THE IMITATION GAME

Detecting and Thwarting Automated Bot Attacks

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

SPONSORED BY:

f5®

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.

Methodology and Demographics

In late 2019, EMA surveyed 209 respondents representing organizations primarily serving North America to learn about how defenders are responding to this increasingly virulent attack vector. The research sought respondents primarily in IT and IT security roles representing organizations with at least 500 employees.

Respondent Industries

Although ecommerce companies are a prime target of automated bot attacks, the public-facing websites of other vertical industries are also on the radar for cyber criminals and other bad actors. Top targets identified by security industry researchers include banking/finance, ticketing, education, government, and gambling. In the EMA bot defense research, top verticals represented in the survey sample include finance/banking/insurance, high-technology software, manufacturing, healthcare/medical/pharmaceutical, and consumer goods retailers/wholesalers.

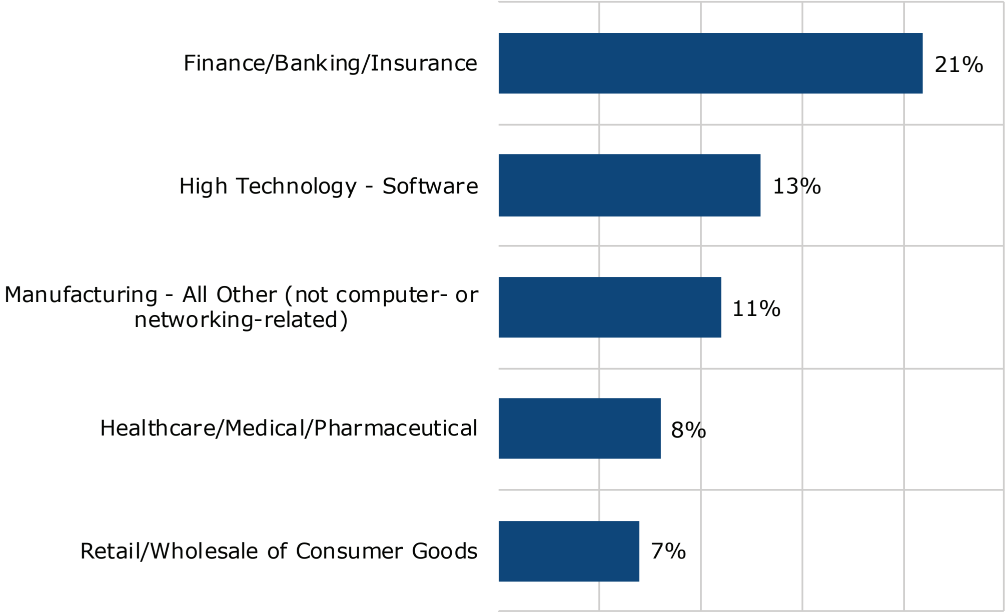


Figure 1: Which of the following best describes your company's primary industry?

It was important to include very large enterprises in the survey sample to reflect their experience with and response to automated bot attacks. These companies often have the largest attack surface to defend, and quite often they are at the forefront of digital transformation initiatives that lead to that increased attack surface. In EMA's sample, very large enterprises (those with annual revenues of at least $1 billion) were well represented, with 40% representing that category. Another 34% of respondents represented organizations with between $100 million to just under $1 billion in annual revenue.

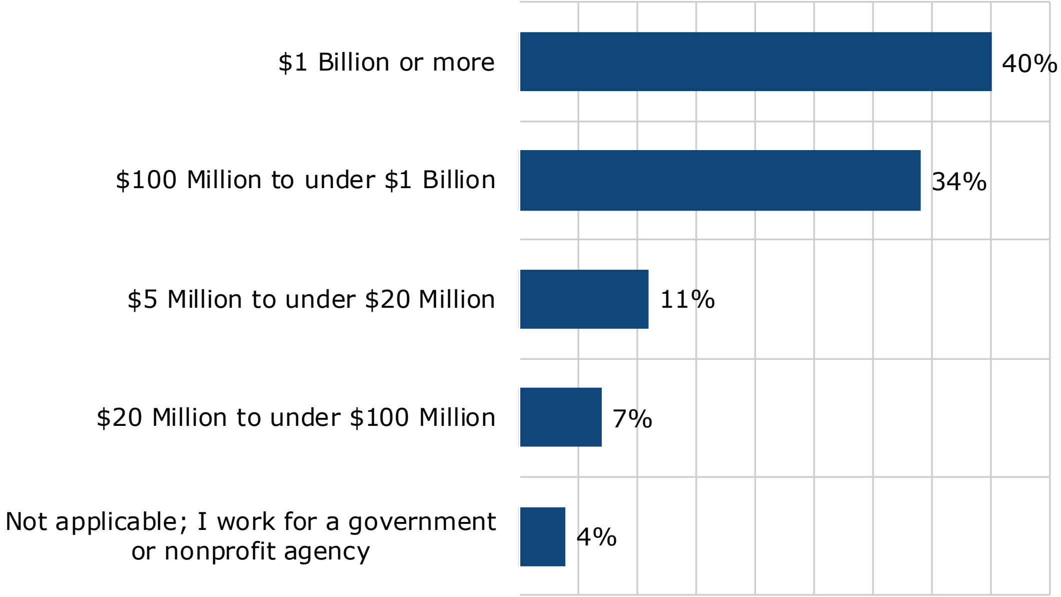


Figure 2: What is your organization's annual revenue?

