Making Everything Easier!™

Corero Network Security Edition

DDoS FOR DUMMIES®

Learn:

- Why DDoS threatens your business
- Who is out to get you — and why
- How to protect your networks

Compliments of

corero NETWORK SECURITY

Lawrence C. Miller

About Corero Network Security

Corero Network Security (CNS:LN) is a leading global provider of Distributed Denial of Service (DDoS) defense solutions and Network Intrusion Prevention Systems (IPS). Enterprises rely on Corero to protect their critical online assets against risks associated with network-borne cyberthreats. Corero is headquartered in Massachusetts, U.S. with offices worldwide.

www.corero.com

DDoS FOR DUMMIES®

CORERO NETWORK SECURITY EDITION

by Lawrence C. Miller

John Wiley & Sons, Inc.

DDoS For Dummies®, Corero Network Security Edition
Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Published by John Wiley & Sons, Inc., Hoboken, New Jersey

ISBN 978-1-118-18253-6 (pbk); ISBN 978-1-118-18279-6 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents

Publisher's Acknowledgments

We're proud of this book and of the people who worked on it. For details on how to create a custom For Dummies book for your business or organization, contact info@dummies.biz. For details on licensing the For Dummies brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Some of the people who helped bring this book to market include the following:

Acquisitions, Editorial, and Vertical Websites

Project Editor: Jennifer Bingham

Editorial Manager: Rev Mengle

Business Development Representative: Sue Blessing

Custom Publishing Project Specialist: Michael Sullivan

Composition Services

Project Coordinator: Kristie Rees

Layout and Graphics: Sennett Vaughan Johnson, Lavonne Roberts

Proofreader: Jessica Kramer

Publishing and Editorial for Technology Dummies

Richard Swadley, Vice President and Executive Group Publisher

Andy Cummings, Vice President and Publisher

Mary Bednarek, Executive Director, Acquisitions

Mary C. Corder, Editorial Director

Publishing and Editorial for Consumer Dummies

Kathleen Nebenhaus, Vice President and Executive Publisher

Composition Services

Debbie Stailey, Director of Composition Services

Business Development

Lisa Coleman, Director, New Market and Brand Development

Introduction

The Internet has revolutionized the way business operates. Today, global businesses move huge volumes of data in real-time, and e-commerce is fast becoming the lifeblood of trade. Financial trading houses conduct business at speeds and scales that were incomprehensible just a few years ago. E-retail has grown on a vast scale, serving remote customers across the globe. Entire industries have sprung up around online gambling and gaming sites. Online companies depend on 24/7 availability and fast, real-time responsiveness to ensure that customers keep coming to their websites. But this new world of high-speed, high-volume e-commerce has created new opportunities for criminals and others who would do harm to thriving online companies. Malicious competitors, extortionists, and hacktivists are orchestrating devastating distributed denial-of-service (DDoS) attacks, turning dependence on the speed and availability of business websites against those who run them.

About This Book

This book explores real-world examples of DDoS attacks, the motivations of their perpetrators, and the operational and business risks to organizations. You also learn why traditional security solutions are ineffective and how Corero's comprehensive DDoS Defense System protects enterprise networks against modern DDoS attacks. This book was written for Corero.

This book is written with both technical and nontechnical readers in mind, so whether you're an executive, line of business manager, or an IT specialist this book is for you.

How This Book Is Organized

This book consists of five short chapters. Here's a brief look at what awaits you!

- **Chapter 1: DDoS Attacks Defined.** I explain the tactics and motives of today's cybercriminals and the impact of DDoS online businesses.
- **Chapter 2: DDoS Countermeasures: What Works and What Doesn't.** Chapter 2 explains why traditional security solutions and defense mechanisms — and most DDoS mitigation methods — aren't sufficient to protect your systems and networks from modern DDoS attacks.
- **Chapter 3: Best Practices for DDoS Attack Mitigation.** Despite your best efforts, your organization may be hit by a DDoS attack. The security solutions you deploy and the policies and plans that you create now will determine whether or not an attack is successful. Chapter 3 will help you prepare.
- **Chapter 4: Your Best Protection: On-Premises DDoS Defense.** Next, I introduce you to the advanced capabilities and features that on-premises protection from Corero brings to the fight against DDoS attacks.
- **Chapter 5: Eight Benefits of Corero's DDoS Defense System.** Finally, in that classic *For Dummies* format, I end with a chapter of compelling reasons for you to deploy Corero's DDoS Defense System.

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. You won't see any smiley faces winking at you or any other little emoticons — distributed denial of service is a serious matter — but you'll definitely want to take note!

This icon points out information that may well be worth committing to memory to help you understand and deal with DDoS attacks day-in and day-out.

This icon offers helpful tips and useful nuggets of information about DDoS attacks and defense.

Don't let this happen to you. These useful alerts offer practical advice to help you avoid potentially costly mistakes.

Chapter 1

DDoS Attacks Defined

In This Chapter

- Analyzing modern DDoS tactics
- Pinpointing opportunities for DDoS attackers in real-world businesses
- Getting to know the enemy

A DDoS attack against your organization's network and systems can bring your online business to a grinding halt, costing you hundreds of thousands — even millions — of dollars, ruining your brand, and driving away your customers.

For a crime to occur — and make no mistake, DDoS attacks are crimes — three elements must be present: means, opportunity, and motive.

In this chapter, you learn about modern DDoS attacks (the *means*), their impacts on real world businesses (the *opportunity*), and the *motives* of their perpetrators.

Examining DDoS Attacks

Today's computing environments are being bombarded by *distributed denial-of-service* (DDoS) attacks that overload critical systems and networks, causing them to become unresponsive and unproductive.

A *DDoS attack* is a cyberattack in which many, usually compromised, computers send a series of packets, data, or transactions over the network to the intended attack victim (or victims) in an attempt to make one or more computer-based services (such as a web application) unavailable to the intended users. DDoS attacks generally result from the

concerted efforts of cybercriminals to stop an Internet site from functioning efficiently or at all.

DDoS attacks have plagued the Internet, corporate websites, and networks for more than a decade. Although DDoS attacks aren't new, modern threats and tactics are more advanced than ever, and DDoS attacks are occurring with increasing frequency and causing greater damage against a rapidly growing number of targets worldwide.

The means for committing DDoS attacks are readily available to practically anyone. Easy-to-use, automated tools can be freely downloaded from various *blackhat* (hacker) websites on the Internet. The resurgence in DDoS attacks can be largely attributed to two factors: the rise of global botnets and new attack techniques for evading detection.

The role of botnets

A *botnet* is a network of compromised PCs or other devices. These compromised PCs are called *bots* (or *zombies*). Bots are PCs that are infected with various types of malware, such as viruses, worms, Trojans, and spyware, that enable the PCs to be compromised by an attacker. A bot can be remotely controlled by an attacker (sometimes called a *bot-herder*) to carry out DDoS attacks, steal data from victim networks and servers, or send out e-mail spam. Bots can be particularly difficult to detect and clean from an infected PC because they're very adaptive and resilient. The bot-herder can quickly and easily change the behavior and characteristics of a bot, making it extremely difficult to detect.

Some bots even detect and clean many common types of viruses from an infected PC, so that your installed anti-virus or anti-malware software doesn't tip you off to the larger (bot) infection!

It has been estimated that up to 80 percent of all Internet-connected computers are infected with some form of spyware or adware.

Botnets are typically comprised of hundreds of thousands to millions of infected bots, and can operate for several years before being discovered or taken down. Criminal organizations

are known to rent out control of botnets to anyone willing to pay the price — often for less than $100 per day.

Types of attacks

The second major factor spurring increased DDoS attacks is a shift in techniques from brute force assaults to more insidious attacks.

In a *brute force* attack, the attacker sends an exceptionally large payload to a targeted organization's network in order to overwhelm the available bandwidth on that network. These traditional DDoS attacks are called *network-layer* DDoS attacks and are still common today (see sidebar, "The devil is in the DDoS details").

