ESG Enterprise Strategy Group | Getting to the bigger truth.™

ESG SHOWCASE

Securing Applications from Sophisticated Bot Attacks with White Ops

Date: February 2020 **Author:** John Grady, Analyst; Jon Oltsik, Senior Principal Analyst and ESG Fellow

ABSTRACT: Fraudulent activity caused by non-human, bot-based web traffic is impacting an increasing number of organizations. However, the sophisticated nature of these bots has made detection more difficult. Existing application security solutions have trouble detecting sophisticated bot activity specifically because it is designed to mimic human actions and compromise user accounts through legitimate application functions. Dedicated, multilayered bot detection and mitigation solutions have become a prerequisite to ensure web transactions are originating from a human, and not a sophisticated bot. White Ops has spent nearly ten years protecting advertising and marketing programs from fraud caused by sophisticated bots. Its new Application Integrity offering expands that protection to online enterprises to protect their websites and applications from fraud and abuse.

Sophisticated Bots Represent an Increasingly Disruptive, But Often Overlooked Threat Vector

Most businesses today rely on of e-commerce capabilities, customer-facing web applications, or open APIs that are susceptible to abuse by sophisticated bots. Bot-based attacks are extremely difficult to detect because they seek to mimic human behavior and execute legitimate transactions that become malicious only by their scale or outcome. Some of the most common fraudulent and abusive bot-based attacks include:

- Account takeover (ATO) – Existing user accounts are compromised and exploited by cyber-criminals, typically through credential stuffing or credential cracking, activities which can run at a high scale through sophisticated bots.
- Automated account creation – Fraudulent accounts created by sophisticated bots can be used for social media disinformation, phony product reviews, and other reputation-based attacks, or more direct financial attacks such as inventory holding and spoofing, fraud, and money laundering.
- Web scraping – While not all web-crawling comes from bots controlled by hackers, malicious scraping may target the database layer to steal pricing, intellectual property, and customer information.

The initial account takeover or creation is only the first stage of the attack and is typically followed by fraudulent purchases, fund extraction, or other financially impactful actions. Alternatively, hackers can sell the validated compromised account information for a premium on the black market. In fact, account access-as-a-service is now commonly seen on the dark web with criminals offering managed access to legitimate services, providing buyers with the benefits of the compromised accounts without the risk or effort involved in the actual takeover.

The Availability of Stolen Credentials, Improvements in Automation, and Insecure Devices Have Created a Perfect Storm for Sophisticated Bot Fraud

Bots are not a new threat vector, so why has this become such a problem? To begin with, the universe of potential targets is massive and continues to expand. While e-commerce or financial entities are typically top of mind when thinking about the impact of bot activity, any organization with a web presence (such as healthcare, insurance, education, retail and government) is a potential mark for a bot operator. Additionally, bot technology and the surrounding ecosystem has improved the success rate and economics of attacks:

- Sophisticated bots can pass for legitimate humans – This was not always the case: the first and second generation of bots were fairly easy to detect due to their inability to store cookies or execute JavaScript, and the presence of easily detectable characteristics signifying the presence of automation. However, the third and fourth generation bots in use today are exceptionally hard to identify through browser and device analysis alone. They look and act like humans and originate from legitimate browsers. Additionally, the utilization of artificial intelligence (AI) by threat actors is on the near-term horizon and will further complicate detection.

- Insecure consumer devices contribute to bot sophistication and scale – Part of the reason bots are able to so closely mimic human activity and originate from seemingly innocuous residential IP addresses is because they exploit compromised consumer devices. Criminals have access to an untold number of malware-infected devices across the globe. These can be used by bots to track, study, and incorporate real-world human activity, such as non-linear mouse movements. Also, by routing bot traffic through the residential IP addresses of these devices or compromised IoT devices, IP reputation-based detection methods lose their effectiveness. It also provides cheap and easy access to bandwidth to massively scale attacks.

- Stolen credentials are numerous and cheap – Tens of billions of credentials from successful attacks are available on the dark web, with as many 7.9 billion records exposed in the first nine months of 2019 alone.[1] While multi-factor authentication (MFA) can improve account security, it is not a failsafe and is far from ubiquitous. ESG research has found that 34% of organizations do not use any form of MFA technology.[2] Attackers can cheaply purchase large quantities of these credentials and, with their sophisticated bots, launch stuffing or cracking attacks leading to ATOs, knowing there is a good chance MFA is not in use to secure authentication.

