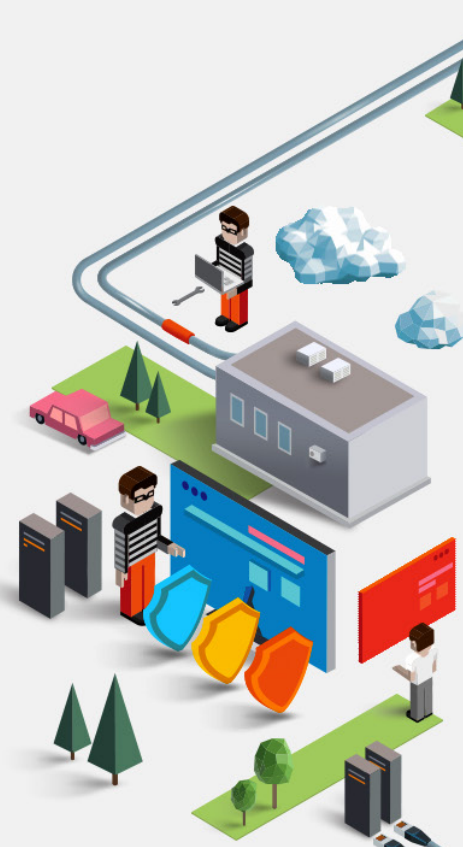

HOW TO REDUCE CYBER RISKS

– A PRACTICAL GUIDE

Akamai
FASTER FORWARD

TABLE OF CONTENTS

FOREWORD

People, processes, and technology are the three key components of all sound security strategies. This whitepaper not only highlights the high-risk areas that organizations should prioritize to secure, but also offers corresponding recommendations from a cyber-risk perspective.

This is highly relevant today when most enterprise security breaches are associated with legitimate users—either unintended actions of employees unfamiliar with good cybersecurity practices, or compromised legitimate accounts providing malicious users access to sensitive data. The issue is compounded by the global shortage of cybersecurity professionals and the propensity of organizations to ignore the importance of proper security practices.

The Ponemon Institute's 2017 report *Trends in the Cost of Web Application & Denial of Service Attacks* reveals that, in 2017,companies are faced with higher frequency of attacks, and mitigation efforts are taking longer. Revenue losses due to customer-facing services being unavailable have increased from USD 517.6 million in 2015 to USD 731.6 million in 2017.

This whitepaper examines the current security landscape under five domains: Governance, Risk, and Compliance (GRC); Domain Name System (DNS); Application and Network Layer Security; Bots; and Identity and Access Management.

We are pleased to share this handbook of best security practices in critical areas of cybersecurity. The ideas presented herein reflect technologies, vulnerabilities, and solutions that have come into focus over the last 12 months.

CHAPTER 1: GOVERNANCE, REGULATION, AND COMPLIANCE

Given the divergence and complexity of modern enterprise technology, incorporating a well-defined framework involving all stakeholders is the need of the hour.

In today's environment, enterprises must combat not only external malicious attacks, but also threats posed by unintended or unauthorized actions of end users. The risk is amplified when organizations do not have adequate cybersecurity guidelines in place. This can be attributed to a lack of common, proven practices and guidelines developed for the IT workforce.

Security standards are absolutely necessary for any company that wants to harness and capitalize on IT for business operations. Contrary to popular belief, cyber criminals do not target only those companies in the finance or tech sectors.

All companies regardless of size, across all verticals are at risk. Brian Krebs, a respected cybersecurity journalist, pointed out the value of a single PC that is hacked as well as the notion that all businesses, no matter how small, are of value to attackers.

THE NEED FOR SOUND FRAMEWORKS AND STANDARDS

What makes frameworks and standards even more relevant in today's scenario are the challenges the enterprise faces with respect to complexity, consistency, and policy.

• Increasing Complexity in IT

Supporting the current IT infrastructure and catering to modern technologies is far more difficult than it was a decade ago. While supporting the hardware side of IT has become easier, supporting the rest of the IT infrastructure is much more difficult today. Given the situation, it's essential for the management and users to come to terms with the difficulties in keeping IT operations running smoothly and securely.

• Consistency Takes a Hit

Without a high-level security framework, the onus falls upon individual security professionals, based on their unique experiences. The results are variable and often undesirable.

• Policies Amiss

Today, most organizations still do not have a well-defined security policy. Where there is a comprehensive security policy, it is not

well-communicated or enforced, because it lacks alignment with best practices and regulatory requirements. The policies tend to address security issues at a micro-level, so it is difficult for professionals to enforce security guidelines. Having a well-defined security policy does not ensure complete protection, though. The organization also needs a well-trained team, consisting of all stakeholders, to introduce and enforce security policies.

Multiple Compliance Regulations

Sensitive data and processes and the systems that support them are becoming subject to oversight by various regulators in order to minimize incidents. One benefit of security frameworks is that they can incorporate multiple compliance standards and help organizations deal with new requirements.