Network-layer DDoS attacks can disrupt communications with your critical e-commerce servers, for example, or overwhelm your network. A botnet comprised of large numbers of hijacked systems simultaneously sends packets to a target server, attempting to open a communication session. When the victim server replies, the attacking systems don't acknowledge the server's response. This overloads the server by causing it to use all its available resources attempting to keep track of the many incoming connections. Service is degraded, and the server may crash.

An overwhelming network-layer DDoS attack can disrupt or overload the network infrastructure to the point where it can't transmit requests or responses. These attacks can affect ISP (Internet service provider) links, routers, switches, firewalls, and servers, causing one or more of them to become bottlenecks, and restricting or eliminating the ability of the server to deliver its service.

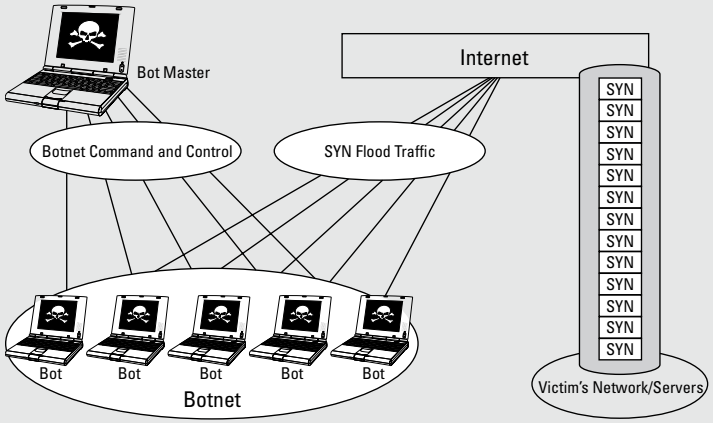
In an effort to thwart the security mechanisms used by most organizations to defend against traditional network-layer DDoS attacks (such as firewalls and some intrusion prevention systems) attackers have adopted a newer variant of the traditional DDoS attack — a*pplication-layer DDoS attacks*.

The devil is in the DDoS details

Traditional network-layer DDoS attacks typically flood the victim's system or network with requests, such as a flood of IP packets, TCP packets, or ICMP packets. The following are some common types of traditional DDoS attacks.

SYN Flood

A SYN-flood attack (see the accompanying figure) takes advantage of the TCP (Transmission Control Protocol) three-way handshake process by flooding multiple TCP ports on the target system with SYN (*syn*chronize) messages to initiate a connection between the source system and the target system. The target system responds with a SYN-ACK (*syn*chronize-*ack*nowledgement) message for each SYN message it receives and temporarily opens a communications port for each attempted connection while it waits for a final ACK (*ack*nowledgement) message from the source in response to each of the SYN-ACK messages. The attacking source never sends the final ACK messages and therefore the connection is never completed. The temporary connection will eventually time out and be closed, but not before the target system is overwhelmed with incomplete connections.



UDP Flood

A UDP (user datagram protocol) flood attack involves the attacker sending UDP packets to each of the 65,535 UDP ports on the target system. The target system is overloaded while processing the UDP packets and attempting to send reply messages to the source system.

ICMP flood

Most network-layer DDoS attacks use bot-infected systems to flood a target with network traffic. ICMP (Internet Control Message Protocol) packets are commonly used for this purpose. ICMP packets are legitimately used for network troubleshooting, but when used for a DDoS attack, these tiny packets can overwhelm a target system, leaving it unable to service valid network requests in a timely fashion.

Application-layer DDoS attacks still take place over the network. But these attacks not only send network packets — they actually complete TCP connections from the attacker to the victim server. Once the TCP connection is made, the attacking computers make repeated requests to the application in an attempt to exhaust the resources of the application, rendering it unable to respond to any other requests.

These more intelligent attacks are harder to defend against because they create denial-of-service conditions without consuming all the available network bandwidth or overloading routers, firewalls, and switches. The attack traffic often looks like legitimate, routine traffic coming into a network or website. It could be something as simple as a request to display a web page or to fill out a "contact us" form. A common example of an application-layer DDoS attack is a repetitive HTTP GET request, which cripples a Web application server with an overwhelming number of requests for a resource.

Compared to a network-layer attack, a successful application-layer attack typically requires a much smaller botnet to overwhelm a victim server. The hijacked bots in an application-layer DDoS attack go beyond simply initiating an open communications session with a victim server. Because the attacking bots are actually communicating with the victim server, more server resources must be allocated, and potentially the resources of other network assets, such as a database server, that are integrated with the victim server.

The goal of all the different types of DDoS attacks is to consume resources that should be available for a system or application to serve its intended customers.

Recognizing the Business Impact of DDoS Attacks

Far too many organizations are ill-prepared to deal with the effects of DDoS attacks and other Internet security threats. They rely on firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), and other security technologies that are inadequate to defend their networks and systems against DDoS attacks (see Chapter 2 to learn more), thereby creating plenty of opportunity for cybercriminals today. In the following sections, I tell you about a few industries that are prime targets for DDoS attacks.

E-commerce

E-commerce is the lifeblood of many businesses around the globe and has become a way of life for millions of consumers who depend on their computers and mobile devices to buy products and services, research product information, and obtain support. JP Morgan projected that 2011 e-commerce revenue would reach $680 billion, up 18.9 percent over 2010. E-commerce works in our modern, fast-paced world because e-commerce sites are responsive, secure, and always available on demand. E-commerce is quickly transforming the Internet from the "information superhighway" into the "information supermall."

Unfortunately, legitimate businesses aren't the only ones taking advantage of the tremendous opportunities created by the Internet. Criminals have been quick to gravitate to the Internet as business volume and the value of online transactions have reached critical mass. There's big money in online business — and therefore big criminal opportunity.

Online companies are victimized by mass, automated attacks that exploit targets of opportunity, as well as targeted attacks that exploit *unpatched* or *zero-day* (previously unknown) vulnerabilities. Organized criminals also employ hacking techniques and malware to commit data theft, extortion, identity theft, and fraud. The crimes are as old as civilization, but the methods are adapted to the times and the impact is devastating.

DDoS attacks are on the rise: Gartner reports a 30 percent increase in attacks in 2010, and that trend has continued through 2011. Cybercrimes are now the FBI's third highest priority, behind terrorism and espionage.

E-commerce companies depend on 24/7 availability and real-time responsiveness on their customer-facing sites. When a DDoS attack strikes, businesses can lose thousands or even millions of dollars if service is slowed or the website goes down. Extended service interruptions can be catastrophic, both in terms of revenue loss and damage to the corporate brand.

To your customers, your Internet website *is* your business. If your website is down, your customers can simply surf over to your competitors' websites and may become your *former* customers. Disruptions to your website for any extended period can impact business and severely undermine customer confidence. Recent DDoS attacks have hit Amazon, PayPal, Visa, Sony PlayStation Network, and MasterCard, among others.

Companies doing business online are also entrusted with and responsible for sensitive customer data, including account credentials, credit cardholder data, and personally identifiable information (PII). Compliance mandates, such as the Payment Card Industry Data Security Standard (PCI DSS), impose stiff penalties on businesses for failing to protect these records against unauthorized access.

A DDoS attack can be a preemptive strike to test your company's security and response capabilities. For companies that aren't ready to properly respond to an attack (see Chapter 3), a panicked and unorganized reaction can weaken your defenses and open the door for further attacks and data theft. Even if a DDoS attack doesn't lead to a data breach, your customers' perception will be that your company's website isn't secure, which may cause them to hesitate when doing online business on your site or to avoid your site altogether.

According to a survey by the Ponemon Institute, the average total cost of a single data breach was more than $7.2 million dollars in 2010.

Financial services

The Internet has revolutionized the way financial institutions do business, from online banking services to high-speed global transactions and payment processing. Financial transactions are processed in huge volumes and at high speeds around the globe, enabling institutions, partners, and customers to react swiftly to changing financial conditions and market requirements.

