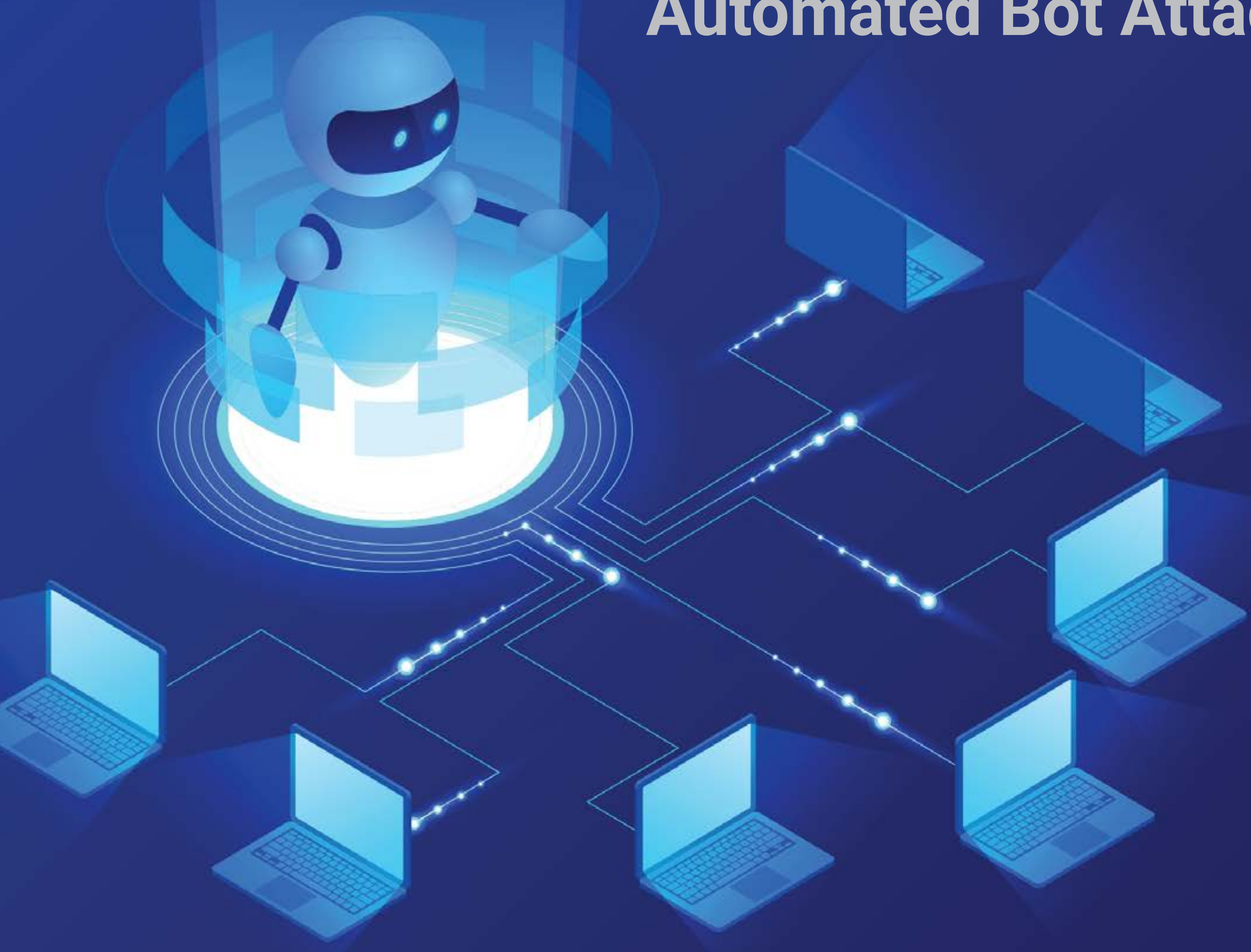
THE IMITATION GAME

Detecting and Thwarting Automated Bot Attacks



ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) RESEARCH REPORT SUMMARY
BY PAULA MUSICH
JANUARY 2020

SPONSORED BY:

CEQUENCE™ SECURITY

EMA™ IT AND DATA MANAGEMENT
RESEARCH | INDUSTRY ANALYSIS | CONSULTING

Table of Contents

Executive Summary

IT executives, contributors, and IT security teams in a range of industries understand that their growing arrays of public-facing applications, whether those are web, mobile, or API-based, are the targets of automated bot attack campaigns. Inexpensive and easy-to-launch automated malicious bot attacks exploit vulnerabilities in the business logic of these applications to hijack user accounts, create fake accounts, scrape content, carry out application distributed denial of service attacks, and carry out other types of attacks.

In this research, 52% of respondents indicated that their organization's public-facing applications had experienced DDoS attacks in the last year, followed by 38% of respondents reporting fake account creation and vulnerability scanning/reconnaissance attacks over that same time period. Depending on the type and size of the organization, the frequency of these attacks ranged anywhere from less than one per day to over 500 times per day. The largest percentage of respondents indicated the frequency of attacks was either one to five, six to 10, or 11 to 25 times per day.

