O'REILLY®

Compliments of ORACLE® + Dyn

Securing Web Applications

Building a Strategy for Defense Against Malicious Bots

Stephen Gates & Allan Liska

ORACLE® + Dyn

Intelligent Web Application Security

Bot Manager | WAF | API Security | DDoS Mitigation

Oracle Dyn Web Application Security services give application delivery and security professionals the tools and expertise they need to intelligently defend their sites, systems and applications from a complex and ever-evolving cyber threat landscape. We use adaptive machine learning and automation to proactively combat cyber attacks for organizations, from DDoS and OWASP Top 10 to bots and API level attacks.

Benefits include:

- Cloud-based – no new hardware, easy integration, scalable.
- Managed 24x7 by a globally distributed team of security professionals.
- Intuitive, web-based dashboard designed for simple management all from one location.

For more information visit **dyn.com/security**.

Securing Web Applications

Building a Strategy for Defense Against Malicious Bots

Stephen Gates and Allan Liska

Beijing • Boston • Farnham • Sebastopol • Tokyo O'REILLY®

Securing Web Applications
by Stephen Gates and Allan Liska

Printed in the United States of America.

Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472.

O'Reilly books may be purchased for educational, business, or sales promotional use. Online editions are also available for most titles (*http://oreilly.com/safari*). For more information, contact our corporate/institutional sales department: 800-998-9938 or *corporate@oreilly.com*.

Editor: Courtney Allen
Production Editor: Justin Billing
Copyeditor: Octal Publishing, Inc.
Proofreader: Chris Edwards
Writer: Melissa Elicker
Interior Designer: David Futato
Cover Designer: Karen Montgomery
Illustrator: Rebecca Demarest

May 2018: First Edition

Revision History for the First Edition
2018-05-10: First Release

This work is part of a collaboration between O'Reilly and Oracle Dyn. See our *statement of editorial independence*.

978-1-492-04024-8

[LSI]

Table of Contents

CHAPTER 1
Introduction

Web application security protects your enterprise applications—the critical applications that drive your business forward—from constant, complex, and sophisticated threats. Most of these applications live on the network edge, where they are internet-facing and where attackers are increasingly focused on gaining access to your downstream data. It's paramount that you focus on mitigating these threats to reduce or neutralize their impact and maintain fast, reliable access to applications and services for your customers.

Web application security is much more than an IT problem. It can become a significant business problem if not handled aggressively. Attacks on web applications can circumvent your security and harm your business in myriad ways by creating unwanted downtime, reducing availability and responsiveness, and shattering trust with your customers when data confidentiality and integrity are compromised. Customers have little patience for slow or unavailable web applications, and if you fail to mitigate these risks, they're likely to take their business elsewhere.

The sophistication of recent web application attacks has grown rapidly and significantly, and this trend is expected to continue. Attackers use increasingly complex methods to access, extract, or steal critical data that lives on the network or cloud edge. In fact, according to a 2018 survey from Synscourt and Vision Solutions on the new IT landscape, 37% of IT professionals stated that their chief security challenge is the increasing sophistication of attacks. These attacks can severely cripple compute-intensive edge applications. The rise of rogue mobile applications and infected Internet of Things (IoT) devices turned into malicious bots is exponentially increasing the risks organizations face. Making matters worse, security teams are often too overwhelmed to promptly patch known vulnerabilities or take normal security precautions, which severely increases the risks they face daily.

Whatever the attack scenario, poorly secured web applications make fertile ground for attackers interested in gaining access to your systems or getting deeper into your data. In fact, it's often a faster, more efficient approach for attackers to use these vectors than compromising internal computers and attacking servers in the datacenter from within. To protect your business from web application security threats, you must be aware of the types and sources of attacks facing modern web applications, understand the threats they pose to your business model, and execute a modern web application security strategy.

This report covers the threats to modern web applications with a special emphasis on a growing risk that represents arguably the most pervasive and significant threat facing web applications today: the massive increase in malicious bots. It also provides you insights on the continuous stream of newly discovered application vulnerabilities, the growth of machine-to-machine communication via application programming interfaces, the upsurge in distributed denial-of-service attacks, and highly sophisticated, server-based malware. The report will help you better understand malicious bots and other threats and the risks they pose, so you can plan and implement effective web application security.

CHAPTER 2

Threats Targeting Your Web Applications

There are numerous security threats to modern web applications, including malicious bots, distributed denial-of-service (DDoS) attacks, malware, and application vulnerabilities, as well as application programming interfaces (APIs) and mobile application risks. In this section, we focus on how these threats work and how they could affect your business.