WHAT FRAMEWORKS BRING TO THE TABLE

A robust framework is essential to constantly refining and enforcing IT security systems. A well-defined framework can only be implemented with the involvement of all stakeholders (rather than via a silo initiative launched by the Chief Information Security Officer). Such frameworks must be continually revised and refined in order to meet the changing needs of security landscape. Yet, most organizations today do not have such robust, effective frameworks.

An information security framework, as defined by security expert Joseph Granneman[1], "is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an enterprise environment".

The framework forms just the blueprint, i.e. the essential guide. Security solutions must be built upon the framework according to a company's changing business models and IT ecosystems. The framework enables enterprises to build bespoke security solutions with agility, speed and efficiency.

[1]Granneman, 2013. IT security frameworks and standards: Choosing the right one. Retrieved from Techtarget.com.

WHY STANDARDS ARE IMPORTANT

Cybersecurity standards have existed over several decades. Users and providers have collaborated in many forums, both domestic and international, to effect necessary capabilities, policies, and practices—generally emerging from work at the Stanford Consortium for Research on Information Security and Policy in the 1990s.

Here's a look at the most popular and widely accepted security frameworks in the industry today:

COBIT

Control Objectives for Information and Related Technology (COBIT). A framework developed by ISACA, for performance, governance and risk management of enterprise IT. COBIT 5 is the latest edition.

The ISO 27000 Series

An outcome of the joint effort of the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). Part of the larger ISO standards family, it has certification practices similar to the more popular ISO standards. The ISO 27000 series provides broad frameworks suitable for organizations of all sizes and levels of complexity.

CCM

Developed by the Cloud Security Alliance, the Cloud Controls Matrix is specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall risk of a cloud provider. By referencing this framework, prospective adopters gain a deeper insight into how cloud solution providers secure their infrastructure and processes that underlie their cloud solution offerings, enabling a comparison and evaluation process.

NIST Cybersecurity Framework

Developed by the U.S. National Institute of Standards and Technology (NIST), this is a government-ordered cyber security framework that can be used by a wide range of private sector organizations in order to assess and improve their ability to prevent, detect, and respond to cyber attacks.

The key benefit of these frameworks is that there are several overlapping areas with regulatory requirements. Hence, organizations which adopt frameworks can potentially lessen the efforts required to comply with new regulations.

Adherence to a particular IT security framework can be driven by multiple factors. One of the deciding factors is the type of industry along with the applicable compliance and regulatory requirements. For instance, publicly traded companies will in all probability follow COBIT, while the ISO 27000 series, as an all-encompassing framework, can find applicability across all industries.

The selection and implementation of the appropriate frameworks and standards is one of the most important responsibilities and tasks of the present day Chief Information Security Officer.

CHAPTER 2: IMPORTANCE OF SAFEGUARDING DNS

Authoritative DNS and Recursive DNS are key to the very existence of the World Wide Web. Yet, Domain Name Systems remain one of the most commonly ignored areas despite being a high-risk and vital component of Internet functionality.

Most organizations have multiple layers of security to protect their IT systems, yet, Domain Name Systems (DNS) are a common blind spot. The inherently open and trusting nature of DNS makes it a favorite target of attackers.

The Mirai botnet DDoS attacks (Distributed Denial of Service) on a managed DNS infrastructure in October 2016 highlighted the importance of DNS services.

The attack brought down many businesses that depended on several DNS and hosting providers thereby demonstrating how prohibitive the business costs of DNS attacks can be[2] with outages lasting the greater part of a day.

The *Akamai SOTI (State of the Internet) Q1 2017* security report recommends all DNS servers responding for a targeted domain to be protected, considering the risk posed by the Mirai DNS query flood attack. The report states that while mega or bigger attacks have reduced in frequency, smaller attacks continue to increase in frequency. However, mega attacks will have an outsized impact on DDoS trends in the coming years.

This chapter discusses various kinds of attacks on Authoritative and Recursive DNS and best practices with regards to DNS services.

First let's examine the key functions that DNS performs, and how DNS works.

[2]**Bolstridge,** 2016. Dyn DDoS Attack: Wide-Spread Impact Across the Financial Services Industry (Part 1). Retrieved from Akamai.com.

UNDERSTANDING DNS

The Internet operates through a worldwide, distributed directory service called the Domain Name System (DNS), which maps human-friendly domain names (words or word combinations, such as www.google.com) to IP addresses that are numerical sequences separated by dots (like 66.94.234.13). Thus, users are saved the hassle of having to remember strings of numbers for the websites they want to access. With the growing adoption of IPv6, which supports much longer 128-bit addresses, DNS becomes even more important.

The Internet Corporation for Assigned Names and Numbers (ICANN), estimates that there are around 30 to 50 million existing DNS servers. For global scaling, the DNS was built as a cascading multi-level reference network.

A simplified representation can be as follows:

- The root servers are at the top in the hierarchy, and is represented by a dot at the end of the URL. This is normally not displayed with the URL.
- Next comes Top Level Domains (TLD) like .com, .gov, and .org, and sometimes regional domains like .br, .in, .fr.
- Next level is domain names, and further down comes sub-domains.
- Each level is separated by a dot in the URL.

