
Securing the
Borderless Network
Security for the
Web 2.0 World
ciscopress.com
Tom Gillis

Securing the Borderless Network

Security for the Web 2.0 World

Tom Gillis

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing April 2010

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58705-886-8

ISBN-10: 1-58705-886-3

Warning and Disclaimer

This book is designed to provide information about the challenges and benefits of creating a secure information network. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests.
For more information, please contact: U.S. **Corporate and Government Sales**
1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States, please contact: **International Sales**
international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Patrick Kanouse

Senior Project Editor: Tonya Simpson

Editorial Assistant: Vanessa Evans

Book Designer: Louisa Adair

Composition: Mark Shirar

Cisco Representative: Erik Ullanderson

Cisco Press Program Manager: Anand Sundaram

Technical Editors: Fred Kost and Patrick Peterson

Copy Editor: Apostrophe Editing Services

Development Editor: Deadline Driven Publishing

Indexer: Ken Johnson

Proofreader: Sheri Cain

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Foreword

"I have been impressed with the urgency of doing. Knowing is not enough; we must apply. Being willing is not enough; we must do."

—Leonardo da Vinci

One fascinating aspect about technology and information security and assurance—if not the most fascinating aspect to me—is that problems and questions seemingly always come before solutions and answers, and the answers oftentimes prove quite elusive. It's like playing a game of chess where strategy, tactics, and time horizon connect, and you find yourself facing a skilled opponent who knows your weaknesses, and how to exploit them. This intellectual challenge of move/counter-move is energizing and exhausting, yet is never the same two days in a row. We face a seminal moment right now, today, in behavior and practice.

Within the past two decades as a practitioner in the Internet Age, I've observed four distinct eras that, in totality, represent the information security art form: Perimeter Security (Era I), Mobile Security (Era II), Application Security (Era III), and now Collaboration Security (Era IV). During the first three, exploitation speeds shortened, electronic crime became its own market, and layered technology became the defense—and also our weakness. And yet, the basic tenets for information security practitioners worldwide were the same—confidentiality, integrity, and availability.

It's time to add trust to the model.

This fourth era, Collaboration, is at least an order of magnitude more complicated to solve. The defense process is quite different and does not naturally build on past, and more traditional, practices. Information today is never simply "in" one physical or logical place. It is available for fast access, and its very location may not be well understood—it might be local, remote, in the data center, in the cloud, on the Web, on P2P, composed from multiple locations—and the list continues. It also may be on a PC; it may well be on a phone, a heads-up display, a television, or something that isn't invented yet.

We also became reliant on technology…somewhere in those 20 years.

Today, we are seeing signs that existing practices are fragile. Antivirus vendors are overwhelmed with malware, IP scanning doesn't work for broad IPv6 networks, and patching is nearly impossible because networks and infrastructures must support 7×24 operations. Our online world is viral, with more than 1.5 billion people around the world connecting, and the systems that support them are increasingly brittle, fragile, and vulnerable to disruption, corruption, and exploitation.

Plainly speaking, the information security art form, as we've practiced it for two decades, is inadequate for the threats we are facing today, especially when juxtaposed against how we are using the networks and technology in our daily lives. Perhaps that's why you are reading this book: Have you come to similar conclusions?

However, all is not lost. I find myself remembering a hobbit from *Lord of the Rings* saying, "Certainty of death, small chance of success…what are we waiting for?" Today and tomorrow's economies will base themselves upon cost-efficient, quality services where first-to-market globally defines the opportunity. It has also been stated that Web 2.0 and Security cannot co-exist and are, in fact, at odds.

I say, provided we have the courage to change course, and the conviction to believe, security as we know it will fundamentally change to face this new reality.

For our digitally connected world, the major influences for tomorrow's information security practices revolve around three important themes: technology evolution (in the forms of collaboration, virtualization, and automation), mobile user communities, and threat (both complexity and speed). Threat is at the list's end because it always seems that we focus on that first when, in fact, arguably it ought to be at least after we define what is valuable.

Mobile, connected, Web 2.0-enabled worlds are going to happen, and in some cases already have—whether we think we can allow them to or not. The human desire to communicate took a radical turn here, and it is fundamentally changing how we live, work, play, and learn. We need to adapt, as methods, not motives, are what need our full attention right now. This book seeks to do that and then provide ideas and answers to the problems it raises.

So turn the page…and as da Vinci observed, be more than willing, and "do."

John N. Stewart
Vice President, Chief Security Officer
Cisco Systems, Inc.

Introduction

In the 1880s, the advent of the railroad spurred the manufacturing economy. The railroad's capability to distribute raw materials and finished goods efficiently unlocked a century of economic growth.