Malicious Bots

Malicious bots are rogue devices that pose a growing risk to modern web applications. The flexibility, increasing sophistication, and power of malicious bots make them formidable threats to your application security. Malicious bots can perform account takeovers, account creations, credit card fraud, DDoS attacks, and more. Malicious bots can exploit application vulnerabilities as well as attack via APIs and mobile applications. Moreover, malicious bots are responsible for launching the world's largest DDoS attacks on record as well as spreading malware and exploit kits. All of these activities can affect performance, availability, and ultimately your bottom line.

Malicious bots are increasingly being utilized to infiltrate enterprise web applications at the network or cloud edge. This particular threat is what poses likely the most significant threat to your web applications. As a result, we cover this topic in more detail in Chapter 3, where you'll learn how malicious bots work, how they circumvent your security posture, and, more importantly, how they can affect your business.

DDoS Attacks

DDoS attacks occur when multiple devices consume and overwhelm the bandwidth of an organization's internet resources, encumber network routing and

switching devices, melt down border firewalls and other security appliances, or overload the resources of one or more web services. DDoS attacks are often the result of multiple compromised devices or systems, operating in sizable botnets and flooding the targeted system with bogus traffic. DDoS attacks can also take advantage of protocols that can return a large amount of data in response to a small query; for example, sending a simple DNS request from a spoofed IP address that returns a large amount of data to that spoofed IP.

Recently, the size of DDoS attacks has grown exponentially due to newly discovered reflective and amplification techniques, most notably in use by malicious bots. The sophisticated use of bots is the catalyst that drives the multiterabyte DDoS attacks we're seeing today and expect we'll see well into the future. Attackers are now abusing malicious bots to drive DDoS attacks more than 51,000 times more powerful than their original strength. This invariably results in failed internet infrastructure, wreaking havoc on major websites, and bringing your ability to do business to a halt.

One of the factors driving the current proliferation of malicious bots and corresponding DDoS attacks is the Mirai malware. Mirai works by using a list of default usernames and passwords to take control of IoT devices. Mirai is self-propagating—each infected device has the ability to scan the internet to find similar devices and subsequently infect them.

Unfortunately, Mirai has also inspired copycat attacks that work by exploiting vulnerabilities in the underlying code on IoT devices instead of relying on default usernames and passwords. When a vulnerability is discovered, attackers quickly develop exploit codes to take advantage of the vulnerabilities. As a result, copycat botnets—like Reaper, Satori, and Okiru—are fueling increasingly powerful attacks themselves, exceeding the power of the original Mirai botnet.

By employing malicious bots, recent attacks have surpassed 1.7 Tbps, a truly massive display of power. According to Arbor Networks, one of the observed attacks targeted the customer of an unnamed US-based internet service provider (ISP). Fortunately, the ISP had proper DDoS defenses in place and no outages were reported, reinforcing the fact that strong defenses are both necessary and possible, even in the face of these colossal attacks. Many DDoS subject-matter experts believe that attacks will continue to grow in size, and multiterabit attacks will become the norm.

DDoS attacks can also easily divert or mask your security team's attention from other malicious activity. For example, decoy attacks frequently employ the use of short-duration attacks that begin and end, over and over again, yet don't completely take your organization offline. These attacks distract your team from other nefarious actions, such as infiltrating networks or systems to steal data.

Malware

Malware is defined as software that has malicious intent that is usually hidden from computer users. Common types of malware include viruses, worms, Trojans, adware, spyware, ransomware, and key loggers. Malware can perform a variety of malicious operations including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions, and monitoring users' computer activity without their permission.

Although often targeting end points, malware is also a continuing security problem that can target web applications and the servers they run on. Malware infections often are triggered by computer users themselves and often spread through simple and necessary business activities. Malware infecting your web applications and servers normally does so due to poor coding practices, questionable file downloads, malicious links, or malicious file uploads. For example, many of today's websites allow customers and visitors to upload files for a variety of business reasons, like a photo of a recent accident sent to an auto insurer or a document with e-signatures. These files can contain malware that can affect your website and applications or, worse, use your websites and applications to host and distribute malware. This has the potential to unknowingly infect customers on your site and spread exponentially from there. Of even greater concern, exploit kits can bombard your visitors with malicious code, targeting their operating systems, browsers, and media players.

Clearly, there are business implications if your organization's sites or applications are identified sources of malware. Unfortunately, without proper security vigilance, websites and web applications can unintentionally serve as hosts to malware for significant periods of time (think months or years). Undetected, malware can be responsible for damages due to spiking network traffic, the loss of critical data, and the erosion of trust by customers infected by malware residing within your web applications.

