WHITE PAPER

IMPERVA®

Four Steps to Defeat a DDoS Attack

Millions of computers around the world are controlled by cybercriminals. These computers, infected with "bot" malware, automatically connect to command and control servers which then instruct the bots to carry out illicit activity. Malicious users can rent these networks of bots, or botnets, to conduct powerful Distributed Denial of Service (DDoS) attacks.

The rise of hacktivism has produced a new source of DDoS attacks: the voluntary DDoS hacker. Hacktivist groups like Anonymous and LulzSec recruit hundreds and thousands of non-technical users through social networking sites to help perform powerful DDoS attacks. Simple browser-based attack tools make it easy for Hacktivist groups to unleash large-scale attacks that can bring down even the most popular Websites.

DDoS attacks, whether launched by bots or by hacktivist recruits, are not isolated, but a regular issue for many organizations. According to recent survey of IT decision makers, 74% reported suffering one or more DDoS attacks in the past 12 months. Of these, 31% said that the attacks disrupted service.[1] Whether the motivation is political, financial or just random, DDoS attacks can be extraordinarily costly for the targeted organizations.

"Like slick advertising executives, botnet operators and even bot malware creators promote their offerings with carefully fine-tuned messaging."

[1] "The Trends and Changing Landscape of DDoS Threats and Protection," Forrester.

DDoS Attacks Explained

DDoS attacks are denial of service (DoS) attacks initiated from multiple machines in order to disrupt normal operations. Traditional DoS attacks attempt to over-utilize network, server, or application resources to disable access to the targeted service. DDoS attacks amplify the effects of DoS attacks by using thousands of machines to launch their assaults. The two main classes of DDoS attacks are network DDoS attacks and application.

Network DDoS Attacks

Network DDoS attacks, sometimes termed 'volumetric' attacks, flood network resources with excessive requests from hundreds or thousands of sources. These attacks may combine a massive number of requests with TCP negotiation and fragmentation exploits to overwhelm devices at the network level. Common network DDoS attacks include SYN flood, teardrop, smurf, ICMP flood, and TCP fragment attacks.

Application DDoS Attacks

Application DDoS attacks are DDoS attacks targeted at overwhelming Web server, application server or database resources. While application-based attacks still only account for 26% of all DDoS attacks, they are more sophisticated and much more challenging to stop. Application DDoS attacks usually bypass most traditional network security devices because attack traffic often mimic regular traffic and cannot be identified by network layer anomalies.

Some application DDoS attacks simply flood a Web application with legitimate requests in an attempt to overwhelm server processing power. Other attacks exploit business logic flaws. For example, a Website's search mechanism may require excessive processing by a back end database server and become a target. An application DDoS attack could exploit this weakness by performing thousands of search requests using wildcard search terms to overwhelm the back end application database.

"Slowloris" emerged as a perilous application DDoS attack in 2009. This attack disrupts application service by exhausting web server connection pools. In the Slowloris attack, the attacker sends an incomplete HTTP request and then periodically sends header lines to keep the connection alive, but never sends the full request. Without requiring much bandwidth, an attacker can open numerous connections and overwhelm the targeted Web server. While multiple patches have been created for Apache and other web servers to mitigate this vulnerability, it nonetheless demonstrates the power of more sophisticated DDoS attacks.

The End Game for DDoS

DDoS attacks have targeted a diverse range of organizations, from government institutions and banks, to social networking companies and even root name server operators. The motivations for DDoS attacks vary: financial, political, religious, entertainment, or even personal notoriety. Many organized cyber criminals use DDoS to extort money from online sites. Authorities convicted a Russian gang of blackmailing over 50 organizations, extracting over $4 million from British companies, typically online gambling sites.[2]

Hacktivism is another key motivation for DDoS attacks. Whether driven by national patriotism or the desire to squelch the opinions of an ideological foe, DDoS is the weapon on choice. Regional hacktivist groups have performed DDoS attacks on government Websites since the mid-1990s. However, in 2010, a new breed of hacktivism emerged. Groups such as Anonymous and LulzSec began bombarding a wide swath of government and private sector Websites with Web application attacks and DDoS attacks.