In the 1980s, a similar revolution began with the introduction of the personal computer, the network, and the World Wide Web. These inventions unlocked the information economy, and we're still harnessing the full efficiencies and potential of this information economy. As with any economic development, up and down cycles, dotcom booms, and recessionary busts occur. But from a historical perspective, the opportunity for growth driven by continued refinement of the tools of the information economy has never looked brighter.

Imagine a business world in which information is efficiently available in the palm of your hand, with anywhere, anytime access. A good idea at 7 p.m. on a Saturday can be captured and efficiently shared with no friction. That world is here, and it involves some significant changes to the way we access and safeguard our valuable information.

Change creates winners and losers. The basic principle of Darwinism suggests that it is not the strongest species that survive, nor the most intelligent, but the one most adaptive to change. Change is flooding in to the corporation, driven by second- and third-generation web apps and handheld computing devices built first for consumers but irresistible to business users. Some companies have found ways to embrace these new techniques, whereas many others attempt to prevent their use.

For example, a national insurance company blocks its employees from using social networking websites and instant messaging—and finds that its policies are driving away younger employees who are hooked on Facebook and Twitter.

A U.K.-based marketing agency prevents its workers from using Google Docs, the popular online document-sharing application—and nearly started an uprising among employees who insisted they needed Google Docs to work with clients and finish projects on time.

Fearing data loss and security compromises, a healthcare provider in the Midwest wants to limit its practitioners to BlackBerry devices when they're working in the field—but their practitioners are pleading to use the Palm Pre or iPhone, which the provider doesn't support.

The wave of new collaboration and mobility technologies promise to change the way we do business and in the process create new efficiencies for businesses large and small. But with the new computing freedoms come new risks. The IT team is caught in the middle of two powerful countervailing forces: One is tearing down traditional enterprise borders, and the other is building those borders higher.

On one hand, new trends such as mobility and handheld computing are changing the way we think about enterprise computing. These always-on devices drive huge gains in productivity. At the same time, the rise of Internet-based collaboration techniques such as social networking, wikis, and high-definition video conferencing systems enable workers

to share information more freely than ever before. Anyone who has joined a Cisco WebEx session from his iPhone can speak to this efficiency directly.

These new technologies are being pushed into the enterprise by enlightened managers who look to gain competitive advantage, or are being pulled in by workers who have used iPhones and Facebook at home and consider them basic tools required to get their jobs done. All these new trends are leading to more people accessing more data residing at more places on the Internet from more types of devices than ever before. This is driving a movement of openness in the enterprise, a trend we call the borderless network.

On the other hand, malware is getting more sophisticated, more malicious, and more difficult to detect than ever before. New technologies such as social networking sites, and a growing realization that employees need to mix some personal traffic with business traffic, are forcing companies to reevaluate their acceptable-use policies. And increasingly, companies are looking for ways to protect their sensitive data, either for regulatory compliance or to safeguard their most precious asset: information. These trends are driving the need for tighter security, or a move toward the closed enterprise.

And the IT team is often in the unenviable position of needing to restrict the business from operating efficiently, resisting new technologies and making users frustrated and angry—when the real value of IT is to become an enabler of new business efficiency.

When I visit with customers of Cisco and IronPort and ask them what their biggest security headaches are, they typically produce smartphones from their pocket, and say, "This." They're worried about workers accessing data on devices they feel they can't fully protect. And they know that this revolution is steamrolling ahead, whether they're ready for it or not.

The borderless network cannot be stopped because it is creating real competitive advantage for companies. At Cisco, the widespread use of its TelePresence high-definition conferencing system has cut the company's travel costs by more than $200 million and has increased the flow of critical information. Statistics like this cannot be ignored.

Although the tools of collaboration and information sharing are changing rapidly, so must the tools of security and policy enforcement change. These tools need to enable the IT team to embrace new technologies and at the same time increase safeguards over valuable information. IT departments must be enablers of new efficiencies and competitive advantage, not inhibitors. Wouldn't it be nice if the IT team could say, "Yes—use your iPhone," instead of always saying no? After all, everyone wants to be loved, even the poor IT team.

In the following chapters, we examine businesses that have embraced these new ways to collaborate and communicate, even as they acknowledge the security pitfalls. We explore the technologies that are revolutionizing business and the threats that have sprung up in the wake of these innovative solutions. And we learn how these threats are being corralled and managed, freeing workers to collaborate with confidence, no matter where or when—or with what technology—they choose to connect with each other.

