Making Everything Easier!™

Palo Alto Networks® 2nd Edition

Cybersecurity

FOR DUMMIES®

A Wiley Brand

Learn to:

- Identify key characteristics of advanced malware
- Recognise malware patterns and attack stages
- Implement effective cybersecurity controls

Brought to you by

paloalto NETWORKS®

Lawrence C. Miller, CISSP

Palo Alto Networks

Palo Alto Networks is leading a new era in cybersecurity by securing thousands of enterprise, government, and service provider networks from cyber threats and protecting our digital way of life. The next-generation platform uses an innovative traffic classification engine that identifies network traffic by application, user, and content.

The Palo Alto Networks next-generation security platform is built on four main principles:

1. **Natively integrated** technologies that support open communication, orchestration, and visibility;
2. **Automation** of protection creation and reprogramming of the security posture across network, endpoint and cloud environments;
3. **Extensibility** that allows for protection of customers as they expand and as market requirements change; and
4. **Threat intelligence sharing** to minimize the spread of attacks by providing protection based on comprehensive global threat data.

The next-generation security platform offers superior protection against the sophistication of modern attacks, can reduce the total cost of ownership for organizations by simplifying their security infrastructure, and eliminates the need for multiple, stand-alone security appliances and software products.

Find out more at **www.paloaltonetworks.com**

Cybersecurity

FOR DUMMIES®

A Wiley Brand

Palo Alto Networks 2nd Edition

Cybersecurity for Dummies

A Wiley Brand

Palo Alto Networks 2nd Edition

by Lawrence C. Miller, CISSP

for Dummies
A Wiley Brand

Cybersecurity For Dummies®, Palo Alto Networks 2nd Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

ISBN 978-1-119-25028-9 (pbk); ISBN 978-1-119-25029-6 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

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

Development Editor: Elizabeth Kuball

Copy Editor: Elizabeth Kuball

Acquisitions Editor: Amy Fandrei

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Antony Sami

Table of Contents

Introduction

Advanced threats have changed the world of enterprise security and how organizations are attacked. These threats, and the cybercriminals behind them, are experts at remaining hidden from traditional security while exhibiting an intelligence, resiliency, and patience that has never been seen before. Controlling these threats requires multiple security disciplines working together in context. Although no single solution will solve the problem of advanced threats on its own, next-generation cybersecurity provides the unique visibility and control of, and the true integration of, threat-prevention disciplines needed to find and stop these threats — both known and unknown.

About This Book

This book provides an in-depth examination of real-world attacks, the shortcomings of legacy security solutions, the necessary capabilities of next-generation cybersecurity, and security best practices.

Foolish Assumptions

First and foremost, despite the title of this book, I assume that you know a little something about cybersecurity and Internet-based threats. I know, it's a bit of an oxymoron, but "Cybersecurity For Geniuses" just isn't that catchy! As such, this book is written primarily for technical readers who are evaluating potential new security solutions to address advanced threats and cyberattacks.

How This Book Is Organized

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

Chapter 1: Understanding the Cybersecurity Landscape

To start, you get some real-world examples of high-profile attacks. You also get a glimpse into the psyche of a cybercriminal to understand what motivates such a person, and you take a walk through the threat life cycle — from cradle to . . . well, the targeted network.

Chapter 2: The Role of Malware in Cyberattacks

This chapter describes the characteristics of advanced malware and dissects some of these evil critters!

Chapter 3: Why Traditional Security Solutions Fail to Control Advanced Malware

Chapter 3 explains why legacy port-based firewalls, intrusion prevention systems, and other security solutions are largely ineffective in the fight against advanced attacks.

Chapter 4: What Next-Generation Security Brings to the Fight

This chapter takes a deep dive into the advanced capabilities and features of next-generation security and lays out a practical methodology to protect your enterprise from advanced threats and cyberattacks.

Chapter 5: Creating Advanced Threat Protection Policies

Chapter 5 explains the importance of developing organizational security policies and controls, and how to implement and enforce those policies with next-generation security.

Chapter 6: Ten Things to Look for in a Cybersecurity Solution

Finally, in that classic *For Dummies* format, the book ends with a Part of Tens chapter chock-full of security best practices!

Glossary

And, just in case you get stumped on a technical term or an acronym here or there, I've included a glossary to help you sort through it all.

Icons Used in This Book

Throughout this book, you'll occasionally see special icons that call attention to important information. You won't see any smiley faces winking at you or any other little emoticons, but you'll definitely want to take note! Here's what you can expect.

REMEMBER

This icon points out information that may well be worth committing to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!

TECHNICAL STUFF

You won't find a map of the human genome or the secret to the blueprints for the next iPhone here (or maybe you will, hmm), but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon and is the stuff legends — well, nerds — are made of!

TIP

Thank you for reading, hope you enjoy the book, please take care of your writers! Seriously, this icon points out helpful suggestions and useful nuggets of information.

WARNING!

Proceed at your own risk . . . *well, okay* — it's actually nothing *that* hazardous. These useful alerts offer practical advice to help you avoid making potentially costly mistakes.

Where to Go from Here

With our apologies to Lewis Carroll, Alice, and the Cheshire cat:

“Would you tell me, please, which way I ought to go from here?”

“That depends a good deal on where you want to get to,” said the Cat — er, the Dummies Man.

“I don’t much care where . . . ,” said Alice.

“Then it doesn’t matter which way you go!”

That’s certainly true of *Cybersecurity For Dummies,* Palo Alto 2nd Edition, which, like *Alice in Wonderland,* is destined to become a timeless classic!

If you don’t know where you’re going, any chapter will get you there — but Chapter 1 may be a good place to start! However, if you see a particular topic that piques your interest, feel free to jump ahead to that chapter. Each chapter is individually wrapped (but not packaged for individual sale) and written to stand on its own, so feel free to start reading anywhere and skip around! Read this book in any order that suits you (though I don’t recommend upside down or backward). I promise that you won’t get lost falling down the rabbit hole!

Chapter 1

Understanding the Cybersecurity Landscape

In This Chapter

- Seeing the threat through real-world examples
- Understanding how cybercriminals have changed

For many years, the security industry was seen as Chicken Little, telling anyone who would listen that "the sky was falling" and that cybercriminals were trying to steal their most precious information. For the most part, that simply wasn't the case. Attackers were largely creatures of opportunity seeking the path of least resistance — if they encountered a secured network, they were likely to move on, looking for a softer target. But today's cybercriminals are highly motivated professionals — often well-funded by criminal organizations or nation-states — who are far more patient and persistent in their efforts to break through an organization's defenses.

In this chapter, you find out why cybercriminals are more dangerous than ever before.

Malware is malicious software or code that typically damages or disables, takes control of, or steals information from a computer system. Malware broadly includes adware, backdoors, bootkits, logic bombs, rootkits, spyware, Trojan horses, viruses, and worms.

The State of Today's Intrusions

Today's threats are more sophisticated and equal opportunity than ever before. All types of organizations and information are being targeted. More and more attacks are increasingly coming to fruition, producing a steady stream of high-profile, sophisticated breaches and intrusions, including

- **Target (customer information):** In December 2013, an intruder compromised Target's network by stealing a third-party vendor's credentials and gaining access to Target's network through its heating, ventilation, and air-conditioning (HVAC) system. The retailer's point-of-sale (POS) systems were not properly segmented from other systems (such as industrial systems) on the network, so the attacker was able to move freely from system to system on the network, installing malware on nearly all of Target's POS devices in stores across the country, and gaining access to more than 70 million customer records and credit card numbers.
- **Sony Pictures (intellectual property):** In November 2014, attackers posted unreleased films and sensitive information pertaining to employees, including executives, online. Though initially attributed to nation-state hackers in North Korea, it was later alleged that these attacks were launched via a spear-phishing attack by cybercriminals in Russia and Ukraine. These attacks not only delayed releases of several Sony films, but also publicly embarrassed several Sony executives.
- **U.S. Office of Personnel Management (employee information):** In June 2015, the U.S. government's Office of Personnel Management (OPM) discovered that attackers had infiltrated their databases by exploiting numerous vulnerabilities, and were sending large data files to destinations outside the organization's network. OPM estimates that personal data (including Social Security numbers) of more than 4 million current, former, and prospective federal employees was stolen, but FBI Director James Comey estimates that as many as 18 million records may have been compromised.
- **Anthem Blue Cross (customer information):** In February 2015, the second largest health insurer in the United States publicly disclosed that attackers had breached

> its servers and stolen as many as 80 million customer records containing personal data and Social Security numbers. The attack is suspected to have been carried out by state-sponsored hackers in China, using malware to exploit Adobe Flash vulnerabilities, and may have gone undetected for almost two months before being discovered by a database administrator whose logon credentials were being used to run a suspicious database query.
>
> - **Lenovo (hacktivism):** In February 2015, Lizard Squad, a loosely organized hacktivist group, hijacked computer manufacturer Lenovo's website and redirected customers to a site that posted selfie slideshows (allegedly of the hackers themselves). This incident caused further reputation damage for Lenovo, which had recently disclosed that it had pre-installed Lenovo laptops with Superfish malware, an adware program that hijacks encrypted connections and facilitates man-in-the-middle attacks.

TECHNICAL STUFF

Spear phishing is a targeted phishing campaign that appears more credible to its victims by gathering specific information about the target, and thus has a higher probability of success. A spear-phishing email may spoof an organization (such as a financial institution) or individual that the recipient actually knows and does business with, and may contain very specific information (such as the recipient's first name, rather than just an email address).

WARNING!

Spear phishing, and phishing attacks in general, are not always conducted via email. A link is all that's required, such as a link on Facebook or on a message board or a shortened URL on Twitter. These methods are particularly effective in spear phishing because they allow the attacker to gather a great deal of information about the targets and then lure them into dangerous clicks in a place where the users feel comfortable. Security awareness training and well-defined processes are an important element in preventing attacks that leverage these delivery tactics and other social-engineering techniques.

Given its flexibility and ability to evade defenses, advanced malware presents an enormous threat to the organization. Advanced malware is virtually unlimited in terms of functionality — from sending spam to the theft of classified information and trade secrets. The ultimate impact of advanced malware is largely left up to the attacker, from sending spam one day to stealing credit card data the next — and far beyond, as many cyberattacks go undetected for months or even several years. For example, the Home Depot security breach of 2014 went undetected for five months and resulted in the compromise of more than 56 million payment cards.

Targeted intrusions

Advanced malware is a key component of targeted, sophisticated, and ongoing attacks, and it can be customized to compromise specific high-value systems in a target network. In these cases, an infected endpoint inside the network can be used to steal login credentials and initiate lateral movement in order to gain access to protected systems and to establish backdoors in case any part of the intrusion is discovered.

These types of threats are almost always undetectable by traditional signature-based antivirus software on the endpoint. They represent one of the most dangerous threats to organizations because they're specifically created with custom components designed to bypass known security technologies and leverage vulnerabilities and weaknesses within the targeted organization. These attacks target the organization's most valuable information, such as research and development, intellectual property, strategic planning, financial data, and customer information, and are typically well financed, as the return on investment is typically more than 1,000 percent.