Respondent Roles

The research sought out respondents most likely involved in the budgeting, evaluation, acquisition, day-to-day management, or use of the different offerings that provide defense against automated bad bot attacks. Those individuals often include the CISO, fraud, and IT security teams, as well as IT infrastructure teams. The use of bot defenses can also impact web application development because some solutions require changes to web applications. The chart shows the breakout of roles represented in the survey sample.

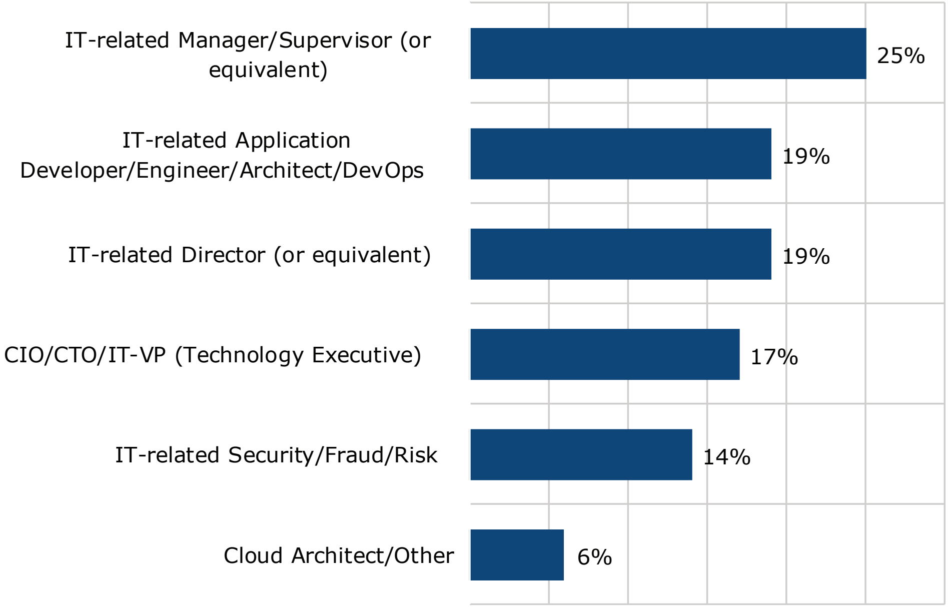


Figure 3: Which of the following best describes your role in the organization?

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.

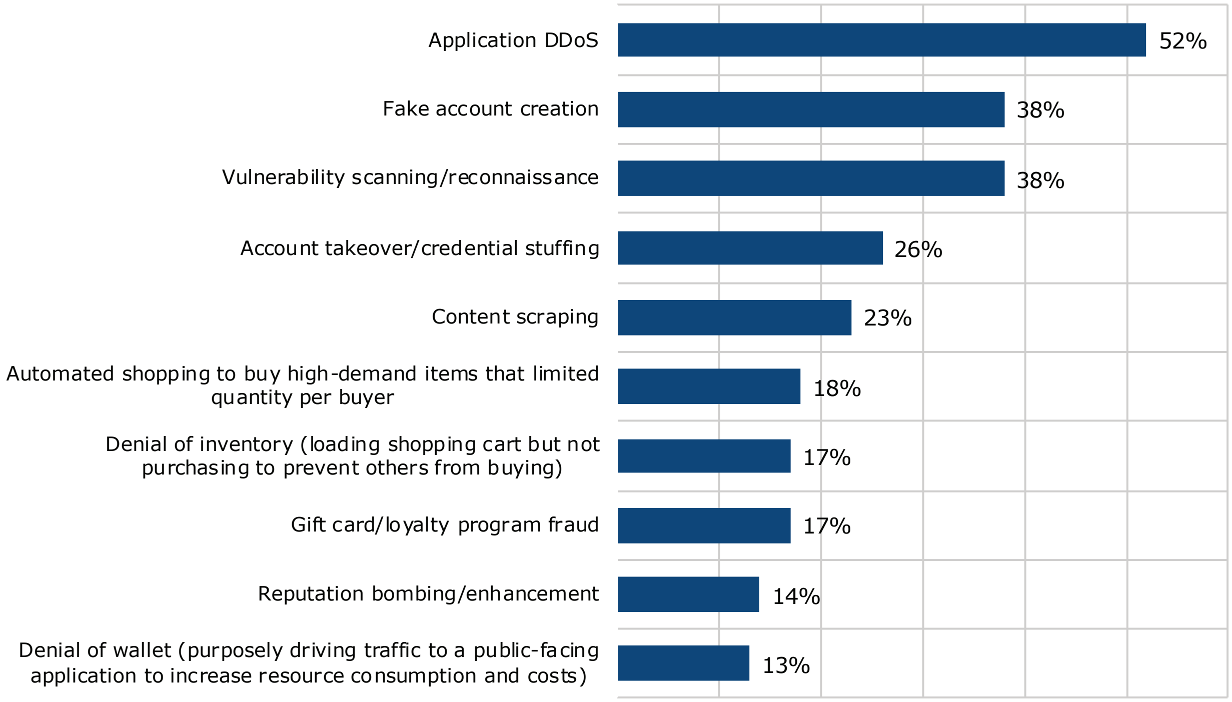


Figure 4: Over the past 12 months, which of the following types of malicious bot attacks have your organization's public-facing web, mobile, and API-based applications experienced?