Customers conduct online transactions from anywhere, at any time, and increasingly, from any number of different devices (such as smartphones and tablets). They expect their information to be secure and that services will be reliable, fast, and always available when they need them.

As the Internet has opened up new business opportunities, it has also introduced new elements of risk in the financial services sector that must be considered in their risk assessment and risk mitigation programs. These risks, broadly speaking, manifest themselves in two categories:

- **DDoS attacks:** For online banking and financial transactions, time is quite literally money. Millions of dollars can be lost in minutes if service is slowed or interrupted. In performance-sensitive environments such as transaction processing and high-volume trading, major service interruptions can be catastrophic, both in terms of actual financial loss and damage to the corporate brand.
- **Data breach:** Like e-commerce companies, financial institutions — from the largest banks and trading houses to regional credit unions — are entrusted with and responsible for sensitive customer data. Financial services providers are required by numerous regulations and obligations to their customers and partners to protect these sensitive records against unauthorized access.

Malicious cyberactivity is a continuous threat to both online transactions and services and sensitive information. Many banks, stock exchanges, and other financial institutions, including Bank of America, U.S. Bancorp, and the New York and Hong Kong stock exchanges, have been victims of DDoS attacks.

Online gaming

Online gaming is big business. Many millions of people engage in Internet gambling from poker to bingo, and play video games such as first-person action shooters and wildly popular role-playing fantasy games on platforms including PCs, Microsoft Xbox, and Sony PlayStation. The stakes are high:

- According to a report by Global Betting and Gaming Consultants, the global online gambling industry grew by 12 percent during 2010 to $29.3 billion.
- According to the Online Gaming Association, 20 million Microsoft Xbox users have spent 17 billion hours online; there are 40 million Sony PlayStation Network accounts.

Performance and availability are critical to the success of online gaming businesses. DDoS attacks can undermine the business in a hurry. If a gambling site goes down, all bets are off. And for gamers, a slow game is no game at all — they will seek entertainment elsewhere, perhaps at a competitor's gaming site. Video game companies, in particular, may face unscrupulous competitors that would attack their site during beta testing to disrupt the launch schedule for a new game, or to ruin gaming sessions in order to drive customer traffic to their own game sites.

In addition to the DDoS threat, online gaming companies and gambling sites, like other businesses that engage in e-commerce and financial transactions, are custodians of sensitive customer data and financial information, and are therefore subject to various compliance mandates, including PCI DSS and numerous state data breach notification laws.

The hacktivist group Anonymous recently directed DDoS attacks against the Sony PlayStation Network to protest the entertainment giant's lawsuit against the person who published code that lets users "jailbreak" the PlayStation 3.

Understanding the Attacker's Motivations

"If ignorant both of your enemy and yourself, you are certain to be in peril."

– Sun Tzu, *The Art of War*

Bragging rights and recognition of hacking skills used to be the primary motivation for DDoS attacks against prominent websites. Today, a number of more sinister motives drive DDoS attacks, including criminal extortion, unfair business advantage, and political or ideological activism — all of which are explained in the following sections.

Criminal extortion

One of the main motivations for DDoS attacks today is criminal extortion. An attacker threatens to take down the intended victim's site or network unless a ransom is paid. A limited denial-of-service attack is often launched concurrently with the threat to establish the attacker's credibility.

An online gaming site recently received just such a criminal extortion threat and got a taste of what was to come with a limited proof-of-concept attack. Rather than knuckle under to the criminals, the would-be victim site installed an on-premises DDoS defense solution and vanquished the threat (see Chapter 4 for details).

Once the ransom is paid, the attacker generally moves on, although the victim risks being branded as a "payer" and being subjected to future ransom demands by the same attacker or other criminals.

Organized crime is now enlisting the aid of and incorporating the techniques of hackers for criminal activities such as identity theft, online fraud, and extortion. Real-time cybercrime attacks are now listed as the FBI's third highest priority, behind terrorism and espionage.

Unfair business advantage

The general decline in business ethics isn't limited to collusion scandals and insider trading. Sadly, it is not a far stretch for companies that engage in corporate espionage to actively engage in corporate sabotage to gain an unfair competitive advantage (see the sidebar, "No charges yet in DDoS attack targeting online U.S. battery retailers").

No charges yet in DDoS attack targeting online U.S. battery retailers

The FBI is still investigating several DDoS attacks that targeted various retail battery websites, including Batteriesplus.com and Batteries4less.com, in October 2010. The attacks have been traced to Russia, but there is speculation that they were sponsored by a U.S.-based rival in the highly competitive online battery-reseller market.

Combined financial losses among the victim sites is estimated to be more than $600,000, with Batteries4less.com incurring damages of approximately $50,000 due to lost sales and expenses associated with recovery and remediation.

Typically, these types of DDoS attacks are carried out by third-party "contractors" on behalf of a company against its competitors. A victim company can suffer significant direct costs that include lost revenues and remediation expenses, as well as indirect costs (that are often far greater than direct costs) due to reputation damage and loss of future business.

Political and ideological activism

Another major motivation for DDoS attacks today is political or ideological activism, also called *hacktivism,* in which an attacker disagrees with an organization's policies or viewpoints (or existence), and attempts to punish the victim or its supporters with a DDoS attack (see the sidebar "Wicked DDoS attacks on behalf of WikiLeaks").

Recent examples of politically or ideologically motivated DDoS attacks include attacks by the hacktivist group LulzSec against the U.S. Senate, the U.S. Central Intelligence Agency, and the Serious Organized Crime Agency (the U.K.'s equivalent of the FBI).

Wicked DDoS attacks on behalf of WikiLeaks

In December 2010, a worldwide hacktivist group known as Anonymous launched Operation Payback, a series of worldwide DDoS cyberattacks, against MasterCard, Visa, PayPal, Amazon, and other major companies and organizations who cut off sources of funding to WikiLeaks in 2010.

Chapter 2

DDoS Countermeasures: What Works and What Doesn't

In This Chapter

- Using the wrong tools (firewalls and IDS) to combat DDoS
- Recognizing the limitations of various DDoS defense techniques

The sad fact is that being the victim of a DDoS attack is a very real threat for every organization doing business over the Internet today. And although your organization may already be protected from many general threats by a robust firewall and an intrusion prevention system (IPS), these devices are ill-suited for the critical task of protecting your network and systems from modern DDoS attacks.

In this chapter, you learn why general security devices, such as firewalls and IPSs, aren't enough to protect your network and systems against DDoS attacks, and the limitations of some familiar anti-DDoS techniques.

Traditional Security Solutions Aren't Sufficient

Many organizations deploy firewalls for network access control and as intrusion detection and prevention systems (IDS/IPS) for monitoring, identifying, and blocking malicious network traffic. However, these traditional security solutions are

largely ineffective at protecting networks and systems from both network-layer and application-layer DDoS attacks.

Firewalls

The *firewall* is an important cornerstone of network security and is generally an organization's first line of defense against Internet-based threats. A firewall's basic task is to control the flow of traffic between computer systems of differing trust levels (for example *trusted* computers inside the corporate network and *untrusted* computers outside the corporate network or on the Internet).

Typically, a firewall is deployed at the perimeter between two networks (for example, between a corporate network and the Internet) and specific access rules are defined. For example, a very simple firewall policy might allow any connections that are initiated from computers inside the corporate network to the Internet, but only allow connections initiated from the Internet to access a web server.

A firewall policy that simply allows all outbound connections from the corporate network is very dangerous. A bot-infected computer inside the trusted network can initiate connections to an entire botnet and indefinitely maintain an open, unsecured connection to the Internet.

Because traditional firewalls aren't designed to inspect application content (they generally only inspect the first few bytes of a packet to minimize latency), an attack from an allowed IP address or port can often simply pass through a firewall. This creates several problem areas, or *blind spots*, for traditional firewalls:

- Common network protocols must be allowed to facilitate certain Internet functions such as the Simple Mail Transfer Protocol (SMTP, for e-mail delivery) and the Domain Name System (DNS, for name resolution).
- Standard TCP and UDP ports are defined for common applications, but these standards aren't enforced, so many application vendors — and particularly malware developers — simply ignore the standards so that their applications can "come along for the ride" with other applications that are permitted by a firewall.