Carbanak: The Great Bank Robbery

Carbanak is one of the latest examples of a targeted attack that began in August 2013 and is currently still active. The attackers sent spear-phishing emails with malicious CPL attachments or Word documents exploiting known vulnerabilities. Once inside the victim's network, money is extracted. Each raid has lasted two to four months. To date the attackers have targeted up to 100 financial institutions, causing aggregated losses estimated at $1 billion.

DoS, DDoS, and botnets

Bots (individual infected endpoints) are often used in distributed denial-of-service attacks (DDoS) — to overwhelm a target server or network with traffic from a large number of bots. In such attacks, the bots themselves are not the target of the attack. Instead, the bots are used to flood some other remote target with traffic. Of course, it usually takes an army of bots, known as *botnets,* to bring down a target network or server, The attacker leverages the massive scale of the botnet to generate traffic that overwhelms the network and server resources of the target. DDoS attacks often target specific companies for personal or political reasons, or to extort payment from the target in return for stopping the DDoS attack.

Botnets themselves are dubious sources of income for cybercriminals. Botnets are created by cybercriminals to harvest computing resources (bots). Control of botnets (through CnC servers) can then be sold or rented out to other cybercriminals for various nefarious purposes.

DDoS botnets represent a dual risk for organizations. The organization itself can potentially be the target of a DDoS attack, resulting in downtime and lost productivity. Even if the organization is not the ultimate target, any bots in the organization that participate in an attack on another organization will consume valuable network resources and facilitate a criminal act, albeit unwittingly.

The DDOS attack against GitHub

GitHub, the largest public code repository in the world, experienced a massive distributed denial-of-service (DDoS) attack in March 2015. The attack appeared to originate from China and specifically targeted two GitHub projects designed to combat censorship in China: GreatFire and cn-nytimes.

Advanced persistent threats

Advanced persistent threats (APTs) are a class of threats that often combine advanced malware and botnet components to execute a far more deliberate and potentially devastating attack. As the name applies, an APT has three defining characteristics:

- **Advanced:** In addition to advanced malware and botnets, the attackers typically have the skills to develop additional exploitation tools and techniques, and may have access to sophisticated electronic surveillance equipment, satellite imagery, and even human intelligence assets.
- **Persistent:** An APT may persist over a period of many years. The attackers pursue specific objectives and use a low-and-slow approach to avoid detection. The attackers are well organized and typically have access to substantial financial backing to fund their activities, such as a nation-state or organized crime.
- **Threat:** An APT is a deliberate and focused, rather than opportunistic, threat that can cause real damage.

Many organizations and individuals have been lulled into a false sense of security by the mistaken belief that the only data an attacker wants to steal — and, thus, the only data that needs to be protected — is financial data, such as credit card numbers or banking information. But breaches are not limited to financial data — if it's valuable to you or your organization, it's very likely to be valuable to someone else as well!

Stuxnet: When sanctions alone aren't enough

Stuxnet is a computer worm that was used in an APT against Iran's nuclear program. It was discovered in 2010, but may have been operating, in different variations, as early as 2005. The worm initially infected endpoints running Microsoft Windows, then targeted programmable logic controllers (PLCs) running Siemens Step7 software. In addition to collecting information about Iran's nuclear program, the attack enabled its controllers to cause Iran's nuclear centrifuges to spin faster and tear themselves apart. Stuxnet is believed to have destroyed 20 percent of Iran's nuclear centrifuges.

The Changing Face of Cybercriminals

Cybercriminals have evolved from the prototypical "whiz kid" — sequestered in a basement, motivated by notoriety, and fueled by oversized cans of energy drinks — into bona fide cybercriminals, often motivated by significant financial gain and sponsored by nation-states, criminal organizations, or radical political groups. Today's attacker fits the following profile:

- Has far more resources available to facilitate an attack
- Has greater technical depth and focus
- Is well funded
- Is better organized

Why does this matter? Because a kid in a basement may be able to break into a corporate network, but doesn't necessarily know what to do with, say, RSA source code. On the other hand, a rogue nation-state or criminal organization knows exactly what to do or who to sell stolen intellectual property to on the gray or black market.

Additionally, criminal organizations and nation-states have far greater financial resources than independent individuals. Many criminal hacking operations have been discovered, complete with all the standard appearance of a legitimate business with offices, receptionists, and cubicles full of dutiful cybercriminals. These are criminal enterprises in the truest sense and their reach extends far beyond that of an individual.

REMEMBER

Not only do we face more sophisticated adversaries today, but the types of information of value to them are continually expanding as well. These groups can do interesting things with the most seemingly innocuous bits of information.

REMEMBER

The sky is *not* falling! Today's threats are not so advanced that they're impossible to control. They aren't completely new, just more common and better organized. Solutions do exist, and organizations can adopt best practices and adapt to changes in the threat landscape to reduce the attack surface and prevent a large number of threats. The attackers have evolved, but security has as well.

Chapter 2

The Role of Malware in Cyberattacks

In This Chapter

- Identifying unique traits of advanced malware
- Analyzing modern cyberattack strategy
- Recognizing opportunities to limit and counter threats

The rise of advanced malware is reshaping the threat landscape and forcing organizations to reassess how they protect themselves. Collectively, advanced malware has outpaced traditional anti-malware strategies and in the process, has established a foothold within organizations that criminals and nation-states can use to steal information and attack sensitive assets.

In this chapter, you learn about this new class of threats — known as advanced malware — what makes them tick, what makes them particularly nasty, and how they play a key role in modern attack strategy.

Recognizing Key Characteristics of Advanced Malware

Information security teams have been doing battle with various types of malware for more than two decades, often ill equipped with only an arsenal of woefully inadequate signature-based antivirus software. Verizon's 2015 *Data Breach Investigations Report* describes a growing "detection deficit" trend in which the time to compromise and time to detect a breach has diverged over the past decade. Trustwave's 2015

Global Security Report found that it takes an average of 188 days from infection to detection of malware "in the wild". That's an awfully long time for an attack — which often begins with an exploit or advanced malware infection — to go undetected and, therefore, unmitigated.

A *vulnerability* is a bug or flaw that exists in software and creates a security risk that may be exploited by an attacker. The attacker crafts an *exploit* that targets the vulnerable software, essentially fooling the vulnerable software into performing functions or running code of the attacker's choice.

This poor "catch rate" is due to several factors. Some malware has the ability to mutate or can be updated to avoid detection by traditional antimalware signatures. Additionally, advanced malware is increasingly specialized to the point where an attacker will develop a customized piece of malware that is targeted against a specific individual or organization.

Advanced malware leverages networks to gain power and resilience, and can be updated — just like any other software application — so that an attacker can change course and dig deeper into the network, based on what he finds, or to make changes and enact countermeasures.

This is a fundamental shift compared to earlier types of malware, which were more or less a swarm of independent agents that simply infected and replicated themselves. Increasingly, advanced malware has become a centrally coordinated, networked application in a very real sense. In much the same way that the Internet changed what was possible in personal computing, ubiquitous network access is changing what is possible in the world of malware. Now, all malware of the same type can work together toward a common goal, with each infected endpoint expanding the attack foothold and increasing the potential damage to the organization.

Here are some important characteristics and capabilities of advanced malware:

- **Distributed, fault-tolerant architecture:** Advanced malware takes full advantage of the resiliency built in to the Internet itself. Advanced malware can have multiple control servers distributed all over the world with multiple fallback options, and can also potentially leverage other infected endpoints as communication channels, providing a near infinite number of communication paths to adapt to changing conditions or update code as needed.

- **Multifunctionality:** Updates from command-and-control servers can also completely change the functionality of advanced malware. This multifunctional capability enables an attacker to use various endpoints strategically, in order to accomplish specific desired tasks such as stealing credit card numbers, sending spam containing other malware payloads (such as spyware), or installing ransomware for the purpose of extortion.
- **Polymorphism:** A *hash signature* is a cryptographic representation of an entire file or program's source code. Changing just a single character or bit of the file or source code completely changes the hash signature. *Polymorphism* is used to avoid detection by hash-based antimalware signatures by regularly mutating to avoid simple hash signature matches. Thus, polymorphism can produce an infinite number of unique signature hashes for even the smallest of malware programs. Some malware applications have entire sections of code that serve no purpose other than to change the signature of the malware.
- **Obfuscation:** Advanced malware often uses common obfuscation techniques to hide certain binary strings that are characteristically used in malware and, therefore, easily detected by antimalware signatures or to hide an entire malware program. Obfuscation can be implemented using a simple substitution cipher (such as an XOR operation) or more sophisticated encryption algorithms (such as AES), or using a *packer* to compress a malware program for delivery and then decompress it in memory at runtime.

Understanding Modern Cyberattack Strategy

Modern cyberattack strategy has evolved. In addition to direct, open attacks against a high-value server or asset, today's attack strategy also employs a patient, multistep, covert process that blends exploits, malware, and evasions in a coordinated attack. The cyberattack life cycle (see Figure 2-1) is a sequence of events that an attacker goes through to successfully infiltrate an organization's network and steal data from it.

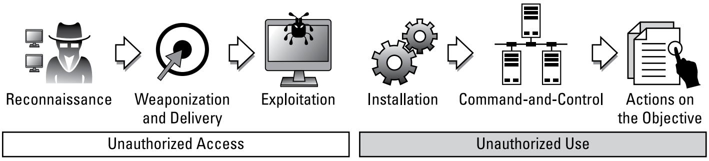

Figure 2-1: The cyberattack life cycle.

Here are the steps of the cyberattack life cycle:

1. **Reconnaissance.** Like common criminals, cybercriminals carefully study their victims and plan their attacks, often using social engineering, phishing, email address harvesting, and other tactics to research, identify, and select targets. They also use various tools to scan networks for vulnerabilities, services, and applications that can be exploited.

2. **Weaponization and delivery.** Next, the attacker determines the malware payload and the method that will be used to deliver it. For example, data files or web pages can be weaponized with exploits that are used to target the victim's vulnerable software and delivered via an email attachment or drive-by download.

   A *drive-by download* delivers advanced malware or an exploit in the background, without the user's knowledge, usually by taking advantage of a vulnerability in an operating system, web browser, or other third-party application.

3. **Exploitation.** The attacker generally has two options for exploitation:

   - *Social engineering* is a relatively simple technique used to lure someone into clicking a bad link or opening a malicious executable file, for example.

   - Software *exploits* are a more sophisticated technique because they essentially trick the operating system, web browser, or other third-party software into running an attacker's code. This means the attacker has to craft an exploit to target specific vulnerable software on the endpoint.

   Once exploitation has succeeded, an advanced malware payload can be installed.

WARNING!

Using exploits to infiltrate a target network has become an efficient and stealthy method to deliver advanced malware because exploits can be hidden in legitimate files. In addition, readily available off-the-shelf exploit kits significantly reduce the technical knowledge needed to develop exploits. After an exploit is run, the attacker can take control of the endpoint and install malware or run an attack entirely in memory, making it even more difficult to detect because no new files are created on the exploited system.