How This Book Is Organized

This book begins by examining how Web 2.0 technologies are dramatically changing the way we work—and how we must think about network security. You learn about the challenges and threats today's businesses face as they struggle to fully embrace the value of mobility and Web 2.0 without sacrificing enterprise security. The book closes with a discussion about the intelligent, intuitive technology required to secure the emerging borderless enterprise.

- **Chapter 1, "Network Security—Yesterday, Today, and Tomorrow"**—Security was simpler when the security perimeter was a well-defined, defensible zone. But Web 2.0, mobility, and handheld devices have changed that. This chapter briefly examines the history of network security, including the evolution of firewalls, and asks the question, "Where do we go from here?"
- **Chapter 2, "Collaboration and Web 2.0 Technologies"**—This chapter discusses how collaboration and Web 2.0 are enhancing productivity and having a profound impact on organizations of all sizes; why easy online collaboration is transforming how people work together; the growth of enterprise-level online collaboration tools; and storage and applications in the cloud.
- **Chapter 3, "Building Relationships with Web 2.0"**—This chapter explores how one industry—financial services—is using Web 2.0 technology, such as social networking, to strengthen customer relationships, build new business, and streamline internal communications to create a more connected workforce.
- **Chapter 4, "The Cloud Computing Revolution"**—This chapter examines how two manufacturing companies use hosted, web-based CRM applications to streamline operations and create an environment for fast, seamless collaboration.
- **Chapter 5, "You're in San Jose, I'm in Bangalore—Let's Meet"**—This chapter examines the new generation of collaboration technologies, such as Cisco TelePresence and WebEx, that enable people to conduct virtual meetings from almost any point on the globe.
- **Chapter 6, "Watson, Can You Hear Us?"**—This chapter offers a brief history of communication and computing tools that have dramatically enhanced our connectivity and mobility—from Bell's telephone to the Osborne luggable to the Apple Newton to today's smartphones, including the BlackBerry and iPhone.
- **Chapter 7, "The Consumerization of IT"**—This chapter explores how there is growing demand in the enterprise both for, and for the acceptance of, new computing tools that first gain popularity in the consumer space. What impact is this trend having on security policies and the workforce?
- **Chapter 8, "The Bad Guys from Outside: Malware"**—Today's malware is smarter and harder than ever to detect. This chapter explains how malware creators ply their trade and examines the dangers that malware poses to enterprise security.

- **Chapter 9, "Who Are These Guys?"**—This chapter offers a deeper look into the world of online criminals and discusses how their business and economic models are constructed.
- **Chapter 10, "Signs of Hope"**—This chapter examines the signs that the "good guys" are succeeding in their battles to thwart online criminals. Security vendors use antimalware technologies and techniques that harness the power of the network and take advantage of processing power improvements.
- **Chapter 11, "Acceptable Use Policies"**—This chapter explains how the consumerization of IT and the growing popularity of handheld mobile devices are forcing companies to move away from antiquated notions of *how* employees should do their work. Meanwhile, management and IT leadership struggle to create realistic, enforceable acceptable use policies for the Web 2.0 world.
- **Chapter 12, "The Realities of Data Loss"**—This chapter explores this question: Given that the data loss problem is snowballing and compliance does not assure security, is data loss prevention even feasible? The answer: Yes and no. First, an organization must recognize that it cannot protect all its data. Second, it must realize that it doesn't need to.
- **Chapter 13, "Collaboration Without Confidence"**—This chapter pulls together discussions about security challenges highlighted in previous chapters and includes insight into how businesses are struggling to find ways to enable employees to harness the power of Web 2.0 tools and fully embrace mobile devices without compromising security.
- **Chapter 14, "Identity Management: We Need to Know if You Are a Dog"**—The ability to differentiate between individual users on a network and their levels of access and control is critical in today's computing environment. This chapter discusses how user identity is becoming a core element of enterprise security.
- **Chapter 15, "Security for the Borderless Network: Making Web 2.0 and 3.0 Safe for Business"**—Companies must accept that the Web 2.0 world is already here—and Web 3.0 is emerging. This concluding chapter discusses the secure borderless network and the need for intuitive security that is widely distributed throughout the network to enforce policies effectively. Also discussed is the Cisco vision to create an interface between policy and enforcement systems that is open and built on industry standards.

Chapter 8

The Bad Guys from Outside: Malware

This chapter includes the following topics:

- Modern Malware Overview
- Finding the Weak Points
- Social Engineering for Success
- Spamming and Phishing Get Targeted
- Profit Motive

Along with acceptable use policies (AUP) and data loss prevention (DLP), malware, or malicious software, is one of the three critical areas that enterprise security policies must address. Malware is pervasive, painful, and expensive to detect and block.