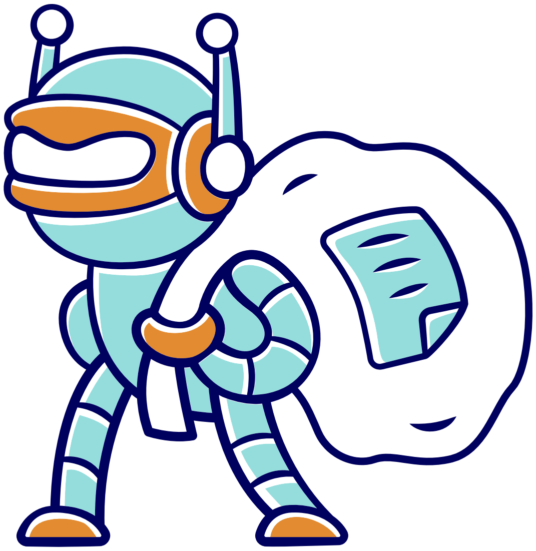
In this barrage of attacks, a significant percentage of defenders making use of different bot detection and mitigation solutions are seeing success in quickly detecting and mitigating the most prevalent types of attacks in less than one day. At the same time, at least one third of respondents indicated that their organizations saw no change in the frequency of attacks over the last year, suggesting that their defenses are holding back the tide of attacks—at least, for the time being. However, this success has in all likelihood contributed to the rapid growth in the use of advanced persistent bots (APBs), which use more sophisticated techniques to get around first-generation defenses and often regroup after being initially stopped, then are reconfigured and relaunched to attempt to overcome those initially successful detections.

The top three bot defenses in use by respondents include web application firewalls (55%), dedicated bot mitigation (51%), and CAPTCHA (48%). The top use cases driving the acquisition of those solutions were protection against application DDoS attacks followed by account takeover protection. Their ability to accurately classify real humans, good bots, and bad bots, as well as their effectiveness at identifying new and previously unseen attack techniques, were rated for the most part as adequate, but respondents indicated there is room for improvement.

Still, organizations are realizing a number of benefits in using these different bot defenses. Reducing fraud resolution costs was the top benefit indicated by 23% of respondents. Another 19% ranked reduced web infrastructure costs through a reduction in malicious traffic as their top benefit. Fifteen percent ranked improved end-user experience as their top benefit.

However, bot detection and mitigation solutions come with their own baggage, including a lack of integration with existing security infrastructure reported by 30% of respondents, too many false positives reported by 28% of respondents, and cumbersome configuration and management reported by 24% of respondents.

Introduction



The growth in the use of both good bots and bad bots aimed at probing commercial websites is well documented by security researchers. Overall, both types make up about 38% of all Internet traffic. Over 20% of all website requests are made by bad bots conducting a range of nefarious activities, including the more ubiquitous application distributed denial of service (DDoS) attacks as well as price scraping, web fraud, account hijacking, and more. These and other types of automated bot attacks don't just target ecommerce websites; they also target websites representing education, government, and perhaps the biggest target: financial services.

As the battle escalates between attackers and website defenders, attackers continue to up their game by increasing the level of sophistication in their campaigns. The use of simple Python or Perl scripts to mimic the behavior of valid website visitors has given way to the use of Javascript and cookies to appear legitimate. More sophisticated bots even have their own moniker: advanced persistent bots (APBs). These APBs, which make up the lion's share of all bad bots, can mimic human behavior, seek to bypass CAPTCHAs, hide behind anonymous peer-to-peer proxies, and dynamically rotate IP addresses. At the same time, they follow the old saw that says *if at first you don't succeed, try, try again*. Increasingly, attackers try to determine how their bots are initially detected and then reconfigure and relaunch the attack in an effort to evade those detections.

Defenders are responding by turning to a range of different bot detection and mitigation providers, including dedicated bot mitigation vendors, web application firewall providers, content delivery networking services, and others. Such providers are raising the stakes by adding a wider range of telemetry to their solutions and adding new detections that employ machine learning techniques, behavioral analysis, and more on top of existing signatures, challenges, and IP reputation detections. However, determining the difference between good bots, bad bots, and human activity is one of the harder problems to solve in application security. Just as enterprises are using more agile development techniques to speed the delivery of new application functionality, so too are attackers using the same techniques to evolve their approaches in order to avoid detection.

The Attack Surface and Who Manages It

The sprawling attack surface is rapidly expanding as organizations carry out their digital transformation initiatives, building out the number of customer-facing web, mobile, and API-based applications designed to improve customer experience and interaction, streamline online transactions, and better tailor messaging to individual interests. The research established a baseline definition of automated malicious bots to ensure respondents were answering questions from a common understanding. The definition is:

> **Automated malicious bots** target the business logic of public-facing web, mobile, and API-based applications and their associated endpoints. Examples of application functions that these bots seek to exploit include, but are not limited to: user login, account signup, password/username reset, browse, compare, discounting, or other checkout functions.