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.

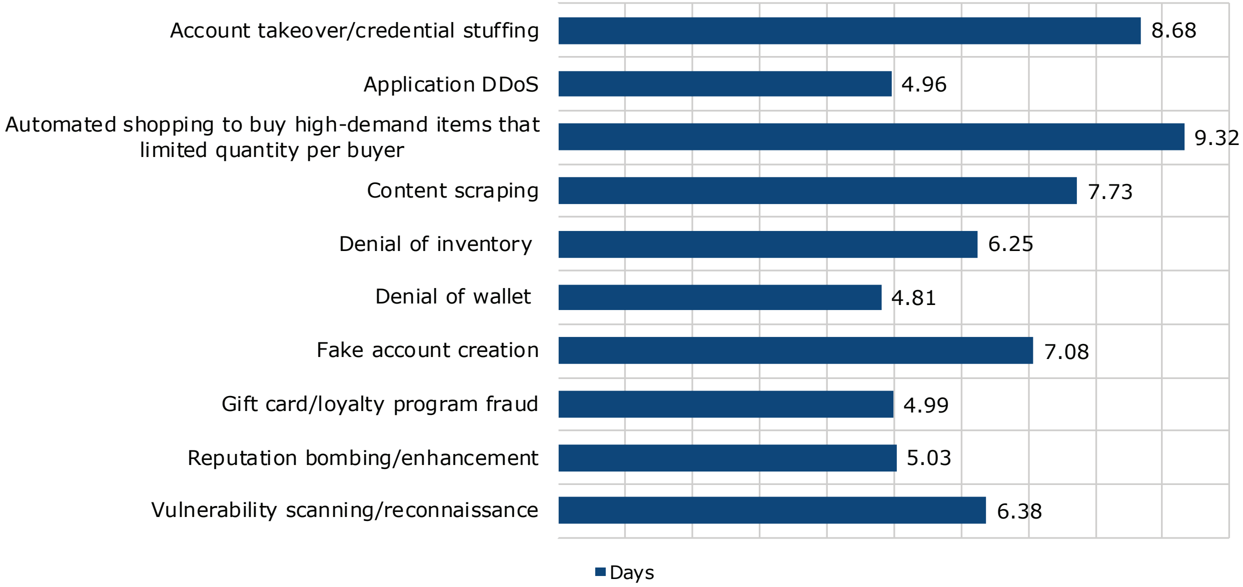


Figure 5: Mean time to detect each type of attack experienced.

Beyond coarse measurements, such as mean time to detect, it's a bit more encouraging to examine the breakout of detection time experienced by respondents according to each answer selected. For the top five most frequently experienced types of automated bot attacks, the good news is that all but one of those was, on average, detected in less than one day by the largest percentage of respondents. Nearly half of respondents reporting application DDoS attacks were able to detect those in less than one day. Fake account creation was the exception, with the largest percentage of respondents experiencing that attack type taking 2-3 days to detect it.

Other attack types experienced by a smaller percentage of respondents took significantly longer to detect, and thus appear to be harder to uncover. For example, of those experiencing denial of wallet attacks, it took 2-3 days for 22% of respondents to discover them and less than one week for another 22% of respondents to discover them. For the automated shopping to buy high-demand items attack type, it took 24% of those respondents 2-3 days to discern those attacks. Of those who experienced gift card/loyalty program fraud, it took 26% 2-3 days to detect the fraud and another 23% took less than one week to discover.