4. **Installation.** Once a target endpoint has been infiltrated, the attacker needs to ensure *persistence* (resilience or survivability). Various types of advanced malware are used for this purpose, including the following:

   - *Rootkits* are malware that provides privileged (root-level) access to a computer.
   - *Bootkits* are kernel-mode variants of rootkits, commonly used to attack computers that are protected by full-disk encryption.
   - *Backdoors* enable an attacker to bypass normal authentication procedures in order to gain access to a compromised system and are often installed as a failover, in case other malware is detected and removed from the system.
   - *Anti-AV software* may also be installed to disable any legitimately installed antivirus software on the compromised endpoint, thereby preventing automatic detection and removal of malware that is subsequently installed by the attacker. Many anti-AV programs work by infecting the master boot record (MBR) of a target endpoint.

5. **Command and control (CnC).** Communication is the lifeblood of a successful attack. Attackers must be able to communicate with infected systems to enable command and control, and to extract stolen data from a target system or network. This communication can also be used by the attacker to move laterally, targeting other systems on the victim's network. Thus, the initially infected target may only be the first entry point that enables lateral movement toward the attacker's ultimate objective.

CnC communications must be stealthy and can't raise any suspicion on the network. Such traffic is usually obfuscated or hidden through techniques that include the following:

- *Encryption* with SSL, SSH, or some other custom application. Proprietary encryption is also commonly used. For example, BitTorrent is known for its use of proprietary encryption and is a favorite tool — both for infection and CnC.
- *Circumvention* via proxies, remote desktop access tools (such as LogMeIn!, RDP, and GoToMyPC), or by tunneling applications within other (allowed) applications or protocols.
- *Port evasion* using network anonymizers or port hopping to tunnel over open or nonstandard ports.
- *Fast Flux (or Dynamic DNS)* to proxy through multiple infected hosts, reroute traffic, and make it extremely difficult for forensic teams to figure out where traffic is really going.

6. **Actions on the objective.** Attackers have many different motives for an attack, including data theft, destruction of critical infrastructure, hacktivism, or cyberterrorism. This final phase of the attack often lasts months or even years, particularly when the objective is data theft, as the attacker uses a low-and-slow attack strategy to avoid detection.

Key Security Lessons and Opportunities

For all their sophistication, advanced attacks exhibit some vulnerabilities of their own. Some key observations and opportunities to consider include the following:

- **Communication is the lifeblood of an attack.** Today's threats are networked threats that need your network to communicate. If a threat can't communicate, the attack can be largely neutralized.

- **Numerous opportunities exist to detect and correlate.** By virtue of the fact that multiple steps are involved in the advanced attack lifecycle, there are multiple chances to identify and counter threats.

- **The framework, rather than the functionality, is the threat.** If an attacker can infect targets, persist on, communicate with, and manage infected hosts, then the attacker can do almost anything. In other words, it matters less what a threat does once it has control, and more that it has the control in the first place. See the threat as an extensible framework, not simply as the functionality of the specific payload.

- **Threats exist across multiple disciplines, and so too must security.** Firewalls, intrusion prevention, advanced endpoint protection, content filtering — these security solutions have traditionally been separated to provide "defense in depth." But this strategy makes it difficult — if not impossible — to identify, correlate, and counter complex, coordinated attacks that take advantage of multiple attack vectors, including the following:

    - *Applications:* Can hide and enable threats.
    - *URLs and websites:* Can host and enable threats.
    - *Exploits:* Create command-line (or shell) access to the target, often with escalated privileges (such as administrator or root).
    - *Malware:* Controls and uses the compromised target.
    - *Files:* Used to update malware and steal data.

- **Security must expand beyond the perimeter to include network, endpoint, and cloud environments.** Organizations need to focus on expanding visibility beyond the network perimeter — both inward and outward. This is best accomplished with network segmentation and natively integrated next-generation security platforms to enforce central controls on internal and external (such as remote and mobile access) network traffic.

Chapter 3

Why Traditional Security Solutions Fail to Control Advanced Malware

In This Chapter

- Tracking the path of malware and exploits
- Discovering the hidden nature of advanced malware
- Hashing out signature-based detection
- Taking aim at targeted malware
- Breaking with traditional security solutions
- Understanding the need for a fully integrated security solution

Today's threat landscape renders traditional port-based firewalls, intrusion prevention systems (IPSs), and other security solutions largely ineffective at protecting an organization's networks, endpoints, and cloud environments.

In this chapter, you see how advanced malware has challenged traditional approaches made up of these legacy security devices beyond their capability to effectively protect the modern organization.

Rapidly Expanding Attack Vectors

In the past, exploits targeted servers and malware was delivered to end-users through email. These threats were largely independent and were handled in different ways. Today, exploits also target end-users and work hand in glove with a number of applications to deliver malware to users in unexpected ways. Sample applications include

- File transfer apps
- Instant messaging
- Webmail, as well as organizational email
- Social media platforms
- Microsoft Office
- Workflow and collaboration applications
- Software-as-a-Service (SaaS) applications

This means that attackers have far more insertion points for their attacks and an expansive arsenal of tools to use against those targets. To make matters worse, these applications often operate on a real-time model. Hardly anyone notices email delays as messages are inspected for malware on an email server prior to delivery. But now threats are streamed using browsers and any number of other application platforms that, if delayed, will elicit widespread complaints from users.

A Lack of Comprehensive End-to-End Visibility

A cyberattack is a well-orchestrated set of tools with a set flow comprising different capabilities. Isolated security solutions that lack the ability to communicate with other security solutions will only have visibility into one part or component of an attack, and will therefore be ineffective in preventing the attack.

In order to maximize their accessibility and use, many applications are designed from the outset to circumvent traditional port-based firewalls by dynamically adjusting how they communicate — often bringing malware along for the ride. Advanced malware has taken this trend and expanded upon it considerably. Simply stated, you can't control threats that you can't see, and advanced malware use a variety of tricks to hide its true nature or existence on the network and on endpoints, including

- **Nonstandard ports and port hopping:** Evasive applications are one of the key factors leading to the demise of traditional port-based firewalls. However, traditional IPS and threat products also rely heavily on port to determine which signatures or analysis to apply to the traffic. This weakness is magnified by the fact that APTs are often communicated from the inside of an infected network back to the remote attacker outside. This gives the attacker full flexibility to use any port, protocol, and encryption that he wants — fully subverting any port-based controls in the process.
- **SSL encryption:** Malware creators rely heavily on various forms of encryption to hide the infection of traffic, as well as the ongoing command-and-control traffic associated with malware. SSL is a favorite, simply because it has become a default protocol for so many social media sites, such as Gmail and Facebook. These sites are coincidentally very fertile ground for social engineering and malware delivery. As a result of SSL encryption, many IT security teams lack the ability to see malware traffic on their network. Other types of encryption have also become popular for hiding malware traffic. Peer-to-peer applications provide both infection and command-and-control capabilities, and often use proprietary encryption, again allowing malicious content to pass through the traditional network perimeter undetected.
- **Tunneling:** Tunneling provides yet another tool for attackers to hide malicious traffic. Many applications and

protocols support the ability to encapsulate private data being sent over a public network within other applications and protocols that are used on the network. This lets attackers disguise their communications as allowed services or applications to get past traditional perimeter security solutions.

- **Proxies:** Advanced malware and hackers use proxies to traverse traditional firewalls. This allows malware to not only protect its own communications, but also establish an anonymous network that anyone can use to hide his tracks while hacking or conducting other illegal activities.
- **Anonymizers and circumventors:** Tools such as UltraSurf, Tor, and Hamachi are purpose-built to avoid network security controls. Unlike most of the other technologies discussed in this section, circumventors have almost no legitimate use in an organizational network. These applications are updated on a monthly (and even weekly) basis to avoid detection in a perpetual cat-and-mouse game with traditional security solutions.
- **Encoding and obfuscation:** Malware almost always encodes transmissions in unique ways. Encoding and obfuscation not only help them avoid detection signatures, but also hide the true goal of the malware. This technique can be as simple as converting strings to hexadecimal, or as sophisticated as developing custom algorithms for detailed translations.

Finally, many new business applications also use these same techniques to facilitate ease of operation while minimizing disruptions for customers, partners, and the organization's own security and operations departments. For example, remote procedure calls (RPCs) and Skype use port hopping because it's critical to how the protocol or application, respectively, functions, rather than as a means to evade detection or enhance accessibility.

Fighting blind: The convergence of online services, SSL, and advanced threats

Online services are a well-established hub for social engineering, malware infection, and command and control. This broad category of applications includes online backup and storage services, social networking, web-based email, instant messaging, web-based file transfer, and a variety of blogs, message boards, and micro-blogging platforms such as Twitter. Today these applications have legitimate business purposes, so their use is justified, making it difficult for IT to simply block access to them.

As a group, these applications have become favorite targets for hackers because they provide easy, largely uncontrolled access to the weakest link in organizational security — the end-user. In particular, these applications provide many opportunities to gain the trust of a target user and offer a wealth of links, scripts, ads, and images, all of which can be used to exploit an unsuspecting user. Additionally, the very popularity of these applications makes it easy for an attacker's traffic to blend in with normal user traffic and traverse the network without suspicion. This characteristic is true for outbound as well as inbound traffic, with a variety of malware known to be using online services, micro-blogging, and message boards as command-and-control channels for the management of an ongoing intrusion.

In an effort to improve privacy for their users, many of these applications have begun to use SSL as a default protection for all traffic. This move to SSL has ironically taken a bad security situation and made it worse by encrypting the very channels that hackers are using to attack the network. Now, instead of trying to hide in plain sight or being forced to use a circumventor application that may draw unwanted attention, the attackers can simply ride within the SSL connection between the application and the target user. This provides a near-perfect platform for an attacker with a wealth of targets, a full complement of attack vectors, and built-in cloaking from security solutions.

Hash-Based Signature Avoidance

The traditional approach to detecting and blocking malware is based on the simple notion of collecting samples of malware and then writing a signature for that sample only. Even at its best, this approach has several drawbacks, such as the inherently long time to protection and high operational cost due to manually intensive processes, simply because of the reactive nature of the strategy. By design, protection can't be delivered until the malware is already "in the wild," during which time networks are vulnerable to the threat. In order to provide protection for networks, a sample of new or unknown suspicious traffic must be captured and identified before a detection signature can be created by security vendors. This means that some users and networks will be successfully breached by new malware until a new detection signature is created, downloaded, and enforced. This reactive model creates a window of opportunity for attackers, leaving networks vulnerable — sometimes for weeks or even months — until new malware is suspected, collected, analyzed, and identified. During this time, attackers have free reign to infect networks and users.

The lack of communication and information sharing among customers and vendors also allows malware to spread as the malware is "new" for every organization.

Advanced malware has taken this weakness and expanded upon it by evolving techniques to avoid being captured in the wild and to avoid the signatures that have already been created. Targeted malware, discussed in the next section, and polymorphism are increasingly common techniques used to exploit the inherent weaknesses of signature-based detection.

