, those tickets quickly ended up on a third-party resale/scalping site with an increase in price that was multiple times higher than their original value.

Like the entertainment industry, the travel industry also deals with substantial fraud as a result of botnet attacks. This includes scraping pricing information and automatically updating their site with a slightly lower price, as well as hotel room "blocking," where reservations are made

to make the hotel appear sold out, thereby forcing consumers to choose a different, higher-priced venue. Once the higher-priced hotel is sold out, the bots then cancel the initial reservations, leaving the first hotel scrambling to sell rooms.

Specific vertical, botnet-driven account takeovers continue to be a challenge for most e-commerce sites. Over the years, there have been numerous examples of various types of **loyalty programs being attacked** and **airline loyalty programs** being abused. While many look at this as an almost victimless crime, research suggests differently. According to a **Financial Times report,** American Airlines estimates its loyalty program to have a value between $18 and $30 billion, and United puts theirs at around $22 billion. Make no mistake, misuse of a passenger's frequent flyer miles could have a direct impact on each of these airlines' financials. When you consider that the average **consumer belongs to more than 14 loyalty programs,** the potential financial impact rapidly explodes.

The botnet fraud problem should be a serious concern for every e-commerce site that is running today. When you consider the potential customer-relations impact of disregarding the problem, along with the potential impact on the bottom line, ignoring the bots that visit your site is a potential catastrophe in the making.

BOTS ARE TARGETING THE PUBLIC SECTOR, AND IT WILL ONLY GET WORSE. WHAT CAN YOU DO?

CHRISTOPHER R. WILDER, TAG CYBER

Hackers target federal and state and local government and education (SLED) organizations cyclically; activity increases close to an election or when school is coming back into session.

Due to the treasure trove of information on the public sector, bad bot attacks against government and education websites have greatly increased over the past several years. Bad bots are malicious bots that do various things, from account takeovers (ATOs), false appointment scheduling and website scraping of public information, including voter registration or research. By our estimation, hackers target federal and state and local government and education (SLED) organizations cyclically. For example, activity increases close to an election or when school is coming back into session. Leading up to the 2020 U.S. presidential election, there was a significant increase in botnet attacks on government websites by China, Russia, Iran, and hacktivist organizations. Today's research shows that nearly 30% of federal and SLED-related attacks originate from bots.

Increasingly, the government and education systems are leveraging bots to help their organizations improve customer services and communications between agencies, constituencies, faculty, and students. These organizations use bots to reduce wait times, improve issue resolution and set appointments. Bots deployed by bad actors, however, are one of the most terrifying and challenging issues security teams face today. A single breach can cause significant damage, reduced trust, lowered productivity and the loss of personal data records.

Bad Bots Cause Real-World Challenges

Public sector automated and distributed security attacks from bots and botnets have become a substantial challenge for governments and educational systems. In the past several years, bad actors used bots to identify weaknesses in public sector websites and systems. Hackers used

this information to attack federal agencies. The Departments of State, Treasury, Commerce, Energy, Education, and Defense, along with the Veterans Administration, were all either compromised or breached.

Bots also play a major role in misinformation campaigns by creating hundreds of thousands of fake or automated social media accounts to post negative information about elections, candidates, policies, and political organizations. During the 2020 election, bots were responsible for several million tweets that likely reached hundreds of thousands of individual social media users. Most of these bots were promoting partisan political or COVID-19 pandemic views or conspiracies.

Regarding education, in 2021, the California Community College organization's central enrollment system of 115 local community colleges came under bot attack, which besieged the system with over 65,000 fake student applications in a quest to obtain student aid and pandemic relief grants. Due to limitations in their infrastructure, these institutions could not have visibility into campus-level data, including enrollment and fraud indicators. According to **EdSource,** about $270 million was distributed to nearly 439,000 community college students, including approximately 56,000 students who dropped out after receiving assistance.

Preventing Bot Attacks

So, what can public sector and SLED organizations do to reduce the threat of bot attacks? Similar to the healthcare and insurance sectors examined in Chapter Four, the first and most obvious answer is to enforce a universal, strong multi-factor authentication (MFA) policy. Secondly, many public organizations use IP blacklisting, also known as bot signatures. Unfortunately, sophisticated bots can quickly cycle through hundreds of thousands of IP addresses to bypass an organization's protection systems, and blocking is often not the best option. The most effective anti-bot strategy must be a holistic approach that understands the risks while building effective defenses against attacks, preparing for the uncertainties of a compromise or breach, and implementing protections without sacrificing productivity or collaboration with customers, partners and employees. Because of the complexities and threats to the federal government and SLED, TAG Cyber recommends deploying an end-to-end platform solution for mitigating bot threats rather than a piecemeal or point-solution approach. HUMAN is a solution that addresses many of the above challenges when enhancing bot defense in federal government and SLED organizations.

HUMAN's Bot Defense Solutions for Federal Government and SLED Entities

HUMAN's Bot Defender solution helps federal government and SLED organizations protect critical systems, such as mobile applications, application programming interfaces (API) and websites. Bot Defender reduces fraud, counterfeiting, and other emerging threats, such as fake account creation, stolen credentials, credential stuffing, ATOs, brute force,

and other known and unknown TTPs. Their seamless platform minimizes friction while augmenting authentication capabilities and enhancing MFA and CAPTCHA policies.

Conclusion

While many solution providers offer end-to-end solutions, Bot Defender provides functionality that focuses on key challenges, while mitigating the various advisory techniques facing public government and education organizations. We believe HUMAN offers a formidable foundation for reducing the threat of bots and bad actors inside and outside the federal government and SLED sectors.

ABOUT TAG CYBER

TAG Cyber is a trusted cybersecurity research analyst firm, providing unbiased industry insights and recommendations to security solution providers and Fortune 100 enterprises. Founded in 2016 by Dr. Edward Amoroso, former SVP/CSO of AT&T, the company bucks the trend of pay-for-play research by offering in-depth research, market analysis, consulting, and personalized content based on hundreds of engagements with clients and non-clients alike—all from a former practitioner perspective.

ABOUT HUMAN SECURITY

HUMAN is a cybersecurity company that protects organizations by disrupting 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. Protect your digital business with HUMAN. To Know Who's Real, visit www.humansecurity.com.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Dr. Edward Amoroso, Christopher R. Wilder, John J. Masserini, Gary McAlum

Publisher: TAG Cyber LLC. ("TAG Cyber"), TAG Cyber, LLC, 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman (lgoodman@tag-cyber.com) if you'd like to discuss this report. We will respond promptly.