- Application traffic is increasingly being encrypted with SSL (Secure Sockets Layer) to protect privacy, but SSL can also be used to hide malicious content.

Firewalls *have to* allow these protocols and are blind when traditional flood attacks use them. And, application-layer attacks establish legitimate connections with the target server and these connections are therefore permitted by the firewall. Firewalls can't simply block a bona fide protocol or application connection.

Nor can firewalls typically throttle down the flow of DDoS traffic using what is known as *rate-limiting,* that is, assigning more or less bandwidth to a particular connection.

In fact, traditional firewalls are sometimes themselves overwhelmed by DDoS attacks. Firewalls are often the first point of failure during an attack, rendering the site offline until the attack ceases and the firewall is reset. Worse yet, some firewalls "fail open" if they become overwhelmed, thereby letting more sophisticated attacks penetrate the network.

Intrusion detection systems

An intrusion detection system (IDS) is a network monitoring tool that detects malicious attempts to access, manipulate, and/or disable computer systems and networks. An intrusion prevention system (IPS) is an intrusion detection system that can be deployed *in line* (in the flow of network traffic) to actively block intrusion attempts. An IDS or IPS typically supplements a firewall to provide more robust network security.

Most IDS and IPS systems maintain a very large database of known attack signatures that must be regularly updated as new threats emerge. A signature-based IDS/IPS operates similarly to antivirus software that relies on known malware patterns to detect attempts to infect your computer. IPS databases are very large, so it is generally not practical to enable all the available rules or signatures because of performance degradation (similar to the performance hit your computer takes when your anti-virus software is doing a full system scan). An IPS deployed in line could create a network bottleneck if performance lags.

Although some IDS/IPS solutions purport to address DDoS attacks, they're not designed for this purpose. IPS typically

has neither the means to identify nor the ability to limit streams of DDoS attack traffic. Traditional network-based DDoS attacks utilize allowed network protocols, such as TCP and UDP. A typical IPS can't detect and block application-layer attacks because it would consist of allowed connections to the target server. Sometimes, hybrid attacks use DDoS to mask a malware attack "hiding" in all that traffic, thereby tricking and/or heavily tasking the security device.

ISP and Cloud-Based DDoS Defense Solutions

Various security vendors and service providers have taken different approaches to DDoS defense. These approaches include overprovisioning of network bandwidth or CPU cycles, *clean-pipe* solutions, and specialized cloud-based anti-DDoS services.

Overprovisioning

Overprovisioning bandwidth is a logical approach, generally speaking, to dealing with increased traffic loads and spikes during heavy business periods, such as e-commerce sales and holiday shopping seasons (particularly Cyber Monday, the first Monday after Thanksgiving in the U.S.).

Businesses also need to ensure that their e-commerce servers have the CPU cycles necessary to handle large volumes of Internet-based transactions, particularly during peak times and as their business grows.

Increasing network bandwidth and server CPU power to meet heavy transaction loads and growing traffic requirements makes good business sense, but these are somewhat limited and inefficient approaches to combating DDoS:

- **Companies are bound to a cycle of never-ending escalation.** Attackers will continue to bombard your networks and increase the volume of their attacks until they succeed at taking down your network. For example, a national government recently suffered a politically motivated 15 gigabit per second attack.

- **Overprovisioning isn't cost effective.** This costly approach requires you to constantly purchase more bandwidth and computing power — not to build your business, but to stay ahead of the attackers. You're throwing good money after bad. It is far better to invest in a security solution with finite and predictable costs.
- **No protection is provided against application-layer DDoS attacks.** Unlike network-layer attacks that flood a target network, application-layer attacks don't consume huge amounts of bandwidth. Therefore, purchasing additional bandwidth is useless in combating this type of attack. An application-layer attack will continue to bombard a target server with legitimate connection requests until the server slows to a crawl or crashes.

Clean-pipe anti-DDoS solutions

Clean-pipe anti-DDoS solutions are generally offered by ISPs in the form of security services. The general idea is that the service provider monitors and inspects Internet traffic, and routes suspect traffic to a proxy that "scrubs" the pipe clean of malicious packets. Clean-pipe services can be effective weapons for combating DDoS, but you should be mindful of several important considerations:

- **Service providers deal with many customers and may tend to take a one-size-fits-all approach for efficiency and cost containment.** Although clean-pipe services offload some of the overhead for combating DDoS, you must work closely with the service provider to help identify the traffic types and patterns that are unique to your company's policies, applications, and business practices. Because the solution provider is servicing many clients, they may be less discriminating than they should be.
- **If you're relying on your service provider, you're paying a premium for good traffic.** One could argue that "clean" traffic should be part of the Internet service.
- **Good traffic may be lost.** The clean-pipe service may throw out the good with the bad using *black hole* routing — especially when it comes to traffic patterns and types that may be specific to your environment.
- **The ISP is reactive.** Your ISP monitors bandwidth usage and reacts after the attack starts.

- **Clean-pipe solutions aren't very effective when there are large numbers of attackers and/or victims.** In the absence of a solution that can be tailored to each organization and in the face of multiple attackers, the clean-pipe approach can't deal effectively with a mass of different types of attacks from multiple sources against many targets.

An ISP may use black hole routing to consign your outbound traffic to oblivion if it detects outbound attack traffic from bots within your network. You need to consider a solution that will effectively detect and mitigate outbound as well as inbound traffic.

Specialty in-the-cloud anti-DDoS providers

Specialty in-the-cloud anti-DDoS service providers are effective against high-volume attacks and offer the advantage of specialization and focus on DDoS, as opposed to ISPs that offer anti-DDoS as a value-added service. Cloud-based service providers have a deeper understanding of DDoS and expertise in combating it. Some considerations before contracting with in-the-cloud anti-DDoS service providers include:

- The anti-DDoS service provider itself may be a high-value target.
- Cloud-based anti-DDoS services have no visibility into outbound traffic or server responses, limiting their effectiveness. Monitoring outgoing traffic also often provides valuable forensic evidence and aids in the detection of bots in the network as they participate in attacks and/or communicate with their command-and-control servers.
- They don't protect against application-layer DDoS attacks.

A purpose-built, on-premises DDoS defense solution provides the best protection against both network- and application-layer DDoS attacks (see Chapter 4 to discover more about just such a solution).

Journal Register prevents DDoS attacks from stopping the virtual presses!

The Journal Register Company is one of the largest newspaper publishers in the U.S. With 324 multiplatform news products that include web and video offerings as well as print, the Journal Register is a digital-first organization serving an audience of 15.8 million people every month.

The Challenge

While transforming itself from a legacy print-only newspaper publisher to a 21st Century digital-first news organization, the Journal Register experienced a DDoS attack at its Michigan location. Malware breached existing defenses, significantly degrading network performance and impacting content delivery.

"As a news and information organization, people depend on us," says CTO Bob Mason. "From a business perspective, reliability is our most valuable competitive asset. If we can't provide our audience with real-time content, they'll seek it elsewhere."

Clearly, the Journal Register needed to stop the attack — fast. "It became quite urgent that we provide mitigation," Mason says. "And, concurrently, we wanted to adopt the appropriate technology to protect us going forward."

The Solution

Quick action was required to mitigate the adverse effects of the DDoS attack. Fortunately, Mason had previously evaluated several security solutions and knew who to call when the attack on the Journal Register began.

"We had planned to go through a regular evaluation process," says Mason, "but the situation required immediate action."

Journal Register opted for an on-premises security appliance to combat its DDoS problems. The initial attack was blocked quickly, and within two weeks of contacting its vendor of choice, Corero Network Security, the Journal Register's multiple sites were secured.

"Now our network staff can sleep at night," Mason says.