Anonymous took on MasterCard, Visa and PayPal in one of its first hacktivist campaigns in late 2010. Imperva's ADC tracked the "Operation Payback" and witnessed how this campaign evolved. In the first stage of the campaign, individuals used a manually-tuned DDoS attack tool. The tool was later enhanced to become an automated DDoS attack tool, allowing any individual without any technical knowledge to participate in a full-fledged DDoS attack. In effect, participants were joining forces to form a "voluntary botnet."[3] In 2011 and 2012, Anonymous and LulzSec performed a number of high-profile attacks, bringing down Sony, Nintendo, News Corp, PBS, Pentagon, CIA, and many others.

[2] "Online Russian blackmail gang jailed for extorting $4m from gambling websites", Sophos.

[3] "Operation Payback: How it Works", Imperva Blog

DDoS Botnets-for-Hire

While hacktivist attacks often rely on voluntary hackers, most DDoS attacks are executed by criminal botnet services. DDoS rental fees typically start at $50 for small attacks, but some researchers have seen DDoS prices as low as $9. To attract customers, botnet owners advertise their services, continually seeking to outclass their botnet brethren. Owners promote their services in underground forums and mailing lists. In the case of the powerful IMDDOS botnet, the owners actually set up a public Website to showcase their offering.[4] On a message board, one botnet operator touted that his botnet offered "the best combination of quality and service" and special pricing for regular customers. Options included HTTP attacks, downloading flood, POST flood, and ping commands "tuned to perfection."[5] Like slick advertising executives, botnet operators and even bot malware creators promote their offerings with carefully fine-tuned messaging.

DDoS 2.0

DDoS attacks traditionally are carried out by computer-based bots. The Imperva ADC uncovered a new breed of DDoS attacks[6] that uses Web servers as payload-carrying bots. Imperva discovered a 300-server strong botnet that set a new standard for power, efficiency and stealth. Using a basic software program equipped with a dashboard and control panel, hackers could configure the IP, port, and duration of the attack. Hackers simply need to type the Website URL they wish to attack and then they can instantly disable targeted sites.

In fact, a single Web server is equal to 3,000 bot infected PCs. With such powerful attack weapons at their command, it is not surprising that DDoS rental services keep increasing the strength of their attacks.

The Four Steps to Mitigate a DDoS Attack

There are a number of measures that organizations can undertake to mitigate the risks of a DDoS attack. Organizations can:

Step 1. Over-Provision Bandwidth to Absorb DDoS Bandwidth Peaks

This is one of the most common measures to alleviate DDoS attacks, but it is also probably the most expensive, especially since DDoS attacks can be ten times or even one hundred times greater than standard Internet traffic levels. An alternative to over-provisioning Internet bandwidth is to use a security service to scale on-demand to absorb and filter DDoS traffic. DDoS protection services are designed to stop massive DDoS attacks without burdening businesses' Internet connections.

Step 2. Monitor Application and Network Traffic

The best way to detect when you are under an attack is by monitoring application and network traffic. Then, you can determine if poor application performance is due to service provider outages or a DDoS attack. Monitoring traffic also allows organizations to differentiate legitimate traffic from attacks. Ideally, security administrators should review traffic levels, application performance, anomalous behavior, protocol violations, and Web server error codes. Since DDoS attacks are almost always executed by botnets, application tools should be able to differentiate between standard user and bot traffic. Monitoring application and network traffic provide IT security administrators instant visibility into DDoS attack status.

[4] "Damballa Discovers New Wide-Spread Global Botnet Offering Commercial DDoS Services," Damballa
[5] "BlackEnergy competitor—The 'Darkness' DDoS Bot," Shadowserver
[6] "Security Advisory: DDoS Advisory—May 2010," http://www.imperva.com/resources/adc/adc_advisories_DDOS_Attack_Method_Payload-05182010.html

Step 3. Detect and Stop Malicious Users

There are two primary methods to identify DDoS attack traffic: identify malicious users and identify malicious requests. For application DDoS traffic, often times identifying malicious users can be the most effective way to mitigate attacks.

- Recognize known attack sources, such as malicious IP addresses that are actively attacking other sites, and identifying anonymous proxies and TOR networks. Known attack sources account for a large percentage of all DDoS attacks. Because malicious sources constantly change, organizations should have an up-to-date list of active attack sources.
- Identify known bot agents; DDoS attacks are almost always performed by an automated client. Many of these client or bot agents have unique characteristics that differentiate them from regular Web browser agents. Tools that recognize bot agents can immediately stop many types of DDoS sources.
- Perform validation tests to determine whether the Web visitor is a human or a bot. For example, if the visitor's browser can accept cookies, perform JavaScript calculations or understand HTTP redirects, then it is most likely a real browser and not a bot script.
- Restrict access by geographic location. For some DDoS attacks, the majority of attack traffic may originate from one country or a specific region of the world. Blocking requests from undesirable countries can be a simple way to stop the vast majority of DDoS attack traffic.