Like most malware attacks, those executing bot attacks against public-facing websites seek to hide their tracks to avoid detection and succeed at whatever their aim is—whether that is taking over legitimate accounts or creating fake ones; content scraping, loading shopping carts but not purchasing to prevent others from buying, purposely driving traffic to a public-facing application to increase resource consumption and costs, automated shopping to buy high-demand items that limit quantity per buyer, gift card or loyalty program fraud, reputation bombing, or vulnerability scanning. Only application DDoS attacks are somewhat easier to detect. To get a baseline understanding of awareness of the problem, the research asked respondents whether they believed their organization's public-facing applications were susceptible to or the target of automated bot attacks. An overwhelming majority indicated that they are under no illusion that their web, mobile, and API-based applications are a target and susceptible except under specific circumstances. A majority of those who believe their applications are not a target indicated that their applications are too complex to be a target (they provide no singular touchpoint for attack) or their applications require a specialized application client to connect.

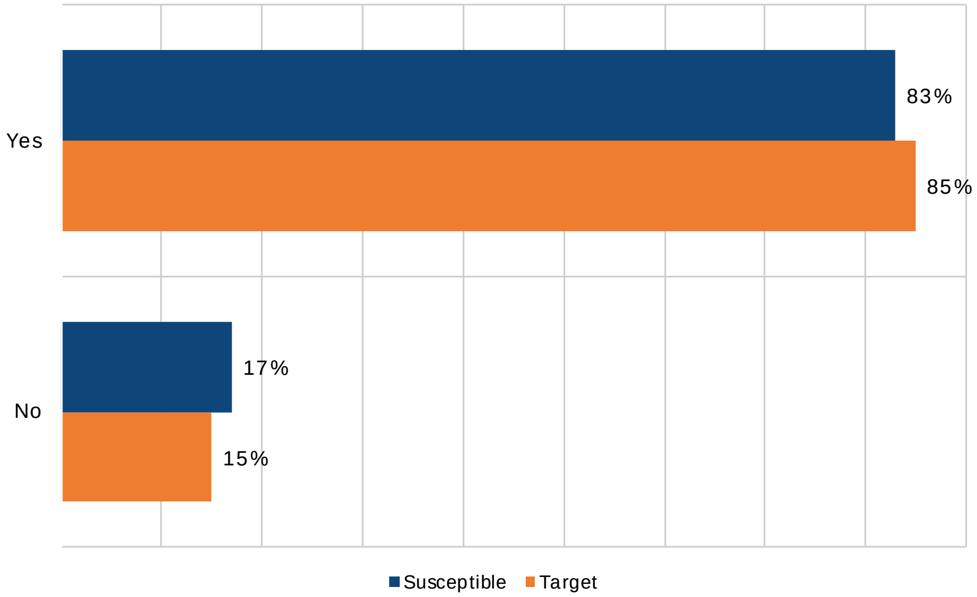


Figure 1: Do you believe your organization's public-facing web, mobile, and API-based applications are susceptible to/are a target for automated bot attacks?

For those who do believe their public-facing applications are susceptible to or the target of automated bot attacks, the majority—a clear 60% of respondents—indicated that their organization's web-based applications are the primary target. Still, 17% indicated their API-based applications are the most frequently targeted applications by automated bot attacks, and that percentage will surely increase as more and more organizations increase their use of modular applications that use APIs to make it faster and easier for developers to build the business logic that underlies those applications. Using and developing APIs facilitates the interoperation of internal systems, tools, and development teams, helps to reduce development time, and allows the functionality of the application to be easily extended. At the same time, using APIs improves the performance and user experience for end users of the application. Attackers can exploit those APIs to enjoy the same benefits and, in fact, they are. The use of APIs is on the rise as a result of those benefits, and so is the exploitation of those by automated bot creators. The frequency of mobile application attacks will continue to rise as well, as mobile devices continue to replace laptops and desktops as the computing and communications device of choice and as enterprises continue to expand the number of mobile applications they enable for their customers and prospects. Hackers are following this trend and increasingly targeting mobile applications. For example, CheckPoint Software Technologies malware researchers found in the first half of 2019 that cyberattacks targeting smartphones and other mobile devices increased 50% compared to one year earlier. Security practitioners working in the banking/finance/insurance category will need to be especially diligent because that rise is attributed in part to the dramatic increase in the use of mobile banking applications.

It's also interesting to note that 33% of those respondents representing midmarket companies indicated they don't believe their company's web-facing applications are susceptible to automated bot attacks. Thirty percent said their public-facing applications are not a target of such attacks. Bad bots are simple to rent, customize, and deploy. They are also cheap to use and offer good return on a cyber criminal's investment. All this is making automated bot attacks fairly ubiquitous. This suggests some level of naiveté among respondents in those smaller organizations.

Attack Surface Size

Understanding the extent of the problem requires a feel for how big the attack surface actually is. The research queried respondents about the number of public-facing applications their organizations deployed, both within their own data centers and in the cloud, as well as the number of web, mobile, and API-based applications that were deployed in both types of locations. Web applications deployed on-premises represent the largest percentage of any category. It should be no surprise that both mobile applications and API-based applications are more evenly split between deployment on-premises and in the cloud, especially compared to web applications. Both are born out of more agile application development techniques that emphasize the speed and functionality that cloud platforms offer. However, securing cloud-based applications is a more difficult task, especially given the lack of experience many IT or cybersecurity teams have in securing cloud applications. The chart indicates those numbers.