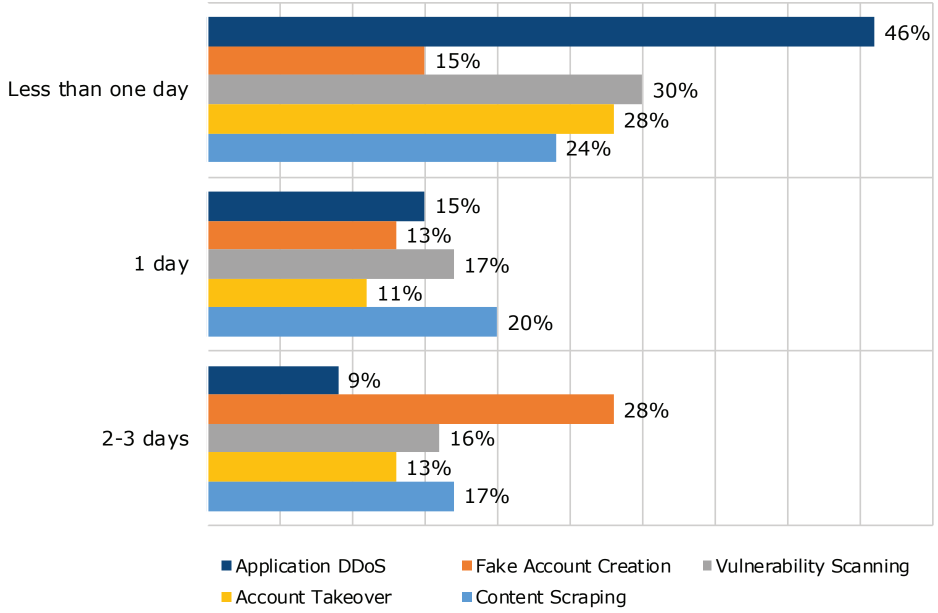


Figure 6: Time to detect top attacks experienced.

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 mitigate 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.

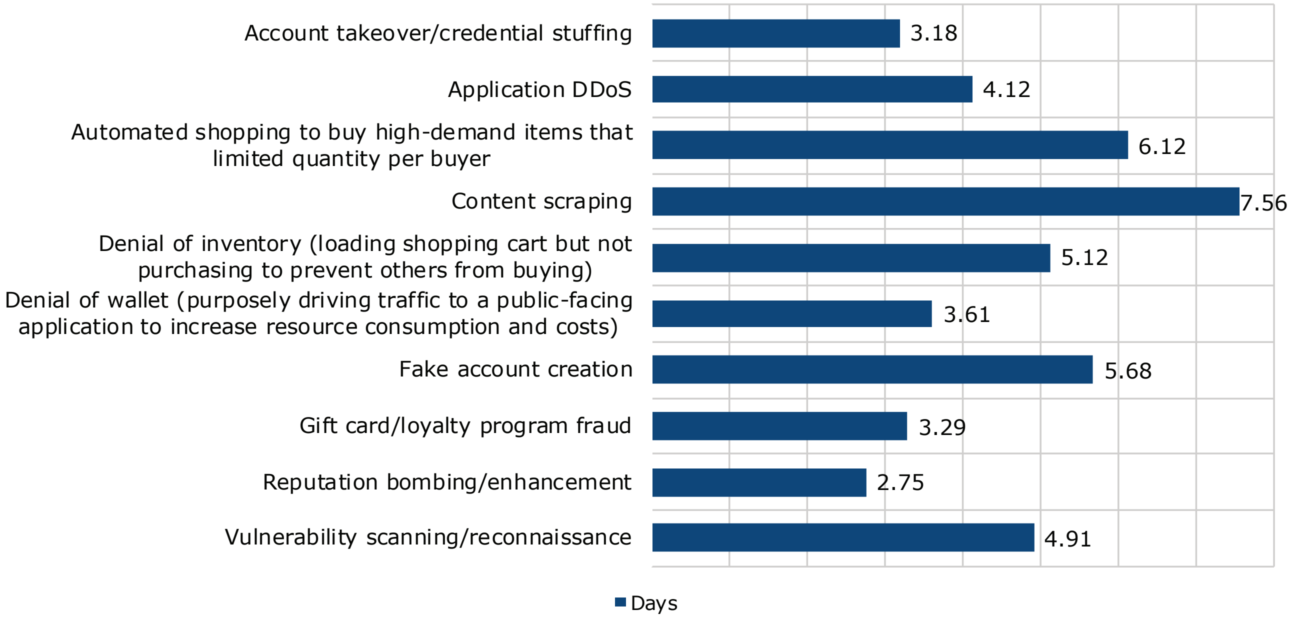


Figure 7: Mean time to mitigate attack types experienced.

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.

Account takeover seems to be a mixed bag, with some teams faster than others at mitigating this top attack type. Gift card/loyalty program fraud took longer for a larger percentage of respondents to mitigate. In that case, 26% of respondents took 2-3 days to mitigate and another 23% took less than one week to mitigate. The longer such attacks continue, the more the organization stands to lose in revenue and customer satisfaction.