Chapter 3

Best Practices for DDoS Attack Mitigation

In This Chapter

- Planning and preparing for a DDoS attack
- Separating the wheat from the chaff

It happens all too often. A company receives an ultimatum threatening a DDoS attack: "We'll take your network down unless US$30,000 is wired to us within a week." Could this happen to you? Absolutely! So, when it happens to you, what will you do?

In this chapter, I present my top recommendations for mitigating the effects of a DDoS attack against your organization.

Create a DDoS Response Team and Plan

A DDoS response team is similar in composition and purpose to a typical incident response team, but with some important differences. As with any incident response team, a designated team lead is one of the most important roles. The team lead needs to make sure certain things are done at key moments:

- **Before an attack:** Ensuring appropriate individuals are assigned to the various team roles, that they understand their responsibilities, and that they're properly trained and prepared to perform their individual functions.

- **During an attack:** Directing and coordinating the mitigation, remediation, and recovery efforts; ensuring timely, accurate, and consistent communications with management, service providers, legal counsel, corporate communications, customers, affected employees, team members, security vendors, partners, and law enforcement (if appropriate).
- **After an attack:** Overseeing the collection of logs and forensic evidence and documenting response and mitigation technology gaps, weaknesses, and lessons learned. Recommending and implementing corrective actions to improve response procedures and, if necessary, augment existing DDoS defense tools and services.

Looking at your DDoS response plan

One of the first important tasks of the DDoS response team is to create the *DDoS response plan*. As with any plan, advance preparation is the key to rapid and effective action. A DDoS response plan lists and describes the steps an organization should take in the event of a DDoS attack against its IT infrastructure to avoid an all-hands-on-deck scramble.

A well-written business continuity plan (BCP) or continuity of operations plan (COOP) will address many of the same objectives of the DDoS response plan with regard to restoring normal business operations. Development of these plans should be closely coordinated to avoid duplication of effort and contradictory information. However, a BCP is *not* a substitute for a DDoS response plan.

I've prepared a detailed checklist of steps you can take to assure that your organization:

- Has the best possible DDoS response plan in place
- Keeps your plan and awareness of current threats up to date
- Reacts quickly and takes appropriate action during and after a DDoS attack.

The first requirement of an effective DDoS response plan is preparation. The preparation checklist provided in Table 3-1 will help you assess your organization's level of preparedness for a DDoS attack.

You should modify the checklists provided in this chapter as necessary to match your organization's unique infrastructure, policies, and business requirements.

Table 3-1 Preparation Plan

Criteria	✓
We have a clearly defined DDoS defense strategy and fully understand how and when to initiate our DDoS response plan.	
We have located our ISP circuit IDs and demarcation points, and have documented all circuits, IP addresses, and ISP routes.	
We have a current ISP contact list detailing how to contact our ISP(s) in case of a DDoS attack.	
We have a current list detailing personnel within the organization who should be notified in the event of a DDoS attack.	
We understand what devices and browser types normally access our public-facing websites and where our business traffic originates from.	
We have a fully documented logical and physical network topology.	
We know what devices and/or networks are high-risk targets of a DDoS attack, and documented IP addresses, ports, and services.	
We have a baseline measurement of our protocols, traffic types, normal traffic flows, and overall network usage, and have deployed technology to monitor real-time activity.	
We have fully cataloged our websites and have a baseline measurement of how often the average user should be accessing pages that are the most server-resource intensive.	
We have fully documented our DNS infrastructure and have patched any relevant DNS vulnerabilities.	
We have a baseline measurement of our web and DNS infrastructure and have documented the average connection rates and connection usage per normal user accessing our infrastructure.	
We have deployed technology at our Internet perimeter to defend against network-layer and application-layer DDoS attacks.	
We have designed a secure remote access configuration that will allow for remote management of our DDoS defenses while under attack.	

Even the best DDoS defense preparation plans can become stale and irrelevant without continuous vigilance. Use Table 3-2 to assess the current state of your organization's DDoS defense posture.

Table 3-2 Vigilance Plan

Criteria	✔
We research and analyze new DDoS attack vectors and other industry trends.	
We constantly review and update our DDoS response plan within the context of defending against newly discovered attack vectors.	
We keep our DDoS defense technology up to date with the latest vendor patches.	
We audit all configuration changes to our DDoS defense technology, ensuring no gaps in our defenses are introduced by improper configuration changes.	
We identify all current web pages on our website(s) and add defense configurations to our DDoS defense technology that detect "behavioral exploitation" of these current web pages.	
We document changes to our web and DNS infrastructure and configure our DDoS defense technology as changes are made.	
We monitor and document trends across our network, web, and DNS infrastructure; we identify times of low activity versus times of peak activity and how our network responds at various times.	
We regularly stress test and validate that our monitoring and logging operations are working as designed and will function properly.	
We regularly test our automated alerting functionality and have set up thresholds in our logging system that alert responders in the event of a DDoS attack.	
We monitor our on-premises DDoS defense devices to ensure they're running as designed with no hardware/software issues.	
We regularly optimize our DDoS defense technology to defend against a wide array of different DDoS scenarios and regularly test our defenses against these scenarios.	

Criteria	✔
We closely monitor employee and staff changes, ensuring logins and passwords to our perimeter defense systems are removed upon termination or if the employee moves.	
We regularly complete third-party assessments of our DDoS on-premises mitigation configurations and have fully tested it in accordance with their recommendations.	

The proof of a robust DDoS response plan is when it is put to the test during an actual DDoS attack. Use Table 3-3 to help you measure your organization's ability to respond rapidly and effectively to a DDoS attack.

Table 3-3 Reaction Plan

Criteria	✔
Our DDoS response team performance falls within response times defined by corporate policy, and we have tested our response performance to ensure compliance.	
Our DDoS response team is available 24/7 in the event of a DDoS attack; we have a tiered backup procedure to engage in the event that initial responders are unavailable.	
Our DDoS response team has the expertise to accurately identify the current DDoS attack vector and knows what to do when various DDoS attack vectors change.	
Our DDoS response team can clearly articulate to management the current DDoS attack that we are experiencing, outline the threat to the business, and recommend mitigation steps.	
Our DDoS response team can identify specially crafted packet attacks and optimize our defenses to block these types of DDoS attacks.	
Our DDoS response team can analyze the size and nature of a DDoS attack.	
Our DDoS response team is able to immediately engage our ISP contact list in the event that the DDoS attack vector is a bandwidth-saturating, network-level DDoS attack.	

(continued)

Table 3-3 *(continued)*

Criteria	✔
Our DDoS response team can identify sources of network-level DDoS attacks and engage our ISP(s) to block attacking sources upstream.	
Our DDoS response team can analyze alerts, logs, reports, and forensics to determine what services, applications, and/or devices are the victims of a DDoS attack.	
Our DDoS response team can detect outbound DDoS attacks that could possibly cause our ISP to black-hole route our subnet to protect other customers.	
Our DDoS response team can optimize requestor behavioral analysis defenses on-the-fly as we come under varying application-layer DDoS attacks.	
Our DDoS response team can identify various DNS attacks and optimize our perimeter DNS defense mechanisms.	
Our DDoS response team is continuously trained in the types of DDoS attack mitigation techniques that will reduce and/or eliminate the negative effects of a DDoS attack.	

Containing an attack

Containing an attack and mitigating or controlling any potential damage is the primary objective when faced with an attack. However, unlike many other types of security incidents — such as a virus infection or a data leak, for example — containing a DDoS attack shouldn't mean shutting down the system or disconnecting it from the network. After all, that is the attacker's ultimate objective: denial of service!

Unfortunately, that is exactly the DDoS attack response for many ISPs — shutting down access to the targeted system or network, also known as *sacrificing the victim* to preserve the service provider's bandwidth and protect other customers. Check your SLAs (Service Level Agreements)! Most ISPs reserve the right to shut down your network or systems in order to contain a DDoS attack against your organization. You need to fully understand the business and legal consequences — and the rights of your organization — in such an event.

When dealing with a virus infection or data leak, after isolating the affected systems and controlling the spread of damage, an incident response team may turn their efforts to restoring lost data, assessing damage or unauthorized disclosures, collecting evidence, analyzing logs, and reconstructing the event.