Payload-based signatures can detect multiple variants of malware, stopping even those variants that haven't been seen in the wild yet.

Targeted Malware

Before malware became a networked threat, the main goal was often to replicate and spread the malware as widely as possible. In fact, this is how the security industry ranked malware for many years — how many endpoints could the malware infect in a certain period of time. This widespread replication made new malware samples readily available and relatively easy to collect.

Advanced malware has changed that model, however. Advanced malware is more intelligent and highly networked, which enables an attacker to remotely control the target user(s). For savvy attackers, this means that they no longer need millions of infected users. Depending on the goal of the attack, even a single infected host may be enough for a skilled attacker to successfully infiltrate an organization.

In such cases, attackers have increasingly turned to highly targeted malware. These types of malware are often specifically designed for a particular user or network. Stuxnet is an example of targeted malware; it's designed to run only in a specific network with specific assets on the network. This approach accomplishes two very important things:

- It makes it extremely unlikely that a sample of the malware will be captured in the wild, because there are only a few samples to be caught instead of millions, making it unlikely that protective signatures will be generated and distributed.
- It's designed to avoid infecting networks that are not the intended target, and thereby avoids drawing unwanted attention to itself. This targeted approach is rapidly becoming a hallmark of some of the world's most sophisticated network attacks targeting intellectual property.

Traditional Network Controls Are Ineffective

Traditional network security solutions simply were never designed to meet the challenges of advanced malware. Traditional firewalls and IPS solutions classify traffic, a firewall allows or blocks traffic, and an IPS determines which signatures to apply, all based on port. As a result, a threat that is evasive and dynamic, such as advanced malware, can simply bounce to an unexpected port, gain access to the network, and avoid detection.

Firewalls

Port-based firewalls are often used as a first line of defense, providing coarse filtering of traffic and segmenting the network into different password-protected zones. One drawback to port-based firewalls is that they use protocol and port to identify and control what gets in and out of the network. This port-centric design is ineffective when faced with malware and evasive applications that hop from port to port until they find an open connection to the network. Such firewalls themselves have little ability to identify and control malware.

Solutions that have added antimalware capabilities to port-based firewalls either as a blade module or as a unified threat management (UTM) platform have typically suffered from poor accuracy and severe performance degradation.

Intrusion prevention

IPSs provide a step in the right direction, in that they look much deeper into the traffic than a traditional firewall does to detect network evasions and exploits that advanced malware may leverage. However, IPS solutions typically don't run a complete set of IPS signatures against all traffic. Instead, the traditional IPS attempts to apply the appropriate signatures to specific types of traffic, based on port. This limitation means that malware or exploits on unexpected or nonstandard ports are likely to be missed. Additionally, IPS solutions lack the depth of exploit detection needed to protect networks — most IPS solutions only look for a few hundred types of common exploits — well short of the tens of thousands that exist.

Effective IPSs utilize a mix of exploit-based signatures, which can be produced quickly but provide limited coverage, and vulnerability-based signatures, which take longer to create but provide coverage for a broad range of exploits. In most cases, IPSs provide interim or long-term protection for vulnerable servers, operating systems, and software within an organization's network infrastructure.

Proxies

Proxy solutions are another means of network traffic control. But they, too, look at a limited set of applications or protocols and only see a partial set of the network traffic that needs to be monitored. By design, proxies need to mimic the applications they're trying to control so they struggle with updates to existing applications and new applications. As a result, although proxies understand a few protocols in depth, they typically lack the breadth of protocol support needed to control the tunnels and protocols within protocols that hackers use to hide their true traffic. A final issue that plagues proxy solutions is throughput performance, caused by the manner in which a proxy terminates an application on the proxy and then forwards it on to its destination.

Endpoint protection

Endpoints are typically the initial target of an attack because they're relatively vulnerable due to the vast diversity of software applications and versions they run, and can thus provide an entry point to the network and access to data that an attacker wants. Legacy endpoint protection, such as host-based antivirus software, has the same weaknesses as other legacy signature-based technology, in that they can only detect malware that is already known — and are completely ineffective for detecting new, modified, or unknown malware threats. Additionally, endpoints such as users' laptops and mobile devices are often not protected by firewalls or IPSs when they're not connected to the organization's network, opening them up to attack when employees use them remotely.

Virtual and cloud protection

As virtualization and cloud computing strategies continue to be widely adopted, security technologies and solutions must evolve to protect these environments.

Within a virtualized data center (or private cloud), legacy port-based firewalls deployed at the network perimeter don't have visibility of more than 60 percent of all network traffic today — the east–west and intra-VM (virtual machine) communications between servers in the data center! Thus, malware threats and attackers are free to move laterally throughout the data center with little risk of detection.

Public cloud environments — including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) — introduce new attack vectors. For example, as SaaS applications like Box, Google Docs, and Salesforce become more widely used, the opportunity increases for attackers to use these applications in order to gain entry into a targeted organization. SaaS applications are convenient for users and require minimal infrastructure resources for organizations, which is a big part of their growing popularity. However, because organizations don't completely control these applications — access to them, security flaws within them, and the content uploaded and downloaded to them — these applications can potentially also be used to deliver and propagate malware and steal data.

And because there are very few purists in the world — and it's rarely practical — we have hybrid cloud environments that combine the best (and worst) of both public and private cloud environments! Thus, security solutions must be deployed strategically to address both public and private cloud attack vectors, in order to provide comprehensive protection of the organization's systems and data.

REMEMBER

Security policies must be based on the identity of users and the applications in use — not just on IP addresses, ports, and protocols. Without knowing and controlling exactly who (users) and what (applications and content) has access to the network and its various assets, networks may be compromised by threats that can easily bypass port-based network controls.

Crossing Legacy Security Silos

Over the years, organizations have tried to compensate for the inherent deficiencies in port-based firewalls by implementing a range of supplementary security devices, such as host-based solutions and standalone appliances.

Network versus host-based approaches

Traditionally, organizations have focused most of their antimalware time and resources either at the network level or at the end-users' desktops, typically in the form of host-based antivirus, personal firewalls, and the like. However, as malware evolves from individually infected endpoints to coordinated malware networks, organizations need to expand and coordinate their security perspective to incorporate both network- and endpoint-level intelligence and controls, following data wherever it resides, in an end-to-end, data centric approach to security. Network security has the unique advantage of allowing you to focus on the very trait that distinguishes advanced malware from earlier forms of malware — its reliance on communication with command-and-control servers. To twist John Gage's famous phrase, "the network is the computer," in a very real sense the threat itself has become a network. If your security measures don't operate at this same level, you run a very real risk of missing the forest for the trees.

Additionally, network security mechanisms provide an independent layer of monitoring and control, as cybercrime evolves and expands to new vectors. Advanced malware can include rootkits that gain root-level access to subvert antivirus protections or other security mechanisms on the target endpoint. This creates a paradox for the security team, because any security software running on a compromised host cannot truly be trusted. This certainly doesn't imply that host-based security is obsolete, but rather illustrates that blended threats against both the host and the network will likewise demand a security response that leverages the unique strengths of both the host and network security measures.

Integrating multidisciplinary solutions

Stopping APTs and cyberattacks requires an integrated, multidisciplinary approach to detect malicious traffic, correlate events, and respond accordingly in the network.

Many organizations have deployed various security solutions in addition to their legacy port-based firewalls, including IPSs, proxy servers, web-content filtering, antivirus gateways, and application-specific solutions — such as instant messaging or email security (antispam) appliances — in an effort to shore up their defenses against advanced threats.

However, this cobbled-together approach to security infrastructure creates problems of its own, such as the following:

- Not everything that should be inspected actually is, because these solutions either can't see all the traffic or rely on the same port- and protocol-based classification scheme as port-based firewalls.
- Information is not easily correlated, and the all-important context between events is lost due to security solutions being separated into their specialized silos.
- Policy management, access control rules, and inspection requirements are spread across multiple devices and consoles, making it difficult to develop and enforce a consistent security policy.
- Performance suffers due to relatively high aggregate latency because the same traffic is scanned and analyzed on multiple devices.

More security appliances don't necessarily mean a more secure environment. In fact, the complexity and inconsistency associated with such an approach can actually be a detriment to your organization's security. How? By overwhelming your security team with data from multiple sources that cannot be easily correlated and analyzed. Attackers are always looking for security gaps. In many cases, the more isolated single-function security solutions are in place, the more gaps there are.

Chapter 4

What Next-Generation Security Brings to the Fight

In This Chapter

- Addressing blind spots with innovative security solutions
- Keeping the organization safe from malware infections
- Finding the indicators of compromise already in the network

Next-generation security provides arguably the most important weapons in the fight against advanced malware — but if used in isolation, these solutions will fail to provide the visibility and control that modern organizations require. Put simply, if you don't fully analyze all available threat data, you can't protect your organization.

In this chapter, I propose a methodology to limit exposure to malware — as well as to detect and remediate network, endpoint, and mobile devices that may already be infected. I also discuss the importance of orchestration and correlation between different security solutions, such as the next-generation firewall and other innovative security solutions for endpoints and cloud environments, to ensure an effective and comprehensive security strategy.

The Next-Generation Firewall

By understanding the full stack behavior of all traffic on the network, you can finely control the behaviors that are allowed in the environment and eliminate the shadows that advanced malware uses to hide. Cyberattacks quite simply must talk in order to function. Finding these telltale communications is a critical component of controlling cyberattacks and the threats they pose.

A next-generation firewall performs a true classification of traffic based not simply on port and protocol, but on an ongoing process of application analysis, decryption, decoding, and heuristics. These capabilities progressively peel back the layers of a traffic stream to determine its true identity (see Figure 4-1). The ability to pinpoint and analyze even unknown traffic — without regard to port or encryption — is the defining characteristic of a true next-generation firewall and is invaluable in the fight against advanced malware, exploits, and other sophisticated threats.

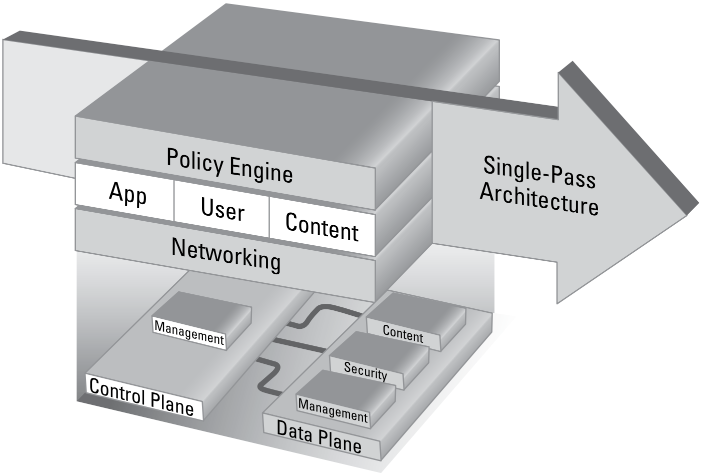

Figure 4-1: Traffic classification in a next-generation firewall.