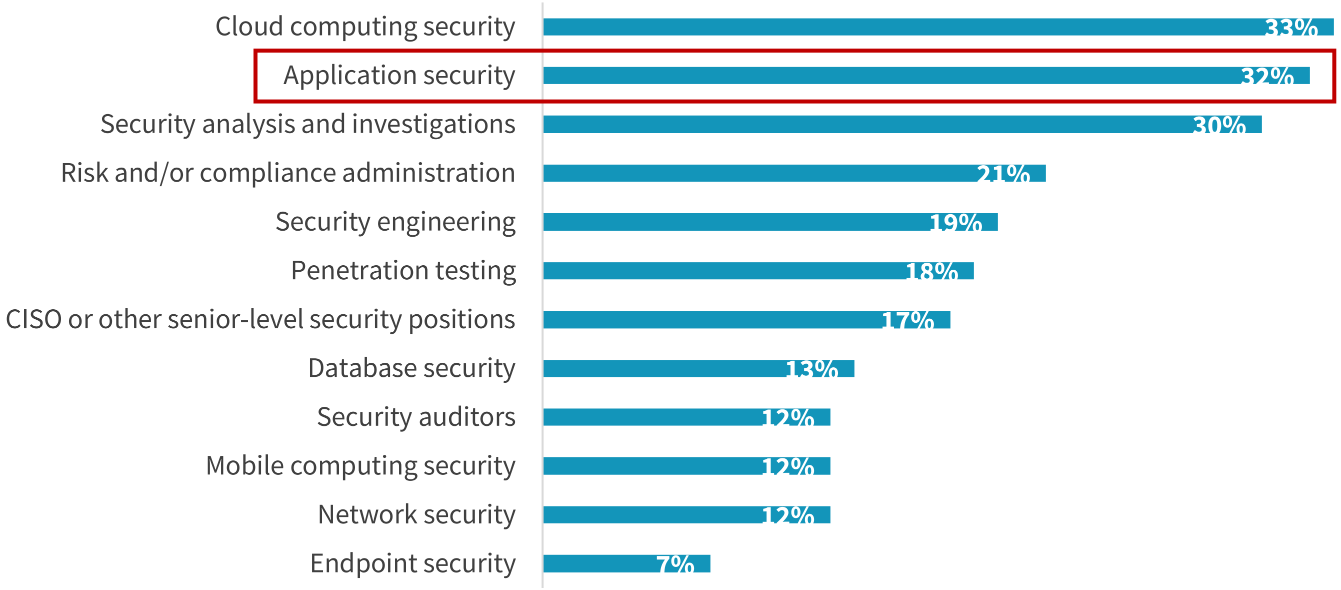
Where Legacy Solutions Fall Short in Sophisticated Bot Mitigation

While awareness of the threat posed by sophisticated bots is growing, existing security tools do not adequately address the issue. Historically, simple bots were focused on web scraping or in some cases would launch a high volume of fraudulent login attempts or account-based attacks. These attacks were basic and straightforward to detect and mitigate via traditional application security tools or manual intervention because of the noticeable volume or source IP addresses used. However, as bots have grown more sophisticated, these defenses have become less effective. ESG research has found that security teams are understaffed and under-skilled as it is, especially regarding application security (see Figure 1).[3] Building and maintaining an effective in-house bot detection team is not a realistic option for most organizations and does not scale to address today's bot-based attacks.

[1] Source: Risk Based Security, *Q3 2019 Data Breach QuickView Report*, November 2019.
[2] Source: ESG Master Survey Results, *Identity and Access Management*, January 2018.
[3] Source: ESG Research Report, *The Life and Times of Cybersecurity Professionals 2019*, May 2019.

Figure 1. Areas With the Biggest Shortage of Cybersecurity Skills

In which of the following areas would you say that your organization has the biggest shortage of cybersecurity skills? (Percent of respondents, N=267, three responses accepted)



Source: Enterprise Strategy Group

Application security has historically included both testing and runtime protection solutions. Testing includes both static and dynamic application security testing (SAST and DAST), while runtime protection includes web application firewalls (WAFs) and runtime application self-protection (RASP). Testing solutions scan the code or production application itself to discover potentially exploitable vulnerabilities, misconfigurations, or authentication issues. Because bots exploit legitimate application operations as opposed to vulnerabilities or misconfigurations, these solutions do not address bot-based threats.

