FIGHTING FIRE WITH FIRE:

How AI Can Protect You From a Bot Attack

Sophisticated ever-evolving bot attacks on business applications cause real financial losses, missed customer opportunities, and hefty operational overhead. Here's how AI-driven machine learning solutions can help.

DATAVISOR

Contents

Introduction

This whitepaper will help you understand how your company can continue to evolve its fraud strategies to counteract a new array of bot-powered threats.

Bot-based attacks are becoming increasingly common. Artificial intelligence (AI) can be used in malware to enable bots to attack enterprise businesses faster and more efficiently than ever before. Bots are even being used to influence our culture around the COVID-19 pandemic. **MIT Technology Review** suggests that between 45% and 60% of the Twitter feeds demanding the reopening of the U.S., spreading false medical information, and conspiracy theories stem from coordinated bot activities.

What do businesses need to understand about how these attacks work and what steps do they need to take to respond effectively? Why won't traditional anti-fraud methodologies keep up with the latest evolution in threat vectors? How can fraud detection software leverage machine learning to keep your business safe?

Understanding Bots

"AI bots are everywhere. People interact with AI when accomplishing tasks such as asking common customer service questions, booking travel, or applying for a loan. "

Bots are software that performs repetitive jobs. A botnet strings together a number of computers to perform a task. They are the workhorses behind a lot of functions on the Internet, and mostly, they do the heavy lifting to enable a smooth user experience.

But general botnets - that were originally a force for good - are frequently harnessed to conduct dirty work, like take over a computer and turn it into a zombie under the control of a remote operator. These botnets make up a spider web of computing horsepower that can perform illegal functions such as banking application fraud.

Now, to make things even more interesting, there are AI botnets.

AI bots are everywhere. People interact with AI when accomplishing tasks such as asking common customer service questions, booking travel, or applying for a loan. Many websites have a layer of cognitive bot interactions with customers on the front end of the buying process.

Individuals can also commonly interact with AI bots by using personal devices such as Alexa or Siri. These tools are growing more sophisticated through the use of natural language processing to understand human speech and machine learning to increase the accuracy of their interactions with the end user.

The problem is, in tandem with the adoption of AI bots by enterprise organizations for a force of good, unscrupulous programmers are using these same tools to wreak havoc, causing real financial losses, missed customer opportunities, and hefty operational overhead.

THE PROBLEM WITH BOTS

The use of AI bots is increasing as corporations invest more in bots. **IDG reports global spending** on AI systems is expected to reach nearly $80 billion by 2022. Companies such as Amazon and Google have invested heavily in this technology. However, malicious actors now make use of bots as well. Fraudsters use botnets for nefarious activities designed to steal identities, data, and cash.

Take just one industry sector—insurance—and you can witness the widespread growth of fraudulent activity. The **Coalition Against Insurance Fraud reports** that hackers cost the industry $80 billion a year. Much of this fraud is handled manually by humans, but that is changing rapidly as AI automation makes fraudsters more efficient.

Part of the problem is that the number of transactions has increased along with the number of payment channels, from smartphones and kiosks to websites. Fraudsters take advantage of these complexities and use AI to automate online and mobile attacks.

The problem—and the benefit—of today's AI technology is that machines can be taught to mimic human behavior. AI-enabled computer bots can perform checkout abuse for online ticket sales by appearing to be consumers and buying out all the tickets for an event within a minute thus forcing customers to pay higher ticket prices on a fraudulent site.

Bots can be programmed to perform click fraud by repeatedly clicking on an advertising link to drain revenue from an advertiser or to generate cash for the host site. Businesses are **losing about $16 billion a year** on this type of fraudulent activity. Here are two examples:

- PC-based botnet 3ve utilized more than a million computers into a botnet to conduct click fraud across websites around the globe. Most owners of the infected machines did not realize it until the FBI and Google took down the botnet scheme in 2019. Before it was stopped, the botnet **siphoned $30 million**.
- **The Daily Mail released footage** of a bot farm that uses the software across thousands of mobile devices, emulating the human activity of liking and rating apps to boost their popularity. AI bots can be used to impersonate humans to unlock security systems and steal money from accounts. These stolen signatures and identities can be used to create new synthetic identities that form the crux of a massive wave of insurance application fraud.

The reality is that AI is now used by cybercriminals to ramp up their attacks. These tools are used for automated CAPTCHA breaking and phishing attacks, repeated attempts to probe security infrastructures for vulnerabilities, and the faster creation of new, improved versions of malware designed to avoid detection. Traditional security technologies are proving ineffective; these tools cannot continuously adapt to the new AI-driven threats.

The increasingly sophisticated nature of AI bot attacks can only be mitigated by the same technologies.

What Companies Need to Know About Bot Attacks

Q&A with Fang Yu, DataVisor Co-founder and CTO

Q **Bot-based attacks appear to be becoming increasingly common. What are some of the kinds of fraudulent bot activities out there today that businesses should be concerned about?**

We are seeing bots increasingly have a negative impact on companies. And a data breach or identity theft are just the start of the process. Bots can create synthetic or steal real identities, then **apply for fraudulent accounts** with credit card, banking, and insurance companies. Bots can take over entire customer accounts. We see bots at work cracking eCommerce sites and on social media with fake news, friending, phishing scams, and even **unemployment scams** during COVID-19. Businesses should understand this isn't a static threat. Five years ago, we didn't see a lot of bot attacks on mobile devices, but today it's a growing problem.