By contrast, the goal of DDoS response is to restore service as quickly as possible without subjecting the organization to further attacks or exposing it to other security threats — instead of engaging in an all-hands-on-deck scramble that may disable other security protections. For example, if an IPS custom attack signature for a new attack "in the wild" is improperly configured, an excessive number of false positives may result in a self-inflicted denial-of-service. A natural — but bad — panicked reaction might be to pull the IPS out of production, thereby leaving the entire network unprotected.

DDoS attacks are increasingly directed against high-profile targets. These attacks are intelligent, focused, and persistent. Today's DDoS attacks are perpetrated by a new breed of highly capable cybercriminals who quickly switch to different attack sources and alternative attack methods as each new attempt is countered or fails. A DDoS response plan must therefore be flexible and adaptive, and should clearly define when and how additional mitigation resources are engaged and surveillance tightened.

Best Practices for Effective DDoS Defense

Implementing your DDoS incident response plan is by far the most important step you must take to protect your organization in the event of a DDoS attack. Everything else you do depends on it. In addition to your DDoS response plan, here are some essential best practices that will help keep your business up and running and help you and your executives sleep better.

Maintain continuous vigilance

DDoS attacks are becoming increasingly sophisticated and stealthy. Don't wait for your network or critical business

applications to become unresponsive before taking action. You're probably already monitoring your network for performance issues, traffic optimization, load balancing, and other important events. Your network operations personnel should be trained to look for signs of DDoS rather than assume a sluggish or unresponsive server is the result of hardware or application issues, or simply a temporary traffic spike.

Put your network team on the alert! They will respond slowly to a DDoS attack if they're not conditioned to look for it and know what to look for (see "Learn how to detect and understand a DDoS attack" in this chapter).

For optimal defense, a DDoS early warning system should be part of a company's solution. Continuous and automated monitoring is required in order to recognize an attack, sound the alarm, and initiate the response plan.

Protect your DNS servers

The Internet Domain Name System (DNS) is a distributed naming system that enables you to access the Internet using recognizable and easy-to-remember domain names (such as `www.google.com`) rather than numeric IP addresses (such as 192.168.0.1). Because DNS is distributed, many organizations use and maintain their own DNS servers in order to make their systems visible on the Internet.

DNS servers are often targeted by DDoS attacks, for example, by launching many DNS requests to flood a targeted name server. If an attacker can successfully disrupt DNS services, all the victims' servers could essentially disappear from the Internet, thereby causing the desired denial of service.

Maintain at least the same levels of vigilance and protection for your DNS servers as you do for your web application servers and other critical components of your IT infrastructure. Make sure your incident response team has a thorough understanding of DNS and your DNS environment. Finally, if you're using an outside DNS service, determine what your provider is doing to protect against DDoS. (There have been several successful attacks against major DNS providers, forcing their customers offline in the process.)

Learn how to detect and understand a DDoS attack

A brute-force or flooding type of DDoS attack is relatively easy to spot. For example, using the `netstat -na` command on a system will display TCP/IP-related connection information. Figure 3-1 illustrates the use of the netstat command and shows a SYN flood attack occurring against port 21 (FTP, file transfer protocol) on the system (note the connections marked SYN_RECEIVED without any corresponding SYN_ACK messages).

```
C:\>netstat -na

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:53             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    192.168.253.22:21      13.204.86.120:48314    SYN_RECEIVED
  TCP    192.168.253.22:21      18.110.83.12:48314     SYN_RECEIVED
  TCP    192.168.253.22:21      21.148.77.12:48314     SYN_RECEIVED
  TCP    192.168.253.22:21      22.142.166.91:48314    SYN_RECEIVED
  TCP    192.168.253.22:21      28.167.128.155:48314   SYN_RECEIVED
  TCP    192.168.253.22:21      59.45.34.100:48314     SYN_RECEIVED
  TCP    192.168.253.22:21      76.58.55.86:48314      SYN_RECEIVED
  TCP    192.168.253.22:21      76.114.111.97:48314    SYN_RECEIVED
  TCP    192.168.253.22:21      80.190.204.244:48314   SYN_RECEIVED
  TCP    192.168.253.22:21      81.28.131.157:48314    SYN_RECEIVED
  TCP    192.168.253.22:21      85.64.198.218:48314    SYN_RECEIVED
```

Figure 3-1: Using netstat to view network connection information.

There are a number of other free (or very inexpensive) tools available for IT staff to investigate initial indications and confirm suspicions of a possible DDoS attack. These include command line utilities, log files, and network protocol analyzers. Figure 3-2 shows an example of Wireshark, a very popular (and free!) network protocol analyzer.

Know your customers

For any of these tools to be effective, IT staff must know how to use them, and they need to know what normal traffic looks like so they know when something isn't right!

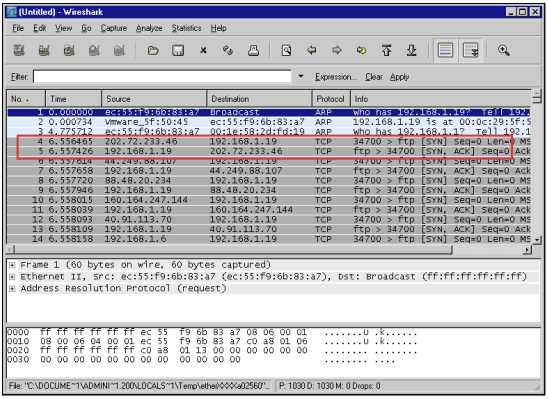


Figure 3-2: Wireshark allows you to capture and analyze network traffic.

Detecting and blocking more insidious application-layer DDoS attacks while simultaneously allowing legitimate traffic requires more sophisticated real-time analysis, and a thorough understanding of the typical behaviors and actions of bona fide customers or employees accessing the applications that are being protected. In much the same way that credit card fraud detection can be automated, on-premises DDoS defense systems establish legitimate usage profiles in order to identify suspicious traffic and respond accordingly.

Deploy an on-premises DDoS defense solution

On-premises DDoS defense solutions installed immediately in front of application and database servers provide a granular response to traditional network-layer DDoS flooding attacks, as well as increasingly frequent application-layer DDoS attacks. For optimal defense, on-premises DDoS protection solutions should be deployed in concert with automated monitoring services to help you rapidly identify and react to evasive, sustained DDoS attacks. Learn more about on-premises DDoS defenses in Chapter 4.

Chapter 4

Your Best Protection: On-Premises DDoS Defense

In This Chapter

- Understanding Corero's 3DP approach for combating DDoS attacks
- Recognizing the importance of robust hardware and software

Although no single approach provides absolute security, on-premises DDoS defense is an essential component of your security infrastructure. Other approaches to DDoS defense are incomplete and, in some cases, introduce additional risk (for more on this, see Chapter 2).

In this chapter, I introduce you to Corero Network Security's DDoS Defense System (DDS). An on-premises security solution, such as Corero's DDS, is the best way to protect your organization's network and systems from distributed denial-of-service (DDoS) attacks.

On-Premises 3DP Protection against DDoS

You need to deploy a security solution that effectively addresses all DDoS threats — at the gates to your enterprise. An on-premises solution provides precise and immediate detection and mitigation of both network-layer and application-layer DDoS attacks. On-premises solutions give you complete control over DDoS detection and response based on your policies, business practices, and application environment.

Corero's DDS uses an integrated, mutually reinforcing approach to network security with its Three Dimensional Protection (3DP), which provides protection against DDoS attacks, undesired access, and malicious content.

Corero DDS combats DDoS attacks ranging from traditional network floods to newer low-and-slow application-layer attacks that don't show up on bandwidth radar screens. The three dimensions of 3DP encompass patented DDoS defense algorithms and extensive rate-based protection mechanisms, stateful firewall filtering, and malicious content protection (see Figure 4-1).