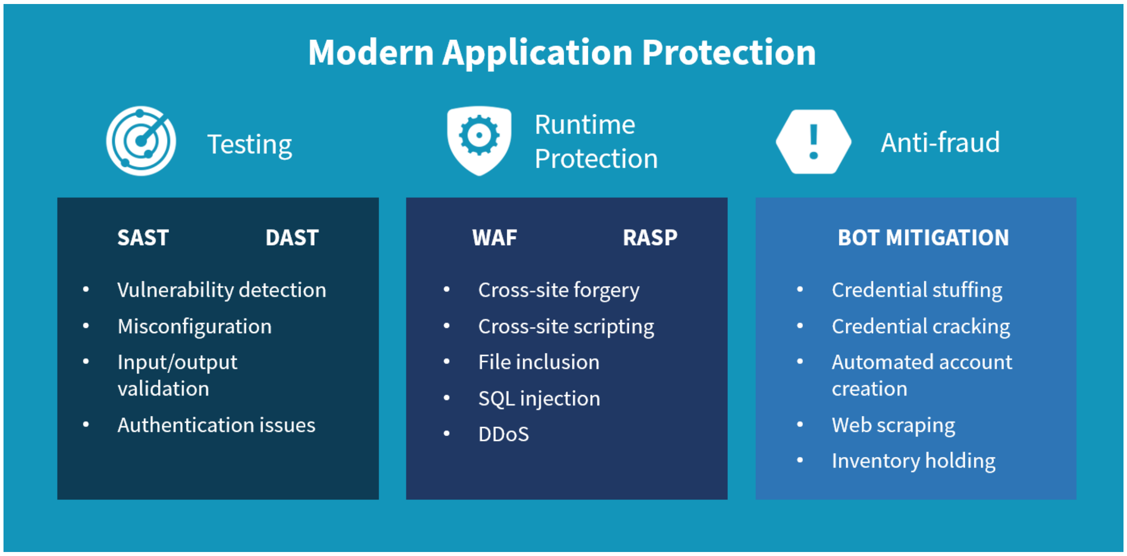
WAF and RASP solutions are more applicable to the simple bot threat, and some vendors have attempted to add functionality to address more sophisticated bots. However, these solutions are ultimately built and deployed to solve a problem other than bots and lack the significant resources needed to remain ahead of attackers and recognize and stop sophisticated bot attacks. Some of the drawbacks of WAFs related to mitigating sophisticated bot attacks include:

- Limited rulesets – WAFs are often deployed simply to maintain PCI compliance, which may mean they are run with a limited ruleset to prevent false positives from impacting user availability, thus decreasing bot detection capabilities.
- Vulnerability focus – WAFs are typically focused on protecting against known software vulnerabilities (such as SQL injections and cross-site scripting). Bot-based attacks do not exploit these vulnerabilities, rendering this focus ineffective in bot mitigation.
- Signature dependency – WAFs have historically relied on signatures for detection. This is changing with third generation solutions but remains a component of many WAFs, and is an insufficient method for detecting sophisticated bot attacks.
- IP reputation-centric – WAFs also rely on IP reputation to identify traffic from known-bad actors. Many sophisticated bots cycle through residential IP addresses, limiting the effectiveness of a reputational defense.

Protecting Applications from Sophisticated Bots Requires Multilayered Solutions

Protecting applications against fraudulent activity is as important as maintaining the integrity of the application itself and a vastly different function. Rather than focusing on code, solutions must weigh intent as it relates to identity and potentially abusive activities. Brand perception and customer trust are at stake. To this end, a third subcategory of application protection solutions focused on anti-fraud extends beyond vulnerability and code-based exploit mitigation, and protects against the malicious use of legitimate application functions (see Figure 2). Sophisticated bot detection is a key component of this subcategory.