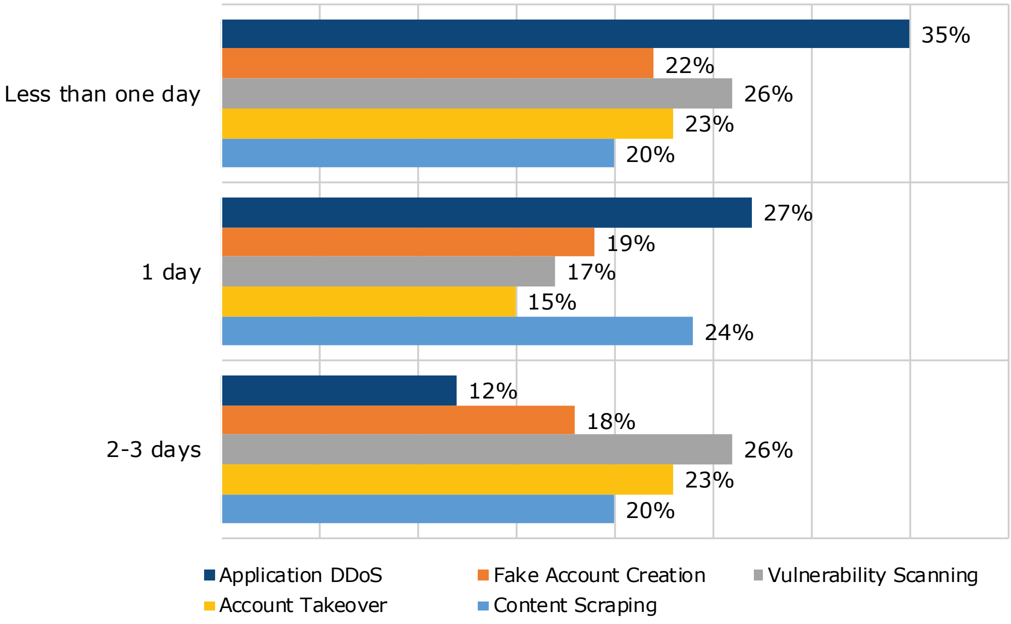


Figure 8: Time to mitigate top attacks experienced.

As organizations continue to evolve their automated bot attack protections, another wrinkle in the cat and mouse game between attackers and defenders is the increasingly persistent attempt to defeat those protections. Advanced persistent bots initially thwarted by an organization's anti-bot defenses attempt to discover how they were detected. Then, after some interval, attackers reconfigure and then relaunch their attack campaigns in an effort to bypass those initial detections. In this research project, EMA sought to gauge how often respondent organizations experience the reconfiguration and relaunching of attacks from the same source. The largest percentage of respondents indicated that such tactics occurred most of the time at 29%, while the second-largest percentage of respondents indicated that it occurred sometimes at 27%. Only 5% indicated that these retries never happen. The typical time interval between iterations of the reconfigured attack campaign cited by the largest percentage of respondents was one to two days at 43%, but another 29% indicated that such reload and relaunch activity occurred within 24 hours of the initial attack. Given the increase in the amount of bad bot attack campaigns that are being documented, along with the increasing sophistication of attackers and continued cat and mouse game between attackers and defenders, the frequency in the use of these tactics will likely increase.

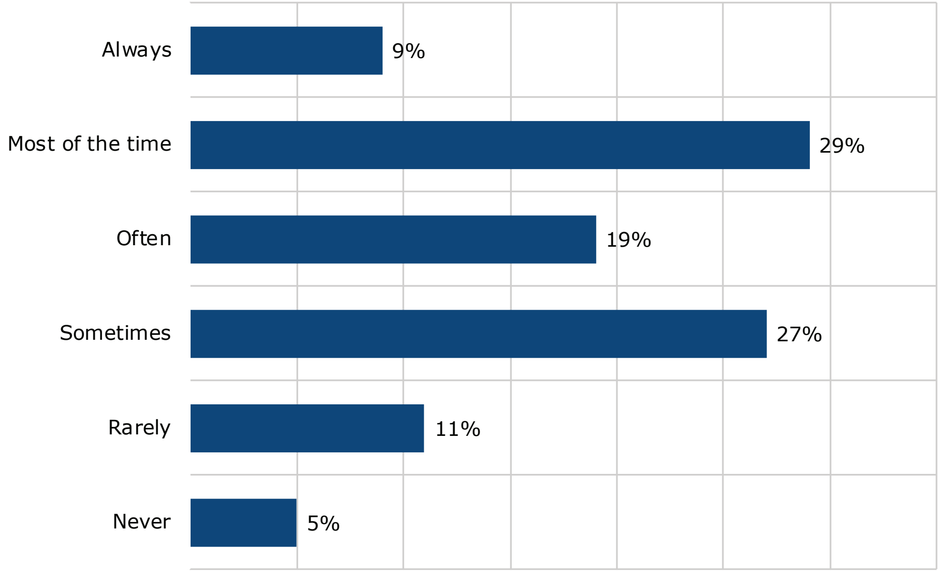


Figure 9: How often has your organization observed bot attack campaigns that attackers reconfigure to attempt to overcome your bot defense solution?

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.