Malware has been part of computing for decades. In the 1990s, it got onto your computer or network when you stuck an infected floppy disk into your drive, or when a clever hacker gained access to your network. Then, with email becoming more prevalent, hackers designed malware to spread as infected email attachments. Today, the Internet is a fantastic distribution mechanism for malware.

In this chapter, you can find out how malware works and why it presents such a threat to the enterprise. In addition, you learn about the newest sophisticated tactics that malware creators use to trick computer users into downloading their wares.

Modern Malware Overview

Malware, which is malicious software that infiltrates computers, networks, and mobile devices, is part of life in the information age. Malware is sent via email, spreads via portable media storage and drives—such as CDs, USB drives, and MP3 players—and can secretly download onto your computer from websites you trust.

Today, the primary distribution mechanism for malware is the World Wide Web. Malware is served not only from entirely malicious, fraudulent websites but also legitimate websites that have been compromised.

One way in which malware has changed over time is that it's a lot smarter and harder to detect than before. This makes it very difficult to get it out of your systems after they are infected. But malware still depends on vulnerabilities in technology—and weaknesses in human nature—to infiltrate computers and networks.

And hackers aren't trying to get malware onto your computers just for fun, or to see how far they can spread the code they wrote. Modern malware is a for-profit, big-business undertaking. Online criminals invest significant amounts of money and time in more efficient malware and better malware distribution mechanisms because they know the financial rewards can be enormous.

Types of Malware

The original email–propagated viruses, such as the circa-2000 Melissa or I Love You viruses, did not do much besides slow down the performance of your computer and your network. They soaked up bandwidth and processing power by sending copies of themselves to millions of people. This type of malware was created primarily to enable its authors to show off their "development" skills. For David Smith of New Jersey, the author of the Melissa virus, the erstwhile use of his computer skills backfired; following a tip from an AOL employee to law enforcement, Smith ended up spending 20 months in prison.

Following the success of these earlier mass-mailer viruses, a new class of malware was born. This malware, or *spyware*, was used to deliver pop-up ads. A full spectrum of pop-up ad malware exists, ranging from the legitimate but annoying to the illegitimate and harmful.

A good example of legitimate but annoying spyware is the pop-up ad generators (also called adware) often embedded in peer-to-peer applications, such as Kazaa. Users downloading the desired application had to agree to install the adware, but the adware was virtually impossible to remove. Many other pop-up generators and tracking cookies are loaded onto a user's PC without their knowledge, creating annoying ads and capturing personal web browsing information to help target more unwanted advertising.

Other forms of malware are more hostile. A particularly ugly variant of malware, known as *ransomware*, shuts down functionality of the end user device unless the victim pays a ransom. In 2008, several kinds of malware and ransomware for mobile phones showed up in Asia, where workers are more likely to have a mobile phone than a personal computer. As VNUnet reported, when the mobile phone was infected, the phone's owner would receive a message instructing them to pay to restore the phone's functionality.[1]

In a classic scam, a lot of computer-based ransomware masquerades as *anti*spyware or *anti*virus software. It pretends to scan your computer for malware, tells you your device is infected, and asks you to fork over money to access the "full" version of the software

that can remove the "found" infections. In 2008, a family of fake antivirus software, known as XP Antivirus, infected millions of computers netting the criminals millions of dollars.

Keylogging malware tracks every keystroke you make and sends the information back to online criminals so that they can use or resell your login names, passwords, credit card numbers, and other useful personal or corporate information.

Rootkits gain access to the core of your operating system and let criminals control your computer or network as administrators. (Some of the fake antimalware products partake in these activities instead of, or as well as, demanding money to "clean" your computer.) After criminals infiltrate your computer, they want to use it to profit. To do so, they make it part of a *botnet*, which is a network of thousands of infected computers that carry out the orders of online criminals by sending out massive amounts of spam, hosting websites, or participating in attacks on websites that are designed to deny visitors access to the sites (also known as a denial of service attack). This type of malware can also turn these websites into malware redirect hubs.

Another technique used by criminals is to create malicious software that looks for a flaw in the browser code or, more often, a flaw in a browser plug-in such as the Flash player. The malware creates a buffer overflow. This is one of the most common and dangerous vulnerabilities; malware piles extra data into a program's buffer or temporary data storage area. Rather than rejecting the extra data, the vulnerable software enables the extra data to be written to the next operation. A carefully crafted exploit can ensure the extra data is an attack vector, which is written to an overflow area that executes the attack. The most common exploits today target web browsers or browser plug-ins such as the Flash player or Adobe Reader. In this case, the victims merely visit a website and can be exploited and have malware installed on their computer without their interaction or knowledge; this is known as a *drive-by download*.