Application Vulnerabilities

Application vulnerabilities are flaws in code or application design that create a possible point of compromise and potentially allow entry for attackers. These flaws can be newly identified by attackers (unannounced) or known by third-party software vendors (announced) and often leave edge apps at risk to security breaches, as attackers fervently write exploits to take advantage of previously discovered and unpatched vulnerabilities. This in turn can lead to serious data breaches that harm your customers, lead to loss of intellectual property, and otherwise damage your business. Common examples of web application vulnerabilities include injection vulnerabilities, cross-site scripting (XSS), broken

authentication and session management, insecure direct object references, and security misconfiguration.

A prime example of the impact of unpatched application vulnerabilities is the much-publicized Equifax breach, in which a flaw in the open source Apache Struts framework used to build its web applications left the credit reporting agency vulnerable, resulting in the exposure of personal information for 143 million US consumers. Although the Equifax breach gained notoriety for its application flaws, this is a common problem that affects organizations of all sizes. Organizations increasingly rely on complex third-party web applications to deliver services to their customers. This leaves security teams heavily dependent on these third parties to release patches in a timely manner when new security flaws are discovered. Unfortunately, this means that at any given time, there are millions of vulnerable hosts available to exploit.

The sprawl of modern distributed systems exacerbates this already significant problem. Modern enterprises have hundreds or thousands of different systems and applications that must be monitored, patched, and otherwise managed in a secure manner. In any given week, a dozen or more patches need to be installed by a limited staff with limited time to addresses these issues, all without affecting usability for customers or internal teams. As a result, web applications with known vulnerabilities might go unpatched for months, depending on the severity of the vulnerability when it is first announced, the available staff resources, and the asset management policies of the enterprise in question.

The other reason that this problem continues to grow is the ease of access to infrastructure-on-demand services. Five years ago, procuring a new service usually meant your staff would go through a process to deploy servers in an organization-controlled datacenter. In today's age of cloud computing, that is no longer the case. Now, nearly any employee with a corporate credit card can feasibly initiate infrastructure deployment. For example, if your marketing team wants to set up a website for a contest, it could simply request the domain it needs and deploy the new website. Although this allows for more employee ownership and reduced necessity of IT resources, it can be a nightmare for security teams. Simply stated, they cannot secure systems they don't know about. That newly procured site could be running an outdated version of WordPress or JBOSS that could be easily exploited, and presumably no one would be monitoring it to mitigate these risks.

It's useful to know that newly announced vulnerabilities are recorded in the National Vulnerability Database (NVD) maintained by NIST. When a new vulnerability is released, NIST includes important information such as the CVE (Common Vulnerability and Exposures) number; affected systems, also known as Common Platform Enumeration (CPE); and the risk of the vulnerability denoted by the Common Vulnerability Scoring System (CVSS) number.

CVSS is important, because it helps your organization determine patch prioritization. For example, a new vulnerability with a CVSS score of 2 is going to be a lower priority than one with a CVSS score of 10. Although helpful, this scoring system is inherently imperfect. The problem with this methodology is that just because a vulnerability has a low score today doesn't mean it always will. So, if a new vulnerability is announced that affects an internet-facing system but has a low CVSS score, it will often be low on the patch priority scale and might stay that way for a long period of time, even if someone figures out how to exploit it and starts automatically scanning and exploiting vulnerable systems.

According to the Veracode State of Software Security 2017 report, vulnerabilities appear in previously untested software at alarming rates—with 77% of applications having at least one vulnerability on initial scan. The report also notes that even the most severe flaws take a long time to fix, with only 14% of very high severity flaws closed in 30 days or less. Increased vigilance is clearly needed.

Malicious bots come into play here, as well. When a vulnerability is found by researchers or attackers, exploit code can often be found in the dark net within days or hours of a vulnerability being discovered. In turn, attackers can modify or reprogram existing bots to continuously scan the internet to find and capitalize on these newly discovered vulnerabilities. A prime example of this is WordPress, which has had its share of vulnerabilities over the years and, more importantly, has thousands of available plugins that are especially prone to vulnerabilities. Attackers program bots to comb through the directory structure of WordPress sites looking to exploit these known vulnerabilities.

APIs and Mobile Application Risks

The majority of web applications use multiple APIs to connect with other applications and keep the online community connected. APIs decrease development time and generally make app development easier. If not used securely, though, unprotected APIs can pose serious risks to data security, leading to data breaches and denial-of-service (DoS) outages. Another challenge with APIs is that inexperienced developers often leave API keys exposed on the internet, either on paste sites or technical support forums. If an attacker stumbles upon an API key, they can use it to extract sensitive information from your applications or push services to the vendor, possibly incurring thousands of dollars in fees that are charged to the victim organization.