Figure 2. Application Protection Subcategories



Modern Application Protection

Testing	Runtime Protection	Anti-fraud
SAST DAST	WAF RASP	BOT MITIGATION
• Vulnerability detection • Misconfiguration • Input/output validation • Authentication issues	• Cross-site forgery • Cross-site scripting • File inclusion • SQL injection • DDoS	• Credential stuffing • Credential cracking • Automated account creation • Web scraping • Inventory holding

Source: Enterprise Strategy Group

Because sophisticated bots are specifically trying to mimic the behavior of normal users, multiple layers of detection are required to ensure efficacy while maintaining a low level of false positives. Rather than focusing solely on the action the entity is taking within the application, detection techniques must consider the surrounding context to accurately detect malicious activity. To this end, the following detection mechanisms, used in conjunction with one another, represent a layered approach to detecting sophisticated bots by determining the intent of the entity behind the request.

- Indicators of compromise – As discussed, today's sophisticated bots emulate browser activity or automate within legitimate browsers originating from benign residential IP addresses, making detection difficult. JavaScript challenges and browser fingerprinting can still identify bots on their own. However, collecting and analyzing a broad set of information about the user device sending the request, the network it is originating from, and the software and applications running on the device helps detect more sophisticated bots with greater accuracy.

- Analytics and continuous iteration – Bots continuously adjust and adapt to detection techniques, making it necessary to cycle and update tests and markers to stay ahead of attackers. Further, incorporating machine learning and analytics to correlate potentially disparate pieces of information can assist in detection even when individual indicators of compromise are not present.

- Threat intelligence – Driving continuous iteration requires a global mechanism to collect up-to-date bot-driven fraud techniques and contextual reputation data. As discussed, IP reputation alone does not work. However, considering patterns, determining the presence of proxies, and correlating across a broad ecosystem of customers and transactions can provide additional context into decision making.

Enter White Ops

White Ops is an established vendor in bot detection and mitigation, historically focused on combating advertising and marketing fraud. The company was founded in 2012 and currently boasts 20 globally distributed data centers. White Ops protects both global enterprises and the largest internet platforms, verifying the humanity of more than 1 trillion interactions per week across its Integrity product lines. Advertising Integrity detects and blocks fraudulent traffic for desktop, mobile application, mobile web, and connected TV platforms. Marketing Integrity helps ensure the validity of marketing metrics by preventing bots from fraudulently visiting websites, filling out forms, and ultimately generating illegitimate leads.

Introducing Application Integrity

Built on the same platform and decision engine as Advertising and Marketing Integrity, Application Integrity leverages White Ops' detection capabilities to protect websites and applications from account fraud and scraping by sophisticated bots. Application Integrity utilizes a multi-layered decision engine incorporating more than 250 algorithms to detect signs of automation, remote control, and manipulated human activity. First, signal collection provides a granular understanding of individual transactions through JavaScript payload or software development kits (SDKs) for mobile applications. Customers can also send signals to the White Ops solution such as session IDs, hashed user IDs, referrers, and timestamps, for complete feedback loops into user account activity.

Next, marker analysis runs the requesting device through hundreds of tests to detect automation. The decisioning engine is designed so that the failure of even one test causes the device to be considered a bot with a high degree of confidence, avoiding false positives. Finally, new tests are continually developed, and existing tests are adjusted, making it even harder for fraudsters to evade detection.The decision engine is supported by machine learning and global threat intelligence capabilities to detect bots even with limited technical evidence. Machine learning capabilities are driven by the more than one trillion weekly transactions White Ops has visibility into. White Ops threat intelligence capabilities enable it to uncover emerging bot-based threats and attribute them to specific botnet operators, campaigns, and threat actors.

The Bigger Truth

In the hierarchy of threats, bot activity has flown under the radar when compared with attacks such as advanced malware, distributed denial of service, and more recently ransomware. This is starting to change as sophisticated bots increasingly focus on account takeover attacks and businesses feel more direct financial impacts. Because of the availability of stolen credentials, compromised machines, and sophisticated bot technology, we appear to be at an inflection point. Security and risk leaders are starting to understand their existing application security tools were not built to detect sophisticated bot activity. To round out application security capabilities, security leaders should consider not just testing and runtime protection, but anti-fraud solutions as well. With a history of protecting organizations from bot-based fraud, White Ops is uniquely positioned to expand its capabilities into the application security space.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188