A 2008 Google study of drive-by downloads indicated that more than 3 million URLs on the Internet were found to initiate drive-by downloads. And 1.3 percent of incoming search queries to Google brought up at least one malicious URL in the search results.[2]

Botnets

Botnets are the backbone of criminal activity on the Internet today, and they keep growing in number and sophistication. Internet experts have likened botnets to a pandemic, and say that at one time, up to 25 percent of all Internet-connected computers were part of a botnet.[3] With the steady rollout of broadband infrastructure and unprotected PCs in the emerging economies of the world, the supply of botnets appears unlimited.

Usually, the computer owner won't even know the computer is part of a botnet except for occasional slowdowns in performance. The malware that turns the computer into a botnet node, or "zombie," often invisibly downloads in the background while the computer user innocently surfs the Web. It can also be very clever at hiding from antivirus software, with code that changes every so often (making it harder to identify) or goes dormant for a while (making it harder to find).

Even Trusted Sites Can't Be Trusted

A recent development in malware distribution is the infection of legitimate websites—in enormous numbers—so they start serving up malware. The advantage for malware creators: These sites have been around for a long time, have a good reputation, and are trusted by large numbers of site visitors and security solutions—so they might be easier to exploit.

Modern malware has managed to penetrate the websites of media organizations and publications such as *BusinessWeek*,[4] major companies, government organizations, banks, and online social networks. This enables criminals to take advantage of the millions of visitors to these trusted sites without having the inconvenience and expense of building appealing malware-distributing websites of their own.

In these cases, online criminals attack millions of legitimate websites looking for weaknesses. If they find a vulnerable site, they insert small bits of code, called iFrames, on these trusted webpages so that they start sending visitors to websites that host malware. The iFrame codes make it possible to embed one HTML document inside another one. For instance, the banner ad found on a webpage is often hosted by a different web server than the main content. Online criminals can simply incorporate a malicious URL somewhere in the iFrame, or they can hide it with JavaScript.

How do online criminals get their malicious iFrame onto a legitimate website? Most often, they use SQL injections.

This technique exploits a vulnerability in the database layer of certain web applications and servers. When website developers don't properly sanitize the data transmitted in user input fields (such as forms and user logins) on webpages that use SQL, criminals can take advantage of this weakness to take control of the website and turn it into a malware redirection hub.

Finding the Weak Points

To gain a foothold on your computer and in your corporate network, malware exploits weak points, or vulnerabilities, in widely used technologies. The myriad rapidly developing applications that make up the Web provide a wealth of vulnerabilities for online criminals to exploit.

The Web is made up of billions of pages created by different people with different levels of technical skills, offering rich content in many different formats. Accessing some of this content requires helper applications, such as media players. Many different types of backend software serve up these webpages and content. And many of those formats, applications, and tools have weaknesses hackers can exploit.

Hackers also can exploit the Web's core infrastructure and basic standards. Many of the standards and much of the infrastructure the Web runs on were designed long before anyone thought of today's amazingly wide-ranging uses of the Web. For example, e-commerce, online banking, online social networking, and enterprise-level cloud-based computing are

all common on the Web today. Ideally, you want to feel secure while engaging in those activities. But in the early days, decisions about the Internet and Web's standards and infrastructure heavily emphasized improving connectivity and access to content rather than walling off content in easily securable chunks. So, underlying infrastructure vulnerabilities, along with vulnerabilities in higher-level applications, remain a concern.

Hackers use these vulnerabilities to create exploits that let them penetrate your computer or network. Often, when you visit an infected webpage or open an infected email, the attack code starts snooping around for any known weaknesses in your system.

The malware found on a malicious website—such as one involved in an iFrame attack—begins a series of probes, looking for unpatched weaknesses in your browser, the myriad browser plug-ins you might have installed, your operating system, or any applications you might have running.

The level of sophistication is remarkable in that the malware sites can actually identify the particulars of your computer and operating system and infect or attack the system appropriately. For instance, if you run Safari as your browser, the malware sites won't bother trying any known Internet Explorer vulnerabilities. Instead, they focus on Safari or Safari plug-in weaknesses.

When a useful vulnerability is found, the goal of the malware attack is to create a buffer overflow condition in your computer. This then gives the malware the capability to initiate the download of harmful code—the keyloggers, botnet software, spyware ad generators, or other malware previously discussed.

Malware doesn't only exploit vulnerabilities in technologies. Malware creators and distributors also take advantage of "weaknesses" in human nature, such as curiosity, trust, desire for connection, and carelessness, to dupe users into handing over the keys to their system security.