Cybercriminals thrive on their ability to blend in with approved or "normal" traffic. The quality of your visibility into that traffic is one of your most critical assets.

Additionally, the next-generation firewall provides a fully integrated approach to threat prevention in a unified context: true coordination of multiple security disciplines (for example, application identity, malware and exploit detection, intrusion prevention, URL filtering, file type controls, and content inspection), as opposed to simply co-locating them on the same box. This integration provides a far more intelligent and definitive understanding of malware than any individual technology can provide by itself — and is needed in order to see and understand the telltale signs of unknown threats.

Preventing Infection with Next-Generation Firewalls

One of the most important steps that an organization can take to control advanced malware is to reduce attack vectors and eliminate the ability for malware to hide in the network. Today the majority of vectors used by malware are virtually unchecked, and malware traffic is typically small enough to easily blend into the background of "normal" network traffic. By regaining full visibility and control of exactly what traffic is allowed into the network and why, security teams can accomplish both of these goals.

Reduce the attack surface

Enforcing positive control is essential in the fight against malware. Positive control greatly reduces the attack surface and mitigates overall risk. Thus, an important first step for the organization is to return to a positive control model. Positive control simply means allowing only the specific applications and traffic you want, instead of trying to block everything that you don't want.

Positive control has long been a defining characteristic of network firewalls that separates them from other types of network security devices. But positive control also needs to extend to endpoints, mobile devices, and cloud environments alike. Your goal is to identify and reduce the attack and threat vectors across your entire environment and tailor protections — including private and public cloud segmentation, virtual firewalls, and SaaS applications — against each, while maintaining a consistent and effective security policy.

For example, if you want to permit Telnet, you allow TCP port 23 through your firewall. Unfortunately, traditional firewalls cannot properly delineate other applications and protocols that may also be using port 23. Applications and malware now use nonstandard, commonly open ports (for example, TCP port 80, 443, and 53) or simply hop between any available open ports to evade traditional firewalls.

Extending positive control to include all applications, irrespective of port, is not as easy as simply flipping a switch. Employees may use certain applications that don't have a readily apparent business value. Additionally, some applications may be used for both personal and work purposes. For example, Facebook can be used for social networking, but it has also become an increasingly important tool for many company marketing, sales, and recruiting initiatives.

As such, organizational IT security teams should consult appropriate groups and departments within the organization to determine approved applications and uses and to establish appropriate policies. These policies should allow only certain users to access specific applications, or limit the use of specific applications to certain approved features.

REMEMBER

To reduce the attack surface on the network, in virtual environments and on endpoints, organizations must

- Enforce positive control of all network traffic to prevent unnecessary or high-risk traffic, even when encryption or port evasion techniques are used to hide the traffic.
- Establish policies for approved applications and uses based on work needs and culture, by determining
  - What applications and protocols are in use on the network, on endpoints and in the cloud
  - What applications are required for work and who needs to use them
  - What dual-use or personal applications does the organization want to allow
  - What data can be shared across IT and non-IT applications
  - What devices can connect to your network and how you ensure that they comply with your security policies

Control advanced malware-enabling applications

Applications are an indispensable part of the cyberattack lifecycle, and are critical to both the initial infection of the target endpoint and the ongoing command and control of the attack. Invariably, applications and data can reside both within an organization's network and outside of it — on endpoints and within public cloud environments.

The association between malware and applications is not new. In the past, the de facto enabling application for malware was organizational email. From a security perspective, viruses and email simply went hand-in-hand. Although email is still used by attackers, it has lost some of its luster, as email security has become a focal point for many organizations. Attackers have shifted much of their attention to softer target applications that interact with users in real-time and provide far more threat opportunities. Attackers have gravitated to applications that facilitate social engineering while hiding the presence of compromise. Social networking and personal use applications meet both of these criteria, and are among the most common sources for malware infection and subsequent command and control (see Figure 4-2). These applications include social networking, web-based email, instant message (IM), peer-to-peer (P2), and file transfer. Additionally, targeted attacks will use more work-related protocols and applications, such as Microsoft Word documents and other non-executable files.

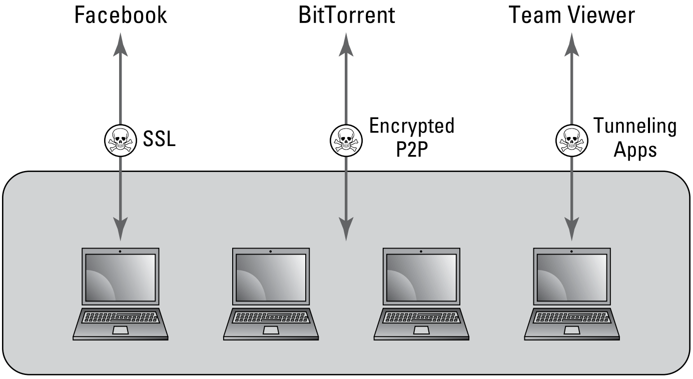

Figure 4-2: Preferred social networking/personal use applications and techniques for advanced malware.

WARNING!

Phishing attacks that utilize email applications are still heavily used by attackers to trick users into clicking malicious links or disclosing sensitive information.

These applications are designed to easily share information in a variety of ways, and people often use them with an implied trust and a more cavalier attitude because they may be accustomed to using them outside the office. This provides an attacker with a multitude of infection opportunities.

Control SSL in context

One of the main drivers for SSL-encrypted traffic is the need to protect communications to and from different sites and applications on the Internet. Twitter has recently joined the ranks of fellow social media giants Facebook and Google by moving to more widespread and default use of SSL to protect their end-users' information. Twitter recently announced that users can set a preference to secure all Twitter communication via HTTPS, which will in time become the default setting for the Twitter service. Such default SSL policies actually make it easier for malware to remain hidden by making it necessary to decrypt and inspect *everything* that traverses the network.

This shift to default SSL encryption highlights a very real and important challenge for organizational security that boils down to this:

- Web-based email applications, like Gmail and Yahoo! Mail also use SSL to encrypt communications, and are heavily used in both opportunistic and targeted attacks.
- Organizations that lack the ability to dynamically look within or enforce security on SSL-encrypted communications are more or less blind to this potentially malicious traffic.

The ramifications for organizational security are clear: If you can't control social media and webmail — and specifically applications that are SSL-encrypted — then you're leaving a clear path open for malware to get into and out of your network. The shift to SSL by default provides a moderate improvement in privacy for the users, but in the process makes the organization far more vulnerable to targeted attacks, lost data, and compromised systems.

Social applications also present an ideal environment for social engineering, enabling an attacker to impersonate a friend or colleague, for example, to lure an unsuspecting victim into clicking a dangerous web link. For all their sophistication, malware infections continue to rely on enticing an unsuspecting user into performing an ill-advised action, such as clicking a malicious link. Instead of opening an email attachment, the click may be a link in a tweet or on a Facebook page that appears to be from a friend. Cross-site scripting can populate dangerous links among friends, and packet sniffing technologies such as FireSheep allow attackers to take over social-networking accounts.

TIP

In addition to security tools and technologies, security awareness training and education for your end-users are critical components of a comprehensive security strategy, especially to defend against social-engineering tactics.

Actively test unknown files

Malware and exploits are easily and automatically modified or customized by attackers so that their attack will not trigger known signatures. This flexibility is one of the key technologies that allows an advanced attacker to gain a foothold within a target network without arousing the suspicion of security.

To address this shift by attackers, you need to integrate new technologies that can identify an unknown threat based on how it behaves, not simply based on how it looks. This sort of active, dynamic analysis can be performed by executing suspicious files in a *sandbox* (an environment where you can run and observe a suspect file to see what the file really does, providing a way of detecting new threats).

However, detection is only part of the battle. Enforcement against these threats is still needed in order to keep the network and its users safe. This makes it critical for the active analysis of malware to be tightly linked with the next-generation firewall, advanced endpoint protection and cloud-based security solutions (such as real-time threat intelligence) so that results of the analysis can be used for enforcement. Typically, in-line enforcements include

- Dynamic protections for newly identified unknown malware, zero-day exploits, and their variants
- Protections for related malware that may use the command and control servers or infrastructure
- Protections for threats that leverage the same command and control strategy
- Protections for threats that use related domains and URLs
- Reports of behavioral indicators of compromise (IoCs) for which to identify infected endpoints on the network
- Automated mechanisms to aid in remediation efforts

Control enabling applications by

- Blocking the use of known "bad" applications, or applications that have no legitimate purpose on your organization's network (such as P2P file-sharing and others)
- Limiting application usage to users and groups that have a legitimate and approved work need
- Disabling specific features in risky applications, such as file transfers, desktop sharing, and tunneling
- Preventing drive-by downloads from compromised web pages that automatically download malicious files without the user's knowledge
- Decrypting SSL traffic selectively, based on application and URL categories (for example, decrypting social networking and webmail, but not financial traffic)
- Inspecting and enforcing any risky application traffic that is permitted using Zero Trust network design and segmentation that will leverage next-generation firewalls, advanced endpoint protection, and SaaS application security, to provide truly integrated intrusion and threat prevention, malware protection, and URL filtering

Security best practices dictate that mission-critical applications and data be separated in secure segments on the network, based on Zero Trust principles ("never trust, always verify"). On a physical network, Zero Trust is relatively straightforward, using firewalls and policies based on application and user identity. In a cloud environment, direct communication between virtual machines within a server host occurs constantly, in some cases across varied levels of trust, making segmentation a real challenge. Mixed levels of trust, when combined with a lack of intra-host traffic visibility by virtualized port-based security offerings may weaken your security posture.

Prevent use of circumventors

Common end-user applications, including SaaS and web-based applications, can be co-opted by malware for use against the organization. Equally important, another class of applications is proactively designed to evade traditional network security. These applications include

- Remote desktop technologies
- Proxies
- Purpose-built circumventing applications

Some of these applications have valid work uses, while others are a sure sign of unauthorized and dangerous behavior. In all cases, they require tight control to prevent unmanaged threat vectors into the organization.

Remote desktop technologies are popular among end-users and IT support teams. Many web-conferencing applications have added the ability to remotely control a user's endpoint. Such technologies introduce two important risks:

- **When a user connects to a remote PC, he is free to surf to any destination and use any application without that traffic being inspected by the firewall.** In addition to circumventing policy, the remote desktop opens an unmanaged threat vector by allowing a user to remotely undertake all kinds of risky behavior and then have the results tunneled back to his endpoint inside the organization.
- **Remote desktop technologies potentially allow an unauthorized user to gain full access to an endpoint inside the trusted network.** This type of remote control is one of the first objectives of malware, and as such it creates a dangerous opportunity to launch an intrusion. According to Verizon's 2015 *Data Breach Investigations Report,* all the breached point-of-sale (POS) vendors in 2014 had their remote access credentials stolen.