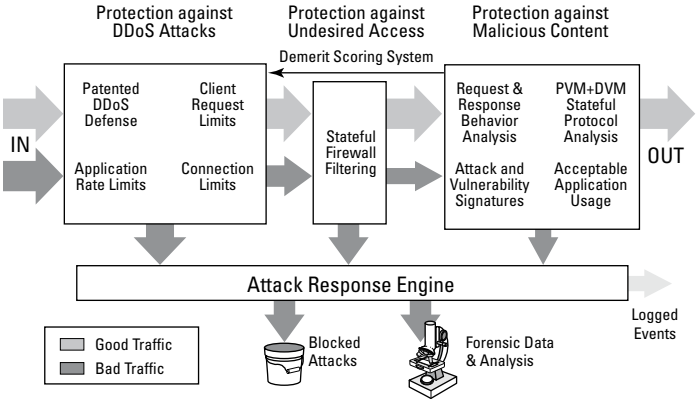


Figure 4-1: Corero's 3DP technology is optimized for DDoS defense.

Based on intelligent behavioral analysis, Corero DDS uses an adaptive, patented DDoS defense algorithm to ensure business continues as usual — blocking malicious incoming requests while passing legitimate traffic to the company's protected servers. This system debits a DDS-maintained *credit balance* associated with each source IP address and blocks further requests from an IP address when the credits are depleted.

Every client connection is assigned a positive credit balance when a session is initiated. Each connected client earns additional credits each minute for good behavior. As long as there are credits available, the client can initiate new transactions through the DDS.

Online gaming site holds winning hand against DDoS extortion threat

An online gaming site that handles predominantly sports-related wagers was recently targeted as part of an increasingly disturbing trend: In the recent past, other similar sites had paid the ransom to avoid the threatened attack. This site decided not to become a victim.

Online gaming site customers place wagers on sports events and play online games, such as poker and blackjack. Typical users of these sites have little loyalty and don't build up equity with a particular site. Providing rapid response, quick payouts, and very good service are vital to customer retention. The site must be available and responsive, particularly during periods of increased wagering such as weekends and high-profile sporting events.

Customers must be able to bet immediately and in real-time, especially given the highly volatile nature of the line or spread. If a site isn't available, the bettor will quickly go to another site.

Highly organized criminal blackmailers seem to understand the online gaming business well. They have devised attacks with a well-considered economic and technical approach, and their timing demonstrates a keen understanding of this particular industry's metrics.

The Threat

The perpetrators initially unleashed a warning attack against the site to provide credibility for their threat. With the Thanksgiving holiday weekend approaching, a peak revenue period for the site was in jeopardy. The initial attack was followed with a demand threatening a full attack unless a ransom fee was wired to an intermediary. The attackers were aware that:

- Typical mitigation solutions would cost approximately twice the amount demanded and take longer to deploy than the attack window
- A peak time of revenue generation was imminent
- Existing in-place technology for the site could not thwart the attack

The Solution

The online company responded to the threat by contacting Corero Network Security prior to the ransom deadline and installing a Corero security appliance.

Having not received their ransom, the attackers unleashed their full attack on Thanksgiving morning. The Corero appliance successfully fended off the attack, consisting of distributed SYN floods and UDP floods, and the gaming site was able to stay up and operational. Realizing they were not having an impact, on Saturday the attackers unleashed a maelstrom of attack methods — but they were holding a losing hand.

For each good request from the client, credits are debited. Good clients can make a lot of good requests, but are still constrained by policy-based rate limits.

But bad behavior from a connected client will quickly result in that client being blocked by DDS. For example, if a client makes repeated HTTP GET requests to the same web page or server object, or multiple DNS requests that result in error responses, many credits are debited. Repeating such requests will result in the client credit balance going to zero, and all new transactions from that client will be blocked until new credits are earned.

This is essential protection for e-commerce and other business-critical web services. By tracking the behavior and evaluating the threat level associated with each client, Corero DDS automatically applies the appropriate treatment to each new transaction, allowing a business's real customers to access the desired services even during an active DDoS attack.

Corero's DDS also monitors and analyzes outbound traffic to effectively detect and mitigate possible attacks coming from compromised computers within your network.

Corero's DDS:

- Automatically detects and mitigates both traditional network layer DDoS attacks and more advanced application layer attacks.
- Protects your network, allowing legitimate communications to pass without delay even while under attack.
- Enables business continuity, allowing your customers to keep receiving quality service.
- Leverages Three Dimensional Protection (3DP) to provide network and application layer DDoS defense, protection against undesired access, and protection against malicious content.
- Provides low latency and high throughput, even while under attack, meaning no network interruption and no service degradation.

- Offers absolute reliability with purpose-built hardware featuring redundant power supply, a rating of 20-to-30-years mean time between failure, no rotating media, and no chip fans.
- Advanced clustering capability and dramatically increased performance through Corero's ProtectionCluster, which allows scalable, transparent deployment in all redundant networks, even those with asymmetric routes.
- Presents an intuitive user interface that facilitates real-time incident response.
- Monitors outbound traffic with its bidirectional inspection and granular security policy controls.
- Thwarts reflective DDoS attacks with its inherent stateful firewall capabilities effectively blocking midflow attacks.
- Detects and mitigates specially crafted packet denial-of-service attacks with its inherent stateful protocol analysis capabilities.
- Detects and blocks server-targeted malware and other remote exploit attempts with its built-in protection against malicious content.

When used as part of a best practice DDoS defense strategy, Corero's DDS sets the gold standard and enables your organization to continuously assess risk, protect against DDoS attacks and malicious code, detect and prevent intrusions into your network, monitor your security posture, and alert key personnel of important security events.

Latency: The Self-Inflicted DOS attack

One paradox of many enterprise security solutions available today is that they introduce latency in the very networks they're deployed to protect. The deep packet inspection and analysis of good and bad network traffic performed by these

security devices often creates a bottleneck in the network — in effect, a self-inflicted denial-of-service attack that can degrade your network's performance.

First-class security solutions are effective, robust, and reliable. Corero's DDS solutions are built on the Core Platform — comprised of powerful Tilera 64-core processors and the CoreOS — to deliver cohesive and integrated network security solutions with low power consumption, a hardened operating system, and the lowest network latency in the security industry (see Figure 4-2).

Brady Distributing Company says "game over" for DDoS

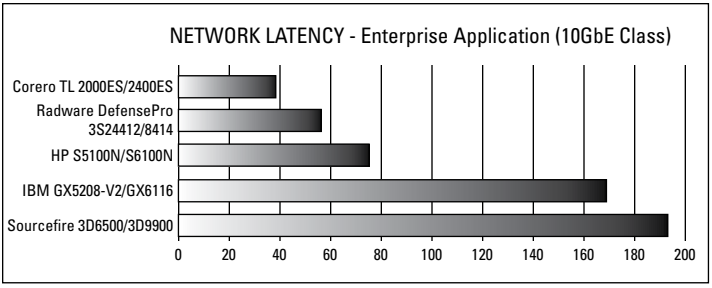
Brady Distributing Company provides sales and service of jukeboxes, amusement games, and vending machines, serving customers that range from individual homeowners with arcade-style game rooms to large amusement companies like Incredible Pizza and Walt Disney World. Based in Charlotte, North Carolina, Brady is the second largest company in its vertical market.

Brady Distributing relies heavily on the Internet, thus DDoS, as well as malware, is disruptive to the business. Rick Baird manages Brady Distributing's IT department. Baird selected Corero Network Security's solution for its Three Dimensional Protection and installed it in the company's Charlotte data center. "Straight out of the box, Corero's differentiated solution had a lot of capabilities, such as protection against distributed denial-of-service (DDoS) attacks, stateful firewall filtering, and protection against botnet attacks," says Baird.

Looking toward the future, Brady Distributing will soon host a new e-commerce website. "About 5 percent of our business comes from online orders today, but we expect that to grow to 15 to 20 percent of our business once the new application is in place. This business would be worth millions of dollars to the company," says Baird. If something like a DDoS attack were to disrupt access to the website, Brady Distributing could lose significant revenue.