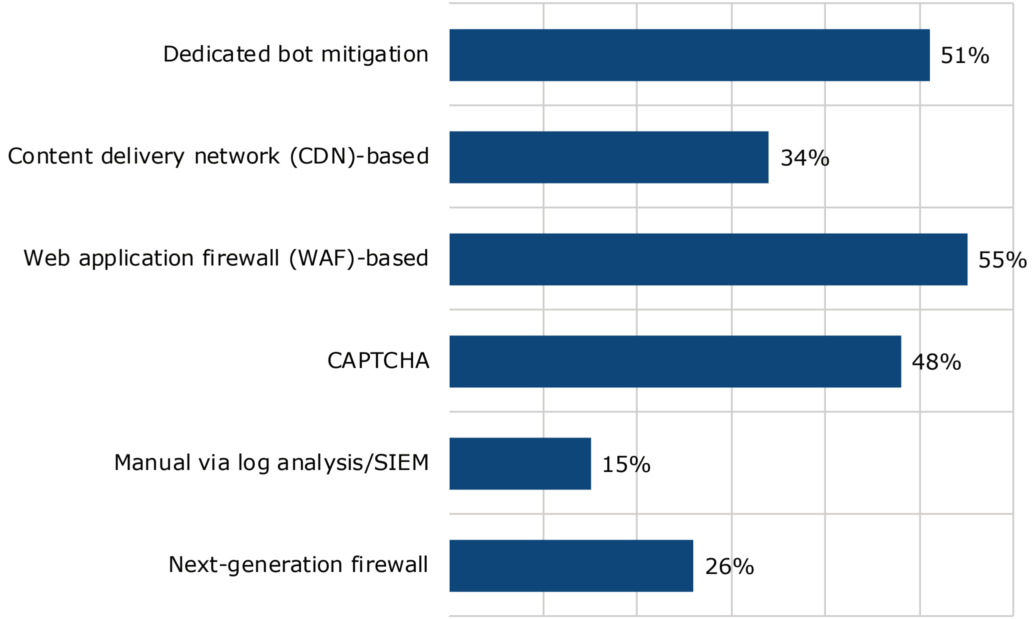


Figure 9: You indicated your organization is using a bot defense solution. Which of the following types of bot defense is your organization using?

Use Cases Driving Acquisition

It's no surprise that the top use case driving the acquisition of bot defense technology for all respondents was protection against application DDoS attacks, followed by account takeover attack protection. The least significant drivers for adoption of automated bot attack defense were also not a surprise, given the distribution of vertical industries represented in the sample. Those use cases—gift card/loyalty program fraud and denial of inventory—would have been higher priorities if the respondent sample had been more heavily weighted toward retail and hospitality/travel.

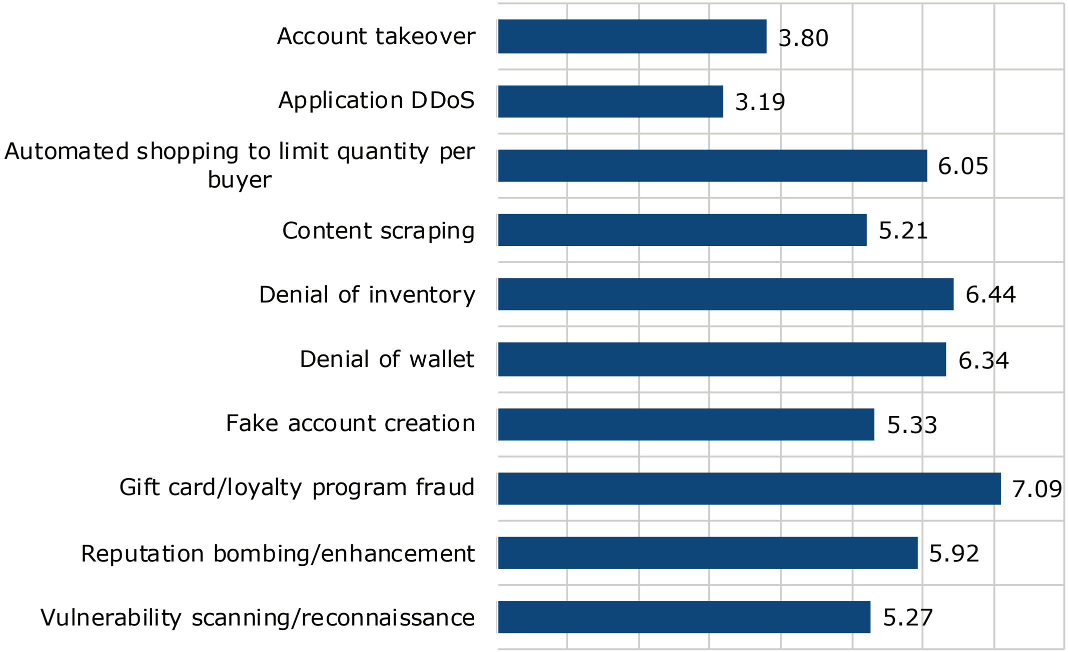


Figure 10: Of the following use cases, please rank each one in the order of importance to your organization's decision to acquire bot defense technology, with 1 being most important and 10 being the least important.

Among the top verticals represented in the sample, the banking/finance/insurance category was the one exception for top drivers, where account takeover was the biggest driver for bot defense acquisition. As more and more consumers conduct their banking, investing, and interaction with their insurance companies online—whether from a laptop or mobile phone—-the need to protect those accounts from cybercriminal access is critical to businesses in this vertical. Often, when a security solution is acquired to address one or more use cases, organizations find additional use cases that the solution can address once it is operational, allowing the buyer to realize greater value from their investment in the technology. Bot defense is no exception to that rule. However, when asked which additional use cases (if any) were realized post-deployment of their bot defense protections, the largest percentage of respondents indicated that application DDoS protection was an additional use case at 44%. Other most often cited additional use cases that came to light after deployment included content scraping at 27% and fake account creation at 26%.