Common applications that have valid uses within the organization can also create unintentional exposures if improperly used, or used by unauthorized or untrained users. For example, many IT departments use SSH to manage systems and applications in a data center. By opening a tunnel into the data center, SSH can provide direct, unmanaged access into an organization's most critical assets. These applications need to be tightly controlled, limited to approved individuals only, and closely monitored and logged.

Finally, a variety of web proxies and encrypted tunneling applications have been developed to provide secure and anonymous communication across firewalls and other security infrastructure. Proxy technologies such as CGIProxy or PHProxy provide a relatively easy way for users to surf securely without organizational control and have been found in more than 75 percent of networks. Applications such as UltraSurf and Tor are purpose-built to traverse security infrastructures and are regularly updated in order to remain undetected. These applications have very few, if any, valid uses within the organization, and their presence generally indicates an attempt to avoid security. These tools not only pass traffic without being inspected, but they also tend to be used for high-risk behaviors, such as file sharing or accessing expressly blocked content and sites that, in turn, carry a significantly higher risk of malware infection. These applications should be blocked in almost all cases.

Prevent the use of circumventors by

- Limiting remote desktop use, for example, to IT support personnel only
- Securely enabling SSH but preventing SSH tunneling
- Blocking unapproved proxies and encrypted tunnels, such as UltraSurf and Hamachi

Investigate any unknown traffic and traffic patterns

When an organization has regained positive control and has the ability to inspect and accurately classify approved traffic on its network, it can examine any remaining unknown traffic on the network. Malware and APT traffic often appear as “unknown” due to their unique behavior and use of proprietary encryption.

Unlike traditional firewalls that typically pass any traffic that uses an approved port, a next-generation firewall provides the ability to find and analyze unknown traffic in the network. Unknown traffic regularly sent by the same client endpoint should be investigated to determine whether it’s being generated by a legitimate application that is not recognized or by a potential malware infection. Security teams can also investigate where the traffic is going:

- Does it go out to known malicious websites or to social-networking sites?
- Does it transmit on a regular schedule?
- Does someone attempt to download or upload files to an unknown URL?

Any of these behaviors can indicate the presence of malware on the client endpoint. Using a next-generation firewall to accurately identify traffic on the network, “unknown” traffic should become increasingly rare, thus enabling potentially malicious traffic to be quickly found and analyzed.

Increasingly, the next-generation firewall goes beyond analyzing unknown traffic and can even automatically analyze unknown files in a sandbox environment to identify the malicious behaviors of threats. This allows you to focus on unknown files and unknown traffic. Unknowns on the network need to be investigated, identified, and managed. You can quickly and systematically manage unknown traffic and traffic patterns by

- Applying a policy on the firewall to block all unknown traffic, or allow and inspect it
- Monitoring traffic to unknown URLs and blocking downloads or uploads on those sites
- Blocking traffic to malicious URLs
- Determining what internal applications exist on the network, and either applying an application override (renaming the traffic) or creating a custom signature
- Analyzing unknown or suspicious files in a sandbox to uncover malicious behaviors

- Using packet captures (PCAP) to record the unknown traffic and submit it to your security vendor
- Utilizing behavioral malware reports and other forensics or reporting tools to determine whether the traffic is a threat

Investigate "unknown" traffic for potential unauthorized user behavior or malware activity:

- Track source, destination, and volumes of unknown traffic.
- Correlate against URL, IPS, malware, and file-transfer records.
- Define custom application IDs for any internal or custom applications, as needed.
- Deliver PCAPs to your security vendor for further analysis and identification.

Finding Infected Hosts with Next-Generation Firewalls

Even with the best of controls, endpoints may inevitably be infected with malware — perhaps through a new type of malware, an unknown vector, or a USB drive. Sandbox analysis takes time. During this gap from unknown to known, malware has proven time and again that it is possible to infect even the most heavily secured systems. Thus, it's prudent to assume endpoints will be infected and develop the skills necessary to find infected endpoints in the network. This can be a challenging task, given that the malware may have already avoided traditional malware signatures and may already have root-level access on an infected endpoint.

To pinpoint infected endpoints, your focus must shift from malware signatures. Instead, you need to analyze unusual or unknown behaviors that are observed on the network. Communication is the Achilles' heel of advanced malware. It must communicate in order to function and must be difficult to find and trace. These basic requirements create patterns that can be used to identify malware traffic or behaviors that stand out from the normal network traffic — even if the malware is completely new and unknown. Integrating endpoint protection that can prevent exploits and malware with next-generation firewalls can provide an additional layer of context around traffic analysis, as well as act as a safety net so that infection is far less likely to take place, even if malware makes it through network defenses.

The result of sandbox analysis should include reports on unique behavior patterns and other information observed during execution and infection, that is delivered to security teams and, most important, to security enforcement products. This capability will help security teams pinpoint malware on infected endpoints more effectively and prevent future spread.

One example of this is the use of information on new malicious CnC domains and URLs. A sandbox or threat intelligence feed can determine new malicious communication channels, and security teams can actively look for endpoints that have connected to them for positive indications of compromise.

Find command-and-control traffic

One of the major advantages of a next-generation firewall is its ability to classify potentially complex streams of traffic at the application level. This includes the ability to progressively scan within traffic and peel back protocols running within protocols, until the true underlying application is identified. The ability to identify complex traffic is crucial to detecting the unique command-and-control communication of advanced attacks. For all intents and purposes, a malware file is an application and its unique traffic can be identified and blocked by a true next-generation firewall.

Automate tracking and correlation

The techniques described in the previous sections are crucial, but many organizations don't have the time or resources necessary to conduct manual investigations. Innovative security solutions like next-generation firewalls and advanced endpoint protection can collect real-time information and other indicators of compromise (IOC), and automate the tracking and correlation of behaviors with intelligent capabilities.

For example, next-generation firewalls can provide threat information about

- **Unknown TCP/UDP:** APT traffic is often encrypted and unknown. Tracking unknown TCP and UDP activity is a great starting point for finding infected endpoints.
- **Dynamic DNS (DDNS):** Malware will often use DDNS to bounce traffic between multiple infected hosts with an ever-changing list of IP addresses, making it very difficult to track the true source and destination of malware.
- **Known malware sites:** The URL filtering engine of a next-generation firewall constantly tracks sites that have hosted malware whether intentionally or unintentionally.
- **Recently registered domains:** Malware often uses new domains as it moves around to avoid detection and to recover. Repeated visits to a newly registered domain are not conclusive but may be evidence of an infection.
- **IP addresses instead of domain names:** Advanced malware often uses IP addresses, as opposed to normal user (human) browsing that typically prefers friendly URL addresses.
- **IRC traffic:** IRC traffic is one of the most well-known communication methods for malware, and provides additional evidence of a malware infection.

After identifying these indicators, acting on them quickly is important. This can be accomplished through native integration, technical partnerships, and open APIs that feed the correlated information above to remediation solutions. Automated processes can then quarantine the suspected compromised endpoint until security teams can investigate and take further action as appropriate.

Chapter 5

Creating Advanced Threat Protection Policies

In This Chapter

- ▶ Developing effective governance
- ▶ Applying policies and controls to protect mobile users and devices

Far too often, technical solutions are implemented without considering the implications for an organization's overall security strategy. To avoid this mistake, it's important to ensure that your policies are up to date and the technology solutions you're considering support a comprehensive security strategy.

This chapter describes the different types of controls that must be considered in an organization's security policies.

Safe Enablement through Smart Policies

The purpose of security policies is to reduce the risk of being infected by advanced threats in the first place. But, as discussed in Chapter 1, even the most secure networks with the best security policies are inevitably susceptible to malware and attacks in some way. Likewise, you have to assume that your network will eventually be compromised, no matter how well designed your policies are, and plan accordingly. Chapters 3 and 4 cover techniques for detecting and stopping infection before it becomes a full-blown breach.

Your security policy must help your organization control malware and reduce risks, while also meeting your organizational requirements. Creating effective security policies requires a keen understanding of the risks posed by the various applications and features used in your network, the business needs of the organization, and your users' work requirements.

IT must play an active role in defining smart policies that enable an organization's users and mitigate risk, but it's important for IT not to be the sole owner of these policies — visible executive support is critical. Adoption of new applications in organizations tends to start from the users themselves, not from policies. But once these applications become integrated into organizational processes and workflows, rooting them out and creating security policies for them after the fact can be extremely difficult to do — even with executive support.

For example, in a heavily regulated environment such as stock trading, the use of instant messaging may be subject to retention and auditability rules. IT's role is to educate the traders on the security risks of instant messaging tools, participate in the development of the acceptable use policy (AUP), and subsequently monitor and enforce its use. In this example, that policy could prevent the traders from using Facebook and MSN chat for instant messaging, but enable an internal chat server instead.

REMEMBER

Governance and management work best if they're based on a set of smart policies, processes, and training, developed by the four major stakeholders in the organization's network landscape: IT, HR, executive management, and the users. Clearly IT has a role to play, but it can't be the strictly defined role that it often plays. Neither can IT be lax about its role as the enabler and governor of applications and technology. Even if IT leads the efforts to create and promote secure procedures and practices, the other three stakeholders should play a part in training employees to be aware of risks and vigilant about potential attacks.

Application controls

Enablement is about knowing and understanding users and their behaviors, and applications and their associated risks. In the case of certain applications that are needed for work but not necessarily controlled by IT (such as social media or online storage), the users have long since decided on the benefits — and are, far too often, oblivious to the threats and risks. As a result, it's vital to match users' needs with the most appropriate applications and features, while also educating users about the implicit risks of those applications and features.

Enabling Facebook usage while protecting the organization

Facebook is rapidly extending its influence from the personal world to the corporate world, because employees now use these applications to get their jobs done. At the same time, many organizations are looking at the nearly 1.1 billion Facebook users as an opportunity to conduct research, execute targeted marketing, gather product feedback, and increase awareness. The end result is that Facebook can help organizations improve their bottom line.

However, formally enabling the use of Facebook introduces several challenges to organizations. Many organizations are unaware of how heavily Facebook is being used, or for what purpose. In most cases, policies governing specific usage are nonexistent or unenforceable. Finally, users tend to be too trusting, operating in a "click now, think later" mentality that introduces significant security risks.

Like any application that is brought into the organization by end-users, blindly allowing Facebook usage may result in propagation of threats, loss of data, and damage to the organization's reputation. Blindly blocking Facebook usage is also an inappropriate response because it may play an important role in the organization and may force users to find alternative means of accessing it (such as proxies, circumvention tools, and others). Organizations should follow a systematic process to develop, enable, and enforce appropriate Facebook usage policies while simultaneously protecting network resources:

1. **Find out who's using Facebook.**

   There are many cases in which a "corporate" Facebook presence may already be established by marketing or sales, so it's critical that IT determine which social networking applications are in use, who is using them, and the associated organizational objectives. By meeting with the business groups and discussing the common organizational goals, IT can use this step to move away from the image of "always

(continued)

(continued)

saying no" and toward the role of business enabler.