	On-Premises	In the Cloud
Web	87.36	48.18
Mobile	33.86	30.54
API-Based	31.71	27.51

Figure 2: Average number of public-facing web, mobile, and API-based applications deployed on-premises and in the cloud.

Who Secures Public-Facing Applications?

IT or cybersecurity teams are the obvious groups responsible for securing their organization's public-facing web, mobile, and API-based applications, with 67% of respondents indicating those teams as leading the effort. That response was followed by IT operations at 17% of respondents, and another 7% indicated that responsibility was shared between two groups. In that instance, IT or cybersecurity was always involved, and they shared responsibility with primarily either application development/DevOps or IT operations.

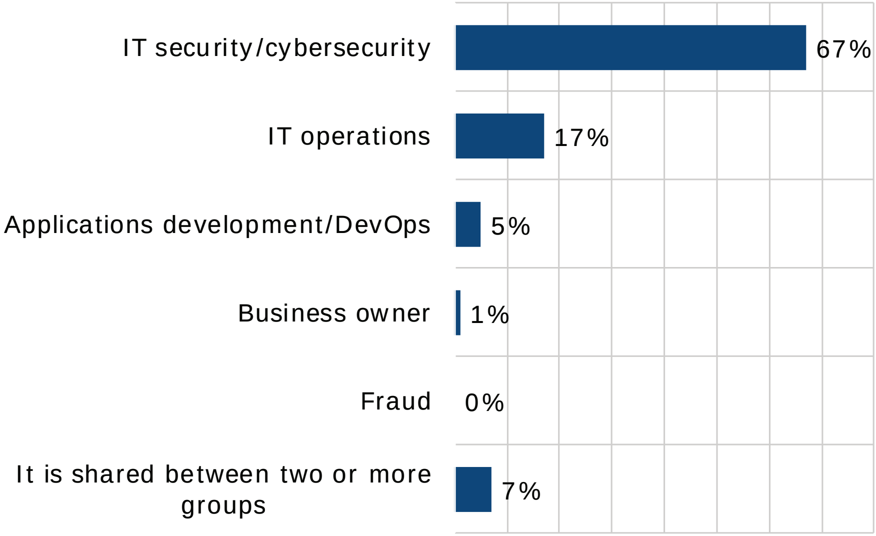


Figure 3: Which group within your organization is responsible for securing your organization's public-facing web, mobile, and API-based applications?

The Attack Landscape

Bad actors, including cybercriminals, unscrupulous competitors, ticket scalpers, other Grinch or sneaker bots, and some shady investment companies employ a range of different automated bot attack techniques against public-facing websites. The application distributed denial of service (DDoS) attack is one of the most common and was the most prevalent as experienced by respondents over the last 12 months, with 52% indicating their websites were targeted. Although these types of attacks are sometimes the easiest to detect, in some cases they can be used as a smokescreen to hide attempts to steal valuable data. In that case they are typically low-volume attacks that are shorter in duration, used to test for vulnerabilities, and utilized to distract security teams from their ultimate aim.

Other prevalent types of attacks include fake account creation and vulnerability scanning/reconnaissance, with 38% of respondents indicating their organizations had experienced each of those within the last 12 months. Another 26% of respondents reported experiencing account takeover/credential stuffing, where malicious bots try to wrest control of user accounts by testing user/password combinations stolen from other websites and published on the dark web.

Attacks aimed primarily at ecommerce companies can include automated shopping to buy high-demand items that limit quantity per buyer and then selling the items at a higher price on secondary markets, as well as denial of inventory in which bots load shopping carts but don’t purchase the items to prevent others from buying. Unscrupulous competitors will use these and other attacks, such as content scraping, reputation bombing, and denial of wallet attacks that purposely drive traffic to a public-facing application to increase resource consumption and costs. Finally, gift card/loyalty program fraud is used to steal the value of loyalty program accounts and is often done using brute-force attacks, in which automated bots use multiple combinations to find valid pairs of card numbers and pin codes.