Social Engineering for Success

To distribute malware, send spam, and acquire sensitive information by posing as a trusted source (also called *phishing*), online criminals increasingly take advantage of human nature to get victims to open an email, visit a website, or give up information. They use sophisticated social engineering techniques, and they hijack reputations of trusted websites and email senders to get their message or malware into your system.

For example, they appear to offer useful Web 2.0 tools, cool games, or interesting news content. When you click the link in the email and visit the site, the site often appears normal. However, in the background it's probing your machine, searching for a vulnerability that lets it install malware on your computer.

Other attacks try to appear like a legitimate bank or commerce site in hopes of capturing your username and password—phishing for your information. Other forms of malware sites try to get you to "buy" something from the site, giving the criminals your credit card information.

In Figure 8-1, we contrast an image of the legitimate ticketing website for the Beijing 2008 Summer Olympics with a scam ticketing website. Oddly enough, the scam site was much better looking and more user-intuitive than the real ticketing site, with better graphics and navigation—which meant visitors to the fake site were lulled into a sense of comfort. Unfortunately, people who entered orders on the fake site received no tickets but had their credit card numbers stolen.

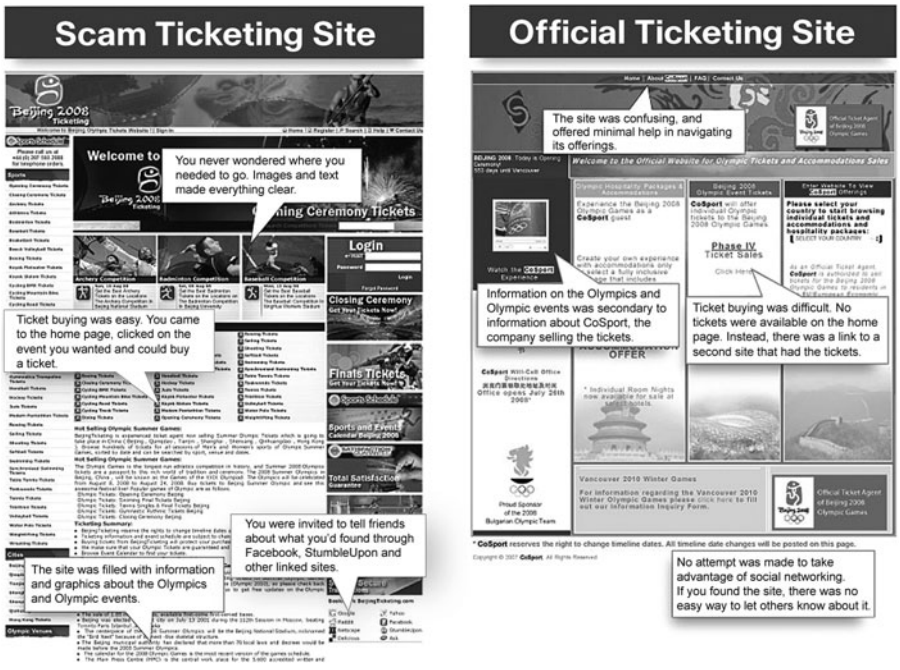

Figure 8-1 *Fake Sites Can Look Better Than the Real Thing*

Some malware is still distributed as email attachments, but the more successful of these campaigns also depend heavily on social engineering to make the emails appear trustworthy so that you'll open them. (And the more sophisticated malware payloads available today can avoid being filtered out by antimalware solutions for a longer period, also increasing the email-borne malware's chance of getting through.) Recent successful email-borne malware campaigns include

- Emails with attachments pretending to be "shipping department profit and loss statement" spreadsheets, which are highly personalized and sent to specific company executives.
- Emails with attachments that pretend to be delivery confirmation requests from major shipping services, such as UPS or FedEx.

- Emails that are highly personalized and pretend to be from tax authorities or consumer information bureaus, asking company executives to fill out the attached form in response to a tax concern or business complaint.

The social engineering involved in the preceding attacks often is irresistible to end users. How many of us wouldn't open an email from FedEx saying the package we sent on a certain date couldn't be delivered, especially if we had sent off a few packages that same week?

Advanced social engineering techniques usually involve additional information to personalize the attack and make it seem closer to legitimate traffic. To support this next wave of personalized attacks, criminals mine social networking sites for personal information that they can later use to personalize phishing messages sent to you, or to your colleagues, friends, or family.

Spamming and Phishing Get Targeted

Spamming and phishing are becoming much more sophisticated. Spam emails use highly topical subject lines, often related to current news events. The content in the message looks and sounds much more legitimate and professional than it used to. Spam often closely mimics legitimate senders' messages—not just in style but by "spoofing" the sender information, making it look like it comes from a reputable sender.