The ubiquity of mobile apps poses serious risks, as well. Consider apps on smartphones that are used to make purchases or book travel reservations. These apps sit on the network edge, often in the internet public domain. Attackers can easily find and reverse engineer them to create havoc and threaten data security.

Mobile apps usually communicate directly with your backend APIs. Mobile devices communicating with servers in these machine-to-machine transactions provide fertile ground for attackers to access private or proprietary data. These automated interactions are prime targets for harmful data breaches, DoS outages, and man-in-the-middle attacks. In a mobile environment, limiting traffic from a single IP address doesn't work to thwart this kind of malicious activity due to Network Address Translation (NAT), which is a way to remap one IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

CHAPTER 3

Malicious Bots Threatening Web Applications

Malicious bots pose an increasingly large risk to web applications. The flexibility, increasing sophistication, and power of malicious bots make them formidable threats to your application security. Malicious bots can perform account take-overs, account creations, credit card fraud, massive DDoS attacks, and more. All of these activities can affect performance, availability, and ultimately your bottom line. Considering the severity of the risk posed by malicious bots, this section will focus on explaining how they work, how they most frequently circumvent security measures, and, most importantly, how they can affect your business.

Simply defined, bots—whether malicious or not—are devices that use software to execute commands automatically with little or no human intervention. Bots can be good or bad. Some examples of good bots include media/data bots, copyright bots, and spider bots used by search engines such as Google to crawl web pages and analyze content for inclusion and ranking in search results. Malicious bots include spam/email bots, impersonator bots, zombie bots/botnets, download/transfer bots, spy bots, scraper bots, and click/ad fraud bots.

Complicating defense against malicious bot activity is the fact that you can't simply block all bot traffic. A surprising amount of modern internet traffic is derived from bot activity. In fact, recent reports indicate that global internet traffic generated from bots is now surpassing human-generated internet traffic. Good bots, such as Google and Yahoo bots that continuously scan your site and catalog search-engine optimization (SEO) data, must be allowed to continue doing their job. At the same time, you must protect against malicious bots that have more nefarious objectives.

Attackers are increasingly utilizing bots to target your enterprise web applications at the network or cloud edge. This, in turn, results in potentially damaging

downtime and commercial losses for your business. Moreover, the bot problem is set to grow exponentially as the volume of IoT devices explodes. According to Gartner, it's estimated that more than 20 billion new devices will be connected to the internet by the year 2020, many of them consumer IoT devices that are poorly secured, vulnerable to attack, and easily hijack-able.

Everyday Bot Attacks and High-Profile Examples

As previously noted, malicious bots can pose a variety of risks. In this section, we discuss the most common attack vectors utilized by malicious bots and how these attack vectors translate to risks to your web applications.

Credential Stuffing

Credential stuffing is an example of a *brute-force attack*, in which large numbers of usernames and passwords are automatically entered into websites until they are matched to an existing account. This particular attack vector is fed by password reuse. Password reuse is the tendency of people to use the same password across multiple accounts, including professional and personal accounts. In large data breaches, attackers often dump lists of usernames and passwords from breached systems and, in turn, other attackers purchase and download long lists of user credentials, hoping that consumers used these same credentials for their banking, ecommerce, and other online accounts. An attacker can feed a password dump from an attack into a botnet under their control and program the bot to try to use those credentials against all internet-facing servers of hundreds of organizations simultaneously. This allows attackers to then hijack the account for their own purposes, often committing fraud, emptying bank accounts, and making bogus purchases.

Denial-of-Inventory

Malicious bots are fully capable of denial-of-inventory (DoI) attacks, repeatedly making and canceling purchases, holding and/or consuming inventory, scraping sites, stealing information, and a host of other unwanted activities. Beyond DoI, attackers also use malicious bots to deplete goods or services from inventory, but without actually purchasing the goods. In short, these attacks use bots to select and hold items from limited inventory or stock by adding them to their carts, but without purchasing. This prevents legitimate users from buying the items themselves.

Mirai

A particularly infamous piece of malware, known as Mirai, uses a somewhat similar approach to take over vast numbers of poorly protected IoT devices, mostly

consumer based. These IoT devices have a default username and password set when sold to consumers. Unfortunately, many consumers and businesses (who also have IoT devices) don't change this default password upon purchase, meaning they can easily be hijacked. Mirai, using a table of common factory default usernames and passwords, continuously scans the internet for the IP addresses of IoT devices with open telnet ports, and then logs into them to infect them with the Mirai malware. Infected devices continue to function normally, marked only by occasional sluggishness and increased use of bandwidth, meaning that the owners of these devices often don't realize that the device has been hijacked.