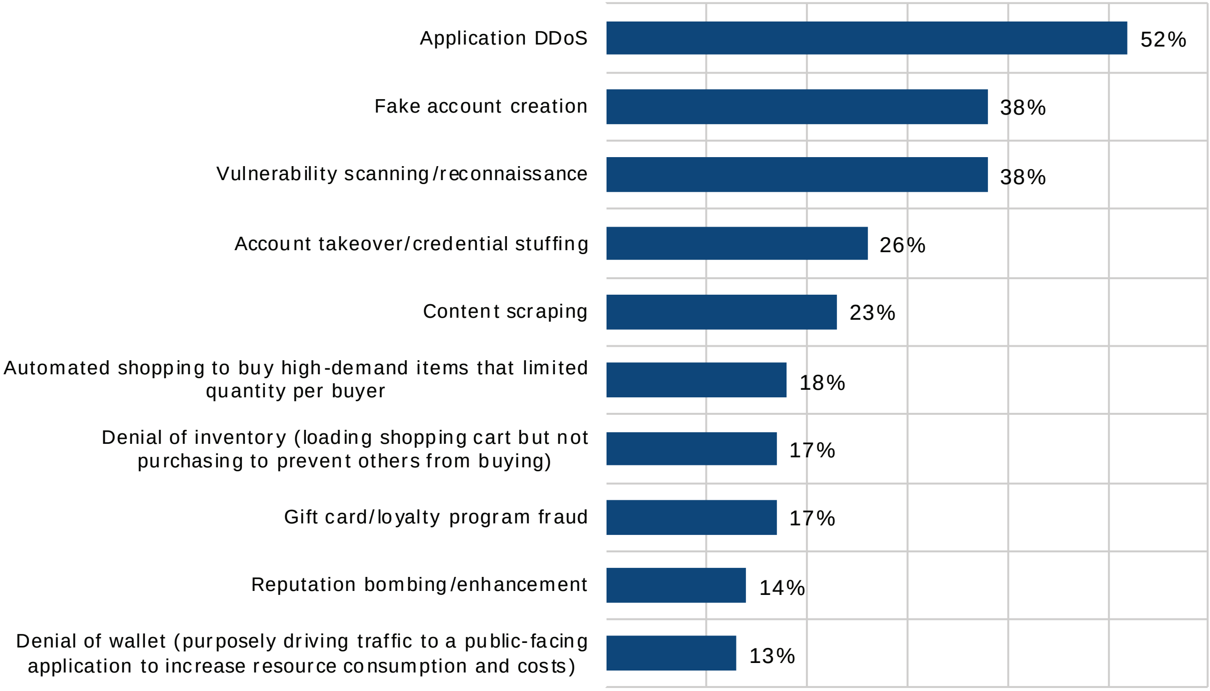


Figure 4: Over the past 12 months, which of the following types of malicious bot attacks have your organization’s public-facing web, mobile, and API-based applications experienced?

Time to Detect Attacks

One of the key metrics used to judge the effectiveness of bot defense solutions, as well as the teams managing them, is how quickly attacks aimed at public-facing web applications can be detected. As attackers increase the sophistication of their evasions in attempting to bypass security controls, this task becomes all the more difficult. EMA's survey asked respondents to estimate how long it took (on average) to initially detect each type of malicious bot attack their organization's public-facing web, mobile, and API-based applications experienced over the last 12 months. Possible answers ranged from less than one day to more than three months. Although the mean number of days for all respondents experiencing each type of attack is a rather coarse measurement, it does provide an overall picture of the state of malicious bot attack detection. It also highlights the relative difference in the time it takes to detect each type of attack. Not surprisingly, the attack type that is fastest to detect is denial of wallet, in which attackers purposely drive traffic to a public-facing application to increase resource consumption and costs at a mean time to detect of 4.81 days, followed by the application DDoS attack type at 4.96 days. On the other end of the spectrum, the attack type that takes the longest to detect is automated shopping to buy high-demand items that limit quantity per buyer at a mean time of 9.32 days, followed by account takeover at a mean time to detect at 8.68 days.

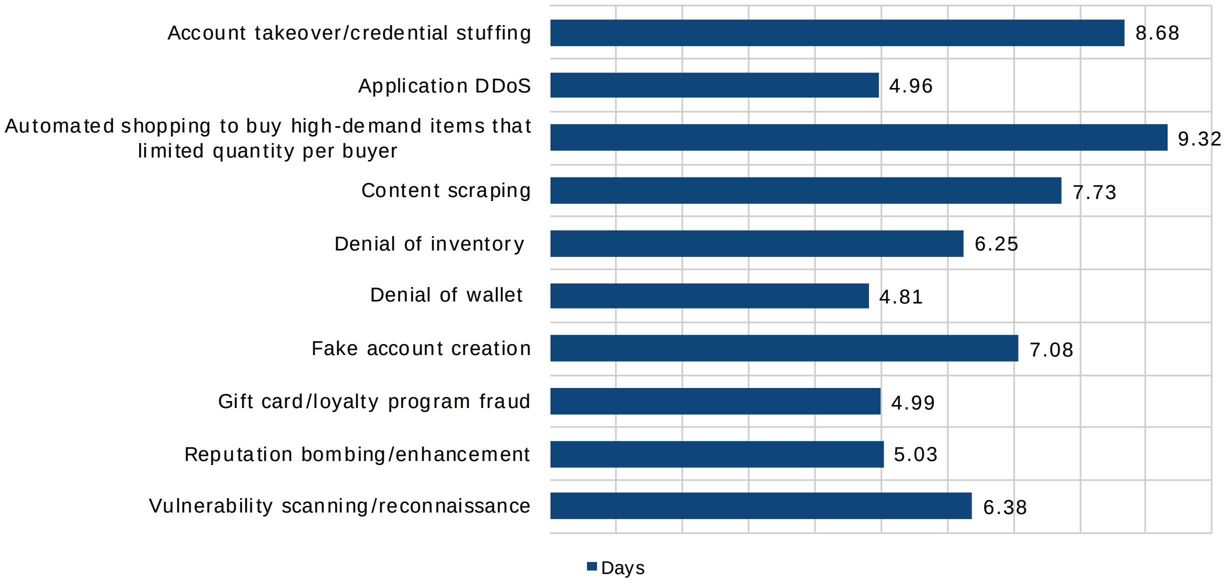


Figure 5: Mean time to detect each type of attack experienced.