	Most Important Use Case	Least Important Use Case
Banking	Account takeover	Gift card/loyalty program fraud
High-Tech Software	Application DDoS	Denial of wallet
Manufacturing	Application DDoS	Gift card/loyalty program fraud

Figure 11: Top vertical industry use cases driving bot defense acquisition.

Rating Bot Defense Effectiveness

Good bots are frequently beneficial to any business that relies heavily on prospects learning of their presence on the internet. Not only do good bots help support businesses by indexing their webpages to improve search engine results, they can also be used to monitor the health of an organization's website and to scan for vulnerabilities in need of patching before those can be exploited by attackers. Discerning the difference between a good bot, a human interacting with a website, and a bad bot is increasingly difficult, especially as attackers become better at mimicking the actions of humans as they interact with a commercial, government, or educational institution's website. Accuracy in classifying legitimate users, good bots, and bad bots is especially critical to any bot defense solution. At the same time, as attackers increase the sophistication of their attack techniques and use new approaches to get around existing defenses, the ability to correctly identify previously unseen bot attacks is becoming a key requirement. The research asked respondents to rate both measures of effectiveness for their bot defense solutions. While just a handful of respondents rated their solutions as highly inaccurate in classifying real users, good bots, and bad bots, there is room for improvement. Only 18% rated their solution as highly accurate. A slightly larger percentage (22%) rated their bot defense as most effective in identifying previously unseen bot attacks, and no respondents gave their solution the least effective rating.

As more and more organizations become reliant on API-based applications and mobile applications to interact with their customers and prospects, it is becoming crucial for bot defense solutions to effectively stop attacks aimed at those large and rapidly-growing attack surfaces. Respondents again were asked to rate the effectiveness of their bot defense's ability to stop such attacks on a scale of 1 to 5, with 1 being highly effective and 5 being highly ineffective. The good news is that the largest percentage of respondents by far gave their bot defense solution a rating of either 1 or 2. For API-targeted attacks 60% of respondents gave their solution a 1 or 2. For mobile application-targeted attacks, 61% gave their bot defense a 1 or a 2.