An illustrative representation is as below:

www.aboutpage.companydomain.com Root

Sub-Domain | Second-level Domain | Top-level Domain

HOW DNS WORKS

Authoritative DNS controls individual domains; but for all practical purposes, individual user queries go to the recursive DNS (rDNS).

When somebody wants to access a website, they type in the human-friendly domain name into the browser. The browser looks up the local cache, and if it finds the information, it opens connection to the requested server. If it doesn't find the mapping in the local cache, it sends a query to the rDNS, which looks up its cache. The rDNS could be hosted at your local Internet Service Provider (ISP) or your third-party DNS provider. If the rDNS cache doesn't have enough information, then it recurses to the Authoritative DNS servers, root servers and TLDs to gather the info.

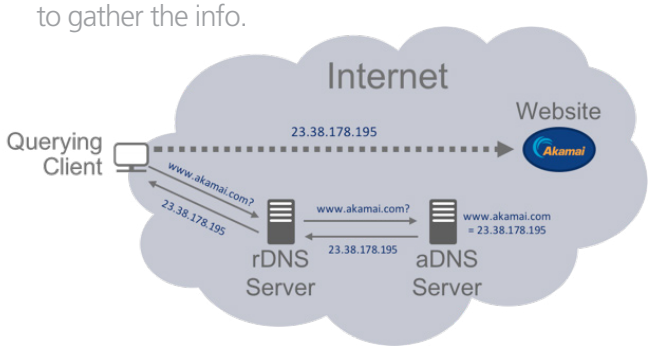

Image Source: Akamai

WHY IS DNS PRONE TO ATTACKS?

Despite having multiple layers of security, most organizations underestimate the security needs of DNS. DNS is typically considered a directory service acting with a high trust factor. It considers almost every query as a genuine query, and responds with genuine information. The DNS does not have a built-in mechanism for assessing whether a user's requested website is "good" or "bad." While this "never questioning" means that DNS operates amazingly quickly and reliably, the inherent trust adds a lot of vulnerability to the system.

Unless organizations add automated solutions that can identify malicious locations, they won't be able to control queries across their DNS infrastructure. Manually reviewing each request put forward by recursive DNS servers is time-consuming and inefficient due to the huge number of requests each second. Furthermore, maintaining an automated warning system is not, in itself, enough; the address databases must be constantly updated to remain current.

Most commonly, DNS attacks take place via malware that ends up on the end user device. The "end user" could also be a connected smart device, such as a light bulb or thermostat, or an employee or visitor's laptop. Phishing emails or targeted spear-phishing emails that lead users to open malicious websites are common hooks used by hackers.

An attack on an authoritative DNS server (not just a recursive DNS server) actually gives the hacker the power to alter the DNS settings for a given domain name, which can lead to redirection of traffic. The worst situation occurs when the attacker redirects the emails or other web services provided by the company or organization. This essentially means that the hacker can communicate with the users on the company's behalf.

ATTACK TACTICS

Malicious agents use multiple tactics to infest machines. The most common ones are:

Targeted Threat Delivery

This involves phishing through attachments or links—via email, ad links, USB keys, etc.

Command and Control (CnC or C2):

Once the communication is established, malicious agents use the channel for further malicious activity like exfiltration of data, remotely controlling the machines, and infecting more network-connected machines, thus developing a botnet (network of bots).

Domain-Generation Algorithms (DGA)

To evade detection by security methods, hackers use domain-generation algorithms that can regenerate domains using different algorithms. DGA domains are numerous; they do not live long enough to be detected and blacklisted.

Fast Fluxing

Attackers set up constantly changing servers, adding redundancy layers in front of their actual CnC server. Thus, they bypass IP-based firewall blocks.

Data Exfiltration

Malicious CnC servers use DNS port 53 of compromised machines to exfiltrate data through DNS tunneling.

SAFEGUARDING AGAINST DNS VULNERABILITIES: BE VIGILANT, ALWAYS

The 2016 Mirai botnet DDoS attack showed companies that the DNS attack vector should be taken more seriously. The attacks also made organizations realize that with a growing network of devices, it is crucial to have all of them protected.

Organizations should always have their recursive DNS and authoritative DNS on two separate servers. If an attacker seizes control of the authoritative DNS server, and if the same server is also running their recursive DNS, the attacker gains control over both the incoming requests and the outgoing data, giving the attacker virtually complete control over all of an organization's web traffic. Also, in case of a large number of requests, if hosted on the same server, both incoming and outgoing connections will be disrupted.

Unprotected rDNS is a serious vulnerability, particularly with the rapid adoption of cloud applications and storage/archival solutions.

The best method for safeguarding against targeted DNS threats is to protect the DNS infrastructure within controllable environments.