Time to Mitigate Attacks

The other key measure of bot defense effectiveness is how quickly attacks can be mitigated once they are detected. Given how quickly losses can mount, whether from lost customers, theft, increases in operational costs, and so on, those responsible for securing public-facing applications need to move quickly to mitigate such attacks. Fortunately, the mean time to mitigate malicious bot attacks is faster than the time it takes to detect the attacks. Relative to other attack types experienced by respondent organizations, the fastest attack to mitigate is reputation bombing, with a mean time to detect of 2.75 days, followed by account takeover at 3.18 days. However, attacks harder to mitigate, such as content scraping, can take an average of 7.56 days to resolve.

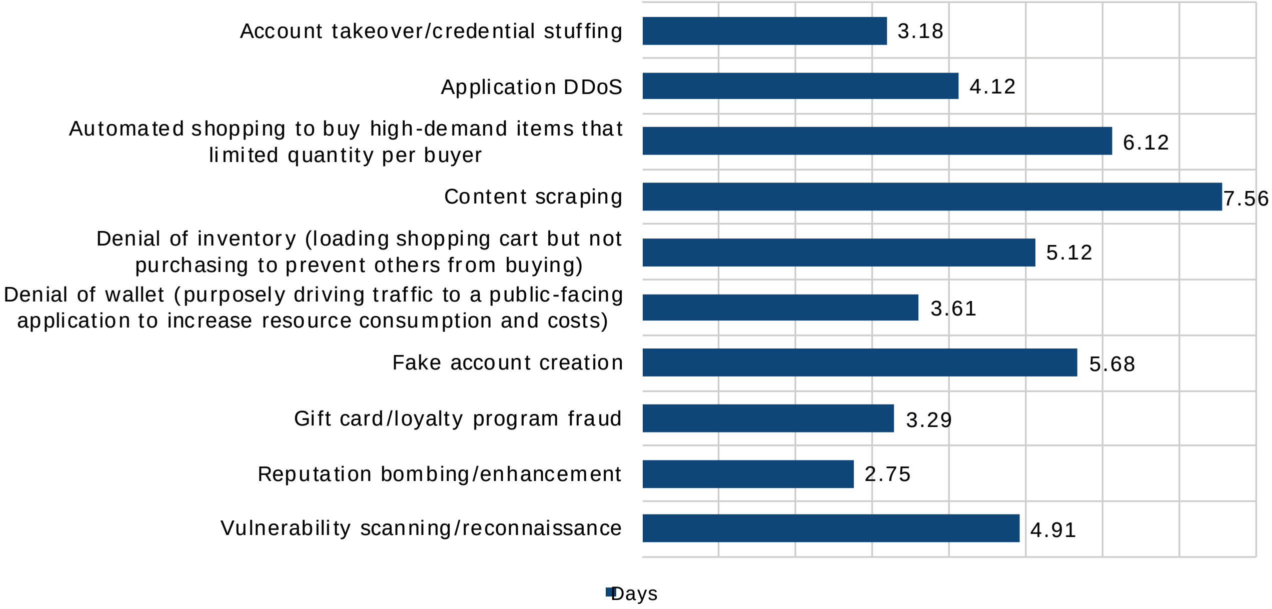


Figure 6: Mean time to mitigate attack types experienced.

For the top five attacks experienced by the largest percentage of respondents, mitigation appears to be a fairly quick win for most. For the top application DDoS attacks experienced by the largest number of respondents, it took 35% of those organizations less than one day to mitigate. For those experiencing fake account creation, once detected, 22% of those organizations were able to mitigate the attack in less than one day—making up for lost time in the lag time to detect. It also appears that some security teams are faster to mitigate vulnerability scanning/reconnaissance attacks that others, with 23% taking less than one day to mitigate those attacks, while another 24% took 2-3 days to mitigate.

How Organizations Combat Automated Bot Attacks

Given the long history, success, and increasing sophistication of automated bot attacks, it's no surprise that a clear majority of respondent organizations were using a bot detection and prevention solution at 68%. This is true across a range of different vertical industries, not just ecommerce companies. Only 11% of respondents indicated their organizations were using a detection-only solution. The more interesting question is, what are organizations using to defend their public-facing web, mobile, and API-based applications? The once pervasive and dominant CAPTCHA, while still in use in a significant number of organizations, has seen more sophisticated competitors seek to unseat it as the primary form of protection. Other defense types include dedicated bot mitigation, content delivery network-based protections, and new modules or functionality added to web application firewalls, as well as next-generation firewalls. Organizations may also apply their log analysis or SIEM solutions to the task of detecting bot attacks against their public-facing applications. The top three bot defenses in use by respondent organizations were WAFs by 55%, dedicated bot mitigation by 51%, and CAPTCHA by 48%. By vertical industry, 90% of high-technology software companies were using dedicated bot detection and prevention, as were 69% of banking/finance respondents and 65% of manufacturing companies. These three vertical industries represent the largest percentage of the survey sample. Given the success rate of bot attacks, it's no surprise that defenders are applying the concept of defense-in-depth by using multiple bot attack protection solutions. In some cases, organizations may use CAPTCHAs not as a frontline detection capability, but as a way to reduce false positives generated by other solutions in use.