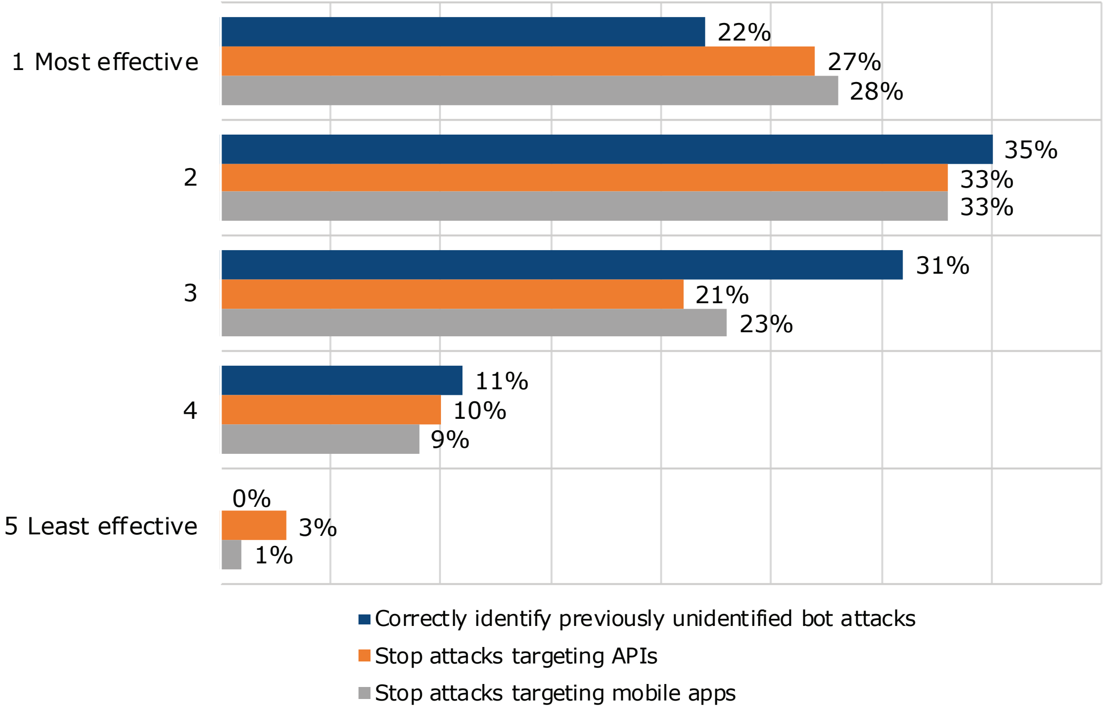


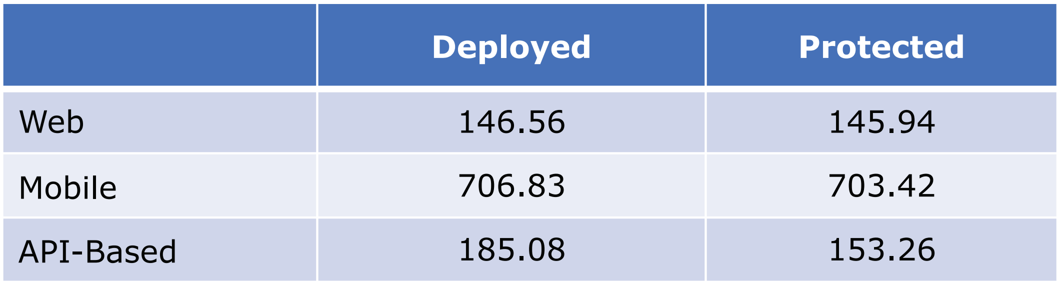
Figure 11: Based on a scale from 1 to 5, with 1 being the most effective and 5 being the least effective, how would you rate your bot defense technology's ability to…

Bot Defense Benefits, Broad Attack Surface

Bot defense technology holds out the promise of a range of benefits for organizations that deploy these solutions. By significantly reducing the amount of malicious traffic going to an organization's public-facing websites, enterprises can reduce the web infrastructure spend needed to ensure acceptable performance and availability for legitimate customers and users. Effectively using bot defense technology also helps to reduce the cost to resolve fraud, as well as reduce product losses/theft, including the theft of intellectual property. The technology can also improve the experience of legitimate users and improve brand reputation, customer experience, and web analytics. It can reduce account hijacking and fake account creation. The benefits realized as a result of implementing bot defense technology that are most important to respondent organizations were also measured in the survey. Respondents were asked to rank nine different benefits in order of importance to their organization. Reducing fraud resolution costs was selected at the most important benefit 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. For the second-most important benefit, the largest percentage of respondents indicated improved end-user experience at 19% and reduced web fraud resolution costs at 18%. Conversely, the largest percentage of respondents that indicated the least important benefit to the organization was improved web analytics, with 28% ranking that benefit as 9th.

For organizations that highly valued reduced cost benefits either from reduced infrastructure costs or a reduction in the cost of product losses/theft, the research queried respondents on the estimated amount of cost avoidance their organization realized through the reduction in such attacks. Forty percent estimated that figure as being between $101,000 and $500,000 annually, and another 26% estimated that figure as being between $501,000 and $1 million annually.

Another less direct way to measure the value that organizations realize from their investments in bot defense technology is to determine how extensively protection is applied across an organization's public-facing web, mobile, and API-based applications. Are organizations only applying it to the most critical applications? Are they protecting their full complement of public-facing applications? Or is that measurement somewhere in between? The research queried respondents on the average number of web, mobile, and API-based applications their organization deployed and the number protected by their bot defense solution. It appears most organizations are using the technology quite extensively, as shown in the chart. It should be noted that the average number of applications rose dramatically when taking into account application endpoints, and the numbers are skewed by a handful of very large enterprises that have thousands of public-facing applications and application endpoints, especially among respondents in the banking/financial services sector, where mobile banking has become a top priority. For the most part, these applications are deployed not only within the organization's data center, but also in the public cloud, with 58% and 59% of respondents reporting those locations for their public-facing applications. Another 44% indicated those applications were deployed in a private cloud.

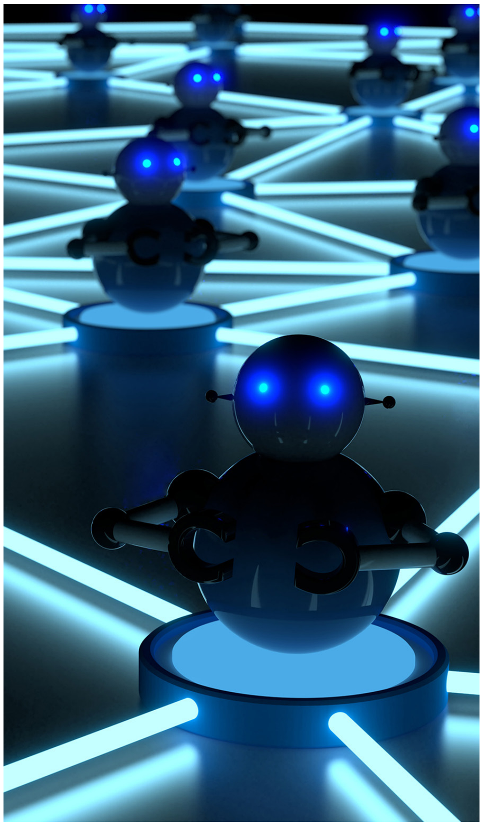


	Deployed	Protected
Web	146.56	145.94
Mobile	706.83	703.42
API-Based	185.08	153.26

Figure 12: Average number of public-facing web, mobile, and API-based application/application endpoints deployed and average number of those protected by bot defense.

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

3929.01272020-F5 Summary