BEST PRACTICES FOR PROTECTING DNS INFRASTRUCTURE

- Update the software regularly; always have the latest version
- Have strong passwords and IP-based ACLs
- Always have authoritative DNS and recursive DNS on two separate servers
- Ensure that the authoritative DNS is hosted on a trusted authority
- Get a secondary DNS provider to ensure availability
- Understand how your DNS providers protect themselves from DDoS attacks. Ask for specific data on geography, capacity and DDoS measures, as well as the amount of attack traffic that can take place
- Understand what happens when your assets are under attack: Will your provider mitigate or simply "black hole" your IPs?
- Ensure that the authoritative DNS filters rDNS queries as per the company's policies
- Prevent end users from installing unauthorised VPNs
- Allow only DNS queries from local DNS servers to external DNS servers
- Lock down employee ability to change DNS settings
- Use a firewall to restrict outbound traffic on DNS port 53 from your internal DNS server
- Allow only traffic from trusted sources, to trusted destinations
- Monitor DNS logs for suspicious patterns. Watch out for DNS queries for domains that are infrequently accessed (long-tail log queries), non-standard naming conventions, and queries outside of normal working hours

CHAPTER 3: APPLICATION AND NETWORK LAYER PROTECTION

The rapid adoption of web and mobile applications introduces new challenges in securing the enterprise and its customers. How prepared are you to protect your application and network against the latest threats?

According to SANS Institute's *2017 Threat Landscape Survey,* DDoS attacks and Application Vulnerabilities are among the top 4 vectors and threats to organisations.

The Ponemon Institute's 2017 report *Trends in the Cost of Web Application & Denial of Service Attacks* revealed that the average cost of DoS attacks and web application attacks have risen to USD 1.5 million and USD 3.7 million respectively over the last 12 months. Companies experience an average of approximately 5 DDoS attacks, and system downtime due to DoS attacks increased from an average of 9 hours to 11 hours.

Over 80 percent of companies surveyed report that their web applications have been compromised, and almost half report that, due to the complexity involved, fixing a single web application vulnerability typically requires weeks of effort.

Among some organizations, there is a misconception that, by hosting applications on cloud service providers, they gain protection by default against DDoS, Application Layer Attacks, and attacks on their APIs. This is not usually the case.

To effectively protect any organization's web properties, a security architecture that consists of both network and application defences is required. This chapter examines the recent advances in cloud-based Distributed Denial of Service (DDoS) protection and Web Application Firewall (WAF), both of which provide significant augmentation to any existing on-premise solutions.

CHALLENGES IN WEB APPLICATION AND API SECURITY MITIGATION

There are several core challenges associated with providing API protection and handling web application vulnerabilities:

1. Web applications are available 24/7 to attackers. Attackers have all the time that they need to search for and exploit application vulnerabilities.

2. Software of unknown pedigree. Software that is custom-developed but contains libraries and dependencies on other software which is not known to the organization.

3. Vendor support is unavailable. Some applications have been abandoned by their developer for a variety of reasons and security updates are not available for them.

4. The delay between the discovery of an application vulnerability and the release of a software update to address the vulnerability. COTS (Commercial Off the Shelf) solutions not only depend on vendors and upstream open-source projects to release software updates/patches but also require additional days for regression testing to ensure that the software update is compatible and does not interact negatively with their environment.

5. Attacks that use Zero Day vulnerabilities. Exploits for vulnerabilities that are not publicly known.

6. Attacks directed against APIs for which there is not a large body of experience and best practices for protection.

ADDRESSING THE CHALLENGES

The abovementioned challenges can be addressed with WAFs that can provide both network and application layer protection.

WAFs are recommended to:

- Be configured to deny all incoming traffic on all UDP/TCP ports, apart from the protocols that are explicitly required, e.g. HTTP and HTTPS.
- Use both wide protections against classes of attacks and narrow protections against vulnerabilities in specific versions of applications.

WEB APPLICATION FIREWALL CORE REQUIREMENTS

The following is a list of critical functionalities that an effective WAF should possess:

- **API and Application Vulnerability Protection**

Capability to protect against known attacks against APIs and application vulnerabilities. Ability to write custom rules in order to tune existing rules or to respond to new vulnerabilities as a virtual patch.

- **API Inspection and Protection**

Core capability to inspect and manage JSON, XML requests and API parameters including rate controls.

- **Cloud for Scale**

Cloud-based WAFs automatically load balance and allocate all traffic to multiple WAF servers, and only relevant traffic (e.g., HTTP) is passed to the Origin Server (customer's web server where the application resides). This is especially significant for applications with users who are geographically distributed.

- **Low False Negative Rate**

This rate is a measure of malicious requests that are classified inaccurately as legitimate requests and, as a result, make it to the web application or website. A false negative results in an attack that is not detected and blocked, instead arriving at its target, potentially causing an impact.

- **Low False Positive Rate**

This rate is a measure of legitimate requests that are classified inaccurately as malicious requests and blocked. A false positive results in a legitimate user being denied access to the web application and significantly impacts customer satisfaction.

- **Visibility into New Attacks**

This capability is a function of how much Internet traffic is being monitored by the solution vendor, data on attack patterns, attack payloads and attack characteristics. A high degree of visibility is essential for effective protection against new, developing attacks.

- **Intelligence Framework**

The capability of WAF vendors to analyse collected data and the structured process of developing actionable intelligence, e.g., intelligence to fine-tune WAF rules and to provide dynamic protection against new emerging attack trends.

- **Client IP Reputation**

WAF solutions should possess a database that tracks source IP addresses and assigns a reputation score based on past behaviour, such as participation in DDoS attacks, web attacks, and scanning activities, allowing for proactive traffic blocking.