Mirai has an even more insidious attribute: it's self-propagating. Not only did it infect large numbers of IoT devices worldwide, but it also came with worm-like capabilities similar to the malware of the early 2000s, such as SQL Slammer, Nimda, CodeRed, Conficker, and others. These pieces of malware spread on their own with no human intervention, and Mirai did the same thing. After a device was infected, it in turn began to scan the internet and infect other IoT devices in the same fashion. To increase the damage if inflicted, Mirai was prepackaged with a plethora of DDoS attack tools baked in.

Industries Facing Malicious Bot Targeting

The threat of malicious bots is a growing concern for many industries, including travel-related enterprises, entertainment companies, and retail organizations. Even though no industry is immune to malicious bots, some have suffered more than others due to their profitability.

Travel Industry

The airline industry has been heavily targeted by and is often particularly susceptible to malicious bots. In fact, according to Distil Networks, in 2017 more than 40% of all inventory-stealing bot traffic was directed toward the airline industry. Frequently, these attacks take the shape of DoS or DoI attacks in which malicious bots are used to deplete goods or services from inventory, but without actually purchasing (or purchasing, but then shortly thereafter canceling the purchase) goods. In short, these attacks use bots to select and hold items from limited inventory or stock by adding them to their carts, but without completing the purchase. This renders legitimate users unable to buy, pay, or confirm the items themselves.

For example, in one real-life scenario, an Asian airline noticed that large numbers of seats were being reserved and then released right before the 24-hour reservation cancellation deadline. As a result, prospective customers booked flights with competitive airlines instead. This resulted in a severe financial hit for the targeted airline. Eventually, the affected airline worked with a security partner to initiate a

series of bot management activities in the form of Java script and human-interaction challenges to successfully thwart the malicious bot onslaught.

In another example, an international car rental agency was seeing a high volume of car rental reservations being made and then cancelled at the last minute. Again, the culprit was identified as a malicious bot being used by a competitor. Bot management solutions were employed to deter the threat.

Retailers

When it comes to online retailers, malicious bots engage in electronic cart-stuffing activities that generate a loss of sales due to the appearance of low inventory, which drives customers to shop other retail options. Competitive advantage is certainly a motivator for deceitful businesses, especially when they manufacture or sell products that are very similar to their competitors. Diverting purchasers away from your sites is a reality that all online retailers face.

Online ticket retailers who sell tickets to concerts, shows, plays, and other venues have also been affected by malicious bots. Scalpers often use bots to hold large numbers of seats in limbo. However, scalpers often won't make a purchase until they have other buyers lined up to purchase the tickets they resell.

This kind of customer- and inventory-stealing bot traffic is not just the domain of criminals. Some unscrupulous companies use bot traffic against their competitors. Even companies that don't engage in that type of behavior still often rely on these types of bots to scrape competitors' websites to find the latest pricing data and ensure they are setting their prices at the same level as their competition.

CHAPTER 4

Prioritizing Your Web Application Security Defenses

With so many possible threats and attack vectors affecting your web applications, it's critical that you have a strategy for how to defend against these diverse threats. You should first prioritize defense against the most disruptive scenarios for customers.

With this construct in mind, you should focus on three pillars integral to maintaining business continuity and keeping customers happy: *availability*, *confidentiality*, and *integrity*. These three principles provide an ideal framework for discussing and addressing the core elements of a web application security program.

Availability

Availability will always be the top priority for your web applications and your business. Simply stated, if your applications are not available to either your staff or your customers, your business suffers as a result. Thus, ensuring availability represents the most important priority for web application security. It's worth noting that availability can be affected by both technical problems (targeted attacks, system failures, etc.) or natural disasters (power fluctuations or outages, flooding or other natural disasters, etc.). However, within the context of application security, we're focused on the implications of attacks.

The business implications of availability are significant. We can measure the high cost of downtime to businesses large and small in terms of cost and productivity. Recent studies show that on average, IT downtime costs businesses $1.55 million every year. Data shows technology downtimes affect productivity, as well, with 545 hours of staff productivity lost annually because of IT outages.

However, the threat is not outages alone. Reduced performance and responsiveness, such as slow load time induced by malicious bots and other attacks, have a negative impact on your business. As cited in a Radware blog, a survey conducted of more than 2,500 online consumers in the US and UK found that 67% of UK shoppers and 51% of those in the US said that site slowness is the top reason they'd abandon a purchase. Accordingly, your security focus begins with ensuring that your websites are always available and cannot succumb to targeted attacks that significantly slow or entirely take down your systems or applications.