2. **Develop an organizational Facebook policy.**

   After Facebook usage patterns are determined, an organization should engage in discussions regarding what should and should not be said or posted about the organization, the competition, and the appropriate language. Educating users on the security risks associated with Facebook is another important element to consider when encouraging usage for work purposes. With a "click first, think later" mentality, Facebook users tend to place too much trust in their network of friends, potentially introducing malware while placing personal and organizational data at risk.

3. **Use technology to monitor and enforce policy.**

   The outcome of each of these policy discussions should be documented with an explanation of how IT will apply security policies at a granular level to safely and securely enable the use of Facebook within organizational environments. For example, access to Facebook might be permitted, but certain high-risk behaviors, such as uploading or downloading files, may be restricted or blocked. As Facebook moves to SSL encryption, organizations should strongly consider decrypting traffic to and from Facebook.

Documenting and enforcing a social-networking usage policy can help organizations improve their bottom line while boosting employee morale. An added benefit is that it can help bridge the chasm that commonly exists between the IT department and business groups.

Application enablement typically includes restricting the use of unneeded high-risk applications while managing allowed applications to reduce the inherent risks they may bring with them. Establishing effective policies requires open dialogue among users, IT, and management to truly understand which applications have legitimate work uses and value. Certain applications are known to be conduits for malware, both in terms of infection and ongoing command and control. Peer-to-peer applications, such as BitTorrent, are iconic examples.

On the other hand, many applications are not definitively good or bad (black or white), and will instead land in a gray area of an organization's security policy. These applications may have organizational value but can also carry considerable risk. Safe enablement should be the goal for these applications. In this case, applications can be allowed but constrained to only allow needed features while blocking higher-risk features. For example, an organization may enable a web meeting application, but not allow the remote desktop capability that could allow a remote attacker to take control of a machine. Enabling policies could also limit certain applications or features to specific approved users, or could scan the application to ensure that no unapproved files or content is being transferred. The ultimate goal is to eliminate or limit the risk in the application, not the application itself.

TIP

Application controls should be part of the overarching organizational security policy. As part of the process of implementing an application control policy, IT should make a concerted effort to learn about new and evolving SaaS and web-based applications. This includes embracing them for all their intended purposes and, if needed, proactively installing them or enabling them in a lab environment to see how they act. Peer discussions, message boards, blogs, and developer communities are also valuable sources of information.

User controls

Most companies have some type of application usage policy, outlining which applications are allowed and which are prohibited. Every employee is expected to understand the contents of this application usage policy and the ramifications of not complying with it, but there are a number of unanswered questions, including

- Given the ever-growing numbers and types of applications, how will an employee know which applications are allowed and which are prohibited?
- How is the list of unapproved applications updated, and who ensures that employees know the list has changed?
- What constitutes a policy violation?
- What are the ramifications of policy violations — a reprimand or termination of employment?

The development of policy guidelines is often a challenging and polarizing process. Determining what should be allowed and what should be prohibited while balancing risk and reward elicits strong opinions from all the major stakeholders.

Further complicating the process is the fact that new applications and technologies, including SaaS and web-based applications that are not within the control of IT, are often adopted within an organization long before appropriate policies governing their safe and appropriate use are ever considered or developed.

REMEMBER

Documented employee policies and end-user training need to be key pieces of the application control puzzle, but employee controls as a stand-alone mechanism are insufficient for safe enablement of new and evolving applications. In addition to policies and training, IT needs the tools and ability to monitor and control these applications — for example, to prevent users from uploading private customer information or sensitive data, instead of leaving such decisions to user discretion.

Network controls

Given that advanced threats most often use the network for infection and ongoing command and control, the network is an obvious and critical policy-enforcement point. Network segmentation needs to be implemented with firewalls, at the boundaries of different user or data divisions, to ensure traffic can be inspected as it traverses different network segments. With application-enablement policies in place, IT can shift its attention to inspecting the content of allowed traffic. This inspection often includes looking at traffic for known malware, command-and-control patterns, exploits, dangerous URLs, and dangerous or risky file types. When possible, policies that focus on the content of traffic should be coordinated as part of a single unified policy, where the rules (and the results of those rules) can all be seen in context. If content policies are spread across multiple solutions, modules, or monitors, piecing together a coordinated logical enforcement policy becomes increasingly difficult for IT security staff. Understanding whether these policies are working after they're implemented will likewise be difficult.

The goal should be to create written policies that reflect the policies' intentions just like someone might describe them orally. For example, "Only allow designated employees to use SharePoint; inspect all SharePoint traffic for exploits and malware; disallow the transfer of files types X, Y, and Z; and look for the word *confidential* in traffic going to untrusted zones."

This kind of whitelisting is an important component in preventing malware from moving laterally and infecting other systems. If policies are properly implemented, every time malware attempts to move it has a high probability of being detected and stopped because of access restrictions and alerts on attempted policy violations.

Another key component of network policies is the absolute need to retain visibility into the traffic content. SSL is increasingly used to secure traffic destined for the Internet. Although this may provide privacy for that particular session, if IT lacks the ability to look inside the SSL tunnel, SSL can also provide an opaque tunnel within which malware can be introduced into the network environment. IT must balance the need to look within SSL against both privacy requirements for end-users and the overall performance requirements of the network. For this reason, it is important to establish SSL decryption policies that can be enforced selectively by application, URL category, and user group. For example, social media traffic could be decrypted and inspected for malware, while traffic to financial or healthcare sites is left encrypted. Alternatively, traffic for specific applications may be decrypted for the Sales and Marketing teams, but left encrypted for HR.

Endpoint controls

The end-user's machine is the most common target for advanced malware and is a critical point for policy enforcement. Endpoint policies must incorporate ways of ensuring that antivirus and various host-based security solutions are properly installed and up to date.

Similarly, you need to have a method for validating that host operating systems are patched and up to date. Many malware infections begin with a remote exploit that targets a known vulnerability in the operating system or application. Thus, keeping these components up to date is a critical aspect of reducing the attack surface of the organization.

However, maintaining system updates on endpoints can be difficult. In 2014 alone, more than 10,000 new common vulnerabilities and exposures (CVEs) were reported. That's a lot of patching! Additionally, some operational environments cannot afford the system downtime needed to apply a patch.

As with employee policies, desktop controls are a key piece to the safe enablement of applications in the organization. Desktop controls present IT departments with significant challenges. Careful consideration should be applied to the granularity of the desktop controls and the impact on employee productivity. The drastic step of desktop lockdown to keep users from installing their own applications is a task that is easier said than done *and,* if used alone, will be ineffective. Here's why:

- Remotely connected laptops, Internet downloads, USB drives, and email are all means of installing applications that may or may not be allowed on the network.
- Completely removing administrative rights is difficult to implement and, in some cases, severely limits end-user capabilities to an unacceptable level.
- USB drives are now capable of running applications, so a web-based application, for example, can be accessed after network admission is granted.

Many of today's readily available legacy endpoint protection products are often single-faceted, providing only virus detection and removal, for example. These products rely upon the same techniques that have been unsuccessfully employed for more than 20 years.

Newer endpoint security suites often incorporate antimalware, personal firewalls, host-based intrusion prevention, and cloud-based signature updates, but still fail to adequately protect the endpoint against today's advanced threats.

Signature-less endpoint controls offer a safety net for these situations. When exploits or malware attempt to execute on endpoints, these controls identify specific properties of malicious behavior common to all threats, and prevent them from being carried out.

Advanced endpoint protection takes a more comprehensive approach that fully integrates with other security solutions, such as next-generation firewalls, real-time threat intelligence, and security information and event management (SIEM).

Advanced endpoint protection requires a different mindset from traditional security methodologies. Rather than a reactive *detect* and *respond* approach as with traditional anti-malware software, advanced endpoint protection employs a proactive *prevention* strategy. Advanced endpoint protection must do the following:

- Prevent all exploits, including those utilizing unknown zero-day vulnerabilities
- Prevent all malware, without requiring any prior knowledge of specific malware signatures
- Provide detailed forensics against prevented attacks, in order to strengthen all areas of the organization by pinpointing the targets and techniques used
- Be highly scalable and lightweight to seamlessly integrate into existing operations with minimal to no disruption
- Integrate closely with network and cloud security for quick data exchange and cross-organization protection

Addressing Mobile and Remote Users

That the modern organization has and continues to become far more distributed than in the past is no secret. Users simply expect to be able to connect and work from any location, whether at an airport, at a coffee shop, in a hotel room, or at home. Increasingly, organizations are accepting this new reality with permissive bring your own device (BYOD) and bring your own app (BYOA) policies. This change means that more and more workers and data may be beyond the physical perimeter of the organization, and thus also beyond the protections of traditional perimeter security solutions. The key is to build a security architecture that doesn't treat these mobile or remote users as exceptions; they need the same application, user, and content protections when they're outside the perimeter that they would receive when they're inside.

Building consistency into the architecture of the network requires careful planning and is a must for any security policy to address the realities of modern computing.

Similarly, security policies must address the use of endpoint devices other than standard equipment issued by the organization. Users working from home may use their own personal computers, which are increasingly as likely to be running Apple OS X as they are to be running Windows. Other devices used to remotely connect to the organization's networks include smartphones, tablets, and iOS devices, such as iPhones and iPads. All these devices must also be addressed in order to prevent blind spots in your organization's security policies.

WARNING!

Mobile malware has also become a major threat. As mobile devices grow more powerful, they'll increasingly be used as replacements for PCs, storing vast amounts of personal — and valuable — data that is largely unprotected.

Chapter 6

Ten Things to Look for in a Cybersecurity Solution

In this chapter, we provide ten recommendations to help you evaluate which cybersecurity solutions are best for your organization!

Enforce Allowed Interactions Between Your Data and Users

To reduce the number of attacks to which your network and data are exposed, your cybersecurity solution must allow you to granularly identify approved interactions between users and data based on the specific data you're trying to protect — what it contains, where it's located, how it should be used, and by whom.

Choosing a solution that enables micro-segmentation is also important. Each network location likely behaves somewhat differently, and thus each requires a slightly different set of allowed behaviors. Identify and group users according to their privilege levels and to which data they should have access. The policies that you construct must be enforced within the context of applications traversing the network and their expected interactions. Granular network access policies are the foundation to reducing the attack surface and to blocking unauthorized transactions, as they provide the most fundamental context around incoming and outgoing traffic.

Identify Threats Everywhere and Always

Data is constantly in transit to and from both physical and virtual locations via a slew of different ports, protocols, and applications. Machine-to-machine communication represents a vector for lateral movement that's rarely monitored, creating opportunities for attackers. Data moves back and forth from things like security cameras, VMs in the cloud via SaaS applications, POS devices, and printers — all of which have been used by attackers to sail past traditional defenses and gain a foothold within the target organization.

Complete, end-to-end threat identification for all applications, users, and devices in all locations, on and off the organization's network, is imperative for an effective cybersecurity strategy.