- **Multi-Vector Attack Protection**

The trend of multi-vector attack methodologies is accelerating. For example, while a very visible and noisy DDoS attack is in progress, a stealthy web application attack is launched to steal data.

- **Integration with Existing Tools and Processes**

Can the WAF be supported by the security operations centre and other security teams? Can the WAF be monitored via a security incident and event-monitoring system?

- **Scale to Run Sufficient Rules**

Enabling a large amount of WAF rules without impacting the speed of throughout requires significant up-scaling of most hardware WAFs. Cloud-based WAFs have an advantage here with the ability to dynamically add computing power to adjust to load.

- **HTTP Layer Rate Controls**

The ability to detect a wide variety of abusive behaviors such as vulnerability scanners, scrapers, and application-layer denial of service by doing rate accounting.

DISTRIBUTED DENIAL-OF-SERVICE (DDOS) MITIGATION

Any organisation that has an Internet presence needs to be concerned with the threat of DDoS.

Any components of Internet-facing systems, including websites (origin servers), applications, APIs, DNS services, and even data centres and network infrastructure are possible targets.

Examining Distributed Denial of Service (DDoS) attack models, the concept is simple: Attacks are looking to deny legitimate users access or to force the target to reduce the number of controls that they employ in their network or WAF.

Over the history of the Internet, we have seen a wide variety of techniques and platforms used to conduct DDoS attacks. The first Denial of Service (DOS) attacks were single machines sending a large amount of ICMP ping requests. Attackers switched to "booters," which are minimalistic web applications that send attack traffic from webservers that have higher bandwidth. Then, malware writers used their tools to join infected desktops and laptops together into a botnet as a platform to launch attacks. The concept of booters and botnets was taken to the next level in 2012 and 2013 with the advent of "Brobot," which infected a large number of outdated content management servers and joined them together into a botnet. Around 2013 and 2014, attackers discovered a new technique called reflection or amplification, in which they pretend to be the victim and request data from a service. The response data overwhelms the victim.

The threat environment has changed over the past 2 years with the rapid rise of Internet of Things (IoT) devices such as web cameras, web video recorders, routers, and other Internet-connected devices which have played significant roles in massive DDoS attacks.

IoT devices are a source of massive botnet resources. Mirai malware and its progeny are **evolving and spreading**, and **older malware is being updated** to take advantage of the proliferation of insecure IoT devices.

In all likelihood, DDoS attacks will increase in size and frequency. We anticipate a higher frequency of smaller-scale attacks, but the largest attacks will almost certainly continue to grow; at the beginning of 2017, the median attack size was just over 500 Mbps. Per Akamai's State of the *Internet Security report Q1 2017,* we expect mega-attacks of over 100 Gbps to continue to have an outsized impact on DDoS trends in the coming years.

Even a typical DDoS attack of less than 4 Gbps can cause denial of service at an unprotected site or one that relies upon on-premise DDoS mitigation hardware. Especially if we consider that many businesses lease uplinks to the Internet in the range of 1–2 Gbps, any attack exceeding 1 Gbps could be large enough to cause an impact and is more than capable of taking the average unprotected business offline.

The current best practice approach is to look at cloud DDoS mitigation solutions to augment existing on-premise solutions, and review the readiness of your DDoS protection plan and process.

BUILDING AND MAINTAINING A DDOS PROTECTION PLAN

These are eight key excerpts from Akamai's "8 Steps to a DDoS Mitigation Plan" whitepaper:

1. Anticipate single points of failure—from your DNS servers to APIs.

2. Verify your ISP's capability and duty of care with regards to DDoS protection.

   - For example, does your ISP "blackhole" traffic to a customer site under DDoS attack?
   - If so, how long before normal traffic resumes?
   - Do you know the point of contact at your ISP?

3. Don't overestimate your infrastructure and consider your tolerance for risk. A typical DDoS attack is less than 4 Gbps today but peak DDoS traffic can exceed 600 Gbps.

4. Identify critical areas to protect, and estimate the business impact of its loss, to build your business case.

   - Is there a risk model deployed and how do you calculate potential losses?

5. Ascertain acceptable time-to-mitigation.

   - Do you need something that is always on or only activated on-demand?

6. Deploy a DDoS protection service *before* you need it.

7. Develop a DDoS response runbook which contains incident response processes, escalation paths, and points of contact.

8. Trial run your DDoS runbook to ensure operational readiness.

DDOS MITIGATION CORE CAPABILITIES

The following is a list of critical criteria to consider when evaluating DDoS mitigation solutions:

- **Solution Architecture**

Consider the choice of architecture. Cloud-based DDoS mitigation solutions will provide much more scalability versus on-premise solutions, and you can augment an on-premise solution with a cloud-based solution without replacing existing equipment.