Q **Can you elaborate on the proliferation of bot attacks on mobile devices?**

One common technique that's growing in popularity is web scraping, where botnets are used to cull specific data from accounts. For example, in 2018, Cambridge Analytica made the news for all the wrong reasons; and a Facebook incident followed where members' phone numbers—about 400 million—were grabbed by bots. Bots can scrape mobile phones and use the data to commit application fraud or other types of malicious activities.

Q **What are the key lessons that businesses often fail to learn after they've been a victim of a bot attack?**

One key lesson is that reactive approaches to existing bot attacks do not work because of the changing nature of these threats. Typically, we see companies experienced the attacks and then moved to block that threat. What they don't realize is that these behaviors change very often. The bot attack is ever-evolving, and a reactive approach does not prepare the company moving forward for future attacks.

How can businesses respond more effectively and proactively to bot attacks?

DataVisor's unsupervised machine learning (UML) is a proactive, holistic approach that deploys different products across a wide swath of a company's digital infrastructure. Each tool is designed to pinpoint the source of a bot attack very early on before traffic is generated and damage occurs.

We have four primary solutions that can identify bot attacks and mitigate threats:

dEdge is designed to protect mobile applications from bot attacks in real-time. It is built to detect advanced attack vectors such as emulators, rooted or hooked devices, or apps that are repackaged by fraudsters, **dEdge delivers advanced mobile and web app protection** suitable for banking, fintech, e-commerce, social, and travel platforms that use these tools to enhance the customer experience. The application also conducts device fingerprinting designed to collect real-time verification data on location, timestamp, languages, user agents, and more.

dOps combines the simplicity of traditional rules analysis with modern machine learning for an enterprise-level solution for your runtime production environment. dOps helps fraud teams adapt to unusual fraud activity as well as real-time business risk with agility, control, and scalability.

dVector is a managed fraud detection service powered by unsupervised machine learning that integrates third-party data, signals, and heterogeneous data sources to minimize financial risk and deliver superior fraud detection. It works to proactively target new and emerging fraud patterns often missed by legacy rules engines and even supervised machine learning tools.

The Global Intelligence Network (GIN) comprises anonymized non-PII data from over 4.2 billion protected accounts and 800 billion events across the globe. The GIN contains rich information on digital data such as IP address subnets, prefixes, proxies and data centers, user agent strings, device types and OS, email address domains, and more. Information from the GIN feeds into machine learning algorithms to further improve overall detection.

Together, these four tools give companies an encompassing solution to combat bot attacks.

How is DataVisor Different From Other Fraud and Risk Solutions?

We are more proactive. Our goal is to detect and mitigate the source of the attack before it costs a company millions of dollars. Traditional cybersecurity tools apply the blacklist approach in a reactive strategy that simply can't keep up anymore.

DataVisor solutions can be applied to a broader range of omni channels than our competitors, who are mostly still focused on the web. In particular, DataVisor has advanced technologies to detect different types of sophisticated mobile attacks. In addition, DataVisor solutions can be applied to call center data, chat data, and more, to give a 360-degree production of user activities.

The other important differentiator of the DataVisor solution is that UML detection results are extremely accurate as it detects a fraudulent ring rather than individual bad behavior. As a result, we don't have the false positives that can disrupt the customer experience that plague many other solutions. Companies need security software that is highly accurate to avoid false positives when trying to detect tricky mobile emulators, which are scripted attacks often used in credential stuffing.

Finally, I would say that we bring a level of fine-grained customization to the digital security solution not seen in traditional approaches. There is no one-size-fits-all for digital security anymore. We can segment the solution to the traffic channel. DataVisor gives companies tools they can mold to fit their particular areas of concern and business strategies, whether those areas are ticketing and e-commerce, insurance, or banking fraud.

Fighting Back: Using AI for Good

DataVisor has been a leader in the AI technology space for years. Our solution makes use of unsupervised machine learning algorithms to help companies work smarter by spotting internal and external fraud to mitigate their risk.

One example of our work includes using our solution to stop bot-scripted ticketing fraud for a major Asian airline company. The company was struggling with:

- Fraudsters leveraging scripted bot attacks to purchase tickets in bulk. Then they would resell or cancel the tickets, falsely claim seats, and manipulate ticket prices—causing revenue loss and negative customer experiences.
- Fraudsters compromising user accounts to redeem loyalty points then using saved credit card information to purchase airline tickets.

dVector, our advanced machine learning solution, helped the company deflect bot attacks before they caused problems. dVector analyzed orders by looking closely at customer digital fingerprints, profiles, and behaviors to spot stealthy fraud patterns in real-time.

With **DataVisor's dEdge**, our fraud prevention software development kit (SDK) for mobile and web, enabled the company to collect real-time data from web browsers and mobile apps to uncover malicious activities targeting web pages and mobile devices.

The end result? DataVisor's innovative fraud detection solution captured **53%** in additional fraud attempts with a detection accuracy of **97%**.

Click here to read more about DataVisor's AI-powered fraud and risk solutions.

About DataVisor

DataVisor is the leading fraud detection platform powered by transformational AI technology. Using proprietary unsupervised machine learning algorithms, DataVisor restores trust in digital commerce by enabling organizations to proactively detect and act on fast-evolving fraud patterns and prevent future attacks before they happen. Combining advanced analytics and an intelligence network of more than 4B global user accounts, DataVisor protects against financial and reputational damage across a variety of industries, including financial services, marketplaces, ecommerce, and social platforms. DataVisor was recently recognized by Gartner as a Cool Vendor in the Identity and Access Management and Fraud Detection report and is a recipient of multiple industry awards.

For more information on DataVisor:

info@datavisor.com

www.datavisor.com

967 N. Shoreline Blvd. | Mountain View | CA 94043

DATAVISOR