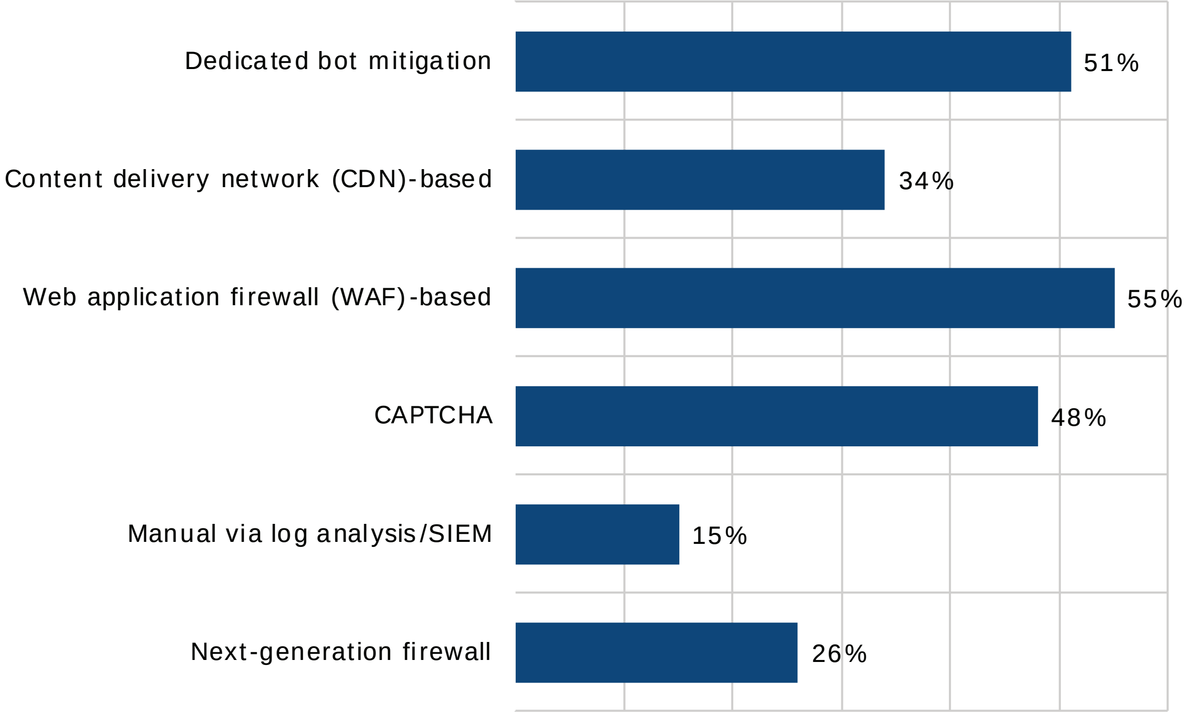


Figure 7: You indicated your organization is using a bot defense solution. Which of the following types of bot defense is your organization using?

Bot Defense Barriers

When organizations embark on bot defense implementation projects, success is not guaranteed. Solutions may be tailored to specific use cases, they may be architected in a way that can negatively impact performance, they may require significant changes to existing applications, they may fail to detect more advanced bot attacks, they may generate too many false positives, they may not integrate well with the organization's existing security systems, and so on. When asked whether respondent organizations experienced any barriers to success in deploying and managing their bot defense technology of choice, the largest percentage of respondents (30%) indicated that their bot defense solution did not integrate with their existing security infrastructure. That was followed closely by too many false positives reported by 28% of respondents, and 24% indicated that their solution was cumbersome to configure and manage. However, the top issues chosen by respondents representing different sizes of organizations varied quite a bit. For example, 44% of respondents at midmarket organizations indicated their solution was cumbersome to configure and manage, while 43% of respondents at very large enterprises said their solution threw off too many false positives. Those same respondents also noted a lack of integration with the existing security infrastructure at 41%. Meanwhile, 35% of respondents at large enterprises reported that their solution's implementation model slowed the application development and rollout process.