- **On-Premise vs Cloud Attack Bandwidth Capacity**

Consider the bandwidth that is available at your data centres and their connections to the Internet. Akamai has seen attack bandwidths that exceed 100 Gbps. Even an average size attack of 5 Gbps can overwhelm most network pipes and on-premise appliance-based solutions. In Asia, the average web hosting environment has 1-2 Gbps of Internet capacity and is at 80% utilization. Even with overprovisioning to 50% utilization, a DDoS attack of 1 Gbps is sufficient to cause a service impact.

- **CDN Capacity vs DDoS Scrubbing Capacity**

CDN service providers might claim very high top-line capacity numbers for their networks, but ask specifically about their capacity to deal with DDoS attacks. For example, 50 Gbps of overall capacity might sound high, but if 80% is already used for CDN traffic, less than 10 Gbps is available to scrub and mitigate attack traffic.

- **Point of Presence**

How many Points of Presence (PoPs) does the DDoS mitigation vendor have, what is the average size of each PoP, and are they close to your users and hosting centre? This is critical as some pure-play DDoS mitigation vendors only have a small amount of scrubbing centres that are only useable in a specific geographic area. For scrubbing centres, a widely-dispersed geographical presence with in-region redundancy, always-on traffic, low latency, and high availability is critical. On the CDN side, some vendors may have only hundreds of servers, while others have hundreds of thousands of servers.

- **Security Operations Centre Coverage**

Number of SOC locations and quantity of staff globally where trained and on-shift security analysts can help to manage the incident response for each DDoS attack. Ideally, the DDoS mitigation provider should be able to provide in-country, in-language 24/7 support to their customer and have a redundant SOC to shift operations to in case the primary SOC becomes unavailable. Good vendors offer a Service-Level Agreement on their SOC response time.

- **Throughput and Round-Trip Latency**

DDoS scrubbing centres that are minimally provisioned with bandwidth do not have enough capacity to mitigate multiple DDoS attacks and drastically oversubscribe their capabilities. These providers are unable to mitigate multiple simultaneous attacks

against their customers and their scrubbing centres are susceptible to cascade failures in some scenarios. Some DDoS mitigation providers and CDNs purchase bandwidth from cheaper tier 3-4 ISPs which impacts their customer traffic when the ISP has stability issues because they, in turn, have oversubscribed bandwidth. As a customer, you should understand the latency impact of each DDoS scrubbing solution and its impact on user experience. Several methods exist to reduce the latency effects of a scrubbing solution such as layering the solution with a CDN, using an in-country BGP community for domestic users, or using a fibre connection or MPLS from the scrubbing centre to your datacentre.

- **Client IP Reputation**

DDoS solutions should block sources known to participate in DDoS attacks. Considerations would be whether the database is updated and owned by the DDoS vendor.

CHAPTER 4:
BAD BOTS: DIGITAL TOOLS OF CYBER CRIME

More than 60 percent of a website's traffic may be generated by bots. Good bots are deployed for a variety of valuable purposes; bad bots, for malicious activities. Outages can do immense damage to an enterprise, potentially maligning the brand image and adding up to huge revenue losses.

WHAT IS A BOT?

A bot is a computer program that functions to automate repetitive tasks over the Internet. Bots are closely linked to DDoS attack but bots are not always bad. Some bots are beneficial to the organization and should be allowed, for example, search engine crawlers. The key to successful bot management is having a flexible framework for detection, categorization, reporting and management (mitigation and blocking).

For the purpose of this guide, we will focus on how to effectively manage bots, both beneficial and malicious.

Based on analysis of traffic across the Akamai Intelligent Platform™, more than 60 percent of a website's traffic may be generated by **bots**[3] . Broadly, they are differentiated as either good or bad. Good or white bots are deployed for a variety of valuable purposes like web crawling by search engines, interacting with business partners or customers, and more. A bad bot, on the other hand, is used for fraudulent or malicious activities and is commonly a device that have been hijacked without the knowledge of its owners, e.g., IP camera, Internet routers, set-top boxes and IoT devices.

In the sections below, we will try to understand the nature, activity and impact of bots, and see how they can be detected and managed.

[3]Akamai, 2016. Akamai Revolutionizes Bot Management Industry-first Web Security Technology – Akamai Bot Manager – Designed to Allow True Management of Bots vs. Detection and Blocking Only. Retrieved from Akamai.com.

MALICIOUS ACTIVITIES OPERATED THROUGH BOTNETS – AND THEIR BUSINESS IMPACT

The programmability and autonomy of bots make them popular tools for carrying out malicious activities, says Frost & Sullivan[4]. From performing distributed denial of service (DDoS) attacks to spamming inboxes, bots are considered one of the most pervasive malware on the internet.

HERE ARE THE MOST COMMON MALICIOUS ACTIVITIES EXECUTED USING BOTNETS:

- **Content and Price Scraping**

Loss of revenue when competitor scrapes pricing data or content to gain a competitive edge. In some cases, competitors can determine the rate of inventory turnover for products and can use this to adjust their selling strategy. However, some price-scraping activity can also originate from legitimate price comparison websites and may not be detrimental to the business.

- **Inventory Grabbing**

Especially prevalent for scarce goods such as limited-edition items, hotel and flight tickets. Bots purchasing limited inventory in bulk to resell at a marked-up price. Some third-party sites request flight-ticket pricing aggressively and unnecessarily.