The increasing personalization and sophistication of spam messages benefits the spammer in two ways:

- If it looks more like legitimate traffic, modern spam is more likely to slip past antispam software.
- Because of the targeted content, more people will actually open the message. More messages getting through filters and more messages opened means increased profits for the spammer.

The majority of spam is still classified as *mass mailing spam*, for example, billions of copies of messages for illegal pharmaceutical sites or the venerable get-rich-quick scams. The original mass mailers would send large volumes of the same message from a few source locations on the Internet. But these types of campaigns are relatively easy for spam filters to block through keyword analysis and blacklists of the mailing sources. Modern mass mailing spam still involves billions (yes, billions) of messages per attack, but they typically come from millions of different sources—coordinated by botnets—to obscure their origin. A modern mass mailer can also include tens of thousands of variations in the content, to defy keyword or signature filters.

Fighting Spam

Stopping today's mass mailers requires large data collection networks and sophisticated correlation techniques that can identify common elements or fingerprints in the campaign. Only a small number of antispam vendors have the reach required to sample enough of these huge attacks and the technical resources required to analyze them.

The constantly increasing investment required to keep a spam filter accurate has led to the consolidation of the spam filter industry. Five years ago, more than a hundred plausible vendors existed; today, you can count them on one hand.

In addition to the increasingly sophisticated camouflage techniques of the high-volume spammers, more and more spam campaigns are aimed at specific groups, such as sports fans, or at people in certain geographic regions. These campaigns are even harder to detect due to the low volume associated with a targeted attack. Figure 8-2 shows the increasing trend of targeted attacks over time.

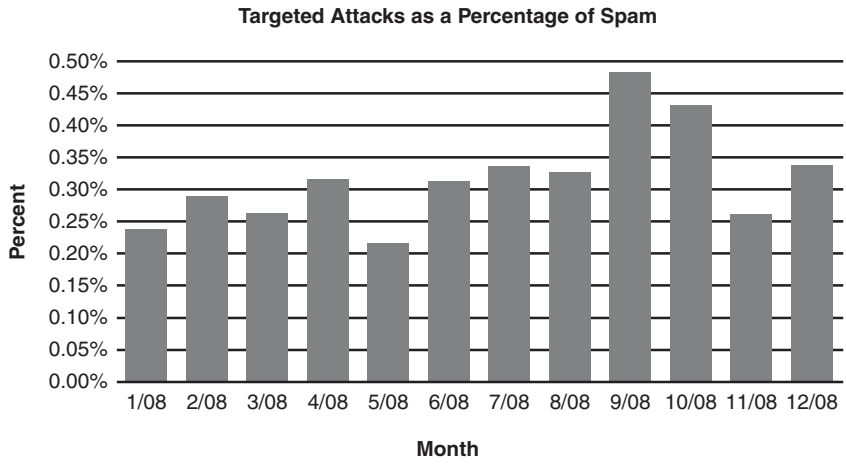

Figure 8-2 *Targeted Attacks as a Percentage of Overall Spam*

For phishing spam that's aimed at obtaining personal or financial information, targeted phishing—also known as *spear-phishing*—has become the norm. Figure 8-3 shows how spear-phishing has become more frequent, and more lucrative, than traditional spam campaigns.

Some recent spear-phishing campaigns involved personalized messages sent to customers of specific banks or frequent flyer programs to prompt them to log in or input their account information on a phishing website. Other campaigns are based on personalized emails sent to company executives, claiming they were subpoenaed or needed to give information to tax authorities. Figure 8-4 shows a sample targeted phishing email.

Criminals aren't solely depending on email and websites to practice their craft. Text messaging to mobile phones, combined with fake call-center setups, are another way they gather information. For instance, they send an SMS (Short Message Service, or text message) that claims to be from a regional bank to mobile phone numbers in a certain area

code. The SMS asks recipients to call a number to confirm their account information, but of course, the number isn't actually that of the bank. It's staffed by criminals.

Figure 8-3 *Spear-Phishing Attacks Versus Traditional Spam*

From: ci@irs.gov [mailto:ci@irs.gov]
Sent: Wednesday, June 06, 2007 1:14 PM
To: [redacted]
Subject: Internal Revenue Service Complaint for [redacted] [case id: #602f41571ba161cc3dc795df7886f000]

Mr./Mrs. [redacted]

We regret to inform you that your company is currently being investigated by our CI department for criminal tax fraud
due to a complaint that was filled by a Mr. Keith McCall on 05/06/2007

Complaint Case Number: MT1CF23A
Complaint made by: Mr. Keith McCall
Complaint registered against: [redacted]
Date: 05/06/2007

You are being investigated for submitting false income tax returns with the Franchise Tax Board.
Instructions on how to resolve this issue aswell as a copy of the original complaint can be found on the link bellow.