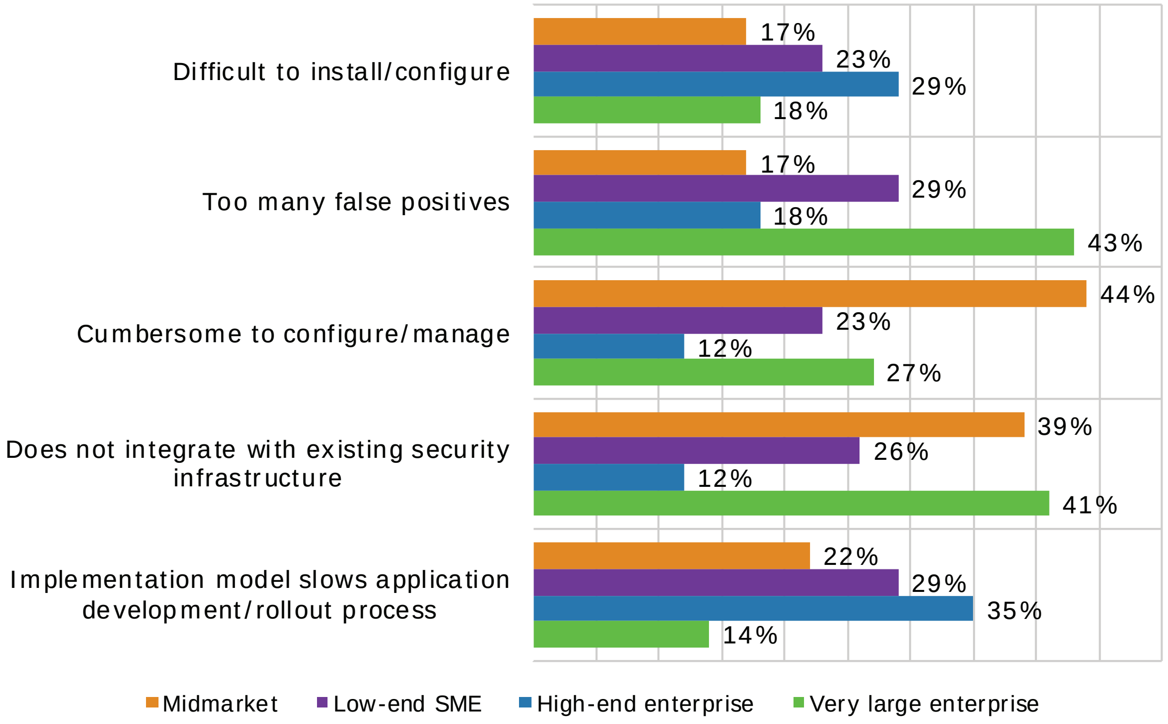
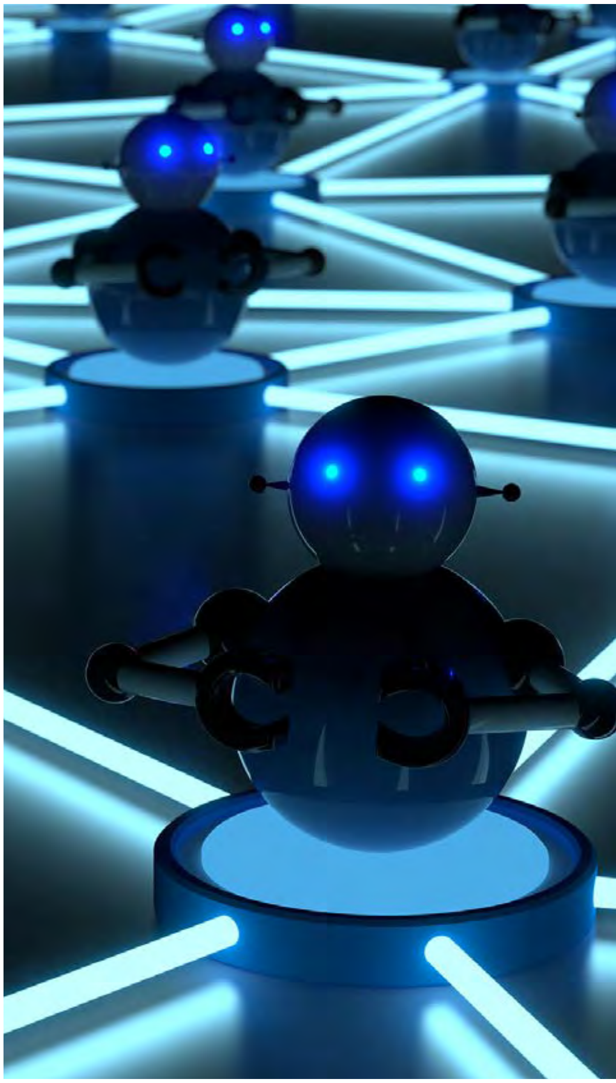


Figure 23: Top bot defense issues by organizational size.

Conclusion

Enabling the execution of bot attack campaigns is becoming a big business in the cyber underground, requiring organizations to step up their defenses and actively engage in the battle to let legitimate users and prospects in while keeping attackers out of online applications and services. These attacks, which are not just limited to ecommerce, target a range of vertical industries. As the attacks grow in sophistication, so do the bot defense solutions available in the market to combat the growing threat. Organizations that have a significant public-facing attack surface are under no illusion that their applications, whether web, mobile, or API-based, are a target for these attacks.



As organizations build out and manage their defenses against automated bot attacks, they are seeing success in detecting and mitigating the most frequently used attack techniques. This is especially true for application-level DDoS attacks, which the largest percentage of respondents indicated were detected and mitigated in less than one day. However, other more subtle attack types, such as denial of wallet and gift card fraud, still most often take two to three days or less than one week to detect and mitigate, leaving a longer time window for attackers to do more damage.

Thankfully, bot defense solutions are enabling users of the technology to limit the amount of damage automated bot attack campaigns are exacting. Respondents in the survey indicated that their use of bot defense technology enabled savings in both fraud resolution and web infrastructure costs. These savings apply to the growing volume of both mobile and API-based applications, which are typically less secure than traditional web applications.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at www.enterprisemanagement.com or blog.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook, or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

3929.01072020