- **Identity Theft and Credential Stuffing**

Bots perform credential stuffing to validate user information leaked from data breaches for resale on the dark Web for account takeover and fraud.

- **Advertisement Click Fraud**

Click fraud uses bots to make it appear that online advertisements have been clicked by legitimate users, falsely inflating reported click-through rates and triggering payments for ads that were never viewed. This leads to loss of trust and revenue from advertisers.

- **Distributed Denial of Service attacks (DDoS)**

Bots carry out attacks on websites and applications, with the intention of blocking access for legitimate users, resulting in revenue losses and reputational damage.

A HIGHLIGHT ON THE DAMAGES CAUSED BY CREDENTIAL STUFFING

Ponemon Institute's report *The Cost of Credential Stuffing* validates that companies incur significant financial losses in the form of application downtime and also losses in their customer base. Companies estimate that every 1 percent of compromised accounts involved in fraudulent activities translates into a loss of USD 500,000.

Credential stuffing attacks are viewed by over 80 percent of companies surveyed as being difficult to detect, primarily because of the challenge in distinguishing between legitimate and malicious users.

[4] Advancing to Bot Management and Security: Credential Stuffing Becomes Top Concern – Frost & Sullivan

DETECTING AND CATEGORIZING BOTS

It is critical to categorize the various good and bad bots active on any network. Multiple bots that act similarly and have a similar impact on the web infrastructure are categorized as a group. This gives an organization the capability to make specific action policies for each category of bots according to its impact on site performance.

A signature-based approach is one way to categorize bots. Under this method, bots can be detected and classified by analyzing recognizable identifiers. They are categorized on the basis of one signature or any combination of multiple signatures like request header content, request header order, origin response header content, user agent, cookie name and content, IPs, geography, AS number and AS company name.

Apart from the signature-based approach, characteristics of the network traffic can also be analyzed for identifying and categorizing bots. This includes looking for any anomalous behavior like a sudden increase in traffic volume, high network latency, passage of traffic through unusual ports, or other irregular system behaviors.

As bots grow increasingly sophisticated in order to mimic real users to avoid detection, it is important to include user behavior analysis, browser fingerprinting, HTTP anomaly detection, high request rate, and workflow validation, to detect traffic from unknown bots ranging from simple scripts to automated and headless browsers.

Reputation data and risk score, generated by machine learning, based on a bot's recent behavior on its entire customer network provides an added advantage.

THE SOPHISTICATED BOTS

The increasing sophistication of bots poses a key challenge to detecting and mitigating attacks. As bots become more advanced, they can mimic human behavior, making them very difficult to track. These "Advanced Persistent Bots" (APBs) can perform advanced web functions such as loading JavaScript, performing browser automation, holding cookies, and continually shifting their IP addresses to avoid detection.

In the 2017 *Online Trust Audit & Honor Roll* report by Online Trust Alliance conducted on the top 1,000 websites in retail, banking, consumer services, government, and media, showed that 95% of websites are defenseless against advanced bots.

EFFECTIVE BOT MANAGEMENT

Appropriate management policies should be applied for all identified known and unknown bots. Traditional IP blocking is not effective, as the bot operator will detect the block, change the IP and restart the bot invasion. Instead, these management policies can be applied:

- **Rate-based actions to delay or slow the response** to manage partner bots or other good bots that might otherwise cause performance degradation.
- **Serve alternate content,** for example, an alternative page that looks exactly like the real page but with higher prices to a competitor's scraper.
- **Serve alternative origin** where specific servers are set up for bot traffic while reserving high-performance servers for legitimate users.
- **Serve cached content** to minimize impact on site performance. This is a possible strategy if a CDN is used.
- **Alert** if the organization simply wants to be alerted to bot traffic.

The goal of enterprise IT should be to never accidentally block legitimate traffic, including search engine crawlers, customers, business partners and other legitimate users. Preferential treatment such as setting aside separate high-performance servers for these visitors can help improve their experience.

It is also vital to continuously monitor and re-evaluate known bots, as their capabilities and nature can change over time.

A bot-management solution which applies real-time analytics with machine learning and behavioral modeling in additional to static rules is necessary to manage bots effectively. Given the prevalence and rapid rise of bot-related attacks, we recommend including bot management a part of an organization's web security strategy.

CHAPTER 5: A NEW ACCESS AND IDENTITY MODEL FOR THE DIGITAL ENTERPRISE

With newer technologies like mobility taking precedence in the enterprise, the methods of accessing, storing and sharing of critical business data have evolved. Successful transformation will require the evolution of traditional network, enterprise network, security and application delivery architectures.

The almost universally adopted multiplayer perimeter security architecture has a very simple concept of security access and control. The Internet is full of threats, and firewalls are implemented to protect the enterprise's assets – so within the confines of the perimeter, no threats can exist.

The rise of new drivers – DevOps initiatives, multi-cloud strategy, SaaSification of IT applications, mobility-first strategy and the importance of third-party ecosystems – have resulted in requirements to open up access to applications to remote users, partners and third-party applications.