Data Confidentiality

Data confidentiality equates roughly to the standard definition of privacy. Data confidentiality is centered on the promise that shared data is being held in confidence—that customers can trust that the data they provide to you is not being leaked, shared inappropriately, or stolen. Ensuring data confidentiality means taking preventative measures to keep sensitive data out of the wrong hands. To protect data confidentiality, you must understand what data your company holds, how sensitive that data is, and the paths that could be taken to access that data. Clearly, the more sensitive or important the data, the more efforts should be taken to protect it. Maintaining data confidentiality protects your reputation for being reliable and trustworthy to partners and customers alike.

Data Integrity

Data integrity addresses one all-important question: can I trust the data? This means, for example, that when bank customers log into their accounts, they trust that the numbers they see are true and accurate—with confidence that the data and data fields have not been manipulated in any way. Like data confidentiality, data integrity protects your reputation and fosters trust with partners, internal stakeholders, and customers.

CHAPTER 5

Maintaining Availability: A DNS-Based Approach

As previously noted, availability must be the highest priority in building a web application security strategy. To do business, your applications must be available to both your staff and your customers. Securing your Domain Name System (DNS) infrastructure is a critical first step to ensuring the availability of your enterprise applications and cloud services. DNS is a foundational piece for protecting availability. A thorough analysis of your DNS infrastructure and its ability to deliver on availability requirements should include building DDoS defenses, implementing a plan for active failover, and coordinating availability plans with your DNS server provider to assure performance and responsiveness. From there, you build up step by step to the application layer to provide both data availability and protection.

The reality is that most organizations don't think about DNS availability until after an incident occurs. Often, organizations simply leave DNS management in the hands of their domain registrar without inquiring about the availability and reliability of the registrar's DNS infrastructure. Yet DNS breaches and outages, aswell as slow DNS performance, can lead to customer dissatisfaction, a tarnished brand image, and revenue loss. As applications and resources become more distributed, addressing DNS at the edge becomes more important to ensuring a high-quality, consistent experience.

DDoS Mitigation

DDoS attacks pose the largest and most likely cyberthreat to availability. Accordingly, mitigating the threat of DDoS attack should be your first priority in maintaining web application availability against security threats. These attacks can leave your websites and applications vulnerable to downtime, reduced perfor-

mance, and downward-spiraling availability. As noted in Chapter 2, the size and strength of these attacks have been growing exponentially. The vast majority of organizations (if any) cannot realistically maintain availability using in-house resources alone.

Regardless of where your websites are hosted, when an attacker locates the IP address of your origin servers, your organization is vulnerable to being taken offline. However, with web applications specifically, an attacker might not even need to locate the IP address of your server to wreak havoc. Instead, the attacker can focus the attack on the targeted web application, making it unavailable and disrupting a critical service at an inopportune time. This happens often during major events. For example, a number of DDoS attacks were directed at various parts of the Olympics website during the 2018 Winter Olympics. The attacks targeted different parts of the website rather than the whole site and were designed to maximize the impact of the attacks.

Attackers can dramatically lower the availability of your website by launching DDoS attacks designed to overwhelm your servers. Whatever the intent of the attack—hacktivism, a disgruntled employee, extortion, or a competitive attack—your customers and your business suffer. DDoS attacks can swiftly and effectively cripple your business model, taking services and sites down for extended periods of time.

Active Failover

Having an active failover plan in place is critical to meeting your top-priority availability requirements. One single point of failure for DNS means greater risk to your availability, regardless of the cause of that failure, and that's insufficient for a variety of reasons. If your authoritative DNS server fails, an active failover solution is required to support availability. With a failover in place, you can point activity to the backup servers in active failover mode. This means that your customers or business partners will have seamless uninterrupted service while your team works to address the source of the initial failure.

In the case of DNS, operators have an even more advanced option for DNS failover: the *ANYCAST* protocol. The ANYCAST protocol is used to automatically redirect traffic to the closest server depending on location, traffic, and destination health. Although ANYCAST is not specific to DNS, it has been adopted by many DNS providers and organizations with complex DNS infrastructure.

Performance and Responsiveness Assurance

Many of the other threats outlined in previous chapters can affect the performance and response times of your web applications at the DNS level, whether these apps are managed in-house or reside with your ISP or other source.

Reduced performance equates to reduced customer interaction and, ultimately, reduced revenue. Even though availability is the biggest priority, performance and responsiveness cannot be ignored.

In this realm, too, DNS infrastructure providers can offer your business benefits. If you are partnered with a full-service DNS infrastructure provider with resources in the cloud, you can move your DNS servers into your partner's cloud as needed to take advantage of its managed, redundant, available, and responsive DNS infrastructure. In this way, you can diminish the negative impact of security-related outages or disruptions to your own DNS servers. Because of the speed of propagation times, it is essential that any move of your DNS servers be carefully planned to assure a smooth transition.