Step 4. Detect and Stop Malicious Requests

Because application DDoS attacks mimic regular Web application traffic, they can be difficult to detect through typical network DDoS techniques. However, using a combination of application-level controls and anomaly detection, organizations can identify and stop malicious traffic. Measures include:

- Detect an excessive number of requests from a single source or user session—Automated attack sources almost always request Web pages more rapidly than standard users.
- Prevent known network and application DDoS attacks—Many types of DDoS attacks rely on simple network techniques like fragmented packets, spoofing, or not completing TCP handshakes. More advanced attacks, typically application-level attacks, attempt to overwhelm server resources. These attacks can be detected through unusual user activity and known application attack signatures.
- Distinguish the attributes, and the aftermath, of a malicious request. Some DDoS attacks can be detected through known attack patterns or signatures. In addition, the Web requests for many DDoS attacks do not conform to HTTP protocol standards. The Slowloris attack, for example, includes redundant HTTP headers. In addition, DDoS clients may request Web pages that do not exist. Attacks may also generate Web server errors or slow Web server response time.

Imperva Cloud DDoS Protection

To mitigate DDoS attacks, organizations can implement the DDoS mitigation measures described in this paper. However, due to the complex and evolving nature of DDoS attacks, many organizations are turning to third party services. Imperva Cloud DDoS Protection is a cloud-based service that stops all types of DDoS threats, including network and application DDoS attacks. As a service, Imperva Cloud DDoS Protection can scale on demand to stop multi-gigabit attacks without requiring businesses to purchase expensive Internet connections or deploy additional networking equipment.

Imperva Cloud DDoS Protection combines multiple defenses to mitigate DDoS attacks. Ironclad network defenses detect network attacks like SYN and TCP floods. Imperva Cloud DDoS Protection detects sophisticated application-layer attacks that bypass traditional DDoS security services through unique bot mitigation defenses. These defenses differentiate between bots and legitimate application users by validating whether the client browser can execute JavaScript, store cookies and perform other basic browser functions. The service also stops known DDoS attacks through a combination of signatures, HTTP protocol conformance, and request rate limiting. Temporary measures like CAPTCHA validation on suspicious clients and access controls by geolocation effectively mitigate even the largest DDoS attacks.

Imperva Cloud DDoS Protection:

- Enables businesses to avoid application outages and brand damage
- Protects in minutes with effortless deployment
- Scales to absorb DDoS attacks that exceed Internet bandwidth limits
- Leverages real-time assistance from Imperva's DDoS experts
- Lowers costs by eliminating need to over-provision bandwidth

Businesses can combine Imperva Cloud DDoS Protection with Imperva Cloud WAF for a full defense against Web application threats. Alternatively, SecureSphere Web Application Firewall (WAF) customers can subscribe to Imperva Cloud DDoS Protection to mitigate DDoS attacks; Imperva Cloud DDoS Protection complements SecureSphere WAF deployments.

Summary

Over the past several years, the industrialization of attacks and the rise of hacktivism have resulted in an explosion of powerful and destructive DDoS attacks. Using off-the-shelf toolkits, criminals can quickly build botnets of thousands or even millions of computers. Malicious users can rent these botnets to unleash destructive DDoS attacks on virtually any victim. Additionally, hacktivists have turned to social networks and attack tools like LOIC and RefRef to unleash powerful DDoS attacks.

The DDoS mitigation techniques presented in this paper are just a few of the measures that organizations can undertake to combat DDoS attacks. Due to the variety of DDoS attack vectors, from massive network attacks like SYN flood and teardrop to application DDoS attacks like HTTP flood, Slowloris, and RUDY, many businesses have begun to outsource their DDoS security to dedicated security service providers. Imperva Cloud DDoS Protection, a powerful, comprehensive cloud-based security service, offers organizations a cost-effective and easy solution for stopping DDoS attacks.

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance.

IMPERVA®

www.imperva.com