Complaint Documents <[redacted]>

Figure 8-4 *Example of a Targeted Phishing Email*

Mining Online Social Networks

Online criminals have also been tapping into all the information—and contacts—available on social networks such as Facebook and MySpace. They're hijacking accounts to beg for money, mining social networking sites for information for phone scams, and constantly finding new ways to capitalize on the wealth of information available on online social networks.

Take the case of Bryan Rutberg. As reported on MSNBC.com's Redtape Chronicles, his Facebook account was hijacked.[5] The online criminal reset the password to lock Rutberg out of his own account, after possibly having obtained the original using a clever phishing

continues

email. Then the criminals changed Rutberg's Facebook "status" message saying he was in trouble while on vacation overseas, and, claiming that his credit card wasn't working, that he needed a quick loan that he'd repay when he got back home.

This was a variant of a classic "419 scam"—named after the section of Nigeria's penal code that covers them because Nigeria is where both classic versions of the scam (faxes or emails asking for assistance in obtaining large amounts of money from overseas bank amounts) and modern versions often originate. It worked; one of Rutberg's concerned friends wired over money.

Similar scams are run on other online social networks and will increase as people spend more of their online time and attention there.

Profit Motive

Much of today's malware has one goal in common: financial profit. Hackers used to create viruses largely for fun and glory. These days, hackers and online criminals are part of a sophisticated shadow economy that wants to make money.

Like any maturing industry, the online crime market has begun to segment into specializations. Some online criminals focus on the social engineering, marketing, and fulfillment of merchandise. Others work on building and maintaining massive bot networks that they make available for rent. And some organizations specialize in building and deploying tools for malware creation and delivery.

Talented developers have been creating ever-better variants of malware. They create malware for a specific, popular purpose and sell it "as is" or together with tech support. They also develop custom malware for specific projects. Of the types of malware now for sale or rent, the following are just a few examples:

- Mass blog-posting tools
- Volume spamming tools
- Account-generating tools for webmail accounts or community posting sites, such as Craigslist
- Keylogging programs
- Botnet management tools

Because malware is generating significant profits for online criminals, they'll keep investing in it. That means more new kinds of malware that take advantage of weaknesses in both existing and newly popular technologies and tools, and malware that works even harder to be efficient and stay hidden.

But how exactly are online criminals profiting from malware? And who's reaping these financial returns? In the next chapter, we explore the business aspects of malware.

Endnotes

[1] Nichols, Shaun. "Ransomware attacks target Symbian mobiles," VNUnet. March 5, 2008. http://www.vnunet.com/vnunet/news/2211194/ransomware-goes-mobile.

[2] Provos, Niels. "All Your iFrame Are Point to Us," Google Online Security Blog. February 11, 2008. http://googleonlinesecurity.blogspot.com/2008/02/all-your-iframe-are-point-to-us.html.

[3] Weber, Tim. "Criminals 'may overwhelm the web,'" BBC News. January 25, 2007. http://news.bbc.co.uk/1/hi/business/6298641.stm.

[4] Cluley, Graham. "Hackers infect BusinessWeek website via SQL Injection attack," Graham Cluley's blog on Sophos.com. September 15, 2008. http://www.sophos.com/blogs/gc/g/2008/09/15/hackers-infect-businessweek-website-via-sql-injection-attack/.

[5] Sullivan, Bob. "Facebook ID Theft Targets 'Friends,'" MSNBC.com. January 30, 2009. http://redtape.msnbc.com/2009/01/post-1.html.

References

Cisco 2008 Annual Security Report. www.cisco.com/en/US/prod/collateral/vpndevc/securityreview12-2.pdf.

IronPort Targeted Phishing Overview PPT 061308—Nilesh Bhandari, IronPort.

IronPort Targeted Phishing Security Trends Overview. www.ironport.com/pdf/ironport_targeted_phishing.pdf.

IronPort 2008 Internet Malware Trends Report—Storm and the Future of Social Engineering. http://www.ironport.com/malwaretrends/.

Cisco IntelliShield Cyber Risk Reports. http://tools.cisco.com/security/center/cyberRiskReport.x.

ZDnet Zero Day blog. http://blogs.zdnet.com/security/.

CNet Security News. http://news.cnet.com/security/.

The Spamhaus Project news blog. http://www.spamhaus.org/newsindex.lasso.

Index

NUMBERS

A

B

C

D

E

F

G

H - I

J - K - L

M

N

O - P

Q - R

S

T

U - V

W

X - Y - Z