CHAPTER 6

Managing Threats to Data Confidentiality and Integrity

Data is the lifeblood of your business. To ensure the confidentiality and integrity of that data means proactively managing and deterring the malicious bots and other threats that are bombarding your data-rich edge applications. In addition to malicious bots scraping your sites or committing fraud, these bots (and the attackers that have dominion over them) are fully capable of finding and exploiting vulnerabilities in your web applications and APIs. Most exploits come with remote code execution, allowing hackers to gain a foothold within your sites and applications. After an attacker gains a foothold, they're often fully capable of stealing your confidential data or affecting the integrity of your data by manipulating data fields. These footholds often have serious consequences and result in data theft and fraud.

Detecting and mitigating these malicious activities also helps maintain your brand reputation and preserve trust between your organization and partner organizations and customers. Today, bot management is top of the list when it comes to ensuring data confidentiality and integrity by eliminating malicious bots—first. Your broader application security focus should also include a Web Application Firewall (WAF), Application Programming Interface (API) security solutions, and malware protection. These technologies are designed to block malicious traffic beyond what is being propagated by bots alone.

Bot Management

Bot management solutions eliminate malicious bot traffic at the edge, where protection of data confidentiality and integrity are critical. The most effective bot-challenge approaches go beyond simple CAPTCHA programs or systems designed to distinguish human from machine input. A more sophisticated

approach is necessary to eliminate malicious bot traffic at the edge—and to stop bots from consuming your resources, bandwidth, and CPUs.

Web forms are an area where bots are particularly problematic. Bots use comment and other forms to spread malicious URLs, taking advantage of legitimate websites to point victims toward websites containing malware or other kinds of attacks.

The goal for bot management is to continuously obstruct malicious bots, without blocking good bot access or legitimate user traffic. Many bot management solutions sit at the network edge to identify and mitigate malicious bot traffic while enabling good bot traffic and customers to access your site and your applications sitting downstream.

A common bot management approach involves challenging bot traffic. In this scenario, activity is closely monitored to identify unfamiliar devices. For example, the bot management solution might issue a JavaScript challenge. In a JavaScript challenge, a bot manager would respond to an HTTP request with a JavaScript cookie providing instructions to the browser. Even though modern computers with browsers are able to run JavaScript, most bots don't have browsers and thus normally do not run JavaScript. The lack of response to the JavaScript command signals that the traffic is likely a malicious bot and the bot would thus fail the challenge and be blocked accordingly.

Another approach is to conduct a human interaction challenge via a quick applet set to see if there is any kind of human interaction, such as mouse movement or page scrolling. Device fingerprint and CAPTCHA challenges are also simple and commonly employed options for identifying and blocking malicious bots.

Cloud-Based WAF

Business websites receive a countless number of traffic requests. Many are legitimate requests coming from actual humans looking to access your website or download information from your website. However, requests can also be very malicious in nature, including application exploits like cross-site scripting (XSS), parameter tampering, or SQL injection. This malicious traffic can threaten the confidentiality and integrity of your data. Code injection attacks can result in your applications exposing significant portions of your data to attackers or allowing them access to values stored in data fields that can be changed.

As cloud adoption rates continue to increase, cloud-based WAFs can provide protection against application attacks, regardless of where sites are hosted. In fact, WAFs are required by the Payment Card Industry Data Security Standard (PCI DSS) as part of the set of security standards to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. Some cloud-based WAFs on the market are also useful for protect-

ing against bot traffic. Cloud-based WAFs use a combination of rules, threat intelligence, and heuristic analysis of traffic to detect and block malicious traffic at the edge to ensure that it never reaches the web applications.

Cloud-Based Malware Detection

The basic approach to pinpointing and eliminating malware is to run antivirus software. However, this comes at a cost. Your web servers and applications take a performance hit from the antivirus programs scanning uploads for malware. And at that point, the malware might have already made its way to your server, where your data confidentiality and integrity are at risk. A more proactive approach would be to choose a solution that sits out in front of the application in the cloud with a web application proxy that handles not only malware protection, but also API security along with bot management and WAF—so all the scanning is done before threats land on your actual web server.

Often, WAF providers include malware detection as part of a package of services. The cloud-based WAF provider will automatically scan all traffic destined for a web application and look for malicious files or malicious code that could be implanted on the web server. These WAF providers block and alert on the malicious files allowing security teams to further investigate the incident and take further action when necessary.

API Security

Although cloud-based WAFs provide good protection, they're most effective when paired with solutions that address web applications' vulnerabilities related to machine-to-machine communication, APIs, and mobile apps that still pose a threat to application security. For that reason, you should implement API security to validate mobile apps and ensure that an app has not been reverse engineered, allowing an attacker to manipulate it to hack into your applications. This, by its very nature, places your data and the integrity of that data at risk.