But this isn't a concern, as Brady Distributing's infrastructure is now secure.

"The issues we had prior to installing this solution have virtually disappeared," says Baird.



Network Latency, uSec (Values taken from respective vendor datasheets April 2011. Value shown represents average of typical latency for two 10GbE appliances {one 4-6 Gbps class} from each vendor)

Figure 4-2: Corero DDS's proven hardware platform delivers the lowest latency.

Corero's DDoS Defense solutions have the lowest latency in the industry, with all models introducing less than 60 microseconds of network delay, which is especially critical for enterprise networks that are rich with data and voice traffic.

Building on the flexible and powerful Core Platform, Corero has developed DDoS Defense (and IPS) products around a common service suite and architecture.

The ingenuity of the Core Platform lies in an extremely powerful, yet elastic and flexible hardware appliance upon which Corero software developers have integrated a network security-specific hypervisor, which performs essential network security processing functions, including deep packet inspection and policy control.

The Tilera processors provide the scope for the versatile assignment of one or multiple cores to execute specific security functions. Instead of being constrained by the hardware, the Tilera architecture enables Corero's world-class developers to rapidly create DDS solutions purely in software, delivering rich and complex functionality with high throughput and unparalleled low latency.

CoreOS is the software portion of the Core Platform, providing the essential foundation capabilities for network security processing, including packet handling, deep packet inspection, and policy management.

These three tightly integrated functional areas combine to perform the functional heavy lifting, and utilize a performance-oriented abstraction layer at the heart of CoreOS that "talks" directly to the mesh of 64 cores, leveraging Tilera's unique processing capabilities to minimize latency and maximize throughput.

By virtue of this architecture, Corero developers are provided granular control to assign optimal processing power from the 64 processor cores. They can also address targeted capabilities and their component application functions according to the requirements of the particular product.

So, Corero DDoS Defense products require heavy emphasis on rate management to throttle the flow of attack traffic and allow legitimate traffic to flow freely, but still require packet analysis to differentiate between good and bad traffic.

Chapter 5

Eight Benefits of Corero's DDoS Defense System

In This Chapter

- Covering everything
- Reaping the benefits of an on-premises DDoS solution

In this chapter, I discuss Corero's DDoS Defense System (DDS) and why it's a great choice for protecting your business and the stability of your computing and network infrastructure.

Comprehensive DDoS Protection

DDoS attacks can cripple your online business, costing you money, disrupting operations, and driving away customers. Traditional security technology, such as firewalls and IPS, fail to deal with DDoS, and anti-DDoS services are, at best, incomplete solutions.

Corero's on-premises DDoS Defense System (DDS) provides the most comprehensive protection available against all types of DDoS attacks. DDS is the only solution that can effectively detect and mitigate DDoS attacks without risk, while allowing your business to continue operating at normal performance levels.

Corero enables you to tailor your DDoS defense to your unique environment, based on your IT infrastructure, application traffic, policies, and business goals.

DDS is the best solution to protect your organization against extortionists, unscrupulous competitors, hacktivist zealots, and dangerous mischief-makers.

Expert, Continuous DDoS Defense Service

Attack techniques are always evolving. DDoS attacks include traditional network-layer flooding and newer, more insidious application-layer attacks that target an organization's most critical applications on public-facing Internet websites.

Your security vendor should partner with you to ensure your success by helping you implement your security solution for your particular business requirements and network infrastructure. It should also help you maintain that solution throughout its lifecycle and respond quickly to an attack when it happens.

Corero's SecureWatch PLUS service provides a combination of a powerful on-premises DDoS product and specialized DDoS defense services, tailored to each customer's specific needs. The service encompasses three stages:

- **Preparation:** Configuration of DDS based on business requirements, corporate policy, and DDoS defense best practices; development of an incident response plan.
- **Vigilance:** 24/7 monitoring to deliver real-time alerts to the customer and Corero Security Operations Center.
- **Response:** Immediate response to an attack, continuous engagement until final resolution, and post-incident assessment.

Proactive, Automated Updates

No matter what security solution you choose to implement, it will require constant updating from a security vendor that has the focus and expertise to protect you from new and evolving threats.

Threat Update Service is an automated protection service that provides Corero's customers with proactive protection and ongoing mitigation of security issues. Threat Update Service

delivers frequent protection pack updates that include data about badly behaving IP addresses (collected from thousands of sensors across the Internet), security advisories about newly discovered threats, and updated vulnerability and attack signatures.

Robust Performance

If your network is moving too slowly, that's almost as bad as it not working at all. Latency and poor performance can create a self-inflicted denial-of-service in your network. Security solutions that aren't purpose-built to handle the high volumes of traffic that arrive with a network-layer DDoS attack — or to analyze more stealthy and CPU-intensive application-layer attacks — can slow your network and servers to unacceptable levels.

Corero DDS is a high-performance switchlike device that doesn't disrupt latency-sensitive applications such as VoIP. It also ensures speedy response times for all applications. Corero's Core Platform, based on Tilera multicore processors and CoreOS software, provides real-time protection at real-world performance levels. Corero delivers in line protection while minimizing latency.

Scalable, Transparent High Availability

Network security solutions require robust deployment options for high availability, scalability, and flexibility.

Corero's ProtectionCluster is a proprietary load sharing technology that can be deployed in configurations of up to eight parallel units to assure nonstop availability and increased throughput and defense capability with each additional unit in both standard and asymmetric redundant network configurations.

Easy, Customizable Deployment

An on-premises DDoS defense solution provides the flexibility to deploy and manage your network in accordance with your organization's established policies.

With highly flexible policies, the Corero DDS solution can be deployed at any number of key areas in your network infrastructure, providing perimeter security, protection of critical servers, remote access and extranet entry points, and inter-departmental segmentation. Corero provides powerful DDS management through an easy-to-use interface.

Real-Time Incident Response

Correlating and analyzing events from multiple security devices can make it extremely difficult to get a complete picture of an impending or ongoing attack.

Corero's Network Security Analyzer provides security event management, real-time alerting, and flexible reporting. It saves time and effort in normal day-to-day security monitoring and incident response, and features:

- Contextually-aware, high-level alerting
- Compliance audit lifecycle management
- Enterprise-wide IPS security intelligence
- Real-time monitoring and correlated alerting

Corero's Attack Response Engine includes a built-in real-time Security Event Viewer that allows users to drill down and identify attackers, victims, and types of attacks, then take immediate action to block or mitigate the threat. In addition, it uses a flexible event-logging format for integration with leading security information event management (SIEM) tools.

Green Design

These days, green design is important in any aspect of technology. When buying new items for the data center, your company needs to think about not just how much it costs to buy, but how much it's going to cost to use.

The energy-conserving design of Corero DDS requires only 1RU of rack space for most models, and has low power consumption. DDS fits right in with initiatives to reduce space, electricity, and cooling requirements in the data center.

Stop DDoS attacks before they cripple your online business

DDoS For Dummies, Corero Network Security Edition, arms you with the knowledge and the understanding you will need to defend your networks against the growing Distributed Denial-of-Service (DDoS) menace. Discover how and why DDoS attacks have emerged as one of today's leading cyberthreats.

- ***Understand the threat* — find out how different DDoS techniques slow networks and web servers to a crawl, then a halt**
- ***Know the enemy* — learn the motives for the crime including extortion, politics, and competitive greed**
- ***Formulate the plan* — prepare your DDoS response strategies and tactics so you'll be ready to counter any attack**
- ***Deploy the solution* — discover how Corero's DDoS Defense System (DDS) thwarts all types of DDoS attacks and keeps your business running**

Open the book and find:

- **The lowdown on insidious, hard-to-detect application-layer DDoS attacks**
- **The blueprint for a comprehensive DDoS response plan**
- **Options for defending your networks**
- **Stories about businesses like yours that took on DDoS and won**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

For Dummies®
A Branded Imprint of
WILEY

ISBN: 978-1-118-18253-6
Not for resale