Protect Data at Multiple Stages in the Attack Lifecycle

Stand-alone security tools, like traditional intrusion prevention system (IPS) or web proxies that focus solely on one stage of the attack lifecycle may fail, especially where new or unknown techniques are used. An effective prevention strategy includes coordinated technologies that detect and prevent across each stage and easily block known and unknown threats to ultimately stop attackers from reaching their objective.

TIP

Choose a cybersecurity solution that focuses on attack behaviors at multiple stages: blocking delivery through compromised web pages and malicious files, protecting against exploits kits and application vulnerabilities, stopping the execution of files (installation) containing known malware through accurate payload identification, shutting down outbound command-and-control communication, and restricting lateral movement through segmentation.

Attack surface reduction, combined with full visibility and prevention mechanisms at each stage, guarantees that as an attack progresses through each attack stage — even those that use new techniques — there is a decreasing probability it will succeed and an increasing likelihood that your network will remain secure.

Outsmart Threats Designed to Outmaneuver Security Tools

Cybersecurity tools that offer protection capabilities in the form of static signatures that are too broad or too unique are limited in that they can only protect against threats that are known — known malware delivered by a known malicious URL using a known exploit, communicating to a known command-and-control domain. It's incredibly easy for attackers to modify existing malware and exploits to make them essentially "unknown" to bypass traditional defenses. These minor variations in threats create moving targets for security tools with static protections. What's more, malicious URLs and command-and-control domains come and go quickly, often only remaining active for a few hours or days at a time.

The sheer number of exploit and malware variations available necessitates protection capabilities that can handle the load, either by an enormous and constantly growing library of exploit and hash-based signatures, or by a smaller set of payload-based signatures capable of detecting and preventing multiple variations individually. Smart signatures capable of uncovering threats deep within each packet and file and comprehensively across many protocols, file types, exploits, and hashes offer increased protection, as well as future protection against variation and reuse of the same attack components.

Translate New Intel into Protections in Security Policies

In 60 percent of attacks, it takes only minutes for compromise to occur. This infection speed necessitates the quick translation of data into intelligence, and then into protections that are enforced, allowing you to prevent network and device infection in near real-time and rely less on manual research-and-remediate processes.

Prevent gaps in prevention capabilities by quickly translating intelligence, such as new malware payloads, URLs hosting exploits, and command-and-control server locations, into protections that can be enforced by existing security technologies across your network.

Consider a solution that is self-learning to automate this process. A constant feed of newly created protections against newly discovered attacks, broken down into its components, translated into protections, and distributed to points of enforcement within your segmented network, increases the effectiveness of your cybersecurity solution.

Get Intel and Protection against the Latest Attacks

Threats are constantly changing as attackers evolve their methods in a continuous effort to be more deceptive and evasive. The rate at which attacks are changing dictates that what protected your network against attacks this morning may not be effective against attacks being launched in the next few minutes. Keeping prevention capabilities within your security technologies as current as possible helps to minimize risk of infection and restricts attackers to threats containing pristine, zero-day exploits and malware, and brand-new command-and-control domains. This seriously increases their cost to attack and severely limits their opportunities for success, resulting in fewer attacks for you to deal with.

Attackers are automating new threats, so your data-to-protection process must also be automated in order to stay ahead of the evolution.

Enable Quick and Accurate Mitigation

After being hit by a sophisticated attack, it's critical to identify the infection quickly and protect other devices and network segments against its spread. Because most network defenses comprise best-of-breed tools from multiple vendors, prevention becomes difficult. The process is arduous, highly manual, and time consuming — especially if threat data is isolated in different systems and stored in different locations.

Infection doesn't necessarily mean you've been breached. If you're able to prevent outbound communication with attackers (command and control), you've effectively stopped the attack, even though you may still need to identify and scrub the infected device. In addition to bolstering prevention capabilities, technologies that ingest a constant feed of threat information can help. Where remediation is concerned, every minute counts.

Consider a solution that correlates suspicious behaviors to highly accurate infection alerts, so you know that infection has taken place and can prioritize accordingly to limit exposure. Many attackers will try to leverage uncommon — and therefore likely undefended — attack vectors, so any threat analysis tool must also cover all locations and devices within your infrastructure.

Coordinate Actions across Individual Security Technologies

Security technologies and individual sensors contain information-gathering and enforcement capabilities that, if built to work together, have the power to make your efforts to secure the organization more effective. Being able to identify what's going on in a given attack stage and correlate it to create a larger picture of the attack as a whole is essential to effectively stopping it. The big picture sets the context of the attack for understanding where gaps in security may exist, where protections must be created, and distributing enforcement to block the attack and close those gaps.

Coordinated cybersecurity technologies are of great importance when it comes to usability and closing security gaps in your infrastructure. Technologies that are natively integrated, or have open APIs that can be easily integrated, are best suited to comprehensively share intelligence and update policies across your entire network, and immediately alert you to infection, regardless of location.

Keep Your Organization Running

Many organizations struggle when it comes to choosing between securing the organization and enabling the thousands of applications that accelerate efficiency and productivity. Turning on security protections often means users must accept high latency or be restricted from using the applications or accessing the data they need.

Reducing the attack surface is a key to maintaining usability. Eliminating unknown or unnecessary traffic and data interactions reduces the amount of traffic that must be scanned for threats, which lightens the processing load that your cybersecurity tools must take on.

Given the requirement for computationally intensive tasks (for example, application identification and threat prevention performed on high-traffic volumes), your cybersecurity solution must provide dedicated, specific processing for management, security, and content scanning, so traffic isn't processed more than once.

Be Easy to Use

Manually integrating data from different products can be an arduous process, often introducing mistakes and imperfect end results. As each additional hour passes after compromise occurs, infection spreads, and the likelihood that you'll need to disclose a breach to your executives and board members increases. You can't afford the extra time associated with arduous monitoring, investigation, and reporting.

Look for a cybersecurity vendor who correlates security data both at a local level (so you know exactly what's going on in your network and can respond accordingly) and at a global level (providing you with actionable intelligence on threat campaign details).

Glossary

advanced persistent threat (APT): An Internet-borne attack usually perpetrated by a group of individuals with significant resources, such as organized crime or a rogue nation-state.

adware: Pop-up advertising programs that are commonly installed with freeware or shareware.

APT: *See* advanced persistent threat.

backdoor: Malware that enables an attacker to bypass normal authentication to gain access to a compromised system.

BitTorrent: A P2P file-sharing communications protocol that distributes large amounts of data widely without the original distributor incurring the costs of hardware, hosting, and bandwidth resources.

bootkit: A kernel-mode variant of a rootkit, commonly used to attack computers that are protected by full-disk encryption.

bot: A target machine that is infected by malware and is part of a botnet (also known as a zombie).

botnet: A broad network of bots working together.

Box: A SaaS-based online storage application that employs SSL encryption. It's frequently used by corporate organizations so that users can upload, download, and share files publicly and privately.

DDNS: *See* dynamic DNS.

DDoS: *See* distributed denial-of-service.

distributed denial-of-service (DDoS): A large-scale attack that typically uses bots in a botnet to crash a targeted network or server.

drive-by download: Software, often malware, downloaded onto a computer from the Internet without the user's knowledge or permission.

dynamic DNS (DDNS): A technique used to update domain name system (DNS) records for networked devices in real time.

Internet relay chat (IRC): An application layer protocol that facilitates near real-time communication in a client–server networking model.

IPsec: An open-standard protocol used for secure VPN communications over public IP-based networks.

IRC: *See* Internet relay chat.

logic bomb: A set of instructions secretly incorporated into a program so that if a particular condition is satisfied, the instructions will be carried out, usually with harmful effects.

malware: Malicious software or code that typically damages or disables, takes control of, or steals information from a computer system. Broadly includes viruses, worms, Trojan horses, logic bombs, rootkits, bootkits, backdoors, spyware, and adware.

master boot record (MBR): Information contained in the first sector of a storage device that identifies how and where an operating system is located so that it can be loaded into memory.

MBR: *See* master boot record.

next-generation firewall (NGFW): A firewall beyond traditional port-based controls that enforces policy based on application, user, and content regardless of port or protocol.

NGFW: *See* next-generation firewall.

Nmap: A security scanner used to discover network hosts and services.

packet capture (PCAP): An API for capturing network packets.

PCAP: *See* packet capture.

RDP: *See* Remote Desktop Protocol.

Remote Desktop Protocol (RDP): A proprietary Microsoft protocol that provides remote access to a computer.

rootkit: Malware that provides privileged (root-level) access to a computer.

Secure Shell (SSH): A set of standards and an associated network protocol that establishes a secure channel between a local computer and a remote computer.

Secure Sockets Layer (SSL): A transport layer protocol that provides session-based encryption and authentication for secure communication between clients and servers.

Skype: An online service that offers instant messaging, voice, and video calls using voice over IP (VoIP) communication methods.

Simple Mail Transfer Protocol (SMTP): An Internet standard for email transmission that uses TCP port 25.

SMTP: *See* Simple Mail Transfer Protocol.

spear phishing: A targeted phishing attempt that seems more credible to its victims and thus has a higher probability of success. For example, a spear-phishing email may spoof an organization or individual that the recipient actually knows.

SSH: *See* Secure Shell.

SSL: *See* Secure Sockets Layer.

SYN: TCP synchronization bit.

TCP: *See* Transmission Control Protocol.

Transmission Control Protocol (TCP): A connection-oriented protocol responsible for establishing a connection between two hosts and guaranteeing the delivery of data and packets in the correct order.

Trojan horse: A program designed to breach the security of a computer system while ostensibly performing some innocuous function.

UDP: *See* User Datagram Protocol.

User Datagram Protocol (UDP): A connectionless-oriented protocol often used for time-sensitive, low-latency communications that don't require guaranteed delivery.

web widget: A small application that an end-user can install and run within a web page.

Restore positive control of your network applications and keep your organization safe!

Advanced malware has evolved over the past decade, and this new breed of highly targeted attacks has become one of the pre-eminent threats to today's enterprise. Understanding the lifecycle of an advanced attack and its framework is critical to employing effective technologies such as next-generation firewalls and security controls to protect your organization data and users. With cybercriminals motivated by far more than notoriety and attacks that are increasingly sponsored by criminal organisations and rogue nation-states, the stakes have never been higher!

- ***How advanced threats enter your organization* — and how to stop it in its tracks by breaking the attack lifecycle**
- ***How malware uses popular applications and SSL to evade security* — and why this has become a preferred method for infecting hosts**
- ***Why traditional security controls are blind to today's threats* — and why you need a fully intregrated, multidisciplinary approach to security**
- ***What next-generation security brings to the fight* — and how to protect your organization from advanced threats**

Lawrence C. Miller, CISSP, has worked in information security for more than 20 years. He is the coauthor of *CISSP For Dummies* and a dozen other titles. He is also a Palo Alto Networks customer and liked it so much he bought the company — well, he's not that rich (yet) — but he did write this book!

Open the book and find:

- **How advanced malware infects enterprises**
- **Why traditional security can't protect you**
- **How next-generation security succeeds where other security solutions fail**
- **What steps to take to protect your organization from targeted attacks**

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

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-119-25028-9
Not for resale