The increasing amount of business-critical information now residing and accessible via mobile devices and cloud means that businesses today can no longer rely on the traditional perimeter or DMZ approach to secure their data and infrastructure – nor can they rely on the assumption that all devices within the perimeter can be trusted.

A new "zero-trust" approach to identity and access is critical to securing today's digital enterprises, where there is "no more inside" anymore.

Hence, instead of using multiple technologies to safeguard data, it is essential to adopt a cloud perimeter or "Zero Trust" model that, in essence, boils down simply to the user and the application the user needs to access. The cloud perimeter uses the Internet as its core network, can be consumed as a service in the cloud, and embraces "verify and never trust" (i.e., zero trust) as a core principle.

If more than 40% of breaches come from authorized users accessing unauthorized systems, why use the verify = trusted model?

FIVE KEY STEPS TO STARTING YOUR CLOUD PERIMETER JOURNEY

1 Establish Effective Monitoring and Reporting

Even with the right systems in place, a key component of zero trust is just that: Trust no one. From access to applications and data to malicious and unacceptable content to application performance, everything should be monitored, logged, and reported on.

With a cloud perimeter, you can export data that enables you to not only look at positive and negative security models in your own SIEM tools, but also start to leverage built-in predictive and behavioral analytics. For example, is that 3 a.m. login really a person, or is it a bot? What about traffic leaving the enterprise and connecting to a domain on the Internet? Is it a malware trying to contact its command and control server, an IoT device performing a legitimate connection (e.g., a copier letting the supplier know it is out of laser toner), or just an employee trying to access a resource on the Internet?

Full visibility is the first step to effectively applying security policy and enforcing compliance. Adopting a cloud perimeter helps to centralize security policy definition but allows distributed policy enforcement.

2 Establish New User Access Policies

Pivot from the common security mantra of "trust but verify" to "verify and never trust" in the new threat landscape. Use the concept of least privilege as a guide: Most users only need access to the applications that enable them to successfully do their jobs. Look for a solution that enables you to provide access to all applications, regardless of where they are hosted, and provides browser-based, application-specific user access. With this, the user should get authorized, secure access to specific applications – but nothing else on the network. It is also key to hide private enterprise applications and infrastructure from the Internet, which minimizes the attack surface by making enterprise infrastructure invisible. Threat actors can't attack what they can't see.

Here are some points to consider:

- How do you provide access to external third-party contractors?
- How often do your users work remotely?
- How do you enforce security policies for end-user devices even if they are off line?
- Should users or devices have full, unfettered network access?
- Is the user an employee or another member of the ecosystem?
- Where are your users accessing applications from?
- What device types are they using?
- Has that device been infected by malicious software? How do you know?
- Are you concerned about user credentials being misused or stolen, and a breach occurring?
- Do you need another layer of validation enabled, like multi-factor authentication or client-side certificates?
- Is it time to consider moving beyond VPN technology?

3 Health Check on Your Existing Security Controls

Apply the "verify and never trust" approach to devices accessing your applications and data. Malicious actors are always evolving, circumventing current defensive measures, and targeting architectural vulnerabilities inherent to security perimeters. Complete a health check on your existing security solutions with advanced threat detection and carry out security penetration testing to see what your systems might be missing. Once you complete the health check, you can determine the appropriate plan of action to solidify your defenses.

4 Update Your Application Delivery Model to Offload your Network and Improve End-User Performance

It is expensive and not realistic for IT organizations to establish private network connections between all of their users, data centers, and the cloud service providers where their applications are hosted. Enterprises cannot rely exclusively on their private WAN to deliver their applications. Instead, consider using a cloud perimeter that takes advantage of the ubiquity and scale of the Internet. Although the Internet in its native form is congested, varies in t erms of reliability, and is often not secure, it becomes a more viable transport mechanism when controlled and secured with a cloud delivery platform.

5 Define Key Capabilities to Validate

Outline the essential competencies to substantiate and prove the migration's progress and success. Common key metrics:

- Reduction in time to deploy new applications
- Reduction in training/enabling of end users
- Reduction in actionable security alerts
- Reduction of false positives (false alarms)
- Increased security posture resulting in fewer security incidents
- Detection of data leakages through DNS exfiltration

CASE STUDY

BitSight technologies, a Cambridge, Massachusetts-based company, manages third- and fourth-party risk. In 2015, it had security concerns as users began using its analytics suite of software from a third-party vendor from different locations. Earlier, only a few employees used its applications, and a traditional VPN method was effective enough. As the number of users kept increasing, going forward with a VPN infrastructure proved to be a challenge for them. They sought a solution that could work effectively with Google Authenticator and Google Directory, the two identity-management products they were already using. They wanted to develop a solution that met their requirements of enterprise-class scalability, simplicity, compliance and low cost.

SOLUTION:

Enterprise Application Access (EAA), a solution developed by Akamai, made it possible for users to connect to their internal applications securely through any browser without VPNs or proxies. EAA was easy to install, deploy, and implement, requiring zero network hardware, software, or configuration changes. BitSight has been able to scale the number of users for this application by 5X. ■

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 of offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers, and contact information for all locations are listed on www.akamai.com/locations.