Emphasizing the high degree of threat here, the 2017 Open Web Application Security Project (OWASP) report of the top 10 most critical application security risks highlights the fact that many web applications and APIs do not properly protect sensitive data. Attackers can steal or modify weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data can be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with browsers.

In a recent Market Trends report, Gartner goes a step further, evolving WAFs into cloud-based web application and API protection (WAAP) solutions. WAAP services might include content distribution and acceleration; DDoS, bot mitigation; and protection for public-facing APIs, application delivery controllers

(ADC), and similar functions. These bundles are evolving into a consolidated solution and promise greater efficiency, potential cost savings, and enhanced visibility into an organization's application security posture.

CHAPTER 7

Web Application Security: Planning Your Next Move

For most small- to medium-sized enterprises, managing the products and resources for web application security is a challenge unto itself. You need to find, hire, and retain the right people, which is a challenge considering the significant skills shortage in the security realm. In many cases, you are balancing a long list of vendors, contracts, products, and specialists to handle your approach to web application security in pieces and parts.

Cutting through the hype, overcoming the fears of malicious bots and other attackers that make up the current threat landscape, and making effective decisions requires a comprehensive and prioritized strategy. Whatever your approach to web application security, consider following a plan for prioritizing the activities discussed in this report. Your plan should first concentrate on the following:

- Build on a strong foundation for DNS infrastructure availability
- Incorporate steps to protect against DDoS-induced outages
- Mitigate malicious bot threats
- Protect against an overabundance of application vulnerabilities
- Address API security issues
- Manage and mitigate malware risks

With a comprehensive plan for web application security in place, your business can move forward with confidence, knowing you are taking proactive steps to reduce risks and control the threats heading toward the edge.

The Benefits of Teaming with an Edge Services Partner

One approach for cloud-based web application security is to partner with an edge services partner that can proactively bolster your defensives before your web applications are threatened. Edge services can play a critical role in your approach to cloud adoption and successful cloud migration. The edge is where many critical decisions are made with respect to how your customers and users can securely get the content and services they're trying to reach in order to get work done and do business with your enterprise. Cloud service providers often manage hundreds or thousands of web applications, so their security teams have a great deal of experience in keeping web applications secure. They see a large number of threats that an individual organization might not see, and this collective insight and knowledge can be very beneficial to keeping all of their customers secure.

Options that partners can provide include the following:

- DNS infrastructure services as edge tools for maintaining sites, improving response time, more efficiently directing traffic, and finding healthy endpoints and paths to those endpoints
- Security services that preemptively identify, throttle, and thwart malicious attacks of every kind at the pre-edge of the cloud before it can reach your own sites

DNS is a prime example of an edge service that is underutilized today as an edge tool for more efficiently directing traffic and finding healthy endpoints and healthy paths to those endpoints.

What a Web Application Security Suite Looks Like

A comprehensive application security suite can be a multitenant, hosted platform with globally distributed point of presence (PoP) and geographically dispersed attack mitigation centers. It also can include security operation centers focused on monitoring and mitigating attacks 24/7. Proprietary machine learning algorithms, coupled with threat intelligence and big data analysis, reside at the core. Specific elements include the following:

- Highly available DNS services
- Hardened DDoS protection and mitigation
- Advanced malicious bot detection and mitigation solutions
- WAF AI-driven web application firewall
- Advanced API protection with token challenges for web and mobile

- Cloud-based malware protection for websites offered as a 24/7 managed cybersecurity service

About the Authors

Stephen Gates, edge security evangelist and SME at Oracle Dyn, brings more than 25 years of computer networking and information security experience to his role at Oracle Dyn. He helps service providers, hosting providers, and enterprises solve their DDoS and web application security problems. He has an extensive background in the deployment and implementation of on-premises and next-generation cloud security solutions.

He has a Master's Degree in Information Security and Technology Management and is in demand as a thought leader and presenter at RSA, Black Hat, SecureWorld, SANs, Infosecurity, IANS, ISSA, InfraGard, ISACA, among other industry events.

Allan Liska has more than 15 years' experience in the world of cybersecurity. Mr. Liska has worked both as a security practitioner and an ethical hacker, so he is familiar with both sides of the security aisle and, through his work at Symantec and iSIGHT Partners, has helped countless organizations improve their security posture using more effective intelligence.

In addition to security experience, Liska also authored the books *The Practice of Network Security* (Pearson) and *Building an Intelligence-Led Security Program* (Syngress), coauthored the book *DNS Security* (Syngress), and contributed the security-focused chapters to *The Apache Administrators Handbook* (Pearson).